Provisioning Circuit Emulation Services

EPN Manager 2.1

Job Aid

Copyright Page

Provisioning Circuit Emulation Services Job Aid

Contents

Basics

Overview

Introduction

While many of you still provide and support the transport networks and TDM and SONET/SDH services that your customers require, the reality is that these networks and their supporting hardware are aging out of the marketplace rapidly.

With support and parts harder to find or non-existent, and extraordinary capital expenditures in space, power, and maintenance to keep them running, you need to modernize while continuing to support these services.

By using a circuit emulation solution, your company can migrate legacy services to packet network technology while maintaining those services in their current states.

Circuit emulation encapsulates the legacy services traffic in containers that new technologies can recognize and manage, while accurately maintaining packet timing and service quality.

The Cisco© circuit emulation solution combines:

- **Cisco Network Convergence System (NCS) 4200 series chassis**
  By using high-density circuit emulation technology, the chassis can convert TDM and SONET/SDH services to pseudowires that transport these services over a packet core.
- **Cisco Evolved Programmable Network Manager (EPN Manager)**
  By using the network management system, operators can provision circuit emulation services while meeting strict quality and control standards.

By using this approach, your company is:

- Modernizing network hardware to support current network technologies and legacy transport networks and services.
- Maintaining legacy TDM services and their timing and quality requirements seamlessly during and after the hardware transition.

And, as your customers move to newer services and technologies, you can turn down legacy services, on demand.

This job aid introduces you to circuit emulation provisioning concepts and processes in Cisco EPN Manager and the steps that you can take to provision circuit emulation services.

Traffic Engineering (TE) Tunnel and Circuit Emulation (CEM) Provisioning

When provisioning circuit emulation (CEM) to support a service, you can begin by provisioning a bidirectional traffic engineering (TE) tunnel, also referred to as a Flex LSP.

By provisioning the TE tunnel, you are configuring the primary, or working, path that the CEM service will use to route the legacy traffic, including:

- The source and destination devices that act as the ingress and egress points for the traffic at each end of the tunnel.
- The bandwidth that defines the traffic capacity.

During this process, you have options to configure:

- Any alternate path or paths on which to route designated traffic in the event of a failure in the working path and how the system manages the alternate routing, referred to as protection type.
- Additional attributes that determine how the system provisions and manages the tunnel and its alternate paths, and routes traffic on those paths.
- Any additional devices that the working path, and any alternate paths, must include or exclude when routing traffic, referred to as constraints.

When the TE tunnel is provisioned and running in the system, you then can provision services, which includes assigning applicable services to the TE tunnel that you provisioned.

Tip: Cisco recommends that you assign circuit services to new or already existing TE tunnels as a best practice.

TE tunnels define key routing attributes that the services will follow.

TE Tunnel Provisioning Pre-Requisites

Administrative Pre-Requisites

To prepare devices to support TE tunnels, administrators need to:

- Configure the OSPF and ISIS routing protocols on all of the devices that operators can provision TE tunnels.
- When configuring more than one device, enable traffic engineering on all of the device links that operators can use for TE tunnel provisioning and ensure they are operationally up.
- Ensure that all source and destination devices on which operators can provision TE tunnels must be reachable.
- Configure the MPLS core network and ensure reachability among source and destination devices.
- If using Cisco NCS 4200 devices with the software version 3.18 service pack installed, run the **sdm prefer ipv4 command** in the global configuration mode on the device.

Note: Executing the command causes the device to restart automatically.

Operational Pre-Requisites

Before provisioning TE tunnels, operators need to validate that:

- The system has completed collection of the device inventory.

CEM Provisioning Pre-Requisites

Administrative Pre-Requisites

To prepare devices to support circuit emulation services, administrators need to configure:

- The CEM loopback settings on the interfaces that you will be provisioning.
- Based on device type, the interface CEM settings for the SONET, SDH, PHD, HOP, or HOP controllers by setting the controller modes.
- The working and backup interface groups that you will use to provide automatic protection switching (APS) for the service.
- The clocking mode, which ensures that the source and destination endpoint times are synchronized.

Note: For detailed instructions on preparing for CEM provisioning, refer to the **Cisco Evolved Programmable Network Manager User and Administrator Guide**.

Operational Pre-Requisites

Before provisioning CEM services, operators need to validate that:

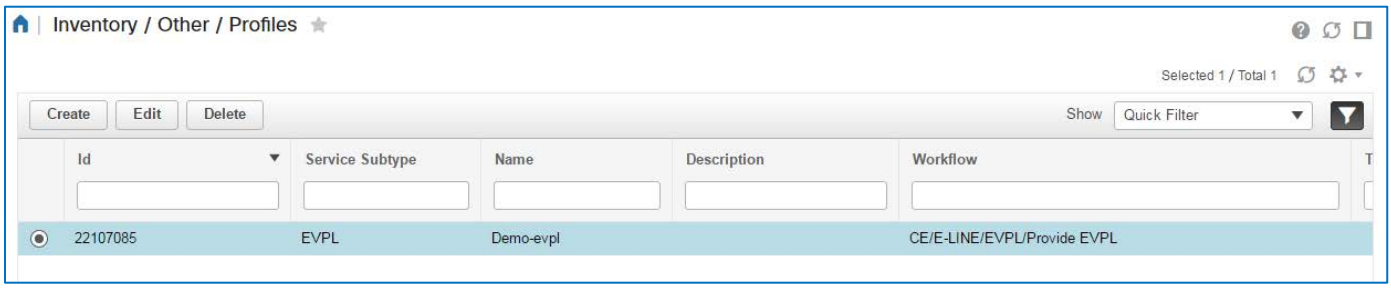
- IP/MPLS connectivity is enabled on the device interfaces that support the source (A) and destination (Z) endpoints for the circuit.
- The system has completed collection of the device inventory.

Optional TE Tunnel or CEM Provisioning Pre-Requisites

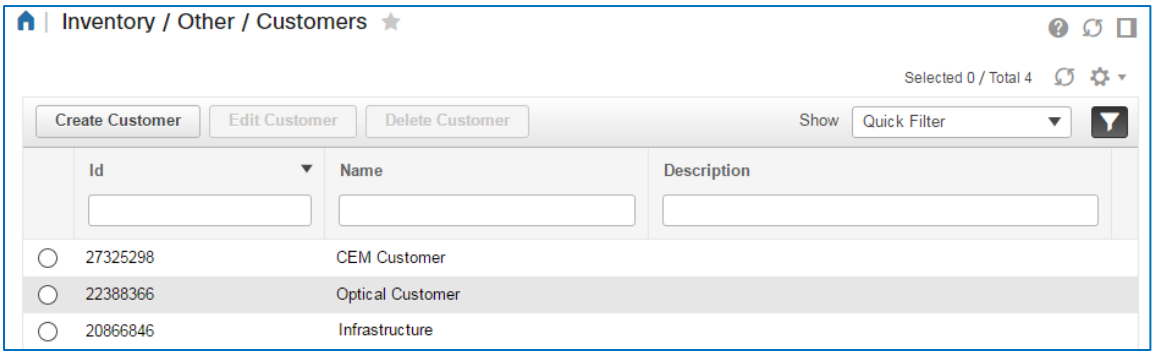
To prepare for TE Tunnel or CEM provisioning, operators also can configure the following items:

- To automate and expedite service provisioning, users can configure profiles.

  When there are common sets of configurations that users provision on a regular basis, they can define those parameters in profiles to automate and expedite complex provisioning tasks.

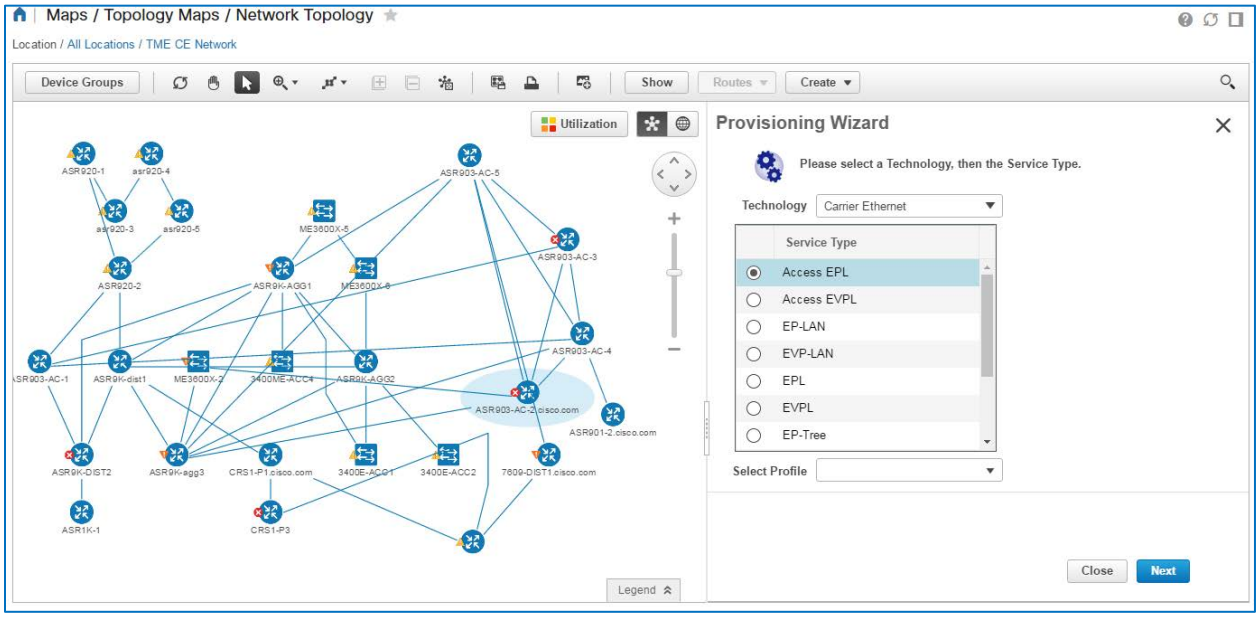


- To identify the customers using the service, operators can configure customer identifiers, which include a unique ID number, the customer's name, and descriptive details.



The Provisioning Wizard

You use the **Provisioning Wizard** to provision circuit emulation services.

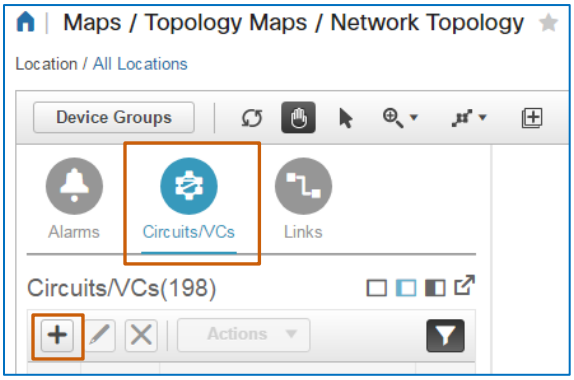


You can access the **Provisioning Wizard** in several areas of the application, including by using:

- The **Network Topology** map.
- The **Circuits/VCs & Network Interfaces** page.
- The **Configuration | Service Provisioning** menu link.

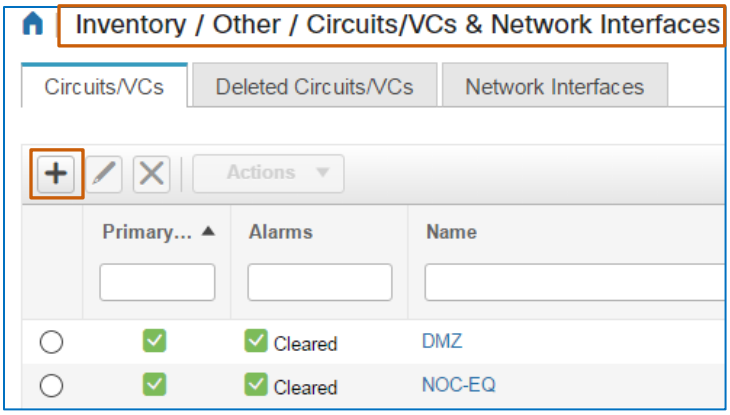
On the Network Topology map, to open the Provisioning Wizard:

- On the **Circuits/VCs** tab, on the toolbar, click **Create**.



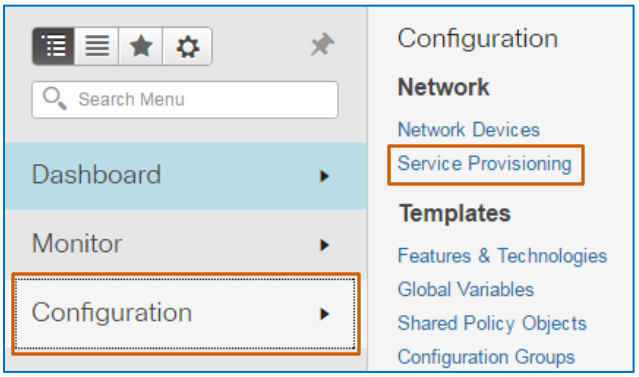
On the Circuits/VCs & Network Interfaces page, to open the Provisioning Wizard:

- On the **Circuits/VCs** tab, on the toolbar, click **Create**, which navigates you to the **Network Topology** map and opens the **Provisioning Wizard**.



On the Configuration menu, to open the Provisioning Wizard:

- Click **Service Provisioning**, which navigates you to the **Network Topology** map and opens the **Provisioning Wizard**.



Skills

To perform this task, you need to be a provisioner with the following experience.

Proficient

- EPN Manager navigation and behaviors

Expert

- Networking and provisioning concepts
- MPLS traffic engineering tunnel concepts
- Circuit emulation services, technologies, and concepts
- Cisco NCS 4200 series device hardware configuration

Terms

SONET/SDH

For more information on SONET and SDH in optical networks, refer to the Cisco© TechNote.

Supporting a Customer's Legacy Traffic

Use Case Scenario

ABC Media Group, a platinum customer, has requested a dedicated path between its primary location and a key branch site through the network core to avoid mixing with external traffic.

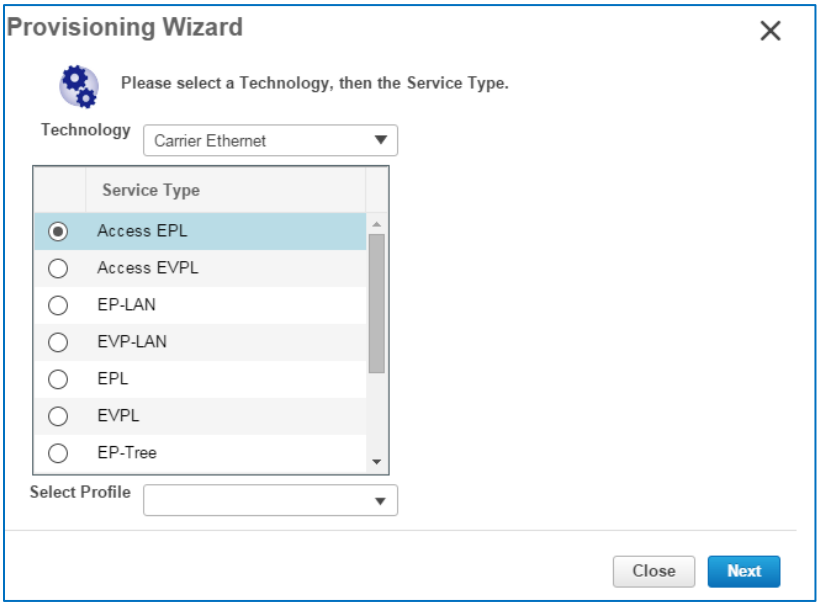
The customer is continuing to use legacy TDM services. At the same time, to keep technology up-to-date, the network is running NCS 4200 series devices.

To transport the customer's TDM traffic on a dedicated path through the network core, you plan to:

- Provision a tunnel between the two provider edge NCS devices.
- Provision a T1 service on each provider edge device endpoint by using circuit emulation, which encapsulates the legacy traffic on arrival and transports it between the more modern devices on the network.
- Assign the T1 service to a tunnel that you provisioned to support the customer's business need.

To start this use case:

- Based on your location in the application, open the **Provisioning Wizard**.



Process Overview

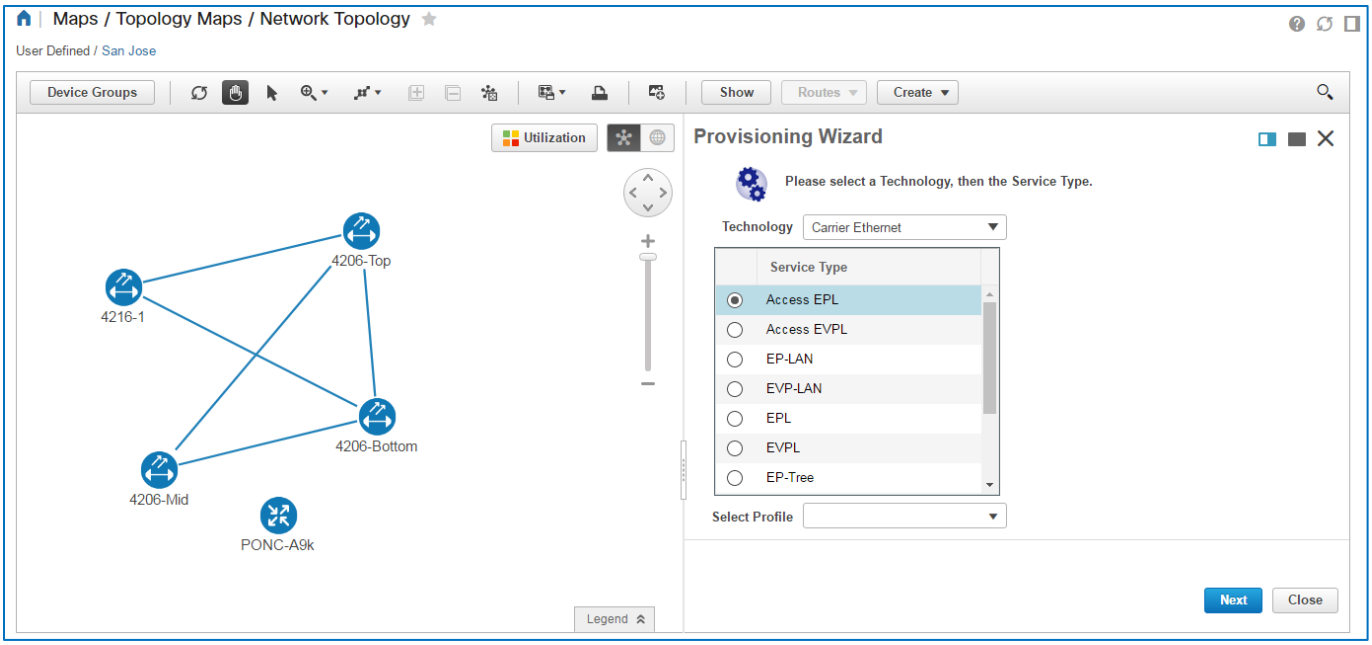
To complete the use case, follow these steps:

1. With the applicable device group open on the map, in the **Provisioning Wizard**, select the **MPLS TE** technology, and then provision the tunnel service.
2. When the system provisions the tunnel successfully and with the applicable device group open on the map, in the **Provisioning Wizard**, select the **Circuit Emulation** technology, and then provision the service.

Process Steps

In this case, to prepare for provisioning the circuit emulation service that will manage the customer's legacy traffic, we are provisioning a dedicated traffic engineering tunnel, which is an **MPLS TE** technology.

With the applicable device group and the **Provisioning Wizard** are open, you are ready to begin. The first page of the wizard populates with the **Carrier Ethernet** technology and service types by default.



Task 1: Provision the Traffic Engineering (TE) Tunnel

You begin the process by identifying the technology and service type, and the overarching service characteristics.

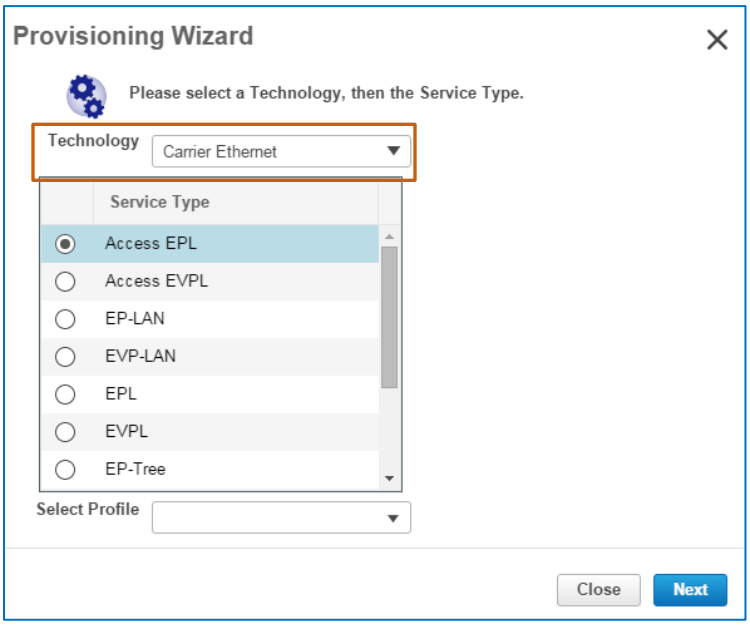
Subtask 1: Identify the Technology and Service

Important Note: While many of the steps to identify a technology and service are similar, there are key differences based on specific technology and service type that you are provisioning.

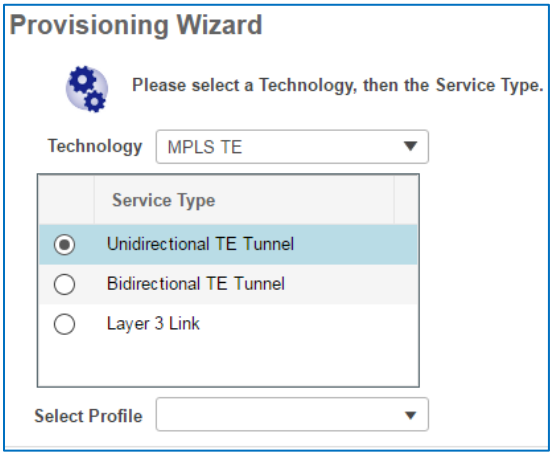
For best understanding, review all of the steps in these tasks, which provides a constructive overview of the types of settings that you can expect to configure.

Based on the use case, follow these steps:

1. In the **Technology** drop-down list, select **MPLS TE**.

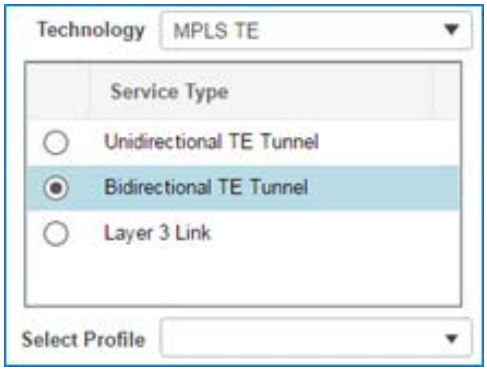


The page updates and displays the **Service Type** list.



2. To indicate the type of MLPS traffic engineering configuration, in the **Service Type** list, select the configuration.

   In this case, to support the configuration of a tunnel to support the T1 service for two-way traffic, we selected the **Bidirectional TE Tunnel** service type.

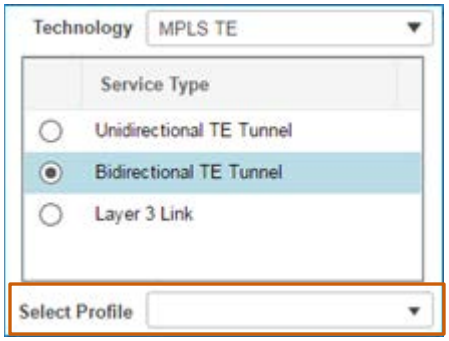


3. In the **Select Profile** drop-down list, accept the default selection, which is blank, or select a profile.

Note: When provisioning tasks include common sets of configurations that users provision on a regular basis, they can define those parameters in profiles to automate and expedite complex provisioning tasks.

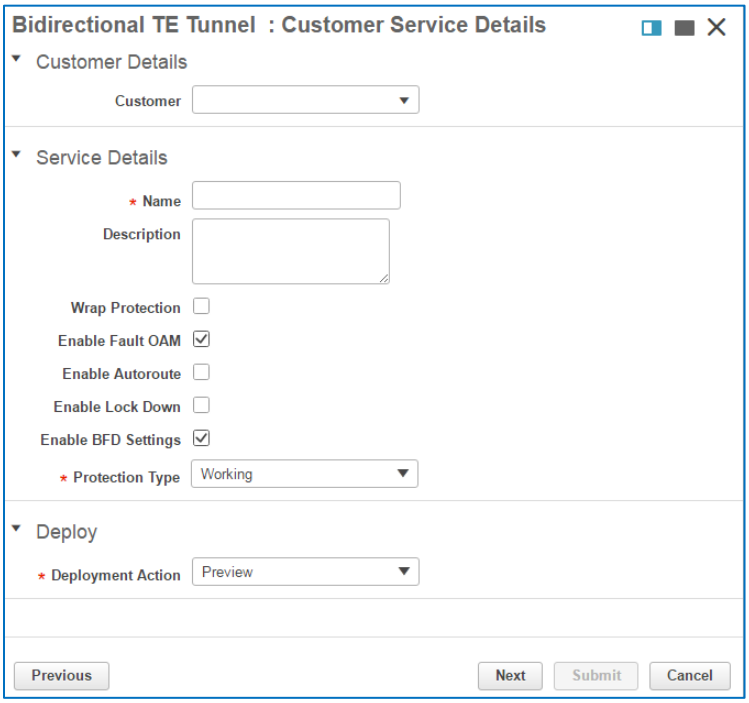
Then, users can apply an applicable profile based on the circuit that they need to provision by using **Select Profile**.

When you are configuring services manually, you do not need to select a profile.



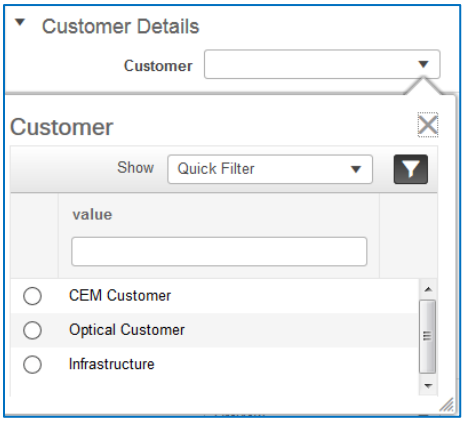
4. To configure the service details, click **Next**.

The **Customer Service Details** page opens.



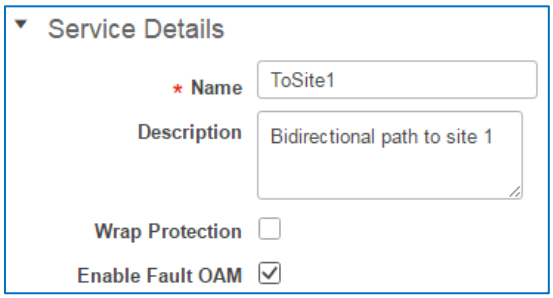
5. Optionally, to identify the customer who will use the service, when applicable, in the **Customer Details** section, in the **Customer** drop-down list, select the name of the customer.

Note: TE tunnels can support numerous services securely for disparate customers and traffic, which commonly makes assigning a customer inapplicable.

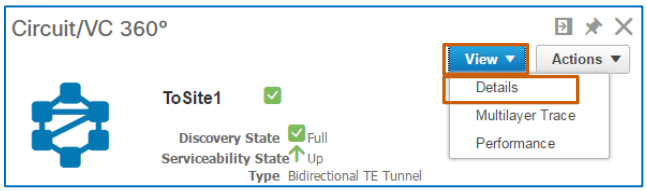


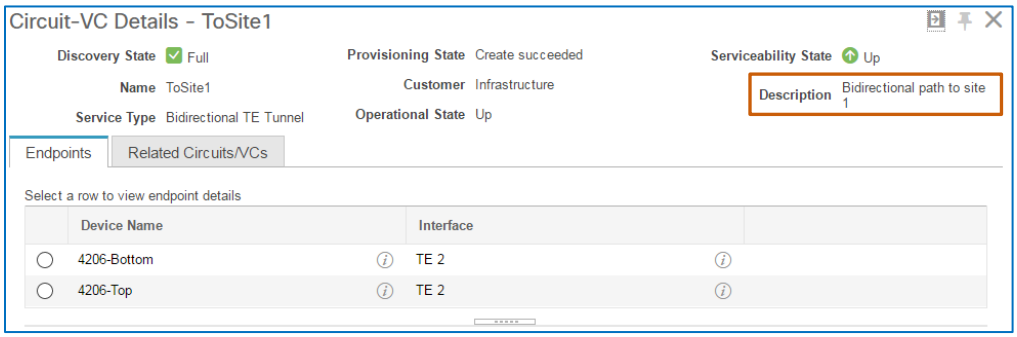
a. In the **Service Details** section, in the **Name** field, type a name for the circuit that makes its use recognizable.

b. To indicate the use of service, optionally, in the **Description** field, type additional information about the service based on operational or business requirements.



Note: When you add a description, it appears in the **Circuit/VC 360⁰** pop-up window details.





6. Optionally, in a working path failure scenario, to ensure that traffic continues to adhere to the SONET 50 millisecond standard restoration time while the system serially transitions traffic from the working path to a protected path, select the **Wrap Protection** check box.

Important Note: In order to support wrap protection, you must:

- Configure the tunnel endpoints on NCS 4200 series or ASR 900 series devices.
- Include a protected or a restore path when you configure the protection type in step 12 below.

Note: When you do not apply wrap protection, the system transitions traffic to the protected path, but cannot guarantee the ability to meet the SONET 50 millisecond standard restoration time.

7. Optionally, to enable the Operations, Administration, and Management (OAM) protocol for fault management, which supports metrics reporting in various application areas, accept the default selection of the **Enable Fault OAM** check box.

Tip: Fault OAM metrics reporting helps support operators who proactively monitor the network. The function verifies that the tunnel is up and running by exchanging messages between endpoints and supports fault reporting when verification fails.

8. Optionally, when provisioning unidirectional tunnels, to ensure that the system consistently routes traffic between endpoints by using only the tunnel that you are provisioning, select the **Enable Autoroute** check box.

Important Note: Cisco recommends that you enable automated routing when provisioning unidirectional tunnels.

Automated routing constrains the pseudowires and related CEM services to use the tunnel by indicating that it is the optimal path for traffic.

This constraint also ensures that traffic is being handled based on the settings that you are configuring for the tunnel.

When you do not enable automated routing, the devices do not force the routing protocol to indicate that the tunnel is the optimal path for traffic to use.

9. Optionally, if you are configuring a tunnel at least one alternate path, to allow the system to manage a working path failure scenario effectively, select **Enable Lock Down**.

Note: When the working path fails, the system automatically begins working to establish an alternate route.

If you also configure an alternate path, such as a protected path, the system also responds to a working path failure by rerouting traffic to the protected path.

If you do not have lock down enabled, and the working path failure corrects itself during failover to the protected path, the system works to reestablish traffic on the working path, which creates an inefficient traffic management situation.

With lock down enabled, the system reroutes traffic to the protected path and does not attempt to return the traffic to the working path if it becomes operational during the failover.

When the working path becomes operational either during or after failover, failback to the working path does not occur automatically.

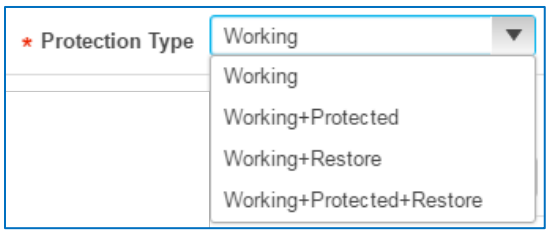
Important Note: For lock down enablement to be useful include a protected path or a restore path, at minimum, when you configure the protection type in step 12 below.

10. To configure bidirectional forwarding detection (BFD), which exchanges messages between the two tunnel device endpoint interfaces to confirm that each can contact the other, accept the default selection of the **Enable BFD Settings** check box.

Note: This setting provides an additional level of detection to determine that device endpoints remain in communication.

You can configure message and down notification intervals in subtask 2.

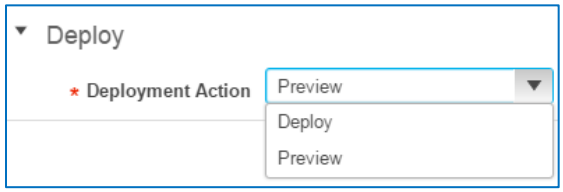
11. To configure the working, or primary, path, and optionally, one or more alternate paths on which to route traffic in the event of a failure on the working path, in the **Protection Type** drop-down list:
    - To configure a working path without any alternate paths, select **Working**.
    - To configure a working path with one or more alternate paths, which act as backups to the working path, select another option in the list.



Note: For detailed information on the types of alternate paths that are available for TE tunnels and their routing behaviors, refer to the **Cisco Evolved Programmable Network Manager User and Administrator Guide**.

Tip: Keep in mind that the types of protection that you configure also consume bandwidth. Consider such items as how often the path is used and the type of traffic that it manages to determine whether you need backup paths, and if so, the configuration for optimal backup route management.

12. To configure what you want to occur when provisioning is complete, in the **Deployment Action** drop-down list:



- To configure the system to present a preview of the CLI code that it will deploy to the endpoints before deploying it, accept the default selection of **Preview**.

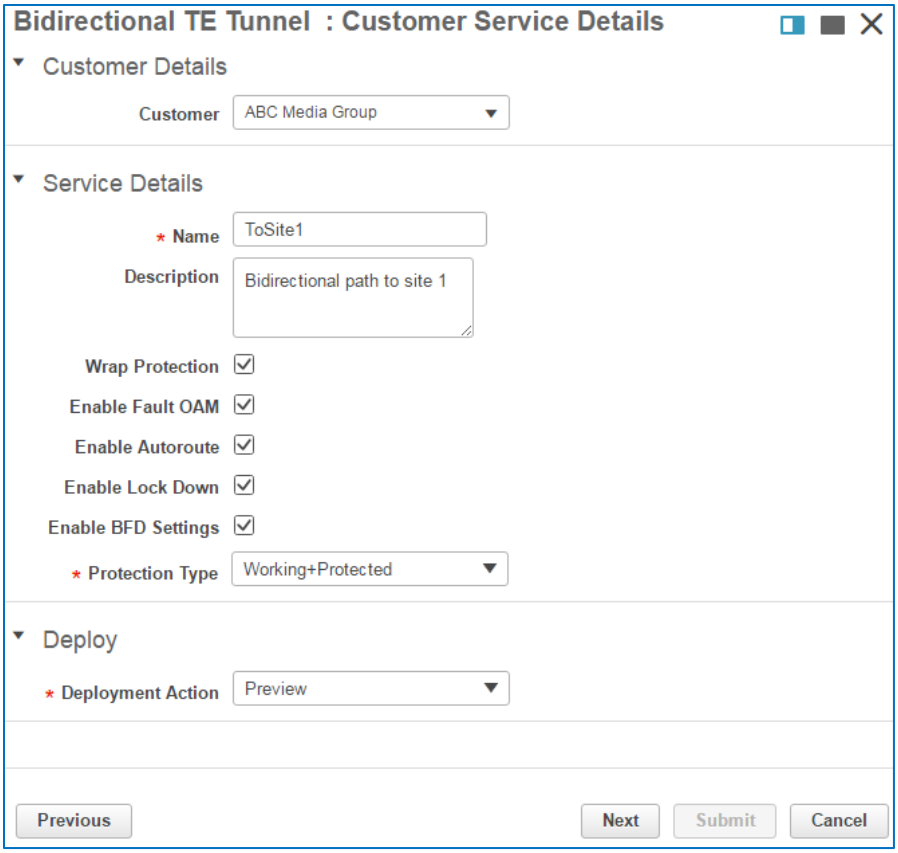
Tip: Cisco recommends that you preview CLI code before deploying the configuration. This approach helps you to avoid unexpected results or operational issues.

When you determine that you need to make changes, you can cancel provisioning at this point, and make the corrections that you need.

- To configure the system to deploy the configuration to the endpoints immediately without reviewing the CLI code, select **Deploy**.

13. To configure the tunnel endpoints and attributes, click **Next**, and then go to subtask 2.

In this case, we are provisioning the tunnel for the use of single customer, and applying all of the protection and reporting settings to help ensure tunnel integrity during and after provisioning.

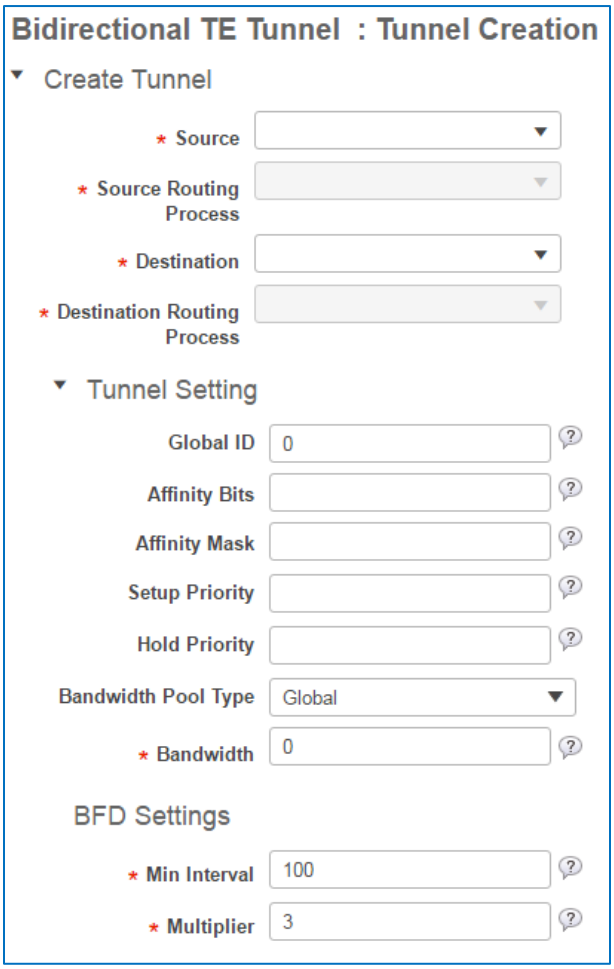


Subtask 2: Configure Tunnel Endpoints and Attributes

At this point, you indicate the source (**A**) and destination (**Z**) endpoint devices. These devices are the ones on which you need to provision the CEM service.

You have additional control of tunnel attributes, which refine the tunnel path and define how the system prioritizes the tunnel among other tunnels using the same endpoints,

You configure the tunnel endpoints and attributes on the **Tunnel Creation** page.



To configure tunnel endpoints and attributes, follow these steps:

1. To indicate the source endpoint device, on the **Tunnel Creation** page, in the **Create Tunnel** section, in the **Source** drop-down list, select the device.

   On the map, the system applies the **A** icon to the device icon of the device that you selected.

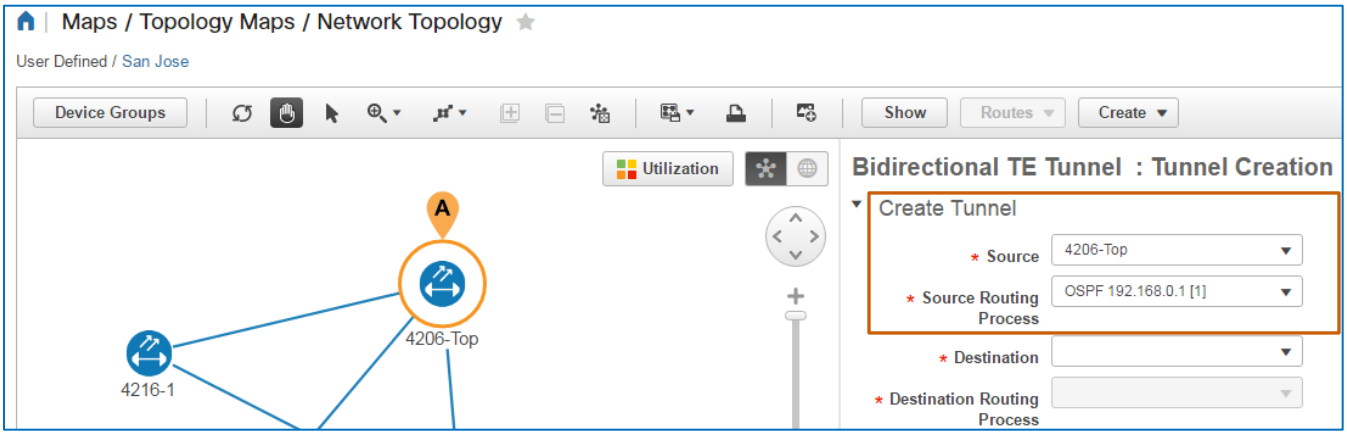
   Tip: Alternately, to populate the **Source** field, you can click a device icon on the map.

   The system then populates the **Source** and **Source Routing Process** fields automatically.

   Based on the device type that you select, in the **Source Routing Process** drop-down list, the system can populate the applicable routing protocol automatically or provide options from which you can select.

   Note: An administrator must configure the routing protocol on the source and destination devices before you can provision tunnels on the devices or the process will fail.

   For more information, refer to the list of administrative pre-requites for TE tunnels.



2. To configure the destination endpoint device, in the **Destination** drop-down list, select the device, which populates or provides options in the **Destination Routing Process** field based on the device type.

3. To configure tunnel attributes, in the **Tunnel Setting** section:

Note: The attributes that you configure in the tunnel settings apply to all of the paths (working, protected, restore) that you are configuring for the tunnel.

- Optionally, to configure a unique identifier that the endpoints recognize, in the **Global ID** field, accept the default or type the identifier number.

Important Note: The system provides a default identifier of 0, which allows the system to apply a unique number on the back end.

- Optionally, to have the tunnel signal the interface to determine whether to include or exclude that network segment as part of its path:

Important Note: When configuring affinity for the tunnel, the device interfaces that comprise the tunnel must have traffic engineering affinity configured.

For more information, refer to the tunnel configuration administrative pre-requisites.

  - To identify the tunnel segment by matching the bit values in the hexadecimal positions that you type here with the affinity bit values preconfigured on the interface, in the **Affinity Bits** field, type the value in hexadecimal format.
  - To indicate whether the tunnel includes or excludes the network segment identified by the affinity bit value that you typed in the **Affinity Bits** field, in the **Affinity Mask** field:
    - To include a network segment, type **1** at each position in the hexadecimal where the affinity bit that you typed above matches the affinity bit configured on the interface.
    - To exclude a network segment, type **0** at each position in the hexadecimal where the affinity bit value does not match the affinity value on the interface.
- Optionally, to configure the priorities that the tunnel has in relationship to any existing tunnels that use, or future tunnels that will use, the same endpoints:
  - To configure the tunnel to have a higher priority during initial tunnel provisioning, in the **Setup Priority** field, type a value that is less than 7, which is the default value.
  - To configure the tunnel to have a higher priority after the tunnel is established, in the **Hold Priority** field, type the value that is less than 7, which is the default value.

Note: For more information on setup and hold priorities, refer to the **Cisco Evolved Programmable Manager User and Administrator Guide**.

- To indicate whether the tunnel uses only available bandwidth or has access to additional bandwidth due to peaking traffic, in the **Bandwidth Pool Type** drop-down list:
  - To indicate that the tunnel use available bandwidth without an overage, accept the default selection of **Global**.
  - To indicate that the tunnel requires a subpool, which provides additional bandwidth when traffic is peaking above the set bandwidth level, select **Subpool**.

Important Note: When you configure a subpool, you are implying that the traffic is important enough to consume additional bandwidth from a reserve pool, as needed, to travel successfully on the tunnel.

As a best practice, apply a high (lower value) setup or hold priority for a tunnel with a subpool, which helps ensure that its traffic will not be blocked by other tunnels with higher priority settings.

- To define the maximum amount of bandwidth that the tunnel traffic can consume, in the **Bandwidth** field, type the amount in kilobytes.

Important Note: When determining bandwidth, consider the amount of traffic, including all services and related sizes, that might be assigned to the tunnel.

The tunnel bandwidth must be large enough to accommodate the anticipated traffic and its overhead, while not be overly large.

If the tunnel is not large enough for traffic, at some point, a pseudowire associated with a service will not have the size it needs and provisioning will fail.

Overly large tunnels can result in unutilized bandwidth.

If you accept the default of 0, the tunnel cannot support traffic.

- If in subtask 1, you accepted the default selection to enable the bidirectional forwarding detection (BFD) settings, which exchanges messages between the two tunnel device endpoint interfaces to confirm that each can contact the other:
  - To configure the interval at which the endpoints send a contact confirmation message, in the **Interval** field, type the time in milliseconds.

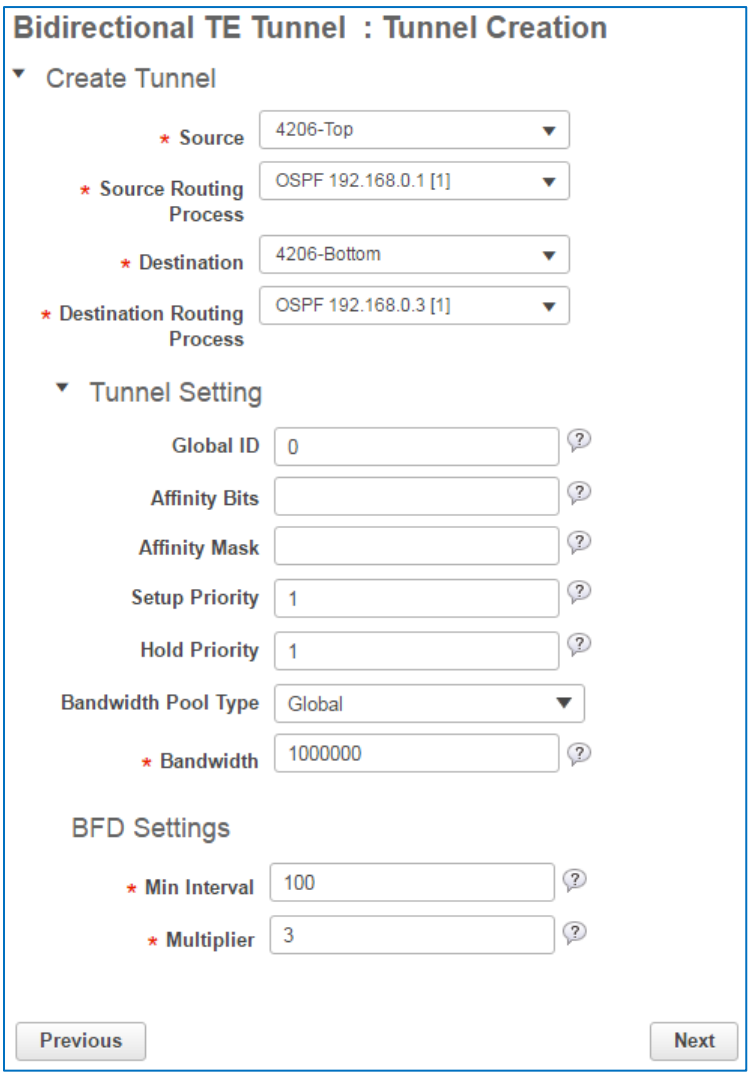
Tip: When provisioning a path that supports a large number of tunnels, use caution when applying the time interval.

Shorter intervals require additional CPU processing time and cause additional traffic.

  - To configure the number of times that the exchange of confirmation messages can fail before prompting a down notification, in the **Multiplier** field, type the value.

4. To configure the working and any alternate paths, click **Next**, and then go to subtask 3.

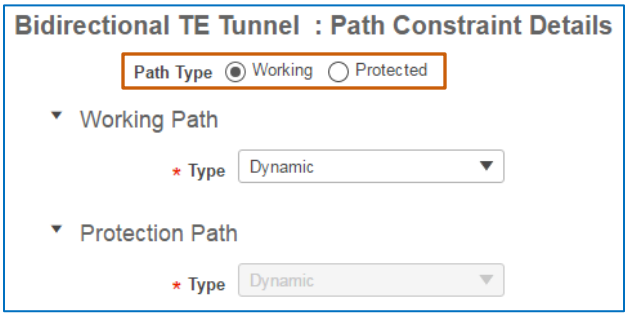
In this case, our tunnel settings include allowing the system to assign the Global ID value and to set the highest hold and setup priorities to help ensure that the system will provision the tunnel and keep it operational during other provisioning processes.



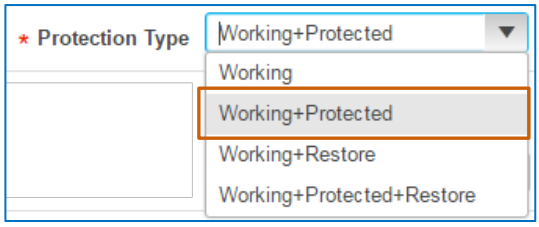
Subtask 3: Configure Working and Alternate (Backup) Paths

With the tunnel endpoints and attributes configured, you are ready to configure the working path and any alternate paths that the tunnel will use as backups in case of a failure.

You configure paths and their constraints on the **Path Constraint Details** page. The system provides path configuration types…

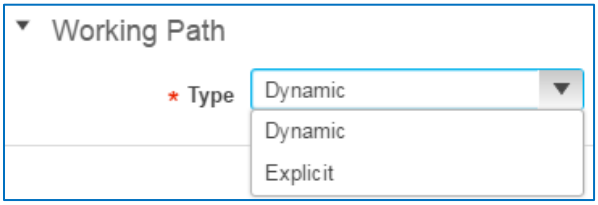


…based on the protection type that you selected when you identified the technology and service.



When you select the **Dynamic** path type for any path, the system identifies and configures an optimal path automatically.

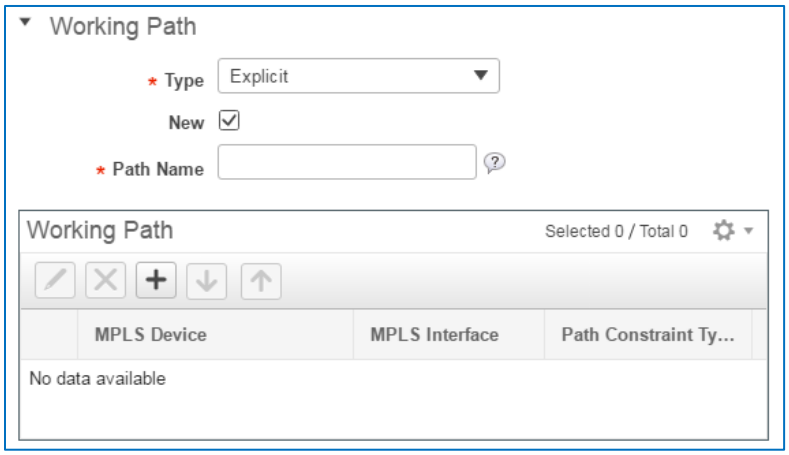
When you select **Explicit**, you can specify devices and interfaces to include or exclude from the path.



To configure working and alternate paths, follow these steps:

1. Beside **Path Type**, accept the default selection of the **Working** option button.
2. In the applicable **Path** section, in the **Type** field:
   - To allow the system to determine and provision the best available working route, accept the default selection of **Dynamic**, and then go to step 5.
   - To select a previously configured route or configure a new route by selecting the devices and interfaces that will support the working path, select **Explicit**.

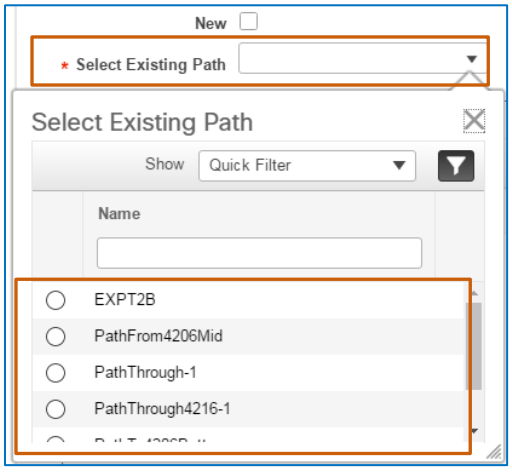
     The system opens the functions so that you can select or configure a path and selects the **New** check box by default.



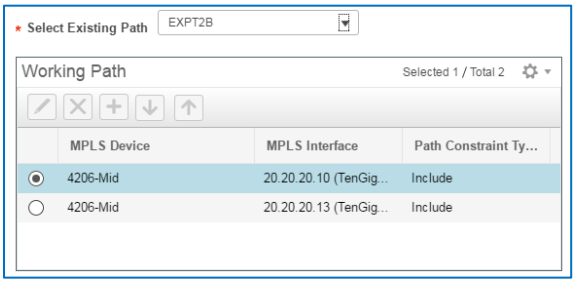
   - To select a path that a previous user has configured, go to step 3.
   - To configure a new path, go to step 4.
3. To select an existing path that a user previously configured:
   a. Clear the **New** check box.

      The system changes the **Path Name** field to the **Select Existing Path** drop-down list.

   b. In the **Select Existing Path** drop-down list, select the applicable path, and then go to step 5.

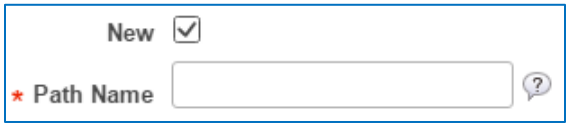


The system populates the applicable **Path** list with the devices and their constraints.



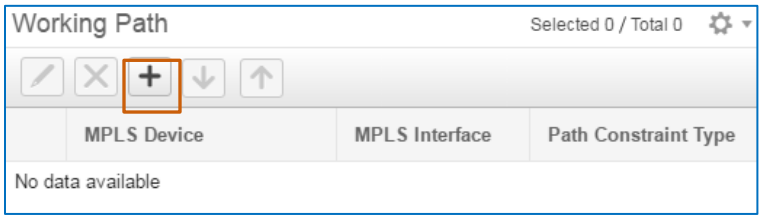
4. To configure a path:
   a. Accept the default selection of the **New** check box.
   b. In the **Path Name** field, type a name that makes its use recognizable to other users.

Note: When you configure a new path, it becomes available to other system users as an existing path after it has been deployed successfully.



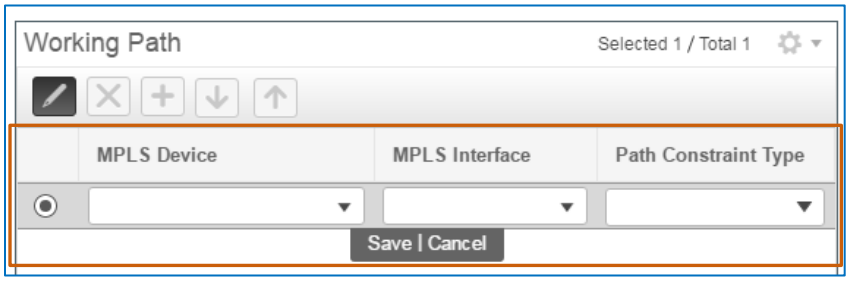
   c. In the applicable **Path** section, on the toolbar, click **Add Row**.

Tip: To refine the path, you can include or exclude device interfaces as needed, based on the constraints that you indicate in the **Path Constraint Type** column.



A blank row opens in the list.

Note: The path will follow the top down order of the devices in the list. You can add the devices in the order, or you can move the devices up or down in the list, as needed.



d. In the **MPLS Device** and **MPLS Interface** drop-down lists, select the device and interface that you want to include or exclude on the path.

Note: The system populates the **MPLS Device** drop-down lists with all of the network devices that are capable of supporting the service that you are configuring.

The list is not restricted to those devices available in the device group that you have open on the map.

e. In the **Path Constraint Type** drop-down list, select **Exclude** or **Include**.

f. Below the row, click **Save**.

The map updates and indicates included and excluded devices based on your selections.

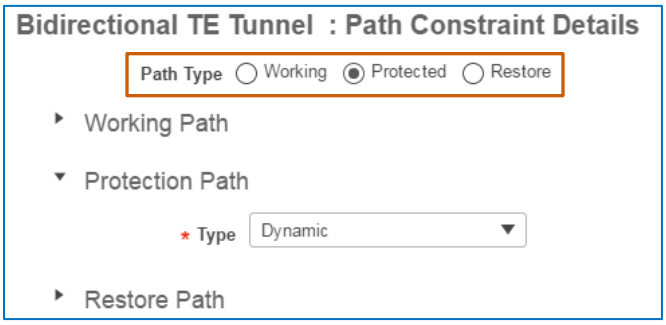
5. To include or exclude another device and interface, return to step 4c, and then go to step 6.

Tip: The path will follow the top down order of the devices in the list.

To change the path's route through the devices:

- In the list, select a device and click the up or down arrow.

6. To configure an alternate path, beside **Path Type**, click the alternate path type option button, and then return to step 2.

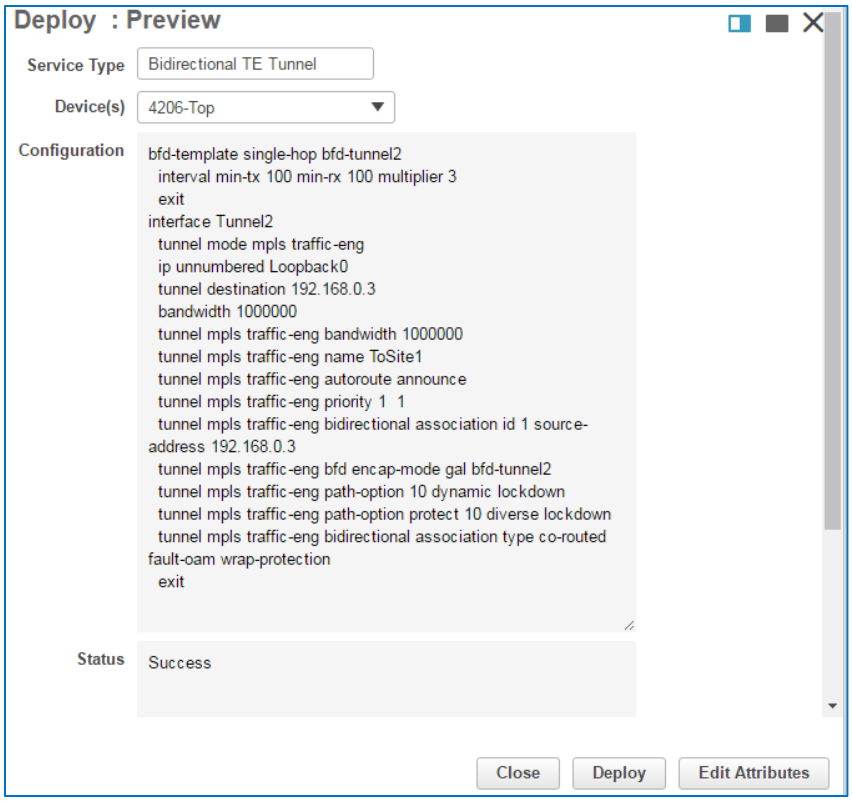


7. To complete the provisioning process, click **Submit**.

The system runs provisioning to determine whether the configuration can occur successfully on the device endpoints. On completion:

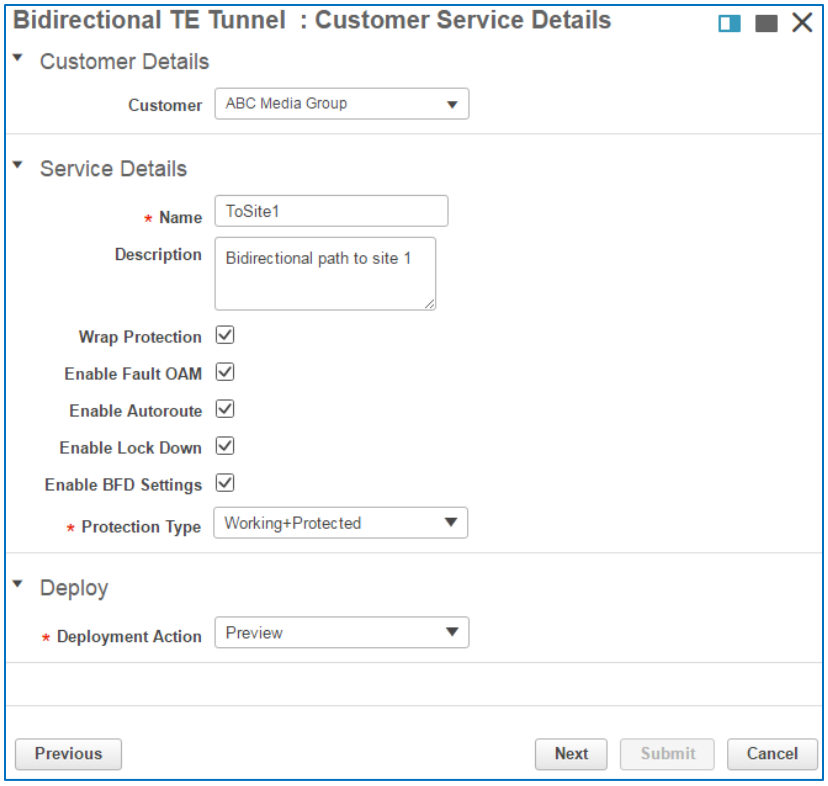
- If you selected **Preview** as the deployment action in subtask 1, the system opens the **Deploy: Preview** page. Go to step 8.
- If you selected **Deploy** in step as the deployment action in subtask 1, the system starts the provisioning process. Go to step 9.

8. On the **Preview** page, in the **Device(s)** drop-down list, select a device endpoint, and:
   a. In the **Configuration** field, review the CLI commands that the system will send to that device.



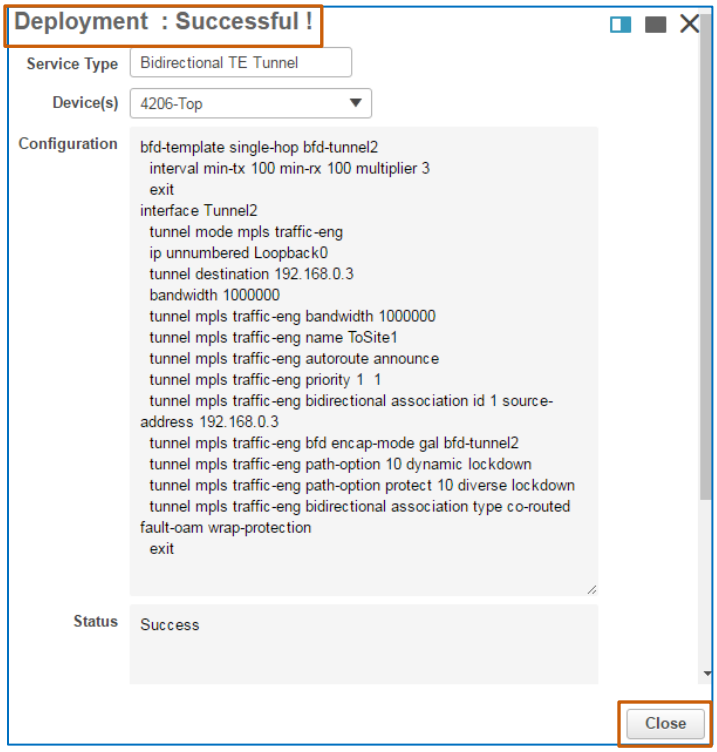
   b. For each device, review the **Status** section to determine whether it indicates a successful result:
      - For each device, if the status is **Success**, click **Deploy**, and then go to step 10.
      - If you need to make configuration changes and retest, click **Edit Attributes**, make the changes that you need, and then return to step 7.

When you click **Edit Attributes**, the wizard returns to the **Customer Service Details** page. You can navigate to and make changes on the applicable wizard page or pages.

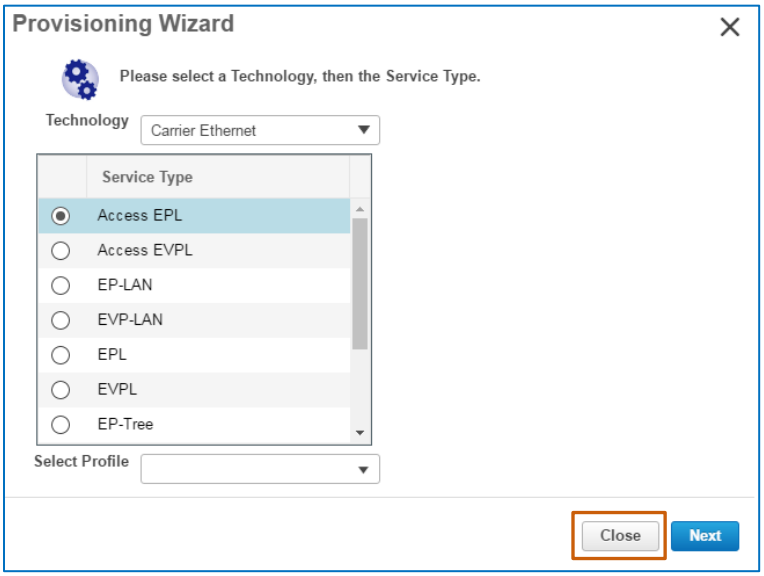


9. When the deployment process completes, review the deployment status message that opens in the wizard, indicating deployment results.
10. To close the **Provisioning Wizard**, click **Close**.

    The system returns to the **Provisioning Wizard** start page.



11. On **Provisioning Wizard** start page, click **Close**.



12. To validate the provisioned service, go to subtask 4.

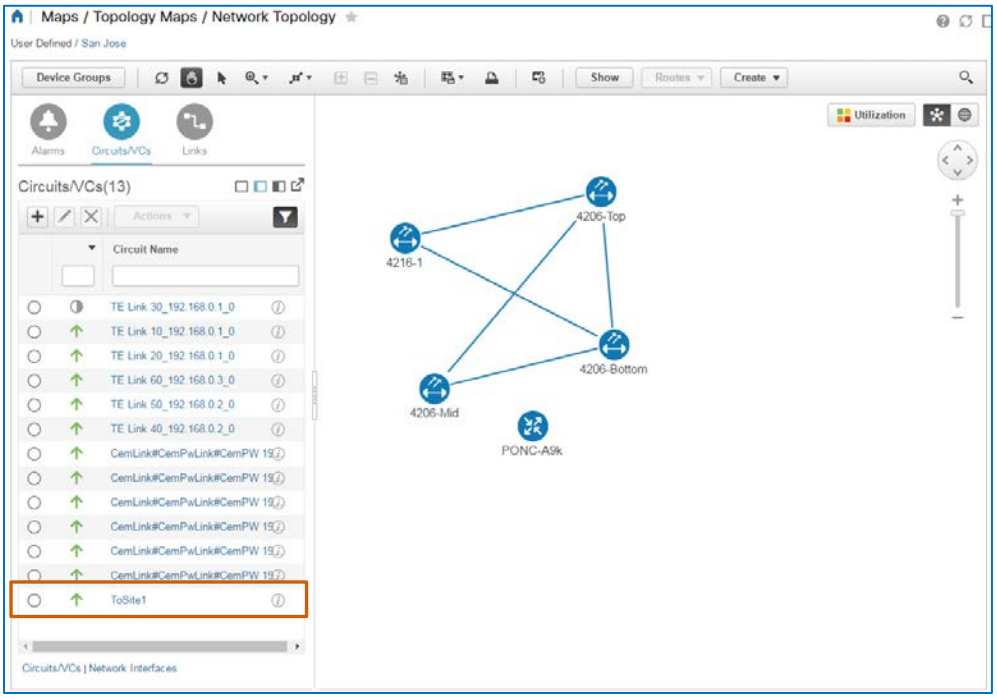
Subtask 4: Validate Service Provisioning

When provisioning tunnels or services, EPN Manager provides several tools that you can use to validate whether provisioning is successful and evaluate connectivity.

To learn more about the validation tools available to you:

- Refer to the **Validating Service Provisioning** job aid.

When the service is operationally up, the system indicates its status in the **Circuits/VCs** list.

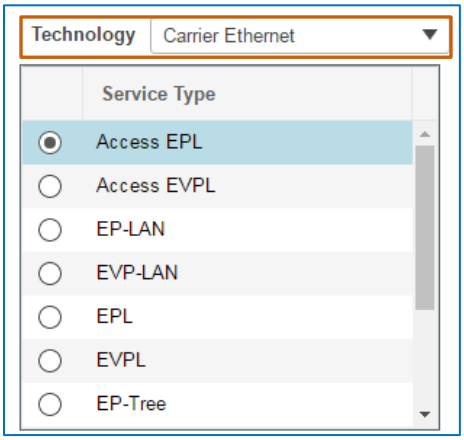


Task 2: Provision the T1 Service

As a best practice, you assign services to tunnels. With a tunnel available that meets the requirements and routing that the service requires, you can provision the service, which uses the same endpoints that support the tunnel.

In this case, the customer has requested a dedicated path that carries legacy traffic between its main site and a branch site. With the dedicated tunnel provisioned and operationally up, you are ready to provision the service.

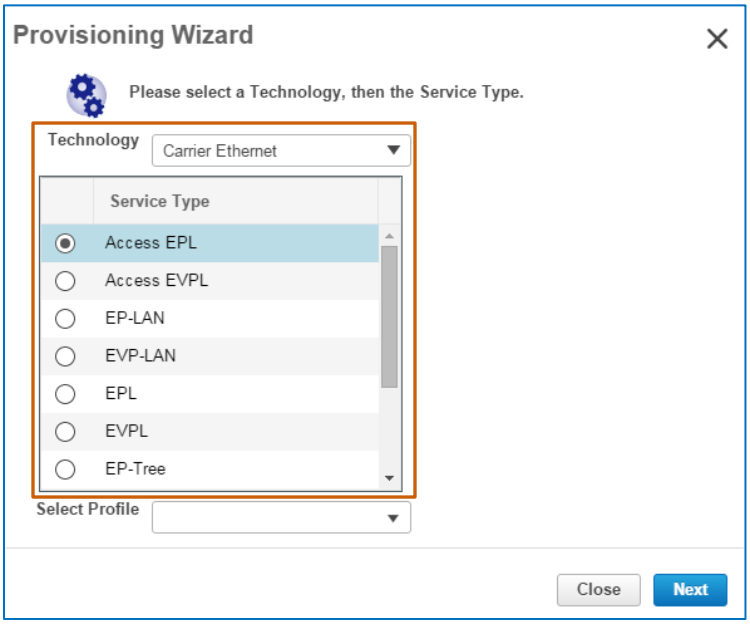
You have the **Provisioning Wizard** open and are ready to begin. The first page of the wizard populates with the **Carrier Ethernet** technology and service types by default.



Subtask 1: Identify the Technology and Service

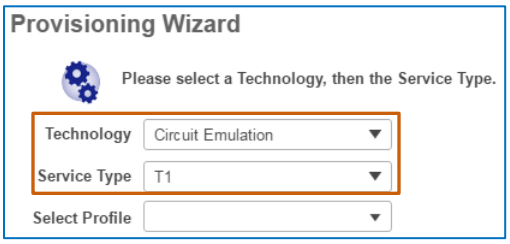
Based on the use case, follow these steps:

1. In the **Technology** drop-down list, select **Circuit Emulation**.



The page updates and displays the circuit emulation **Service Type** drop-down list.

2. In the **Service Type** drop-down list, select the data transmission rate that you need to provision.

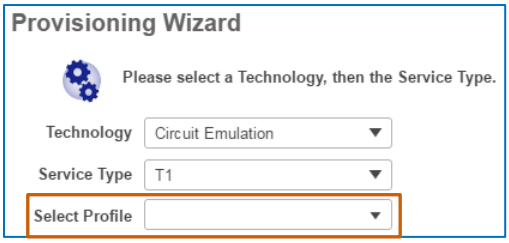


3. In the **Select Profile** drop-down list, accept the default selection, which is blank, or select a profile.

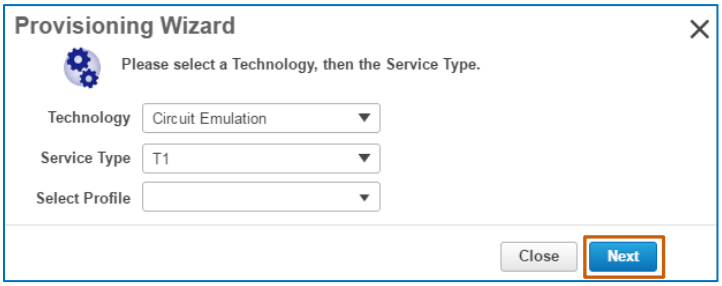
Note: When provisioning tasks include common sets of configurations that users provision on a regular basis, they can define those parameters in profiles to automate and expedite complex provisioning tasks.

Then, users can apply an applicable profile based on the circuit that they need to provision by using **Select Profile**.

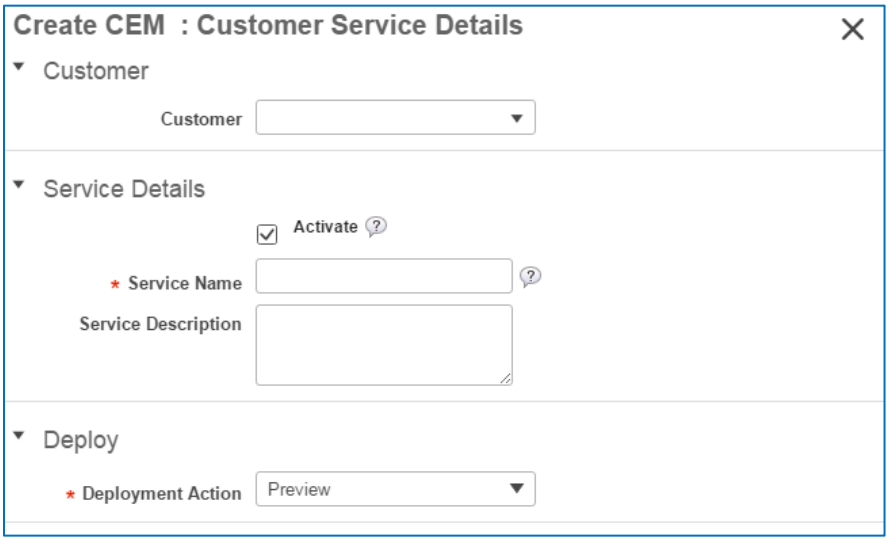
When manually provisioning circuits, you do not select a profile.



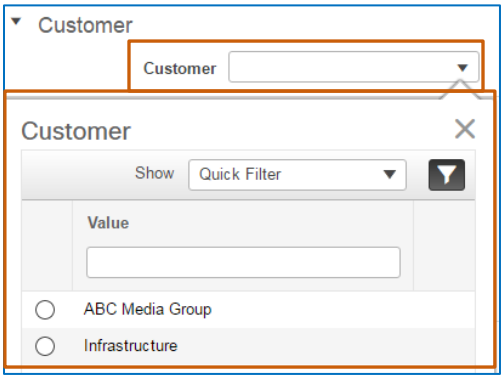
4. To configure the service details, click **Next**.



The **Customer Service Details** page opens.

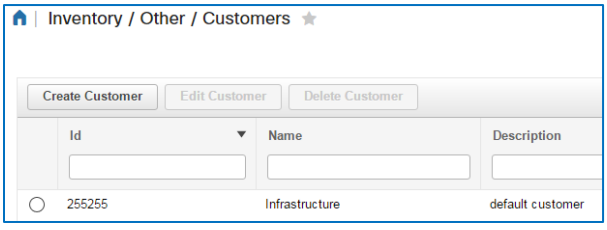


5. To identify the customer who will use the service, when applicable, in the **Customer** section, in the **Customer** drop-down list, select the name of the customer.

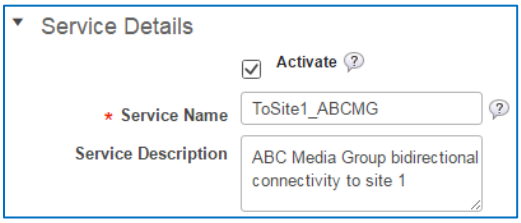


Note: System users can add customers in EPN Manager and associate them with network services during provisioning.

This association helps users to identify service users during monitoring and troubleshooting activities.

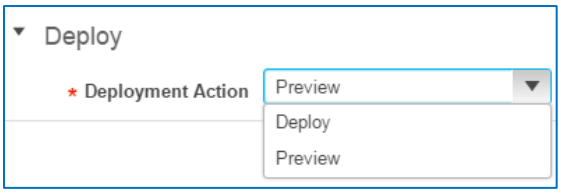


6. In the **Service Details** section:



   a. To have the service operationally up when provisioning is complete, accept the default selection of the **Activate** check box.
   b. In the **Service Name** field, type a name for the service that makes its use recognizable.
   c. To indicate the use of service, optionally, in the **Service Description** field, type additional information about the service based on operational or business requirements.

7. To preview the CLI code or deploy the code immediately when you finish service configuration, in the **Deployment Action** drop-down list:



   - To configure the system to present a preview of the CLI code that it will deploy to the endpoints before deploying it, accept the default selection of **Preview**.

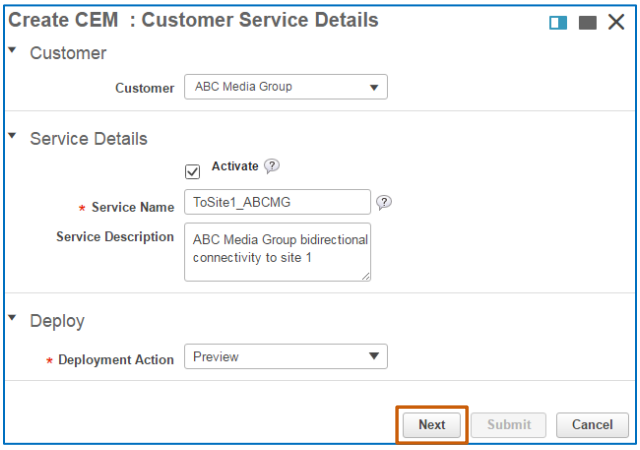
Tip: Cisco recommends that you preview CLI code before deploying the configuration. This approach helps you to avoid unexpected results or operational issues.

When you determine that you need to make changes, you can cancel provisioning at this point, and make the corrections that you need.

   - To configure the system to deploy the configuration to the endpoints immediately without reviewing the CLI code, select **Deploy**.

8. To configure the **A** endpoint, click **Next**, and then go to subtask 2.

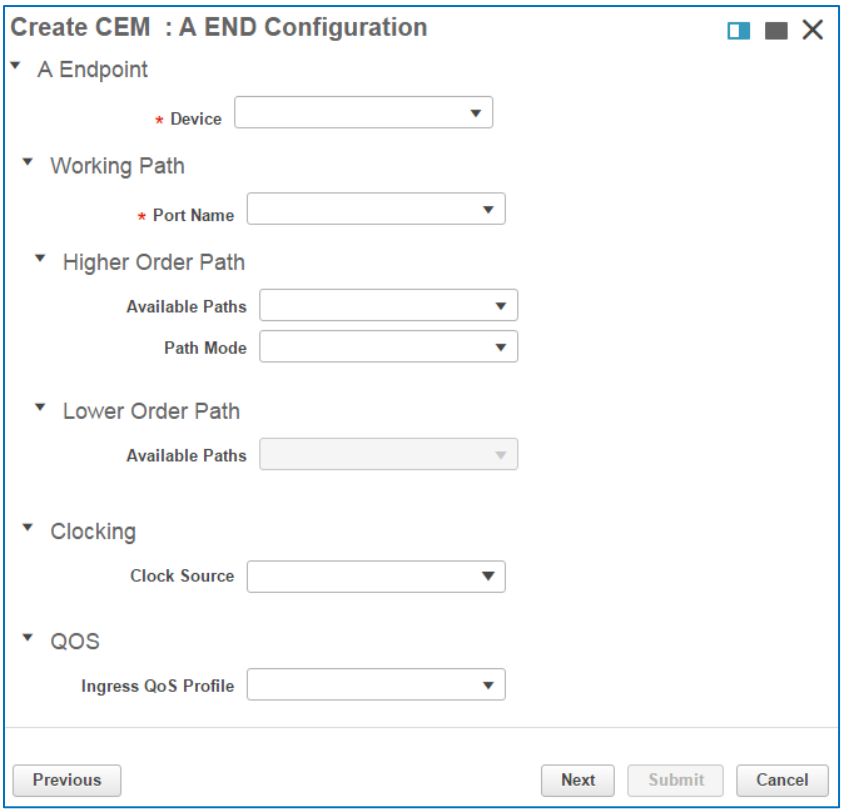
In this case, we have assigned the customer, we need the service operationally up after provisioning, and as a best practice, we want to preview the configuration code.



Subtask 2: Configure the A Endpoint

When you navigate to the **A END Configuration** page, you configure the **A** endpoint for the emulated service. Based on the type of device and service that you are provisioning, the system removes those features that do not apply when you select the device's interface.

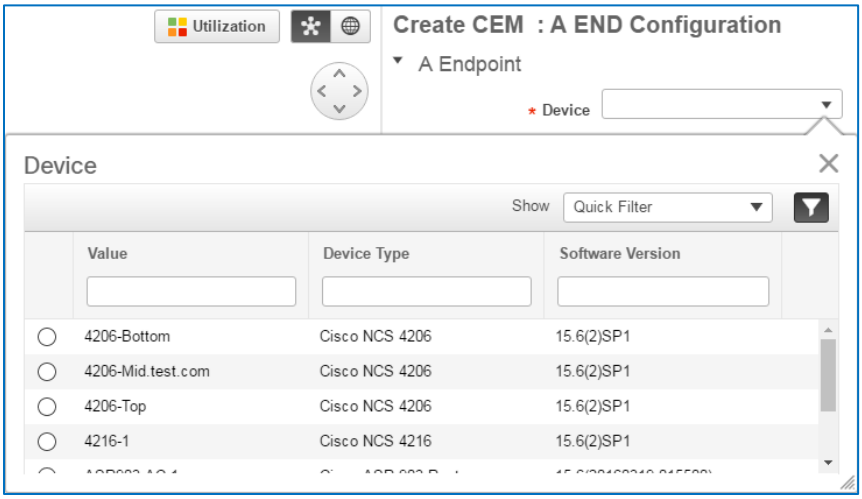
You configure the **A** and **Z** endpoints separately. The **A** endpoint will be the same device and port that you assigned to the tunnel source endpoint.



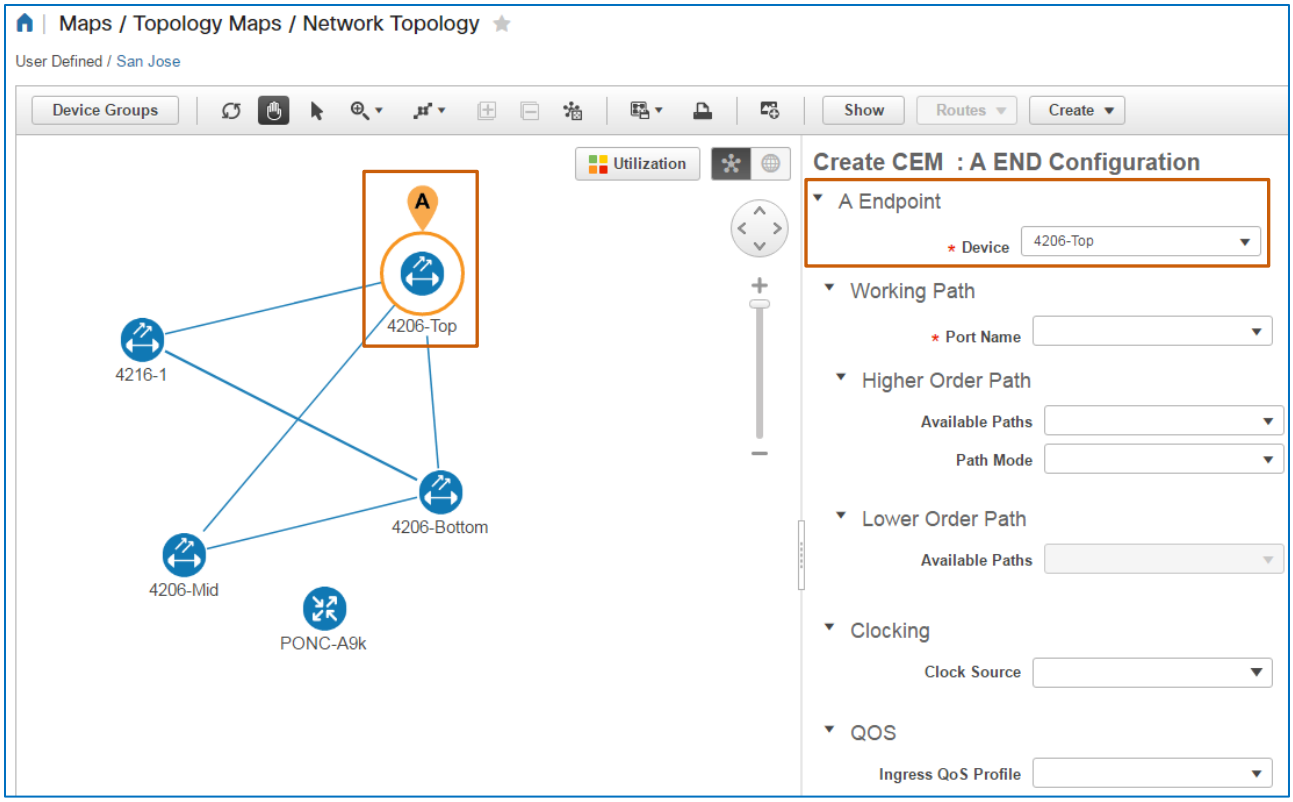
To configure the A endpoint, follow these steps:

1. To indicate the device on which you are configuring the **A** endpoint, in the **Device** drop-down list, select the device.

Note: If you previously provisioned a tunnel that you will assign to support this service, the **A** endpoint that you select in this step needs to be the same as the source endpoint of the tunnel.



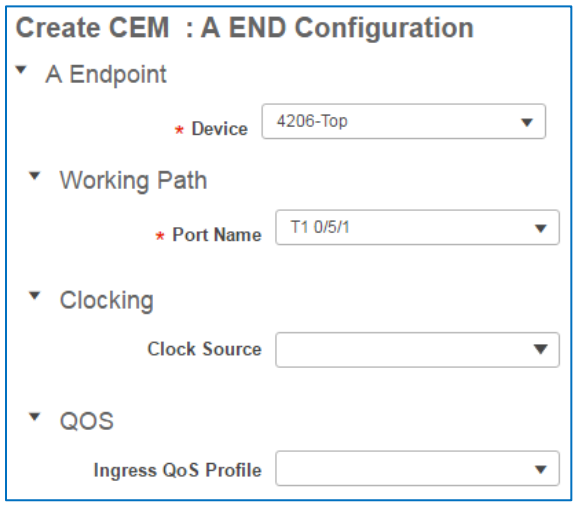
The system applies the **A** icon to the device icon on the map, and populates the **Working Path** drop-down list with the device's interfaces, or ports, that are available for the service.



Tip: You also can click a device on the map to populate the **Device** drop-down list.

2. To configure the interface for the **A** endpoint, in the **Working Path** section, in the **Port Name** drop-down list, select the interface.

   In this case, we are configuring a CEM service to support T1 traffic, so the page updates to provide the **Clocking** and **QOS** sections.

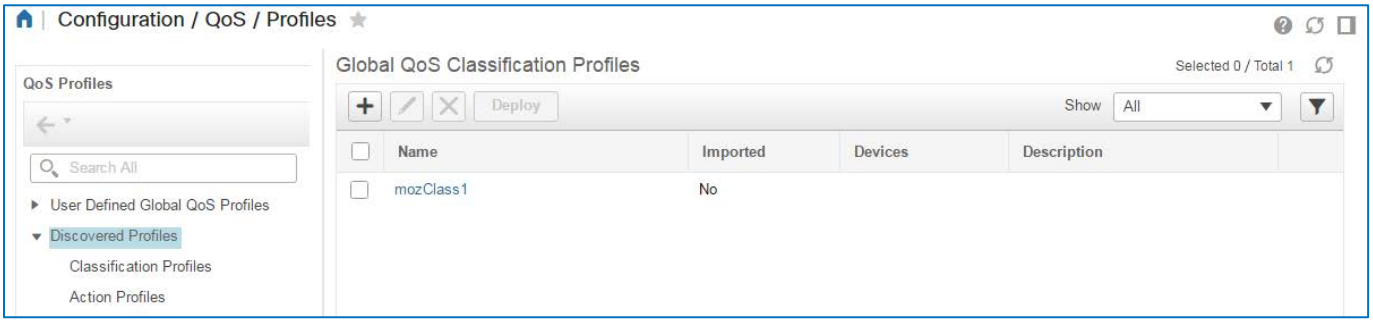


3. To configure endpoints to apply a single, synchronized clock time, which helps ensure that (**A**) endpoint does not drop or reread information sent to it, in the **Clocking** section, in the **Clock Source** drop-down list, select one of the following:

   - **Internal**
     The system obtains the clock rate from the device that contains the related endpoint.
   - **Line**
     The endpoint obtains the clock rate from the payload of the inbound traffic.
   - **Adaptive Clock Recovery**
     Commonly used for CEM services, the endpoint obtains the clock rate by capturing the average transmission rate from the inbound traffic, which helps negate the effect of random packet delay variations.
   - **Differential Clock Recovery**
     Commonly used for CEM services, the endpoint obtains the clock rate based on the difference between the sending and receiving endpoint clocks. Each end device uses a traceable clock so that the packet transfer process does not affect the recovered clock rate.

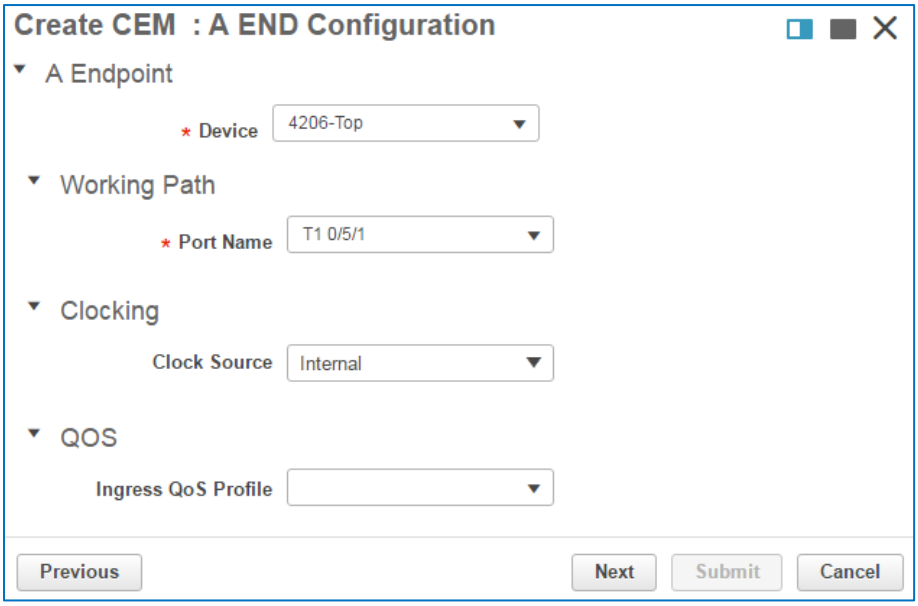
4. To assign a quality of service profile, which manages the speed available to the traffic on the **A** endpoint, in the **QOS** section, in the **Ingress QoS Profile** drop-down list, select the profile.

Note: To populate QoS profile drop-down lists, system users must configure profiles and deploy those profiles to the device on which you are configuring the endpoint.



5. To configure the **Z** endpoint, click **Next**, and then go to subtask 3.

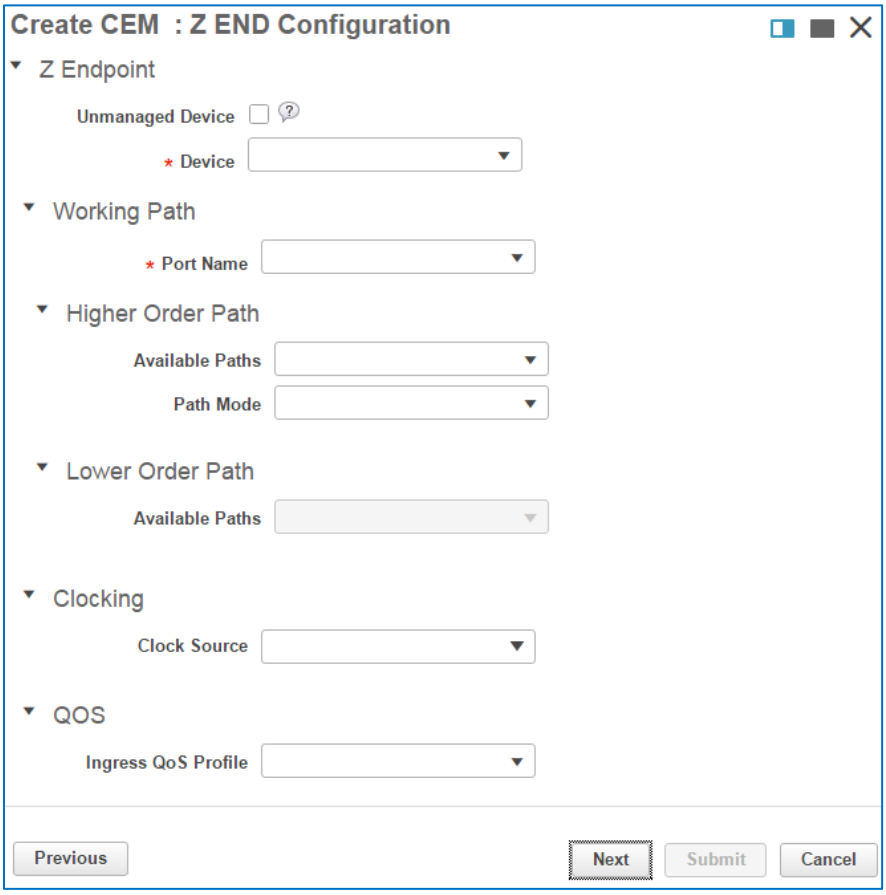
In this case, we want the clock rate from the device that contains the related endpoint. And, because T1 traffic moves at a constant bit rate, we do not need to include a QoS profile, which primarily regulates bandwidth.



Subtask 3: Configure the Z Endpoint

When you navigate to the **Z END Configuration** page, you configure the **Z** endpoint for the emulated service.

The **Z** endpoint will be the same device and port that you assigned to the tunnel destination endpoint.



To configure the Z endpoint, follow these steps:

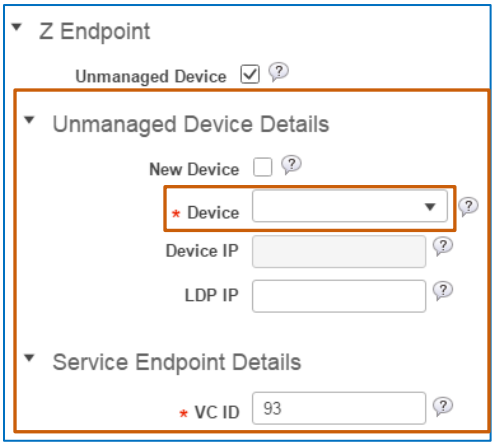
1. Determine whether you are configuring the endpoint on a device that the system manages or a device that it does not manage:
   - To configure the **Z** endpoint on an unmanaged device, go to step 2.
   - To configure the **Z** endpoint on a device that the system manages, go to step 5.

> **Note:** When you are configuring a CEM service that you will assign to a TE tunnel, you cannot use an unmanaged device.
>
> When using a tunnel, you assign the **Z** endpoint to the same device on which you provisioned the destination endpoint for the tunnel.

2. To configure the **Z** endpoint on a device that the system does not manage, select the **Unmanaged Device** check box.

   The system opens fields so that you can indicate the device, and populates the **Device** drop-down list with unmanaged devices that users have added previously.

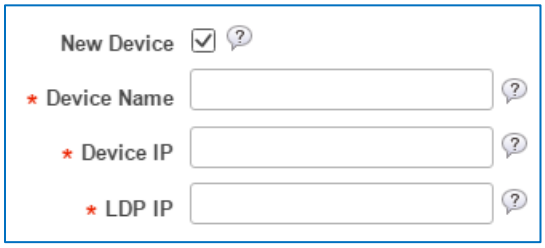
> **Note:** Users can add unmanaged devices by using functionality available in the network device inventory, on the topology map, or by using this process.



   - To add a new, unmanaged device, go to step 3.
   - To use an unmanaged device that is not already included in the system, go to step 4.

3. To indicate that this is an unmanaged device not already available in the list, select the **New Device** check box.

   The **Device** and **Device IP** drop-down lists change to editable fields.



   a. In the **Device Name** field, type a name for the device that makes it recognizable to system users.
   b. In the **Device IP** field, type the device's IP address.

c. To configure the label discovery protocol (LDP) IP address, which the system uses to connect to and communicate with the device, in the **LDP IP** field, type the LDP IP address.

d. In the **Service Endpoint Details**, to configure the virtual circuit (VC) ID that will allow the system to bind the managed device circuit to the unmanaged device circuit, in the **VC ID** field, accept the default value, which is populated by the device that you are configuring, and then go to step 7.

Note: When you know that another service is using the VC ID value appearing in the field, you can change the value to the applicable identifier for the service that you are provisioning.

4. To select an unmanaged device that a user previously added to the system:

a. Accept the default that the **New Device** check box is not selected.

b. In the **Device Name** drop-down list, select the device.

c. To configure the label discovery protocol (LDP) IP address, which the system uses to connect to and communicate with the device, in the **LDP IP** field, type the LDP IP address.

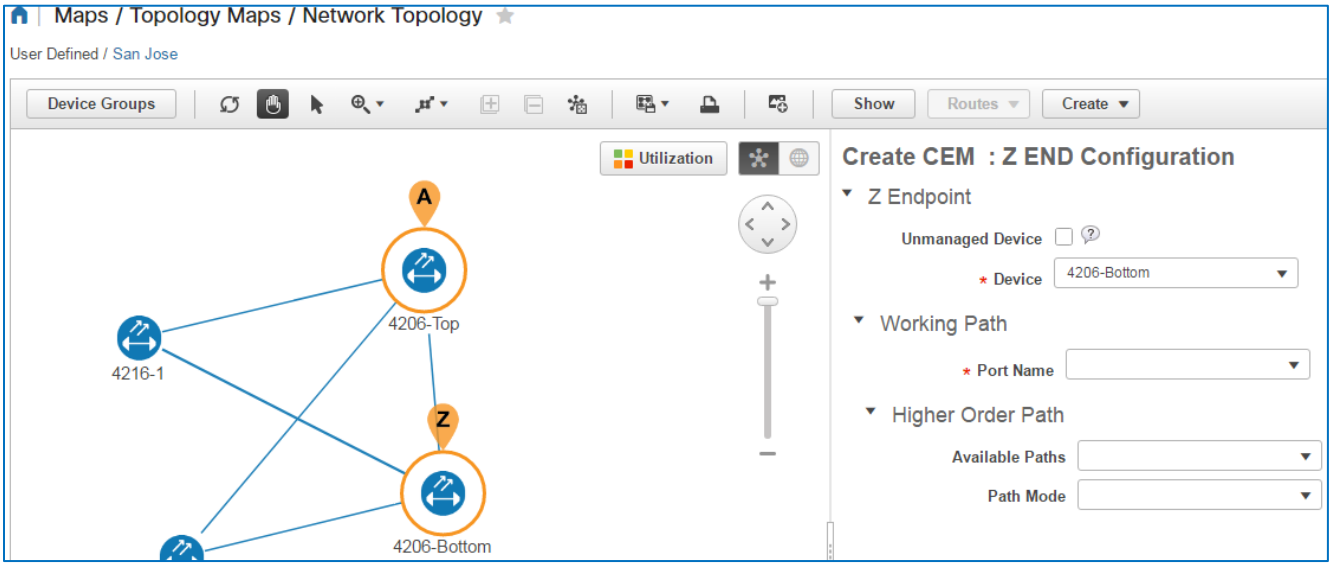
d. In the **Service Endpoint Details**, to configure the virtual circuit (VC) ID that will allow the system to bind the managed device circuit to the unmanaged device circuit, in the **VC ID** field, accept the default value, which is populated by the device that you are configuring, and then go to step 7.

Note: When you know that another service is using the VC ID value appearing in the field, you can change the value to the applicable identifier for the service that you are provisioning.

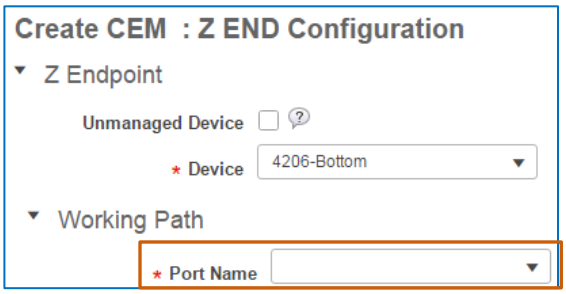
5. To configure the **Z** endpoint on a device that the system manages, in the **Device** drop-down list, select the device.

Note: When you are provisioning a service that will use a previously configured tunnel, configure the service's **Z** endpoint on the same device that is supporting the tunnel's destination endpoint.

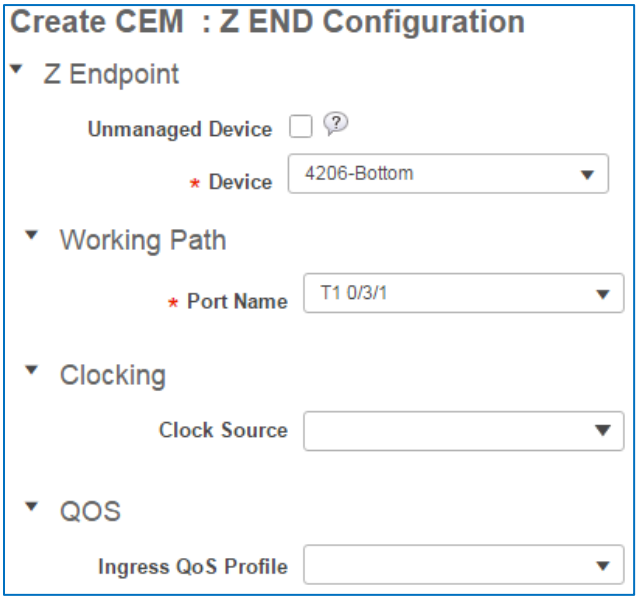
The system applies the **Z** icon to the device icon on the map, and populates the **Working Path** drop-down list with the device's interfaces, or ports, that are available for the circuit.



6. To configure the interface that will become the **Z** endpoint working path, in the **Working Path** section, in the **Port Name** drop-down list, select the interface.



As when configuring the **A** endpoint, the page updates to provide those functions that support T1 service configuration.



7. To configure endpoints to apply a single, synchronized clock time, which helps ensure that the receiving endpoint does not drop or reread information sent to it, in the **Clocking** section, in the **Clock Source** drop-down list, select the clock source type.

Note: Depending on the device configuration for each of the endpoint devices, the **A** and **Z** endpoint clock sources can differ, although, in most cases, the clock sources remain consistent.

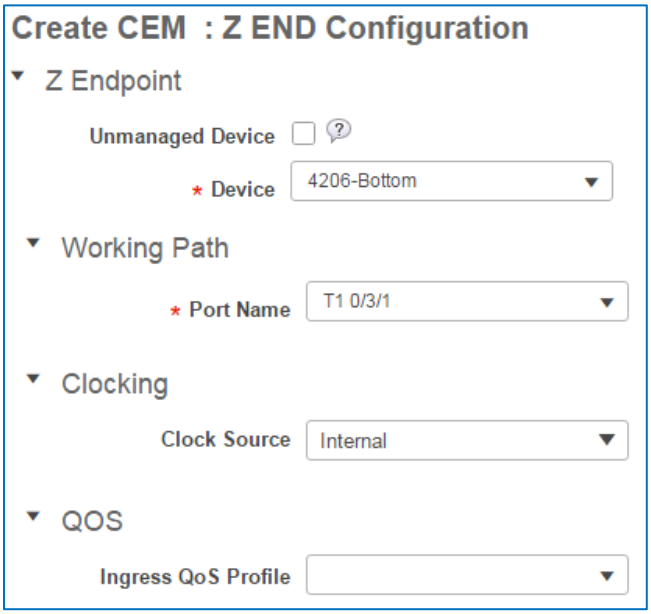
To review the clock source types, refer to **A** endpoint configuration step 3.

8. To assign a quality of service profile, which manages the speed available to the traffic on the **Z** endpoint, in the **QOS** section, in the **Ingress QoS Profile** drop-down list, select the profile.

Note: To populate QoS profile drop-down lists, system users must configure profiles and deploy those profiles to the device on which you are configuring the endpoint.

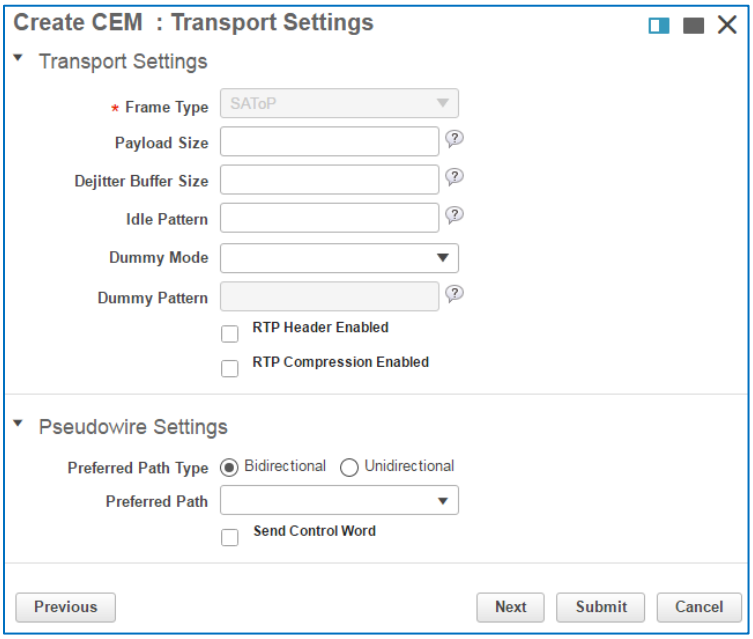
9. To define the attributes of the traffic that is using the service, click **Next**, and then go to subtask 4.

The following screenshot illustrates the **Z** endpoint configuration for the use case.



Subtask 4: Configure Transport Settings

The transport settings define the parameters for the packets that encapsulate the T1 traffic for transport through the core network and how the system manages the packets at the receiving endpoint.



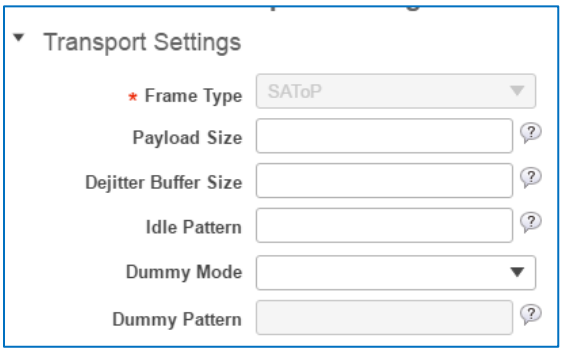
When you open the **Transport Settings** page, the **Frame Type** drop-down list is read-only and populates based on the type of service that you are provisioning.

In this case, the system is transporting T1 traffic over a packet network, which uses the structure-agnostic TDM over packet (SAToP) frame type, and we want the system to use the default transport settings in the device's configurations.

Important Note: When you accept, the default blank entries in the **Transport Settings** section, the system uses the settings for the associated service that are already configured on the devices and interfaces that you are provisioning.

In many cases, these default device settings are tested and validated before being deployed in the network.

Use caution when applying setting values here, which override the device default settings. Improper sizing or patterning can result in transmission issues, such as dropped or incorrectly converted traffic.



To configure transport settings, follow these steps:

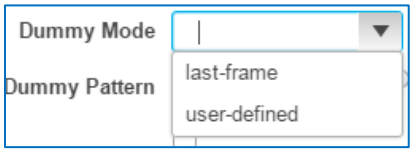
1. To configure the maximum number of bytes that a packet can contain, between 32 and 1312, in the **Payload Size** field, type the value.

   Note: To optimize network usage, consider the type and quality of the traffic that the packet is carrying.

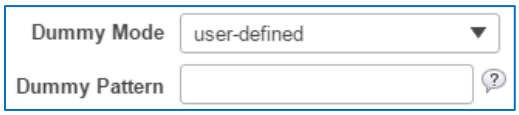
2. To configure the size of the buffer where the terminating endpoint accumulates packets before converting them back to their original format, in the **Dejitter Buffer Size** field, type the value, between 1 and 32.

   Note: For more information on the relationship of the payload size to the dejitter buffer size, refer to the **Cisco Evolved Programmable Network Manager User and Administrator Guide**.

3. To ensure a constant bit rate during pauses in the transmission of related packets by inserting a matching pattern, in the **Idle Pattern** field, type the value in 8-bit hexadecimal format.
4. To configure a bit pattern to fill lost or corrupted frames:
   - To apply the same pattern that was applied to the last frame that the endpoint receive, in the **Dummy Mode** drop-down list, select **last-frame**.
   - To configure a custom pattern:
     a. In the **Dummy Mode** drop-down list, select **user-defined**.

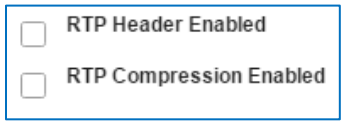
     b. In the **Dummy Pattern** field, type the pattern.

5. To include the real-time transmission protocol (RTP) in each frame header, select the **RTP Header Enabled** check box.

   Note: RTP supports the transmission of audio or video traffic.

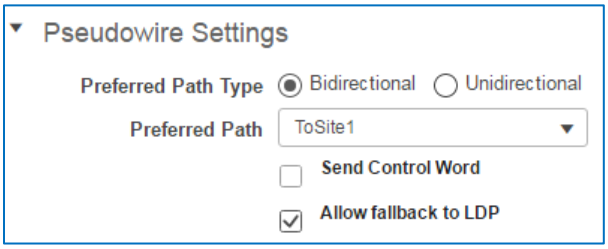
6. To compress RTP in the frame header, which reduces network overhead and increases RTP transmission speeds, select the **RTP Compression Enabled** check box.

7. To assign the T1 service to the bidirectional TE tunnel that you configured in task 1, in the **Preferred Path** drop-down list, select the tunnel.

   When you select the tunnel, the system makes the **Allow fallback to LDP** check box available and selects it by default.

   Note: The LDP fallback option becomes available when you are assigning the service to a tunnel.

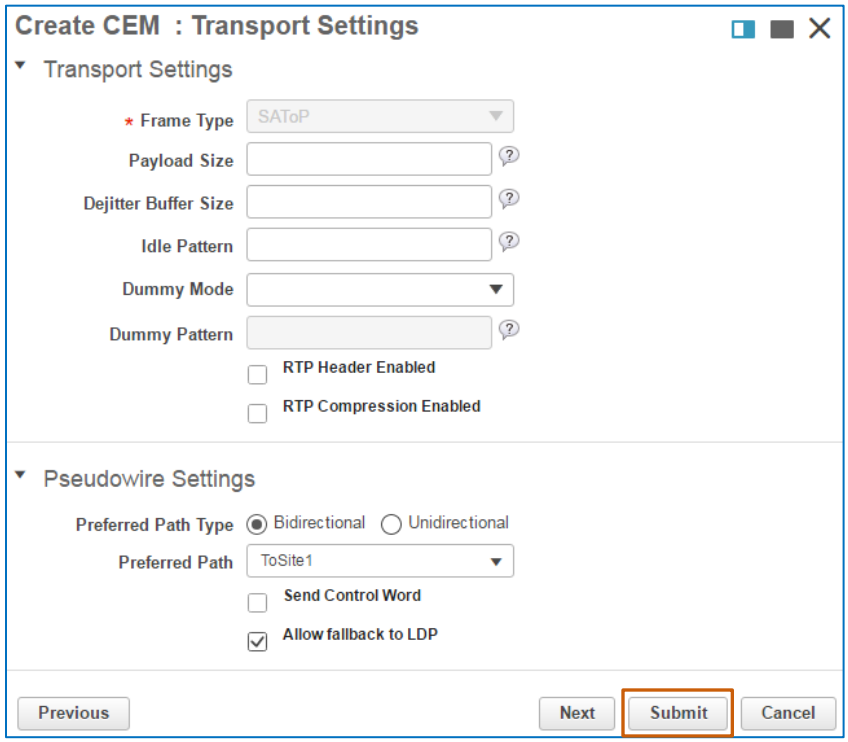


8. To send a control word during the negotiation process, which helps negotiate communication between the two endpoints that support the pseudowire, select the **Send Control Word** check box.
9. In a tunnel failure scenario, to allow the system to revert to using the MPLS Label Distribution Protocol (LDP) for communication, accept the default selection of the **Allow fallback to LDP** check box.

   Note: In complex provisioning scenarios, you can apply templates that contain CLI code that extend device provisioning functionality.

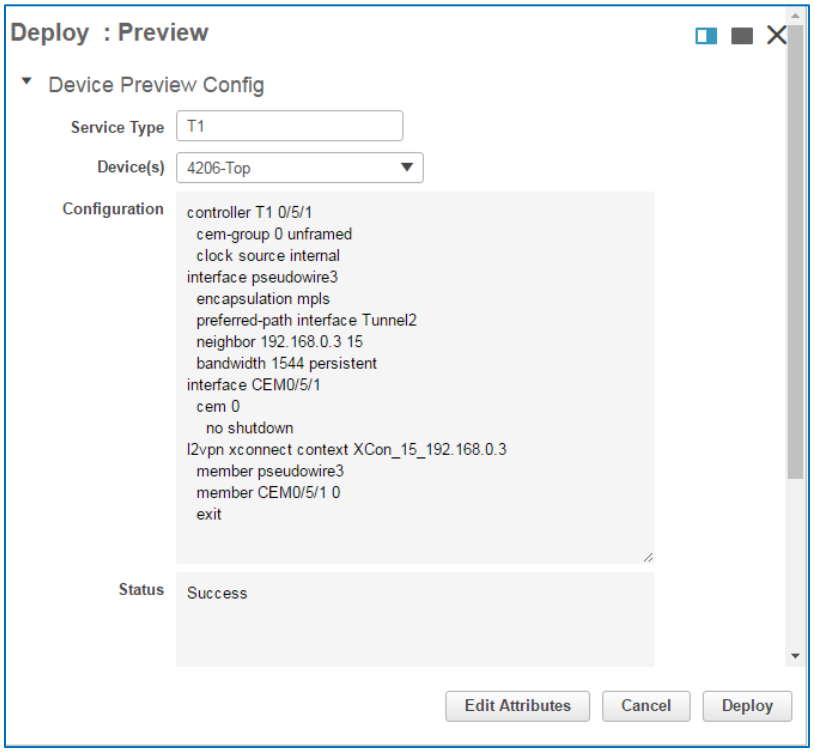
   For more information, refer to the **Extending Provisioning Functions** topic.

10. In this case, to complete the provisioning process, click **Submit**.



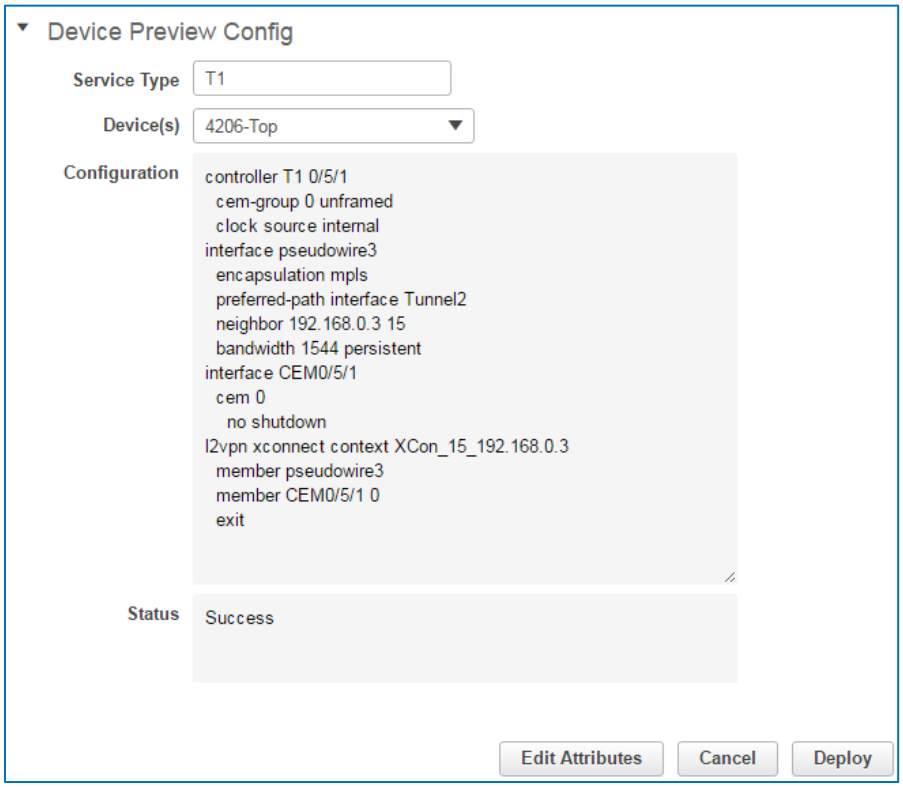
The system runs provisioning to determine whether the configuration can occur successfully on the device endpoints. On completion:

- If you selected **Preview** as the deployment action in subtask 1, the system opens the **Deploy: Preview** page. Go to step 11.

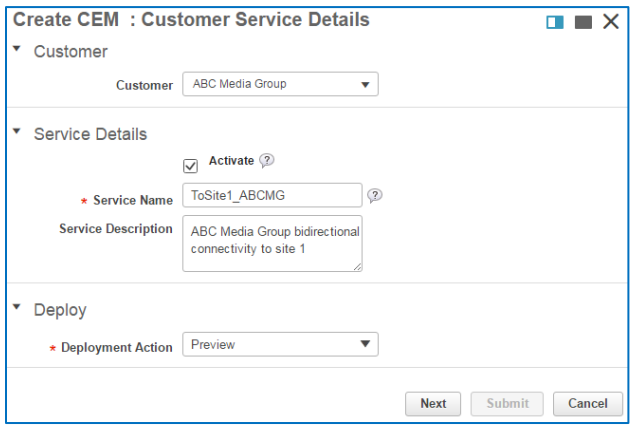


- If you selected **Deploy** as the deployment action in subtask 1, the system starts the provisioning process. Go to step 13.

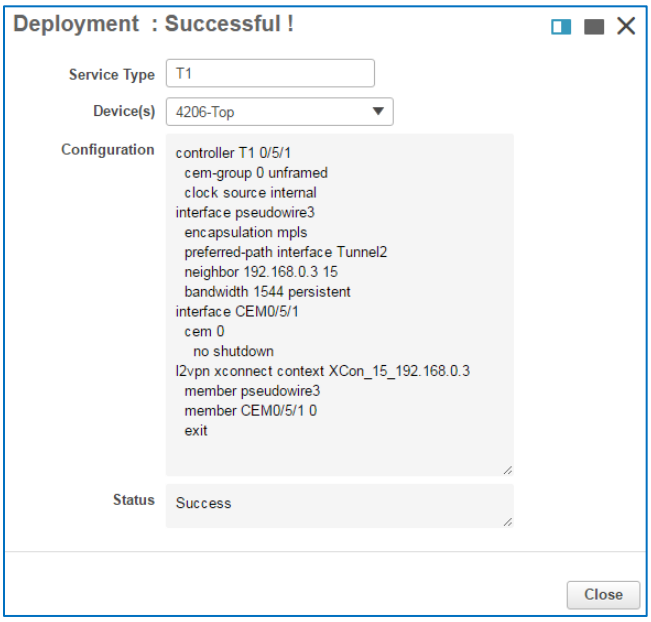
11. On the **Preview** page, in the **Device(s)** drop-down list, select a device endpoint, and:
    a. In the **Configuration** field, review the CLI commands that the system will send to that device.
    b. For each device, review the **Status** section to determine whether it indicates a successful result:
        - For each device, if the status is **Success**, click **Deploy**, and then go to step 10.
        - If you need to make configuration changes and retest, click **Edit Attributes**, make the changes that you need, and then return to step 10.



When you click **Edit Attributes**, the wizard returns to the **Customer Service Details** page. You can navigate to and make changes on the applicable wizard page or pages.



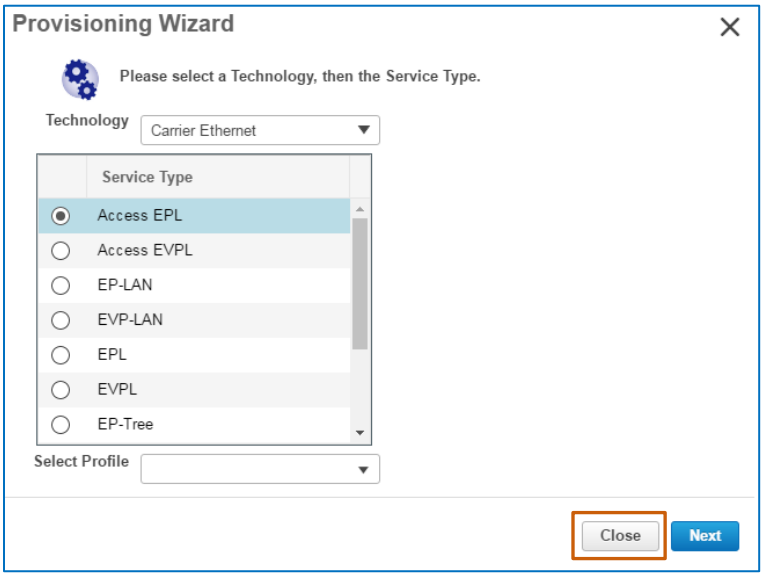
12. When the deployment process completes, review the deployment status message that opens in the wizard, indicating deployment results.



13. To close the **Provisioning Wizard**, click **Close**.

    The system returns to the **Provisioning Wizard** start page.

14. On **Provisioning Wizard** start page, click **Close**.



15. To validate the provisioned service, go to subtask 6.

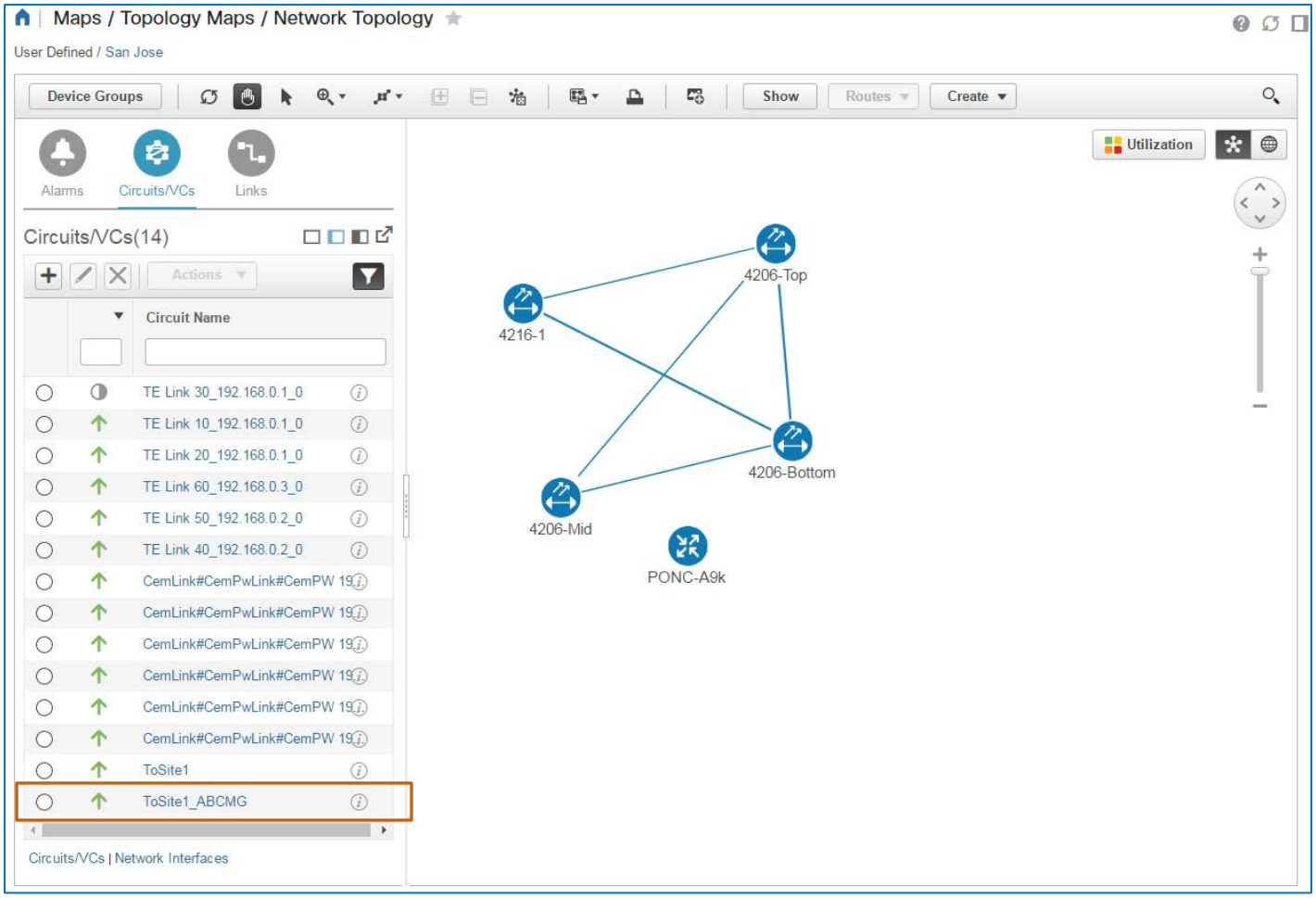
Subtask 6: Validate Service Provisioning

When provisioning tunnels or services, EPN Manager provides several tools that you can use to validate whether provisioning is successful and evaluate connectivity.

To learn more about the validation tools available to you:

- Refer to the **Validating Service Provisioning** job aid.

When the service is operationally up, the system indicates its status in the **Circuits/VCs** list.



Provisioning CEM Synchronous Transport Signal (STS) Services

Introduction

STS provisioning provides another solution for supporting hardware upgrades while retaining the ability to manage legacy traffic.

For example, if you are supporting a SONET ring and are upgrading hardware to the Cisco NCS 4200 series system, you can provision STS services on the 4200s to continue managing the traffic on the SONET ring.

You provision STS services by using the **Provisioning Wizard**.

STS Provisioning Process

Overview

When you provision STS services, you perform the same tasks and settings configurations that you do when provisioning a T1 service, including:

1. If there is no TE tunnel available that contains the paths, protection, and other parameters that the STS service requires, provision a TE tunnel.
2. Identify the technology and service.
3. Configure the **A** endpoint, and its working path and protecting path higher order paths.
4. Configure the **Z** endpoint, and its working path and protecting path higher order paths.
5. Configure the transport settings.
6. Select additional device configurations.
7. Validate service provisioning.

Note: The step 7 link opens a separate document.

The key differences when configuring STS service provisioning are that you:

- Configure the **A** and **Z** endpoint working path's higher order paths.
- Configure **A** and **Z** endpoint protection paths and their higher order paths.

Note: Depending on the circuit emulation service that you are provisioning, you also configure lower order paths.

While this document addresses the configuration of higher order paths, similar concepts apply to a service's lower order path configuration.

- Do not configure clock sources.

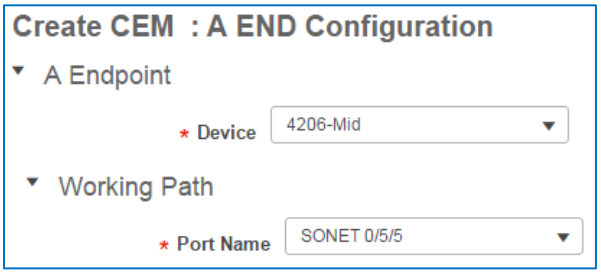
Configuring Higher Order Paths

In STS configuration, you begin by indicating the device and SONET interface at each endpoint on which you need to provision the STS service.

Note: When you select the devices that will support the **A** and **Z** endpoints, the system will indicate all of the available tunnels provisioned on those same devices.

This action helps ensure that you provision the service endpoints on the same devices that are supporting the TE tunnel.

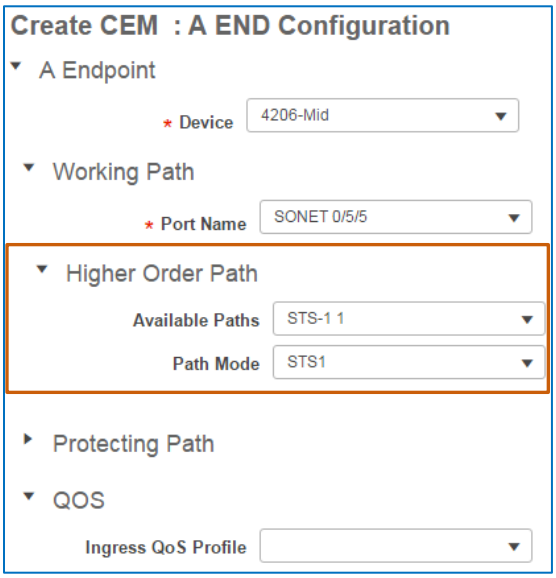
Each SONET interface carries the STS service, among many other services, based on bandwidth parameters.



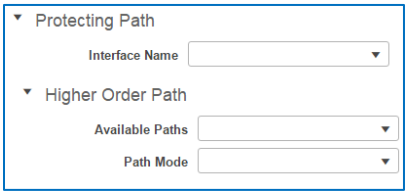
For the service's working path, you then indicate its higher order path and path mode.

Important Note: Configuring the higher order path for each path that you include is required to provision STS services successfully.

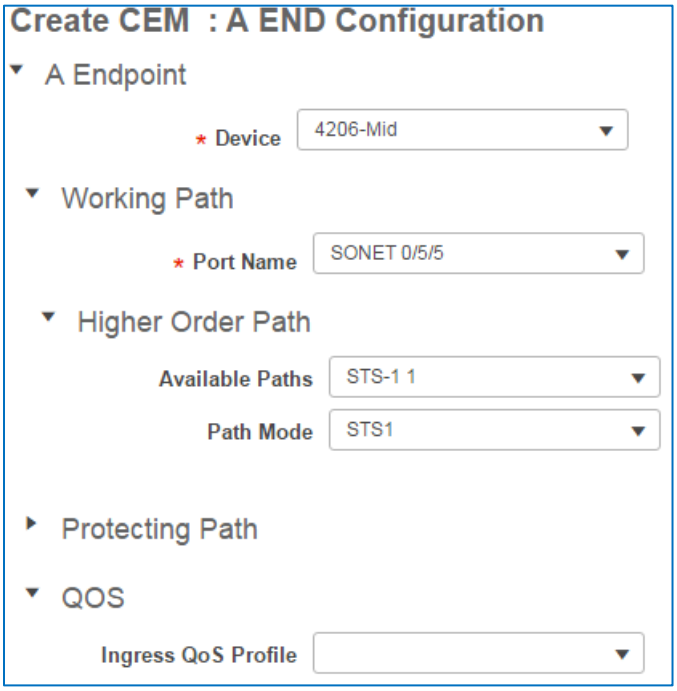
If you do not complete the **Higher Order Path** field for the working path and click **Submit** to start the provisioning process, a system message opens alerting you to the issue.

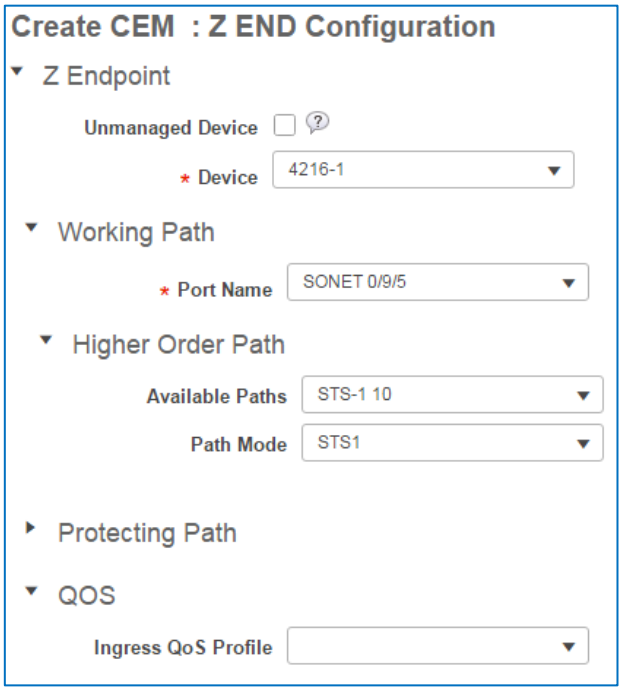


If you select a protecting path, you must also include its higher order path configuration.



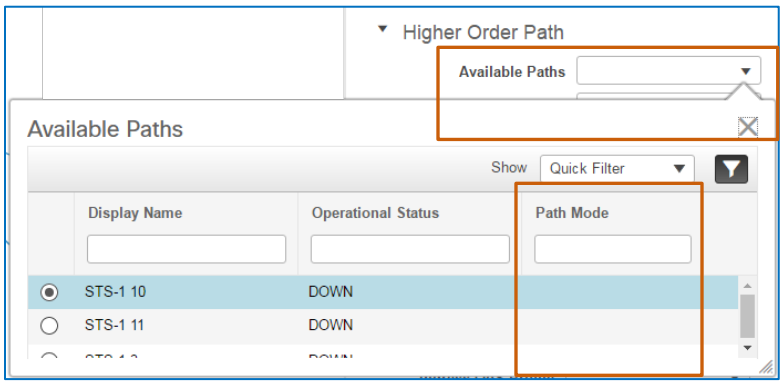
At minimum, you need to configure the working path and its higher order path.

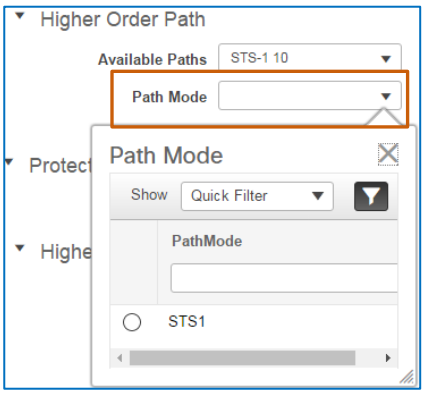




When you select an available path and the path mode is not already configured for the path, the **Path Mode** field will be blank.

In that case, the system automatically populates the **Path Mode** drop-down list with the applicable mode or modes available that can support the path.





When you select an available path with an associated path mode, the system populates the applicable **Path Mode** field automatically with the associated path.

The protecting path provides an additional route that the STS traffic can use when the working path fails.

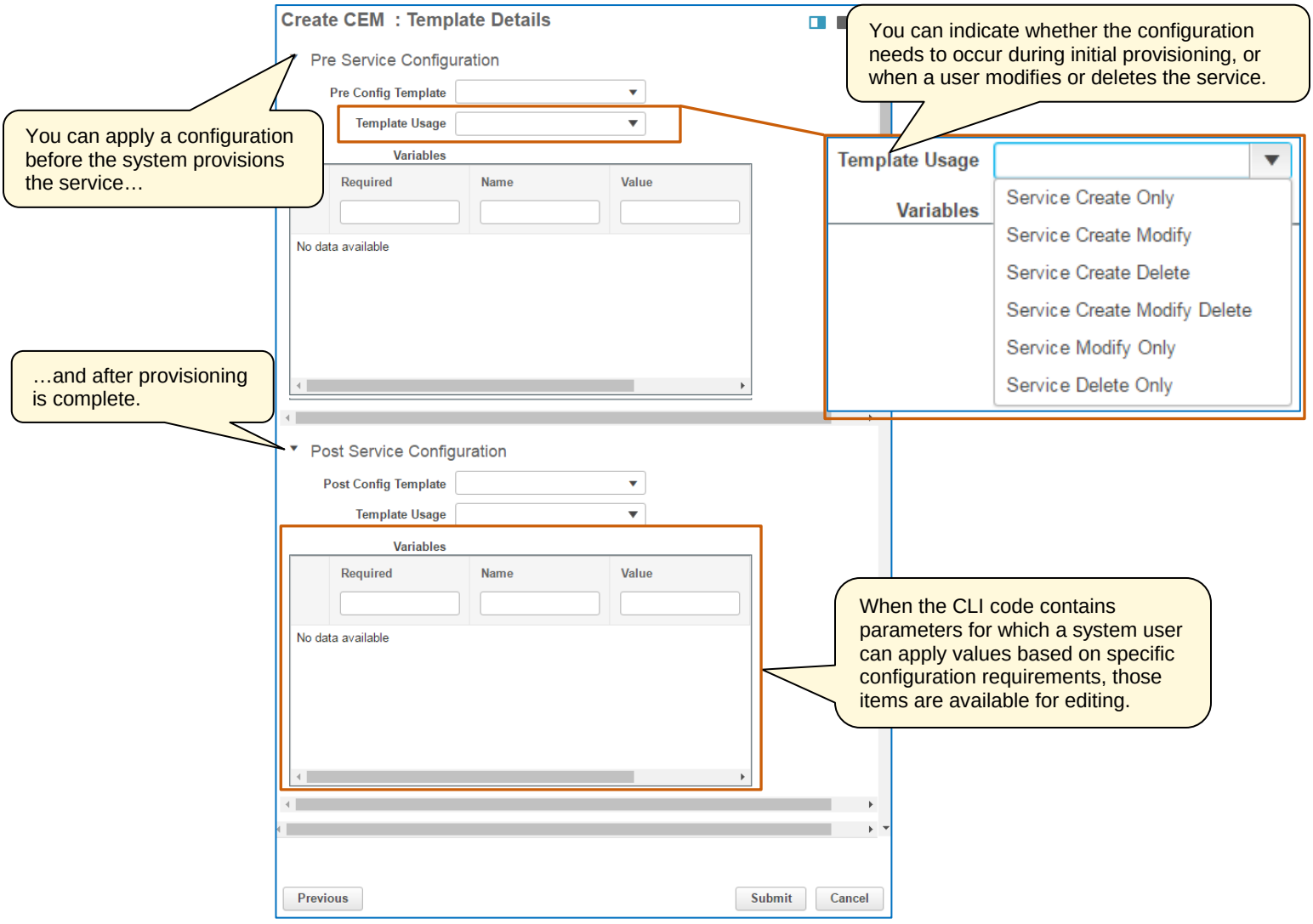
Ingress QoS profiles are used most commonly to manage bandwidth speeds and generally do not apply to constant bit rate services.

Extending Provisioning Functions

Deploying Additional Device Configurations

When you need to extend provisioning functions beyond those that are available with the system, you can include the additional configuration that you need on the **Template Details** page, which is the last page in the **Provisioning Wizard** for CEM services.

This page populates with templates that contain CLI code for device configuration. Cisco EPN Manager provides many templates that include code that uses Cisco validated designs. System users also can configure templates that include code to support unique business or operational requirements.



Video Demonstration

Watching Demonstrations

To watch a demonstration:

- Click a demonstration link below, which opens an MP4 file.

  Based on your system and configuration, you might need to start the video manually.

Note: Video download and streaming times can vary.

Supporting a Customer's Legacy Traffic

Watch the Demonstration

To review the process to provision tunnels and circuit emulation services, watch the **Supporting a Customer's Legacy Traffic** video.

Approximate runtime: 15:00

Links

To Product Information

Visit the Cisco Web site to learn more about EPN Manager.

Visit the Cisco Web site to review or download technical documentation.

To Training

Visit the Cisco Web site to access other EPN Manager learning opportunities.

Visit the Cisco Web site to access learning opportunities for other Cisco products.

To Contact Us

Send us a message with questions or comments about this job aid.

Note: Please send messages that address the content of this job aid or other training questions only.

Please follow your regular business process to request technical support or address technical or application-related questions.