Cisco Crosswork Hierarchical Controller 10.0

Service Provisioning User Guide

December 2024

Introduction

This document is a how-to-use guide for provisioning services for use in Cisco Crosswork Hierarchical Controller.

The services supported are:

- **Cisco Crosswork Hierarchical Controller for optical services**:
    - IP Link
    - OCH Link
    - OCH-NC Link
    - OTN-Line
    - SDH-Liner
    - Circuit E-Line
    - Packet E-Line
- **Cisco Crosswork Hierarchical Controller for dynamic IP VPN services**:
    - L2-VPN
    - L3-VPN

Note: The optical services are provisioned in Service Manager and the dynamic IP VPN services are provisioned via NSO. The dynamic IP services may be viewed in the Service Assurance application.

Architecture

The Crosswork Hierarchical Controller solution includes the Brain and embedded NSO. In the southbound interface, both the Brain and embedded NSO communicate with the domain controller.

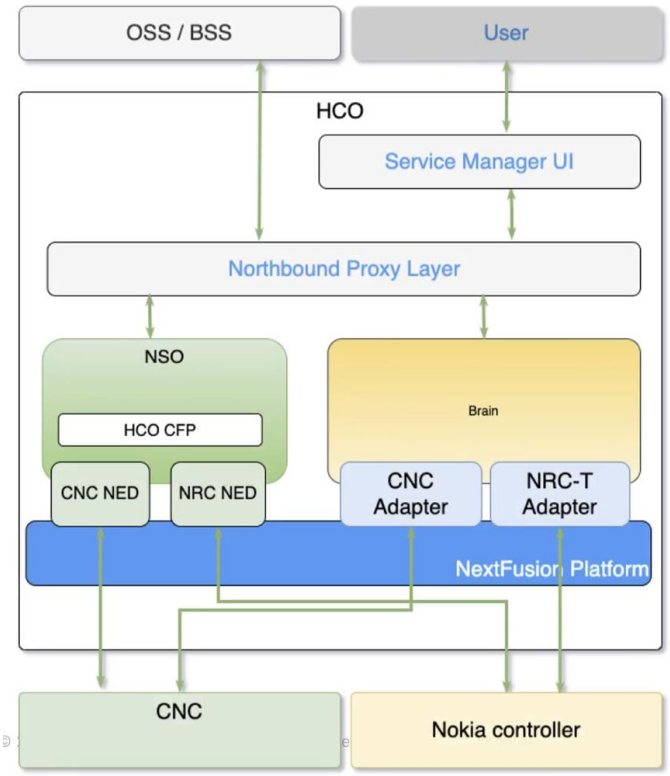


Figure 1.
Crosswork Hierarchical Controller Architecture

In the Northbound interface:

- The embedded NSO provides an RESTCONF, IETF-based interface to L2-VPN and L3-VPN service CRUD (Create, Read, Update, Delete).
- The Brain provides a REST-based interface to get full topology, inventory, and TE paths, all using SHQL queries embedded into REST APIs, and get traffic utilization APIs for ports and TE tunnels.

Contents

The document contains the following sections and explains:

- The need for services management
- Tunnels
- Point to Point
- NSO Provisioning
- Service Settings
- Service Manager Operations
- Network Services Orchestrator Crosswork Hierarchical Controller - Function Pack Appendix

Terminology

Table 1. Terms

Term	Definition
Adapter	The software used by Cisco Crosswork Hierarchical Controller to connect to devices or to device managers.
Agg link	A Link Aggregation Group (LAG) where multiple ETH links are grouped to create higher bandwidth and resilient link.
BGP	Border Gateway Protocol
Circuit E-Line	An Ethernet connection between two ETH client ports on Transponder or Muxponder over OTN signal.
CNC	Cisco Crosswork Network Controller.
CO	Domain controller.
Device	Optical network element, router, or microwave device.
Device Manager	The application that manages the deployed adapters.
eMBB	Enhanced Mobile Broadband.
ETH link	An ETH L2 link that spans from one ETH UNI port of an optical device to another, and rides on top of ODU.
ETH chain	A link whose path is a chain of Ethernet links cross-subnet-connected (found using Crosswork Hierarchical Controller cross-mapping algorithm). Eth-chain is a replacement for R_PHYSICAL link in cases where one side of the link is in a device out of the scope discovered by Crosswork Hierarchical Controller.
Fiber segment	Physical fiber line that spans from one passive fiber endpoint (manhole, splice etc.) to another and is used as a segment in a fiber link.
Fiber	Chain of fiber segments that spans from one optical device to another.
GIS	Geographic Information System.
IGP	The link between two routers that carries IGP protocol messages. The link represents an IGP adjacency.
IP-MPLS	IP multi-protocol label switching.
L3-VPN link	The connection between two sites of a specific L3-VPN (can be a chain of LSP connections or IGP path).
L3 physical	L3 physical is the physical link connecting two router ports. It may ride on top of an ETH link if the IP link is carried over the optical layer.
L3-VPN	A virtual private network based on L3 routing for control and forwarding.
Logical link, IGP, LSP	Logical link connects VLANs on two IP ports.
LSP	Label Switched Path, used to carry MPLS traffic over a label-based path. LSP is the MPLS tunnel created between two routers over IGP links, with or without Traffic Engineering (TE) options.
MLPS Tunnels	MPLS TP tunnels may use ETH (L1 Ethernet links) or R_PHYSICAL (L2 Ethernet links) underlay topologies, and can be used as an underlay for Packet E-Line services,
NMC (OCH-NC, OTSiMC)	The link between the xPonder facing ports on two ROADMs. This link is the underlay for OCH and it is an overlay on top of OMS links. This is relevant only for disaggregation cases where the ROADM and OT box are separated.
NMS	Network Management System.
Nokia NSP	Nokia Network Service Provider.

Term	Definition
OC/OCG	SONET/SDH links that span from one optical device to another and carry SONET/SDH lower bandwidth services, the links ride on top of OCH links and terminate in TDM client ports.
OCH	OCH is a wavelength connection spanning between the client port one OT device (transponder, muxponder, regen) and another. 40 or 80 OCH links can be created on top of OMS links. The client port can be a TDM or ETH port.
OCH-NC	Wavelength link. New service is added as NMC link.
ODU	ODU links are sub-signals in OTU links. Each OTU links can carry multiple ODU links, and ODU links can be divided into finer granularity ODU links recursively.
ONC	Cisco Optical Controller (ONC).
OSPF	Open Shortest Path First, an Interior Gateway Protocol between routers.
OTN-Line	An OTN connection between two ODU client ports over OTN path.
OTS	OTS is the physical link connecting one line amplifier or ROADM to another. An OTS can be created over a fiber link.
out	OTU is the underlay link in OTN layer, used for ODU links. It can ride on top of an OCH.
Packet E-Line	A point-to-point connection between two routers or transponders/muxponders over MPLS-TP or IP-MPLS.
PCC	Path Computation Client. Delegated to controller. Router is responsible for initiating path setup and retains the control on path updates.
PCE	Path Computation Element. Controller-initiated.
QAM	Quadrature Amplitude Modulation.
QPSK	Quadrature Phase Shift Keying modulation. This carries less information per symbol than QAM modulation.
Radio Media	The media layer as a carrier of radio channels.
Radio Channel	Multiple radio channels can be on top of radio media, each channel represents a different ETH link with its own rate.
RD	Route Distinguisher.
RSVP-TE	Resource Reservation Protocol to control traffic engineered paths over MPLS network.
RT	Route Target.
SCH	A super-channel is an evolution of DWDM in which multiple, coherent optical carriers are combined to create a unified channel of a higher data rate, and which is brought into service in a single operational cycle.
SDH-Line	SDH line between STM-64 or STM-256 ports.
SDN Controller	Software that manages multiple routers or optical network elements.
SR Policy	Segment Routing Policy. A segment routing path between two nodes, with mapping to the IGP links based on SIDs list.
STS	Large and concatenated TDM circuit frame (such as STS-3c) into which ATM cells, IP packets, or Ethernet frames are placed. Rides on top of OC/OCG as optical carrier transmission rates.
TDM	Time Division Multiplexing.

Term	Definition
uRLLC	Ultra-Reliable Low Latency Communications.
VRF	Virtual Routing Function, acts as a router in L3-VPN.
ZR Media	The media layer as a carrier of ZR channels, on top of OCH link.
ZR Channel	Multiple ZR channels can be on top of ZR media, each channel represents a different IP link with its own rate.

Service Provisioning

Crosswork Hierarchical Controller supports the creation of new transport client services and photonic services.

Crosswork Hierarchical Controller abstracts the service model and provides users with a simple and intuitive user interface to provision new services.

It is assumed that domain controller implicitly handles the creation/use of the underlay path (OTSiMC, OTN, MPLS-TP) as required to fulfil the service request.

The table below defines the required parameters per service type.

Crosswork Hierarchical Controller requires the optical controller to support the connectivity-service API by TAPI. A proper use of the layers is needed per the service type.

Table 2. Provisioning parameters

Service Type	Provisioning Parameters
IP Links	• Service name • Service ID • Link rate mode • Endpoints and transmit power • Link IP addresses • L Band/C Band • Frequency • Digital-to-Analog Converter (DAC) rate • Modulation • Included nodes/links in path • Excluded nodes/links from path • Disjoint from a path of an existing service
OCH-NC/OTSiMC (between ROADMs)	• Service name • Service ID • Bandwidth

Service Type	Provisioning Parameters

	• Baud rate
	• Frequency
	• Protection option (1+1, 1+1+r)
	• Endpoints
	• Optimization goal (minimize path by admin cost, latency, or number of hops)
	• Per path, for main, redundant, and restored paths
	  ◦ Included nodes/links in path
	  ◦ Excluded nodes/links from path
	• Disjoint from a path of an existing service

Photonic Services (OCH Trail between OT/Transponders)	• Service name
	• Service ID
	• Bandwidth
	• Baud rate
	• Frequency
	• Protection option (1+1, 1+1+r)
	• Endpoints
	• Optimization goal (minimize path by admin cost, latency, or number of hops)
	• Per path, for main, redundant, and restored paths
	  ◦ Included nodes/links in path
	  ◦ Excluded nodes/links from path
	• Disjoint from a path of an existing service

Circuit E-Line /OTN Line/SDH Line	• Service name
	• Service ID
	• ODU signal/ETH rate/SDH STM rate
	• Protection option (1+1, 1+1+r)
	• Endpoints
	• Optimization goal (minimize path by admin cost, latency, or number of hops)
	• Per path, for main, redundant, and restored paths
	  ◦ Included nodes/links in path
	  ◦ Excluded nodes/links from path
	• Disjoint from a path of an existing service

Service Type	Provisioning Parameters

Packet E-Line	• Service name
	• Service ID
	• Protection option (1+1, 1+1+r)
	• Endpoints
	  ◦ CIR/EIR
	  ◦ VLAN IDs
	• Optimization goal (minimize path by admin cost, latency, or number of hops)
	• Per path, for main, redundant, and restored paths
	  ◦ Included nodes/links in path
	  ◦ Excluded nodes/links from path
	• Disjoint from a path of an existing service

Crosswork Hierarchical Controller in Brief

The Crosswork Hierarchical Controller product family is a set of software applications built on a common Crosswork Hierarchical Controller platform, designed to accelerate automation and to increase efficiency and reliability of service providers networks. Crosswork Hierarchical Controller addresses the role of the multi-domain, multi-layer, and multi-vendor network controller.

This innovative capability to learn the mapping between IP/MPLS and optical layer ports (cross-layer mapping) is key to providing a comprehensive view of the network. This has historically been a very difficult problem to solve since there are no standards to automatically provide discovery of such links. This process applies to IP/MPLS-optical links, as well as to cross-domain optical links.

Achieving automation of the complete process, without compromising on resiliency must involve fibers discovery and GIS information. Both enable the understanding of risks in planning phases and crucial information to assess failure impact on services in operations.

Crosswork Hierarchical Controller is fully multi-layer and multi-vendor. The system interfaces with SDN Domain Controllers for the packet layers (IP, MPLS) and transport layers (WDM, OTN, Packet-Optical, Microwave) to create a coherent view of the entire transport network, as shown in Figure 1 below, and enables automation of its functions and simplified abstracted interaction with Service Orchestrators and OSS tools.

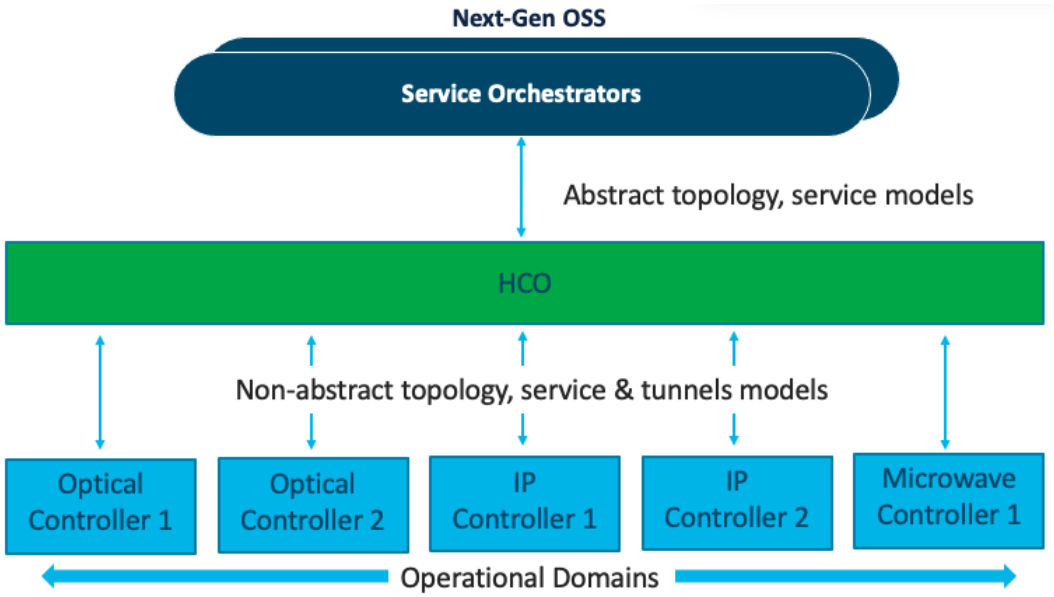


Figure 2.
Transport SDN Architecture

Service Management – The Need

Service Manager is a key Cisco Crosswork Hierarchical Controller application that allows for the creation of L1-L3 services and L1-L3 underlay tunnels and links across the entire SP network.

Crosswork Hierarchical Controller can discover L1-L3 services from area/domain controllers. It can discover intra-domain and inter-domain E-Line and L3-VPN services while completing the information on all LSPs along the path, VRFs, and all inter-AS options. This allows Crosswork Hierarchical Controller to discover existing services, as well as new services it has provisioned.

Crosswork Hierarchical Controller supports service lifecycle state (provisioned, pending, planned), operational state and admin state.

Basic service instantiation is supported by the Domain Controller for each domain. However, none of the Domain Controllers understand how to achieve a globally optimal path for an end-to-end service.

Using its own global Path Computation Element (PCE), Crosswork Hierarchical Controller can calculate the optimal end-to-end multidomain path for the service, set it up in each Domain Controller and make sure the service parts are stitched together across domain boundaries.

In fact, a service can span different layers for its delivery. For example, an E-Line service can start on an OTN metro network, then be handed off to the MPLS core network, where it is carried over a pseudowire (PW) in an MPLS tunnel, and then over a packet-optical access network to its final destination. Crosswork Hierarchical Controller figures out which layers should be used to set up the service, based on user-defined policies.

Crosswork Hierarchical Controller supports IP services as defined by IETF in L2NM, L3NM and optical services as defined by ONF TAPI interface.

Crosswork Hierarchical Controller abstracts the service configuration and provides simple, intent-based API and UI to create new services with endpoint details, SLA, and associations to a predefined template that can be overridden for better adjustment.

Services and tunnels currently supported for provisioning and modification by the Service Manager:

- Tunnels:
    - RSVP-TE tunnel over single domain
    - SR policy over single domain
    - MPLS-TP tunnel
- Point-to-Point:
    - IP links between two routers over ZR/+ and over alien lambda (as multi-vendor optical network)
    - OCH Link
    - OCH-NC Link
    - OTN Line
    - SDH Line
    - Circuit E-Line
    - Packet E-Line over packet-optical network

Endpoints can be added to the UI wizard by selecting them from the inventory. Ports enabled for selection are those applicable for the service type. Per endpoint, the bandwidth can be defined (as CIR, EIR, CBS, PBS) and VLAN and COS classification can be added.

Crosswork Hierarchical Controller has a sophisticated global multilayer PCE to calculate services and underlay paths. The calculation is based on the selected criteria: number of hops, latency, or admin cost. It also considers the preferences for protection, diversity, SRLG, specific links, devices, or service paths to include or exclude, and resources available per the requested bandwidth.

PCE works over multiple domains, where it can calculate paths' diversity between domains as a full path of end-to-end service.

Depending on the implementation, PCE knows how to work with vendor-specific capabilities and constraints and how to verify the feasibility of a path before putting it in action.

Creation of a service is managed as a network transaction. Commands are sent to all participating Domain Controllers. Upon completion, the configuration undergoes validation in all domains before notifying the user of configuration success. In the event of failure, PCE knows to roll back and leave no broken configuration in any Domain Controller.

This transaction mechanism knows how to overcome a failure in Crosswork Hierarchical Controller because the backup system can continue tracking the transaction and act according to the response from the Domain Controllers.

Each action on a service or tunnel (creation, modification, deletion) done via the UI or via APIs is recorded as an operation. An operation contains the full details of the action and its results, log of the service

scheme sent to the controllers, the returned results, error messages from domain controllers, and the operation status.

Operations can be viewed per selected service or tunnel and as a list of all operations.

Modify Payload

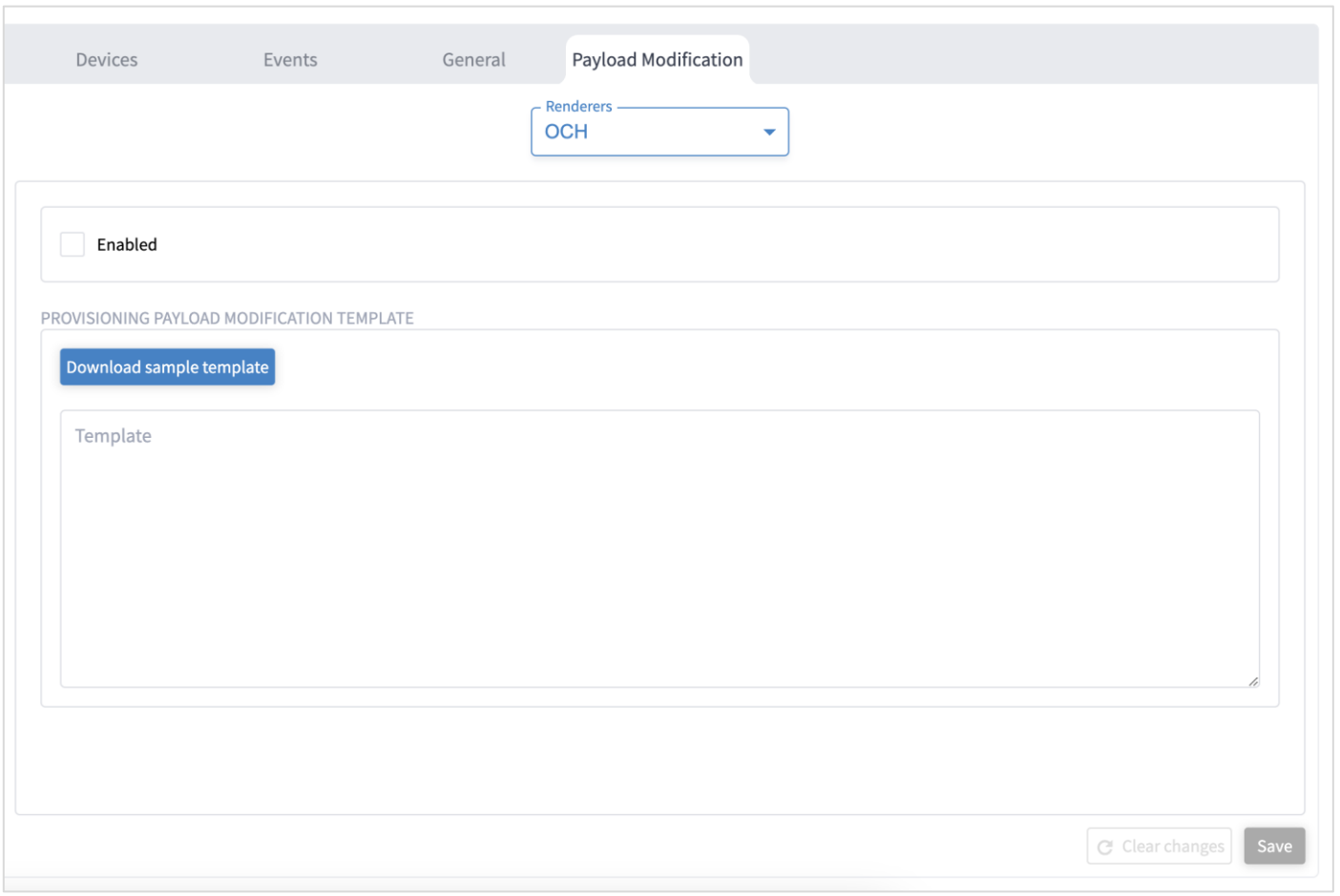
The Service Manager application in Crosswork Hierarchical Controller provides service intents with a common set of parameters supported by all the vendors. in many cases vendors provide extensions to the service model with unique service attributes which are not covered in the common model.

The Payload Modification feature enables you to set a default value for these extended attributes so that Crosswork Hierarchical Controller can set the desired values when activating a service. The configuration that will be set on the controller will be the common service intent plus the default values as set in the Payload Modification feature.

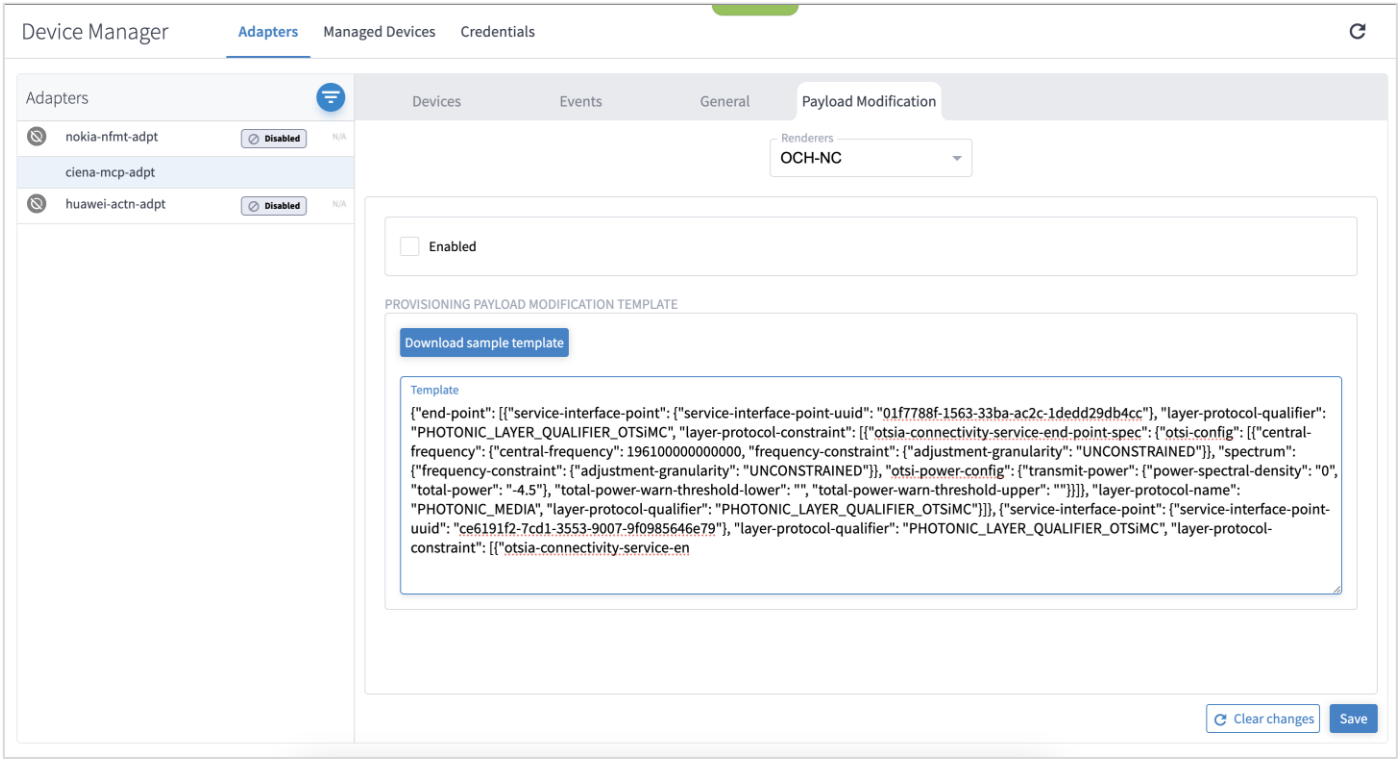
The ability to edit the adapter payload in the Device Manager application (and the **Payload Modifications** tab) is only available for specific adapters and for OTN-Lines.

To modify the payload:

1. In the applications bar in Crosswork Hierarchical Controller, select **Services > Device Manager**.
2. Select the required adapter.
3. Select the **Payload Modification** tab.
4. From the **Renderers** dropdown, select the required payload.



5. To download a sample payload, click **Download sample template**.
6. Make the modifications to the template and copy it into the **Template** area.



7. To enable the payload, select **Enabled**.
8. Click **Save**. The template is validated and if valid, applied to the adapter for the specific renderer.

OTN-Line Service Provisioning Payload Example

You can use an existing service provisioning payload and add keys (with their values) or modify existing key values. You cannot delete keys. For example, this creates a Vendor tag and assigns the value Ciena to all the inventory items with vendor equal to Ciena.

```
{
  "end-point":[
    {
      "service-interface-point":{
        "service-interface-point-uuid":"01f7788f-1563-33ba-ac2c-1dedd29db4cc"
      },
      "layer-protocol-qualifier":"ODU_TYPE_ODU4"
    },
    {
      "service-interface-point":{
        "service-interface-point-uuid":"ce6191f2-7cd1-3553-9007-9f0985646e79"
      },
      "layer-protocol-qualifier":"ODU_TYPE_ODU4"
    }
  ],
  "name":[
    {
```

```
            "value-name":"label",
            "value":"ODU2-Service"
          }
        ],
        "layer-protocol-name":"ODU",
        "resilience-type":{
          "protection-type":"NO_PROTECTION"
        },
        "include-link":[
          "12345678-7cd1-3553-9007-9f0985646e79"
        ]
      }
```

Brownfield Services

Service Manager allows you to view and delete services that were not created by Crosswork Hierarchical Controller but are discovered and managed by the CO (domain controller). For these services, they appear as **Is Brownfield: True**.

The following delegated service types are supported: Packet E-Line, Circuit E-Line, OTN-Line, and OCH (Wavelength) services.

Tunnels

A tunnel is a unidirectional link between source and destination routers, riding over IGP links with only primary, or primary and secondary LSPs. You can create tunnels of type:

- RSVP
- SR Policy
- MLPS-TP Tunnel

View Tunnels

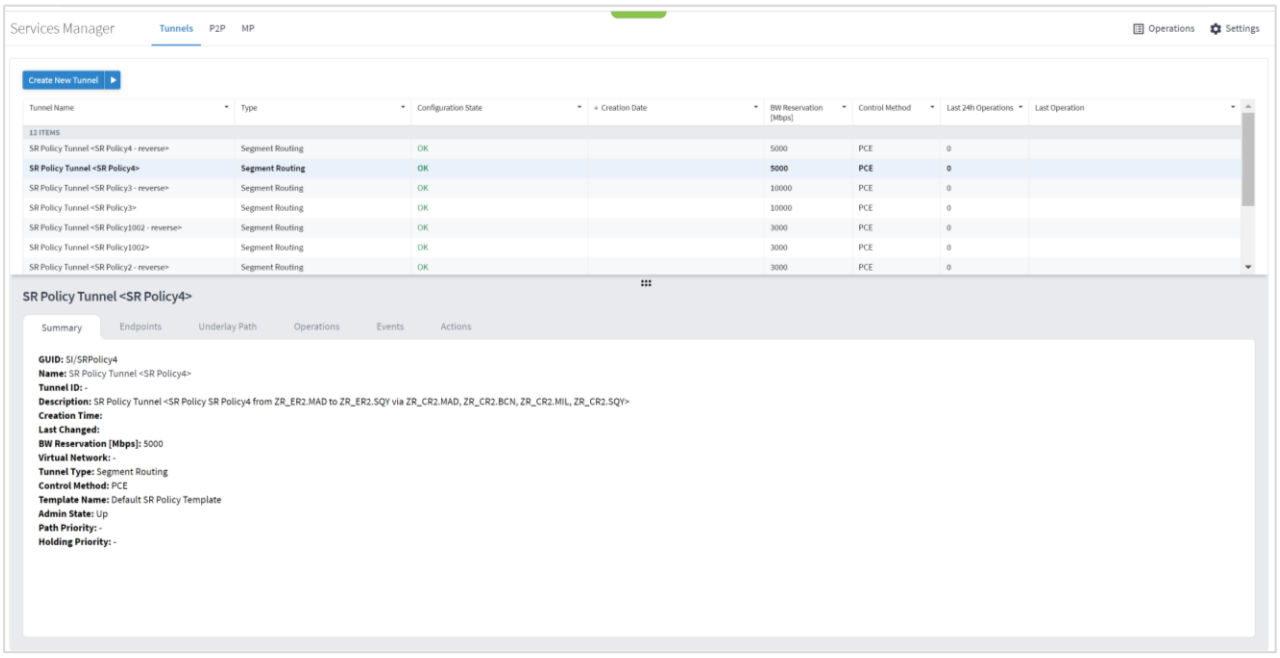
You can view a list of the tunnels.

To view tunnels:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Tunnels**. A list of the tunnels appears in the **Tunnels** pane with the following information:
    - **Tunnel Name:** The tunnel name.
    - **Type:** The type of tunnel, for example, **Segment Routing**.
    - **Configuration State**: The configuration state (**OK**, **ABANDONED**, **REMOVED**).
    - **Creation Date:** The date the tunnel was created.
    - **BW Reservation (Mbps):** The bandwidth reserved for the tunnel.
    - **Control Method:** The control method: by device **(PCC)** or by controller **(PCE).**
    - **Last 24H Operations:** The volume of operations in last 24 hours.

- **Last Operation:** The last operation executed on the tunnel.

2. Select the required tunnel.
3. To view more tunnel details, see the lower pane view with the following tabs:
    - **Summary:** Additional details about the tunnel, such as, Description, Admin State.
    - **Endpoints:** The source and destination endpoint details.
    - **Underlay Path:** The underlay path items traversed by the tunnel.
    - **Operations:** The tunnel operations.
    - **Events:** The tunnel events.
    - **Actions:** The modification actions (if applicable) and the option to **Delete Tunnel.**

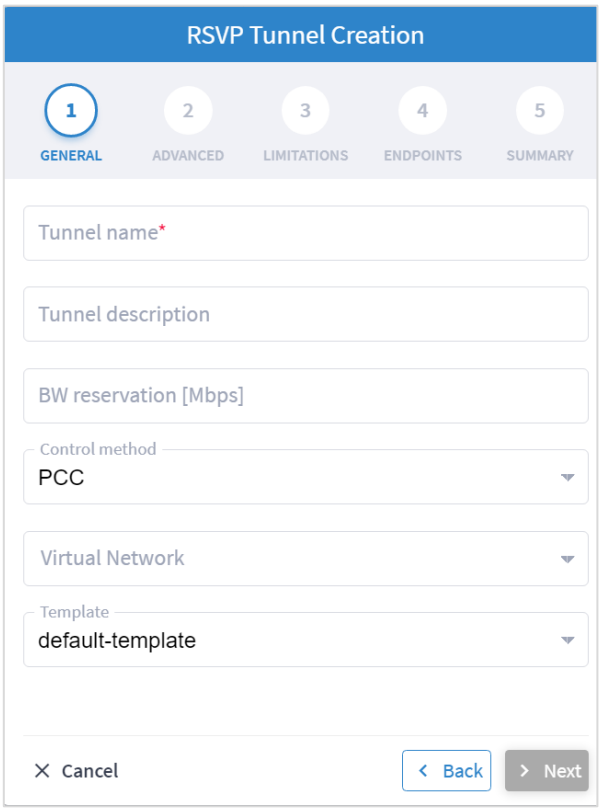


Add RSVP Tunnel

You can create an RSVP tunnel between source and target endpoints, with a bandwidth reservation, controlled by device or controller, associated with a specific virtual network. Various advanced settings and limitations (items to be included or excluded from the path) can be added. An RSVP tunnel can only be created over a single domain.

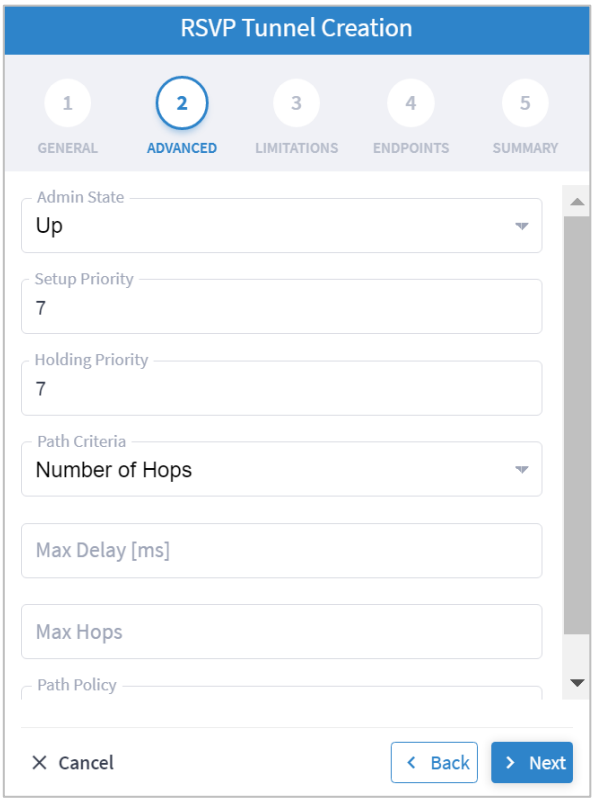
To add a RSVP tunnel:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Click **Create New Tunnel**.
3. Select **RSVP**.



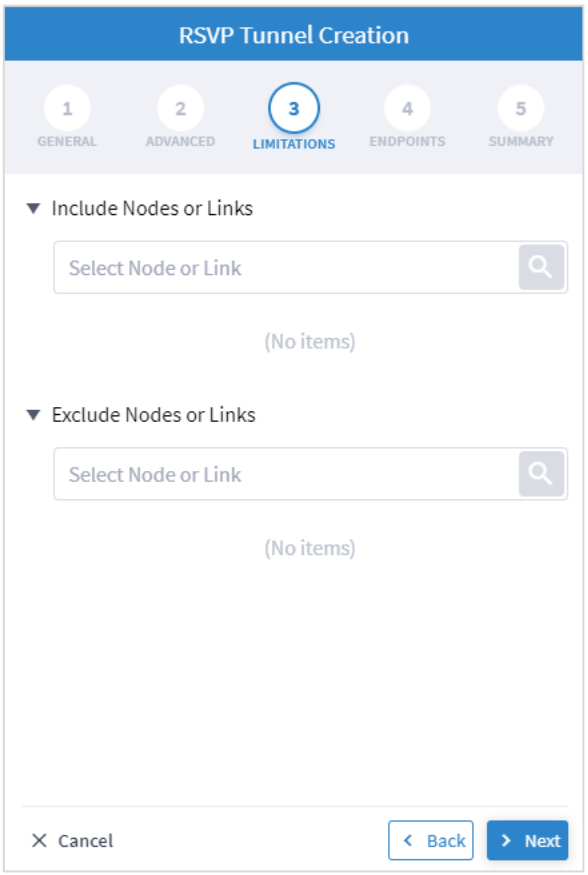
4. Specify the following **GENERAL** settings:
    - **Tunnel name**: The unique user defined name of this tunnel.
    - **Tunnel description**: A description of the tunnel.
    - **BW reservation (Mbps)**: The bandwidth reserved for this tunnel.
    - **Control method**: The control method, by device (**PCC**) or by controller (**PCE**).
    - **Virtual Network**: The virtual network (tunnels can be grouped using tags to construct a virtual network. L3-VPN can be assigned to specific virtual network).
    - **Template**: This is not available in the current version (there is a **default-template**).

5. Click **Next**.

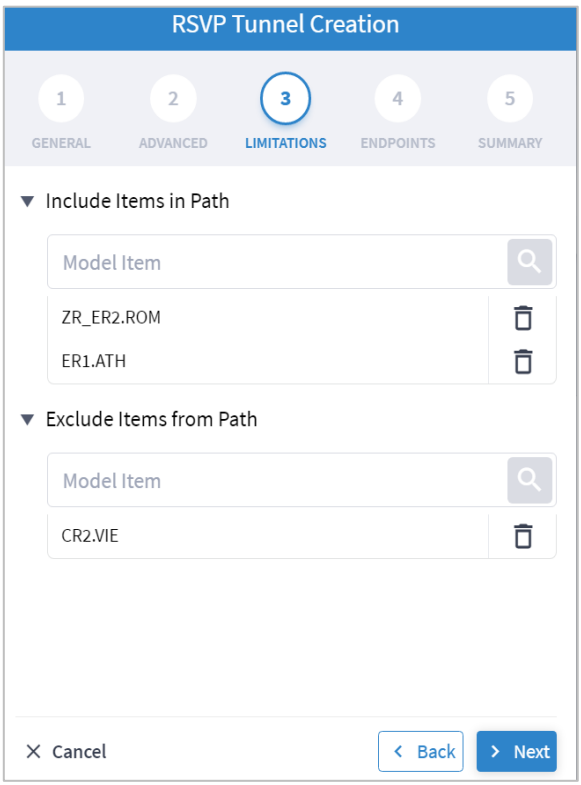


6. Specify the following **ADVANCED** settings:
    - **Admin State**: The admin state (**Up** or **Down**).
    - **Setup Priority**: The setup priority (between 0 and 7). Default is 7.
    - **Holding Priority**: The holding priority (between 0 and 7). Default is 7.
    - Path Criteria: The path control method (Number of Hops or Latency or Admin Cost).
    - **Max Delay (ms)**: The maximum permissible delay in 100 of ms (between 0 to 500). Only relevant when the path criteria is set to **Latency**.
    - **Max Hops**: The maximum number of hops (between 1 to 100). Only relevant when path criteria is set to **Number of Hops**.
    - **Path Policy**: Select a policy (**Strict** or **Loose**). If **Strict**, must include the list of nodes and IGP links to be included in the new tunnel path.

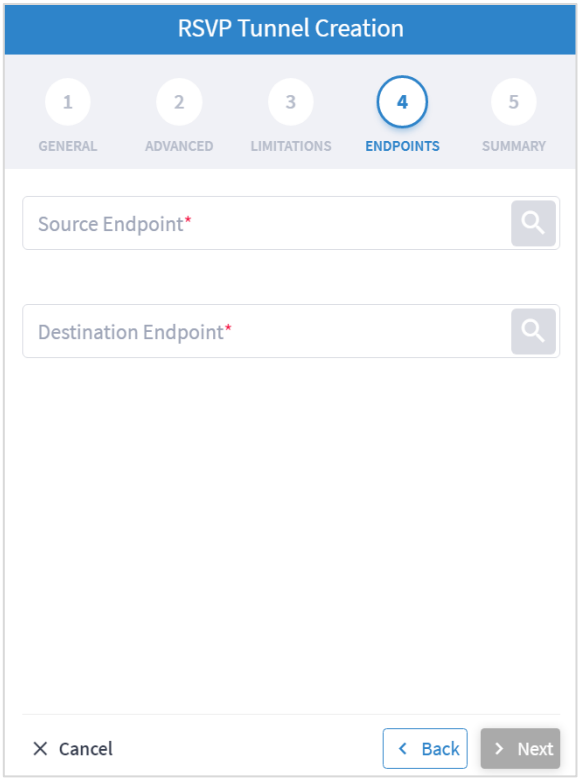
7. Click **Next**.



8. Specify the following **LIMITATIONS** settings:
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select node or IGP link, or click on the **3D Explorer** tab to select node or IGP link.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select node or IGP link, or click on the **3D Explorer** tab to select node or IGP link.
    - (Optional) Click to remove any of the include/exclude items.



9. Click **Next**.

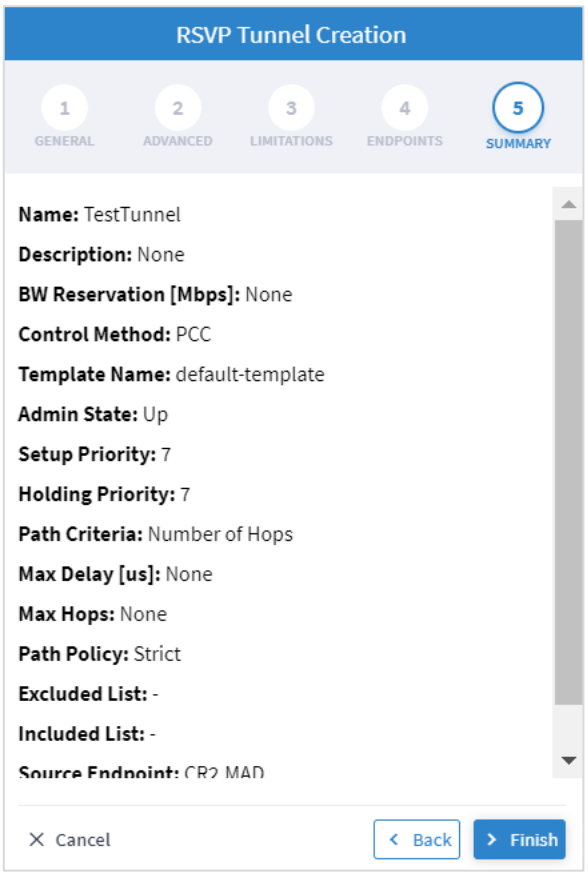


10. Specify the following **ENDPOINTS** settings:

    - **Source Endpoint**: Click and select the node (router) or IGP interface as the source endpoint.

- **Destination Endpoint**: Click and select the node (router) or IGP interface as the destination endpoint.

11. Click **Next**.
12. Review the **SUMMARY**.



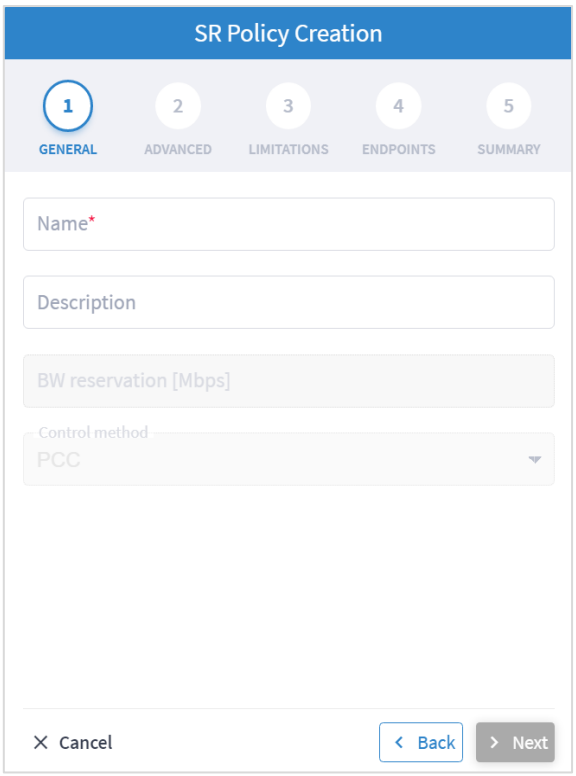
13. Click **Finish**.

Add SR Policy Tunnel

The Crosswork Hierarchical Controller network model supports Segment Routing (SR) Policies and SR Segments over IGP links, and the Crosswork Hierarchical Controller adapters can discover policies from network controllers, with their SID list, color, preference, and candidate path attributes. It maps all discovered policies to create SR Segments as a layer between IGP links and SR policies. An SR Segment is the path between two SIDs, shared by multiple SR policies. An SR Policy tunnel can only be created over a single domain.

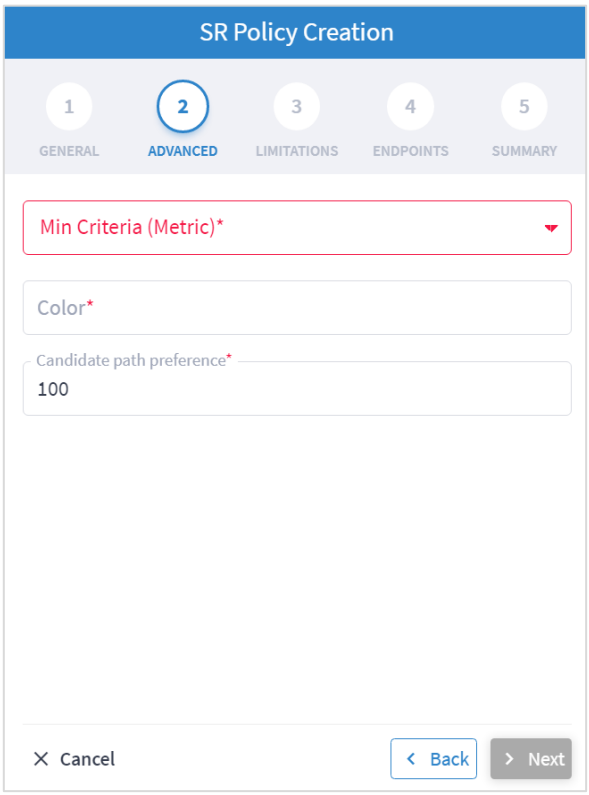
To add an SR Policy tunnel:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
1. Click **Create New Tunnel**.
2. Select **SR Policy**.



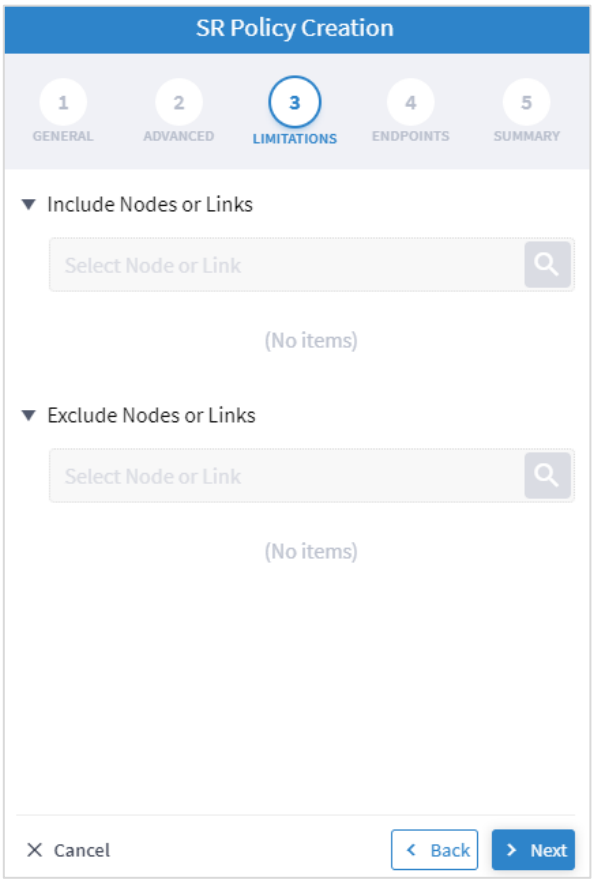
3. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this SR Policy.
    - **Description**: A description of the SR Policy.

4. Click **Next**.



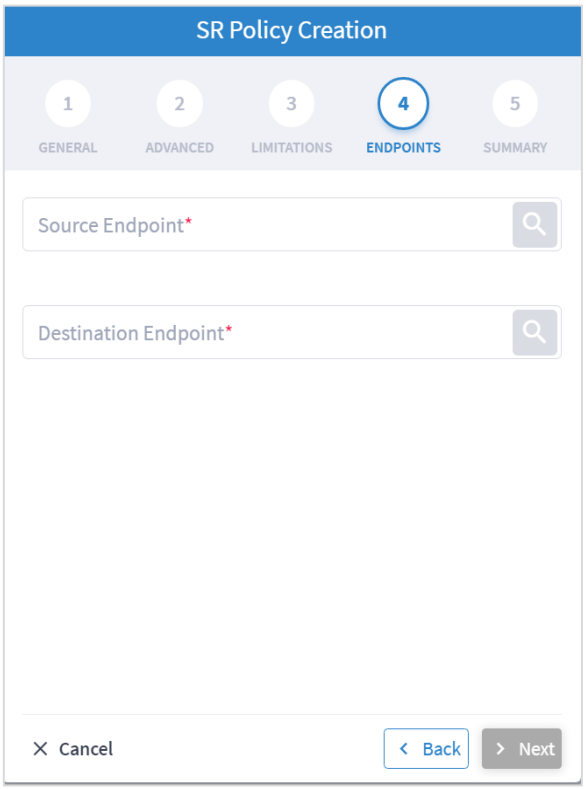
5. Specify the following **ADVANCED** settings:
    - **Min Criteria (Metric)**: The criteria metric to minimize (**IGP**, **TE**, **Delay** or **Number of Hops**).
    - **Color**: The SR Policy color (a unique identifier of the policy). This is a numerical value that distinguishes between two or more policies to the same node pairs.
    - **Candidate path preference**: The candidate path preference (integer value). The highest preference path is the active one. Multiple candidate paths per policy are currently not support.

6. Click **Next**.



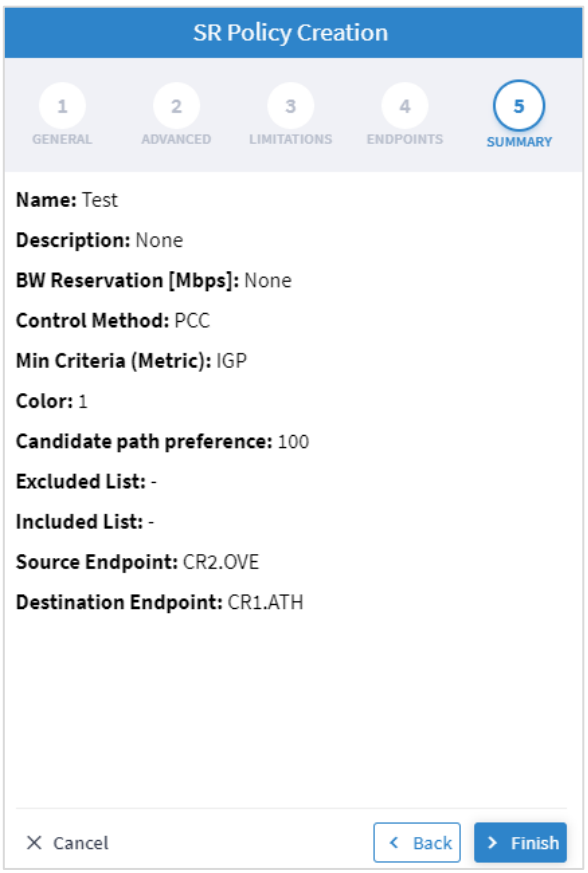
7. Specify the following **LIMITATIONS** settings:
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select node or IGP link, or click on the **3D Explorer** tab to select node or IGP link.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select node or IGP link, or click on the **3D Explorer** tab to select node or IGP link.
    - (Optional) Click  to remove any of the include/exclude items.

8. Click **Next**.



9. Specify the following **ENDPOINTS** settings:
    - **Source Endpoint**: Click and select the node (router) or IGP interface as the source endpoint.
    - **Destination Endpoint**: Click and select the node (router) or IGP interface as the destination endpoint.

10. Click **Next**.
11. Review the **SUMMARY**.



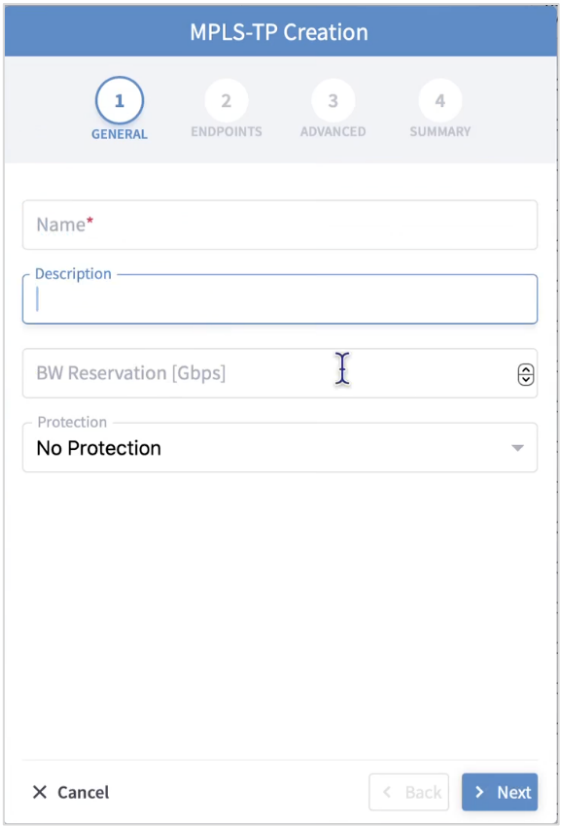
12. Click **Finish**.

Add MPLS-TP Tunnel

You can create an MPLS-TP tunnel as an underlay for Packet E-Line services between source and target endpoints, with a bandwidth reservation. Various advanced settings and limitations (items to be included or excluded from the path) can be added.

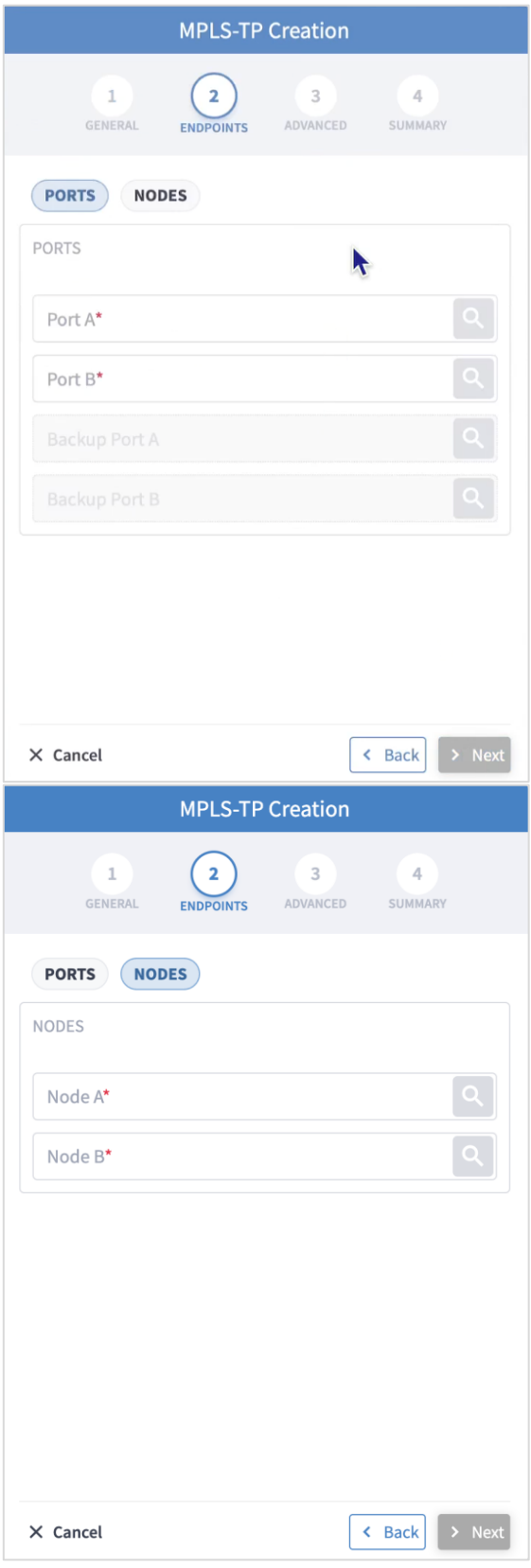
To add an MPLS-TS tunnel:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Click **Create New Tunnel**.
3. Select **MPLS-TS**.

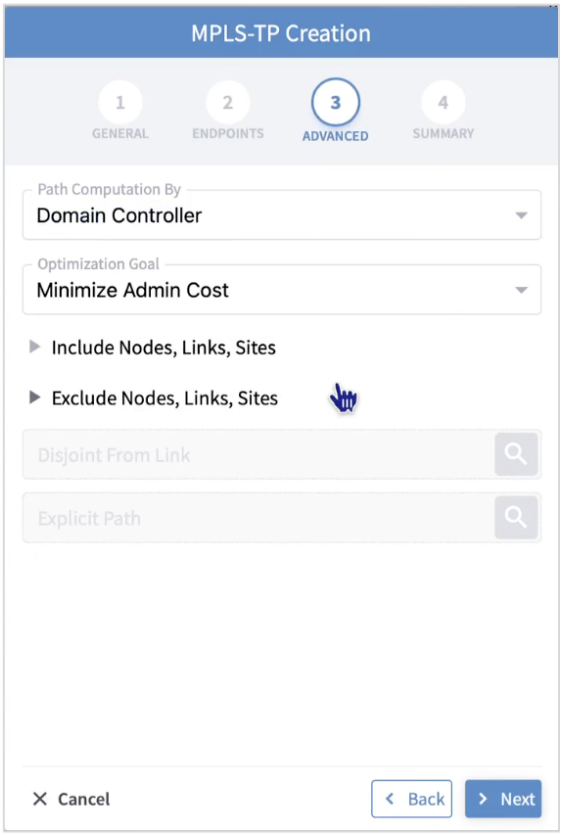


4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this MPLS-TS tunnel.
    - **Description**: A description of the MPLS-TS tunnel.
    - **BW Reservation [Gbps]**: The bandwidth reserved for the tunnel.
    - **Protection**: The service protection (**No Protection** or **Protection 1+1**)

5. Click **Next**.



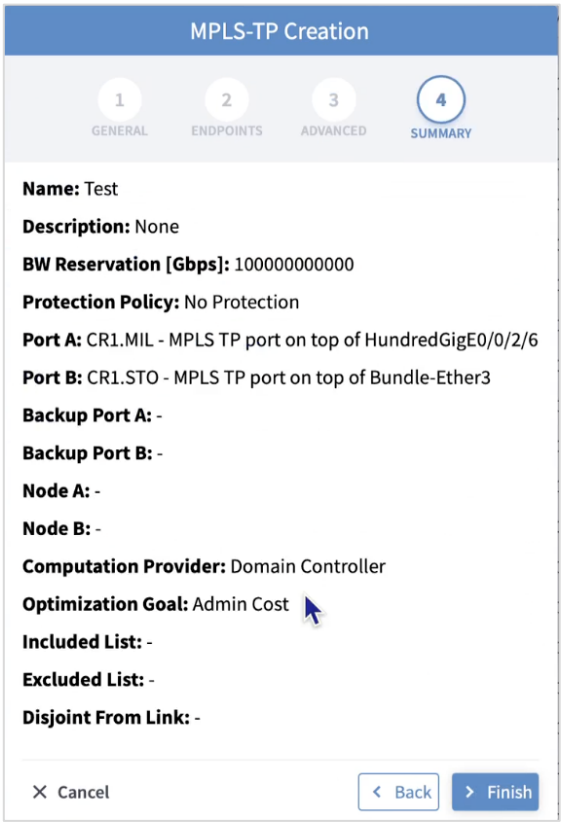
6. Specify the following **ENDPOINTS** settings, by selecting the **PORTS** or **NODES**:
    - **Port A**: Click and select the source port.
    - **Port B**: Click and select the destination port.
    - **Backup Port A**: Click and select the backup source port (only available for **Protection 1+1**).
    - **Backup Port B**: Click and select the destination port (only available for **Protection 1+1**).
    - **Node A**: Click and select the source endpoint (only available for **No Protection**).
    - **Node B**: Click and select the destination endpoint (only available for **No Protection**).
7. Click **Next**.



8. Specify the following **ADVANCED** settings:
    - **Path Computation By**: Select **Domain Controller** or **HCO**.
    - **Optimization Goal**: The optimization goal (**Minimize Latency** or **Minimize Admin Cost**).
    - **Include Nodes, Links, Sites**: Click , select node, link, or site, or click on the **3D Explorer** tab to select node, link, or site.

- **Exclude Nodes, Links, Sites**: Click and in the **Advanced** tab, select node or IGP link, or click on the **3D Explorer** tab to select node or IGP link.
- (Optional) Click to remove any of the include/exclude items.

9. Click **Next**.



10. Review the **SUMMARY**.
11. Click **Finish**.

Delete Tunnel

To delete a tunnel:

1. In the applications bar in Crosswork Hierarchical Controller, select **Device Manager**.
2. Select a tunnel.
3. Select the **Actions** tab.
4. Click **Delete Tunnel**. A confirmation message appears.
5. Click **Confirm**. The tunnel is deleted.

Point-to-Point

You can create a point-to-point service of type:

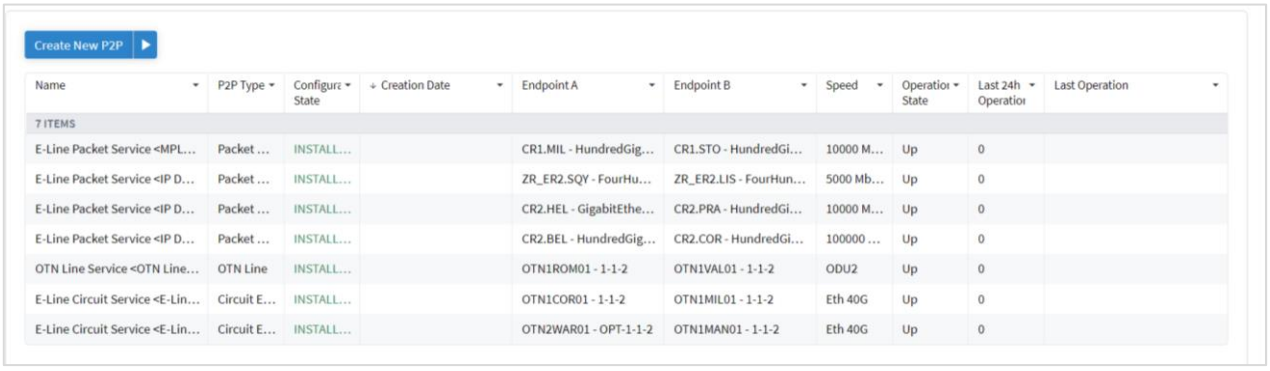
- IP Link
- OCH Link
- OCH-NC Link
- OTN-Line
- SDH-Line
- Circuit E-Line
- Packet E-Line

View Point to Point

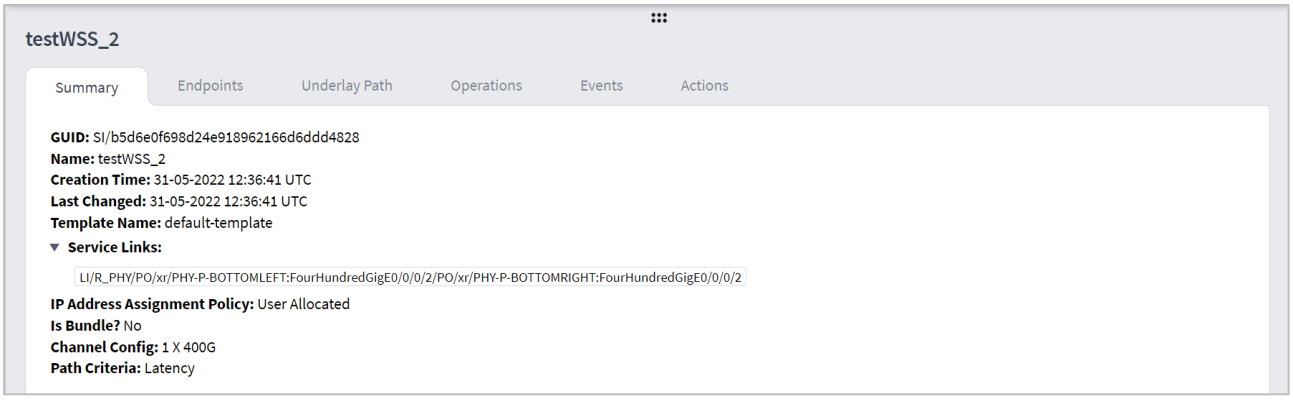
You can view a list of the Point to Point services.

To view PSP services:

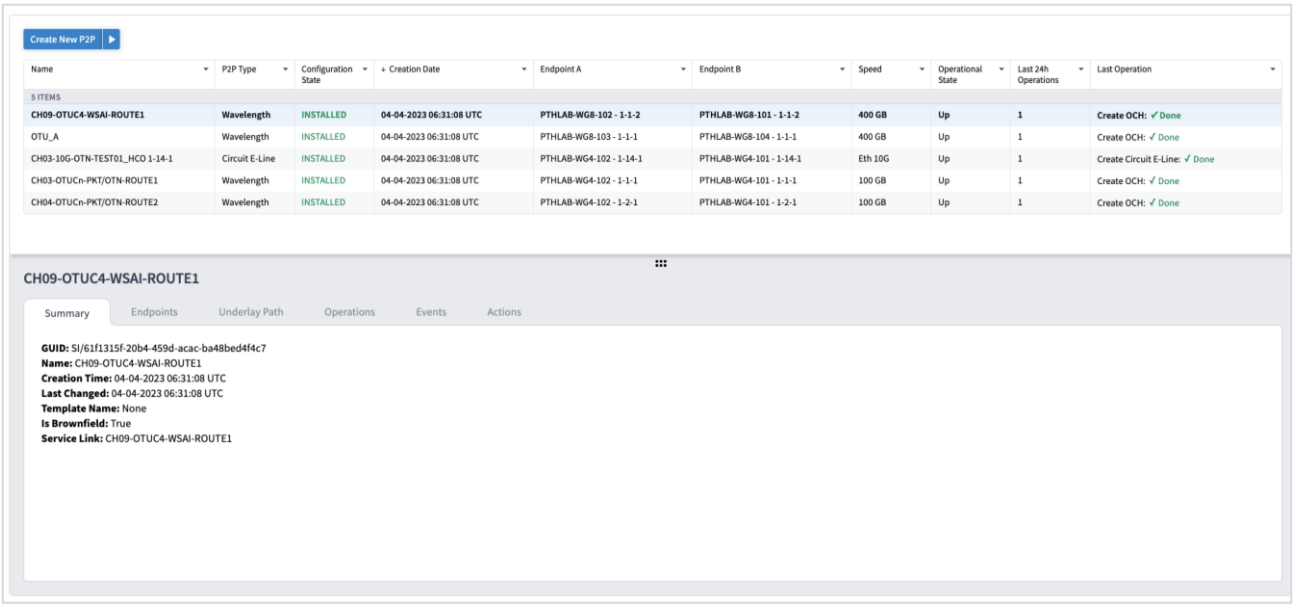
6. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Point to Point**. A list of the point-to-point services appears in the **Point to Point** pane.



7. Select the required point-to-point service.
8. To view more point to point link details, see the lower pane view with the following tabs:
    - **Summary:** Additional details about the point to point links.
    - **Endpoints:** The source and destination endpoint details.
    - **Underlay Path:** The underlay path items traversed by the link.
    - **Operations:** The point to point link operations.
    - **Events:** The point to point link events.
    - **Actions:** The modification actions (if applicable) and the option to Delete P2P.



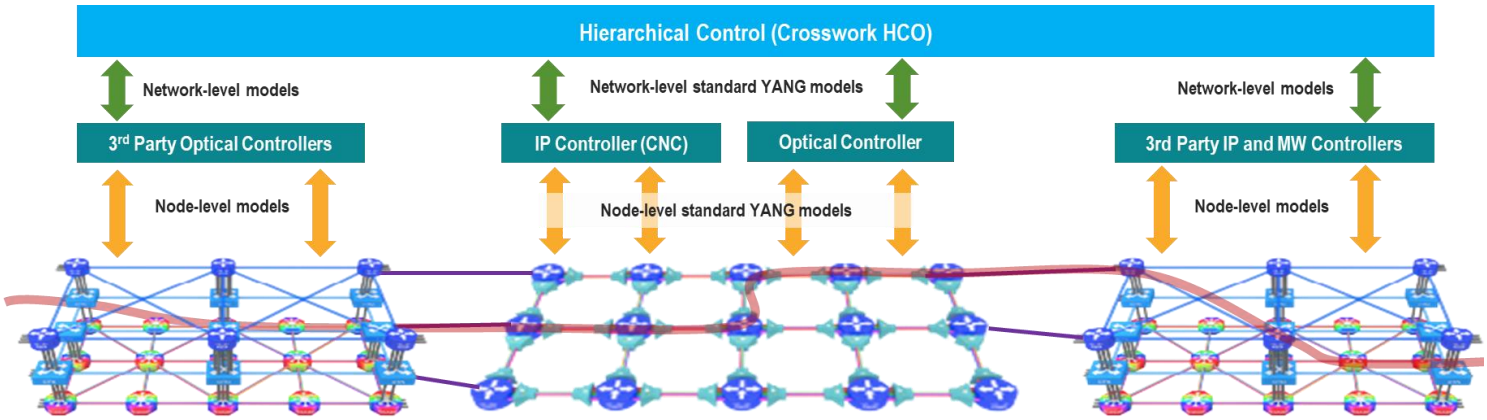
For services that were created by using the MCP controller and not the Services Management application, the service appears as **Is Brownfield: True**. The Crosswork Hierarchical Controller MCP adapter discovers these services and creates service intent for each of them. The following delegated service types are supported: Packet E-Line, Circuit E-Line, OTN-Line, SDH-Line and OCH (Wavelength) services.



Create IP Link

You can create an IP Link between two ZR pluggable components in routers (creating a new link or adding it to a LAG). Various advanced settings and limitations (such as node or link to be included in the path or excluded from the path of the OCH Link) can be added. The end-to-end service between ZR/+ ports may optionally traverse through OLSs (or ONEs, Optical Network Elements, Cisco, or 3rd party). Crosswork Hierarchical Controller decomposes the service into domains and provisions the optical line between ROADMs on the optical domain controller. The activation mode works directly from Crosswork Hierarchical Controller to IP and optical domain controllers (Cisco Crosswork Network Controller, ONC).

ZR and ZR+ pluggables manufactured by Cisco output a maximum of -10dBm. There are ROADM setups that can benefit from or require a stronger signal. The new ZR bright pluggable outputs 0dBm and is supported for IP provisioning. BRT appears in the device description, for example, Cisco QDD 400G BRT ZRP Pluggable Optics Module.



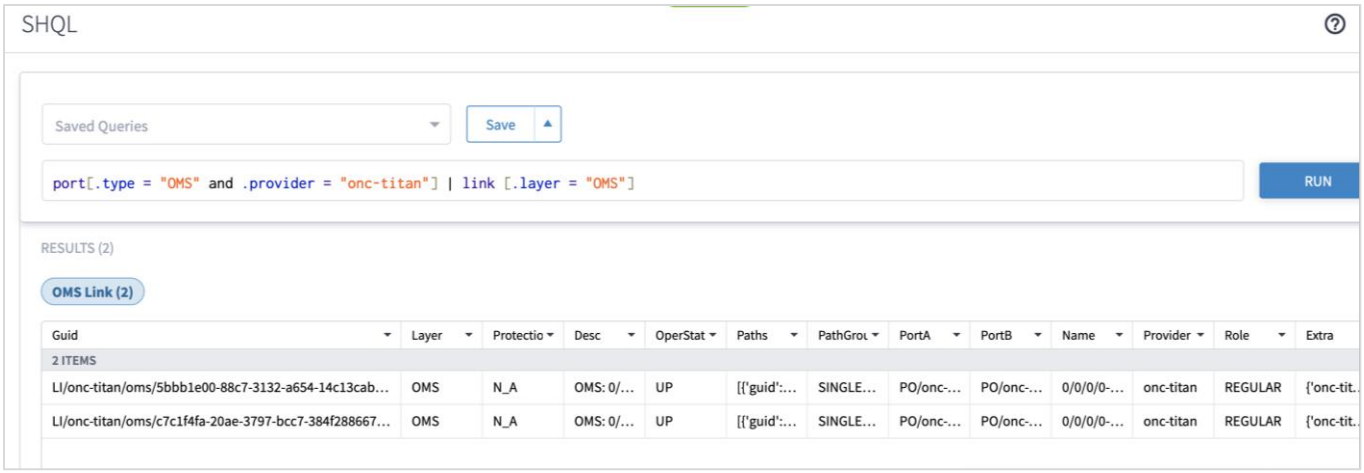
You can create L Band and C Band links. L-Band introduces a second OMS over the line-side OTS.

For example, Fiber-1 (OTS link is used) by two OMS-1 and OMS-2 (OMS links).

With both L Band and C Band, for a single OTS there are 2 (or more) OMS links.

For example:

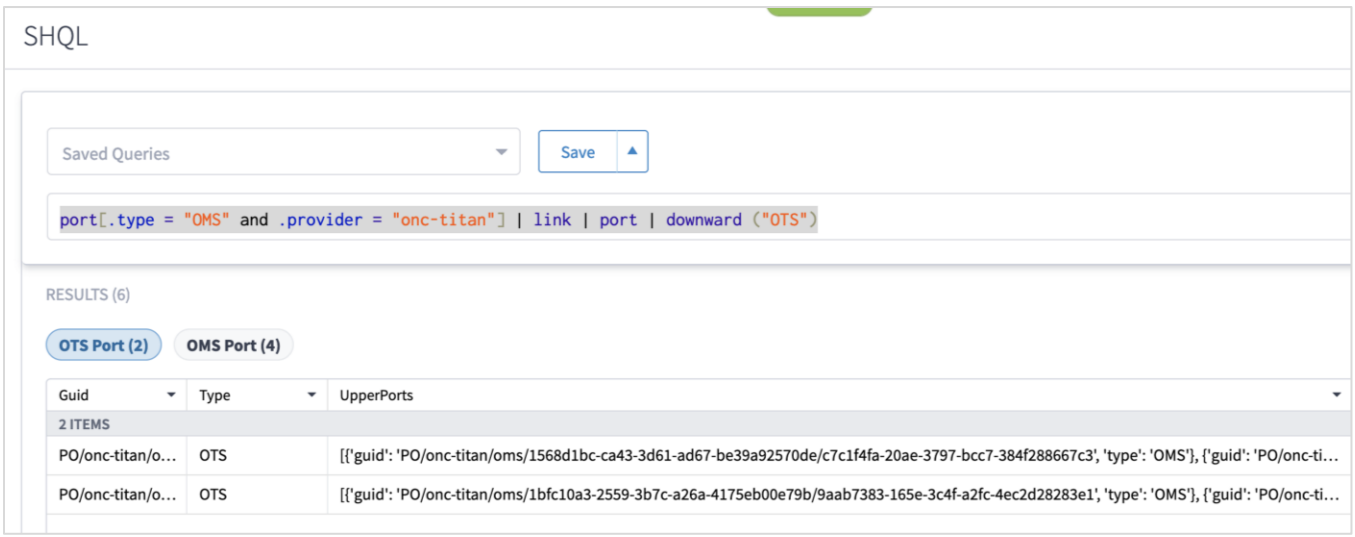
port[.type = "OMS" and .provider = "onc-titan"] | link [.layer = "OMS"]



For a single OTS link, there are 2 OTS ports and 4 (or more) OMS ports where the UpperPorts field holds the “upper” OMS ports for each OTS port.

For example:

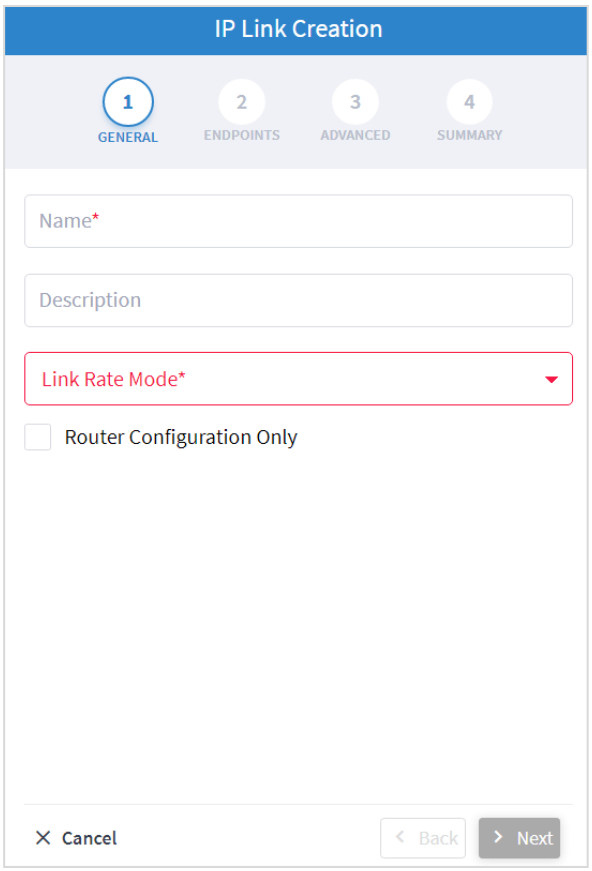
port[.type = "OMS"] | link | port | downward ("OTS")



For more info on how to view links and ports in SHQL, see the *Cisco Crosswork Hierarchical Controller NBI and SHQL Reference Guide*.

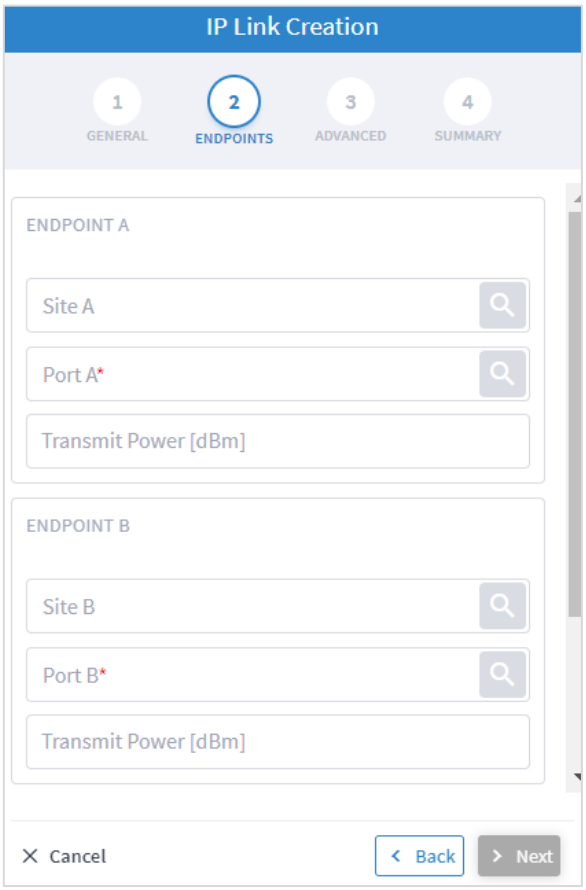
To create an IP Link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **IP Link**.



4. Specify the following **GENERAL** settings:
    - **Name**: Enter a name for the service.
    - **Description**: Enter a description for the service.
    - **Link Rate Mode**: Select a link rate mode, for example, **100G – 1x100G**. Bundles are offered when the selected rate is for muxponder mode. From version 7.0, a bundle option is offered for 400G.
    - **Router Configuration Only**: Select this option when configuring a router only (direct routers connections, not via OLS).

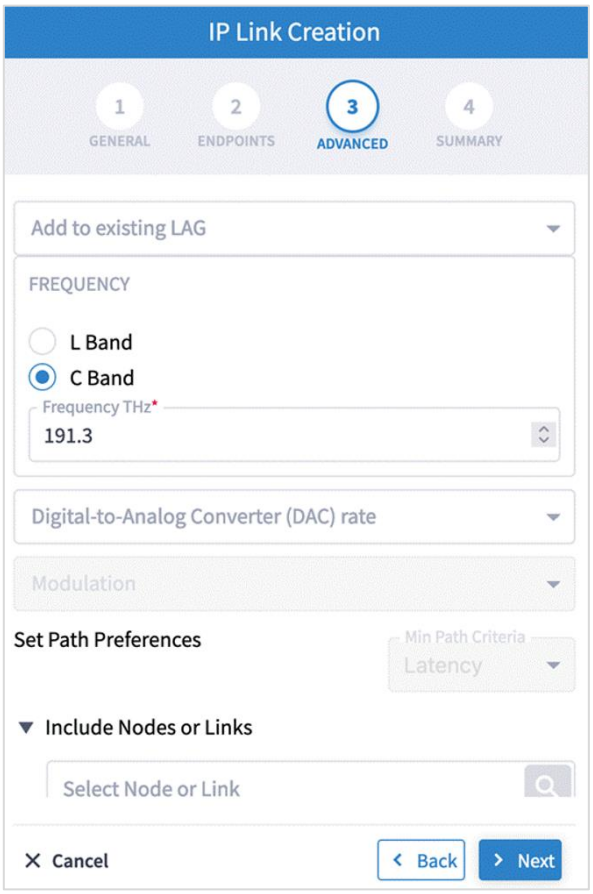
5. Click **Next**.

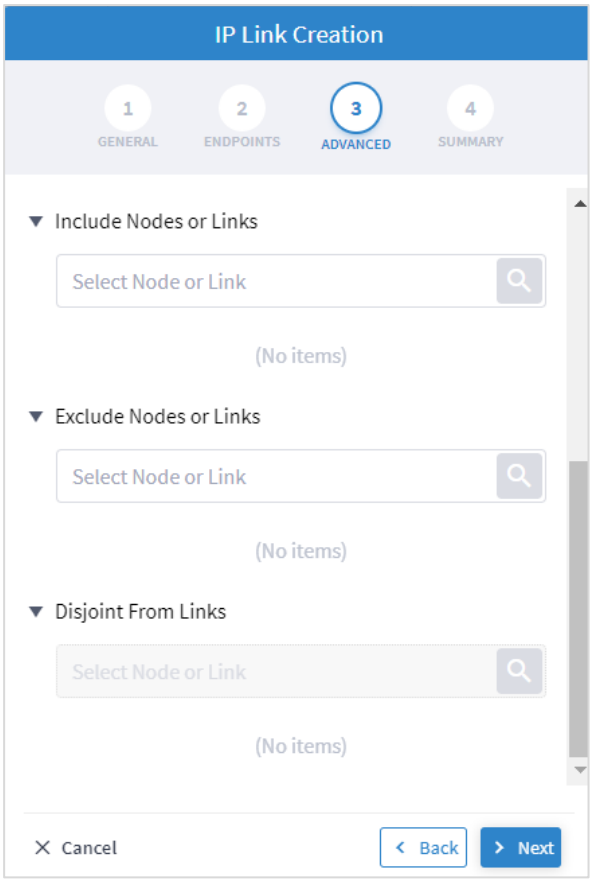


6. Specify the following **ENDPOINTS** settings:

   - **Site A**: Click and in the **Advanced** tab, select a site, or click on the **3D Explorer** tab to select a site.
   - **Port A**: Click and in the **Advanced** tab, select an OCH port, or click on the **3D Explorer** tab to select a port. If the port selected is an adjacency port, endpoint B is automatically updated and cannot be edited.
   - **Transmit Power (dBm):** Select the transmit power for Endpoint A.
   - **Site B**: Click and in the **Advanced** tab, select a site, or click on the **3D Explorer** tab to select a site.
   - **Port B**: Click and in the **Advanced** tab, select an OCH port, or click on the **3D Explorer** tab to select a port.
   - **Transmit Power (dBm):** Select the transmit power for Endpoint B.
   - **LINK #1 IP ADDRESSES**: Enter the **IP Address A (CIDR)** and **IP Address B (CIDR)**.
   - (Optional depending on the **Link Rate Mode** selected) Enter the **LINK #2 IP ADDRESSES**, **LINK #3 IP ADDRESSES** and **LINK #4 IP ADDRESSES**.

7. Click **Next**.

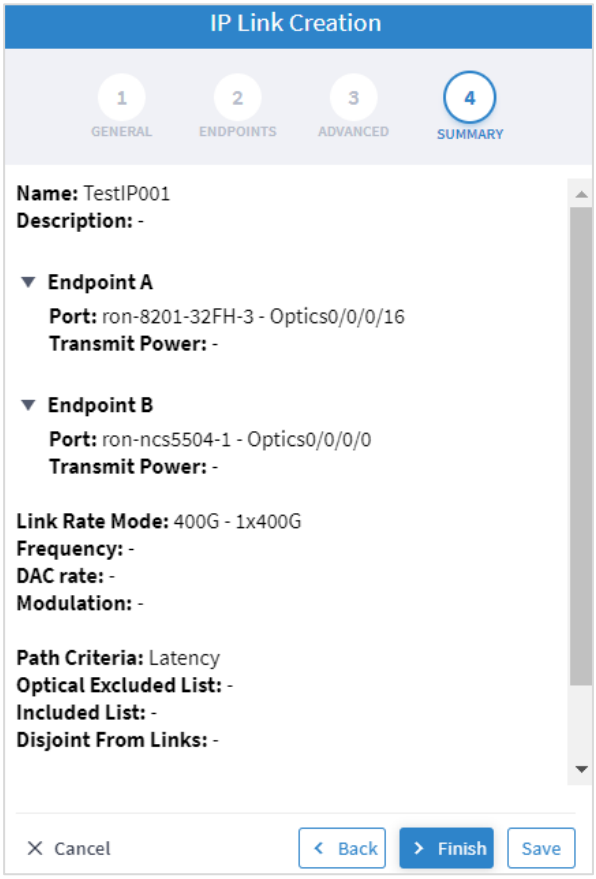




8. Specify the following **ADVANCED** settings:
    - **Add to existing LAG:** Select one of the existing LAGs (bundles) between the two selected routers. This option is only available if there is a bundle already configured between the routers.
    - **Frequency**: Select **L Band** or **C Band** and specify the **Frequency Thz** for this link. L-Band introduces a second OMS over the line-side OTS.
    - **Digital-to-Analog Converter (DAC) rate**: The DAC rate is only relevant for ZR+ and bright ZR port selection. For 100G, there is no need to change the DAC rate. Select **1 X 1** (standard compatible mode) or **1 X 1.25** (Cisco-proprietary mode if both ends of the link are Cisco pluggables). For QAM modulation, only **1 x 1.25** is supported.
    - **Modulation**: Select **8 QAM**, **16 QAM** or **QPSK** (default) to reduce the baud rate for 200G links. It is not necessary to apply modulation to 100G, 300G or 400G links as the correct modulation is automatically applied: 100G (QPSK), 300G (8 QAM) and 400G (16 QAM).
    - **Set Path Preferences**: Not enabled. Set to **Latency**.
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select a ONE node or OTS/OMS link, or click on the **3D Explorer** tab to select the required item.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select a ONE node or OTS/OMS link, or click on the **3D Explorer** tab to select the required item.
    - **Disjoint From Link**: Not enabled.

- (Optional) Click to remove any of the include/exclude items.

9. Click **Next**.



10. Review the **SUMMARY**.
11. Click **Finish**.

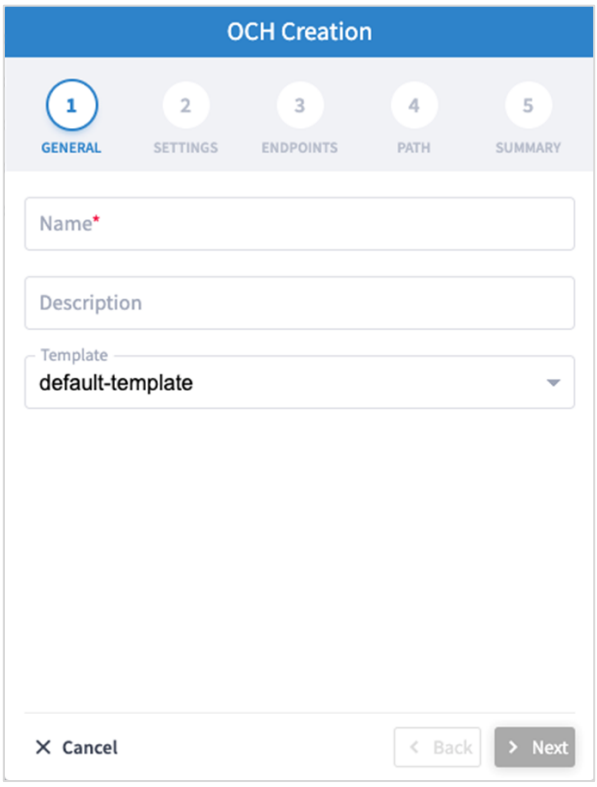
Create OCH Link

You can create an OCH Link between line side of Transponders/Muxponders, define its capacity, add 1+1 protection if required, and optimize based on number of hops, latency, or admin cost. Various advanced settings and limitations (such as nodes or links to be included or excluded from the OCH Link) can be added.

In this phase, the Transponder and the ROADM must be controlled by the same optical controller.

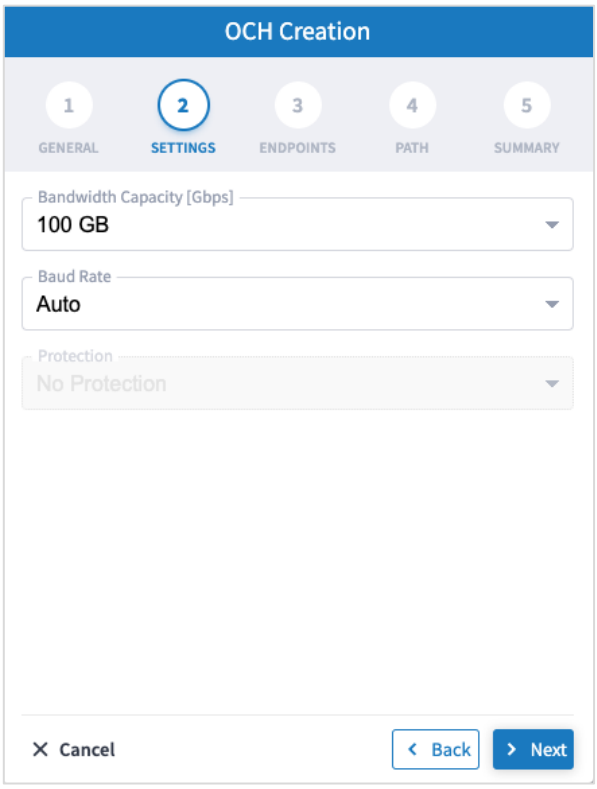
To create an OCH Link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **OCH Link**.



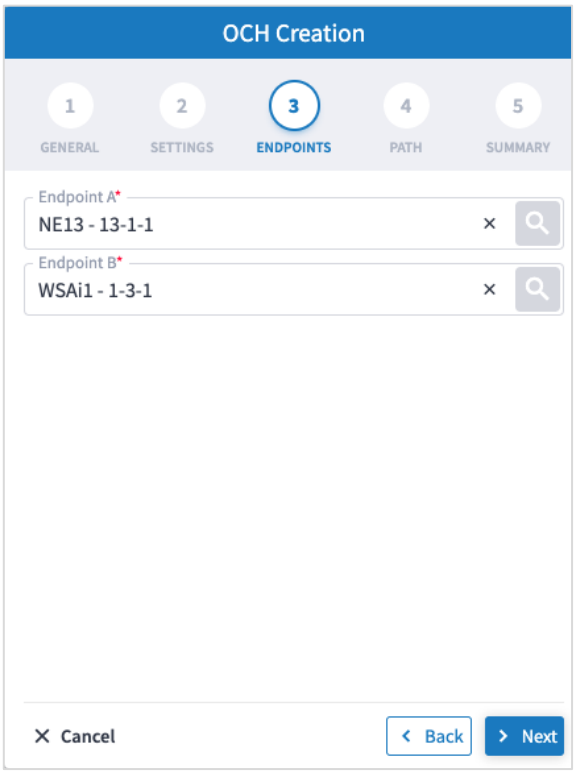
4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this link.
    - **Description**: A description of the link.

5. Click **Next**.



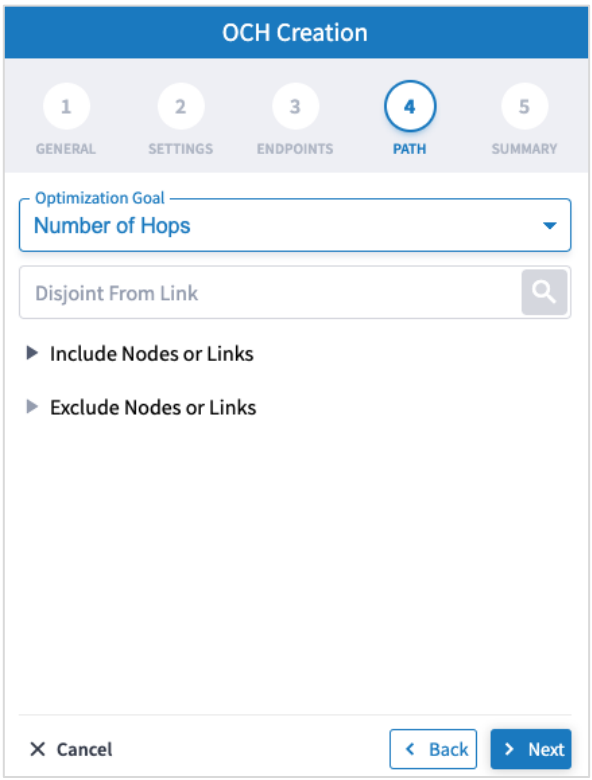
6. Specify the following **SETTINGS**:
    - **Bandwidth Capacity (Gbps)**: The bandwidth capacity for this OCH link (100 GB, 200 GB, 300 GB, 400 Gb or 800 GB).
    - **Baud Rate**: The baud rate for this IP link (Auto or 35 G or 56 G).

7. Click **Next**.



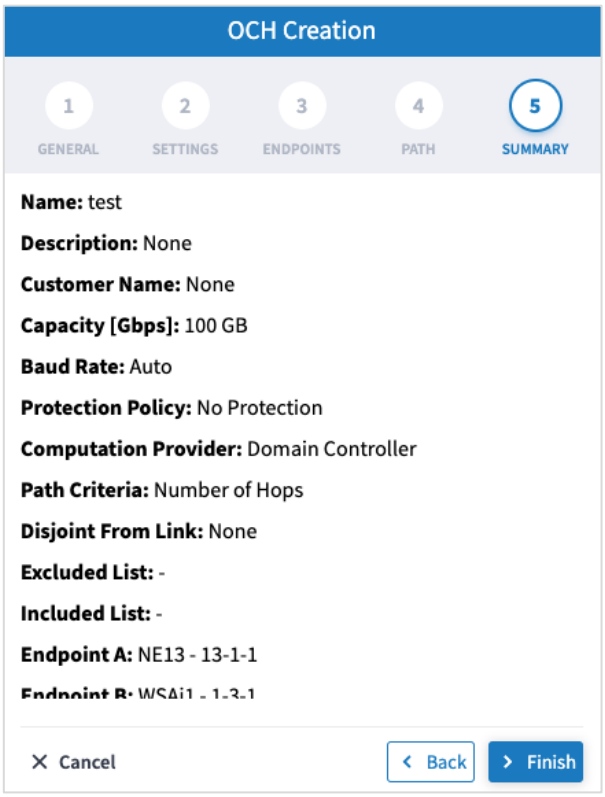
8. Specify the following **ENDPOINTS** settings:
    - **Endpoint A**: Click and in the **Advanced** tab, select an OCH endpoint, or click on the **3D Explorer** tab to select an OCH endpoint.
    - **Endpoint B**: Click and in the **Advanced** tab, select an OCH endpoint, or click on the **3D Explorer** tab to select an OCH endpoint.

9. Click **Next**.



10. Specify the following **PATH** settings:
    - **Optimization Goal**: The optimization goal (**Number of Hops** or **Latency** or **Admin Cost**).
    - **Disjoint From Link:** and in the **Advanced** tab, select an OCH link, or click on the **3D Explorer** tab to select an OCH link. This means that the new OTN-Line must not traverse this exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select an optical node or OMS link, or click on the **3D Explorer** tab to select an optical node or OMS link.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select an optical node or OMS/OTS link, or click on the **3D Explorer** tab to select an optical node or OMS/OTS link.
    - (Optional) Click to remove any of the include/exclude items.

11. Click **Next**.



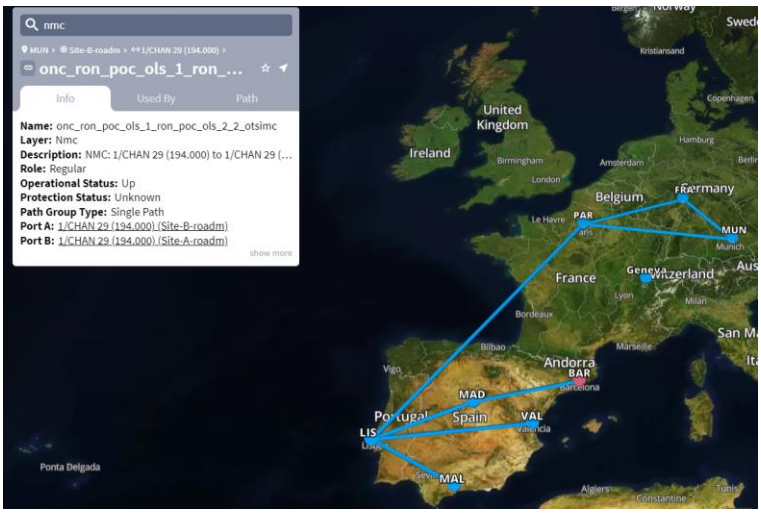
12. Click **Finish**.

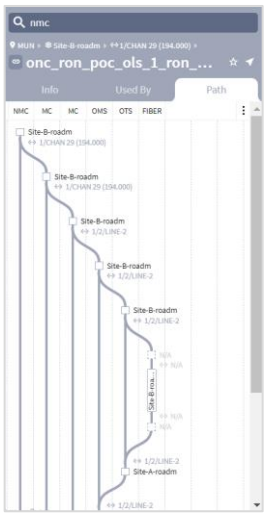
Create OCH-NC Link

You can create an OCH-NC (or OTSiMC) link. This is the connection between client sides of ROADMs, the ports facing Transponder/Muxponder. You can define its capacity, add 1+1 protection, if required, and optimize based on number of hops or admin cost. Various advanced settings and limitations (such as nodes or links to be included or excluded from the OCH-NC Link) can be added.

Before using this wizard, go to the Settings page and upload a file of app codes. Once the file is uploaded, the wizard enables you to select specific codes, which selects an item from the list in the uploaded file.

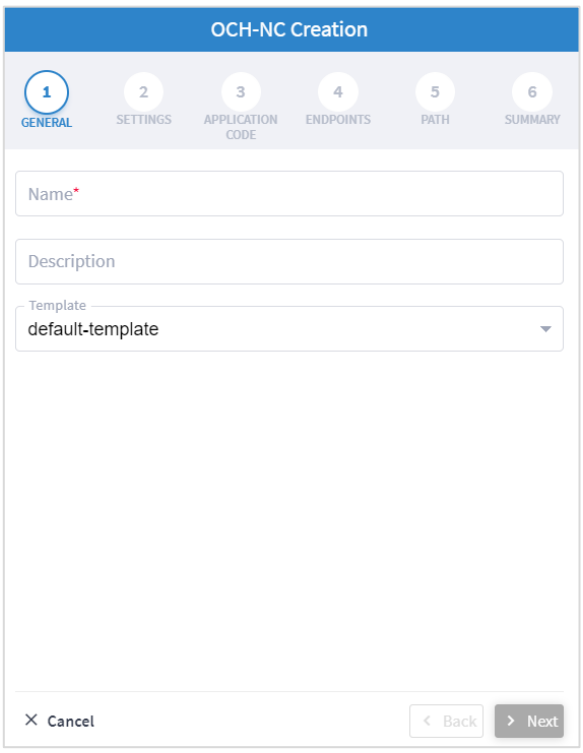
This only works with Cisco Optical Controller (ONC). The new service is added as an NMC link.



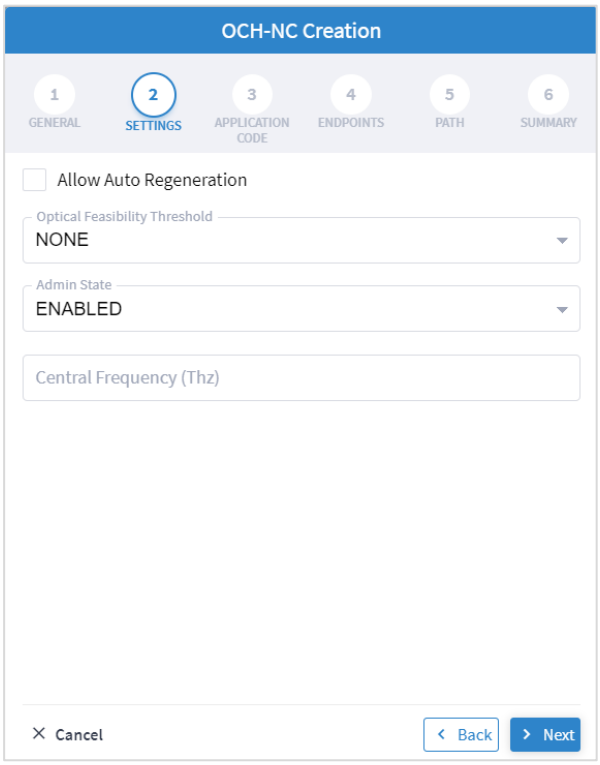


To create an OCH-NC Link:

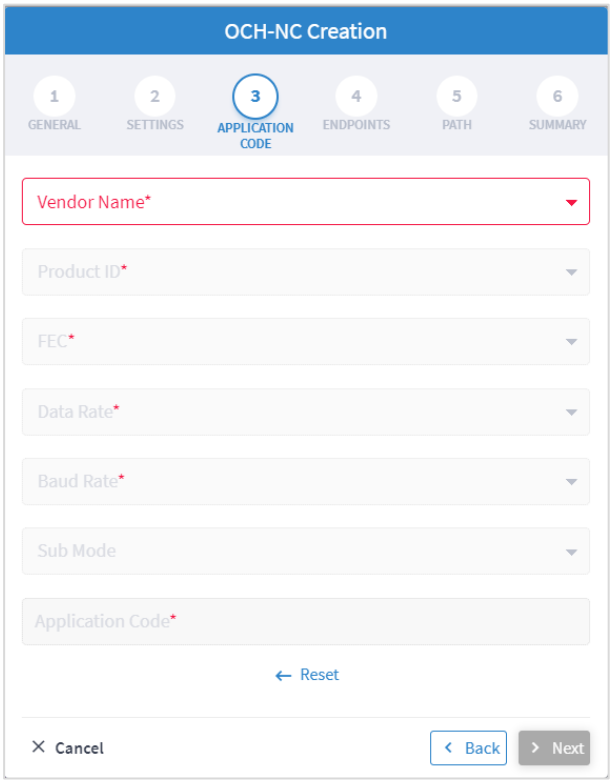
1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **OCH-NC Link**.



4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this link.
    - **Description**: A description of the link.
5. Click **Next**.

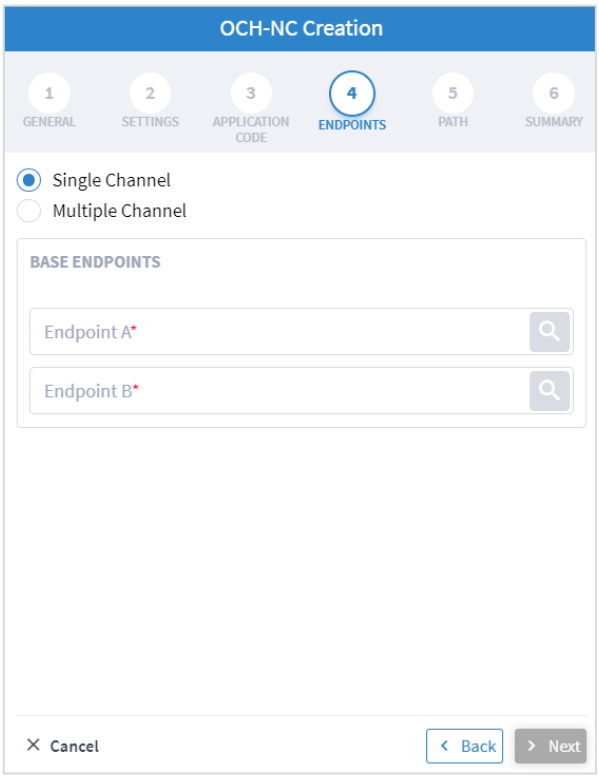


6. Specify the following **SETTINGS**:
    - **Allow Auto Regeneration:** Whether to allow auto regeneration.
    - **Optical Feasibility Threshold**: Select **RED**, **GREEN**, **YELLOW** or **NONE**.
    - **Admin State**: Select **ENABLED** or **DISABLED**.
    - **Central Frequency (Thz)**: The frequency for this OCH-NC link. A number in range of nine digits, with a dot after the first 3 digits (xxx.xxxxxx). Range is between 000.000000 to 999.999999 in steps of 000.000001.
7. Click **Next**.



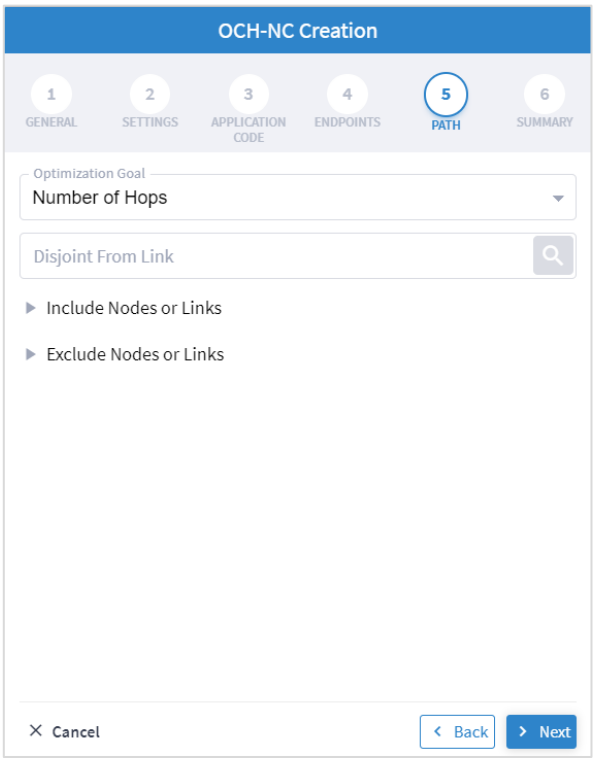
8. Specify the following **APPLICATION CODE** settings to generate the required **Application Code**:
    - **Vendor Name**: The vendor name.
    - **Product ID**: The product ID.
    - **FEC**: The FEC depending on the product, for example, CFEC or OFEC.
    - **Data Rate**: The data rate supported by the selected product.
    - **Baud Rate**: The baud rate supported by the selected product.
    - **Sub Mode**: This may appear depending on the other settings.

9. Click **Next**.



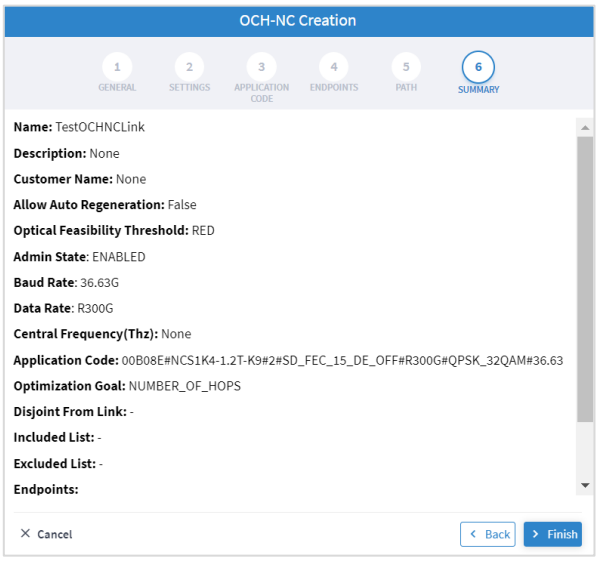
10. Specify the following **ENDPOINTS** settings:
    - Select **Single Channel** or **Multiple Channel**.
    - **Endpoint A**: Click and in the **Advanced** tab, select an NMC port, or click on the **3D Explorer** tab.
    - **Endpoint B**: Click and in the **Advanced** tab, select an NMC port, or click on the **3D Explorer** tab.

11. Click **Next**.



12. Specify the following **PATH** settings:
    - **Optimization Goal**: The optimization goal (**Number of Hops** or **Admin Cost**).
    - **Disjoint From Link:** and in the **Advanced** tab, select an OCH-NC link, or click on the **3D Explorer** tab to select an OCH-NC link. This means that the new OCH-NC link must not traverse this exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select a ONES or OMS link, or click on the **3D Explorer** tab to select a ONES or OMS link.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select a ONES or OMS/OTS link, or click on the **3D Explorer** tab to select a ONES or OMS link.
    - (Optional) Click to remove any of the include/exclude items.

13. Click **Next**.



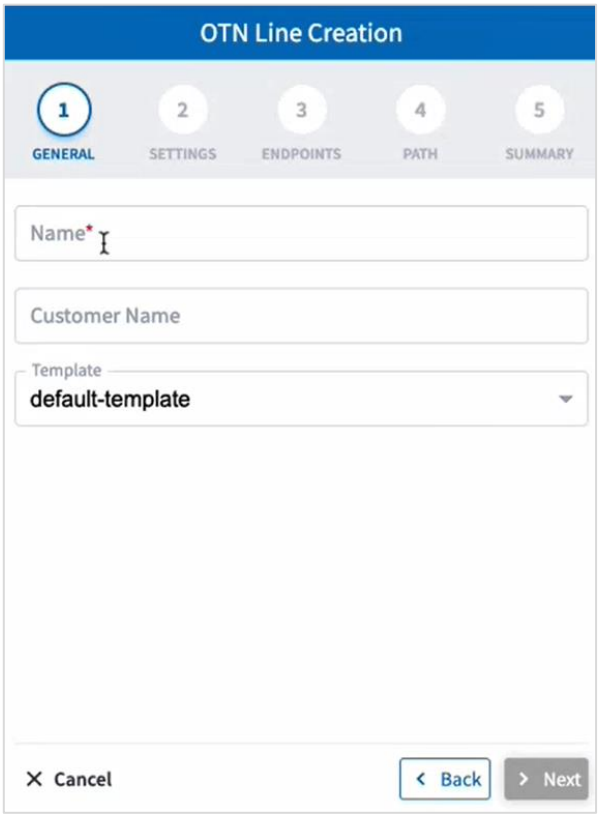
14. Click **Finish**.

Create OTN Line

You can create an OTN Line service between OTN client ports on Transponders/Muxponders, define its capacity, add 1+1 protection and/or restoration if required, and optimize based on **number of hops, latency,** or **admin cost.** Various advanced settings and limitations (such as node or links to be included in or excluded from the OTN Line) can be added.

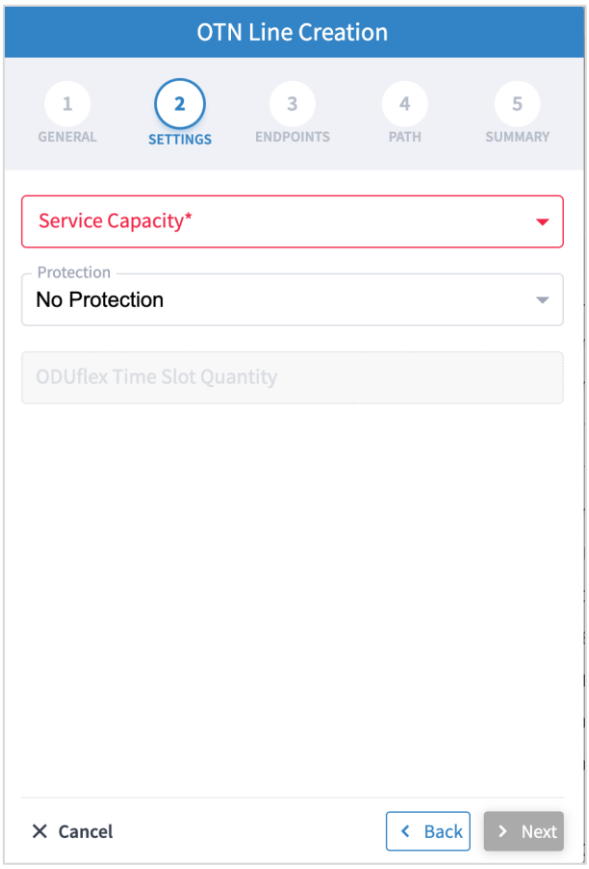
To create an OTN Line:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **OTN Line**.



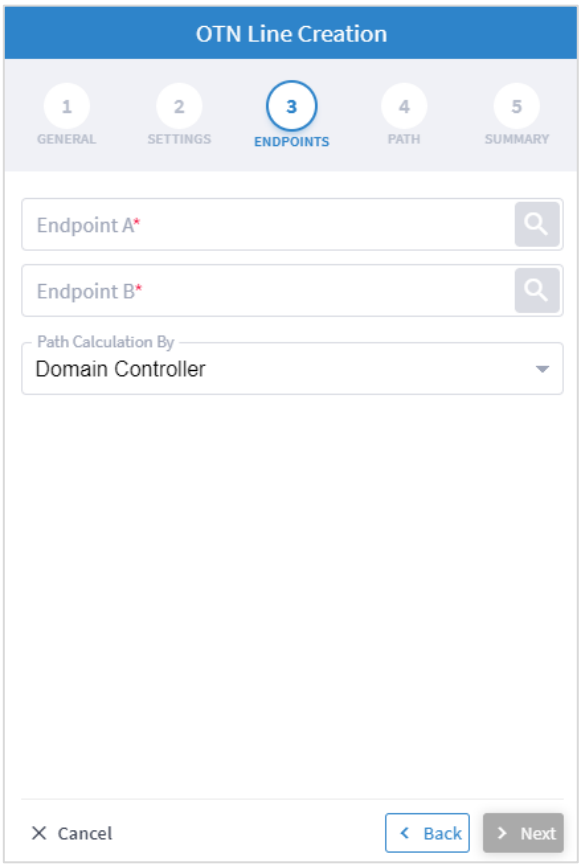
4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this OTN Line.
    - **Customer Name**: The OTN Line customer name.

5. Click **Next**.



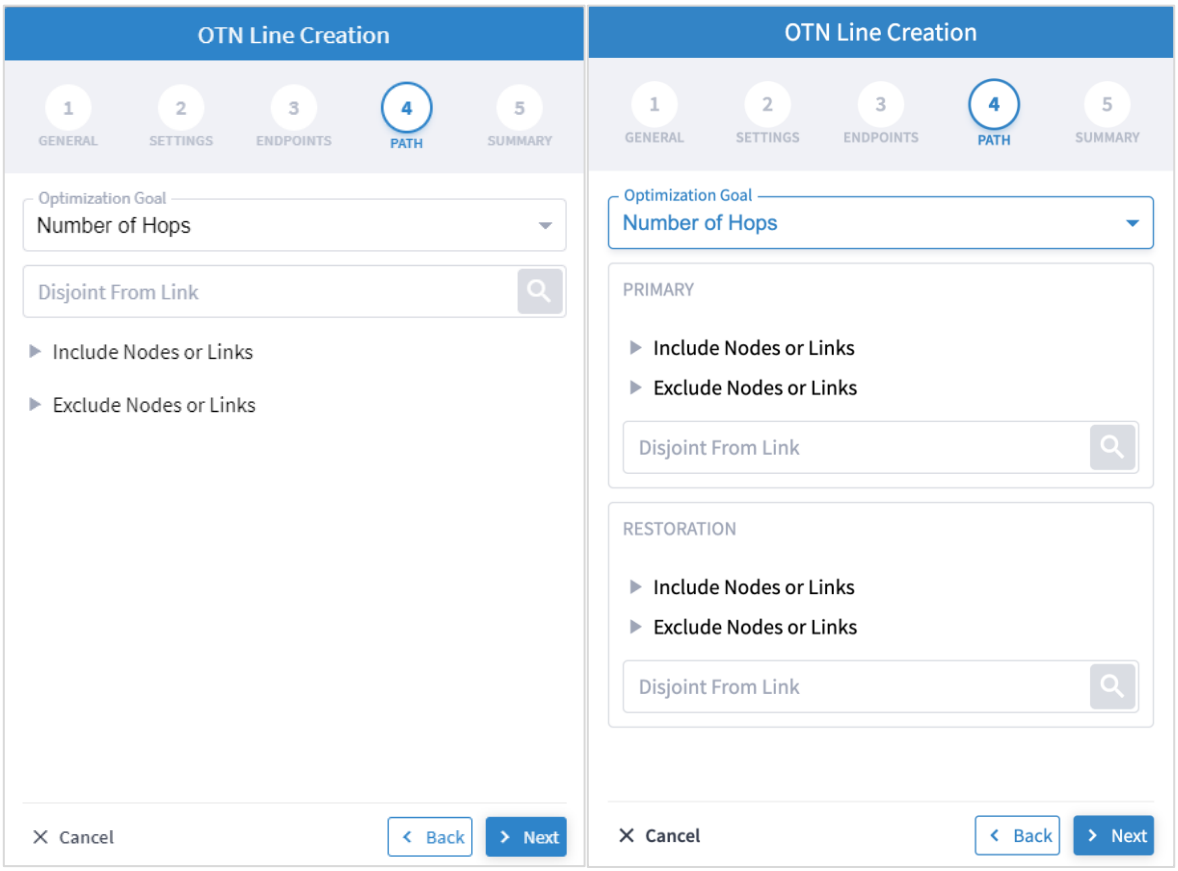
6. Specify the following **SETTINGS**:
    - **Service Capacity**: The capacity for this OTN Line, for example, **ODU2**.
    - **Protection**: The service protection (**No Protection** or **Protection 1+ Restoration** or **Protection 1+1** or **Protection 1+1+ Restoration**).
    - **ODUflex Time Slot Quantity**: The ODU-Flex unit is a flexible optical channel data unit. The time slot quantity parameter is only available if the **Service Capacity** is set to **ODU FLEX Allocated Slots** and the adapter supports this feature. Enter a value less than or equal to 80.

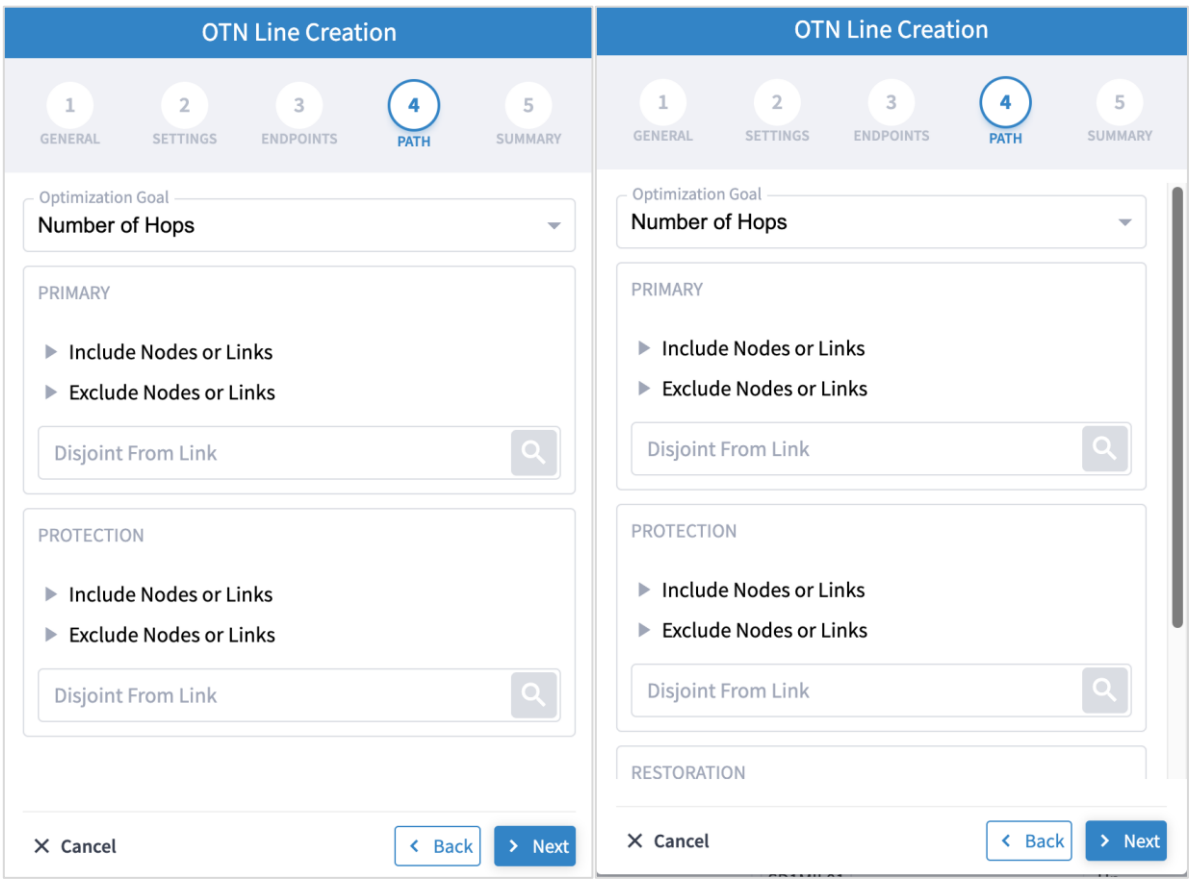
7. Click **Next**.



8. Specify the following **ENDPOINTS** settings:
    - **Endpoint A**: Click and in the **Advanced** tab, select an endpoint as ODU client port, or click on the **3D Explorer** tab to select an endpoint.
    - **Endpoint B**: Click and in the **Advanced** tab, select an endpoint as ODU client port, or click on the **3D Explorer** tab to select an endpoint.
    - **Path Calculation By**: Select **Domain Controller** or **HCO**.

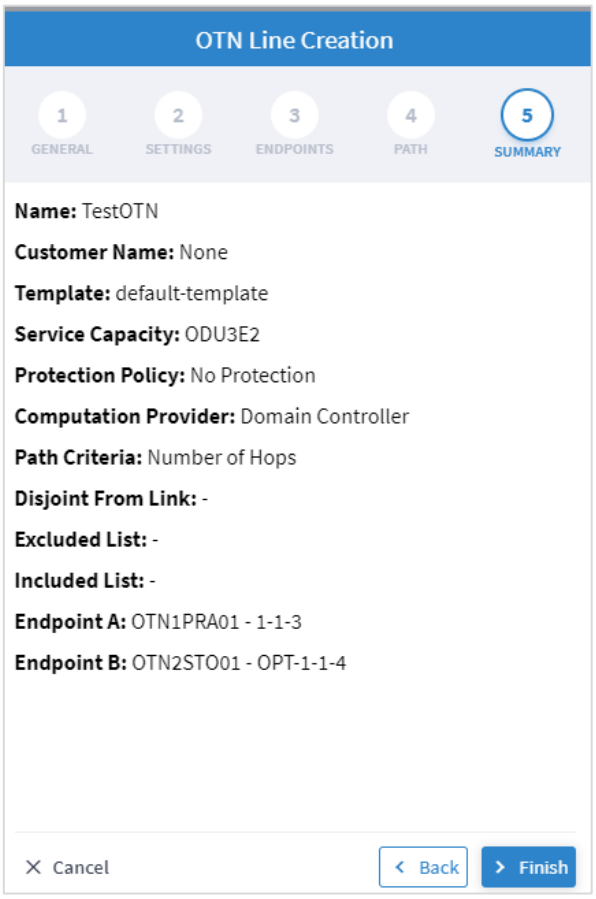
9. Click **Next**.





10. Specify the following **PATH** settings (depending on the **Protection** specified in **SETTINGS**, specify these options for the **PRIMARY**, **PROTECTION**, and **RESTORATION** paths):
    - **Optimization Goal**: The optimization goal (**Number of Hops** or **Latency** or **Admin Cost**).
    - **Disjoint From Link:** and in the **Advanced** tab, select an OTN line, or click on the **3D Explorer** tab to select an OTN line. This means that the new OTN Line must not traverse this exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select a node or OTU link, or click on the **3D Explorer** tab to select a node or OTU link.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select a node or any optical link, or click on the **3D Explorer** tab to select a node or any optical link.
    - (Optional) Click to remove any of the include/exclude items.

11. Click **Next**.



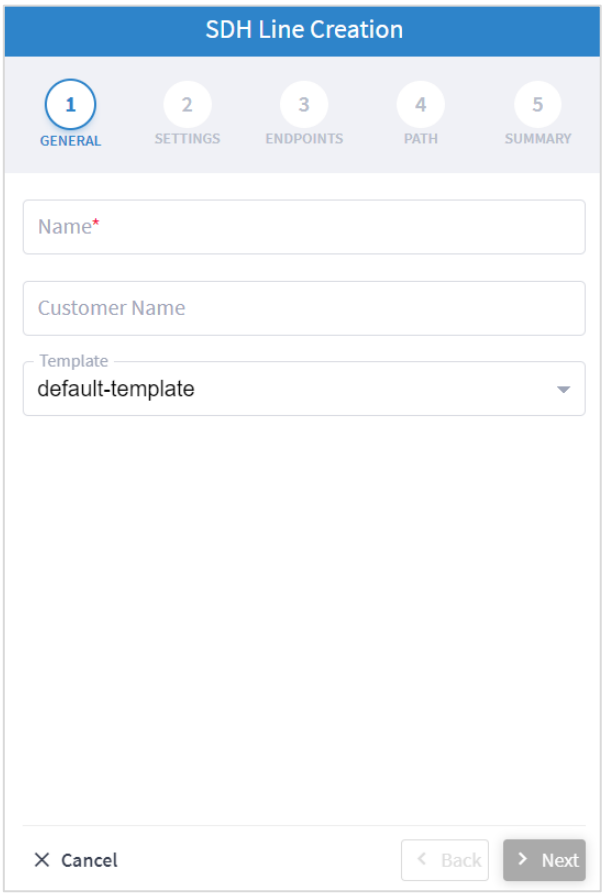
12. Click **Finish**.

Create SDH Line

You can create an SDH Line service between STM client ports, define its capacity, add 1+1 protection if required, allow the path to be calculated by the Domain Controller or HCO, and optimize based on **number of hops, latency,** or **admin cost.** Various advanced settings and limitations (such as node or links to be included in or excluded) can be added.

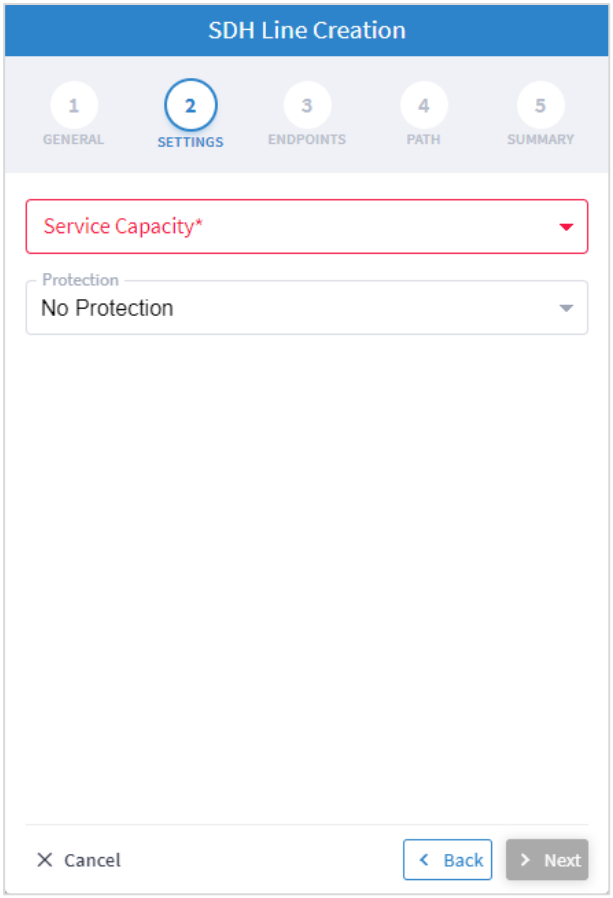
To create an SDH Line:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **SDH** Line.



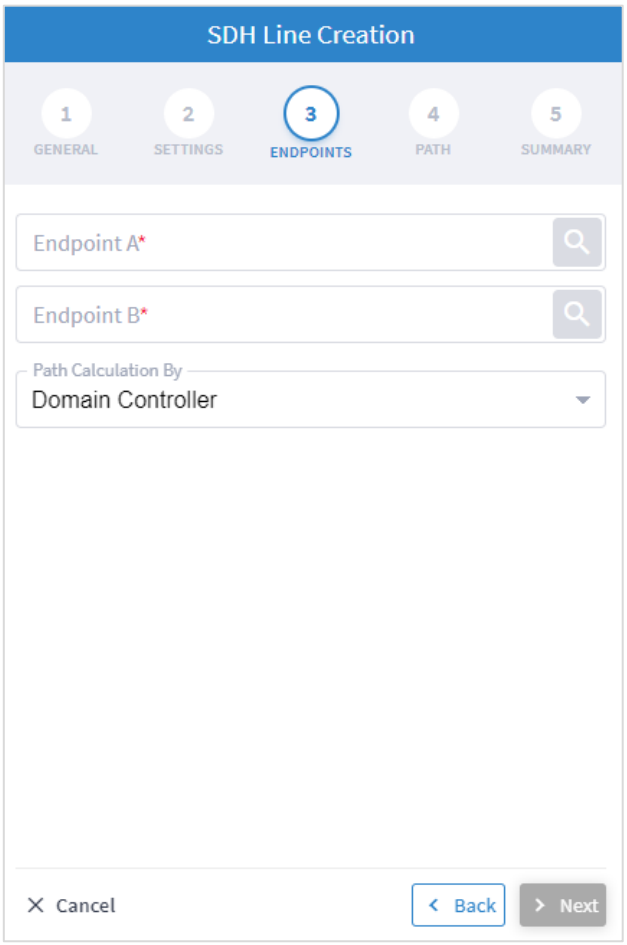
4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this SDH Line.
    - **Customer Name**: The SDH Line customer name.

5. Click **Next**.

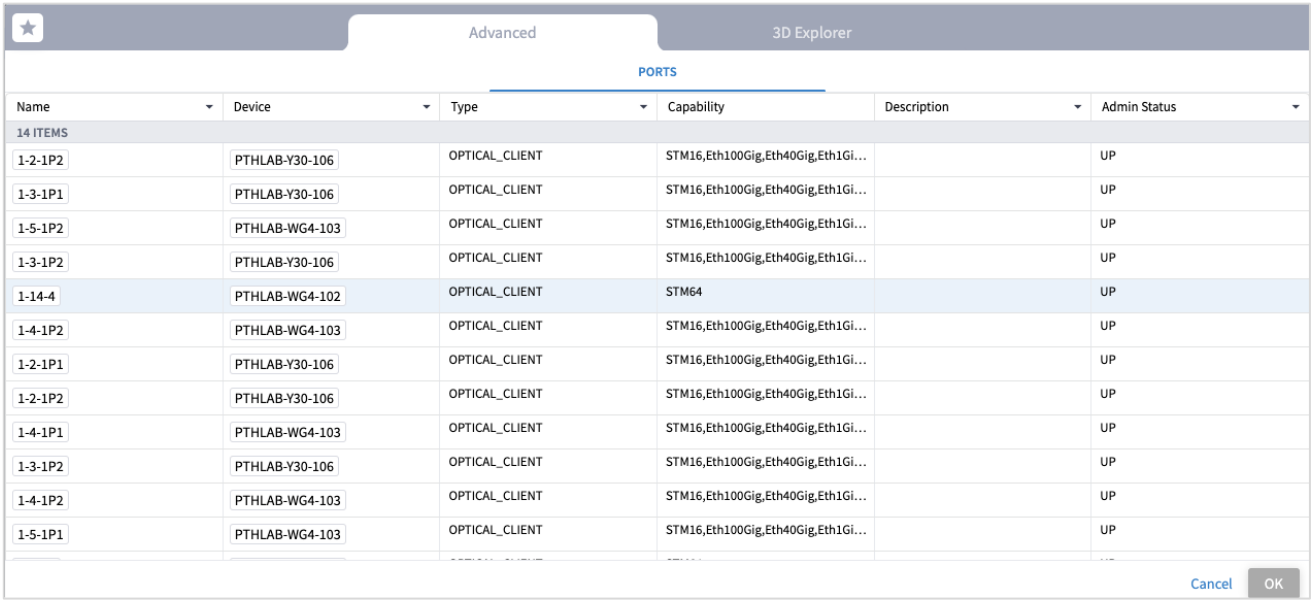


6. Specify the following **SETTINGS**:
    - **Service Capacity**: The capacity for this SDH Line, for example, **STM64** or **STM256**.
    - **Protection**: The service protection (**No Protection** or **Protection 1+1**).

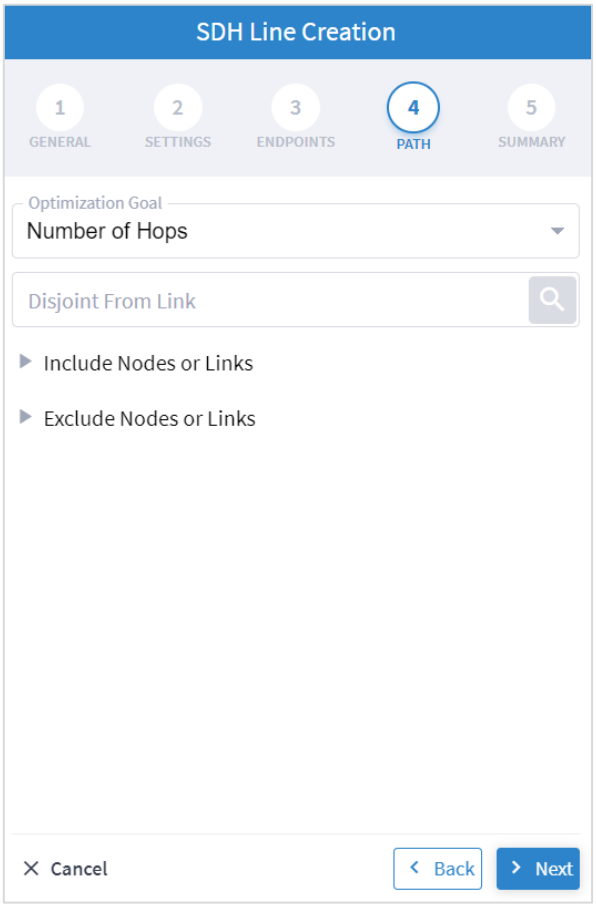
7. Click **Next**.



8. Specify the following **ENDPOINTS** settings:
    - **Endpoint A**: Click and in the **Advanced** tab, select an endpoint as STM client port, or click on the **3D Explorer** tab to select an endpoint.
    - **Endpoint B**: Click and in the **Advanced** tab, select an endpoint as STM client port, or click on the **3D Explorer** tab to select an endpoint.
    - **Path Calculation By**: Select **Domain Controller** or **HCO**.



9. Click **Next**.

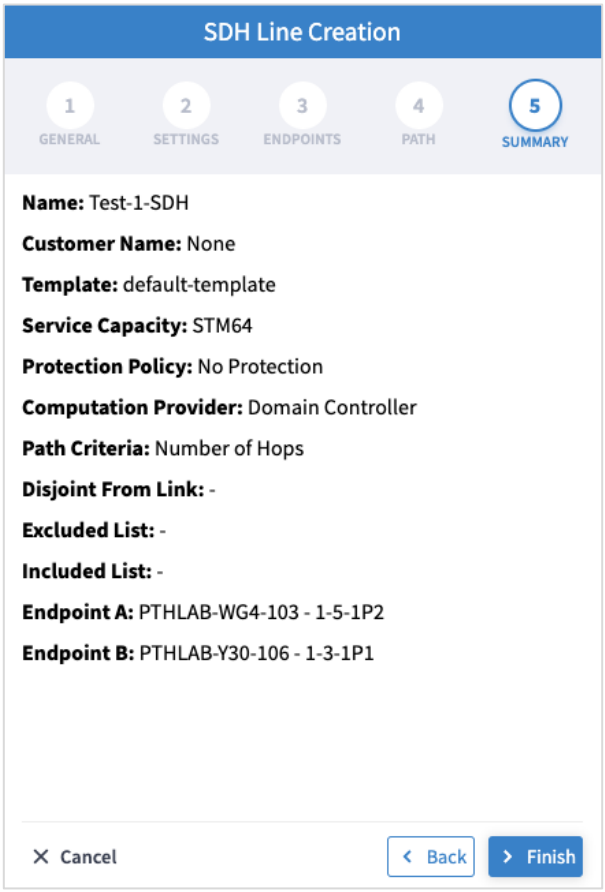


10. Specify the following **PATH** settings:
    - **Optimization Goal**: The optimization goal (**Number of Hops** or **Latency** or **Admin Cost**).
    - **Disjoint From Link:** and in the **Advanced** tab, select an OTN line, or click on the **3D Explorer** tab to select an SDH line. This means that the new SDH Line must not traverse this

exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).

- **Include Nodes or Links**: Click and in the **Advanced** tab, select a node or SDH link, or click on the **3D Explorer** tab to select a node or SDH link.
- **Exclude Nodes or Links**: Click and in the **Advanced** tab, select a node or any optical link, or click on the **3D Explorer** tab to select a node or any optical link.
- (Optional) Click to remove any of the include/exclude items.

11. Click **Next**.



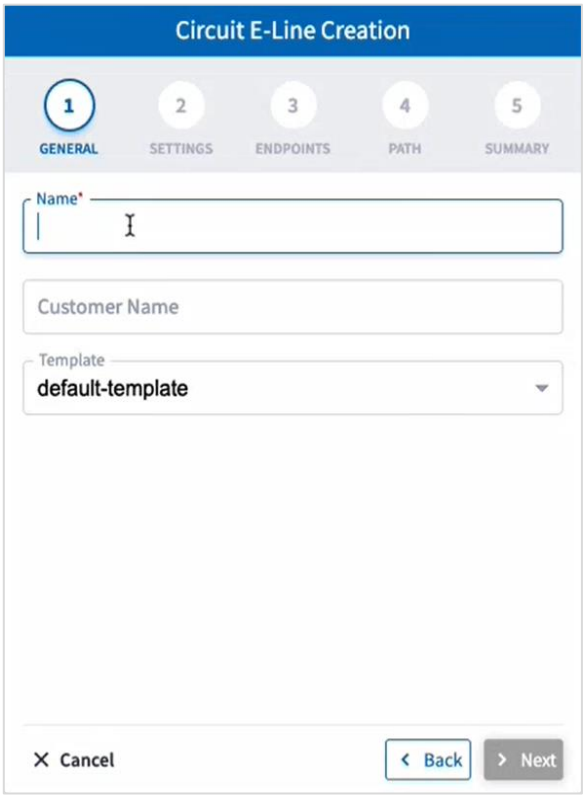
12. Click **Finish**.

Create Circuit E-Line

You can create a Circuit E-Line, as an Ethernet connection between ETH client ports on Transponders/Muxponders, define its capacity, add 1+1 protection and/or restoration if required, and optimize based on **number of hops, latency, or admin cost.** Various advanced settings and limitations (such as nodes or links to be included in or excluded from the Circuit E-line) can be added.

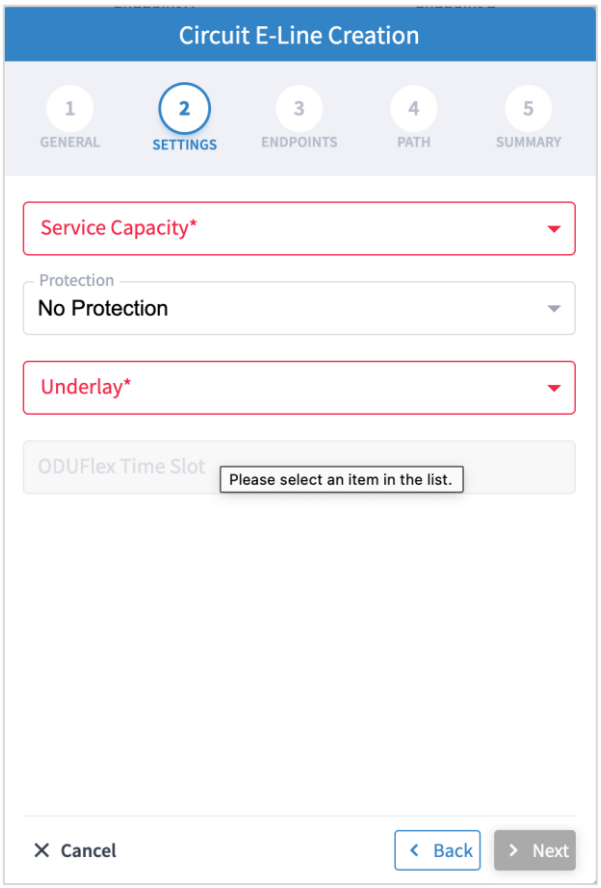
To create a Circuit E-Line:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
2. Select the **Point to Point** tab.
3. Click **Circuit E-Line**.



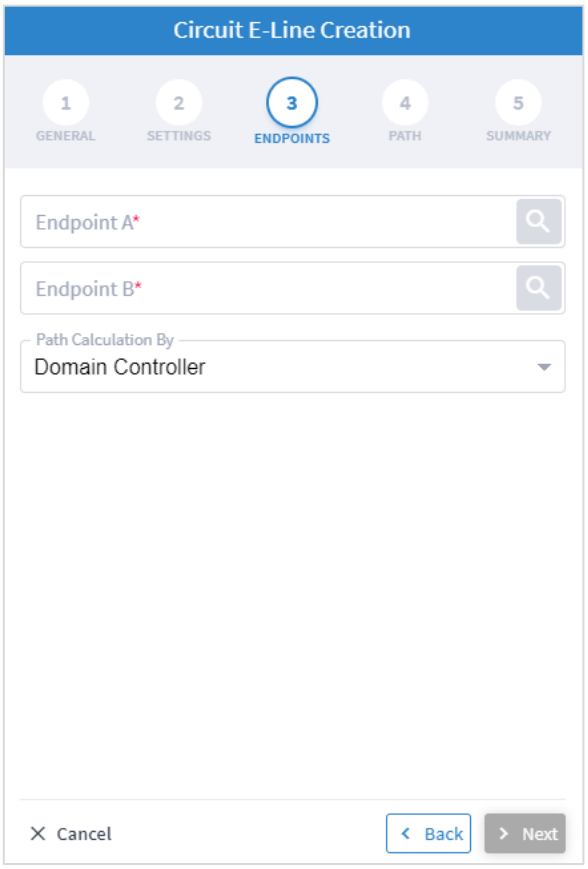
4. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this Circuit E-Line.
    - **Customer Name**: The Circuit E-Line customer name.

5. Click **Next**.



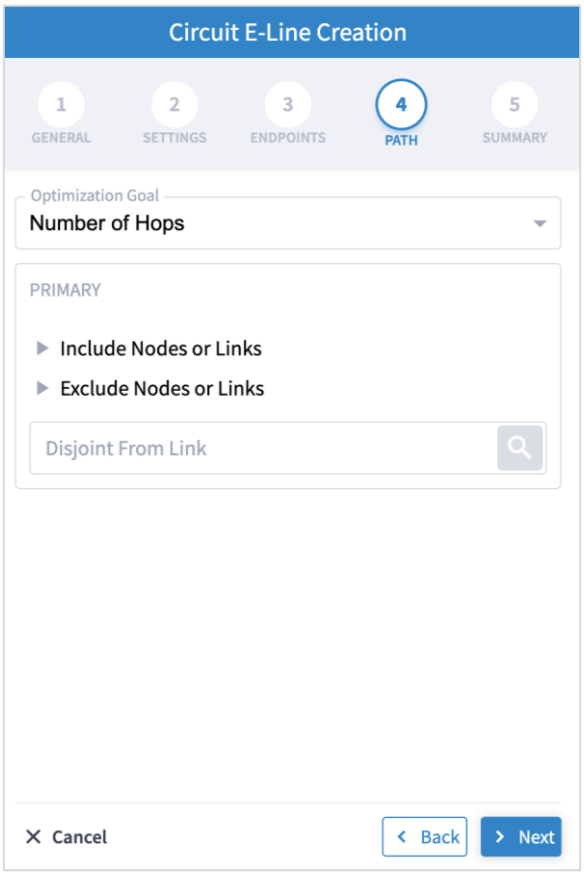
6. Specify the following **SETTINGS**:
    - **Service Capacity**: The capacity for this Circuit E-Line, for example, 10 GB WAN.
    - **Protection**: The service protection (**No Protection** or **Protection 1+ Restoration** or **Protection 1+1** or **Protection 1+1+ Restoration**).
    - **Underlay**: The underlay, either **ODU FIX** or **ODU FLEX Allocated Slots**.
    - **ODUFlex Time Slot**:

7. Click **Next**.



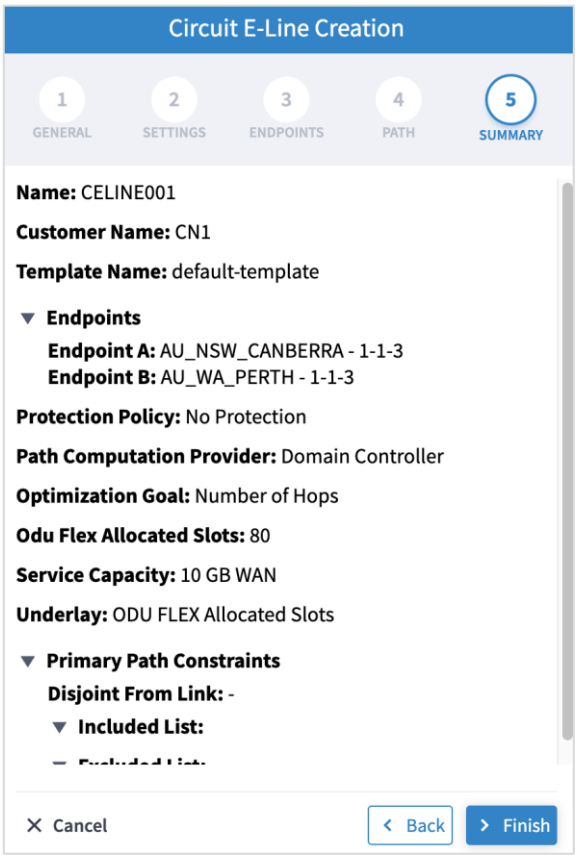
8. Specify the following **ENDPOINTS** settings:
    - **Endpoint A**: Click and in the **Advanced** tab, select an ETH endpoint, or click on the **3D Explorer** tab to select an endpoint.
    - **Endpoint B**: Click and in the **Advanced** tab, select an ETH endpoint, or click on the **3D Explorer** tab to select an endpoint.
    - **Path Calculation By**: Select **Domain Controller** or **HCO**.

9. Click **Next**.



10. Specify the following **PATH** settings (depending on the **Protection** specified in **SETTINGS**, specify these options for the **PRIMARY**, **PROTECTION**, and **RESTORATION** paths):
    - **Optimization Goal**: The optimization goal (**Number of Hops** or **Latency** or **Admin Cost**).
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select a Circuit E-Line, or click on the **3D Explorer** tab to select a Circuit E-Line.
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select node or any optical link, or click on the **3D Explorer** tab to select node or any optical link.
    - (Optional) Click to remove any of the include/exclude items.
    - **Disjoint From Link**: and in the **Advanced** tab, select Circuit E-Line, or click on the **3D Explorer** tab to select Circuit E-Line. This means that the new Circuit E-Line must not traverse this exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).

11. Click **Next**.



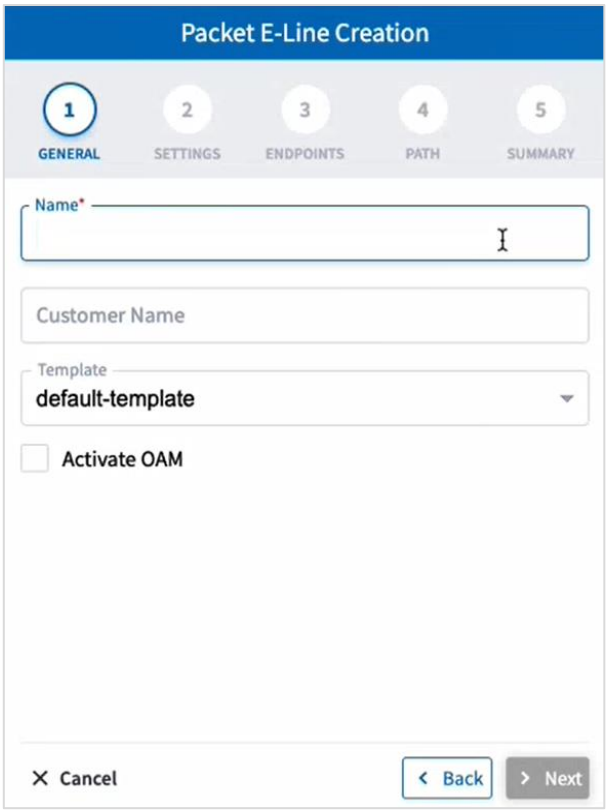
12. Click **Finish**.

Create Packet E-Line

You can create a Packet E-Line as an Ethernet service between Routers over RSVP-TE tunnels or SR policies, or between Transponders/Muxponders over MPLS-TP tunnels, define its capacity, add 1+1 protection if required, and optimize based on **number of hops, latency, or admin cost.** Various advanced settings and limitations (such as items to be included or excluded from the Circuit E-line) can be added.

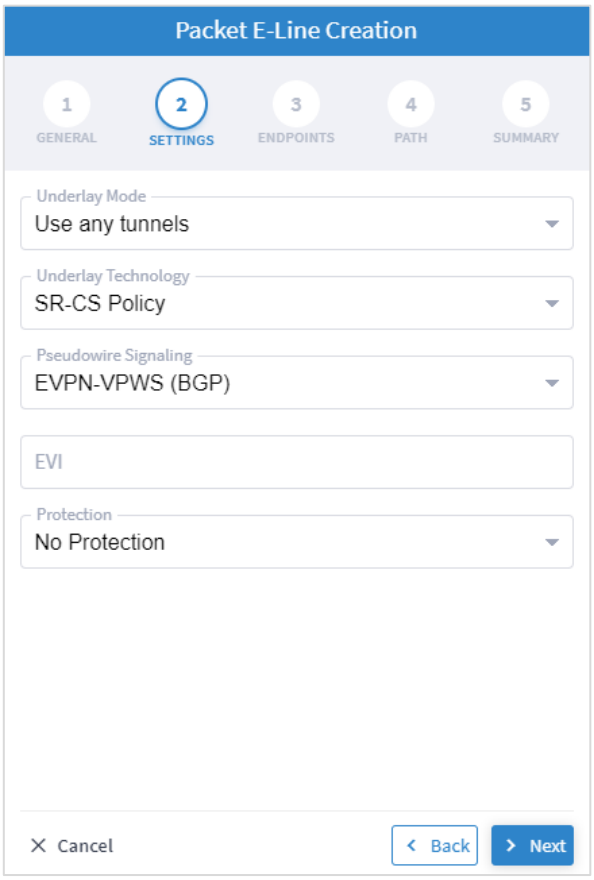
To create a Packet E-Line:

1. Before creating a Packet E-Line service, create the MPLS-TP tunnels to be used (this is assumed to be handled implicitly by the optical controller).
2. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager**.
3. Select the **Point to Point** tab.
4. Click **Packet E-Line**.



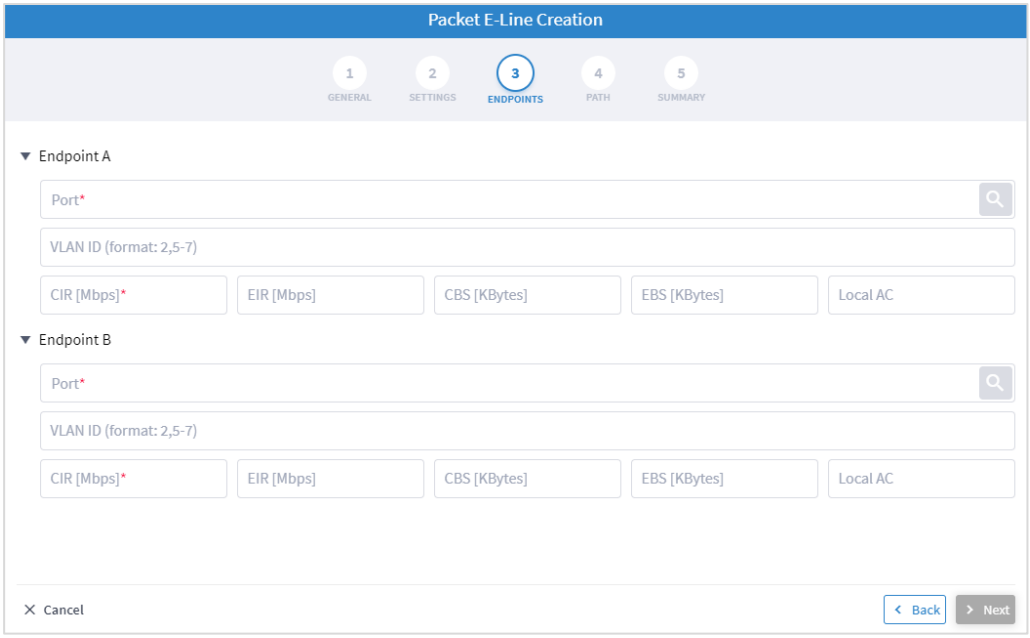
5. Specify the following **GENERAL** settings:
    - **Name**: The unique user defined name of this Packet E-Line.
    - **Customer Name**: The Packet E-Line customer name.
    - **Activate OAM**: Whether to enable OAM PM activation.

6. Click **Next**.



7. Specify the following **SETTINGS**:
    - **Underlay Mode**: The underlay mode, for example, **Use any tunnels**.
    - **Underlay Technology**: The underlay technology, for example, **MPLS-TP**.
    - **Pseudowire Signaling**: The pseudowire signaling, for example, **EVPN-VPWS (BGP)**.
    - **EVI**: The **EVPN** instance.
    - **Protection**: The service protection (**No Protection** or **Protection 1+1**).

8. Click **Next**.



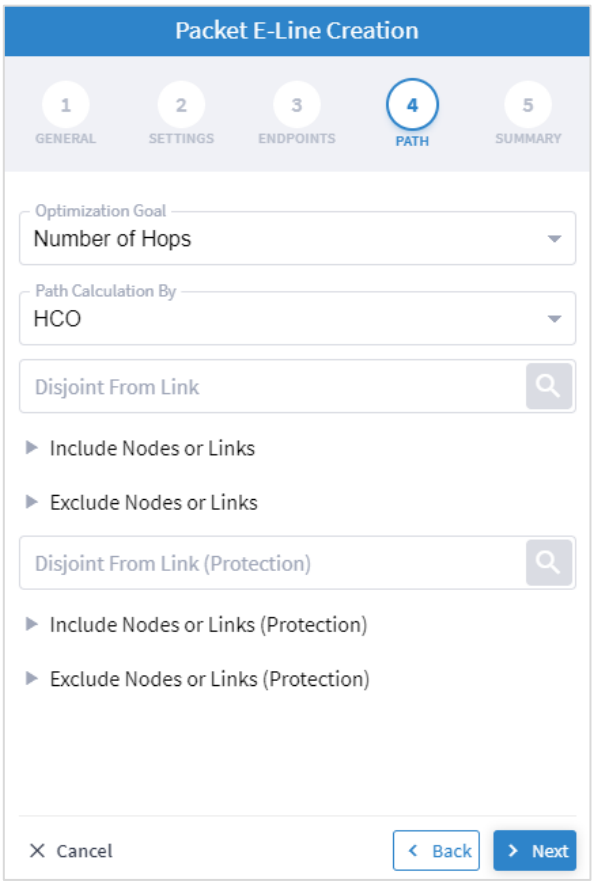
9. Specify the following **ENDPOINTS** settings for **Endpoint A** and **Endpoint B**:

   - **Port**: Click and in the **Advanced** tab, select a port, or click on the **3D Explorer** tab to select an Ethernet port. The port rates should be the same. In case selected ports has already a packet E-Line service defined, with VLAN IDs, the VLAN IDs must be specified for per endpoint for the new service.
   - **VLAN ID**: The VLAN ID in a range of 1-4094. Enter a single value, multiple values separate by commas, and/or ranges, where '-' designates the range, for example: 390-780. If the selected endpoint has no services on it, the VLAN ID field is optional. Once defined, a VLAN ID must be defined in both endpoints, although different values/ranges can be specified. If you specify multiple VLANs, you must use the same values for both endpoints.

   Bandwidth parameters are all optional

   - **CIR (Mbps)**: The CIR rate in Mbps, range is 0 to <port rate>. The values can be different per endpoint.
   - **EIR (Mbps)**: The EIR rate in Mbps, range is 0 to <port rate>. The values can be different per endpoint.
   - **CBS (Kbytes)**: The CBS rate in Kbytes, range is 0 to <port rate>. The values can be different per endpoint.
   - **EBD (Kbytes)**: The CBS rate in Kbytes, range is 0 to <port rate>. The values can be different per endpoint.
   - **Local AC**: The local AC.
   - **Endpoint B**: Click and in the **Advanced** tab, select a port, or click on the **3D Explorer** tab to select a port.

10. Click **Next**.



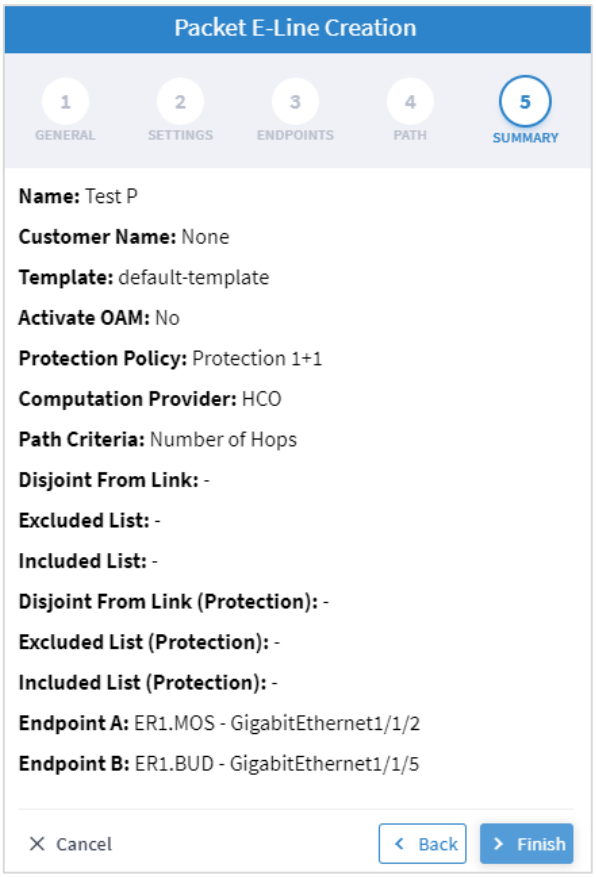
11. Specify the following **PATH** settings:

    - **(Only required if tunnels are implicitly created) Optimization Goal**: The optimization goal (**Number of Hops** or **Latency** or **Admin Cost**).
    - **(Only required if tunnels are implicitly created) Path Calculation By: The path calculation mechanism**: **Domain Controller** or **HCO**. Currently in this version only the Domain Controller option is available.
    - **Disjoint From Link:** and in the **Advanced** tab, select a Packet E-Line, or click on the **3D Explorer** tab to select a Packet E-Line. This means that the new Circuit E-Line must not traverse this exclusionary path (this would be equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).
    - **Include Nodes or Links**: Click and in the **Advanced** tab, select node or underlay link (IGP or OTU), or click on the **3D Explorer** tab to select node or underlay link (IGP or OTU).
    - **Exclude Nodes or Links**: Click and in the **Advanced** tab, select node or underlay link (IGP or OTU) or click on the **3D Explorer** tab to select node or underlay link (IGP or OTU).
    - **(Only required with protections) Disjoint From Link (Protection):** and in the **Advanced** tab, select a Packet E-Line, or click on the **3D Explorer** tab to select a Packet E-Line. This means that the new Circuit E-Line must not traverse this exclusionary path (this would be

equivalent to adding all the links that constitute the disjoint path to the exclude items from path list).

- **(Only required with protections) Include Nodes or Links (Protection)**: Click and in the **Advanced** tab, select node or underlay link (IGP or OTU), or click on the **3D Explorer** tab to select node or underlay link (IGP or OTU).
- **(Only required with protections) Exclude Nodes or Links (Protection)**: Click and in the **Advanced** tab, select node or underlay link (IGP or OTU) or click on the **3D Explorer** tab to select node or underlay link (IGP or OTU).
- (Optional) Click to remove any of the include/exclude items.

12. Click **Next**.



13. Click **Finish**.

Delete P2P

To delete a P2P Link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Point to Point**.
2. Select a link.
3. Select the **Actions** tab.
4. Click **Delete P2P**. A confirmation message appears.
5. Click **Accept**. The link is deleted.

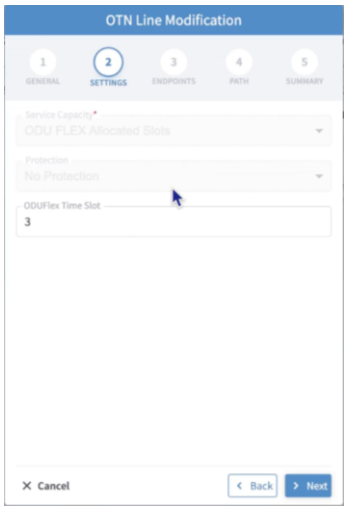
Edit P2P

For Circuit E-Line and OTN Line services, you can edit the **ODUFlex Time Slot**. The time slot quantity parameter is only available if the **Service Capacity** is set to **ODU FLEX Allocated Slots** and the adapter supports this feature.

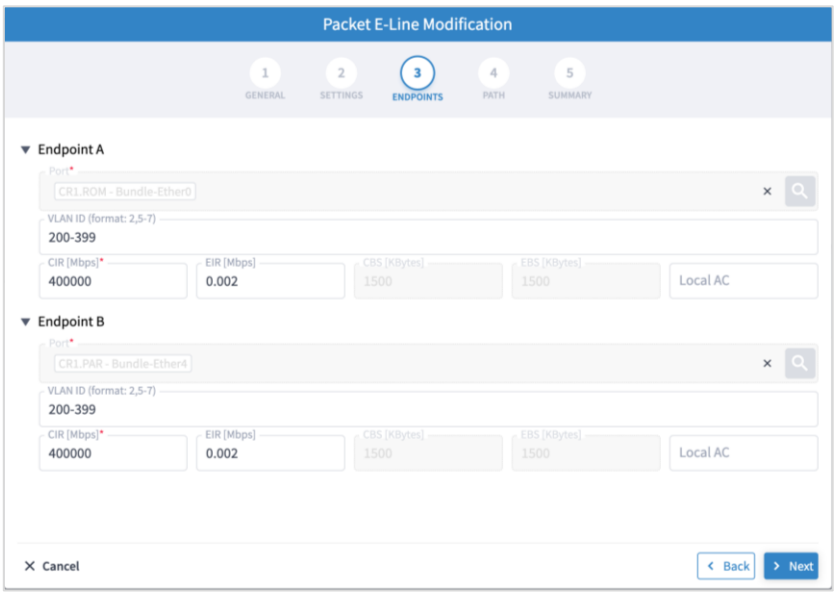
For Packet E-Line service, you can modify various endpoint and path parameters.

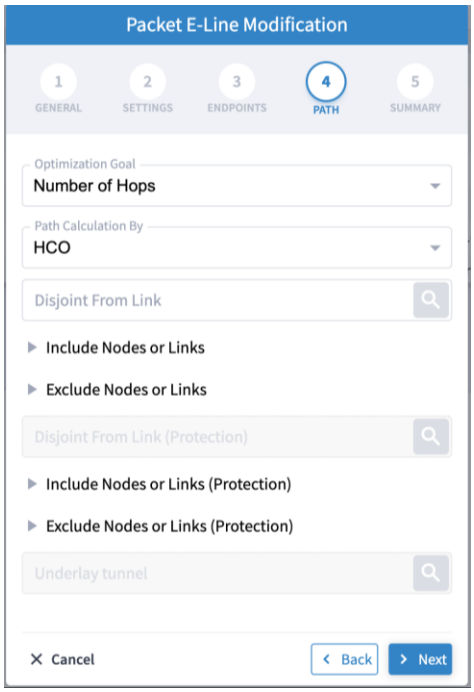
To edit a P2P Link:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Point to Point**.
2. Select a link.
3. Select the **Actions** tab.
4. Click **Edit P2P**.
5. Click **Next** until you reach a setting that can be edited.
6. For an **OTN Line** service, in **SETTINGS**, you can modify the **ODUFlex Time Slot** by entering a value less than or equal to 80.



7. For a **Packet E-Line** service, in **ENDPOINTS**, you can modify the endpoint parameters (**VLAN ID**, **CIR** and **EIR**), and in **PATH**, you can modify the various path parameters. For more details, see Create Packet E-Line.





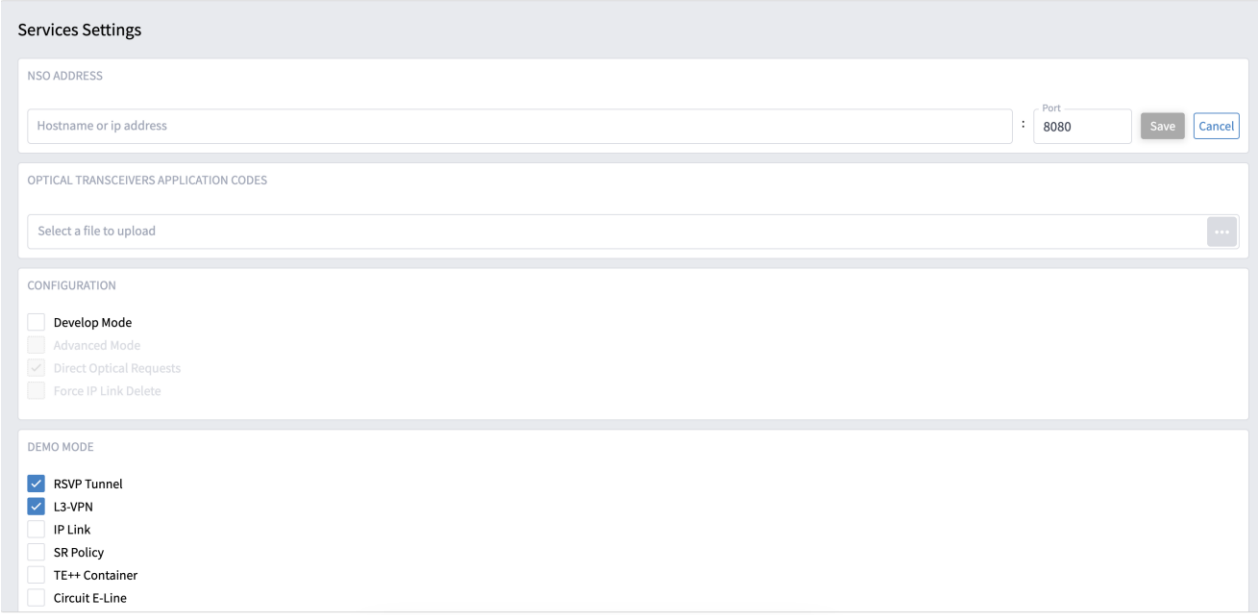
8. Click **Next** until your reach the **SUMMARY**.
9. Click **Finish**.

Service Settings

You can configure which rollbacks are allowed. For example, to prevent partial provisioning for IP Link, if the ONC provisioning succeeds and the CNC provisioning fails, and rollback is selected, the ONC provisioning is rolled back.

To view the service settings:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Settings**. A list of the service settings appears.



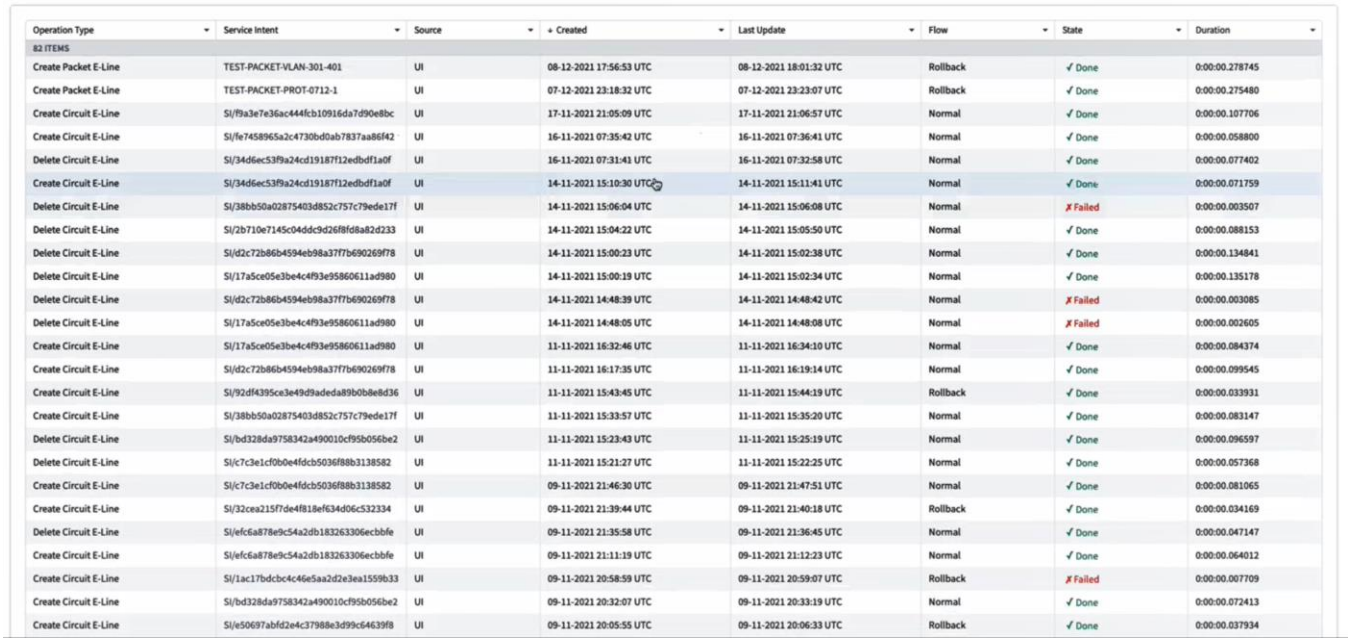
2. In **NSO ADDRESS**, enter the NSO host name or IP address. This appears in the **NSO Provisioning** tab.
3. In **OPTICAL TRANSCEIVERS APPLICATION CODES**, click ... to select a file with the application codes. It is recommended to export the required JSON file from the ONC controller.
4. Select which rollbacks are allowed when the services are provisioned (**RSVP Tunnel, L3-VPN, IP Link, SR Policy, TE++ Container, Circuit E-Line, OTN Line, OCH, Packet E-Line** and/or **OCH-NC**).

Service Manager Operations

You can view the latest Service Manager operations.

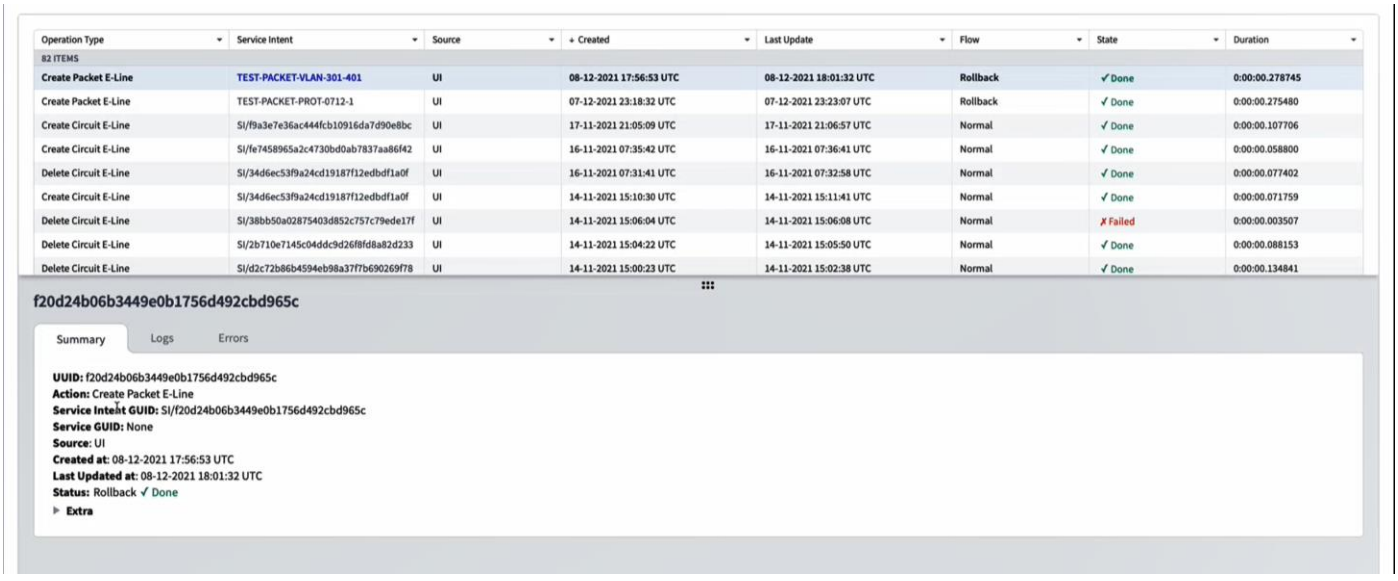
To view the operations:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > Operations**. A list of the operations appears.



Operation Type	Service Intent	Source	+ Created	Last Update	Flow	State	Duration
82 ITEMS							
Create Packet E-Line	TEST-PACKET-VLAN-301-401	UI	08-12-2021 17:56:53 UTC	08-12-2021 18:01:32 UTC	Rollback	✓ Done	0:00:00.278745
Create Packet E-Line	TEST-PACKET-PROT-0712-1	UI	07-12-2021 23:18:32 UTC	07-12-2021 23:23:07 UTC	Rollback	✓ Done	0:00:00.275480
Create Circuit E-Line	SI/f9a3e7e36ac444fcb10916da7d90e8bc	UI	17-11-2021 21:05:09 UTC	17-11-2021 21:06:57 UTC	Normal	✓ Done	0:00:00.107706
Create Circuit E-Line	SI/fe7458965a2c4730bd0ab7837aa86f42	UI	16-11-2021 07:35:42 UTC	16-11-2021 07:36:41 UTC	Normal	✓ Done	0:00:00.058800
Delete Circuit E-Line	SI/34d6ec53f9a24cd19187f12edbdf1a0f	UI	16-11-2021 07:31:41 UTC	16-11-2021 07:32:58 UTC	Normal	✓ Done	0:00:00.077402
Create Circuit E-Line	SI/34d6ec53f9a24cd19187f12edbdf1a0f	UI	14-11-2021 15:10:30 UTC	14-11-2021 15:11:41 UTC	Normal	✓ Done	0:00:00.071759
Delete Circuit E-Line	SI/38bb50a02875403d852c757c79ede17f	UI	14-11-2021 15:06:04 UTC	14-11-2021 15:06:08 UTC	Normal	✗ Failed	0:00:00.003507
Delete Circuit E-Line	SI/2b710e7145c04ddc9d26f8fd8a82d233	UI	14-11-2021 15:04:22 UTC	14-11-2021 15:05:50 UTC	Normal	✓ Done	0:00:00.088153
Delete Circuit E-Line	SI/d2c72b86b4594eb98a37f7b690269f78	UI	14-11-2021 15:00:23 UTC	14-11-2021 15:02:38 UTC	Normal	✓ Done	0:00:00.134841
Delete Circuit E-Line	SI/17a5ce05e3be4c4f93e95860611ad980	UI	14-11-2021 15:00:19 UTC	14-11-2021 15:02:34 UTC	Normal	✓ Done	0:00:00.135178
Delete Circuit E-Line	SI/d2c72b86b4594eb98a37f7b690269f78	UI	14-11-2021 14:48:39 UTC	14-11-2021 14:48:42 UTC	Normal	✗ Failed	0:00:00.003085
Delete Circuit E-Line	SI/17a5ce05e3be4c4f93e95860611ad980	UI	14-11-2021 14:48:05 UTC	14-11-2021 14:48:08 UTC	Normal	✗ Failed	0:00:00.002605
Create Circuit E-Line	SI/17a5ce05e3be4c4f93e95860611ad980	UI	11-11-2021 16:32:46 UTC	11-11-2021 16:34:10 UTC	Normal	✓ Done	0:00:00.084374
Create Circuit E-Line	SI/d2c72b86b4594eb98a37f7b690269f78	UI	11-11-2021 16:17:35 UTC	11-11-2021 16:19:14 UTC	Normal	✓ Done	0:00:00.099545
Create Circuit E-Line	SI/92df4395ce3e49d9adeda89b0b8e8d36	UI	11-11-2021 15:43:45 UTC	11-11-2021 15:44:19 UTC	Rollback	✓ Done	0:00:00.033931
Create Circuit E-Line	SI/38bb50a02875403d852c757c79ede17f	UI	11-11-2021 15:33:57 UTC	11-11-2021 15:35:20 UTC	Normal	✓ Done	0:00:00.083147
Delete Circuit E-Line	SI/bd328da9758342a490010cf95b056be2	UI	11-11-2021 15:23:43 UTC	11-11-2021 15:25:19 UTC	Normal	✓ Done	0:00:00.096597
Delete Circuit E-Line	SI/c7c3e1cf0b0e4fdcb5036f88b3138582	UI	11-11-2021 15:21:27 UTC	11-11-2021 15:22:25 UTC	Normal	✓ Done	0:00:00.057368
Create Circuit E-Line	SI/c7c3e1cf0b0e4fdcb5036f88b3138582	UI	09-11-2021 21:46:30 UTC	09-11-2021 21:47:51 UTC	Normal	✓ Done	0:00:00.081065
Create Circuit E-Line	SI/32cea215f7de4f818ef634d06c532334	UI	09-11-2021 21:39:44 UTC	09-11-2021 21:40:18 UTC	Rollback	✓ Done	0:00:00.034169
Delete Circuit E-Line	SI/efc6a878e9c54a2db183263306ecbbfe	UI	09-11-2021 21:35:58 UTC	09-11-2021 21:36:45 UTC	Normal	✓ Done	0:00:00.047147
Create Circuit E-Line	SI/efc6a878e9c54a2db183263306ecbbfe	UI	09-11-2021 21:11:19 UTC	09-11-2021 21:12:23 UTC	Normal	✓ Done	0:00:00.064012
Create Circuit E-Line	SI/1ac17bdcbc4c46e5aa2d2e3ea1559b33	UI	09-11-2021 20:58:59 UTC	09-11-2021 20:59:07 UTC	Rollback	✗ Failed	0:00:00.007709
Create Circuit E-Line	SI/bd328da9758342a490010cf95b056be2	UI	09-11-2021 20:32:07 UTC	09-11-2021 20:33:19 UTC	Normal	✓ Done	0:00:00.072413
Create Circuit E-Line	SI/e50697abfd2e4c37988e3d99c64639f8	UI	09-11-2021 20:05:55 UTC	09-11-2021 20:06:33 UTC	Rollback	✓ Done	0:00:00.037934

2. Select the required operation.



3. To view more details, select the **required** tab:
    - **Summary**: Additional details about the operation, e.g., Status: Rollback Done.
    - **Logs**: The operation logs for normal and rollback flows.
    - **Errors**: The operation errors, e.g., Discovery took too long.

Service Manager APIs

Crosswork Hierarchical Controller provides APIs to create OTN Line, Packet E-line, and MPLS-TP tunnel service-intents, and provision OTN Lines, Packet E-Lines, and MPLS-TP tunnels on underlying controllers.

You can access the Shared Risk API using Swagger:

- https://<host>/8443/service-manager-app/public/rest/doc

The APIs include:

- Get the list of the operations created by calling the create/update/delete service intent APIs
- Get existing OTN Line service-intents and matching discovered services from underlying controllers
- Create new OTN Line service-intents and provision a new OTN Line on underlying controllers
- Get existing Packet e-Line service-intents and matching discovered services from underlying controllers
- Create new Packet e-Line service-intents and provision a new Packet e-Line on underlying controllers
- Get existing MPLS-TP tunnel service-intents and matching discovered tunnel services from underlying controllers
- Create new MPLS-TP tunnel service-intents and provision a new MPLS-TP tunnel on underlying controllers
- Delete and unprovision an existing service intent of any type

For more details, see the *Cisco Crosswork Hierarchical Controller NBI and SHQL Reference Guide*.

Network Services Orchestrator Crosswork Hierarchical Controller - Function Pack Appendix

Crosswork Hierarchical Controller uses the Network Services Orchestrator (NSO) Crosswork Hierarchical Controller – Function Pack to provision dynamic IP VPN services (**L2-VPN** and **L3-VPN** services).

Provisioning of L2-VPN and L3-VPN services in Crosswork Hierarchical Controller is based on the IETF RFC L2NM and L3NM service scheme. However, not all vendors support the same set of attributes in these models. To avoid failures in provisioning, it is recommended to review the available service scheme options.

There are several payload combinations that allow you to create or modify a service using Network Services Orchestrator:

- **Common Payload:** The attributes that are commonly supported by Nokia NSP and Cisco Crosswork Network Controllers. This is the minimum subset that supports both Nokia NSP and Cisco Crosswork Network Controllers.
- **Nokia NSP Payload:** All attributes supported by Nokia NSP IP controller. Although the Nokia NSP controller will accept the full set of parameters in the RFC LxNM, the Nokia NSP controller may not use all the data.
- **Cisco Crosswork Network Controller Payload:** All attributes supported by Cisco Crosswork Network Controller IP controller. The Cisco Crosswork Network Controller does not accept the full

set of parameters in the RFC LxNM and if a parameter is not supported, Crosswork Network Controller returns an error message.

Once the services are provisioned using NSO (using the UI or JSON files), they are detected by Cisco Crosswork Hierarchical Controller and can be viewed in the Service Assurance application.

This appendix describes some examples of the Network Services Orchestrator (NSO) deployment, as part of Cisco Crosswork Hierarchical Controller.

Note: These payload examples were tested with specific versions of the adapters. There may be some variation in these payloads with different versions of the adapters.

Note: This appendix is intended to introduce you to the capabilities of the function pack. For full details on L2-VPN and L3-VPN service provisioning using NSO, see the Cisco NSO Crosswork Hierarchical Controller – Function Pack User Guide. There are sample templates included in the function pack, for example, cisco-nsp-l2vpn-service.xml, cisco-nsp-l3vpn-service.xml, cisco-cnc-l2vpn-service.xml, and cisco-cnc-l3vpn-service.xml.

NSO has two major components to provide the service CRUD:

- **NED** – a driver to map the relevant get and set operations towards a device or controller and provide them as a YANG model that can contain configuration, NED provides a device configuration model (device can be controller as well). The NEDs for IP COs implement the LxNM model as exposed by the vendors.
- **Function pack** – a template of service specific configuration and the mapping to NED model. A function pack can abstract the service request, can include a complex processing to generate the request to the NED. Such processing can be to decompose a request into multiple NEDs, use topology info to complete configuration not provided by user, and more.

Note: Since optical services are not handled in NSO, NSO has no role in the deployment of optical use cases.

Configure Common L3-VPN (JSON)

A subset of the L3NM service scheme, with the attributes that are commonly supported by Nokia NSP and Cisco Crosswork Network Controllers.

For full details on L3-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller – Function Pack User Guide*.

Table 3. Common L3-VPN Parameters

Parameter	Description
vpn-service	
vpn-id	The VPN ID.
vpn-service-topology	The topology: **ietf-vpn-common:hub-spoke** or **any-to-any**.
vpn-instance-profiles	
vpn-instance-profile	
profile-id	
role	The profile role: **ietf-vpn-common:hub-role**

Parameter	Description
rd	For example: 0:171:171
address-family	
address-family	The address family, for example: **ietf-vpn-common:ipv4**
vpn-targets	
vpn-target	
id	The VPN target ID.
route-targets	
route-targets	The route target, for example: 0:71:71
route-target-type	For example: **both** or **import** or **export**.
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID. Use the vpn-id and add **-R3** or **-R4** as a suffix.
local-as	
active-vpn-instance-profiles	
vpn-instance-profile	
profile-id	The VPN instance profile ID.
vpn-network-accesses	
vpn-network-access	
id	The VPN network access ID.
interface-id	The VPN network access interface ID, for example, **GigabitEthernet0/0/0/2.** This is the access port and may change according to the router.
connection	
encapsulation	
type	The connection encapsulation type: **ietf-vpn-common:dot1q** (VLAN) or **untagged** (port-mode).
dot1q	
tag-type	The tag type: **ietf-vpn-common:c-vlan**
cvlan-id	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 2060.
ip-connection	
ipv4	
local-address	
prefix-length	

Parameter	Description
routing-protocols	
routing-protocol	
id	The routing protocol id, for example: **EBGP**
type	The routing protocol type: **ietf-vpn-common:bgp-routing**
peer-as	
address-family	ietf-vpn-common:ipv4
neighbor	
multihop	
redistribute-connected	
address-family	ietf-vpn-common:ipv4

Detailed JSON Example


```
{
  "ietf-l3vpn-ntw:l3vpn-ntw": {
    "vpn-services": {
      "vpn-service": [
        {
          "vpn-id": "l3vpn-hub-spoke",
          "vpn-service-topology": "ietf-vpn-common:hub-spoke",
          "vpn-instance-profiles": {
            "vpn-instance-profile": [
              {
                "profile-id": "l3vpn-p1-70",
                "role": "ietf-vpn-common:hub-role",
                "rd": "0:171:171",
                "address-family": [
                  {
                    "address-family": "ietf-vpn-common:ipv4",
                    "vpn-targets": {
                      "vpn-target": [
                        {
                          "id": 71,
                          "route-targets": [
                            {
                              "route-target": "0:71:71"
                            }
                          ],
                          "route-target-type": "both"
```

```
            },
            {
              "id": 72,
              "route-targets": [
                {
                  "route-target": "0:72:72"
                }
              ],
              "route-target-type": "import"
            },
            {
              "id": 73,
              "route-targets": [
                {
                  "route-target": "0:73:73"
                }
              ],
              "route-target-type": "export"
            }
          ]
        }
      }
    ]
  },
  {
    "profile-id": "l3vpn-p2-70",
    "role": "ietf-vpn-common:spoke-role",
    "rd": "0:171:171",
    "address-family": [
      {
        "address-family": "ietf-vpn-common:ipv4",
        "vpn-targets": {
          "vpn-target": [
            {
              "id": 71,
              "route-targets": [
                {
                  "route-target": "0:71:71"
                }
              ],
              "route-target-type": "both"
            },
```

```
            {
              "id": 72,
              "route-targets": [
                {
                  "route-target": "0:72:72"
                }
              ],
              "route-target-type": "import"
            },
            {
              "id": 73,
              "route-targets": [
                {
                  "route-target": "0:73:73"
                }
              ],
              "route-target-type": "export"
            }
          ]
        }
      }
    ]
  },
  {
    "profile-id": "l3vpn-p3-70",
    "role": "ietf-vpn-common:spoke-role",
    "rd": "0:171:171",
    "address-family": [
      {
        "address-family": "ietf-vpn-common:ipv4",
        "vpn-targets": {
          "vpn-target": [
            {
              "id": 71,
              "route-targets": [
                {
                  "route-target": "0:71:71"
                }
              ],
              "route-target-type": "both"
            },
            {
```

```
                    "id": 72,
                    "route-targets": [
                      {
                        "route-target": "0:72:72"
                      }
                    ],
                    "route-target-type": "import"
                  },
                  {
                    "id": 73,
                    "route-targets": [
                      {
                        "route-target": "0:73:73"
                      }
                    ],
                    "route-target-type": "export"
                  }
                ]
              }
            }
          ]
        }
      ]
    },
    "vpn-nodes": {
      "vpn-node": [
        {
          "vpn-node-id": "PE-A",
          "local-as": 1,
          "active-vpn-instance-profiles": {
            "vpn-instance-profile": [
              {
                "profile-id": "l3vpn-p1-70"
              }
            ]
          },
          "vpn-network-accesses": {
            "vpn-network-access": [
              {
                "id": "1",
                "interface-id": "GigabitEthernet0/0/0/2",
                "connection": {
```

```
          "encapsulation": {
            "type": "ietf-vpn-common:dot1q",
            "dot1q": {
              "tag-type": "ietf-vpn-common:c-vlan",
              "cvlan-id": 401
            }
          }
        },
        "ip-connection": {
          "ipv4": {
            "local-address": "70.70.10.1",
            "prefix-length": 30
          }
        },
        "routing-protocols": {
          "routing-protocol": [
            {
              "id": "EBGP",
              "type": "ietf-vpn-common:bgp-routing",
              "bgp": {
                "peer-as": 100,
                "address-family": "ietf-vpn-common:ipv4",
                "neighbor": [
                  "70.70.10.2"
                ],
                "multihop": 11,
                "redistribute-connected": [
                  {
                    "address-family": "ietf-vpn-common:ipv4"
                  }
                ]
              }
            }
          ]
        }
      }
    ]
  }
},
{
  "vpn-node-id": "PE-B",
  "local-as": 1,
```

```
"active-vpn-instance-profiles": {
  "vpn-instance-profile": [
    {
      "profile-id": "l3vpn-p2-70"
    }
  ]
},
"vpn-network-accesses": {
  "vpn-network-access": [
    {
      "id": "1",
      "interface-id": "GigabitEthernet0/0/0/1",
      "connection": {
        "encapsulation": {
          "type": "ietf-vpn-common:dot1q",
          "dot1q": {
            "tag-type": "ietf-vpn-common:c-vlan",
            "cvlan-id": 401
          }
        }
      },
      "ip-connection": {
        "ipv4": {
          "local-address": "70.70.11.1",
          "prefix-length": 30
        }
      },
      "routing-protocols": {
        "routing-protocol": [
          {
            "id": "EBGP",
            "type": "ietf-vpn-common:bgp-routing",
            "bgp": {
              "peer-as": 100,
              "address-family": "ietf-vpn-common:ipv4",
              "neighbor": [
                "70.70.11.2"
              ],
              "multihop": 11,
              "redistribute-connected": [
                {
                  "address-family": "ietf-vpn-common:ipv4"
```

```
                    }
                  ]
                }
              }
            ]
          }
        }
      ]
    }
  },
  {
    "vpn-node-id": "Spitfire-RON-16",
    "local-as": 1,
    "active-vpn-instance-profiles": {
      "vpn-instance-profile": [
        {
          "profile-id": "l3vpn-p3-70"
        }
      ]
    },
    "vpn-network-accesses": {
      "vpn-network-access": [
        {
          "id": "1",
          "interface-id": "FourHundredGigE0/0/0/1",
          "connection": {
            "encapsulation": {
              "type": "ietf-vpn-common:dot1q",
              "dot1q": {
                "tag-type": "ietf-vpn-common:c-vlan",
                "cvlan-id": 401
              }
            }
          },
          "ip-connection": {
            "ipv4": {
              "local-address": "70.70.12.1",
              "prefix-length": 30
            }
          },
          "routing-protocols": {
            "routing-protocol": [
```

```
                                {
                                  "id": "EBGP",
                                  "type": "ietf-vpn-common:bgp-routing",
                                  "bgp": {
                                    "peer-as": 100,
                                    "address-family": "ietf-vpn-common:ipv4",
                                    "neighbor": [
                                      "70.70.12.2"
                                    ],
                                    "multihop": 11,
                                    "redistribute-connected": [
                                      {
                                        "address-family": "ietf-vpn-common:ipv4"
                                      }
                                    ]
                                  }
                                }
                              ]
                            }
                          }
                        ]
                      }
                    }
                  ]
                },
                "cisco-hco-nm:hco-controller": "CNC"
              }
            ]
          }
        }
      }
```

Configure Common L2-VPN using NSO (JSON)

A subset of the L2NM service scheme, with the attributes that are commonly supported by Nokia NSP and Cisco Crosswork Network Controllers.

For full details on L2-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide*.

Table 4. Common L2-VPN Parameters

Parameter	Description
vpn-services	
vpn-service	

Parameter	Description
vpn-id	The VPN ID.
vpn-type	The VPN type: **ietf-vpn-common:mpls-evpn**.
vpn-service-topology	The topology: **ietf-vpn-common:hub-spoke** or **any-to-any**.
global-parameters-profiles	
global-parameters-profile	
profile-id	
vpn-target	
id	
route-targets	
route-target	The route target, for example: 0:12:12
route-target-type	The route target type, for example: both
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID. Use the vpn-id and add **-R3** or **-R4** as a suffix.
role	The VPN node role, for example: **ietf-vpn-common:hub-role** or **ietf-vpn-common:spoke-role**
signaling-option	
evpn-policies	
mac-learning-mode	The mac learning mode: **ietf-l2vpn-ntw:control-plane**
vpn-network-accesses	
vpn-network-access	
id	The VPN network access ID in the format **int_<number>**, for example, int_223_1.
interface-id	The VPN network access interface ID, for example, **GigabitEthernet0/0/0/2**. This is the access port and may change according to the router.
connection **encapsulation**	
encap-type	The connection encapsulation type: **ietf-vpn-common:dot1q** (VLAN).
dot1q cvlan-id	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 2060.
tag-operations	
push	null
tag-1	The tag, for example: 202

Parameter	Description
cisco-hco-nm:hco-controller	The controller, for example: CNC

Detailed JSON Example


```
{
  "ietf-l2vpn-ntw:l2vpn-ntw": {
    "vpn-services": {
      "vpn-service": [
        {
          "vpn-id": "ETREE-HS-ABCD",
          "vpn-type": "ietf-vpn-common:mpls-evpn",
          "vpn-service-topology": "ietf-vpn-common:hub-spoke",
          "global-parameters-profiles": {
            "global-parameters-profile": [
              {
                "profile-id": "test",
                "vpn-target": [
                  {
                    "id": 1,
                    "route-targets": [
                      {
                        "route-target": "0:12:12"
                      }
                    ],
                    "route-target-type": "both"
                  }
                ]
              }
            ]
          },
          "vpn-nodes": {
            "vpn-node": [
              {
                "vpn-node-id": "PE-A",
                "role": "ietf-vpn-common:hub-role",
                "signaling-option": {
                  "evpn-policies": {
                    "mac-learning-mode": "ietf-l2vpn-ntw:control-plane"
                  }
                },
                "vpn-network-accesses": {
                  "vpn-network-access": [
```

```
        {
          "id": "285",
          "interface-id": "GigabitEthernet0/0/0/2",
          "connection": {
            "encapsulation": {
              "encap-type": "ietf-vpn-common:dot1q",
              "dot1q": {
                "cvlan-id": 285,
                "tag-operations": {
                  "push": [
                    null
                  ],
                  "tag-1": 202
                }
              }
            }
          }
        }
      ]
    }
  },
  {
    "vpn-node-id": "PE-B",
    "role": "ietf-vpn-common:spoke-role",
    "signaling-option": {
      "evpn-policies": {
        "mac-learning-mode": "ietf-l2vpn-ntw:control-plane"
      }
    },
    "vpn-network-accesses": {
      "vpn-network-access": [
        {
          "id": "285",
          "interface-id": "GigabitEthernet0/0/0/2",
          "connection": {
            "encapsulation": {
              "encap-type": "ietf-vpn-common:dot1q",
              "dot1q": {
                "cvlan-id": 285,
                "tag-operations": {
                  "push": [
                    null
```

```
                    ],
                    "tag-1": 202
                  }
                }
              }
            }
          ]
        }
      },
      {
        "vpn-node-id": "PE-C",
        "role": "ietf-vpn-common:spoke-role",
        "signaling-option": {
          "evpn-policies": {
            "mac-learning-mode": "ietf-l2vpn-ntw:control-plane"
          }
        },
        "vpn-network-accesses": {
          "vpn-network-access": [
            {
              "id": "285",
              "interface-id": "GigabitEthernet0/0/0/2",
              "connection": {
                "encapsulation": {
                  "encap-type": "ietf-vpn-common:dot1q",
                  "dot1q": {
                    "cvlan-id": 285,
                    "tag-operations": {
                      "push": [
                        null
                      ],
                      "tag-1": 202
                    }
                  }
                }
              }
            }
          ]
        }
      }
    ]
```

```
            },
            "cisco-hco-nm:hco-controller": "CNC"
          }
        ]
      }
    }
  }
```

Configure Nokia NSP L3-VPN using NSO (JSON)

For full details on Nokia NSP L3-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide*.

The L3-VPN JSON requires the following high-level structure.

```
{
   "ietf-l3vpn-ntw:l3vpn-ntw":{
      "vpn-services":{
         "vpn-service":[
            {
               "vpn-id":"Abcd100",
               "vpn-name":"Abcd100",
               "vpn-description":"Abcd100",
               "customer-name":"1",
               "vpn-type":"ietf-vpn-common:l3vpn",
               "vpn-service-topology":"ietf-vpn-common:hub-spoke",
               "status":{},
               "vpn-instance-profiles":{},
               "underlay-transport":{},
               "vpn-nodes":{}
            }
         ]
      }
   }
}
```

This corresponds to the L3-VPN service page in the NSO user interface.

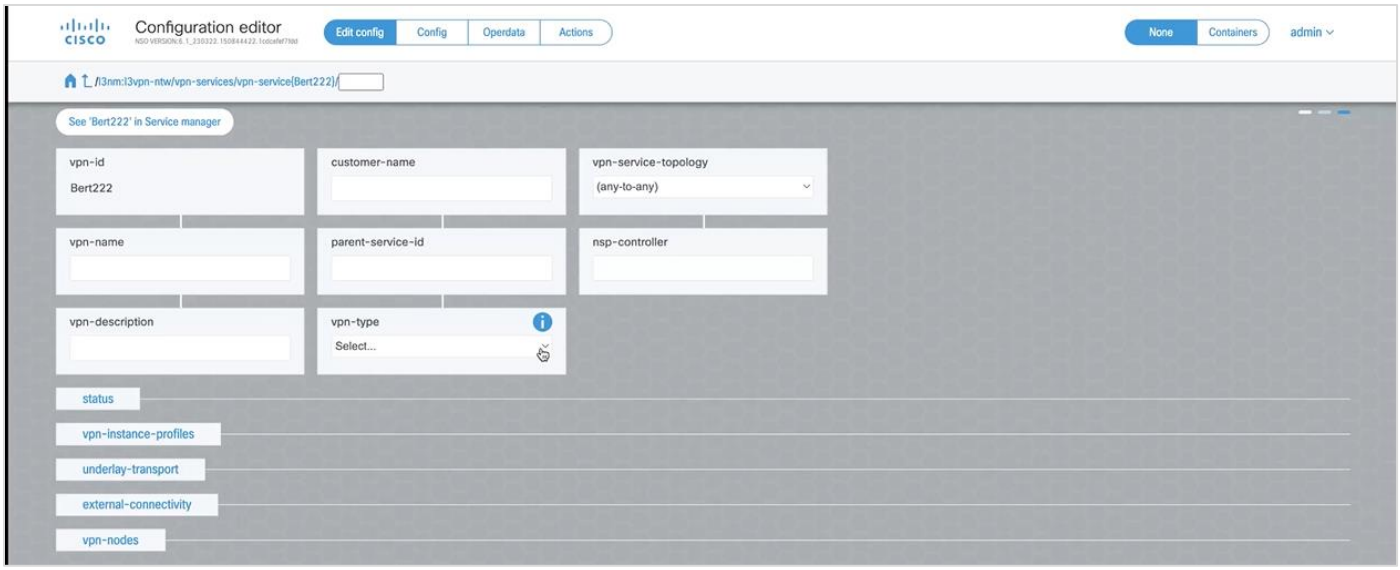


Table 5. Nokia NSP L3-VPN Parameters

Parameter	Description
vpn-service	
vpn-id	The VPN ID.
vpn-name	The VPN name as a string.
vpn-description	The VPN description as a string.
customer-name	The customer's name exactly as configured in the Nokia NSP controller (this is an integer and not a string)
vpn-type	The VPN type, ietf-vpn-common:l3vpn.
vpn-service-topology	The topology: ietf-vpn-common:**hub-spoke** or **any-to-any**.
status **admin-status** status	The status of the vpn-service: vpn-common:**admin-up**.
vpn-instance-profiles	
vpn-instance-profile	
profile-id	The profile ID.
rd	The rd. For example, 0:65000:223.
address-family	
address-family	The address family. For example, ietf-vpn-common:ipv4.
vpn-targets	
vpn-policies	
import-policy	The import policy.

Parameter	Description
export-policy	The export policy.
underlay-transport protocol	The underlay-transport: ietf-vpn-common:**rsvp-te**
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID.
description	The VPN node description.
ne-id	The NE ID.
router-id	The router ID.
active-vpn-instance-profiles **vpn-instance-profile** profile-id	The profile ID.
vpn-network-access	
id	The VPN network access ID in the format **int_<number>**, for example, int_223_1.
interface-id	The VPN network access interface ID, for example, 1/1/c1/1.
description	The VPN network access description.
vpn-instance-profile	The VPN network access VPN instance profile.
status **admin-status** status	The status of the VPN network access interface.
connection **encapsulation**	
type	The connection encapsulation type: ietf-vpn-common:dot1q
dot1q cvlan-id	The CVLAN ID for the dot1q encapsulation.
ip-connection **ipv4**	
local-address	The IP connection local address.
prefix-length	The IP connection prefix length.

Detailed JSON Example

```
{
  "ietf-l3vpn-ntw:l3vpn-ntw": {
```

```
"vpn-services": {
  "vpn-service": [
    {
      "vpn-id": "Abcd100",
      "vpn-name": "Abcd100",
      "vpn-description": "Abcd100",
      "customer-name": "1",
      "vpn-type": "ietf-vpn-common:l3vpn",
      "vpn-service-topology": "ietf-vpn-common:hub-spoke",
      "status": {
        "admin-status": {
          "status": "ietf-vpn-common:admin-up"
        }
      },
      "vpn-instance-profiles": {
        "vpn-instance-profile": [
          {
            "profile-id": "profile_1",
            "rd": "0:65000:223",
            "address-family": [
              {
                "address-family": "ietf-vpn-common:ipv4",
                "vpn-targets": {
                  "vpn-policies": {
                    "import-policy": "Alpha-223-Import",
                    "export-policy": "Alpha-223-Export"
                  }
                }
              }
            ]
          }
        ]
      },
      "underlay-transport": {
        "protocol": [
          "ietf-vpn-common:rsvp-te"
        ]
      },
      "vpn-nodes": {
        "vpn-node": [
          {
            "vpn-node-id": "Alpha-223-R1",
            "description": "Alpha-223-R1",
            "ne-id": "10.10.10.1",
            "router-id": "10.10.10.1",
            "active-vpn-instance-profiles": {
              "vpn-instance-profile": [
                {
                  "profile-id": "profile_1"
                }
              ]
            },
            "status": {
              "admin-status": {
                "status": "ietf-vpn-common:admin-up"
              }
            },
            "vpn-network-accesses": {
              "vpn-network-access": [
                {
                  "id": "int_223_1",
                  "interface-id": "1/1/c1/1",
                  "description": "int_223_1",
                  "vpn-instance-profile": "profile_1",
                  "status": {
                    "admin-status": {
```

```
            "status": "ietf-vpn-common:admin-up"
          }
        },
        "connection": {
          "encapsulation": {
            "type": "ietf-vpn-common:dot1q",
            "dot1q": {
              "cvlan-id": 223
            }
          }
        },
        "ip-connection": {
          "ipv4": {
            "local-address": "1.1.1.1",
            "prefix-length": 24
          }
        }
      }
    ]
  }
},
{
  "vpn-node-id": "Alpha-223-R5",
  "description": "Alpha-223-R5",
  "ne-id": "10.10.10.5",
  "router-id": "10.10.10.5",
  "active-vpn-instance-profiles": {
    "vpn-instance-profile": [
      {
        "profile-id": "profile_1"
      }
    ]
  },
  "status": {
    "admin-status": {
      "status": "ietf-vpn-common:admin-up"
    }
  },
  "vpn-network-accesses": {
    "vpn-network-access": [
      {
        "id": "int_223_1",
        "interface-id": "1/1/3",
        "description": "int_223_1",
        "vpn-instance-profile": "profile_1",
        "status": {
          "admin-status": {
            "status": "ietf-vpn-common:admin-up"
          }
        },
        "connection": {
          "encapsulation": {
            "type": "ietf-vpn-common:dot1q",
            "dot1q": {
              "cvlan-id": 223
            }
          }
        },
        "ip-connection": {
          "ipv4": {
            "local-address": "5.5.5.5",
            "prefix-length": 24
          }
        }
      }
    ]
```

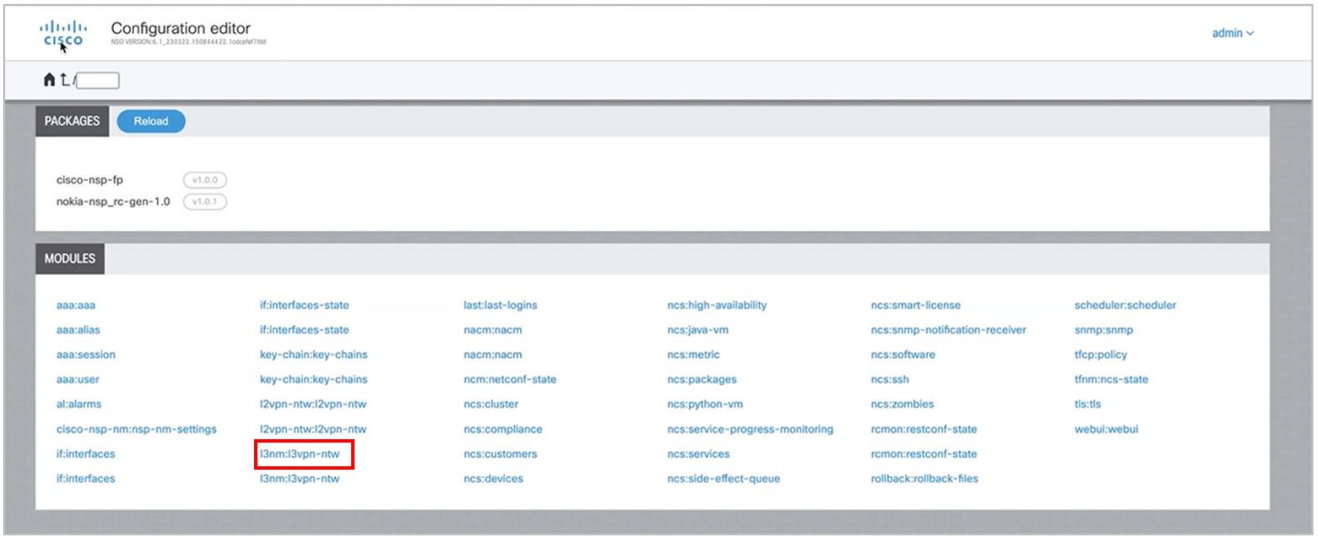
```
                    }
                }
            ]
        }
    }
]
}
}
}
```

Configure Nokia NSP L3-VPN using NSO (UI)

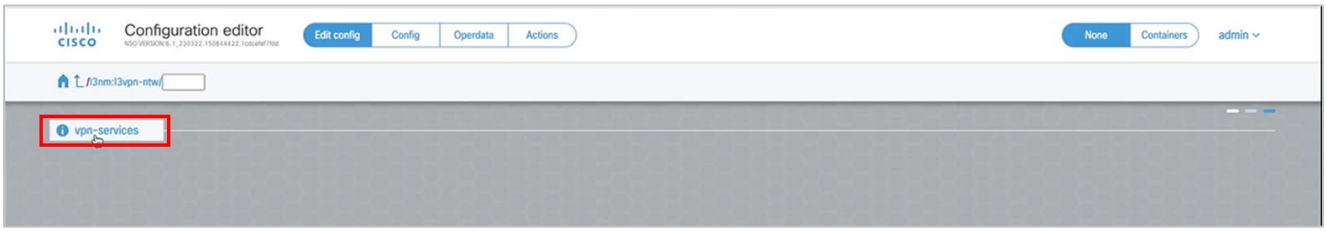
To add a Nokia NSP L3-VPN service, add two VPN nodes, each with their interface. This is useful for testing a L3-VPN service.

To add a Nokia NSP L3-VPN:

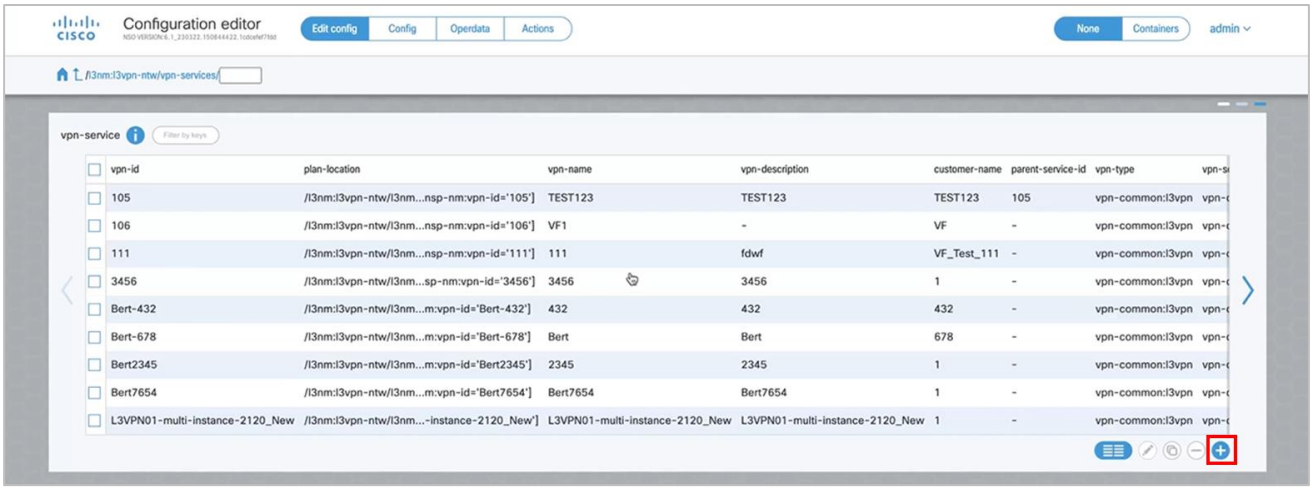
1. Launch NSO.



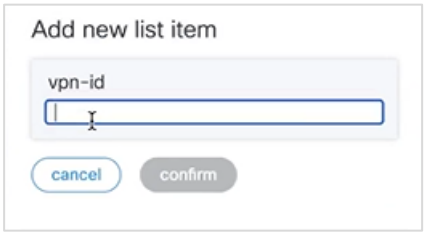
2. Click **l3nm:l3vpn-ntw**.



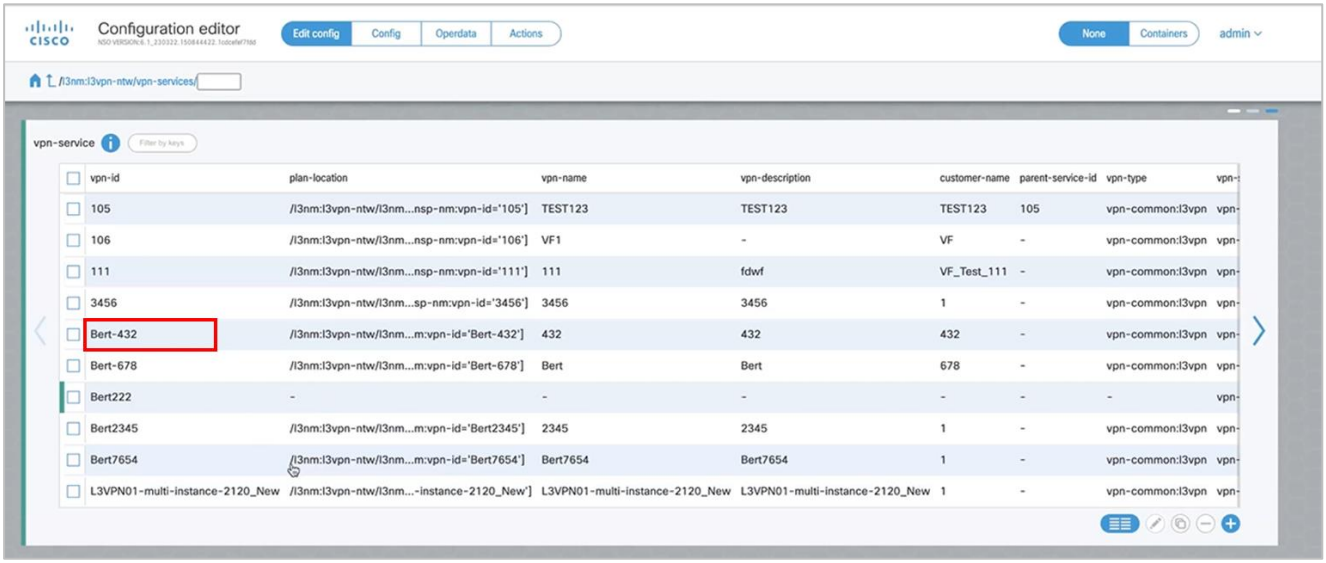
3. Click **vpn-services**.



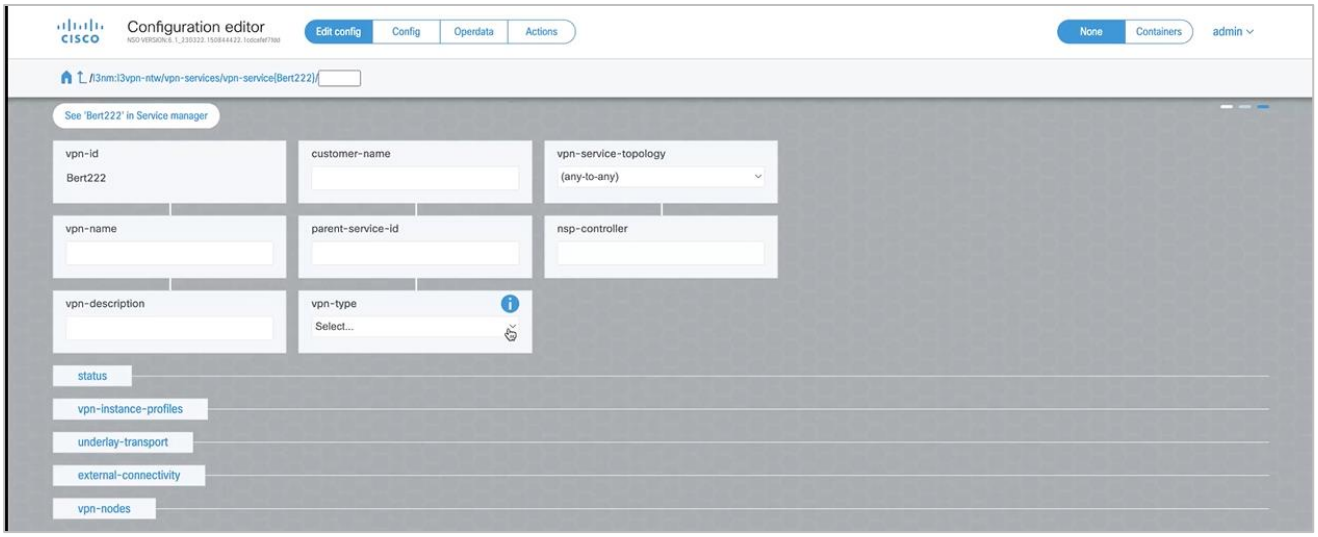
4. Click **+**.



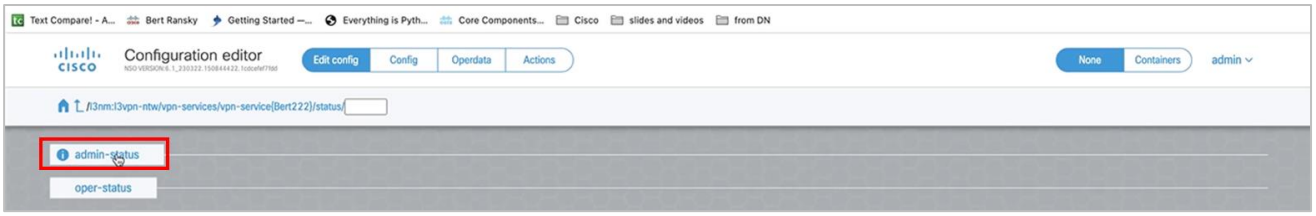
5. Enter a unique **vpn-id** and click **confirm**.



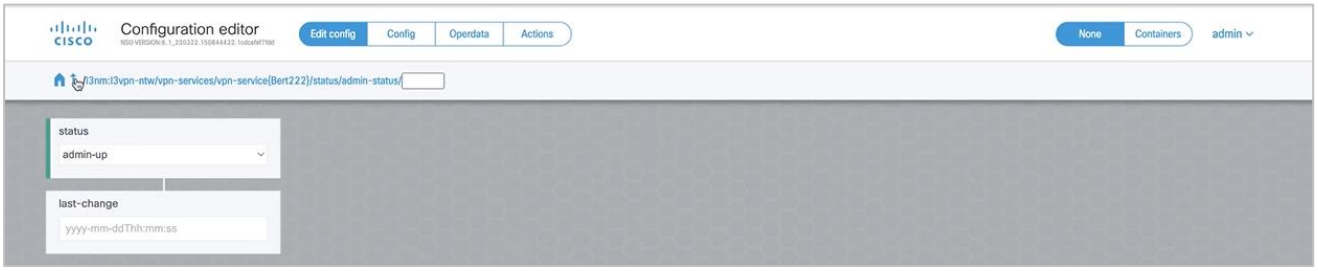
6. Click the **vpn service**.



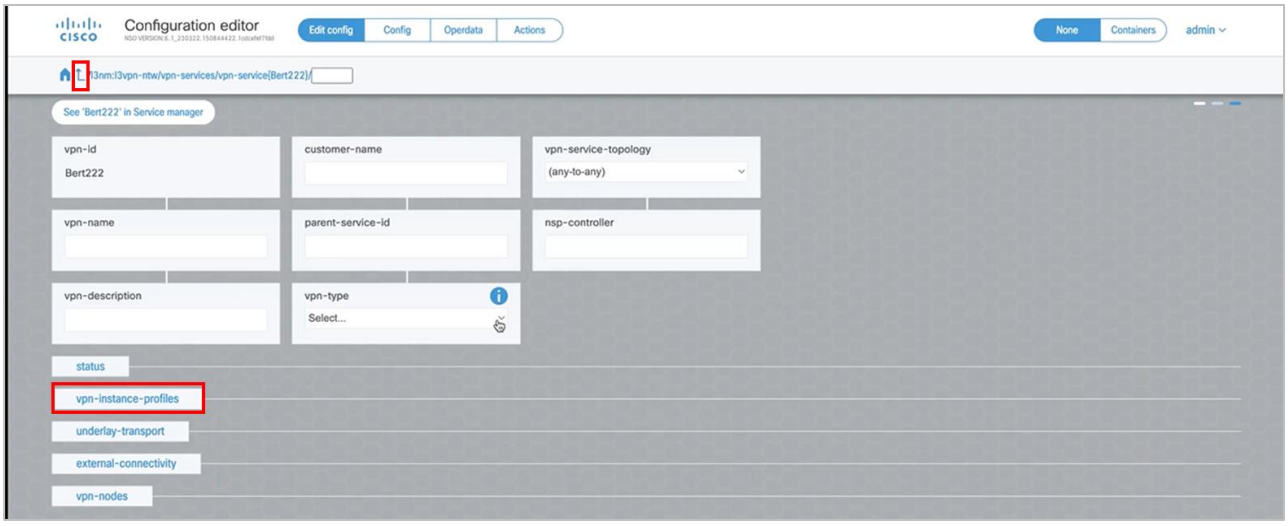
7. Enter the **customer-name** exactly as configured in the Nokia NSP controller (this is an integer and not a string).
8. Enter the **vpn-name** as a string.
9. Enter the **vpn-description** as a string.
10. Set the **vpn-type** to **l3vpn**.
11. Set the **vpn-service-topology** to **hub-spoke** or **any-to-any**.
12. Select the **nsp-controller** (if there is a default nsp-controller, then you can skip this).
13. Click **status**.



14. Click **admin-status**, and then set the **status** to **admin-up**.



15. Return to the vpn (using the breadcrumbs at the top of the page).

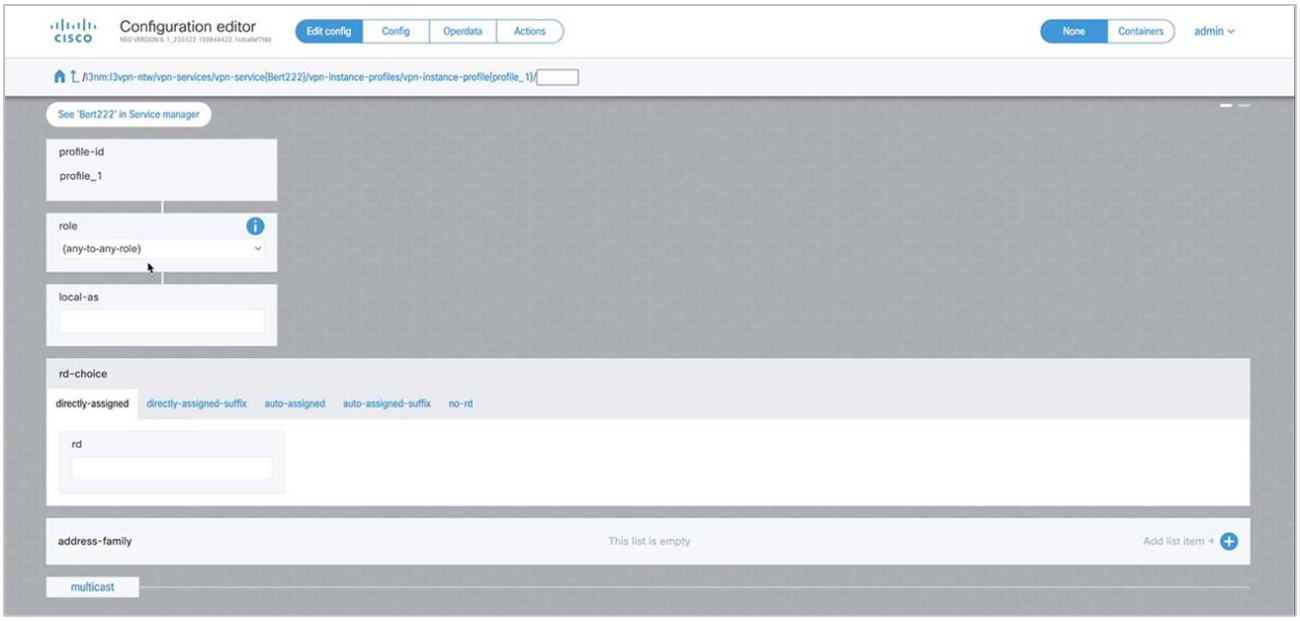


16. Click **vpn-instance-profiles**.

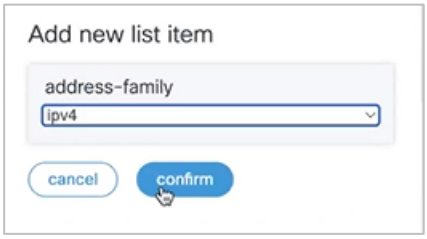
17. Click **+**.

18. Enter a **profile-id** and then click **confirm**.

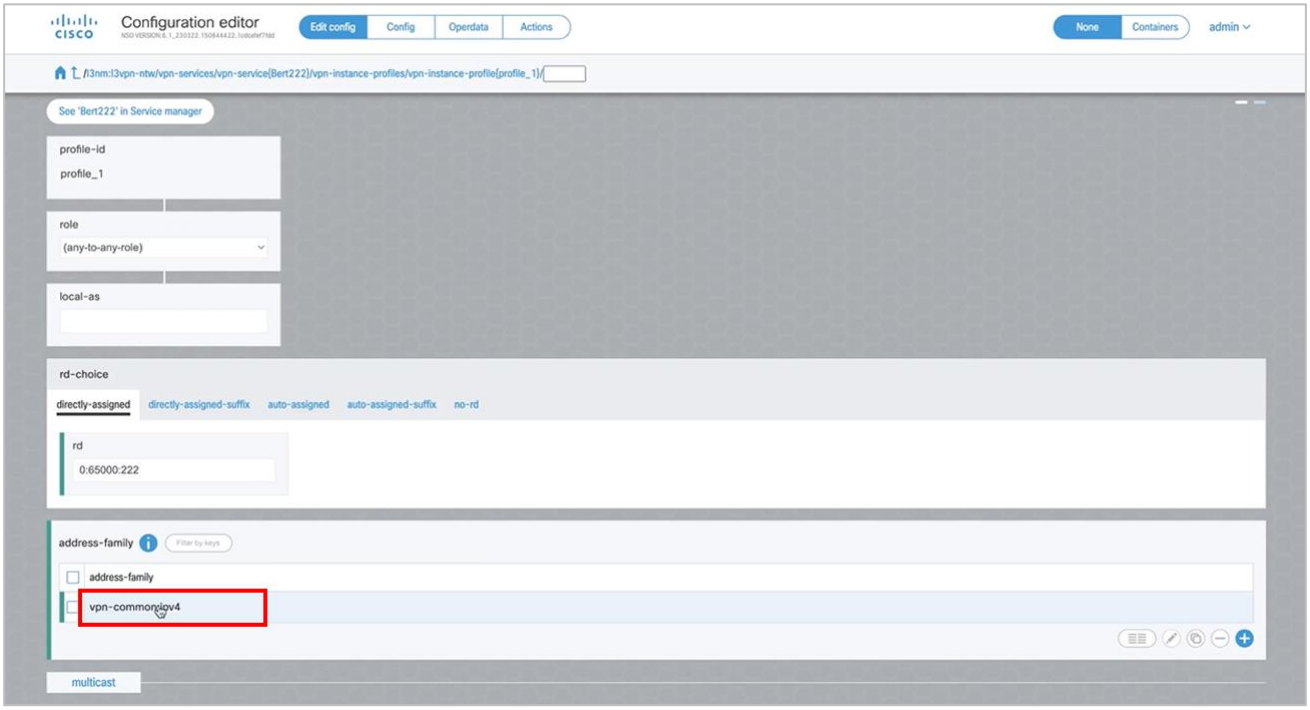
19. Click on the profile.



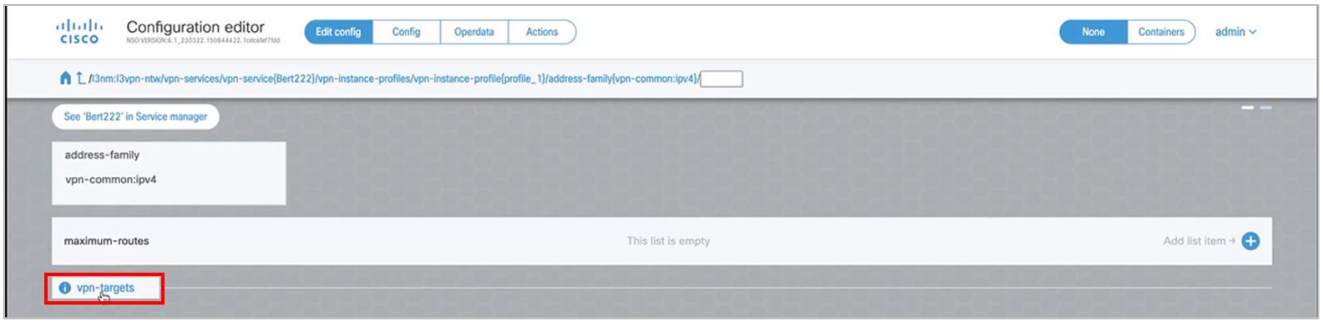
20. Enter the **rd** in the **directly-assigned** tab.
21. Click **+** in the **address-family**.



22. Select **ipv4** and click **confirm**.

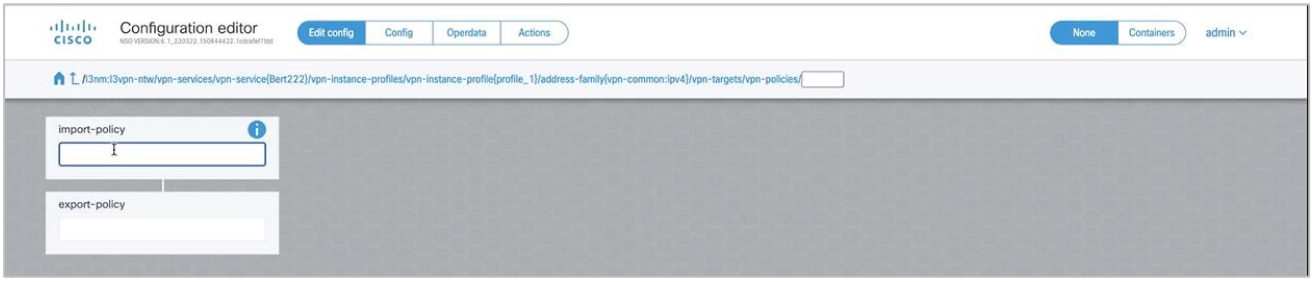


23. Click on the address-family.

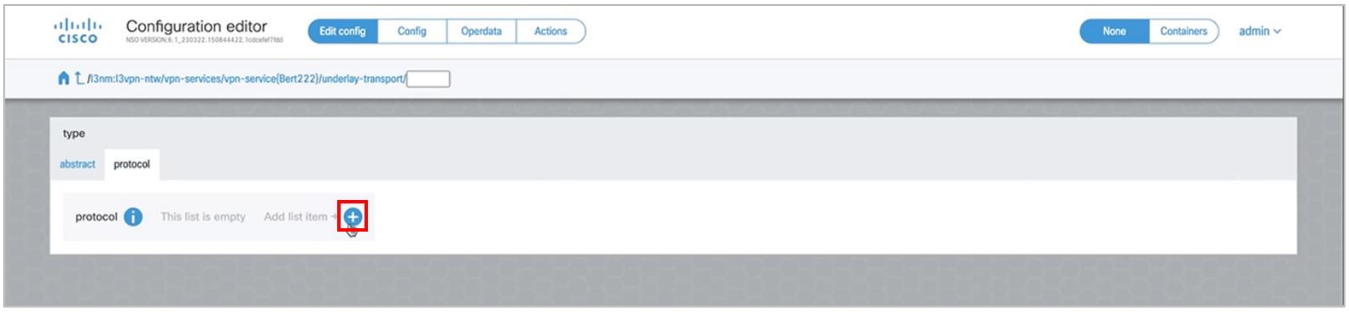


24. Click **vpn-targets**.

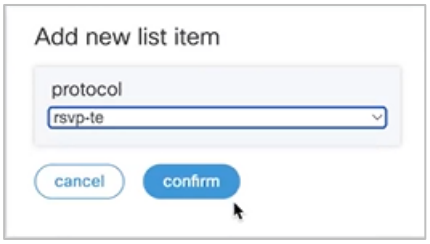
25. Click **vpn-policies**.



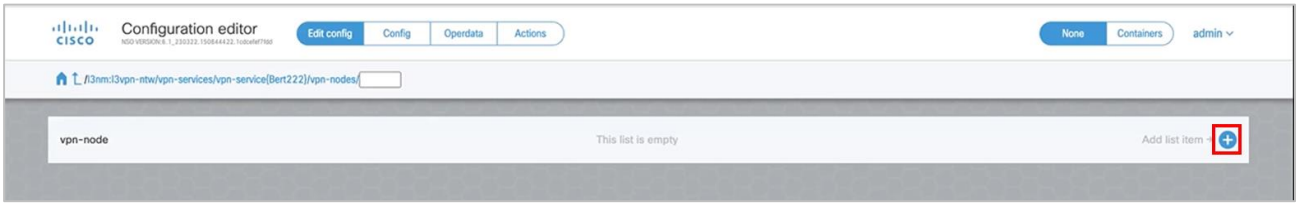
26. Specify the **import-policy** and **export-policy**.
27. Navigate back to the L3VPN service page and click **underlay-transport**.
28. Select the **protocol** tab.



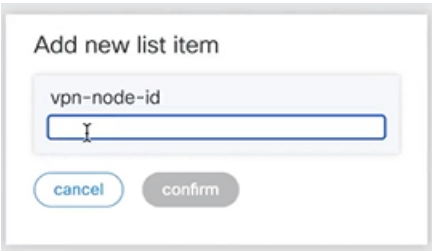
29. Click **+**.



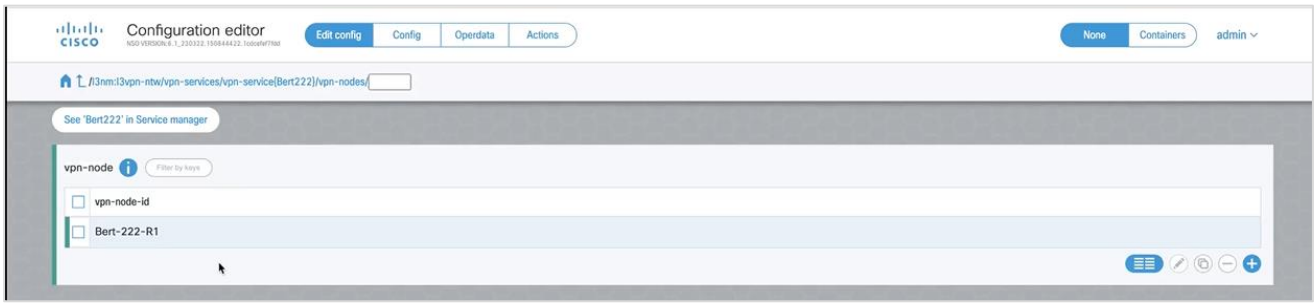
30. Select **rsvp-te** and click **confirm**.
31. Navigate back to the L3VPN service page and click **vpn-nodes** (**external-connectivity** is not required).



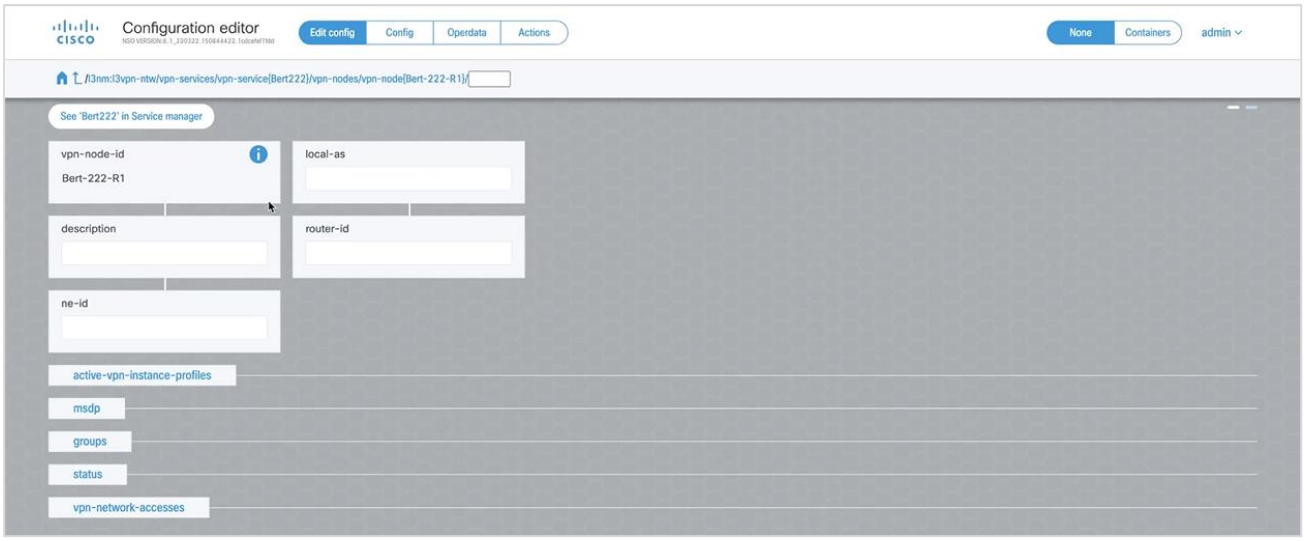
32. Click **+**. The vpn=node is a router participating in the VPN. For example, R1 and R5 in this topology.



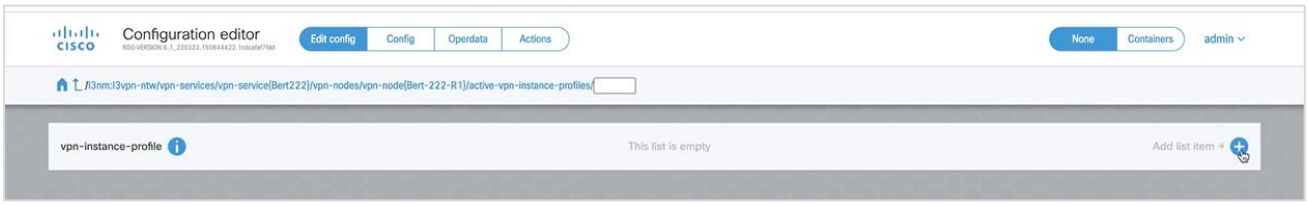
33. Enter the **vpn-node-id** and click **confirm**. This will appear on the router as the endpoint of the tunnel.



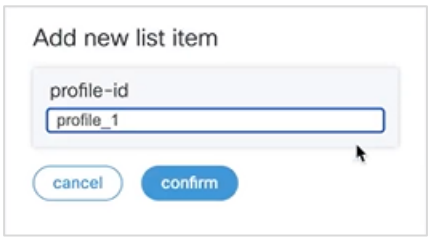
34. Click on the vpn-node.



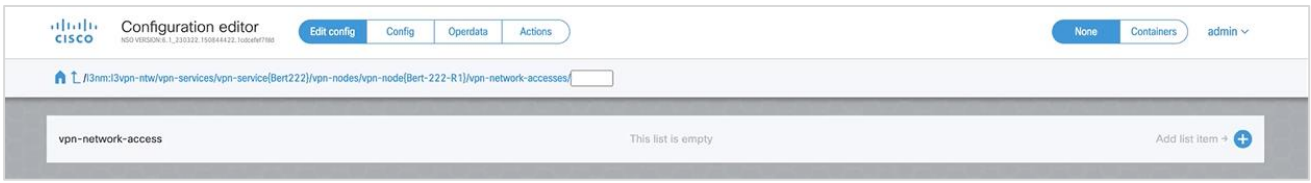
35. Enter a **description**.
36. Specify the **router-id** and the **ne-id**.
37. Click **active-vpn-instance-profiles**.



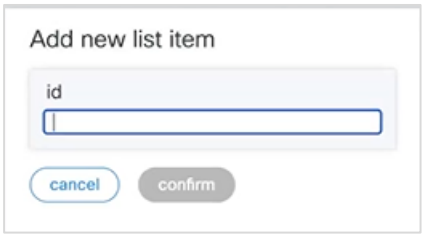
38. Click +.



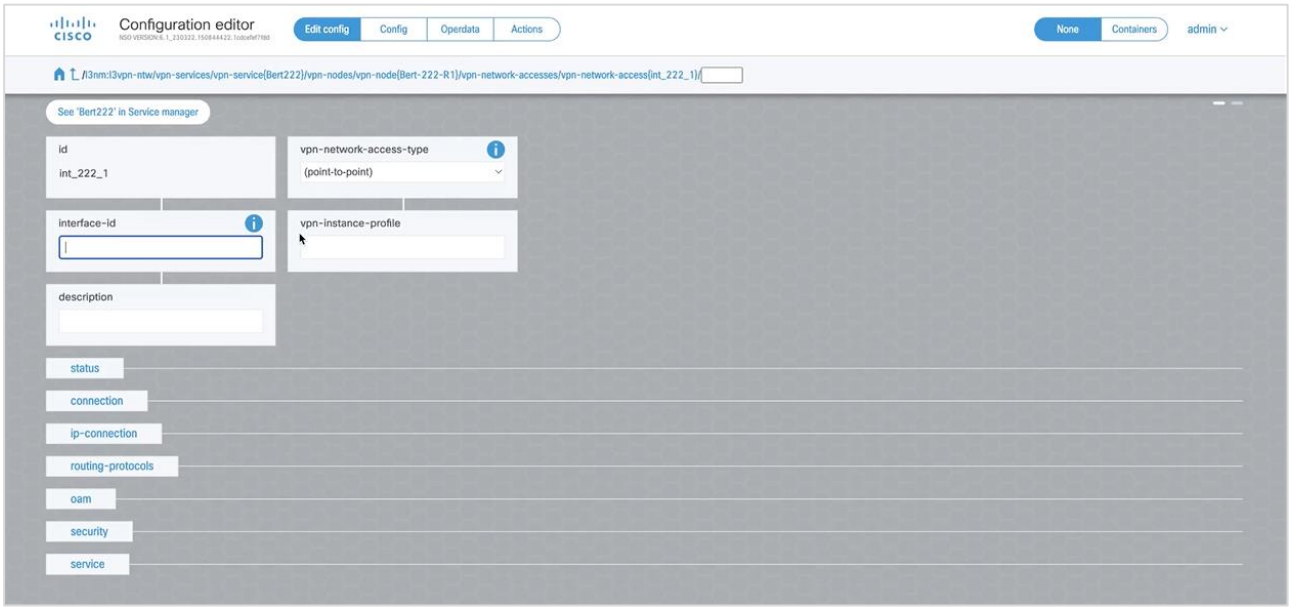
39. Enter a **profile-id** and click **confirm**.
40. Navigate back to the vpn-node page and click **status**. And as done previously, set this to **admin-up**.
41. Navigate back to the vpn-node page and click **vpn-network-accesses**.



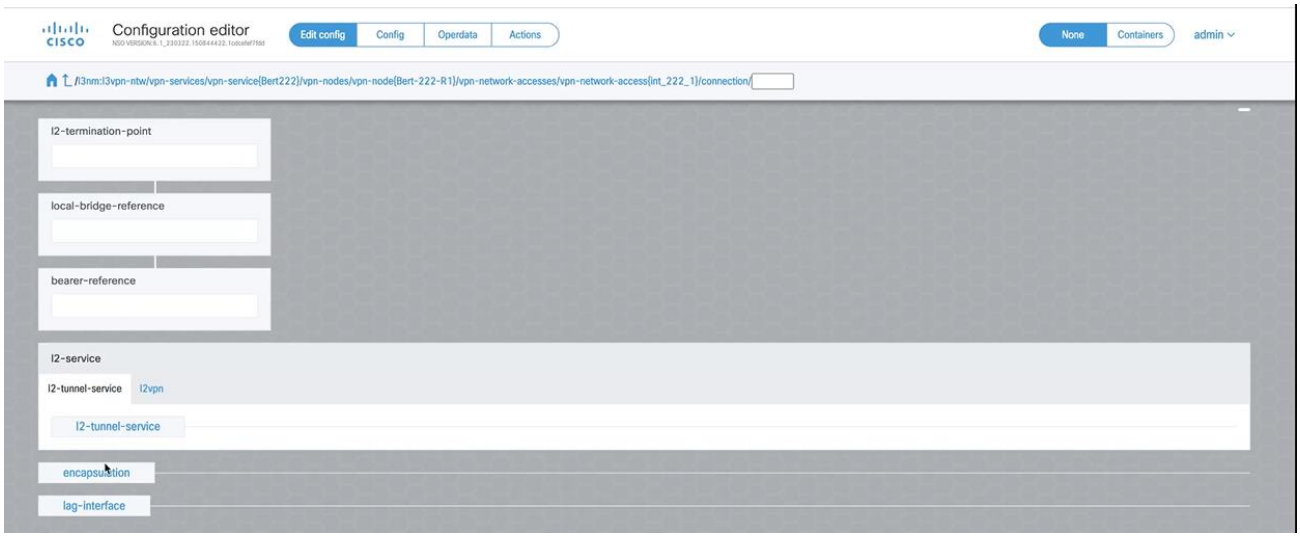
42. Click +. This defines the interfaces participating in the VPN.



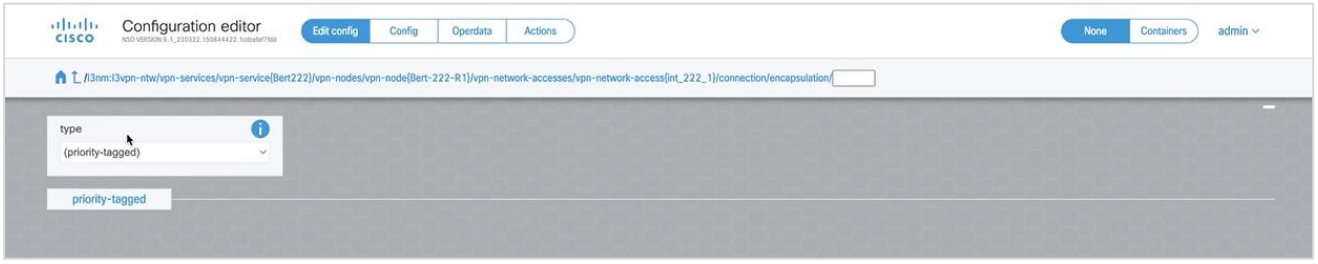
43. Specify the interface **id** and click **confirm**. This is in the format **int_<number>**, for example, **int_222_1**.
44. Click on the interface.



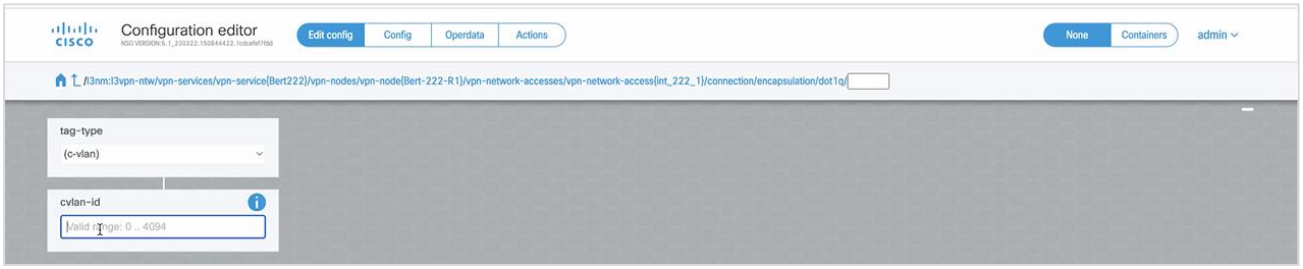
45. Enter the **interface_id**. This is the interface name, for example, from R1
46. Enter the **description** as a string.
47. Select the **vpn-instance-profile**.
48. Click **status**.
49. Click **admin-status**, and then set the **status** to **admin-up**.
50. Navigate back to the interface page.
51. Click **Connection**.



52. Click **encapsulation**.

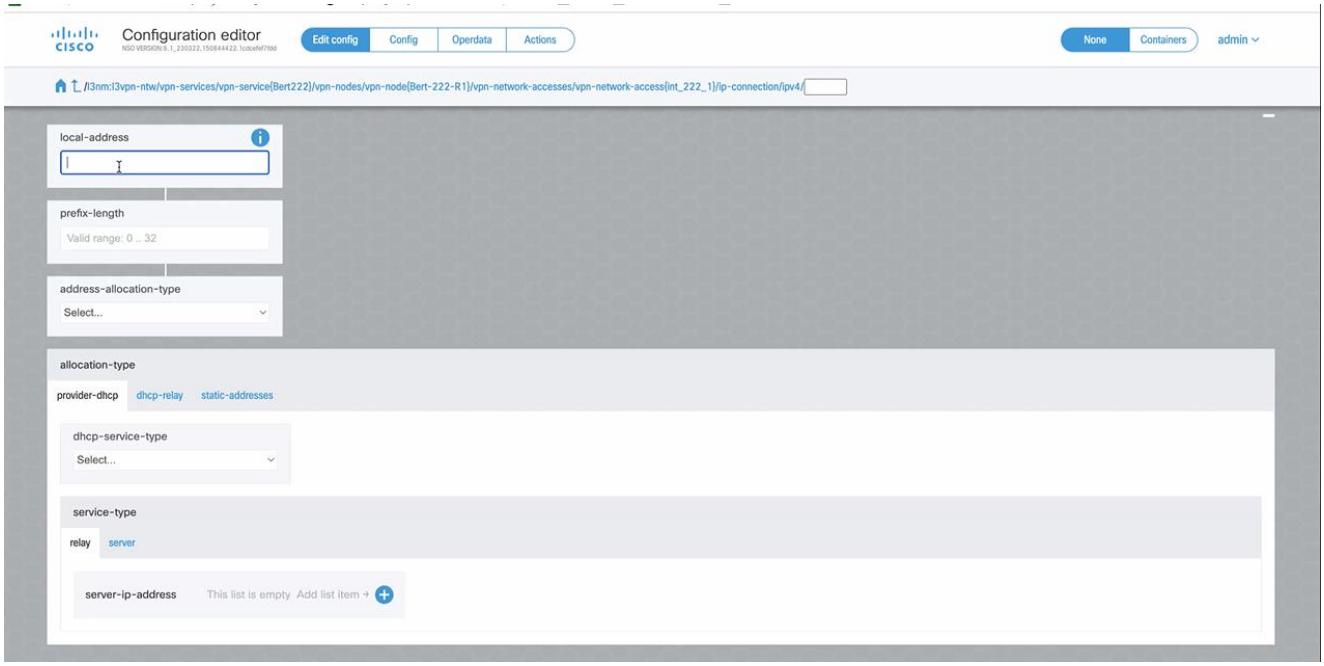


53. Set the **type** to **dot1q**.
54. Click **dot1q**.



55. Enter the **cvlan-id**.
56. Navigate back to the interface page.
57. Click **ip-connection**.

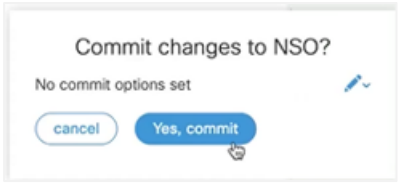
58. Select **ipv4**.



59. Enter the **local-address**.
60. Enter the **prefix-length**.
61. Navigate back to the VPN service page.
62. Add another **vpn-node** following the process previously described to also add an interface.
63. Click Commit Manager (at the bottom of the screen).

    .
64. Review the configuration.
65. Click **Commit**.

66. Click **Yes, commit**.
67. Once it has finished, check the VPN.

Configure Nokia NSP L2-VPN using NSO (JSON)

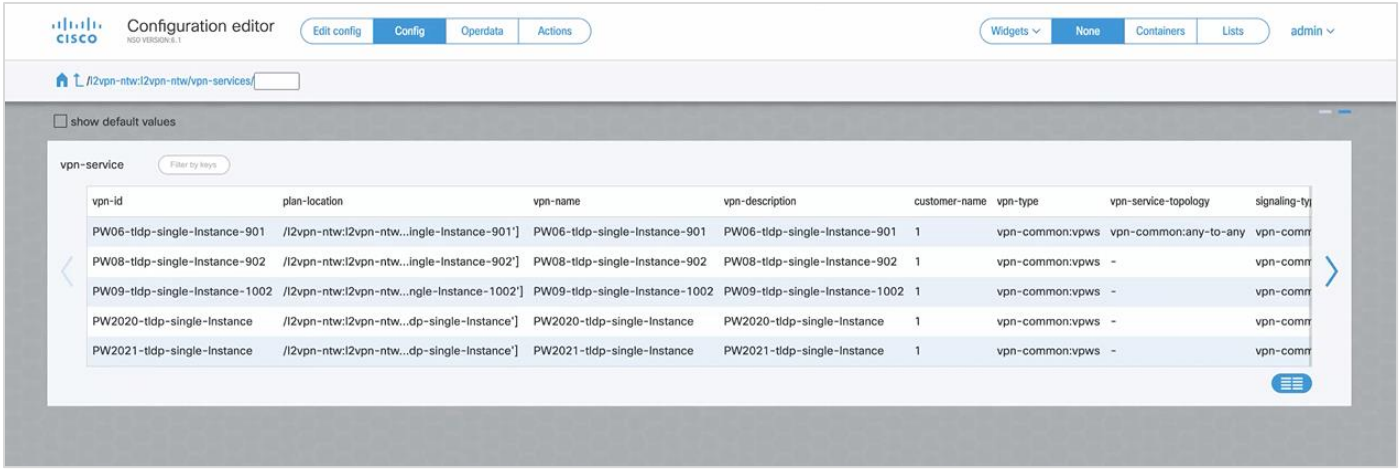
For full details on Nokia NSP L2-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide*.

The L2-VPN JSON requires the following high-level structure.

```
{
   "ietf-l2vpn-ntw:l2vpn-ntw":{
      "vpn-services":{
         "vpn-service":[
            {
               "vpn-id":"Abcd100",
               "vpn-name":"Abcd100",
               "vpn-description":"Abcd100",
               "customer-name":"1",
               "vpn-type":"ietf-vpn-common:vpws",
```

```
                    "vpn-service-topology":"ietf-vpn-common:any-to-any",
                    "signaling-type":"ietf-vpn-common:ldp-signaling",
                    "underlay-transport":{},
                    "status":{},
                    "vpn-nodes":{}
                }
            ]
        }
    }
}
```

This corresponds to the L2-VPN service page in the NSO user interface.



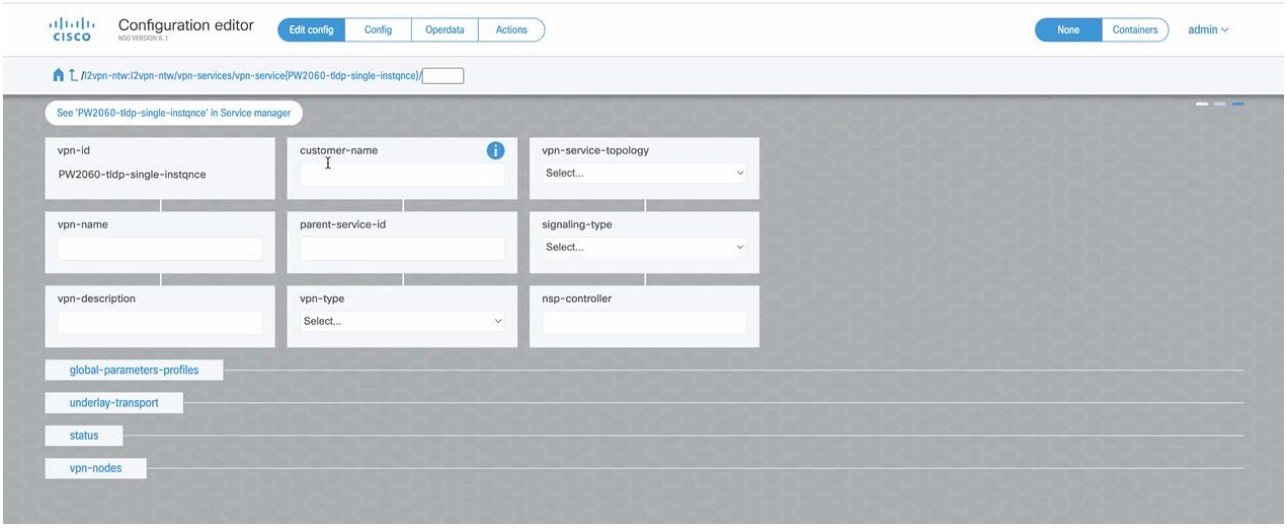


Table 6. Nokia NSP L2-VPN Parameters

Parameter	Description
vpn-service	
vpn-id	The VPN ID.
vpn-name	The VPN name as a string.
vpn-description	The VPN description as a string.

Parameter	Description
customer-name	The customer's name exactly as configured in the Nokia NSP controller (this is an integer and not a string)
vpn-type	The VPN type: **ietf-vpn-common: vpws**.
vpn-service-topology	The topology: **ietf-vpn-common:hub-spoke** or **any-to-any**.
signaling-type	The signaling type: **ietf-vpn-common:ldp-signaling**.
underlay-transport	
protocol	The underlay-transport: **ietf-vpn-common:rsvp-te**
status **admin-status** status	The status of the vpn-service: **ietf-vpn-common:admin-up**
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID. Use the vpn-id and add **-R3** or **-R4** as a suffix.
description	The VPN node description.
ne-id	The NE ID.
router-id	The router ID.
status admin-status status	The status of the node: **ietf-vpn-common:admin-up**
signaling-option	
signaling-type	The signaling type: **ietf-vpn-common:ldp-signaling**
ldp-or-l2tp	
t-ldp-pw-type	The t-ldp-pw-type: **ietf-l2vpn-ntw:vpws-type**
pw-type	The pseudowire type: **ietf-l2vpn-ntw:ethernet**
ac-pw-list	
peer-addr	The peer address. When configuring R3, this is R4, and when configuring R4, this is R3.
vc-id	The pseudowire id, for example, 2060.
pw-priority	The PW priority, for example, 1.
vpn-network-accesses	
vpn-network-access	
id	The VPN network access ID in the format **int_<number>**, for example, int_223_1.
interface-id	The VPN network access interface ID, for example, **Port 1/1/9**. This is the

Parameter	Description
	access port and may change according to the router.
status admin-status status	The status of the interface: **ietf-vpn-common:admin-up**
connection **encapsulation**	
encap-type	The connection encapsulation type: **ietf-vpn-common:dot1q** (VLAN) or **priority-tagged** (port-mode).
dot1q/priority-tagged cvlan-id	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 2060.
service	
mtu	The MTU.

Detailed JSON Example


```
{
   "ietf-l2vpn-ntw:l2vpn-ntw":{
      "vpn-services":{
         "vpn-service":[
            {
               "vpn-id":"PW2060-tldp-single-instqnce",
               "vpn-name":"PW2060-tldp-single-instqnce",
               "vpn-description":"PW2060-tldp-single-instqnce",
               "customer-name":"1",
               "vpn-type":"ietf-vpn-common:vpws",
               "vpn-service-topology":"ietf-vpn-common:any-to-any",
               "signaling-type":"ietf-vpn-common:ldp-signaling",
               "underlay-transport":{
                  "protocol":[
                     "ietf-vpn-common:rsvp-te"
                  ]
               },
               "status":{
                  "admin-status":{
                     "status":"ietf-vpn-common:admin-up"
                  }
               },
               "vpn-nodes":{
                  "vpn-node":[
                     {
                        "vpn-node-id":"PW2060-tldp-single-instqnce-R3",
                        "description":"PW2060-tldp-single-instqnce",
                        "ne-id":"10.10.10.3",
                        "router-id":"10.10.10.3",
                        "status":{
                           "admin-status":{
                              "status":"ietf-vpn-common:admin-up"
                           }
                        },
                        "signaling-option":{
                           "signaling-type":"ietf-vpn-common:ldp-signaling",
                           "ldp-or-l2tp":{
                              "t-ldp-pw-type":"ietf-l2vpn-ntw:vpws-type",
```

```
            "pw-type":"ietf-l2vpn-ntw:ethernet",
            "ac-pw-list":[
               {
                  "peer-addr":"10.10.10.4",
                  "vc-id":"2060",
                  "pw-priority":1
               }
            ]
         }
      },
      "vpn-network-accesses":{
         "vpn-network-access":[
            {
               "id":"1",
               "interface-id":"Port 1/1/9",
               "status":{
                  "admin-status":{
                     "status":"ietf-vpn-common:admin-up"
                  }
               },
               "connection":{
                  "encapsulation":{
                     "encap-type":"ietf-vpn-common:dot1q",
                     "dot1q":{
                        "cvlan-id":2060
                     }
                  }
               },
               "service":{
                  "mtu":1492
               }
            }
         ]
      }
   },
   {
      "vpn-node-id":"PW2060-tldp-single-instqnce-R4",
      "ne-id":"10.10.10.4",
      "router-id":"10.10.10.4",
      "status":{
         "admin-status":{
            "status":"ietf-vpn-common:admin-up"
         }
      },
      "signaling-option":{
         "signaling-type":"ietf-vpn-common:ldp-signaling",
         "ldp-or-l2tp":{
            "t-ldp-pw-type":"ietf-l2vpn-ntw:vpws-type",
            "pw-type":"ietf-l2vpn-ntw:ethernet",
            "ac-pw-list":[
               {
                  "peer-addr":"10.10.10.3",
                  "vc-id":"2060",
                  "pw-priority":1
               }
            ]
         }
      },
      "vpn-network-accesses":{
         "vpn-network-access":[
            {
               "id":"1",
               "interface-id":"Port 1/1/9",
               "status":{
                  "admin-status":{
                     "status":"ietf-vpn-common:admin-up"
```

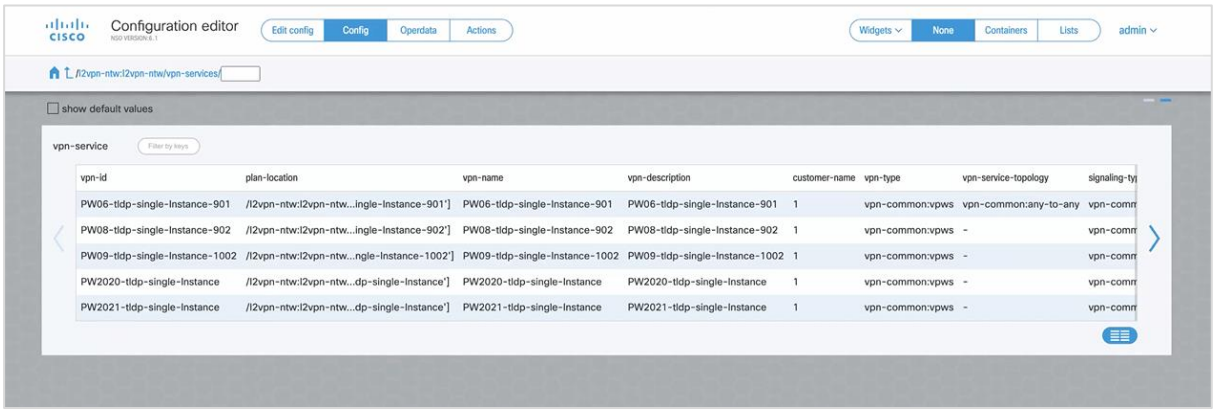
```
                                    }
                                },
                                "connection":{
                                    "encapsulation":{
                                        "encap-type":"ietf-vpn-common:dot1q",
                                        "dot1q":{
                                            "cvlan-id":2060
                                        }
                                    }
                                },
                                "service":{
                                    "mtu":1492
                                }
                            }
                        ]
                    }
                }
            ]
        }
    }
}
```


Configure Nokia NSP L2-VPN using NSO (UI)

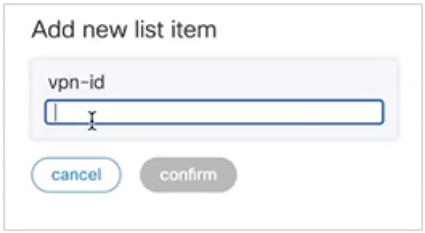
To add a Nokia NSP L2-VPN service, add two VPN nodes, each with their interface. This is useful for testing an L2-VPN service.

To add a Nokia NSP L2-VPN:

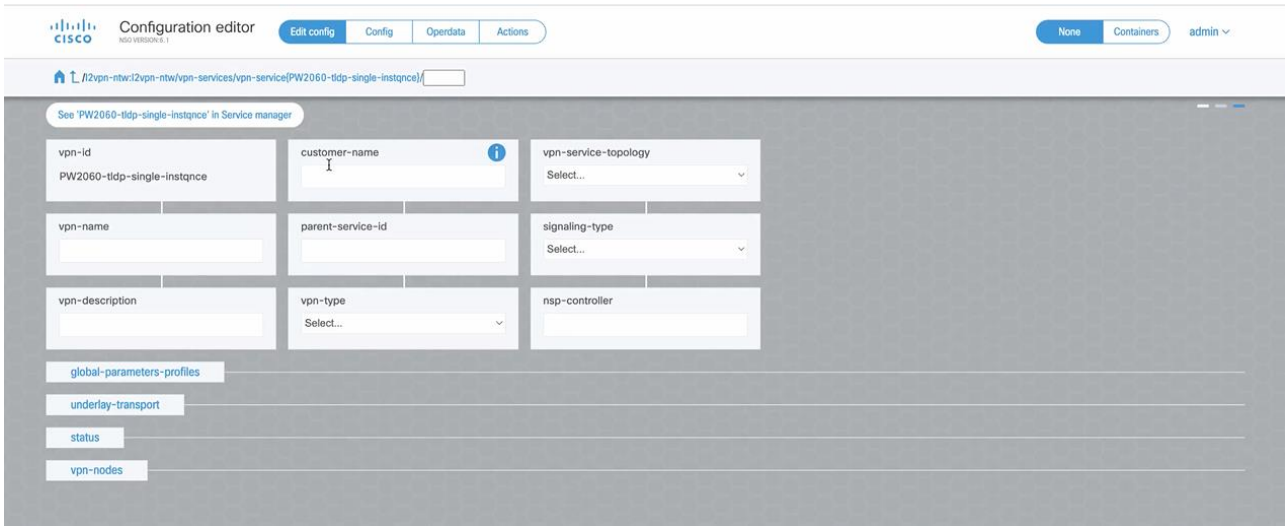
1. Launch NSO.
2. Click **l2vpn:ntw12vpn-ntw**.
3. Click **vpn-services**.



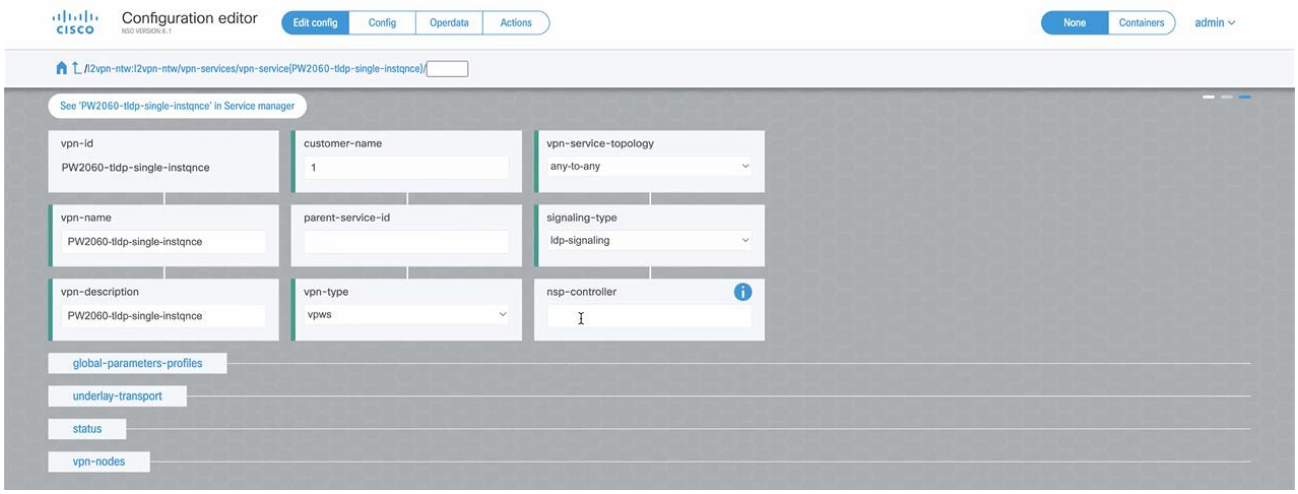
4. Click **+**.



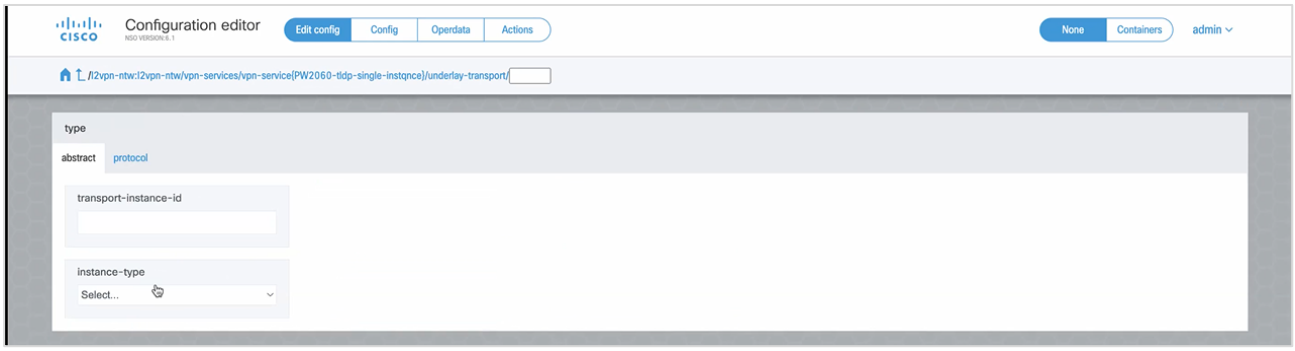
5. Enter a unique **vpn-id**, for example, **PW2060-tldp-single-instance**, and click **confirm**.
6. Click the **vpn service**.



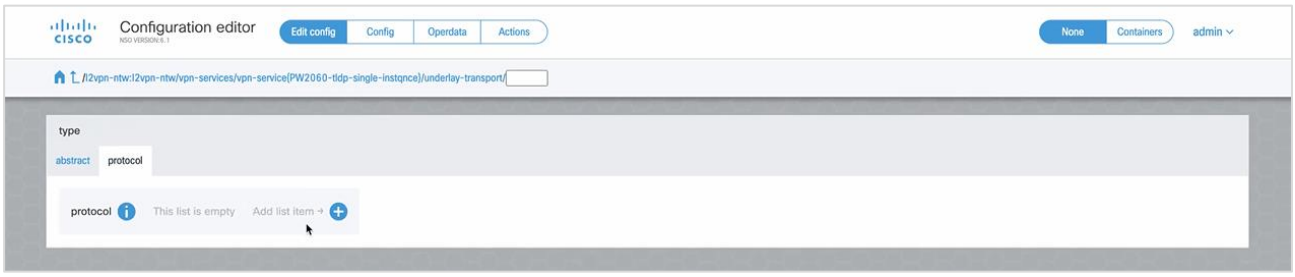
7. Enter the **customer-name** exactly as configured in the Nokia NSP controller (this is an integer and not a string).
8. Enter the **vpn-name** as a string.
9. Enter the **vpn-description** as a string.
10. Set the **vpn-type** to **vpws**.
11. Set the **vpn-service-topology** to **hub-spoke** or **any-to-any** or **hub-spoke-disjoint**.
12. Set the **signaling-type** to **idp-signaling**.
13. Select the **nsp-controller** (if there is a default nsp-controller, then you can skip this).



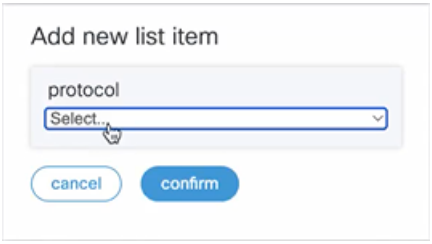
14. Click **underlay-transport**.



15. Click **protocol**.



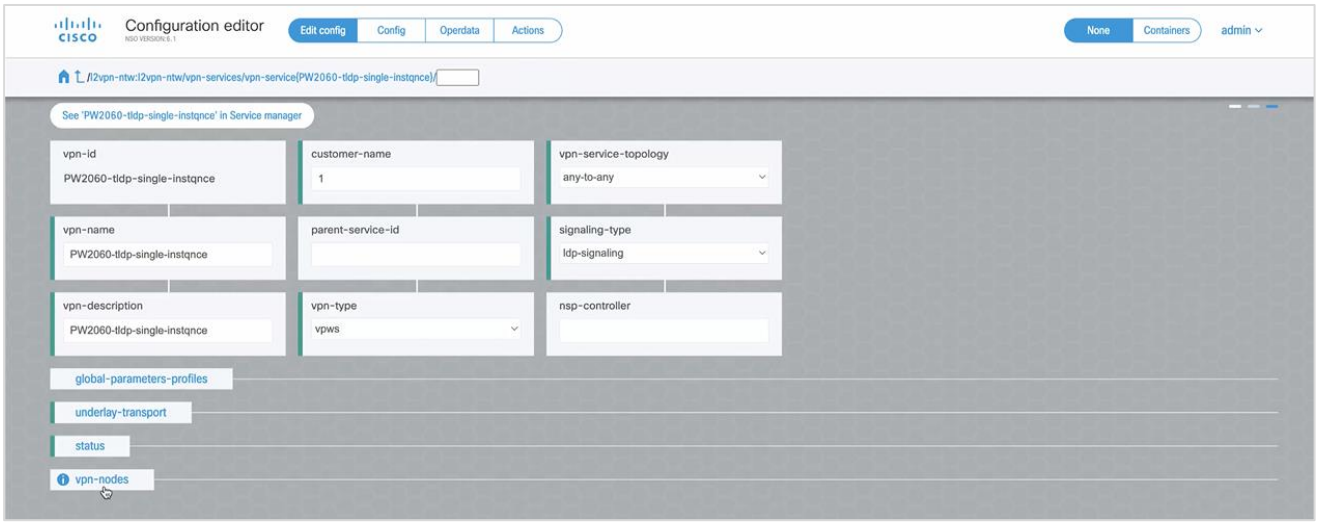
16. Click **+**.



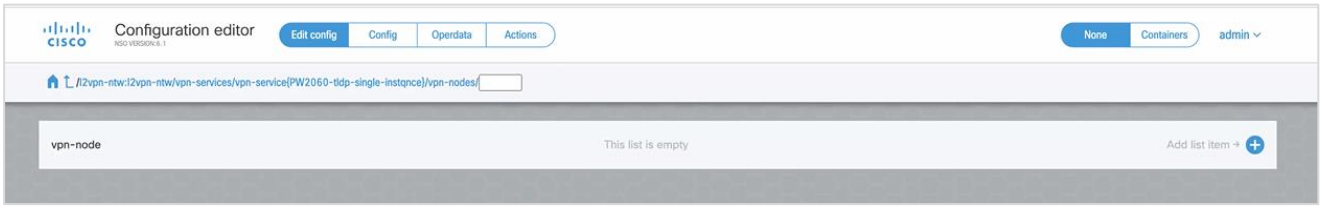
17. Select **rsvp-te** and click **confirm**.
18. Return to the vpn (using the breadcrumbs at the top of the page) and click **status**.

19. Click **admin-status**, and then set the **status** to **admin-up**.

20. Return to the vpn (using the breadcrumbs at the top of the page).

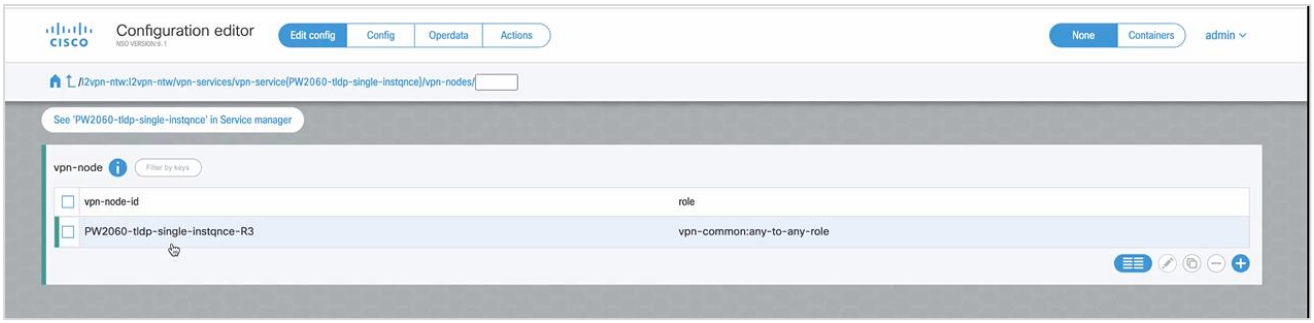


21. Click **vpn-nodes**.

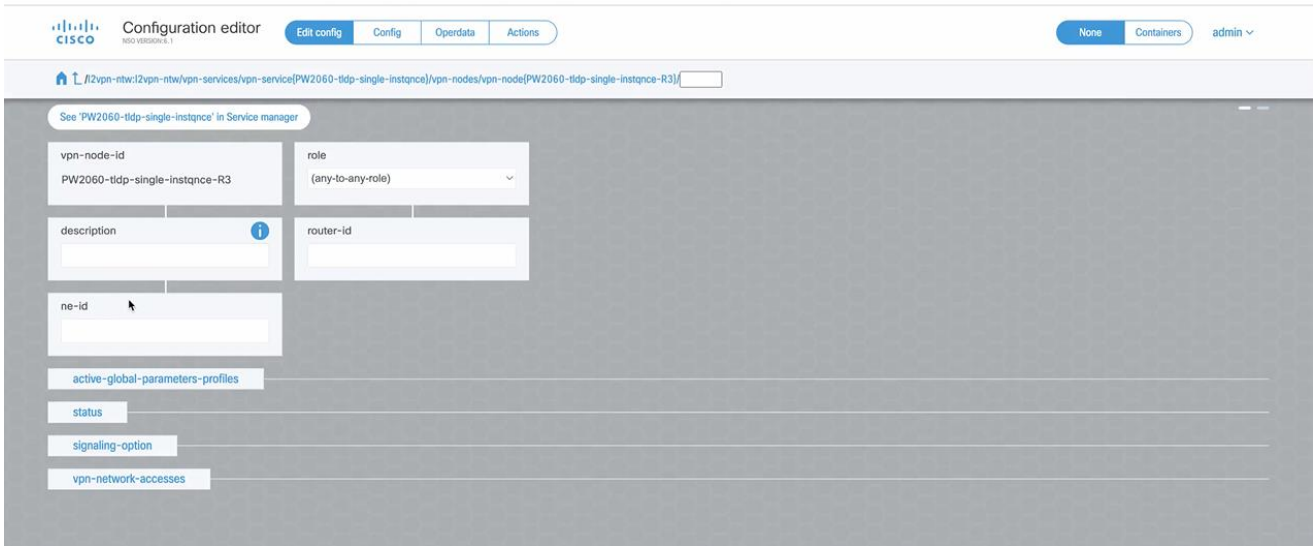


22. Click **+**.
23. Use the vpn-id and add **-R3** as a suffix (when you configure the second node use **-R4**).

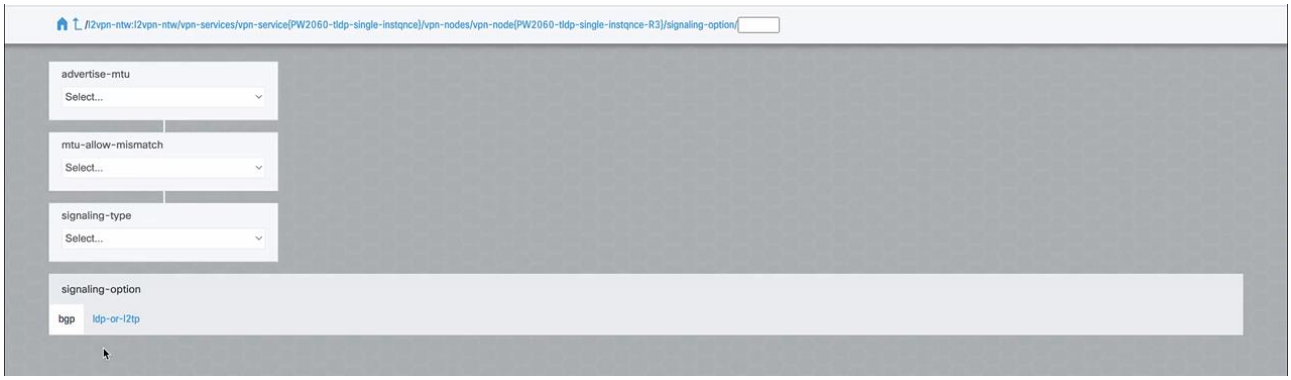
24. Click **confirm**.



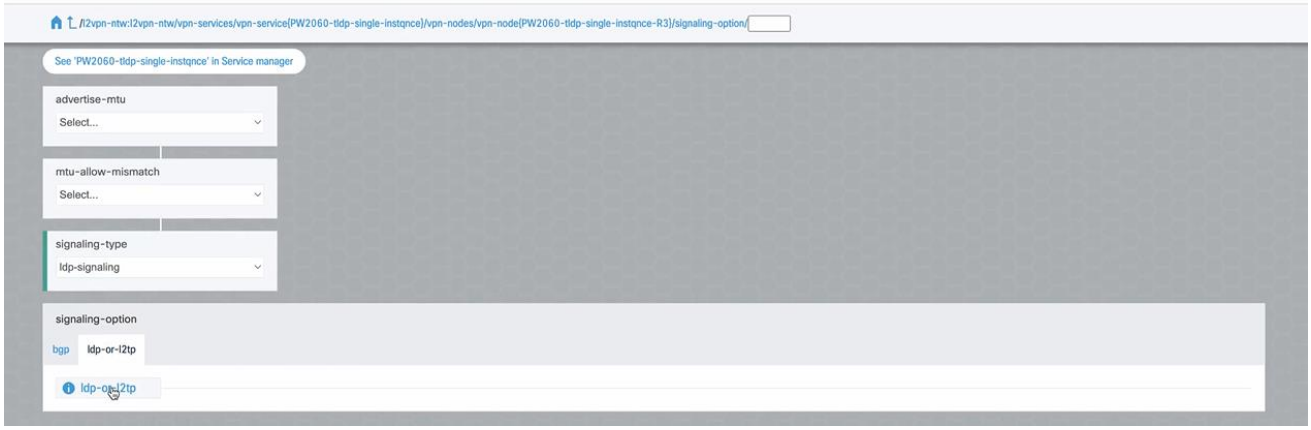
25. Click on the vpn-node.



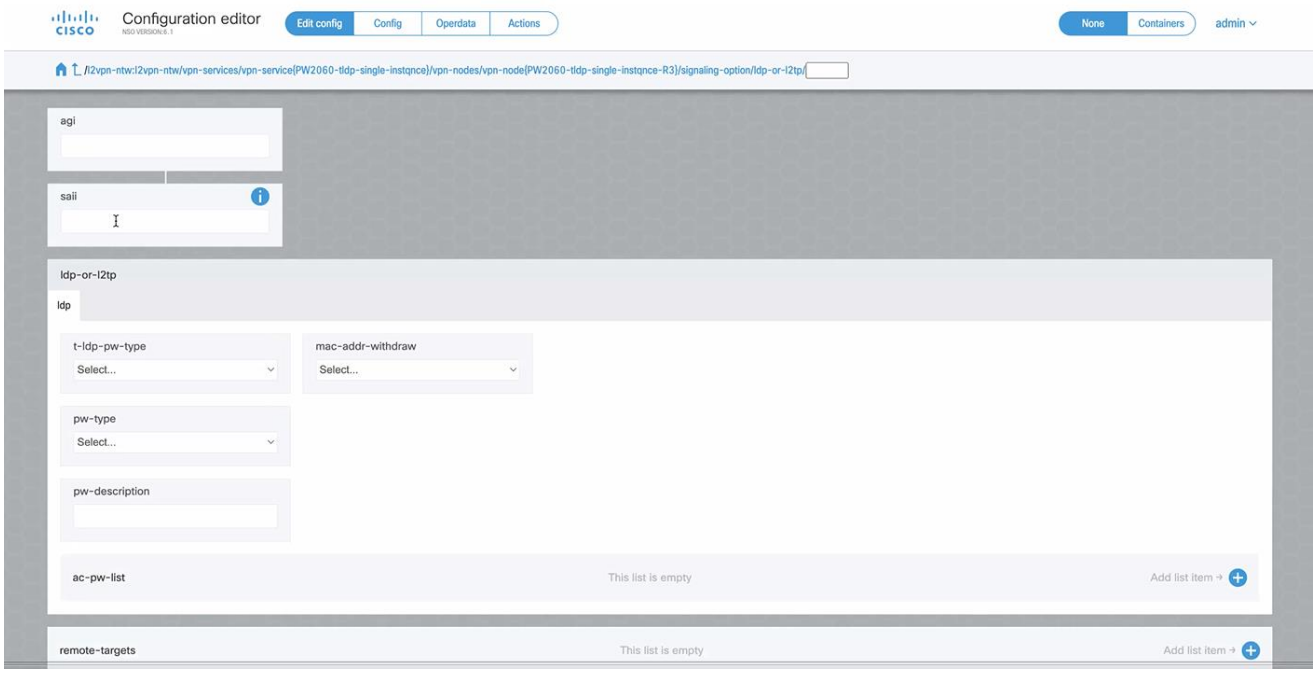
26. Enter a **description**.
27. Specify the **router-id** and the **ne-id**.
28. Click **status**. And as done previously, set this to **admin-up**.
29. In the vpn-node, click **signaling-option**.



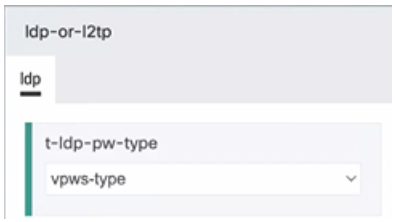
30. Click **signaling-type** and select **ldp-signaling**.



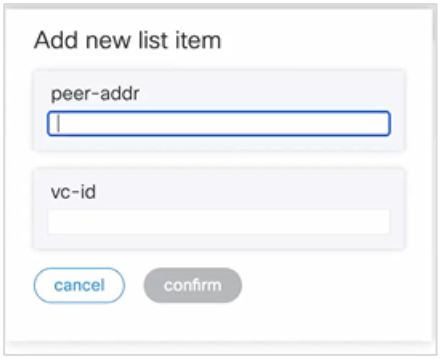
31. Select the **ldp-or-l2tp** tab and then click **ldp-or-l2tp**.



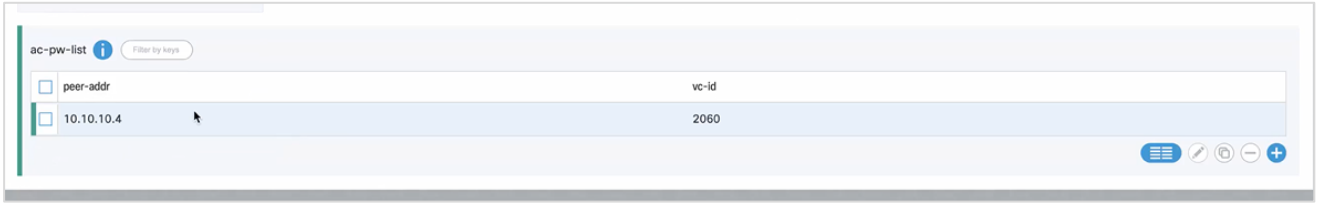
32. Click **t-ldp-pw-type** and select **vpws-type**.



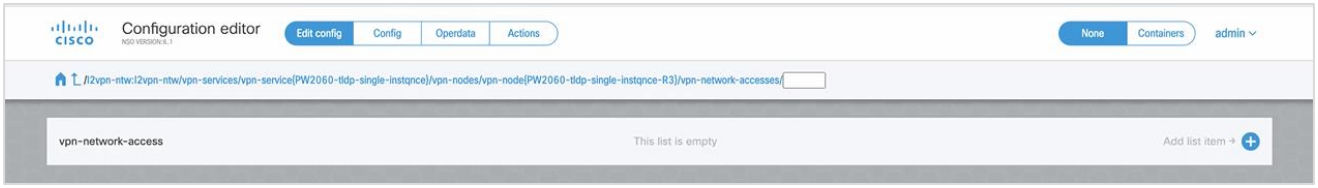
33. Click **pw-type** and select **ethernet**.
34. In the **ac-pw-list**, click **+**.



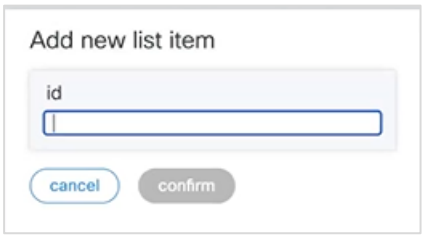
35. Enter a **peer-addr** (of the router).
36. Enter the **vc-id**, for example, **2060**, and click **confirm**.



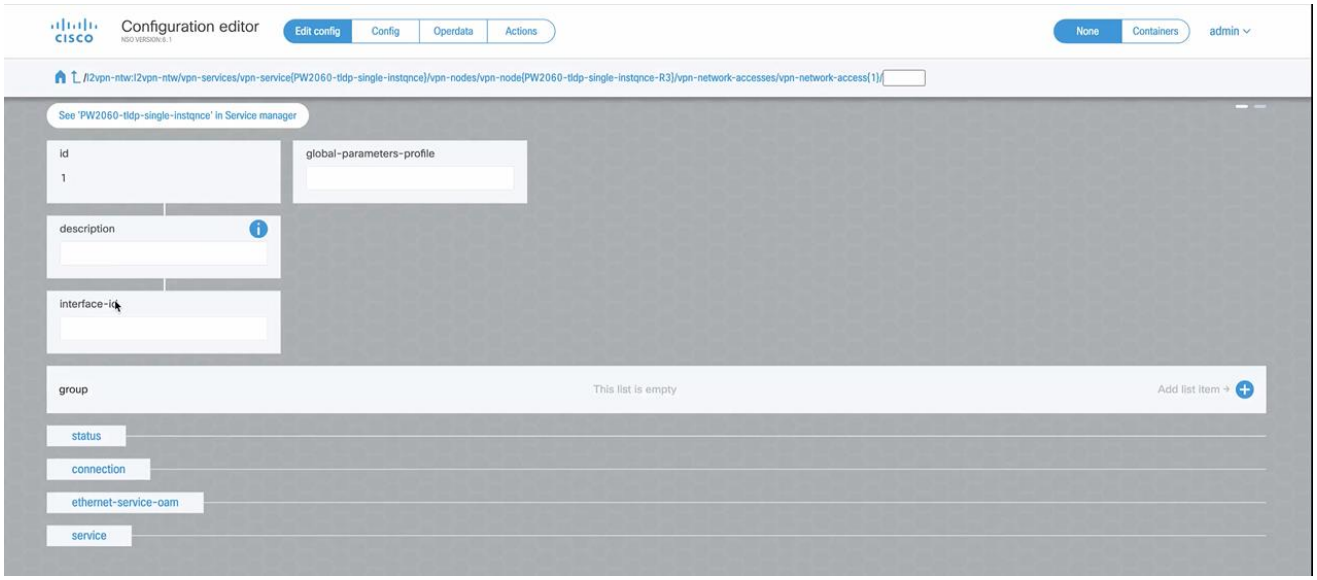
37. Navigate back to the vpn-node page and click **vpn-network-accesses**.



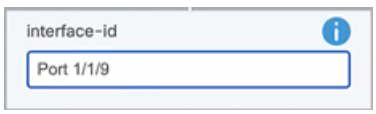
38. Click +. This defines the interfaces participating in the VPN.



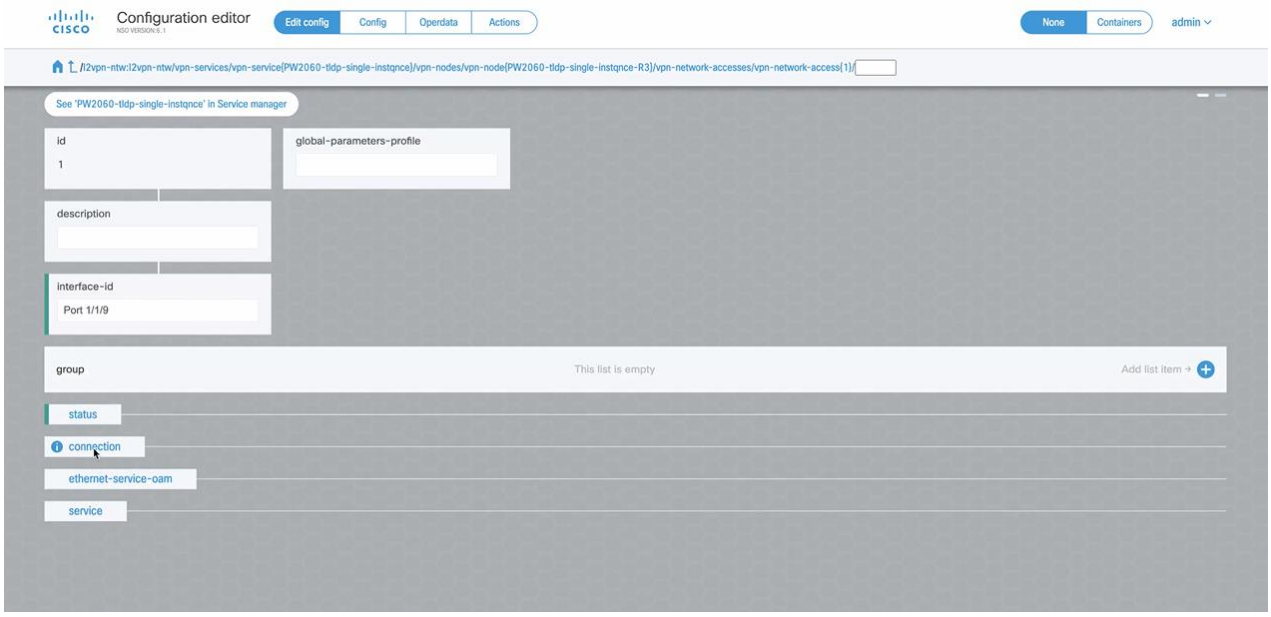
39. Specify the interface **id** and click **confirm**. This is in the format **int_<number>**, for example, **int_222_1**. In this example it is set to 1.
40. Click on the interface.



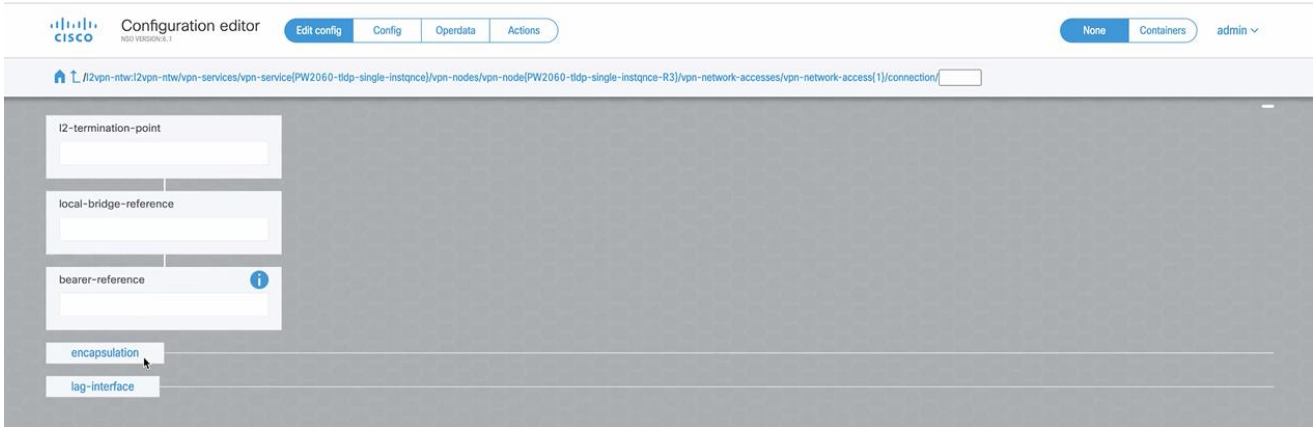
41. Enter the **interface_id** as **Port 1/1/9** (this is the access port and may vary according to the router).



42. Enter the **description** as a string.
43. Click **status**.
44. Click **admin-status**, and then set the **status** to **admin-up**.
45. Navigate back to the interface page.

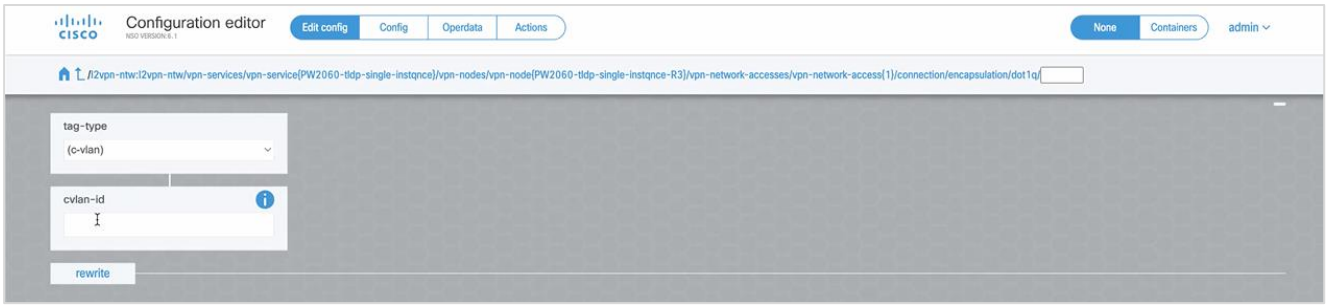


46. Click **Connection**.

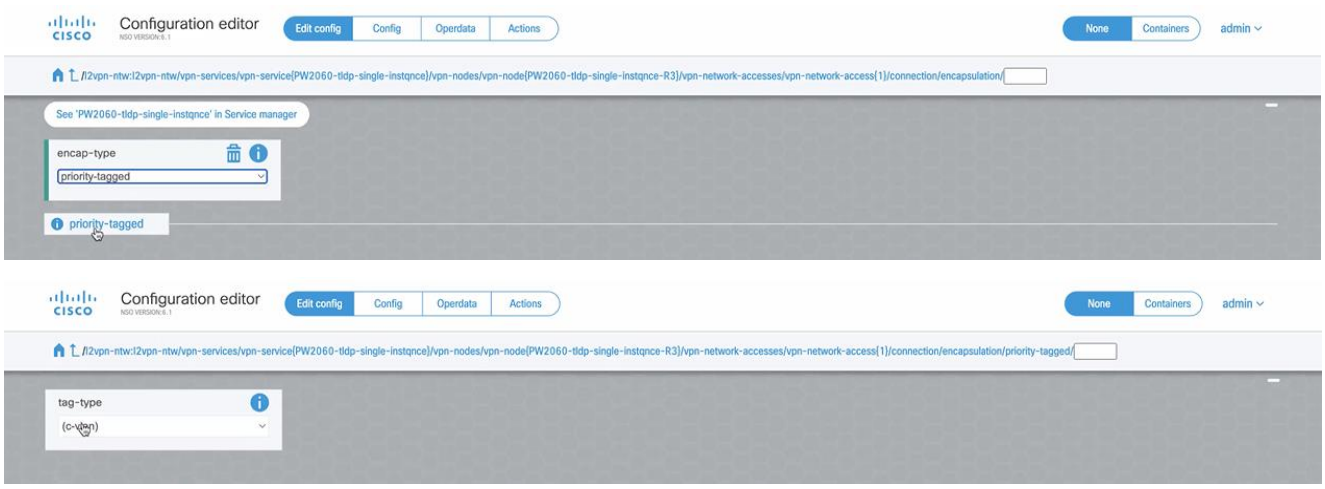


47. Click **encapsulation**.

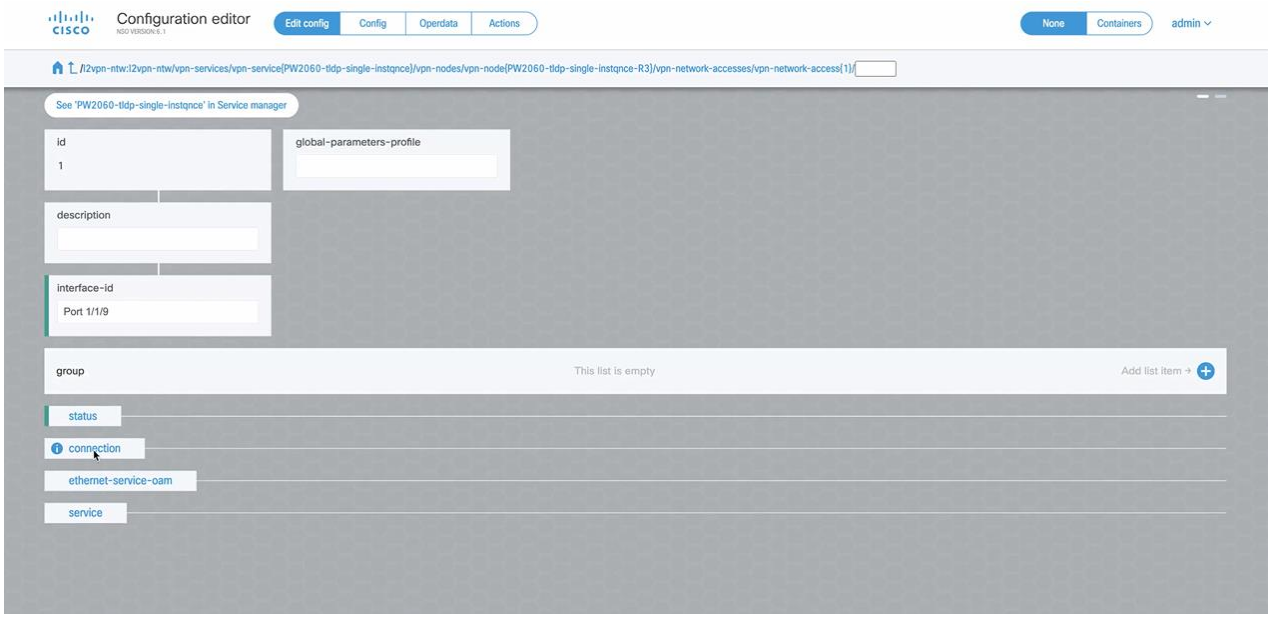
48. Set the **encap-type** to **dot1q**.
49. Click **dot1q**.



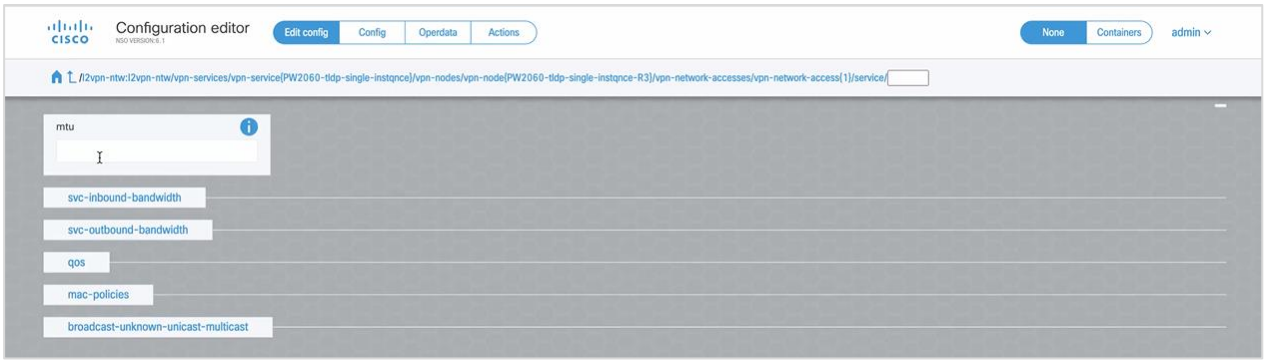
50. Enter the **cvlan-id**.
51. Alternatively, you can set the **encap-type** to **priority-tagged**, and then click priority-tagged and select the tag-type (**c-vlan**).



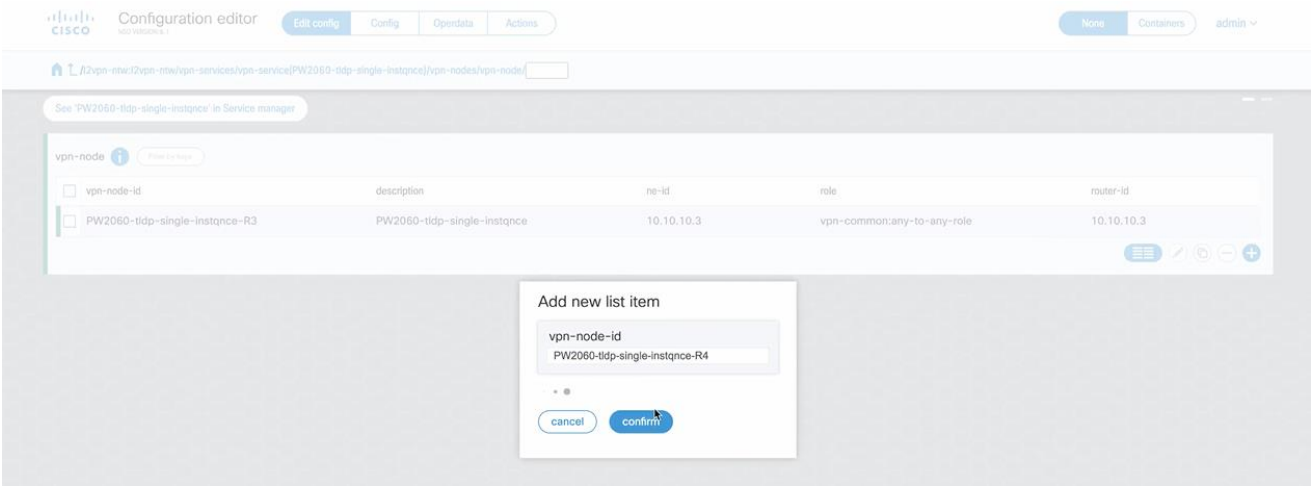
52. Navigate back to the interface page.



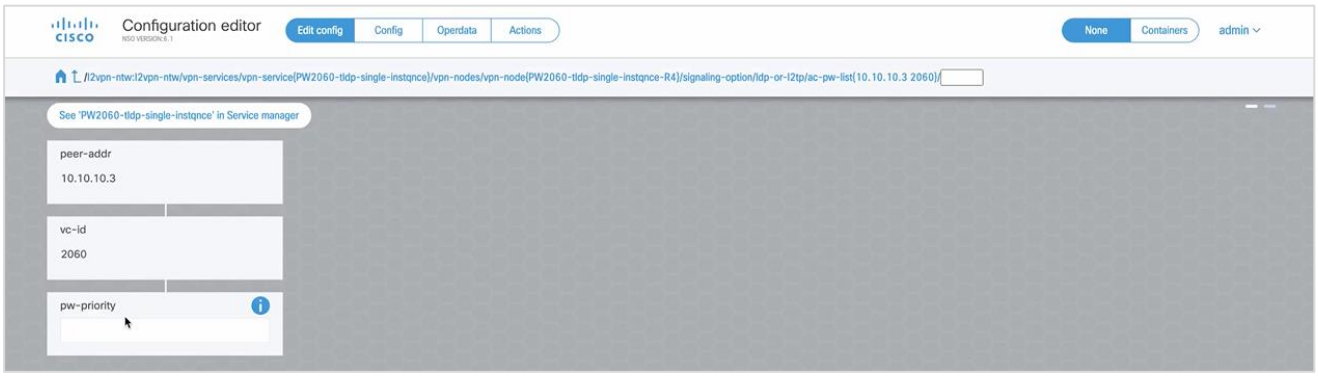
53. Click **ethernet-service-oam**.



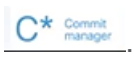
54. Enter the **mtu**.
55. Navigate back to the VPN service page.
56. Add another **vpn-node** following the process previously described, adding the suffix -R4 to the name.



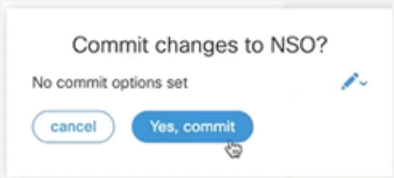
57. Follow the procedure above, but when you specify the **peer-addr**, you should also specify the **pw-priority**.



58. Once you have finished setting up the second vpn node, click Commit Manager (at the bottom of the screen).



59. Review the configuration.
60. Click **Commit**.



61. Click **Yes, commit**.
62. Once it has finished, check the VPN.

Configure Cisco Crosswork Network Controller L2-VPN using NSO (JSON)

For full details on Cisco Crosswork Network Controller L2-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide* for instructions how to onboard the controller as a device to the NSO device tree and how to deploy the L2-VPN service on a default Cisco Crosswork Network Controller.

The L2-VPN JSON requires the following high-level structure.

```
{
   "l2vpn-ntw":{
      "vpn-services":{
         "vpn-service":[
               "vpn-id":"alpha",
               "vpn-type":"vpn-common:vpws-evpn",
               "vpn-nodes":{}
         ]
      }
   }
}
```

The example below is provided as an L2-VPN configuration example.

Table 7. Cisco Crosswork Network Controller L2-VPN Parameters

Parameter	Description
vpn-service	
vpn-id	The VPN ID.
vpn-type	The VPN type: **vpn-common:vpws-evpn**.
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID.
vpn-network-accesses	
vpn-network-access	
id	The VPN network access ID in the format **<number>**, for example, 3501.
interface-id	The VPN network access interface ID, for example, **GigabitEthernet0/0/0/4**. This is the access port and may change according to the router.
connection	

Parameter	Description
encapsulation	
encap-type	The connection encapsulation type: **vpn-common:dot1q** (VLAN).
dot1q/priority-tagged cvlan-id	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 555.
tag-operations	
tag-1	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 555.

Example

```
<config xmlns="http://tail-f.com/ns/config/1.0">
  <l2vpn-ntw xmlns="urn:ietf:params:xml:ns:yang:ietf-l2vpn-ntw">
    <vpn-services>
      <vpn-service>
        <vpn-id>alpha</vpn-id>
        <vpn-type>vpn-common:vpws-evpn</vpn-type>
        <vpn-nodes>
          <vpn-node>
            <vpn-node-id>PE-A</vpn-node-id>
            <vpn-network-accesses>
              <vpn-network-access>
                <id>3501</id>
                <interface-id>GigabitEthernet0/0/0/4</interface-id>
                <connection>
                  <encapsulation>
                    <encap-type>vpn-common:dot1q</encap-type>
                    <dot1q>
                      <cvlan-id>555</cvlan-id>
                      <tag-operations>
                        <push/>
                        <tag-1>555</tag-1>
                        <!-- <mode xmlns="http://cisco.com/ns/nso/fp/examples/cisco-l2vpn-
ntw">symmetric</mode> -->
                      </tag-operations>
                    </dot1q>
                  </encapsulation>
                </connection>
              </vpn-network-access>
            </vpn-network-accesses>
          </vpn-node>
          <vpn-node>
            <vpn-node-id>PE-B</vpn-node-id>
            <vpn-network-accesses>
              <vpn-network-access>
                <id>3501</id>
                <interface-id>GigabitEthernet0/0/0/4</interface-id>
                <connection>
                  <encapsulation>
                    <encap-type>vpn-common:dot1q</encap-type>
                    <dot1q>
                      <cvlan-id>556</cvlan-id>
                      <tag-operations>
                        <push/>
                        <tag-1>556</tag-1>
                        <!-- <mode xmlns="http://cisco.com/ns/nso/fp/examples/cisco-l2vpn-
ntw">symmetric</mode> -->
                      </tag-operations>
                    </dot1q>
```

```
                </encapsulation>
              </connection>
            </vpn-network-access>
          </vpn-network-accesses>
        </vpn-node>
      </vpn-nodes>
    </vpn-service>
  </vpn-services>
 </l2vpn-ntw>
</config>
```

Configure Cisco Crosswork Network Controller L3-VPN using NSO (JSON)

For full details on Cisco Crosswork Network Controller L3-VPN service provisioning using NSO, see the *Cisco NSO Crosswork Hierarchical Controller - Function Pack User Guide* for instructions how to onboard the controller as a device to the NSO device tree and how to deploy the L3-VPN service on a default Cisco Crosswork Network Controller.

The example below is provided as an L3-VPN configuration example.

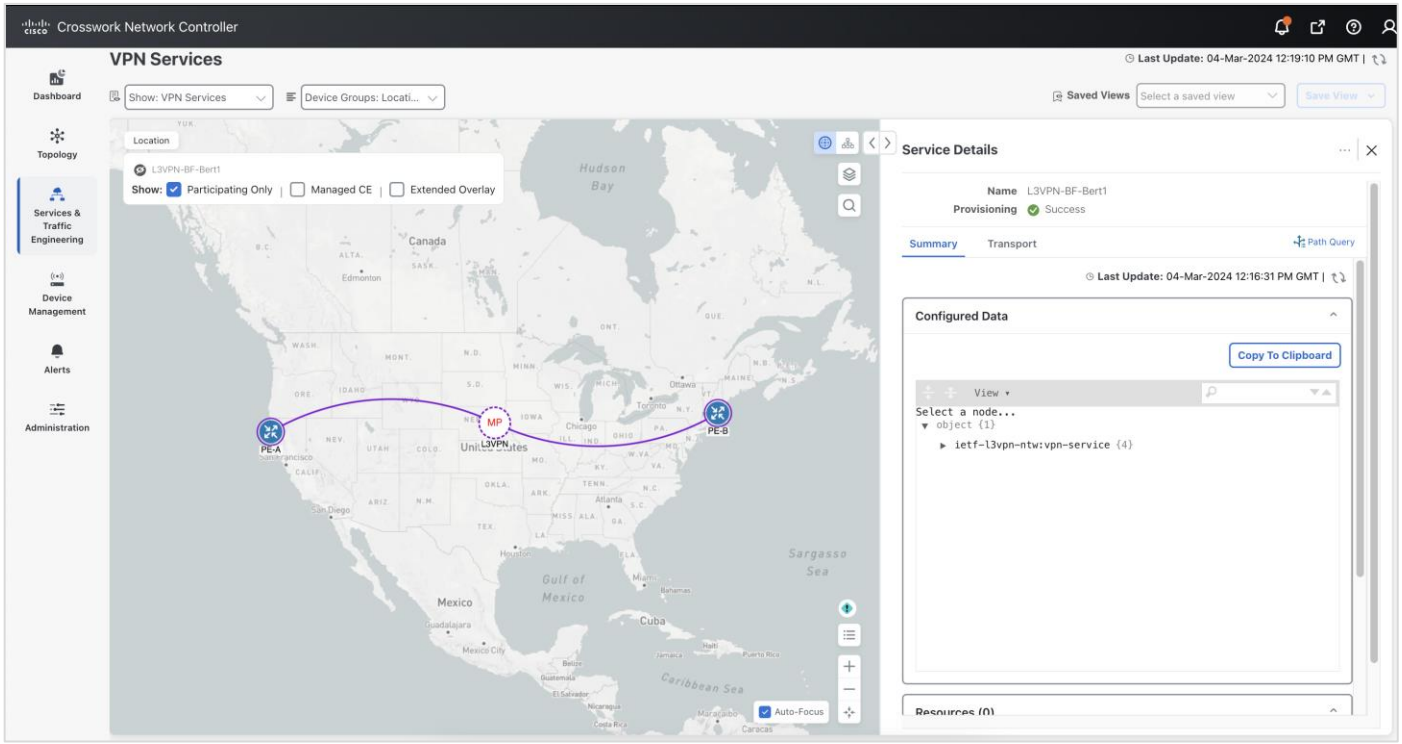


Table 8. Cisco Crosswork Network Controller L3-VPN Parameters

Parameter	Description
vpn-service	
vpn-id	The VPN ID, for example, PE-A.
vpn-nodes	
vpn-node	
vpn-node-id	The VPN node ID.

Parameter	Description
vpn-network-accesses	
vpn-network-access	
id	The VPN network access ID in the format **<number>**, for example, 1.
connection **encapsulation**	
type	The connection encapsulation type: **vpn-common:dot1q** (VLAN).
dot1q cvlan-id	The CVLAN ID (circuit ID) for the dot1q encapsulation, for example, 1777.
interface-id	The VPN network access interface ID, for example, **GigabitEthernet0/0/0/4**. This is the access port and may change according to the router.
ip-connection **ipv4**	
local-address	The IP connection local address.
prefix-length	The IP connection prefix length.
active-vpn-instance-profiles	
vpn-instance-profile profile-id	THE VPN instance profile.
vpn-service-topology	ietf-vpn-common:any-to-any
vpn-instance-profiles **vpn-instance-profile** rd	The profile ID.
profile-id	
address-family **vpn-targets** **vpn-target** id	The VPN target ID.
route-target-type	The route target type, for example, both.
address-family	

JSON Example

```
{
   "ietf-l3vpn-ntw:vpn-service":{
      "vpn-id":"L3VPN-BF-Alpha1",
      "vpn-nodes":{
         "vpn-node":[
            {
```

```
            "vpn-node-id":"PE-A",
            "vpn-network-accesses":{
               "vpn-network-access":[
                  {
                     "id":"1",
                     "connection":{
                        "encapsulation":{
                           "type":"ietf-vpn-common:dot1q",
                           "dot1q":{
                              "cvlan-id":1777
                           }
                        }
                     },
                     "interface-id":"GigabitEthernet0/0/0/5",
                     "ip-connection":{
                        "ipv4":{
                           "local-address":"194.195.196.1",
                           "prefix-length":24
                        }
                     }
                  }
               ]
            },
            "active-vpn-instance-profiles":{
               "vpn-instance-profile":[
                  {
                     "profile-id":"any"
                  }
               ]
            }
         },
         {
            "vpn-node-id":"PE-B",
            "vpn-network-accesses":{
               "vpn-network-access":[
                  {
                     "id":"1",
                     "connection":{
                        "encapsulation":{
                           "type":"ietf-vpn-common:dot1q",
                           "dot1q":{
                              "cvlan-id":1777
                           }
                        }
                     },
                     "interface-id":"GigabitEthernet0/0/0/5",
                     "ip-connection":{
                        "ipv4":{
                           "local-address":"194.195.196.2",
                           "prefix-length":24
                        }
                     }
                  }
               ]
            },
            "active-vpn-instance-profiles":{
               "vpn-instance-profile":[
                  {
                     "profile-id":"any"
                  }
               ]
            }
         }
      ]
   },
   "vpn-service-topology":"ietf-vpn-common:any-to-any",
```

```
      "vpn-instance-profiles":{
         "vpn-instance-profile":[
            {
               "rd":"0:55:65",
               "profile-id":"any",
               "address-family":[
                  {
                     "vpn-targets":{
                        "vpn-target":[
                           {
                              "id":1,
                              "route-target-type":"both"
                           }
                        ]
                     },
                     "address-family":"ietf-vpn-common:ipv4"
                  }
               ]
            }
         ]
      }
   }
}
```

Comparison of L3-VPN Parameters for Nokia NSP and Cisco Crosswork Network Controller

The following table lists the parameters shared by Nokia NSP and Cisco Crosswork Network Controller L3-VPN. This list includes the most common parameters used and tested in the examples detailed in this guide. For the full schema, refer to the Network Services Orchestrator (NSO) Crosswork Hierarchical Controller - Function Pack documentation.

Table 9. L3-VPN Parameters

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
vpn-service	**vpn-service**	**vpn-service**
vpn-id	vpn-id	vpn-id
vpn-name	vpn-name	vpn-name
vpn-description	vpn-description	vpn-description
customer-name	customer-name	customer-name
	vpn-type	
vpn-service-topology	vpn-service-topology	vpn-service-topology
	status	
	admin-status	
	status	
vpn-instance-profiles	**vpn-instance-profiles**	**vpn-instance-profiles**
vpn-instance-profile	**vpn-instance-profile**	**vpn-instance-profile**

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
profile-id	profile-id	profile-id
role	role	role
rd	rd	rd
address-family	**address-family**	**address-family**
address-family	address-family	address-family
vpn-targets	**vpn-targets**	**vpn-targets**
	vpn-policies	
	import-policy	
	export-policy	
	underlay-transport	
	protocol	
vpn-target	**vpn-target**	**vpn-target**
id	id	id
route-targets	**route-targets**	**route-targets**
route-targets	**route-targets**	**route-targets**
route-target-type	route-target-type	route-target-type
vpn-nodes	**vpn-nodes**	**vpn-nodes**
vpn-node	**vpn-node**	**vpn-node**
vpn-node-id	vpn-node-id	vpn-node-id
local-as	local-as	local-as
	description	
	ne-id	
	router-id	
active-vpn-instance-profiles	**active-vpn-instance-profiles**	**active-vpn-instance-profiles**
vpn-instance-profile	**vpn-instance-profile**	**vpn-instance-profile**
profile-id	profile-id	profile-id
	status	

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
	admin-status	
	status	
vpn-network-accesses	**vpn-network-accesses**	**vpn-network-accesses**
vpn-network-access	**vpn-network-access**	**vpn-network-access**
id	id	id
interface-id	interface-id	interface-id
	description	
	vpn-instance-profile	
	status	
	admin-status	
	status	
connection	**connection**	**connection**
encapsulation	**encapsulation**	**encapsulation**
type	type	type
dot1q	**dot1q**	**dot1q**
tag-type	tag-type	tag-type
cvlan-id	cvlan-id	cvlan-id
		interface-id
ip-connection	**ip-connection**	**ip-connection**
ipv4	**ipv4**	**ipv4**
local-address	local-address	local-address
prefix-length	prefix-length	prefix-length
routing-protocols	**routing-protocols**	**routing-protocols**
routing-protocol	**routing-protocol**	**routing-protocol**
id	id	id
type	type	type
peer-as	peer-as	peer-as

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
address-family	address-family	address-family
neighbor	neighbor	neighbor
multihop	multihop	multihop
redistribute-connected	**redistribute-connected**	**redistribute-connected**
address-family	address-family	address-family

Comparison of L2-VPN Parameters for Nokia NSP and Cisco Crosswork Network Controller

The following table lists the parameters shared by Nokia NSP and Cisco Crosswork Network Controller L2-VPN. This list includes the most common parameters used and tested in the examples detailed in this guide. For the full schema, refer to the Network Services Orchestrator (NSO) Crosswork Hierarchical Controller - Function Pack documentation.

Table 10. L2-VPN Parameters

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
vpn-services	**vpn-services**	**vpn-services**
vpn-service	**vpn-service**	**vpn-service**
vpn-id	vpn-id	vpn-id
vpn-name	vpn-name	vpn-name
vpn-description	vpn-description	vpn-description
customer-name	customer-name	customer-name
vpn-type	vpn-type	vpn-type
vpn-service-topology	vpn-service-topology	vpn-service-topology
	signaling-type	
global-parameters-profiles	**global-parameters-profiles**	
global-parameters-profile	**global-parameters-profile**	
profile-id	profile-id	
vpn-target	**vpn-target**	
id	id	
route-targets	**route-targets**	

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
route-target	route-targets	
route-target-type	route-target-type	
	underlay-transport	
	protocol	
status	**status**	**status**
admin-status	**admin-status**	**admin-status**
status	status	status
vpn-nodes	**vpn-nodes**	**vpn-nodes**
vpn-node	**vpn-node**	**vpn-node**
vpn-node-id	vpn-node-id	vpn-node-id
	description	
	ne-id	
role	role	role
	router-id	
	status	
	admin-status	
	status	
signaling-option	**signaling-option**	**signaling-option**
evpn-policies	**evpn-policies**	**evpn-policies**
mac-learning-mode	mac-learning-mode	mac-learning-mode
	signaling-type	
	ldp-or-l2tp	
	t-ldp-pw-type	
	pw-type	
	ac-pw-list	
	peer-addr	
	vc-id	

Common L3-VPN	Nokia NSP L3-VPN	Cisco Crosswork Network Controller L3-VPN
	pw-priority	
vpn-network-accesses	**vpn-network-accesses**	**vpn-network-accesses**
vpn-network-access	**vpn-network-access**	**vpn-network-access**
id	id	id
interface-id	interface-id	interface-id
	status	
	admin-status	
	status	
connection	**connection**	**connection**
encapsulation	**encapsulation**	**encapsulation**
encap-type	encap-type	encap-type
dot1q	**dot1q**	**dot1q**
cvlan-id	cvlan-id	cvlan-id
	priority-tagged	
tag-operations	**tag-operations**	**tag-operations**
push	push	push
tag-1	tag-1	tag-1
cisco-hco-nm:hco-controller		
service	**Service**	**service**
mtu	Mtu	mtu

Configure L2-VPN/L3-VPN via API

The API endpoint for provisioning L2-VPN and L3-VPN services using the Network Services Orchestrator Crosswork Hierarchical Controller - Function Pack is defined as:

- https://x.x.x.x:8443/nso/restconf/data

To execute the L3-VPN API from Postman:

- https://xx.x.x.x:8443/nso/restconf/data/ietf-l3vpn-ntw:l3vpn-ntw/vpn-services/

To execute the L2-VPN API from Postman:

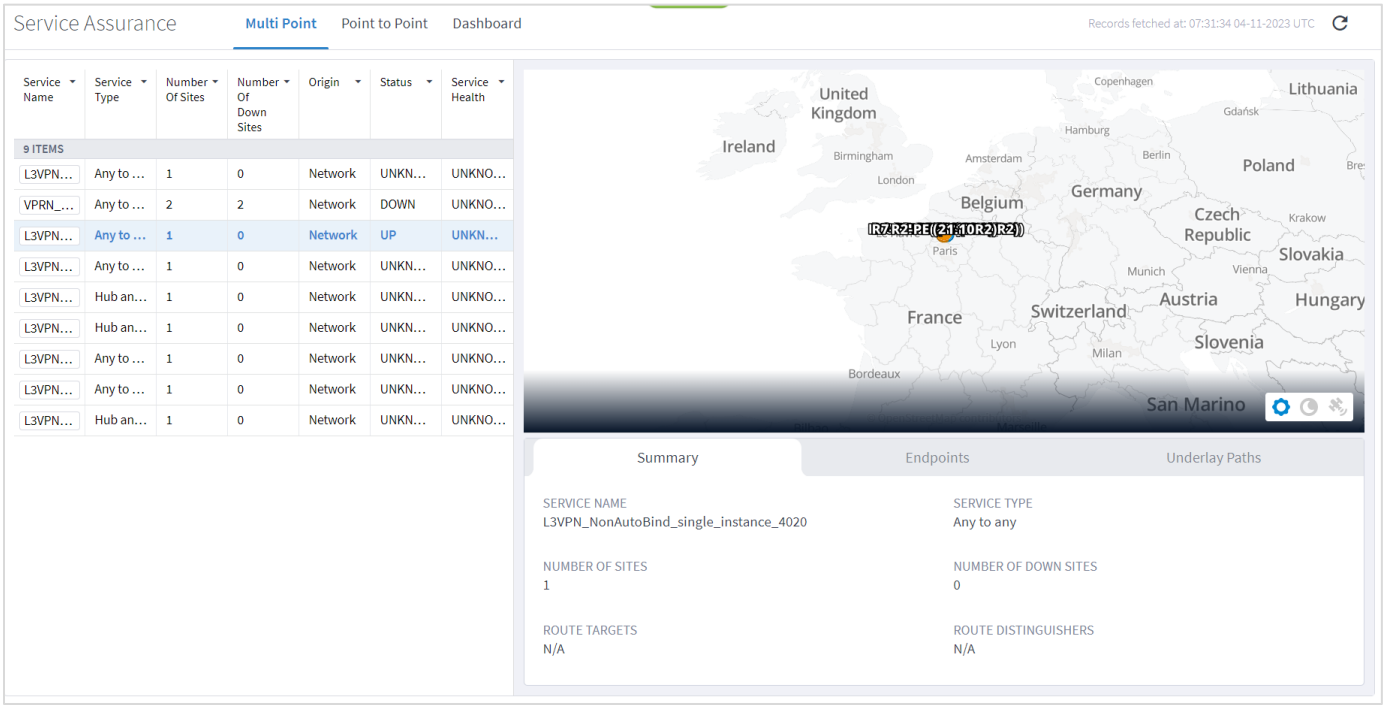
- https://xx.x.x.x:8443/nso/restconf/data/ietf-l2vpn-ntw:l2vpn-ntw/vpn-services/

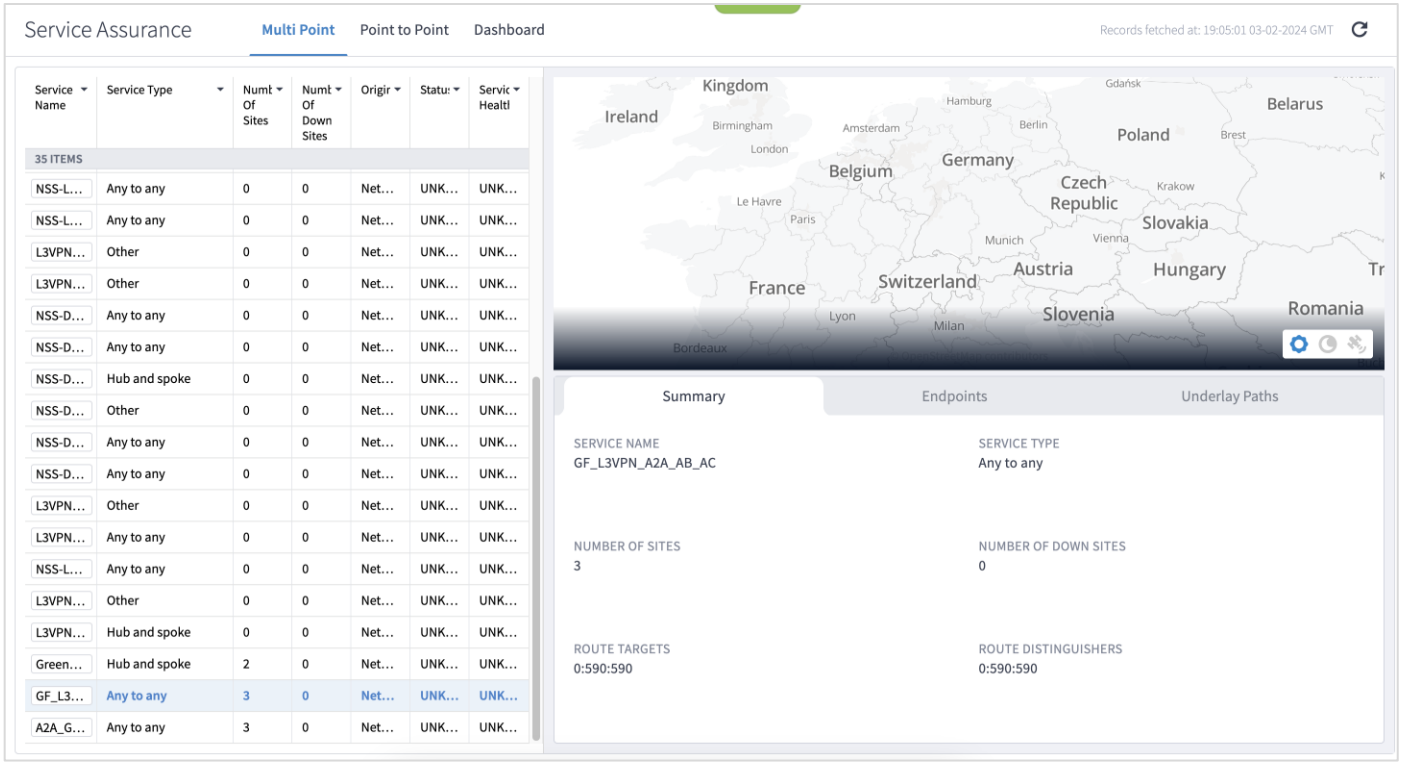
View L2-VPN and L3-VPN in Service Assurance

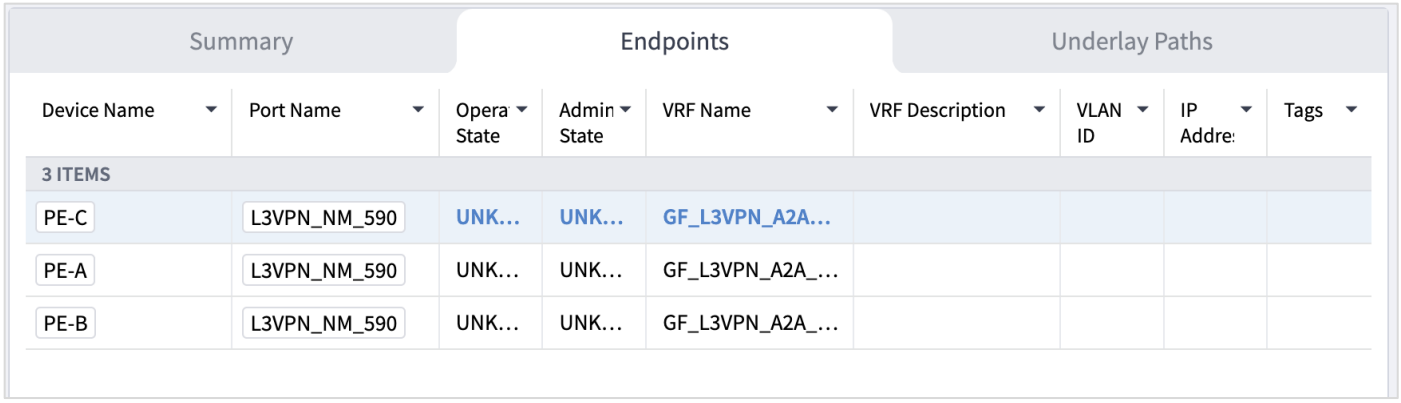
The services provisioned using NSO can be viewed in the Service Assurance application.

The services typically take the following period to be provisioned and appear in Crosswork Hierarchical Controller:

- **NSP:** Between 10 seconds and 3 minutes.
- **Cisco Crosswork Network Controller:** Between 30 seconds and 2 minutes.







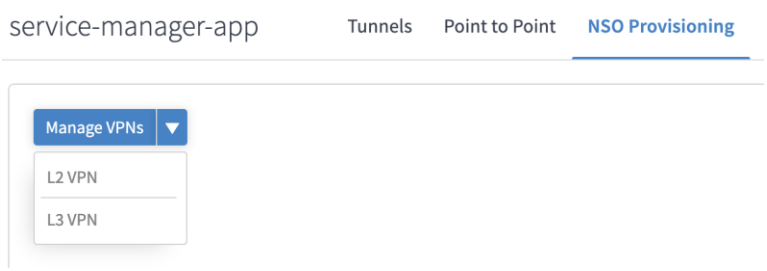
NSO Provisioning

You can view L2-VPNs and L3-VPNs provisioning tools. To access the NSO Web UI, configure the **NSO Address** in the **Service Settings**.

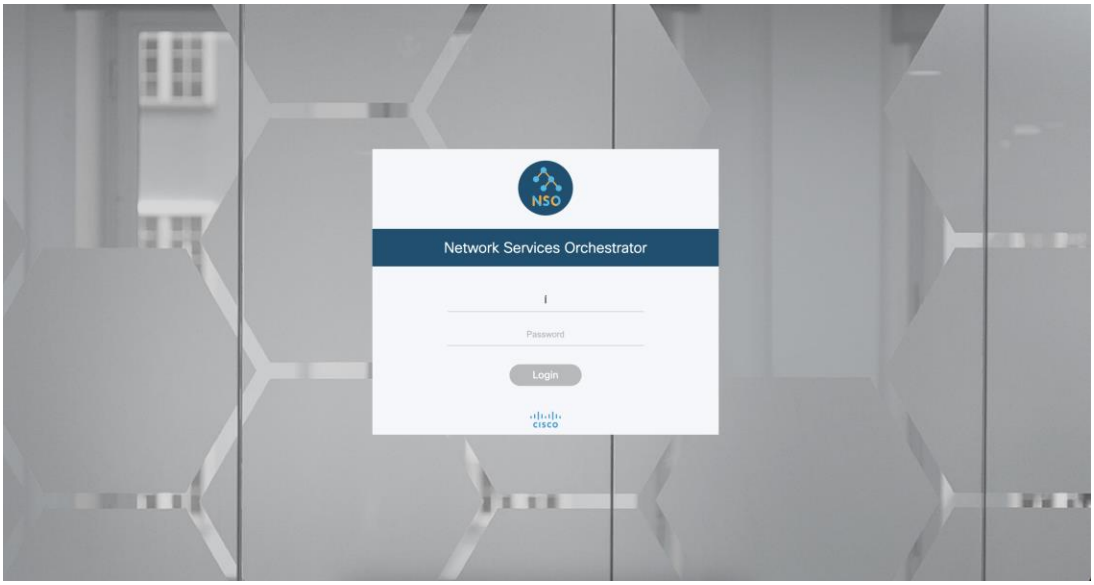
View L2 VPN/L3 VPN

To view L2 VPN/L3 VPN:

1. In the applications bar in Crosswork Hierarchical Controller, select **Service Manager > NSO Provisioning**.



2. Select **Manage VPNs**.
3. Select **L2 VPN** or **L3 VPN**.
4. The log in to the server configured in the Service Settings appears.



NSO APIs

NSO implements RESTConf standards and its core is Netconf. Any additional module loaded will have CRUD functionality via API based on the model. See:

https://developer.cisco.com/docs/nso/api-reference/

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **https://www.cisco.com/go/offices**.

Printed in USA 7/24