NOKIA

NSP
Network Services Platform
Release 20.3

Service Fulfillment Application Help

3HE-16070-AAAA-TQZZA

Issue 1

March 2020

Legal notice

Contents

1 Service Fulfillment

1.1 Why use Service Fulfillment?

The Service Fulfillment application allows for multi-vendor service provisioning and activation across all networks accessible to the NSD. It authorizes northbound interface (NBI) service requests, executes routing algorithms that allocate network resources for these services, and then deploys the services to the network. Network deployment is performed through the mediation framework. The Service Fulfillment application can use existing tunnels or create new tunnels to satisfy service demands. The services that can be provisioned from the Service Fulfillment application are L3 VPN, C-Line, E-LAN, E-Line and IES services.

The Service Fulfillment application also provides an abstract, real-time view of the network resources that can be consumed by services, allowing service providers and end users to interact with the network through simple APIs, and to programmatically control the network. Network abstraction is used to simplify how the network appears to the IT/OSS layer. This allows services to be defined and enhanced more quickly by presenting only the subset of network services and endpoints that are relevant to a specific application, thereby greatly reducing the complexity the application is exposed to.

After a service request has been communicated through simple RESTful APIs, or through the Service Fulfillment application, the NSD uses operator-defined policies to guide dynamic network resource selection and automated provisioning. These policies use a real-time view of the network (including link and tunnel utilization) to map service connection requests to the best available tunnels/paths (Layer 0 to Layer 3) that meet the customer's Service Level Agreement (SLA) requirements and the operator's network efficiency goals. For example, the NSD can track booking and use real-time network KPIs to assess whether existing tunnels/paths are congested. If so, the NSD uses operator-defined policies to bind incoming service requests to less utilized paths that provide approximately the same connection attributes. It can revert the services to the optimal paths when demand subsides. If no path that meets the requested attributes is available, the NSD asks the relevant NRC to compute a new path.

Note: For IP-only deployments, the NSD must integrate with the NFM-P, CPAM, vCPAA, and VSR-NRC. For optical-only deployments, the NSD must integrate with NFM-T.

1.2 MDM adaptors and Service Fulfillment

Available application functions for model-driven NEs in Service Fulfillment can vary based on the adaptors installed. To verify the adaptors you have installed, check the Discovered Nodes list in the Device Administrator application. The Summary panel for the NE provides the list of adaptors installed for each application.

1.3 Access control in Service Fulfillment

Operator visibility of network equipment is based on access control settings that are specified by an NSP administrator. Depending on your access settings, some equipment may not be available to you. Users with associated roles and group access permission can create, view, update, or delete

services. In addition, administrators can specify resource (NEs, ports, services) permissions per user role. See the *NSP User Manager Application Help* and your NSP administrator for more information.

1.4 Navigating in Service Fulfillment

When you launch the Service Fulfillment application, the landing page displays the Service List view which displays all created services. You can view and manage the services, and also create a service using the Create a Service button in the top right corner.

There are two tabs in the SF application. The SERVICES tab is where you create and edit services. You can use the Service List drop-down menu to navigate to the Dashboard page. The Dashboard displays the customizable service topology map. You can also create a service from the Dashboard.

The INVENTORY tab is where you manage ports, service tunnels, physical links and endpoints. You can also create or delete physical links from this page.

1.5 Service topology map format

To view the service topology map, click on the Service List drop-down menu and choose Dashboard.

The service topology map allows you to perform the following:

- **View NE information.** Hover over an NE or physical link to display basic information for the object.
- **Refresh map data.** Click **Refresh Map** to update the map contents.
- **Sync with network data.** Click **More** **Sync with Network Data** to show the most recent changes to the network.
- **Rebuild map.** Click **More** **Rebuild Map** to delete the map from the server and rebuild the map.

Use the following controls to modify the appearance of the service map:

- Fit the map to available screen area
- Show or hide text labels for vertexes, adjust vertex size, cluster distance, and on-screen cluster density, set vertex clustering on or off
- Show or hide links, adjust link curvature and link spacing, specify the link grouping threshold
- Zoom in and zoom out of the map

1.6 What is Object Life Cycle?

Object Life Cycle (OLC) is used to manage state transitions of services inside the NSD as they go from the planning phase to the deployment phase.

1.6.1 Planning phase

The planning phase includes four states:

- Planned

- Routing
- Routing Failed
- Routed and Save

1.6.2 Deployment phase

The deployment phase includes five states:

- Waiting for Deployment
- Deploying
- Partially Deployed
- Deployment Failed
- Deployed

Note: The state of a service discovered or re-synchronized from the NFM-P is Deployed.

1.6.3 Saving service configuration without deployment

The Service Fulfillment application allows you to save a configured service without deploying it to the network. The system stores all user-configured parameters in the database for the service. However, a saved service does not reserve any bandwidth or network resource, and the system does not check the availability of resources for a saved service. The system checks for resources when the saved service is deployed to the network, and validates the resources or returns the appropriate errors.

Only fully configured services can be saved. The Service Fulfillment application treats any saved service as a service that you can deploy immediately. The system does not support saving services that are partially configured.

The Service Fulfillment application allows you to modify a saved service. Then you can either deploy the service with the modified configuration or save the modified service again. A modified saved service does not reserve any network resources, which are allocated and validated only when a service is deployed.

1.7 Validating service configuration

The Service Fulfillment application can validate E-LAN, E-Line, L3 VPN, and IES service configuration forms and their augmented attributes only if the schema form has a validate property for the attribute.

To validate a service configuration form, you must create a service template using the Policy Management application. On the service template form, enable the Add Trigger for Validation Workflow in Creation Form parameter and select an existing validation workflow. When you create a service using the Service Fulfillment application and apply this template, a VALIDATE button will be displayed on the service creation form.

To validate individual properties in the augmentation schema, you must add "validate”:"your-validation-workflow-name". This will cause a VALIDATE button to display on the service configuration form next to the specified property. When you click the VALIDATE button, a workflow execution is run and a dialog box appears.

Validation workflows are created using the Workflow Manager application and must include a state object and an output object that consists of a message field and a validation field. The state object indicates whether the workflow has been successfully run. If it was run successfully, the contents of the output object's message field will be displayed in the Service Fulfillment application's dialog box. The output object's validation field indicates whether or not the service or property has been successfully validated.

1.8 What is service CAC?

1.8.1 Bandwidth CAC and validation

The NSD can perform bandwidth CAC and validation on access ports. Every port available for use in E-Line, C-Line, E-LAN, and L3 VPN services will have their available ingress bandwidth and available egress bandwidth displayed as read-only properties in the Service Fulfillment application and the NSP's REST APIs. When any of these ports are discovered, available bandwidth is initialized to port speed. In some cases, such as the 60-port 10/100 card when the port is operationally down, the port speed is zero. On fixed port speed cards, the port speed is populated, allowing services with bandwidth to be configured even when the port is down.

Note: Service CAC is not available on the variable-speed SFP-based cards.

Any changes to port speed will be reflected in the displayed available ingress bandwidth and available egress bandwidth. This may result in these fields displaying a negative value. No alarms or notifications will occur but a WARN level log will be generated.

Service CAC is disabled by default.

Note: Service CAC is supported on services originating from the NFM-P that have had their 'NSD-managed' flag enabled.

Note: Service CAC is not supported on multi-vendor services for which there is no access port bandwidth tracking.

1.8.2 Bandwidth calculation and booking

A formula is used to calculate both the ingress and egress aggregate bandwidth of all endpoints used by E-Line, C-Line, E-LAN, and L3 VPN services. The formula yields the sum of the CIR values, which is based on each of the configured queues and the scheduler policy of the QoS. This same value is used for E-Line service tunnel bandwidth calculation. No overbooking is applied to the formula. When the NSD creates a service on one of these endpoints, the validation code will make sure that the sum of the formula is less than, or equal to, the current available bandwidth on the port, otherwise the service will not be created and an error is returned.

The bandwidth is only booked after the traversal operation is run to match with the current behavior of the core bandwidth. It is possible that between the validation check and the traversal operation, the port bandwidth was consumed by another service. In this case, the OLC state is changed to Routing Failed, and you are notified that either the access port ingress or egress bandwidth was exceeded. Modifying the CIR will reinitiate the traversal operation. Similar operations occur when adding endpoints to an existing service and modifying endpoints. In the latter case, it is the

bandwidth delta which is applied to the available ingress or egress bandwidth. Upon deletion of an endpoint or service, the available ingress or egress bandwidth is increased by the bandwidth of the endpoints.

Service CAC is available on both access and hybrid ports. If there are network interfaces on hybrid ports, these are not tracked as part of the available ingress or egress bandwidth. When an upgrade is performed, the available ingress and egress bandwidths will be calculated based on all existing services within the NSD. This may result in negative values. When in an overbooked state, any request that will not cause a change to bandwidth reservation, or that will cause a shrink in bandwidth reservation, will be permitted.

1.9 How do I enable service CAC?

1

On your NSD and NRC server, navigate to the following directory: */opt/nsp/server/tomcat/webapps/sdn/WEB-INF/config/*

2

Modify the system.config file as follows:

```
algo

{

serviceCAC="on"

multiVendorServiceCAC = "on"

}
```

3

Save your changes and close the system.config file.

END OF STEPS

1.10 How does NSD handle service access QoS?

This feature includes an implementation of a normalized model for access QoS: a generic QoS policy that can be used for 7450 ESS, 7750 SR, 7210 SAS, and third party routers. The enhancement in QoS also facilitates Bandwidth on Demand functionality.

This feature includes the following QoS setup and usage procedures:

1. The operator/admin defines QoS catalog including, for example, Gold, Silver, and Bronze categories. This user also uses the NFM-P GUI to define the QoS Generic Policies. The policy model is generic, therefore, it can be applied to 7450 ESS, 7750 SR, 7210 SAS, and third party routers.

2. While provisioning an endpoint, either via ReST NBI or Service Fulfillment application, the user can select one of the predefined QoS categories (gold, silver, or bronze).
3. If Bandwidth on Demand is used (meaning the bandwidth constraints are modified), then the user can only select another policy.

   The behavior is as follows for each of the supported node categories:
   - 7450 ESS and 7750 SR: the changes only affect the SAP that is being changed
   - 7210 SAS: queue changes are not addressed
   - Third party routers: changes are defined by the corresponding driver

1.11 How does the Service Fulfillment application choose a GQP on a brownfield service?

For MDM managed NEs, the Service Fulfillment application resolves the synced/discovered ingress and egress policy names in the NE service configuration to the equivalent GQP, and assigns the GQP to the service.

The NSD retrieves all GQPs and removes all QoS policies (per policy type) that do not reside on the current NE. Then an exact match is performed for both ingress and egress against (NE filtered GQPs) and service configurations. If multiple results are found, then the lowest GQP ID is chosen.

Use the following tables to determine how the GQP ID is chosen, based on the policy types and service configurations on an MDM managed NE.

NEs with QoS policy definitions

NE	Policy name/type	Policy name/type	Policy name/type
Nokia SR 1 NE “B”	"sapEgr987" / sap-egress	"Scheduler_Policy_1" / scheduler	"sapIng987" / sap-ingress
Nokia SR 2 NE “C”	"sapEgr987" / sap-egress	"sapIng987" / sap-ingress	
Cisco XE NE “D”	“CiscoPolicy1” / policy-map		
Juniper NE “E”	“JuniperPolicyAny1” / filter		

NSD Generic QoS Policy (GQP) and entries

GQP ID	Policy name	Policy name	Policy name
1	sapEgr987 (Egr)	Scheduler_Policy_ 1(Egr)	
2	sapEgr987 (Egr)		
3	sapEgr987 (Egr)	sapIng987(Ing)	Scheduler_Policy_1(Egr)
4	sapEgr987 (Egr)	Scheduler_Policy_ 1(Egr)	CiscoPolicy1 (Egr)

GQP ID	Policy name	Policy name	Policy name
5	sapIng987 (Ing)	Scheduler_Policy_ 1(Ing)	

Use case examples:

1. If NE “B” service 1 has the SAP egress configured as "sapEgr987", the match will be GQP 2.
2. If NE “B” service 2 has the SAP egress configured as "sapEgr987" and Scheduler Policy 1 is selected, the match will be GQP 1. The NSD finds two matches: GQP 1 and GQP 4. A warning message is logged in the NSP and the NSD chooses GQP 1 because it is the lowest GQP ID.
3. If NE “C” service 1 has the SAP egress configured as "sapEgr987", the match will be GQP 1. NE “C” does not have a Scheduler Policy selected, so there will be two matches: GQP 1 and GQP 2. The NSD logs a warning and chooses GQP 1 because it is the lowest GQP ID.
4. If CiscoXE service 4 has "CiscoPolicy1" on the egress or if Juniper service 4 has "JuniperPolicyAny1" on the egress, the match will be GQP 4.
5. If NE “B” service 5 has the SAP ingress configured as "sapIng987", there is no match. If you delete Scheduler Policy 1 on NE “B” and do a resync, the match will be GQP 5.

1.12 How does NSD handle brownfield LSPs and SDP tunnels?

The NSD is capable of discovering LSP and SDP tunnels created previously within the NFM-P, including multi-vendor LSP and SDP tunnels, with the following exceptions:

- A single SDP tunnel that uses multiple LSPs
- Multiple SDP tunnels that use the same LSP

1.12.1 Service tunnels (SDP)

The NSD will discover, and allow you to create services with bandwidth constraints on service tunnels created previously within the NFM-P. The NSD will operate with initial allocated bandwidth on these tunnels and will keep track of used bandwidth for all the services created by the NSD. It is assumed that the NSD is the only entity creating services on these tunnels. The NSD can be used to delete or resize the allocated bandwidth, as well as to modify the LSPs associated with service tunnels previously created within the NFM-P.

1.12.2 RSVP-TE LSPs

The NSD will discover, and allow you to create service tunnels on RSVP-TE LSPs created previously within the NFM-P. The NSD will operate with initial allocated bandwidth on these LSPs and will keep track of used bandwidth for all the service tunnels created on these LSPs by the NSD. It is assumed that the NSD is the only entity creating service tunnels on these LSPs. The NSD cannot be used to delete, resize the allocated bandwidth, or modify LSPs previously created within the NFM-P.

1.12.3 Bandwidth update on existing LSP

When the reserved bandwidth of a previously-discovered LSP is modified, the NSD receives an event, and will update the both initial and available bandwidth on the LSP and SDP tunnel. This case should apply to all LSP and SDP tunnels managed by the NSD, regardless of their origin, with the following exceptions:

- A single SDP tunnel that uses multiple LSPs
- Multiple SDP tunnels that use the same LSP

The following bandwidth utilization considerations apply:

- When an LSP is used by an SDP tunnel, but is not yet bound to any service, the initial and available bandwidth of the LSP is updated. However, since the LSP is used by an SDP tunnel, the SDP tunnel takes the entire bandwidth. As there are no services using the SDP tunnel, the available bandwidth must be equal to current bandwidth.
- When an LSP is used by an SDP tunnel and there are services bound to the SDP tunnel, the SDP tunnel will take all the LSP current bandwidth. The LSP available bandwidth must be 0, and depending on the services bound to the SDP tunnel, the available bandwidth of the SDP tunnel is adjusted to reflect the current bandwidth, minus the total bandwidth of all services running on that SDP tunnel.

1.13 How do I create a physical link between ports?

Physical links exist only in the NSD database; nothing is provisioned to the NFM-P. The operational state of one or both of the linked ports determines the operational state of the physical link. Updates to the link may be required when the port operational state changes. The Service Fulfillment application can also be used to delete physical links that have been created using the Service Fulfillment application.

1

Click on the **INVENTORY** tab of the Service Fulfillment application, and then click **Physical Links**. The application displays a list of existing physical links.

2

Click **CREATE LINK**. The Create Physical Link form opens.

3

Click **SELECT PORTS** and search for available ports. You can search for a specific port by NE Name or Port Name.

4

Select the endpoint ports and click **DONE**.

5

Click **CREATE**. The system creates the physical link.

END OF STEPS

1.14 LLDP link discovery

In the MDM framework, the NSD supports the LLDP-based discovery of physical links in the network topology. The discovery mechanism uses the MDM to read the LLDP neighbor information. The NSD adds the discovered links to the common store so that all applicable applications can access the link information. This functionality is supported only for the physical links with the Nearest Bridge transmission scope.

1.15 How do I re-synchronize ports?

1

Click on the **INVENTORY** tab of the Service Fulfillment application and then click **Ports**.

2

You can re-synchronize one or more ports at a time.

a. Select a port and click **Resync** .

b. Use the Shift or CTRL key to select more than one port, and then click **Resync Selected** in the top right corner of the dashboard.

The port or ports are re-synchronized.

END OF STEPS

1.16 How do I re-synchronize or delete services on a selected port or service tunnel?

For maintenance, planning, or migration purposes, you can correlate services associated to an equipment or tunnel resource and perform a re-synchronization of one or more services on a selected port or service tunnel.

You can also delete a service or multiple services on selected ports or service tunnels.

1

Click on the **INVENTORY** tab of the Service Fulfillment application and then click **Ports** or **Service Tunnels**.

2

Move the mouse pointer to the right of the port entry or service tunnel entry and click **Services Using Port** or **Services Using Tunnel** .

The services using this port or tunnel are displayed.

3

You can re-synchronize or delete one or more services at a time.

a. Select a service and click **Resync** or **Delete** .

The service is re-synchronized or deleted.

b. Use the Shift or CTRL key to select more than one service, and then click **Resync Selected** or **Delete Selected** in the top right corner of the dashboard.

The service or services associated with this port or tunnel are re-synchronized or deleted.

END OF STEPS

1.17 What are E-LAN services?

E-LAN services are configured with the same parameters that are used for E-Line service creation. Objectives/constraints are enforced for the LSPs. The default endpoint QoS template is applied to all endpoints. Zero bandwidth is reserved in the core. E-LAN services can use service tunnels that were not created using the Service Fulfillment application.

1.17.1 Can I create E-LAN services on multi-vendor NEs?

The Service Fulfillment application supports the creation of most of the E-LAN services on Cisco nodes. When this is done, the Service Fulfillment application configures a property called bridgeDomainId during the site creation.

The Service Fulfillment application does not support the creation of E-LAN services on Juniper nodes.

1.17.2 What are EVPN-based E-LAN services?

The Service Fulfillment application supports the creation of EVPN-based E-LAN services over tunnel types that are supported in a BGP-EVPN MPLS context. The EVPN-based E-LAN service is not established over pseudowire. You can configure EVPN-based E-LAN services on all the Nokia NEs that support EVPN. The configuration of EVPN-based E-LAN services on multi-vendor NEs is not supported.

The EVPN-based E-LAN service supports the same topology types as those supported by the pseudowire E-LAN service: Hub and Spoke and Full Mesh.

To configure an EVPN-based E-LAN service, you need to start the E-LAN service creation in the Service Fulfillment application, as usual, and select the Enable EVPN Tunnel Selection check box in the Additional Properties form. After enabling the EVPN service, you are able to select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. There is also the ANY option, which indicates to the NSD that any supported tunnel type in the EVPN context can be selected following the order of preference.

The following considerations apply to the EVPN-based E-LAN service configuration in the Service Fulfillment application:

- The Service Fulfillment application supports only the configuration of greenfield EVPN-based E-LAN service. The modification of existing EVPN-based E-LAN services that were created in

the NFM-P is not supported. The opposite is also true: EVPN-based E-LAN services that were created in the Service Fulfillment application cannot be modified in the NFM-P.

- The NSD assumes that the network is correctly configured to support the selected tunnel type. The service can fail if the network is not correctly configured. For example, if the network does not have SR-TE LSPs configured, then an EVPN-based E-LAN service configured with the SR-TE tunnel type is operationally down.
- The tunnel type parameter is modifiable, as required. However, the Service Fulfillment application does not support switching from the EVPN-based E-LAN (the Enable EVPN Tunnel Selection check box is selected) to a pseudowire-based E-LAN (the Enable EVPN Tunnel Selection check box is not selected).
- Each service is associated with a unique EVPN instance (EVI) number that the NSD generates automatically. The NSD synchronizes the EVIs defined in the network to ensure the EVI uniqueness.

  In the Full Mesh topology, the NSD sends the EVI to the NE to auto-derive the RD/RT for the NE. The RT import and export label is the same for all NEs in the Full Mesh topology.

  In the Hub and Spoke topology, the NSD sends the EVI to the NE to auto-derive only the RD for the NE. The NSD generates the RT to ensure that the RT import and export labels on the hub endpoint are inverted with respect to the RT import and export labels on the spoke endpoints. That is, the hub RT import label matches the spoke RT export label, and the hub RT export label matches the spoke RT import label. The unique RT labels are stored in the cache, and the NSD continuously resynchronizes the existing RT labels from the NFM-P to ensure uniqueness.

To ensure consistency when configuring multiple similar services, you can create EVPN-based E-LAN service templates that you can then apply to your service. Just select the appropriate Tunnel Type for EVPN-based E-LAN in the template properties, as required.

1.17.3 What are E-LAN L2 extension devices?

The Service Fulfillment application extends the E-LAN model to natively support the ability to provision CPE devices as L2 extension devices. This capability is applicable only for MDM managed devices. Only one L2 extension device per endpoint is supported. Enable the L2 Extension parameter for the E-LAN ports to list applicable ports for the L2 extension device. You can add an L2 extension to a new or existing endpoint and modify the augmented properties on the L2 extension.

Note: Brownfield discovery of an L2 extension device is not supported.

1.18 How do I provision E-LAN services?

1

Click on the **SERVICES** tab and then click **CREATE A SERVICE** in the top right corner.

Select a template

2

From the **Select a template to start** drop-down menu, choose the type of service you want to create, or choose All Templates to see a list of all preconfigured templates.

Choose the default template or a preconfigured template from the list. Recently used templates are shown in the right panel.

You can also search for a template in the search field.

Name and define the service

3

Type a Service Name for the E-LAN service.

You can edit the service type and the template. If the template is changed after you configure the sites and endpoints, the site and port selections are not saved and you must select and configure the ports again.

Set the service parameters

4

Click **ADDITIONAL PROPERTIES** to configure the service parameters, as required.

Parameter	Configuration
Description	Describes the service.
Customer ID	The customer ID is associated with a newly created service. If a customer ID is not provided during service creation, the customer ID provided by the associated service template will be used. If no customer ID is found, the default customer ID of 1 will be used. The customer ID applies only to SR NEs.
Tunnel Profile	Set the Tunnel Profile (also known as a policy) to apply to the service.
Path Profile	Set the path profile to be used by the service.
Admin State	Set the administrative state of the service.
Bidirectional	Specify whether or not a return path is required, and if so, what type of return path should be determined. Select one of the following options: Symmetric Reverse Route Preferred or Any Reverse Route.
Objective	Specify the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Set the MTU for the service. The range is 0 to 9194.
Maximum Hops	Set the maximum number of hops to consider.
Maximum Latency	Set the maximum latency to consider.

Parameter	Configuration
Maximum Cost	Set the maximum cost to consider.
Enable EVPN Tunnel Selection	Enable or disable the configuration of an EVPN-based E-LAN service. If enabled, you can select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. The ANY option indicates to the NSD that any supported tunnel type in the EVPN context can be selected in the order of preference. Applicable to MDM-managed nodes.

5

Click **OK**. The Additional Properties form closes.

6

Click **CONTINUE**. The service configuration focus moves to the endpoint configuration area.

Add the endpoints

7

Select a topology type. Your topology type selection (Full Mesh or Hub and Spoke) determines the endpoint selection.

8

Select the service endpoints.

1. Click **SELECT PORTS** to display the list of available ports. You can filter by a list of available attributes.
2. Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.

   Repeat this step to select additional ports, as required.
3. Click **DONE**.

You can click **VIEW ENDPOINT LIST** to display the list of selected endpoints. To return to the map view, click **VIEW SERVICE MAP**.

9

Click **CONTINUE**. The system checks the selected endpoints and informs you that one or more endpoints is missing required values. You need to perform additional configuration on each endpoint.

10

Click an endpoint entry. The Configure Endpoints form opens.

11

Click on the endpoints that are missing configuration and configure the required parameters.

Parameter	Configuration
Admin State	Specifies the current administrative state of the endpoint.
Outer Tag	Specifies the outer tag for Dot1Q or QinQ ports.
Inner Tag	Specifies the inner tag for Dot1Q or QinQ ports.
QoS Profile Name	Specifies the QoS Profile to be used. You can only assign a Generic QoS policy to a service endpoint if any one of the ingress and egress associated policies (if assigned) within the Generic QoS policy already exist on the NE.
L2 Extension	Specifies whether to attach an L2 extension.

12

If you set a QoS Profile in the previous step, click **SHOW QOS SETTINGS** to view the QoS settings applied by the profile.

13

If you enabled L2 Extension, perform the following:

1. Click **Select NNI Port or Select UNI Port** to display the list of available ports. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.
2. Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.
3. Click **DONE** after selecting the port.
4. Configure the Inner and Outer tag parameters for the port, as required.
5. Click **SAVE** or **DEPLOY**.

14

Click **OK**. The Configure Endpoints form closes.

15

Repeat Step 10 through Step 14 for each service endpoint.

Review your service

16

Click **CONTINUE** and review the service configuration summary. You can click  to view the service representation in the map.

Deploy or save your service

17

At this point you can deploy, save, or modify your service:

a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.

c. If you need to modify the service configuration, click **BACK** to go to previous service configuration steps, as required.

d. If you applied an E-LAN service template to this service, and you enabled the Add Trigger for Validation Workflow in Creation Form parameter in the E-LAN service template, a Validate button is available. Click **VALIDATE** to run the workflow and validate the service configuration.

End of steps

1.19 What are E-Line services?

An E-Line service connects two customer Ethernet ports over a WAN. The Service Fulfillment application supports the creation of E-Line services over IP networks. When an E-Line service is deployed, the selection of the endpoints utilizes automatically the requisite technology tunnels. For example, when the tunneling technology is MPLS, a service tunnel with a single LSP satisfying the service-specified constraints and objectives is automatically selected. The service is then bound to that LSP via the service tunnel. The NSD tracks the LSP available bandwidth and adjusts it automatically to accommodate the E-Line service, which reserves bandwidth on the LSP.

If an existing E-Line service is modified (for example, to increase bandwidth), the service tunnel is resized to accommodate it, if permitted by policy. If the service tunnel resizing fails, the service tunnel may be rerouted onto links that cannot accommodate the resized service tunnel. If the reroute fails, then a new service tunnel is created. It is possible for E-Line services to use service tunnels that were not created using the Service Fulfillment application.

Note: Policies for service-to-tunnel binding dictate the rules associated with the service binding. If no service tunnel meets all the constraints, and this is a new E-Line service, a new service tunnel is created.

Other parameters of the E-Line service are obtained from the specific templates referenced in the abstract API definition. The service definition in the abstract API, the detailed configuration in the service templates, and other network and tunnel parameters form the complete service definition, which is represented in the normalized model for E-Line. Specific configurations based on the devices are then constructed and deployed using the NFM-P.

Note: You can provision SAP-to-SAP E-Line services if you select different ports for each endpoint.

1.19.1 Can I create E-Line services on multi-vendor NEs?

The Service Fulfillment application supports the following multi-vendor endpoint combinations for E-Line services:

- Cisco-Nokia
- Juniper-Nokia
- Cisco-Juniper
- Cisco-Cisco
- Juniper-Juniper

The following considerations apply to the E-Line multi-vendor support:

- Cisco LSP names must be in the format of Tunnel*number*, where *number* is an integer between 0 and 65535.
- Cisco LSP-Path Bindings contain a property called Path Option. This property must be set to 1 for primary and 2 for secondary.
- Cisco and Juniper endpoints support only secondary paths, and do not support standby paths. When Cisco or Juniper endpoints are used and the Tunnel Creation Template has the Protection Type set to *Standby*, the Service Fulfillment application creates secondary paths instead.

When creating an E-Line service on multi-vendor NEs, the Service Fulfillment application attempts to find a tunnel based on the criteria specified in the Tunnel Selection Profile (TSP). If no tunnel exists, and the TSP specifies that new tunnels must be created, then the Service Fulfillment application creates MPLS RSVP-TE tunnels, including the Dynamic LSP and LSP-Path Bindings.

1.19.2 What are brownfield E-Line services?

The E-Line services created within the NFM-P (brownfield E-Line services) can be managed by the Service Fulfillment application. In order for the Service Fulfillment application to discover these services, their “NSD-managed” flag must be enabled within the NFM-P. Once discovered by the Service Fulfillment application, these services will function the same as E-Line services created within the Service Fulfillment application itself, provided that they meet the NSD requirements. Any change made to these services within NFM-P after discovery will be propagated to the Service Fulfillment application, provided the change impacts the topology of the service.

Note: E-Line services created within the NFM-P have an “Auto-delete” flag. When enabled, services without service sites are automatically deleted. This flag should not be enabled on services being managed by the Service Fulfillment application, as the “NSD-managed” flag is disabled upon service deletion, and remains so even if the service is recreated and resynchronized into the Service Fulfillment application.

1.19.3 What are multi-domain E-Line services?

The Service Fulfillment application supports multi-domain E-Lines that span any mix of MPLS and non-MPLS domains. The service tunnels must be already created in the MPLS domains. The non-MPLS domains can consist of only peer-to-peer Ethernet links.

In addition to the SAP-to-SAP and SAP-to-SDP service sites, the multi-domain E-Line service also supports SDP-to-SDP connections through the use of pseudowire switching. However, the NEs eligible for SDP-to-SDP pseudowire switching must be pre-configured with a pw-switching flag that is enabled on the NE.

The NSP calculates an optimal end-to-end path that traverses existing service tunnels, including VLAN handoff. Only strictly-routed RSVP-based service tunnels have calculations for the number of hops and accumulated IGP metric and latency. The VLAN handoffs have hard-coded hops, IGP metric and latency to 1. Other service tunnels have very large numbers for hops, IGP metric and latency and are usually less preferred. The non-RSVP service tunnels have zero bandwidth.

1.19.4 What types of multi-domain E-Line services can I create?

The multi-domain E-line service provisioning allows you to create the following types of E-Lines:

- vc-switched—in addition to the two terminating sites, an E-Line can include one or more switching sites
- composite—a composite E-Line consists of multiple component services connected through VLAN handoff to provide end-to-end connectivity

  A composite E-Line can include a vc-switched e-line.

To support the multi-domain functionality, the E-Line service template provides the VC Type parameter, which allows you to specify the type of pseudowire for the E-Line service.

1.19.5 What are EVPN-based E-Line services?

The Service Fulfillment application supports the creation of EVPN-based E-Line services over tunnel types that are supported in a BGP-EVPN MPLS context. The EVPN-based E-Line service is not established over pseudowire. You can configure EVPN-based E-Line services on all the Nokia NEs that support EVPN. The configuration of EVPN-based E-Line services on multi-vendor NEs is not supported.

To configure an EVPN-based E-Line service, you need to start the E-Line service creation in the Service Fulfillment application, as usual, and select the Enable EVPN Tunnel Selection check box in the Additional Properties form. After enabling the EVPN service, you are able to select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. There is also the ANY option, which indicates to the nodes that any supported tunnel type in the EVPN context can be selected following the order of preference.

The following considerations apply to the EVPN-based E-Line service configuration in the Service Fulfillment application:

- The Service Fulfillment application supports only the configuration of greenfield EVPN-based E-Line service. The modification of existing EVPN-based E-Line services that were created in the NFM-P is not supported.
- The Service Fulfillment application assumes that the network is correctly configured to support

the selected tunnel type. The service can fail if the network is not correctly configured. For example, if the network does not have SR-TE LSPs configured, then an EVPN-based E-Line service configured with the SR-TE tunnel type is operationally down.

- The tunnel type parameter is modifiable, as required. However, the Service Fulfillment application does not support switching from the EVPN-based E-Line (the Enable EVPN Tunnel Selection check box is selected) to a pseudowire-based E-Line (the Enable EVPN Tunnel Selection check box is not selected).
- Each service is associated with a unique EVPN instance (EVI) number that the Service Fulfillment application generates automatically and then sends to the NE to auto-derive the unique RD/RT for the NE. The Service Fulfillment application synchronizes the EVIs defined in the network to ensure the EVI uniqueness.
- The EVPN-based E-Line service uses an Ethernet Tag (eth-tag) that is pre-configured by the NSD and not visible in the GUI. The NE uses the Ethernet Tag to identify its remote BGP peer and establish the MP-BGP connection.

To ensure consistency when configuring multiple similar services, you can create EVPN-based E-Line service templates that you can then apply to your service. Just select the appropriate Tunnel Type for EVPN-based E-Line in the template properties, as required.

1.19.6 What are E-Line services with MC LAG termination?

The Service Fulfillment application supports the creation of E-Line services with MC-LAG termination. The NSD support for MC-LAG requires the preconfiguration of MC-LAG on the NFM-P, including the MC Peer Group and the MC LAG Group. The Service Fulfillment application discovers the preconfigured MC LAG Group as a service object in the physical layer. This service object can be selected as an endpoint for service creation. The MC-LAG object represents both the active and the standby NE members of the LAG.

An E-Line service with MC-LAG termination has zero bandwidth in the core.

When an MC-LAG is selected as an endpoint for E-Line service creation, the NSD automatically considers it as two separate endpoint requests: one request for each LAG member. The NSD decomposes the request into two endpoint requests: one for the active NE LAG and one for the standby NE-LAG. All of the configuration in the original request, including the encapsulation values, is copied to two new separate requests. As a result, the NSD assumes that both MC-LAG members are configured with the same encapsulation mode and type.

The NSD supports the creation of an E-Line service with MC-LAG termination between the following endpoint types:

- from regular port to MC-LAG
- from SC-LAG to MC-LAG
- from MC-LAG to MC-LAG

Note: A regular endpoint consists of a single NE and a single port. When a regular endpoint is selected, the NSD creates a service site on that NE using the specified port as the termination point.

For the SC-LAG, two VLL endpoints must be configured on the NFM-P:

- The first VLL endpoint must have an SC-LAG SAP.

- The second VLL endpoint must have a primary and a secondary spoke SDP bindings to the two SC-LAG members.

For the MC-LAG, two VLL endpoints must be configured on the NFM-P:

- The first VLL endpoint must have an MC-LAG SAP and a spoke SDP binding destined for its MC-LAG peer, with ICB enabled.
- The second VLL endpoint must have one or two spoke SDP bindings to the far end.

1.19.7 What are E-Line L2 extension devices?

The Service Fulfillment application extends the E-Line model to natively support the ability to provision CPE devices as L2 extension devices. This capability is applicable only for MDM managed devices. Only one L2 extension device per endpoint is supported. Enable the L2 Extension parameter for the E-Line ports to list applicable ports for the L2 extension device. You can add an L2 extension to a new or existing endpoint and modify the augmented properties on the L2 extension.

Note: Brownfield discovery of an L2 extension device is not supported.

1.20 What are E-Access services?

The NSD supports the creation of E-Line services between an NE that is managed by an NSD instance and an NE that is located in a different domain and managed by a different NSD instance or by a third-party system. This applies to cases in which your NSD does not manage the entire network. This type of service is called an E-Access service. An E-access service is only supported on NFM-P managed NEs. The NSD supports the creation of an E-Access service only by way of the NSD REST API. To create an E-Access service, use the POST /api/v4/services/eaccess operation, Create an IP E-Access service.

For the E-Access service creation to work, you must use an SDP tunnel, a path and an LSP that were already configured on each NE between the two NEs. You also need to configure a Tunnel Selection policy to apply to the E-Access service. Select the Use existing tunnels option as the service provisioning rule.

A few pointers to help you configure an E-Access service:

- The NSD books bandwidth only at the Access interface level, not on the LSP in the core.
- The service uses the VC-ID label specified on the Adjacency on the spoke-sdp binding.
- If the Service ID is not already in use, the NSD assigns the VC-ID label as the Service ID. If that Service ID is already in use, the NSD auto-assigns the next available ID.
- If you specify a VC-Type label, then it must match the VC-Type defined at the far end. The default value is Ethernet_Tagged_Mode, which maps to VLAN on the NE.
- E-Line service templates can be applied to E-Access services.

After creating the E-Access service, you can view the service and its properties in the Service Fulfillment application.

- The Service layer shows just the NE, along with the service endpoint, that is in the network managed by your NSD.

- The Service Tunnel layer shows the Service Tunnel connection. This is the existing SDP that you created for the service.
- The MPLS layer shows the LSP. This is the existing LSP that you created for the service.
- The service does not show an IGP layer because your NSD does not manage the far-end NE and therefore is not aware of the IGP path.
- The service does not show a physical layer because your NSD does not manage the far-end NE.

1.21 How do I provision E-Line services?

You can create and modify an E-Line service using a Properties form that is enabled by default. The Properties form shows all fields at once. Default values appear in the fields, if applicable. You can switch back and forth between the Properties form and the Service Builder using the icons in the top right corner. The icons are available only after you click **CREATE A SERVICE** and select a template. The Service Fulfillment application will remember your setting until the browser history is cleared.

1

Click on the **SERVICES** tab and then click **CREATE A SERVICE** in the top right corner.

Select a template

2

From the **Select a template to start** drop-down menu, choose the type of service you want to create, or choose All Templates to see a list of all preconfigured templates.

Choose the default template or a preconfigured template from the list. Recently used templates are shown in the right panel.

You can also search for a template in the search field.

Identification

3

Type a Service Name for your service.

You can edit the customer ID, template, and description. If the template is changed after you configure the sites and endpoints, the site and port selections are not saved and you must select and configure the ports again.

Characteristics

4

Configure the parameters, as required.

Parameter	Description
Tunnel Profile	Specifies the Tunnel Profile to apply to the service.
Path Profile	Specifies the path profile to be used by the service.
Diverse From Service	Specifies an existing NSD-managed E-Line service for the new E-Line service to be diverse from. As a result, the new E-Line creates LSPs with the same path profile and group ID as the LSPs used in the specified E-Line.
Admin State	Specifies the initial administrative state of the service on deployment.
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined. Select one of the following options: Symmetric Reverse Route Preferred or Any Reverse Route.
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Specifies the MTU for the service. The range is 0 to 9194.
Maximum Hops	Specifies the maximum number of hops to consider
Maximum Latency	Specifies the maximum latency to consider.
Maximum Cost	Specifies the maximum cost to consider.

Parameter	Description
Enable EVPN Tunnel Selection	Enables the configuration of an EVPN-based E-Line service, so that you can select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. The ANY option indicates to the NSD that any supported tunnel type in the EVPN context can be selected in the order of preference. Applicable to MDM-managed nodes.

Sites and Endpoints

5

Click **SELECT PORTS** to display the list of available ports. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.

6

Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.

Perform this step to select additional ports, as required.

7

Click **DONE** after selecting the ports.

8

Configure the required endpoint parameters.

Parameter	Description
Admin State	Specifies the current administrative state of the endpoint.
Description	Specifies a description for the endpoint.
Outer Tag	Specifies the outer tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
Inner Tag	Specifies the inner tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
QoS Profile Name	Specifies the QoS Profile to be used. You can only assign a Generic QoS policy to a service endpoint if any one of the ingress and egress associated policies (if assigned) within the Generic QoS policy already exist on the NE.
L2 Extension	Specifies whether to attach an L2 extension.

9

If a QoS Profile was specified in the previous step, click **SHOW** to view the QoS settings applied by the profile.

10

If you enabled L2 Extension, perform the following:

1. Click **SELECT NNI PORT or SELECT UNI PORT** to display the list of available ports. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.
2. Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.
3. Click **DONE** after selecting the port.
4. Configure the Inner and Outer tag parameters for the port, as required.

11

Perform one of the following tasks:

a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.

c. If you applied an E-Line service template to this service, and you enabled the Add Trigger for Validation Workflow in Creation Form parameter in the E-Line service template, a Validate button is available. Click **VALIDATE** to run the workflow and validate the service configuration.

END OF STEPS

1.22 What are C-Line services?

C-Line services connect two SAPs that can be defined on SONET/SDH, DS3/E3,T1/E1 ports or TDM channels. The NSD supports the creation of C-Line services over IP networks. When a C-Line service is deployed, the selection of the endpoints automatically utilizes the requisite technology (MPLS or L0 WDM) tunnels.

It is possible for C-Line services to use service tunnels that were not created using the NSD.

Note: Policies for service-to-tunnel binding dictate the rules associated with the service binding. If no service tunnel meets all the constraints, and this is a new C-Line service, a new service tunnel is created.

Other parameters of the C-Line service are obtained from the specific templates referenced in the abstract API definition. The service definition in the abstract API, the detailed configuration in the

service templates, and other network and tunnel parameters form the complete service definition, which is represented in the normalized model for C-Line. Specific configurations based on the devices are then constructed and deployed using the NFM-P.

Note: The SAP-to-SAP C-Line services can be provisioned if different ports are used for each endpoint.

For C-Line creation, the NSD supports the 7x50 and 7705 SAR NE types. Third-party vendor NEs are supported via MDM.

The C-Line service creation requires you to specify a type of VC (pseudowire). The options are:

- SAToP T1 (unstructured DS1)
- SAToP E1 (unstructured E1)
- CESoPSN (structured)
- CESoPSN CAS (structured with CAS)

You can use pre-configured channel groups or the NSD can auto-create channel groups as part of service creation. When channel groups are auto-created, the channel group ID will be the first timeslot.

Note: The number of timeslots in the channel groups must match in order to create a C-Line using the channel groups. For unchannelized endpoints, specifying the timeslots is not required.

The following behavior applies to NFMP-mediated C-Lines:

- If there is an existing channel group that uses the full set of specified timeslots, that channel group will be used for the C-Line endpoints.
- If the existing channel group is used by an existing service, the validation fails with a warning that the channel group is already being used by an existing service.
- If a channel group with all the specified timeslots does not exist, a new channel group with the specified timeslots will be configured.
- When configuring a new channel group, if one or more timeslots are already being used by other channel groups, validation fails with a warning saying that the timeslot is being used by another channel group.
- If the C-Line reuses existing channel groups, and if the channel group ID is not the first timeslot, a validation error is not triggered and the NSD will use that channel group regardless.
- If the channel group parameters configured on the endpoint of the C-Line do not match those on the existing channel group, the NSD will change the parameters of the channel group to match what is specified on the C-Line endpoint.
- If a C-Line service that was created using the NSD is deleted, the NSD will delete the channel groups that are in use.

1.22.1 What are brownfield C-Line services?

C-Line services created within the NFM-P can be managed by the NSD. In order for the NSD to discover these services, their "NSD-managed" flag must be enabled within the NFM-P. Once discovered by the NSD, these services function the same way as C-Line services created within the

NSD, provided that they meet the NSD requirements. Any change made to these services within NFM-P after discovery is propagated to the NSD if the change impacts the topology of the service.

Note: The C-Line services created within the NFM-P have an “Auto-delete” flag. When enabled, services without service sites are automatically deleted. This flag must not be enabled on services managed by the NSD, as the “NSD-managed” flag is disabled upon service deletion, and remains so even if the service is recreated and resynchronized into the NSD.

1.23 How do I provision C-Line services?

You can create and modify a C-Line service using a Properties form that is enabled by default. The Properties form shows all fields at once. Default values appear in the fields, if applicable. You can switch back and forth between the Properties form and the Service Builder using the icons in the top right corner. The icons are available only after you click **CREATE A SERVICE** and select a template. The Service Fulfillment application will remember your setting until the browser history is cleared.

1

Click on the **SERVICES** tab and then click **CREATE A SERVICE** in the top right corner.

Select a template

2

From the **Select a template to start** drop-down menu, choose the type of service you want to create, or choose All Templates to see a list of all preconfigured templates.

Choose the default template or a preconfigured template from the list. Recently used templates are shown in the right panel.

You can also search for a template in the search field.

Identification

3

Type a Service Name for your service.

You can edit the customer ID, template, and description. If the template is changed after you configure the sites and endpoints, the site and port selections are not saved and you must select and configure the ports again.

Characteristics

4

Configure the parameters, as required.

Parameter	Description
Tunnel Profile	Specifies the Tunnel Profile to apply to the service.
Include RTP Header	Enables the inclusion of CEM RTP across the IP/MPLS core network.
Admin State	Specifies the initial administrative state of the service on deployment
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined.
Maximum Hops	Specifies the maximum number of hops to consider.
Maximum Latency	Specifies the maximum latency to consider.
Maximum Cost	Specifies the maximum cost to consider.
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
MTU	Specifies the MTU for the service. The range is 0 to 9194.
VC Type	Specifies the type of VC (pseudowire).

Sites and Endpoints

5

Click **SELECT PORTS** to display the list of available ports. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.

6

Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.

Perform this step to select additional ports, as required.

7

Click **DONE** after selecting the ports.

8

Configure the required endpoint parameters.

Parameter	Description
Description	Specifies a description for the endpoint.
Admin State	Specifies the current administrative state of the endpoint.
Time Slots	Specifies the range of time slots to be used by the channel group or endpoint.
QoS Profile Name	Specifies the QoS Profile to be used. You can only assign a Generic QoS policy to a service endpoint if any one of the ingress and egress associated policies (if assigned) within the Generic QoS policy already exist on the NE.

9

If a QoS Profile was specified in the previous step, click **SHOW** to view the QoS settings applied by the profile.

10

Perform one of the following tasks:

a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.

END OF STEPS

1.24 What are L3 VPN services?

The NSD supports the creation of L3 VPN services. L3 VPN services utilize layer 3 VRF (VPN/ virtual routing and forwarding) to routing tables for each customer utilizing the service. The customer peers with the service provider router and the two exchange routes, which are placed into a routing table specific to the customer. Multiprotocol BGP (MP-BGP) is required to utilize the service.

The RD and RT is auto-generated as per policy direction and the topology type selected. Other parameters specified in the referenced template complete the service definition. Other parameters of the L3 VPN service are obtained from the specific templates referenced in the abstract API definition. The service definition in the abstract API, the detailed configuration in the service templates, and other network and tunnel parameters form the complete service definition, which is represented in the normalized model for L3 VPN. Specific configurations based on the devices are

then constructed and deployed using NFM-P. L3 VPN services can use service tunnels that were not created using the Service Fulfillment application.

The discovery and deployment of a hub-and-spoke L3 VPN service where two hubs are configured for redundancy is supported on NFM-P and MDM managed NEs. Redundancy is achieved by having the hubs advertise the same import/export routes with a unique route distinguisher. This feature is not supported on Wavence SM NEs.

The Service Fulfillment application allows you to configure the properties on each hub-and-spoke L3 VPN service site. You can also configure one or more SAPs on an L3 VPN service site.

Note: Before provisioning L3 VPN services using the NSD, you must have MP-BGP configured and working between the PE nodes to support IP VPN. The Peer CE nodes must also be configured. Only one AS is supported per provider.

1.24.1 What are multi-domain L3 VPN services?

For L3 VPN services, the NSD supports the RSVP-TE option, since multi-vendor nodes do not support SDP tunnels. As a result, if an L3 VPN service is created on a multi-vendor node, the NSD algorithm tries to find or to create RSVP-TE tunnels and always sets the auto-bind property to RSVP-TE on the multi-vendor nodes.

1.24.2 What are multi-domain L3 VPN services from L2 endpoints?

Multi-domain L3 VPN services from L2 metro areas are supported. These services are created between PE routers on metro areas. However, because some PE routers are not L3 capable, the NSD performs the path search across the network, from L2 metro areas to L3 core, and finds the best exiting routers from metro to core. Then, the NSD provisions L2 E-Line services on all metro areas and L3 VPN services in the core. Finally, the services are stitched together by the NSD using VLAN hand-off.

The intra-domain tunnels must be created in advance, and all metro domains are interconnected via Ethernet links (VLAN handoff) to the core. Since none of the routers on L2 metro domains are L3 VPN capable, the NSD uses this property to run the path search algorithm. This property can be set using the NSP's REST APIs.

The NSD uses L2 and L3 service templates to define the common attributes for the auto-created services. Profiles are used for QoS and the auto-assignment of L3 RD/RT. The NSD also uses the tunnel selection profile to include and exclude specific tunnels during path search. The path search objectives (such as minimizing hop or cost) and other values specific to the VPN (such as the IP addresses of the L3 access points) are defined either from the Service Fulfillment application or the NSP REST APIs. The NSD uses the QoS CIR values to book the bandwidth on tunnels.

1.24.3 Can I create L3 VPN services on Wavence SM NEs?

The NSD supports the creation of L3 VPN services on Wavence SM NEs that support L3 VPN through SNMP. To create such a service in the Service Fulfillment application, choose L3 VPN as the service type and then select endpoints that are already configured on Wavence SM NEs.

L3 VPN configuration supports:

- Service provisioning between Wavence SM NEs
- Service provisioning between SR and Wavence SM NEs

Static LSP based L3 VPN configuration

During service creation within a Wavence domain, the NSD will create all static LSPs needed to fulfill the service. Static routes configured in the domain, along with physical topology, will determine the feasibility of the static LSP path. The NSD will also configure all labels along the LSP path and ensure there are no duplicates. The NSD will cache all labels used by current LSPs to ensure they are not reused during provisioning. The NSD will not re-route these LSPs after they are created.

The Service Fulfillment application supports only the configuration of greenfield static LSP based L3 VPN services.

Note: You can create a full mesh or Hub and Spoke service using IPv6 as the Primary IP Address within a Wavence domain.

SR-OSPF based L3 VPN configuration

During service creation within a Wavence domain, the NSD will create only SR-OSPF enabled service tunnels. Since OSPF based configuration of dynamic LSPs is already discovered in the NFM-P, the creation of LSPs is not required to fulfill the service.

The Service Fulfillment application supports only the configuration of greenfield SR-OSPF based L3 VPN services.

Note: Only IPv4 configuration is supported for SR-OSPF based L3 VPN services.

When you create an L3 VPN service on Wavence SM NEs in the Service Fulfillment application, take into account the following considerations:

- Both Full Mesh and Hub and Spoke topology types are supported. When Hub and Spoke is selected, the NSD will automatically assign ingress and egress labels on the spoke SDP bindings.
- In the service's advanced properties, set the Auto Bind parameter to None.
- On each service endpoint, configure the Outer Tag, Primary IP Address, and GQP parameters. If required, also configure the Static Route, Next Hop and Preference parameters associated with the Primary IP Address.

When the Full Mesh topology type is selected, the Service Fulfillment application will automatically configure static routes on all endpoints to achieve the required mesh topology.

When the Hub and Spoke topology type is selected, the Service Fulfillment application will automatically configure the black hole static routes on all spoke sites to prevent traffic between them. Default route static routes will also be automatically configured on Spoke endpoints with the next hop being the Hub endpoint.

Note: Only one hub endpoint can be configured, regardless of topology type. This hub endpoint must be configured in the SR domain.

Static LSP based L3 VPN configuration and SR-OSPF based L3 VPN configurations cannot co-exist.

SAP endpoints are in access mode and do not support network mode.

1.24.4 Can I create composite L3 VPN services?

The NSD supports the creation of a composite L3 VPN service across multiple domains of Wavence SM NEs without MP-IBGP and one domain of 7x50 SR NEs with MP-IBGP.

A physical link (VLAN uplink) is required between access ports on the adjacent Wavence SM and 7x50 SR that connect the two domains.

To be able to create a composite L3 VPN service, you must perform pre-configuration tasks on all Wavence SM and 7x50 SR NEs that are part of the service, and on the NFM-P.

Configuration in the Wavence SM NE domain:

- Provision static LSPs between all the Wavence SM NEs

Configuration in the 7x50 SR domain

- Create an L3 VPRN service with service tunnels between all the 7x50 SR NEs. IGP, MPLS (RSVP-TE or LDP) and MP-IBGP must be configured on the NEs.

Configuration on the NFM-P

- Create a physical link between network ports on the Wavence SM NEs.
- Create a physical link between network ports on the adjacent Wavence SM NE and 7x50 SR NE that connect the two domains.

  If the physical links are not present, then the L2 service fails to deploy.

To configure a composite L3 VPN service successfully, apply the following guidelines during the service creation:

- Set the Tunnel Type to None. The composite service does not support a specific tunnel type across the two domains.

During the service creation, the NSD performs the following tasks automatically:

- Provisions both local and remote static routes to configure the service level (VRF) route table on each Wavence SM NE.
- Provisions static routes on each end of the physical link (VLAN uplink) to enable the inter-domain IP routing.
- Creates two L3 internal service endpoints, one on each side of the physical link.

1.25 How do I provision L3 VPN services?

1

Click on the **SERVICES** tab and then click **CREATE A SERVICE** in the top right corner.

Select a template

2

From the **Select a template to start** drop-down menu, choose the type of service you want to create, or choose All Templates to see a list of all preconfigured templates.

Choose the default template or a preconfigured template from the list. Recently used templates are shown in the right panel.

You can also search for a template in the search field.

Name and define the service

3

Type a Service Name for the L3 VPN service.

You can edit the service type and the template. If the template is changed after you configure the sites and endpoints, the site and port selections are not saved and you must select and configure the ports again.

Set the service parameters

4

Click **ADDITIONAL PROPERTIES** to configure the service parameters.

Parameter	Description
Description	Describes the service.
Customer ID	The customer ID is associated with a newly created service. If a customer ID is not provided during service creation, the customer ID provided by the associated service template will be used. If no customer ID is found, the default customer ID of 1 will be used. The customer ID applies only to SR NEs.
Tunnel Profile	Specifies the Tunnel Profile to apply to the service.
Path Profile	Specifies a path profile for the service.
Admin State	Specifies the current administrative state of the service
Bidirectional	Specifies whether or not a return path is required, and if so, what type of return path should be determined.
Objective	Specifies the primary goal when identifying resources and/or paths for service creation. Select one of the following options: Latency, Hops (Span) or Cost.
Encryption	Specifies whether or not IP VPN encryption is enabled.
Tunnel Type	Specifies the type of tunnel to be used by the L3 VPN service.

Parameter	Description
MTU	Specifies the MTU for the service. The range is 0 to 9194
Maximum Hops	Specifies the maximum number of hops to consider
Maximum Latency	Specifies the maximum latency to consider
Maximum Cost	Specifies the maximum cost to consider

5

Click **OK**. The Additional Properties form closes.

6

Click **CONTINUE**. The service configuration focus moves to the endpoint configuration area.

Add the endpoints

7

Select the Topology Type for the service. Your topology type selection (Full Mesh or Hub and Spoke) determines the endpoint selection.

Note: If Hub and Spoke is selected, multiple spoke endpoints for this service can be configured on the same node. You can configure multiple hubs for redundancy purposes, with one or more endpoints on each hub.

8

Select the service endpoints.

1. Click **SELECT PORTS** to display the list of available ports.
2. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.
3. Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.

   Perform this step to select additional ports, as required.
4. Click **DONE** after selecting the ports.
5. If required, click **VIEW ENDPOINT LIST** to display the list of selected endpoints. To return to the map view, click .

9

Click **CONTINUE**. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

10

Click on the endpoint entry. The endpoint configuration form opens.

11

Configure the required endpoint parameters.

Note: The endpoint configuration supports both IPv4 and IPv6 addresses.

Parameter	Description
Description	Describes the endpoint configuration.
VRF Name	Specifies the service name of the VRF spoke or hub site on the NE. All spoke or hub endpoints with the same VRF Name will be deployed on the same VRF. **Note:** If two hub-and-spoke L3 VPN services are configured on the same NE, the hub-and-spokes cannot have the same VRF Name.
Interface Name	The name of the service interface. Maximum of 32 characters. Must begin with a letter.
Admin State	Specifies the current administrative state of the endpoint.
Outer Tag	Specifies the outer tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
Inner Tag	Specifies the inner tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
Primary IP Address	Specifies the primary IP address assigned to the service endpoint.
Secondary Addresses	Add as many valid IP addresses as required using the Add (+) icon.
Static Routes	Add as many static routes as required using the Add (+) icon. Specify the destination network IP address and subnet mask of the static route assigned to the service endpoint.
eBGP Peers	Add as many eBGP peers as required using the Add (+) icon, and specify the IP address and the AS for each eBGP peer.
QoS Profile Name	Specifies the QoS Profile to be used. You can only assign a Generic QoS policy to a service endpoint if any one of the ingress and egress associated policies (if assigned) within the Generic QoS policy already exist on the NE.

12

If a QoS Profile was specified in the previous step, click **SHOW QOS SETTINGS** to view the QoS settings applied by the profile.

13

Click **SAVE**. The endpoint configuration form closes.

Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

14

Click **CONTINUE**. The system displays the service configuration summary so that you can review it.

Review your service

15

Review the service configuration summary. Click  to view the service representation in the map.

Save or deploy your service

16

Perform one of the following tasks:

a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.

c. If you need to modify the service configuration, click **BACK** to go to previous service configuration steps, as required.

d. If you applied an L3 VPN service template to this service, and you enabled the Add Trigger for Validation Workflow in Creation Form parameter in the L3 VPN service template, a Validate button is available. Click **VALIDATE** to run the workflow and validate the service configuration.

END OF STEPS

1.26 What are IES services?

An IES is a routed connectivity service in which the customer traffic passes through an L3 IP router interface to the Internet. IES allows customer-facing IP interfaces in the same routing instance to be used for service network core-routing connectivity. IES requires that the IP addressing scheme that

is used by the customer be unique among other provider addressing schemes and potentially the entire Internet. Packets that arrive at the edge device are associated with an IES based on the access interface on which they arrive. An access interface is uniquely identified using:

- port
- service ID
- IP address

The Service Fulfillment application groups MDM IES service sites based on common Global-IDs supplied by the MDM adaptors. When any service sites have at least one common Global-ID, the service sites will be grouped into a single service. If a Global-ID linking the sites together is removed, the service will be split into multiple services.

1.27 How do I provision IES services?

1

Click on the **SERVICES** tab and then click **CREATE A SERVICE** in the top right corner.

Select a template

2

From the **Select a template to start** drop-down menu, choose the type of service you want to create, or choose All Templates to see a list of all preconfigured templates.

Choose the default template or a preconfigured template from the list. Recently used templates are shown in the right panel.

You can also search for a template in the search field.

Name and define the service

3

Type a Service Name for the IES service.

You can edit the service type and the template. If the template is changed after you configure the sites and endpoints, the site and port selections are not saved and you must select and configure the ports again.

Set the service parameters

4

Click **ADDITIONAL PROPERTIES** to configure the service parameters.

Parameter	Description
Description	Describes the service.

Parameter	Description
Customer ID	The customer ID is associated with a newly created service. If a customer ID is not provided during service creation, the customer ID provided by the associated service template will be used. If no customer ID is found, the default customer ID of 1 will be used. The customer ID applies only to SR NEs.
Admin State	Specifies the current administrative state of the service
MTU	Specifies the MTU for the service. The range is 0 to 9194

5

Click **OK**. The Additional Properties form closes.

6

Click **CONTINUE**. The service configuration focus moves to the endpoint configuration area.

Add the endpoints

7

Select the service endpoints.

1. Click **SELECT PORTS** to display the list of available ports.
2. If required, use the drop-down menu and the text box at the top of the list to filter the ports by a list of available attributes.
3. Select a port: move the mouse pointer to the right of the port entry and click the applicable selection icon.

   Perform this step to select additional ports, as required.
4. Click **DONE** after selecting the ports.
5. If required, click **VIEW ENDPOINT LIST** to display the list of selected endpoints. Click **VIEW SERVICE MAP** to return to the map view.

8

Click **CONTINUE**. The system checks the selected endpoints and informs you that the endpoint is missing required values. You need to perform additional endpoint configuration.

9

Click on the endpoint entry. The endpoint configuration form opens.

10

Configure the required endpoint parameters.

Note: The endpoint configuration supports both IPv4 and IPv6 addresses.

Parameter	Description
Description	Describes the endpoint configuration.
Interface Name	The name of the service interface. Maximum of 32 characters. Must begin with a letter.
Admin State	Specifies the current administrative state of the endpoint
Outer Tag	Specifies the outer tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
Inner Tag	Specifies the inner tag. Applicable to ports with encapsulation type Dot1Q or QinQ.
Primary IP Address	Specifies the primary IP address assigned to the service endpoint.
Secondary Addresses	Add as many valid IP addresses as required using the Add (+) icon.
Static Routes	Add as many static routes as required using the Add (+) icon. Specify the destination network IP address and subnet mask of the static route assigned to the service endpoint
eBGP Peers	Add as many eBGP peers as required using the Add (+) icon, and specify the IP address and the AS for each eBGP peer.
QoS Profile Name	Specifies the QoS Profile to be used You can only assign a Generic QoS policy to a service endpoint if any one of the ingress and egress associated policies (if assigned) within the Generic QoS policy already exist on the NE.

11

If a QoS Profile was specified in the previous step, click **SHOW QOS SETTINGS** to view the QoS settings applied by the profile.

12

Click **SAVE**. The endpoint configuration form closes.

Perform the additional configuration steps for each service endpoint. When all the service endpoints are correctly configured, continue to the next step.

13

Click **CONTINUE**. The system displays the service configuration summary so that you can review it.

Review your service

14

Review the service configuration summary. You can click to view the service representation in the map.

Save or deploy your service

15

Perform one of the following tasks:

a. If the service configuration is correct, click **DEPLOY**. The system attempts to deploy the service, and displays a message to inform you that the service was successfully created or that there are service configuration errors. Investigate the errors, correct the service configuration and deploy the service again.

b. If you want to save the service without deploying it, click **SAVE**. A saved service does not reserve any bandwidth and network resources, and the system checks the availability of resources for a saved service only at deployment time.

c. If you need to modify the service configuration, click **BACK** to go to previous service configuration steps, as required.

d. If you applied an IES service template to this service, and you enabled the Add Trigger for Validation Workflow in Creation Form parameter in the IES service template, a Validate button is available. Click **VALIDATE** to run the workflow and validate the service configuration.

END OF STEPS

1.28 Can I create services on SDPs with multiple loopback IP addresses?

The NSD supports the configuration of services on SDP tunnels using a loopback IP address as either the source or destination IP address when routing services. A potential benefit of having services on SDP tunnels using a loopback IP address is the ability to configure routing on tunnels established on different paths between two NEs. However, you can configure such services only on brownfield SDP tunnels that were created in the NFM-P or on NEs. The NSD does not support the creation of new service tunnels using loopback IP addresses.

Before you start configuring a service in the NSD, you must create SDP tunnels with loopback IP addresses in the NFM-P or on the NE. The following list captures the high-level configuration tasks required for each NE.

- Configure the loopback interfaces on routers.

- Configure peers on the targeted LDPs. Use the loopback interface name as the local-lsr-id option and enable tunneling to enable LDP over the tunnels.
- Configure the SDP tunnels using the loopback interface IP addresses for the service far end. Optionally, you can apply a steering parameter to the tunnel to help the selection of the correct SDP tunnel when creating the service.

The service tunnels that you created can be viewed in the Service Fulfillment application, on the INVENTORY tab. The service tunnel Destination IP is the IP address of the loopback interface and the service Transport type is MPLS.

If you applied the optional steering parameter to the tunnel, then you can also create a tunnel selection policy for the steering parameter in the Policy Management application.

1.29 How do I find and edit a specific service?

You can modify and save the Service Name of any service type which already exists in the SF application, including services that were deployed from Service Fulfillment, brown-field discovered services, or a combination of both.

1

On the **SERVICES** tab, use the Service List drop-down menu to navigate to the **Dashboard** page. Click in the **Find a service** field. The system displays a drop-down list of existing services.

If you know the service name or part of it, start typing it in the **Find a service** field. The system filters the list of services and shows only the service names that contain the characters that you typed.

2

Click on a service. The system displays general information about the service in the Service Info panel and highlights the service on the map.

3

Click **EDIT** at the bottom of the Service Info panel. The Edit Service page opens.

You can modify the service name, service properties, and endpoints.

4

Click **UPDATE**. The Service Fulfillment application saves the modifications.

END OF STEPS

1.30 How do I find services that are using a specific endpoint?

1

Click on the **INVENTORY** tab, and then click **Service Endpoints**. The application displays a list of existing endpoints.

2

Specify an endpoint in the Endpoint Name field to list all services that are using that endpoint.

You can filter the endpoints using the available attributes. For example, use the Port Name field to filter the list by the physical port name.

END OF STEPS

1.31 How do I view, edit, or delete a service?

You can modify and save the Service Name of any service type which already exists in the SF application, including services that were deployed from Service Fulfillment, brown-field discovered services, or a combination of both.

1

Click on the **SERVICES** tab. The **Service List** displays a list of all created services.

2

Choose from the following:

a. To view a service, select it from the list. The system displays general information about the service in the Info panel.

b. To edit or view information about a service, point to the service and click one of the following:

- **Edit**
  The Edit Service page opens. You can modify the service name, service properties, and endpoints.
  When you have made your modifications, click UPDATE. The Service Fulfillment application saves the modifications and deploys the service.
- **View Service Map**
  The Service Map opens with information about the service in the Service Info panel. Click **More Details** at the bottom of the info panel to see additional information. You can hover over the map elements to view information about the NE and its components. From the service map, you can click **Edit Service** in the top right corner of the dashboard. Click **More** **Open in Service Supervision** to display the service in the Service Supervision application. For details about the tasks that you can perform on the service, see the documentation for the Service Supervision application. You can also delete the service from the **More** menu.
- **View Components**
  The Service Components page opens. Use the Service Endpoints drop-down menu to view service endpoints, service tunnels, or physical links associated with the service. Click on a component to view details about it in the Info panel.
- **More** **Open in Service Supervision**
  The service is displayed in the Service Supervision application. For details about the tasks that you can perform on the service, see the documentation for the Service Supervision application.
- **More** **Hide Info Panel / Show Info Panel**

Use this option to show or hide the Info panel.

- **More ⋮ Delete**
  The system prompts you to confirm your choice and then deletes the service.

c. To delete a service or services, select the service and click **More ⋮ Delete**. Use the Shift or CTRL key to select multiple services and then click **Delete selected** in the top right corner.
   The service or services are deleted.

END OF STEPS

1.32 What are brownfield service tunnels?

Brownfield service tunnel are tunnels created previously in the NFM-P that you can discover and then use with services created using the Service Fulfillment application.

You can modify the parameters of a discovered brownfield service tunnel in the Service Fulfillment application. This enables you to support services with bandwidth booking in the core and to restrict or to allow for consumption, modification and deletion in a different way from how the service tunnels were discovered.

1.33 How do I manage service tunnel bandwidth?

Note: You must perform the bandwidth management tasks on the service tunnel for both tunnel directions.

1

Click on the **INVENTORY** tab, and then click **Service Tunnels** to display a table with the available service tunnels.

2

Search for the service tunnel that you need to manage.

You can filter the service tunnels displayed in the list by Tunnel Name, Source IP, Destination Node, Transport type, Bandwidth, and Available Bandwidth. Type numbers or characters, or both, in the search boxes and the system filters dynamically the services that meet your criteria.

3

Click on a service tunnel to display information about it in the Info panel.

4

Click **Edit** . The Manage Service Tunnel form opens.

5

Modify the bandwidth management parameters of the service tunnel, as required:

- Consumable

Controls whether or not the tunnel can be used for creating services in the NSD and NRC. This parameter is enabled by default. Disable the Consumable parameter to prevent the services created in the Service Fulfillment application from using the service tunnel.

- Auto Modifiable

  This parameter allows you to give the NSD and NRC full control of the available bandwidth on the service tunnel. When you enable the Auto Modifiable parameter, the NSD and NRC calculates the available bandwidth automatically and, as a result, the Available Bandwidth parameter is not modifiable anymore. Now the NSD and NRC treat the brownfield service tunnel as a green field tunnel, except the tunnel cannot be deleted in the NSD and NRC.

- Available Bandwidth

  This parameter allows you to set how much bandwidth is available to the NSD and NRC to use on a brownfield service tunnel. Then you must use the same bandwidth values when creating a service that uses the service tunnel. When the service is deleted, the available bandwidth on the service tunnel reverts to the previous value.

6

Click **SAVE**. The service tunnel modifications are saved.

END OF STEPS

1.34 How do I enable NSD management on services created using NFM-P?

The NSD can manage a service that was created using NFM-P if the following conditions are met:

- The NSD supports the service type.
- The service's NSD Managed parameter is enabled within NFM-P.

A service created using NFM-P and discovered in the NSD functions the same as a service created in the NSD. Any change that impacts the topology of the service made in the NFM-P after discovery is propagated to the NSD.

This procedure describes how to enable the NSD Managed parameter for a service in the NFM-P:

1

Choose **Manage→Service→Services** from the NFM-P main menu. The **Manage Services** form opens.

2

Click **Search** and choose a service.

The following table maps the service names defined in the NFM-P to the corresponding NSD service names.

NFM-P service	NSD service
CPIPE	C-LINE

NFM-P service	NSD service
EPIPE	E-LINE
VPLS	E-LAN
VPRN	L3 VPN

3

Enable the check box in the NSD Managed column for the selected service.

4

Save your change and close the form.

END OF STEPS

1.35 How do I augment services, sites, or endpoints?

In order to deploy IP services to NFM-P, NSD uses NFM-P templates that are installed into NFM-P during NSD installation. The use of these templates are hard-coded in NSD, however, the NSD service definition is very abstract and models only a small subset of available attributes on the network elements. As a result, you cannot configure certain attributes from the Service Fulfillment application that would otherwise be available from the NFM-P GUI.

The following workflow can be used to augment NSD services, sites, and endpoints such that additional attributes can be configured from the Service Fulfillment application.

1

Create one or more json files that define the additional attributes to be made accessible from the Service Fulfillment application, and store them in the NSD database. For an example of how the files should be written, see the *NSP DevOps Portal*.

2

Use the GET /v4/mediation/augmentation-meta/ API command to create an augmentation meta. The *pathName* (specifies the entity to be augmented), *templateName* (specifies the custom NFM-P system script that will be used to interpret the additional attributes), and *augmentationMetaJsonFileName* (specifies the path to the json file) parameters must be configured. The *pathName* parameter supports only the following values:

- 'nsd-service:/services/elan-sites'
- 'nsd-service:/services/eline-sites'
- 'nsd-service:/services/l3vpn-sites'
- 'nsd-service:/services/ies-sites'
- 'nsd-service:/services/elan-sites/site'
- 'nsd-service:/services/eline-sites/site'
- 'nsd-service:/services/l3vpn-sites/site'

- 'nsd-service:/services/ies-sites/site'
- 'nsd-service-evpn:/services/elan-evpn-sites/site'
- 'nsd-service-evpn:/services/eline-evpn-sites/site'
- 'nsd-service:/services/elan-sites/site/endpoints/endpoint'
- 'nsd-service:/services/eline-sites/site/eline-groups/eline-group/port-endpoints/port-endpoint'
- 'nsd-service:/services/l3vpn-sites/site/endpoints/endpoint'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint'
- 'nsd-service-evpn:/services/elan-evpn-sites/site/endpoints/endpoint'
- 'nsd-service-evpn:/services/eline-evpn-sites/site/port-endpoints/port-endpoint'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint/static-routes/static-route'
- 'nsd-service:/services/l3vpn-sites/site/static-routes/static-route'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint/bgp-peers/bgp-peer'
- 'nsd-service:/services/l3vpn-sites/site/bgp-peers/bgp-peer'

3

Create a custom NFM-P template to interpret the additional attributes and install into NFM-P, as follows:

- For an example of how a custom template should be written, see the default templates located at */opt/nsp/configure/nfmpTemplates/nfmpTemplates.zip*.
- Copy the *nfmpTemplates.zip* and *install_nfmpTemplates.sh* files and Chmod 777 them.
- Execute the *su samadmin -c "bash ./install_nfmpTemplates.sh"* command and wait for the nfmp log message “Script complete”.
- Verify that your custom script is returned using the GET /sdn/api/v4/template/nfmp-template API command.

4

From the Policy Management application, create a new mediation profile that includes the newly-created custom NFM-P script. Access the Policy Management help page from the NSP Help Center for more information about configuring mediation profiles.

5

From the Policy Management application, create a new service template that includes the newly-created mediation profile. Access the Policy Management help page from the NSP Help Center for more information about configuring service templates.

6

From the Service Fulfillment application, create a new service that uses the newly-created service template. The Service Fulfillment application retrieves augmentation data associated to this template and automatically renders the defined attributes at the service, site, and endpoint levels. The Service Fulfillment application stores the input to these fields and invokes the

custom NFM-P script defined in the service template during service creation and modification. Access the Service Fulfillment help page from the NSP Help Center for more information about configuring services.

END OF STEPS

1.36 How do I re-synchronize augmented properties?

Once additional attributes have been made accessible to the Service Fulfillment application via the above workflow, it is possible that the attributes may be modified elsewhere (such as the NFM-P GUI), resulting in incorrect displayed values within the Service Fulfillment application. To rectify this, re-synchronization augmentation scripts can be created and placed in tomcat's classpath as a jar archive which will be picked up when tomcat starts up. Alternatively, these scripts can be deployed into a configurable location in the filesystem.

The default location is */opt/nsp/configure/nfmpResyncAugmentationScripts/*. If scripts are available in both tomcat's classpath and a location in the filesystem, the filesystem version will be given preference. This is because the scripts in the filesystem can be modified without having to restart tomcat. To change the default location in the filesystem, add the following text to the sam-plugin section of the */opt/nsp/configure/config/arm-system.conf* file:

```
sam-plugin
{
  resync_augmentation_scripts_path="<custom_location>"
}
```

Where *custom_location* is the location where re-synchronization augmentation scripts will be stored.

Re-synchronization augmentation scripts should be named as follows:

```
<classname>.resync-augenmentation.js
```

Where *classname* is one of the supported NFM-P class names listed below:

- epipe.Epipe
- vpls.Vpls
- vprn.Vprn
- ies.Ies
- epipe.Site
- vpls.Site
- vprn.Site
- ies.Site
- vll.L2AccessInterface
- vpls.L2AccessInterface
- service.L3AccessInterface
- bgp.Peer

- rtr.StaticRoute

Perform the following workflow to jar the re-synchronization augmentation scripts package:

1

Execute the following commands:

```
cd opt/nsp/configure/nfmpResyncAugmentationScripts
jar cvf  ./nfmp-resync-augmentation.jar ./*.resync-augmentation.js
```

2

Copy *nfmp-resync-augmentation.jar* to sdn app's lib folder. Execute:

```
cp ./nfmp-resync-augmentation.jar
/opt/nsp/server/tomcat/webapps/sdn/WEB-INF/lib/
```

3

Restart nsp-tomcat. Execute:

```
nspdctl restart
```

END OF STEPS

2 Service Fulfillment use cases

2.1 Service creation using templates in Service Fulfillment

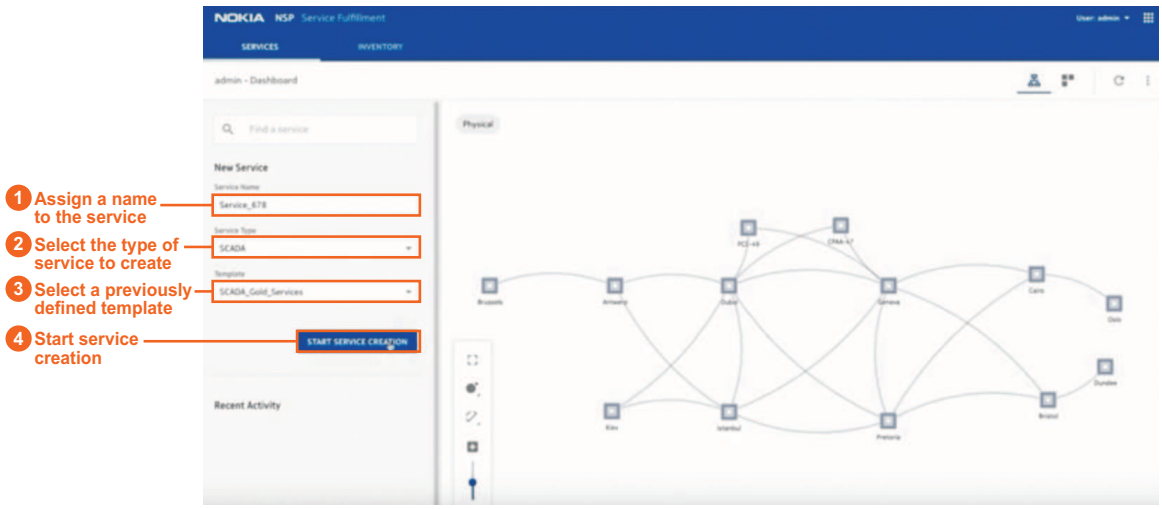
This article shows how to use the Service Fulfillment application to rapidly create a SCADA service in a hub-and-spoke topology. Service monitoring and the examination of the tunnel layers are shown.

Templates based on standard network and service configurations are used to provision the network services. Basic assurance of service correctness and connectivity is performed. This confirms that all configuration operations have been performed accurately.

Note: The images in this article show NSP Release 19.11.

2.1.1 Let's go

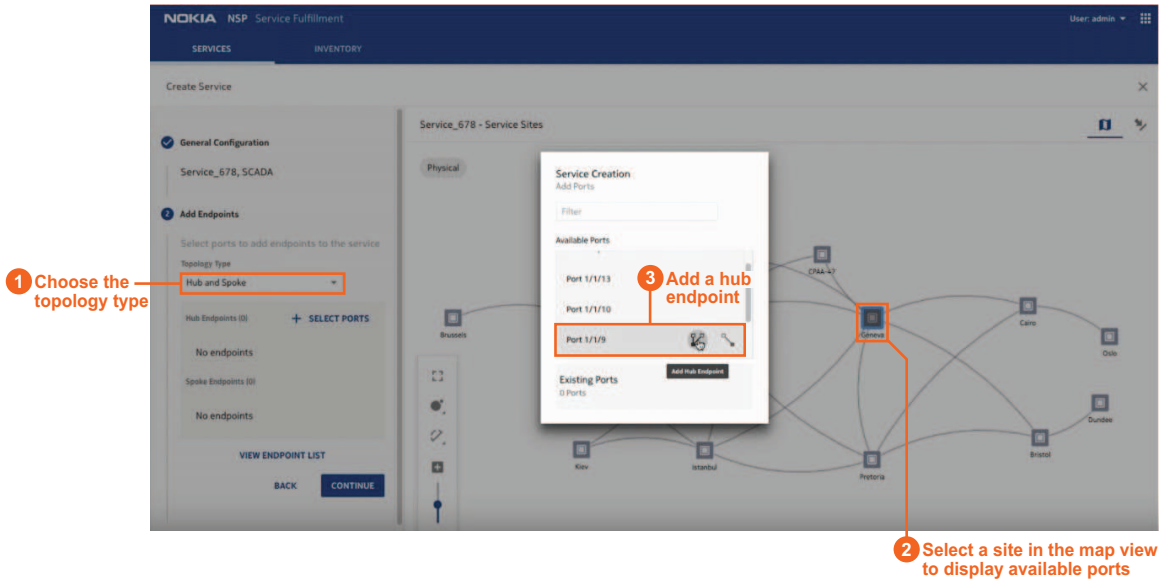
The first step is general configuration:

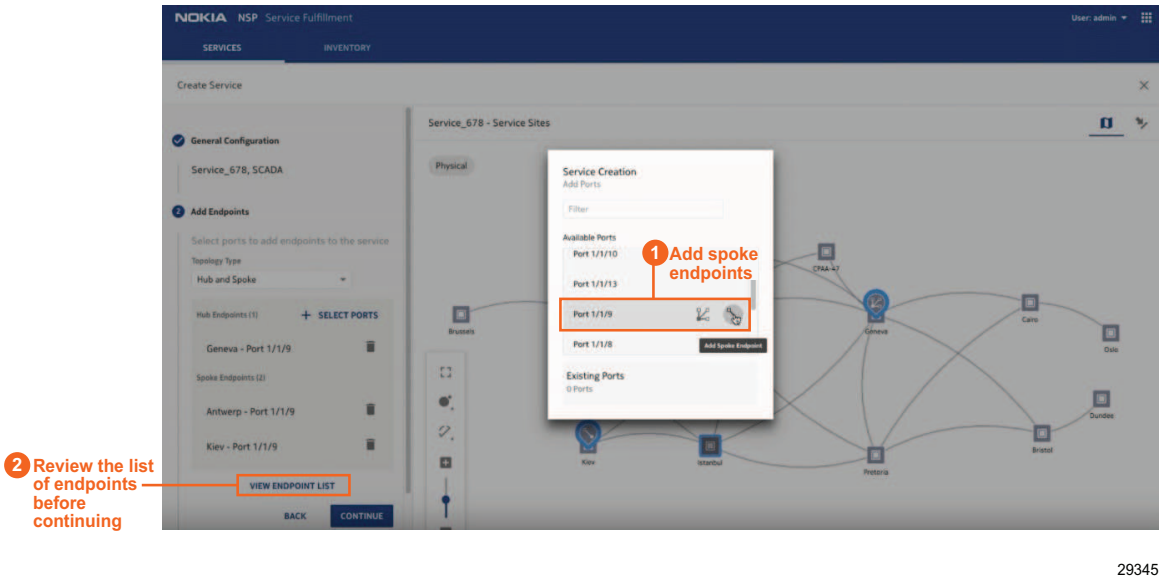


29343

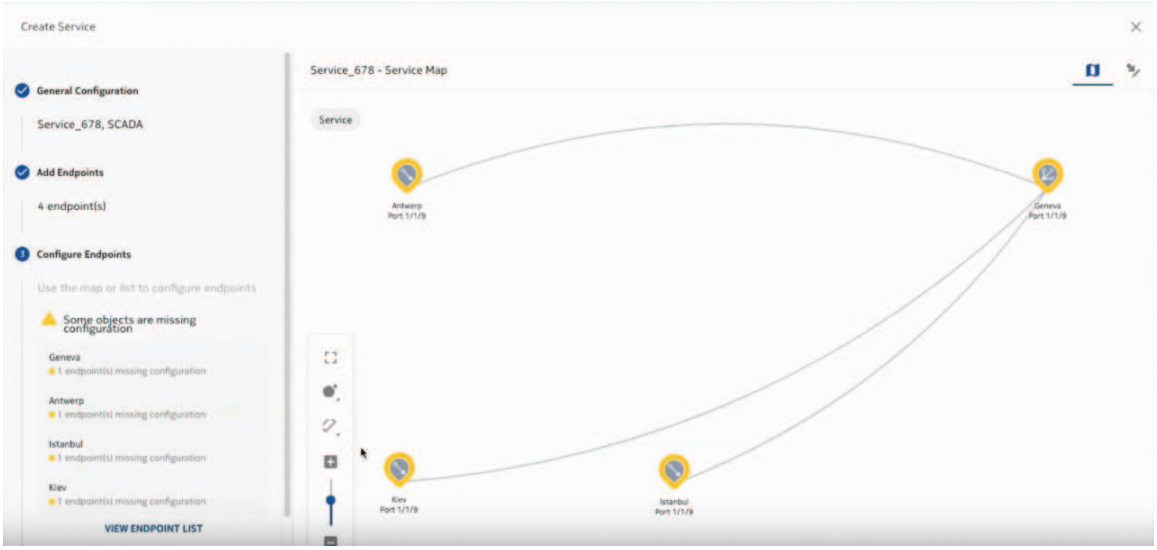
With a template, QoS settings, such as tunnel selection and routing optimization, can be defined. Details, such as latency and cost-based optimization rules, can also be specified. Using templates makes the process simple and greatly reduces human error.

Next, the endpoints are added:



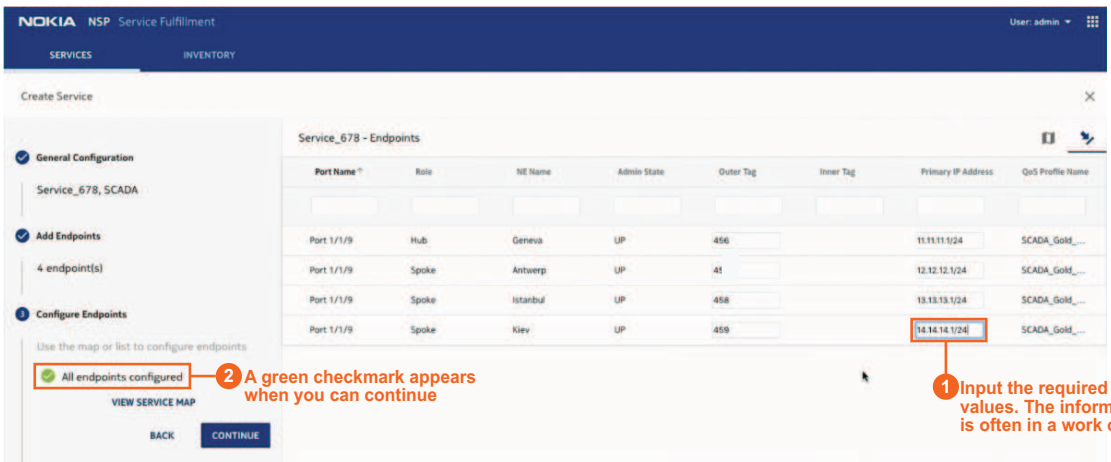


When you click **CONTINUE**, the service map displays the new service and the relationships between the selected sites. The yellow warning symbol indicates that there are missing values:



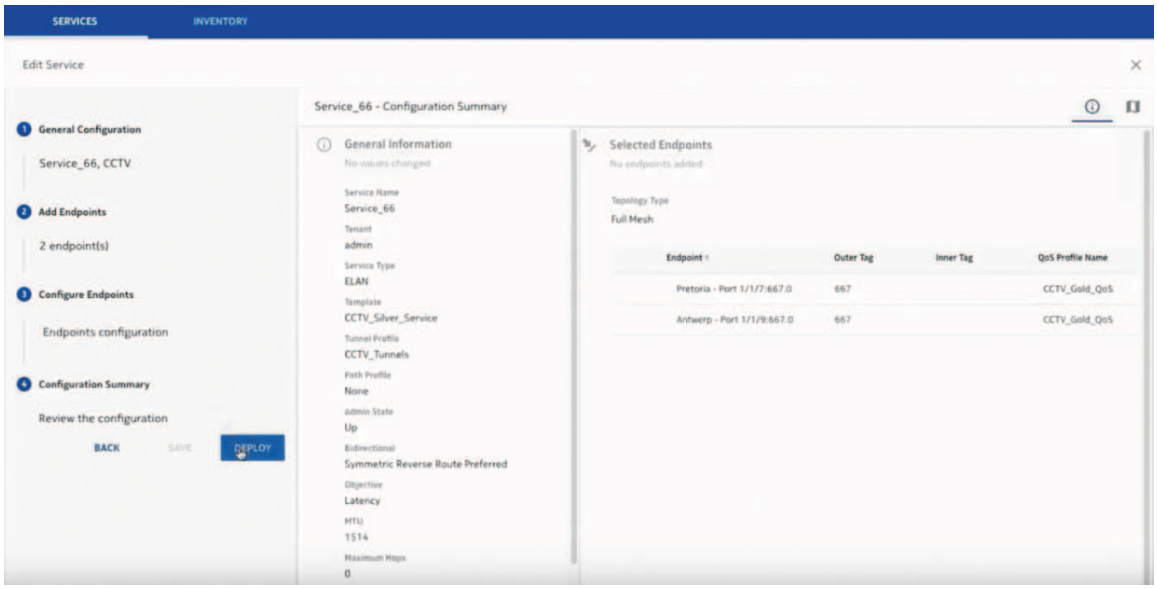
29435

To make the updates, click the list view icon to switch to the list view and input the required values:



29346

Review the summary of service information:

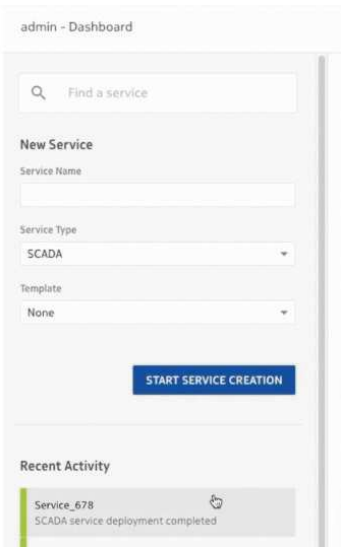


29421

You can save the service to deploy it later, or you can deploy it now.

The Service Fulfillment application will automatically find, create and select the required technologies to deploy the service.

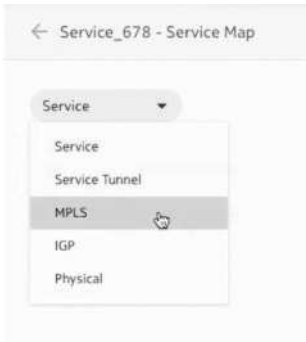
Let’s look at the successfully created service. You can open it from the Recent Activity panel:



A map of the service is displayed. If faults exist, they will appear here on the service map:

29437

All layers of the service are shown here, and can be examined for confirmation or for troubleshooting. Select a layer from the drop-down list to load the map again:

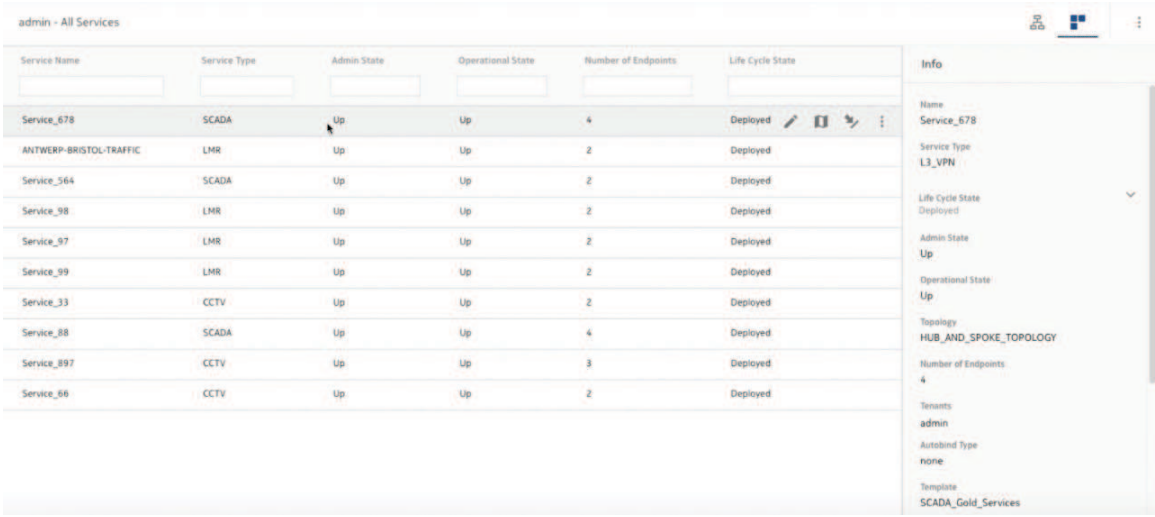


Use other tools within the NSP, such as Fault Management, to diagnose any faults.

2.1.2 We’re done

Let’s look at all the services. Return to the main dashboard and click the All Services icon .

The new service is displayed along with all the other services in this network, including CCTV, LMR, and other SCADA services:



29438

2.1.3 Where can I find more information?

- 1.18 “How do I provision E-LAN services?” (p. 15)
- 1.29 “How do I find and edit a specific service?” (p. 43)

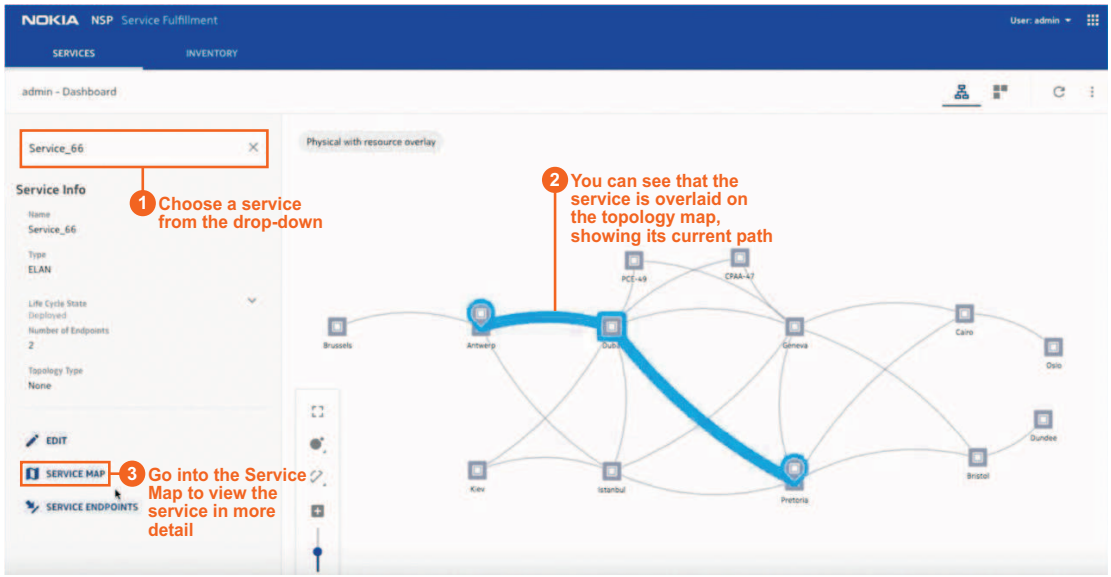
2.2 QoS modification with templates in Service Fulfillment

This article shows how to use the Service Fulfillment application to change the QoS of a CCTV transport service with predefined service templates in use.

Note: The images in this article show NSP Release 19.11.

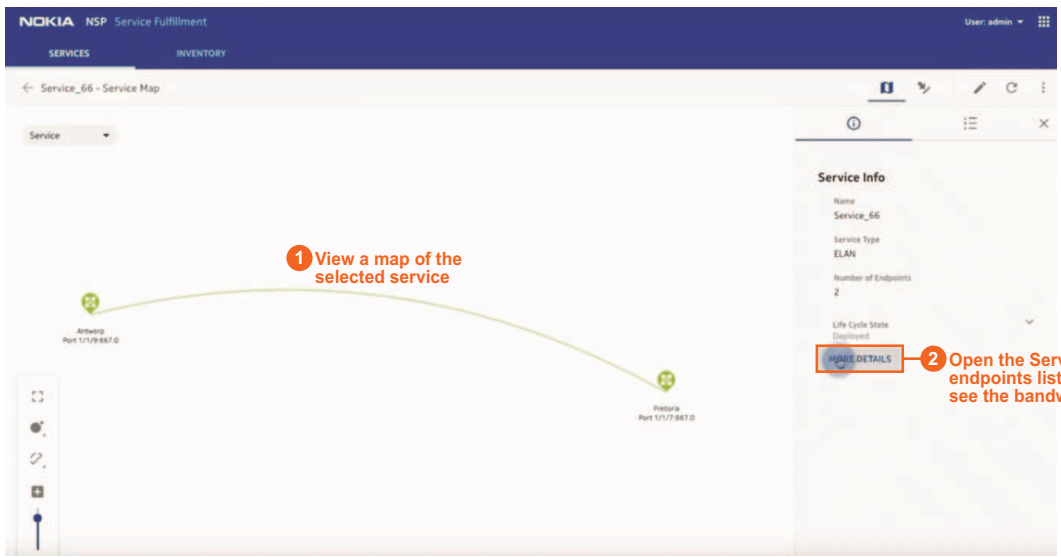
2.2.1 Let’s go

To start, let’s select an existing CCTV transport service. The service is displayed on the topography map:



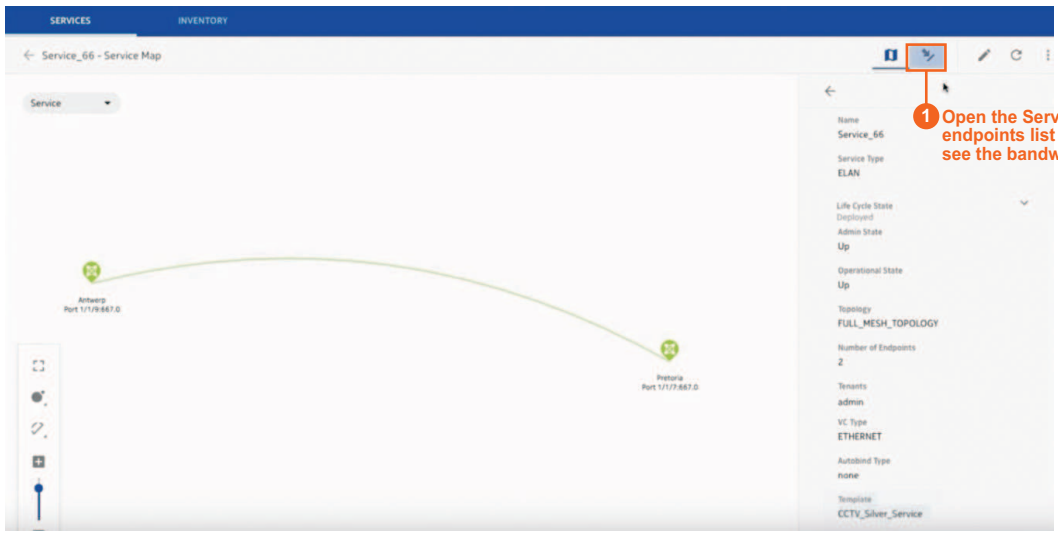
29342

The service map shows a map view of the selected service, with general service information:



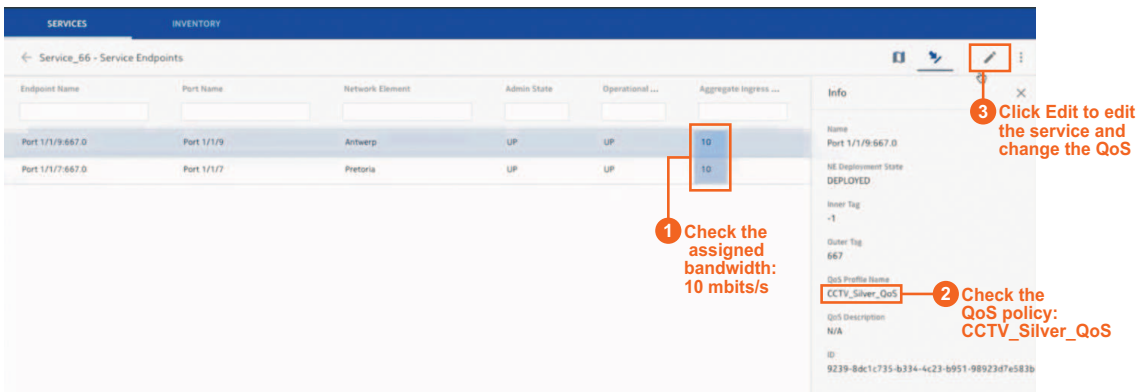
29340

The More Details screen shows the template in use:



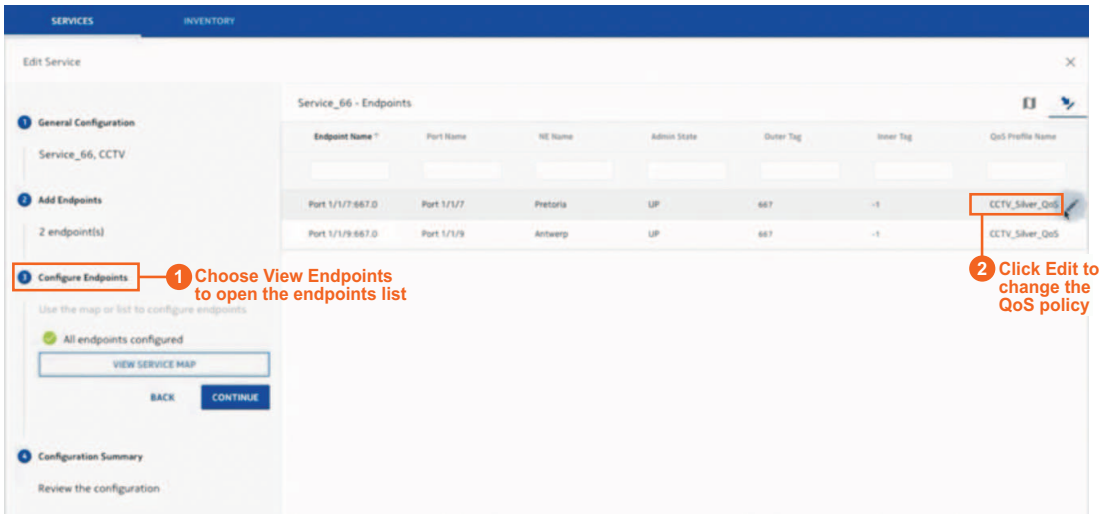
29339

The service endpoints view shows the current bandwidth of the service, and the QoS profile in use. From here, we can edit the service to change the QoS.



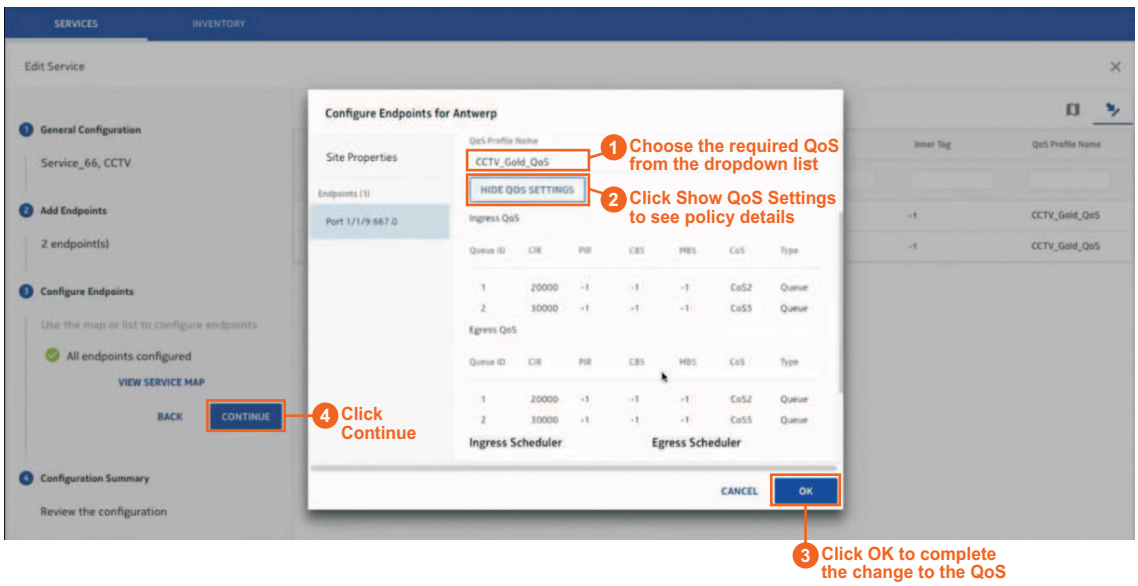
29337

From the Edit Service screen, we can change service parameters:



29336

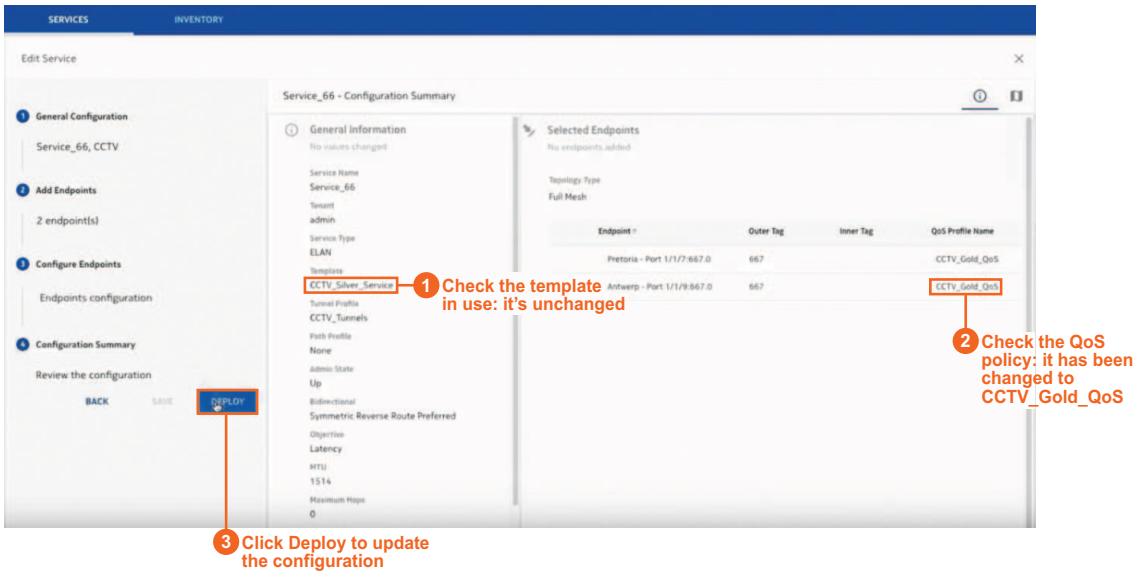
Make the changes in the Edit screen:



29335

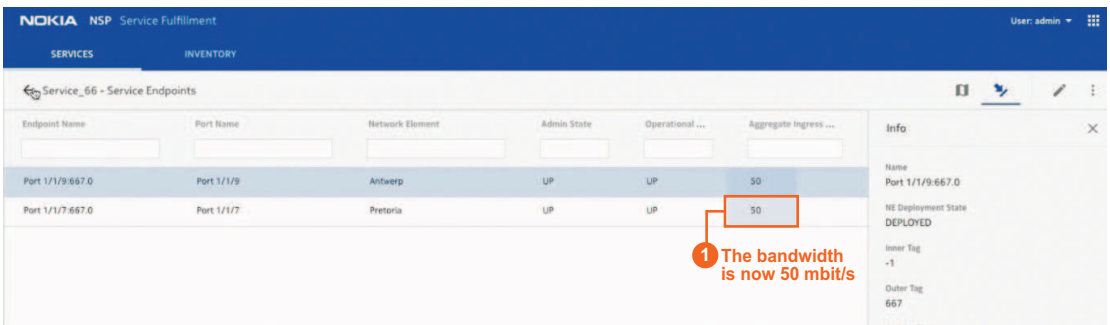
Review the configuration. You can save the changes to deploy later, or you can deploy the updated service now.

Notice that the template for defining the routing of the service has not changed, only the endpoint QoS policy has changed:



29338

When the configuration is deployed, the endpoints list shows the updated bandwidth assignment:



29341

2.2.2 We're done

The QoS has been modified. The service is still running and the route has not changed. Only the configuration of the endpoints has been modified.

2.2.3 Where can I find more information?

- 1.18 "How do I provision E-LAN services?" (p. 15)

- 1.29 “How do I find and edit a specific service?” (p. 43)