NSP
Network Services Platform
Release 25.4

Service Management Guide

3HE-21465-AAAA-TQZZA
Issue 2
January 2026

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document

Purpose

This document is intended to manage services.

Document support

Customer documentation and product support URLs:

- Documentation Center
- Technical support

How to comment

Please send your feedback to documentation.feedback@nokia.com.

1 Service Management overview

1.1 How does NSP enable service management?

1.1.1 Service management for NSP

The NSP service management function allows for service provisioning and activation across networks that are accessible to the NSP. Through the GUI, or through the northbound interface (RESTConf), NSP enables users to make service requests that deploy services to the network using the NSP's mediation framework.

A library exists with a product set of service models (such as L3 VPN, EVPN, C-Line, E-LAN, E-TREE, E-Line, and IES services) for both classic and model-mode SR OS networks. These service models can be installed and utilized by the built-in, intent-based engine (NSP's Network Intents views) to provide assurance that service configuration is completed as planned/requested, and is easily adaptable for custom service model requests. New service models that support custom needs can also be developed with the aid of the NSP's automation practice team, or if your deployment includes the NSP's programmability suite, self-development.

Note: The library of product service models (intent types) is obtained from the artifacts section of the Nokia Support Portal; however, customers should consult with Nokia prior to deploying these models in live networks, in order to ensure that they will suit their needs. The models are contained in the *NSP_Product_Service_Artifacts_<Rr>.zip* file. An important readme file is also bundled with the models.

Note: The NSP service models are composed of YANG modules. Users can create additional YANG modules with the intention of augmenting the existing service models, which may result in the configuration of custom parameters from the NSP. Visit the Nokia Network Developer Portal for more information about extending the operational service models.

Network abstraction is used to simplify how the network appears to the IT/OSS layer and users of the NSP service management function. This allows services to be defined and enhanced more quickly by presenting only the network service attributes and endpoints that are relevant to specific customer needs, thereby streamlining service fulfilment operations.

Service management provides real-time, service-related inventory, including available Ports, LAGs, and Service Tunnels (SDPs). This allows users to view the availability of resources in the network before starting with the fulfilment process. Service offerings with customer-centric naming can be created by the user, thereby enabling the dynamic creation of the service catalogue based on installed service models. NSP supports the configuration and deployment of services on third-party devices.

Users have granular control over the entire life cycle of a service. This allows them to define services without deploying them into the network, to plan services so that resources are reserved within NSP, to deploy services in the network that are fully synchronized with the intended configuration, or even to remove services from the network without deleting them entirely. Additionally, users can view all the services in the various life cycle states, as well as view the real-time operational state of deployed services.

Service topology views are available within the service management network map, but users are also provided with the ability to easily navigate to the NSP's Network Map and Health views in order to see multi-layer topology maps and accomplish additional assurance tasks.

To ensure that intended service configurations are maintained in the network, users can audit individual services in order to view and correct any deviations, thereby ensuring configuration assurance in addition to operational assurance.

Automation is achieved using the NSP workflows function. During the life cycle of a service, a workflow can be invoked to carry out specific tasks. For example, when planning a service, a workflow that pre-configures policies into the network can be invoked prior to deployment. Alternatively, when removing a service from the network, a workflow can be invoked to ensure that OAM tests and/or telemetry subscriptions are paused. Automation of user-focused workflows can also be invoked through those views, or via API on an ad hoc basis against the services.

Note: If you wish to use service management for NSP multivendor management, please consult Nokia.

1.2 How do I navigate the service management views?

1.2.1 The service management views

The NSP service management function consists of the following views. You can navigate from one view to another by selecting from the drop-down list.

Services view

The Services view displays a list of all existing services. Additional services can be created by clicking **+ CREATE** in the top right corner.

Click ⋮ (Table row actions) in-line with any service to present the following options:

- Edit
- Clone
- View Service Definition
- Execute Workflow
- Service details
  - Map
  - Components
  - Workflow executions
  - Life cycle history
- Open in Object Troubleshooting

If the service was created using the NSP service management function, rather than an integrated network management system (such as NFM-P), the following additional options will be presented:

- Audit config
- Resync

Note: Users can select up to 10 services at a time to run the Audit Config action against.

If the service is not currently associated with any service template, the following additional option will be presented:

- Associate template

Note: Associating a service template with a brownfield service grants NSP complete life cycle management of the service, including the ability to perform CRUD operations. However, if a service template is applied to a service with attributes that the YANG model has not been extended to support, those attributes will be lost if the service is subsequently removed from the network and redeployed. If the brownfield service originated from a model-driven device, then an API must be used to stitch orphan services prior to associating the service with a service template as described above.

Note: NSP does not support the modification of service names post-creation. Therefore, once a service template has been applied to a brownfield service, NFM-P must not be used to

change the name of the service. If the service name changes, and NSP subsequently aligns that service by pushing to the network, the service will revert to its previous name.

Note: The services displayed in the service list are always grouped by the service type, even when they are sorted based on other criteria. For example, you will see a sorted group of E-Line services followed by a sorted group of E-LAN services, and so on.

If the service is Aligned, the following additional option will be presented:

- Align
  - Push to network
  - Pull from network

Note: Users can select up to 10 services at a time to run Align actions against.

Note: When an L2 microwave backhaul service is deleted from WebCT, the above Align operations will not push or pull the configuration changes to or from nodes. This is because the connect and deploy actions are performed by workflows, and workflows will not be triggered in this scenario. To restore the missing cross connections in NFM-P, service management's Edit and Deploy operations must be used.

If the service is associated with a service template, the following additional options will be presented:

- Unassociate
- Migrate

Note: Users can select up to 10 services at a time to run the Unassociate or Migrate actions against.

Note: To be eligible for the Unassociate action, services must have at least one site and a life cycle state of Deployed.

Depending on the Life Cycle State of the service, one or more of the following additional options will be presented:

- Plan
- Deploy
- Remove
- Delete

Composite Services view

The Composite Services view displays a list of all existing composite services. Additional composite services can be created by clicking **+ CREATE** in the top right corner.

Click ⋮ (Table row actions) in-line with any composite service to present the same options as described in the “Services view” (p. 9) section. Refer to that section for details.

Approved Misalignments view

The Approved Misalignments view displays a list of all misaligned attributes, missing objects, and undesired objects that have been approved by users. See 4.29 “How do I approve misalignments?” (p. 163) for more information.

Ports view

The Ports view displays a list of all existing ports.

Click ⋮ (Table row actions) in-line with any port to present the following options:

- Services Using Port
- Configure

Click **Services Using Port** to display a list of the services that are using that port. Click **Configure** to open the Deploy Physical Configuration form. See the *NSP Device Management Guide* for more information about configuring this form.

If the port was configured using the NSP device management function, the following additional options will be presented:

- Audit
- Align

LAGs view

The LAGs view displays a list of all existing LAGs.

When LAGs are selected, click ⋮ (Table row actions), **Services Using LAG** in-line with any LAG to view a list of the services that are using that LAG.

Service Tunnels view

The Service Tunnels view displays a list of all existing service tunnels.

Click ⋮ (Table row actions) in-line with any service tunnel to present the following options:

- Edit
- Execute Workflow
- Assign Steering Parameter
- Tunnel details
  - Workflow executions
  - Life cycle history
- Services using tunnel

If the service tunnel was created using the NSP, rather than an integrated network management system (such as NFM-P), the following additional option will be presented:

- Audit config

If the service tunnel is Aligned, the following additional option will be presented:

- Align

- Push to network

Depending on the Life Cycle State of the service tunnel, one or more of the following additional options will be presented:

- Plan
- Deploy
- Remove
- Delete

L2 Service Endpoints view

The L2 Service Endpoints view displays a list of all existing L2 service endpoints.

Click **Edit** in-line with any L2 service endpoint to open the Update Service form.

Note: The endpoints displayed in the L2 Service Endpoints view are always grouped by parent service type, even when sorted based on other criteria. For example, you will see a sorted group of E-Line service endpoints followed by a sorted group of E-LAN service endpoints, and so on.

L3 Service Endpoints view

The L3 Service Endpoints view displays a list of all existing L3 service endpoints.

Click **Edit** in-line with any L3 service endpoint to open the Update Service form.

Note: The endpoints displayed in the L3 Service Endpoints view are always grouped by parent service type, even when sorted based on other criteria. For example, you will see a sorted group of E-Line service endpoints followed by a sorted group of E-LAN service endpoints, and so on.

Customers view

The Customers view displays a list of all existing customers.

When Customers are selected, click ⋮ (Table row actions) in-line with any customer to present the following options:

- Edit
- Delete
- Associated services
- Customer sites

Network Policies view

The Network Policies view displays a list of all existing network policies, including routing policies and QoS policies.

Click ⋮ (Table row actions) in-line with any network policy to present the following options:

- Configure

- Audit
- Align

Service Templates view

The Service Templates view displays a list of all existing service templates. Additional service templates can be created by clicking **+ CREATE** in the top right corner.

Click ⋮ (Table row actions) in-line with any service template to present the following options:

- Edit
- Services Using Template
- Delete

Steering Parameters view

The Steering Parameters view displays a list of all existing steering parameters. Additional steering parameters can be created by clicking **+ CREATE** in the top right corner.

Tunnel Templates view

The Tunnel Templates view displays a list of all existing tunnel templates. Additional tunnel templates can be created by clicking **+ CREATE** in the top right corner.

Click ⋮ (Table row actions) in-line with any tunnel template to present the following options:

- Edit
- Delete

Intent Type Catalogue view

The Intent Type Catalogue view displays a list of all existing intent types within service management.

Click ⋮ (Table row actions), **Delete** in-line with any intent type to remove that intent type from service management.

1.3 What is the state of my service or tunnel?

1.3.1 Service and service tunnel states

The NSP service management views provide the visibility of multiple service and service tunnel states to assist with assessing the current condition of a given resource and diagnosing any potential problems. The states that can be seen, and their associated values, are described below.

Note: The values described below are limited to those that are supported by the Nokia-provided, product intents. Depending on your specific system configuration, some additional state values may be visible to you.

1.3.2 Life Cycle State

Life Cycle State indicates the current status of the service or tunnel as it transitions from the planning phase to the deployment phase and beyond. The following states may be observed:

- **Saved**

  During the service or tunnel creation process, a user can save their initial configurations within service management (an associated intent instance is created). The entity name will be reserved, and the user will be able to resume creation when desired. Entities in a Saved state can be deleted, or modified and saved again. When configuration is complete, Saved entities can transition to either a Planned or Deployed state.

- **Planned**

  Newly-created services or tunnels, or services or tunnels in a Saved state, can transition to a Planned state. In this state, an associated intent instance is created in the NSP Network Intents function, but the entity is not deployed to the network. In a Planned state, the entity's resources are reserved, and therefore cannot be used by any other entity. Entities in a Planned state can be deleted (in addition to deleting the entity from service management, this deletes the intent instance and removes the resource reservations), or modified and kept in a Planned state. When configuration is complete, Planned entities can transition to a Deployed state.

- **Deployed**

  Services or tunnels in a Planned state can transition to a Deployed state. In this state, the desired configuration is sent down to the network and synchronized. Entities in a Deployed state must transition to a Removed state before being deleted. If a Deployed entity is modified, it will no longer be aligned with the associated intent instance. At this point, the user can either save their changes (which will place the entity in the Deployed-Modified state until network synchronization occurs), or redeploy the entity (which keeps the entity in the Deployed state by triggering network synchronization).

- **Deployed-modified**

  Services or tunnels in a Deployed-modified state have been modified by the user, but are not synchronized to the network. Entities in a Deployed-modified state must transition to a Removed state before being deleted. Deployed-modified entities can be further modified and saved again, (which keeps the entity in the Deployed-Modified state until network synchronization occurs), or redeployed (which transitions the entity to the Deployed state by triggering network synchronization).

- **Removed**

Services or tunnels in a Removed state can be deleted. In this state, the entity is removed from the network, but its resources remain reserved and its associated intent instance continues to exist. Removed entities can be deployed/redeployed (which transitions the entity to the Deployed state) or modified and saved (which keeps the entity in the Removed state).

Note: Services in a Removed state will display an Operational State of Unknown.

- **Planned-failed**

  Newly-created services or tunnels, or services or tunnels in a Saved state, can transition to a Planned state. When this transition fails, these resources are assigned the Planned-failed state.

- **Deployed-modified-failed**

  Deployed-modified services or tunnels can be further modified and saved again, or they can be transitioned to Deployed. When this transition fails, these resources are assigned the Deployed-modified-failed state.

- **Pull-from-network-saved**

  A brownfield service is associated to a template to make it intent-aware. As the association is triggered, the service moves through this transitory state.

- **Pull-from-network-failed**

  A brownfield service is associated to a template to make it intent-aware. During the association, if the pull from network does not succeed, the service is assigned this state.

1.3.3 Alignment states

Alignment state specifies the alignment state of the service or tunnel. The following states may be observed:

- **Aligned**

  This state indicates that the service or tunnel is aligned with the network.

- **Misaligned**

  This state indicates that the service or tunnel is not aligned with the network. The intent instance and the network copy are not aligned.

1.3.4 Admin states

Admin State indicates the administrative state of the service or tunnel. The following states may be observed:

- **Unknown**

  The administrative state of the resource is not known.

- **Unlocked**

  The resource is administratively up and ready to perform services.

- **Locked**

  The resource is administratively down and is prohibited from performing services.

1.3.5 Operational states

Operational State indicates whether the service or tunnel is currently operable. The following states may be observed:

- **Unknown**

The operational state of the resource is not known.

- **Enabled**
  The resource is operable and available for use.
- **Disabled**
  The resource is inoperable and unable to provide services.

1.3.6 Deployer states

Deployer State specifies the state of the deployer. The following states may be observed:

- **Running**
  The deployer is in progress.
- **Success**
  The deployer succeeded.
- **Failed**
  The deployer failed.

1.3.7 Job states

Job State indicates the state of the job. The following states may be observed:

- **New**
  The job is new, and has not yet been processed.
- **Running**
  The job is queued, or in progress.
- **Success**
  The job has been processed, and succeeded.
- **Failed**
  The job has been processed, and failed.
- **Cancelled**
  The job was cancelled.

1.4 How does service management implement user access control?

1.4.1 Action Permissions

Users of the NSP service management function are assigned a role with defined action permissions. These permissions either allow them to, or prevent them from, performing specific operations. When granting permissions, the available scopes are as follows, and are assigned by an NSP administrator within the Users and System Security views:

- None
- Read
- Read/write
- Read/execute
- Read/write/execute

The following operations are exclusive to users with write permissions:

- Create a service, tunnel, customer, or steering parameter
- Create a service template or tunnel template
- Associate a service with a template, including bulk association (which requires admin privileges)
- Migrate a service to another template
- Unassociate a service from a template
- Change the state of a service or tunnel
- Align (push and pull), audit, or synchronize a service
- Align (push) or audit a tunnel
- Modify service or tunnel definitions
- Assign steering parameters to brownfield tunnels

The following operations are exclusive to users with execute permissions:

- Delete a service, tunnel, customer, or steering parameter
- Delete a service template or tunnel template
- Delete an intent type
- Invoke a workflow against a service (the NSP workflow function will limit the workflows that the user can invoke)

Consult the *NSP System Administrator Guide* or your NSP administrator for more information.

Note: In addition to the above permissions, non-admin service management users must have Read permission for Network Intents enabled. If any custom RPC actions need to be executed, the non-admin service management users must have Operate Intents permission for Network Intents enabled as well. In general, service management users must have access control enabled - within Network Intents - for any intent type they intend to use.

Note: The Edit service action is disabled for users who only have Read permission. These users can manually navigate to the modifications forms via URL, and make changes on these forms, but the Apply button will be disabled.

1.4.2 Resource Groups Access

Users of the NSP service management function are assigned a role with defined resource group access. Their resource group access either allows them to, or prevents them from, accessing specific resources - such as services or network elements. A user's access to a service or network element will affect inventory listings, service CRUD operations, intent suggest functions, and intent RPC calls. When granting access, the available options are as follows, and are assigned by an NSP administrator within the Users and System Security views:

- ‘Access to all Services' is selected — The user has Read/Write/Execute permissions for the full span of services. No further user access control validation is performed.
- ‘Access to all Services' is deselected — The administrator can specify a permission scope for the full span, or a subset, of services.
- ‘Access to all Equipment' is selected — The user has Read/Write/Execute permissions for the full span of network elements. No further user access control validation is performed.
- ‘Access to all Equipment' is deselected — The administrator can specify a permission scope for the full span, or a subset, of network elements.

Note: NSP administrators have Read/Write/Execute permissions for the full span of services and network elements. No further user access control validation is performed.

The following limitations apply when resource group access is defined:

- Due to the additional user access control validations that evaluate network element access, there is a degradation of the service provisioning rate at >2 seconds per service.
- Only site spans are currently supported - not port spans. If a user has access to a given network element, they are assumed to have access to all of its ports.
- There is only user access control for composite services when defining network element group access - not when defining service group access.
- The Inventory Find function on network elements only checks for Read permissions on a group. Therefore, resources are listed if the user has Read access to the network elements group. In this case, service management will validate the group permission scope (Read/Write/Execute) and validate accordingly for the intended action.
- When network elements access is defined, all service management objects are visible, even those that are not associated to network elements. This includes service templates, tunnel templates, steering parameters, etc.
- The user will be able to see a full audit report on a service, regardless of their network element access.
- The user will be able to approve misalignments and remove approvals, regardless of their network element access.
- Network element access is not applied to service tunnels, customer sites inventory, or network policies inventory.

1.5 How does service management interact with NFM-P?

1.5.1 Service management and NFM-P

Services created using Classic Management (NFM-P) can be managed by the NSP service management function if the service's NSD-managed parameter is enabled in NFM-P. NSP can discover LSP and SDP tunnels that are previously created in NFM-P. NFM-P is used to define QoS generic policies so that NSP can handle service access QoS.

To deploy IP services to NFM-P, the NSP uses NFM-P templates that are installed into NFM-P during NSP installation. The templates are hard-coded in NSP, however; the NSP service definition is very abstract and models only a small subset of available attributes on the NEs. Operators can use these templates to augment services, sites, and endpoints so that additional attributes can be configured from the NSP service management views.

The following table maps the service names defined in NFM-P to the corresponding NSP service names:

Table 1-1 Service type naming

NFM-P service	NSP service
CPIPE	C-Line
EPIPE	E-Line
VPLS	E-LAN
VPRN	L3 VPN

1.6 What artifacts does service management require?

1.6.1 Required artifacts

Some NSP artifacts are required to perform service management. Artifacts are any piece of software that can be installed in a running NSP system to enable functionality for a use case. See “What is an artifact?” in the *NSP Network Automation Guide* for more information. The artifacts required for service management functions include predefined intent types and datasync mapping files. These artifacts are packaged for download in zip format as the service management artifact bundles. You can obtain these bundles from the Nokia NSP software download site and install them from the NSP Artifact Bundles view. See “What is an artifact bundle?” in the *NSP Network Automation Guide* for more information.

Note: If you are upgrading from a previous release, it is recommended that the latest service management artifacts are used in place of any previous versions.

1.7 What adaptor artifacts does service management support?

1.7.1 Supported adaptor artifacts

NSP supports a variety of Nokia and multi-vendor devices via pluggable adaptor artifacts, sometimes called "MDM adaptors". In service management, the application functions that are available for model-driven NEs can vary based on the installed adaptor artifacts. To verify the adaptor artifacts you have installed, check the Managed Network Elements list in the NSP Device Management views. The Applicable Adaptors view for the NE provides the list of adaptor artifacts that are installed for each application.

1.8 What service management APIs are supported?

1.8.1 Supported APIs

The NSP service management functions are available for OSS using programmable APIs. For general information about developer support, visit the Nokia Network Developer Portal. For API documentation, visit the API documentation page.

For specific documentation about REST APIs for service management, click on API Reference in the Service Fulfillment and Resource Control > Carrier SDN row.

1.9 How do I enable event-based auto-auditing?

1.9.1 Event-based auto-auditing

NSP supports the automatic auditing of E-Line and VPRN services. Once configured, an audit will be triggered automatically whenever a service-affecting configuration event originates from another source (for example, CLI).

To enable this feature, the autoAudit parameter must be set to true in the nsp-service-oper-model-app-config-configmap file (it is set to false by default). After this step is completed, the nsp-service-oper-model pod must be restarted.

It is also essential that the E-Line and VPRN service intents that are in use must be from NSP Release 23.11 or later.

There is a default hold timer that buffers the network service configuration events. By default, this set to 2 minutes, thereby reducing the chances of multiple audits occurring on the same service in a short period of time.

2 Intents and templates

2.1 How does service management acquire intent types?

2.1.1 Service management and NSP Artifacts

The NSP service management function uses intent types to build service and tunnel templates, which are then used to create services and service tunnels. The library of product service models (intent types) is obtained from the artifacts section of the Nokia Support Portal. The models are contained in the *NSP_Product_Service_Artifacts_<Rr>.zip* file. An important readme file is also bundled with the models. These intent types can be imported into the NSP from the Artifacts views. Importing the artifact bundle also imports the models into service management. Users with the NSP programming suite can also create custom intent types within the NSP Network Intents views.

For more information about using the NSP Artifacts function and cloning intent types, see the *NSP Network Automation Guide*.

Note: Intent types must have the ServiceFulfillment label applied in order to be used by service management. Users should exercise caution when modifying or deleting any intent types with the ServiceFulfillment label.

Note: Once an intent type is used by service management, any change made to that template in one location - such as the NSP Network Intents views - will be propagated to the other.

2.2 How do I create a service template?

2.2.1 Steps

1

From the **Service Management** view, select Service Templates from the drop-down list and click **+ CREATE**.

The Create a service template form opens.

2

Configure the parameters, as required:

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	Specifies the service intent type to associate with the template
Intent Version	Specifies which version of the selected service intent type to associate with the template
State	Specifies the state of the template, Released or Draft
Config Form	Specifies the interface to be used with the template

3

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

4

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution

Parameter	Description
Blocking	Specifies whether the unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

5

Click **+ ADD**.

The Add Workflows form closes and the workflow is added to the service template.

6

If required, select a Default Service Category in the Bulk Association panel to specify a service type to which this service template can be applied in bulk.

7

Click **+ CREATE**.

The service template is created.

END OF STEPS

2.3 How do I create a tunnel template?

2.3.1 Steps

1

From the **Service Management, Tunnel Templates** view, select Tunnel Polices from the drop-down list and click **+ CREATE**.

The Create a tunnel template form opens.

2

Configure the parameters, as required:

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	Specifies the tunnel intent type to associate with the template
Intent Version	Specifies which version of the selected tunnel intent type to associate with the template
State	Specifies the state of the template, Released or Draft
Config Form	Specifies the interface to be used with the template

3

If required, click **+ ADD** in the Workflows panel to add workflows to the tunnel template.

The Add Workflows form opens.

4

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution

Parameter	Description
Blocking	Specifies whether the unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that the unsuccessful execution of the workflow will prevent tunnel life cycle state changes

5

Click **+ ADD**.

The Add Workflows form closes and the workflow is added to the tunnel template.

6

Click **+ CREATE**.

The tunnel template is created.

END OF STEPS

2.4 How do I configure a port template?

2.4.1 Steps

1

From the **Service Management, Ports** view, perform one of the following:

a.

1. To configure an existing port, click **+ CONFIGURE**. A list of available port templates is displayed.
2. Click on a port template from the list. The NSP Device Management view opens.

b. To configure a port template for a specific port, click ⋮ (Table row actions), **Configure** in-line with that port. The NSP Device Management view opens.

2

Perform one of the following:

a. If an existing port template, or a port associated with an existing port template was selected, the selected port template is displayed in the Deploy Physical Configuration form.

b. If a port without a port template was selected, a blank Deploy Physical Configuration form is displayed.

3

See the *NSP Device Management Guide* for more information about configuring port templates using the Diploy Physical Configuration form.

Note: The Configuration Alignment column on the **Service Management, Ports** view indicates whether a port is aligned or misaligned as it relates to its device management configuration instance. If a port is not configured with a port template, this field will be blank.

END OF STEPS

2.5 How do I configure a LAG template?

2.5.1 Steps

1

From the **Service Management, LAGs** view, perform one of the following:

a.

1. To configure an existing LAG, click **+ CONFIGURE**. A list of available LAG templates is displayed.
2. Click on a LAG template from the list. The NSP Device Management view opens.

b. To configure a LAG template for a specific LAG, click ⋮ (Table row actions), **Configure** in-line with that LAG. The NSP Device Management view opens.

2

Perform one of the following:

a. If an existing LAG template, or a LAG associated with an existing LAG template was selected, the selected LAG template is displayed in the Deploy Physical Configuration form.

b. If a LAG without a LAG template was selected, a blank Deploy Physical Configuration form is displayed.

3

See the *NSP Device Management Guide* for more information about configuring LAG templates using the Diploy Logical Configuration form.

END OF STEPS

2.6 How do I configure a network policy template?

2.6.1 Supported network policies

the NSP service management function supports both routing policies and QoS policies.

2.6.2 Steps

1

From the **Service Management, Network Policies** view, perform one of the following:

a.

1. To configure an existing network policy, click **+ CONFIGURE**. A list of available network policy templates is displayed.
2. Click on a network policy template from the list. The NSP Device Management view opens.

b. To configure a network policy template for a specific network policy, click ⋮ (Table row actions), **Configure** in-line with that network policy. The NSP Device Management view opens.

2

Perform one of the following:

a. If an existing network policy template, or a network policy associated with an existing network policy template was selected, the selected network policy template is displayed in the Deploy Physical Configuration form.

b. If a network policy without a network policy template was selected, a blank Deploy Physical Configuration form is displayed.

3

See the *NSP Device Management Guide* for more information about configuring network policy templates using the Display Physical Configuration form.

Note: The Alignment State column on the **Service Management, Network Policies** view indicates whether a network policy is aligned or misaligned as it relates to its device management configuration instance. If a network policy is not configured with a network policy template, this field will be blank.

END OF STEPS

2.7 How do I create a steering parameter?

2.7.1 Steps

1

From the **Service Management, Steering Parameters** view, click **+ CREATE**.

The Create Steering Parameter form opens.

2

Configure the name parameter, which specifies the name of the steering parameter, and click **+ CREATE**.

The steering parameter is created.

END OF STEPS

3 Inventory Management

3.1 How does NSP discover brownfield customers?

3.1.1 Discovering brownfield customers

NSP uses both NFM-P and MD resync mapping files to populate the NSP operational model with brownfield customer information. These files can be obtained from the artifacts section of the Nokia Support Portal. Once installed, these files will continue to automatically discover new customers that are created using CLI/NFM-P and MD SR OS. A product artifact for customer life cycle management (create/distribute/audit/align/delete) is interpreted by the NSP as network-created customer instances (CLIs), and will be discovered as such.

Note: It may take up to 24 hours (default) for customers created using MD CLI to appear in the NSP service management views.

If a global NFM-P customer (with no related services) is deleted, the global NSP customer instance will remain. If a new service is created with this customer, the customer instance will be populated back down to the NFM-P. An MD node has no concept of a global customer. During resync, the global NSP customer will be created if it does not already exist.

The NSP customer key is ID. The NFM-P customer key is ID, and the name is set to ID by default. On MD CLI, the key is customer-name, and customer-id is mandatory. This may create a scenario in service management where multiple customers have the same name, but different IDs. Also, attempting to create a customer from one source (NFM-P, for example) that uses the same ID as a previously-discovered customer from another source (MD CLI, for example) will instead add an additional site to the existing customer.

It is also possible that an NE customer site has a different name than the global NSP name.

3.2 How do I create a customer?

3.2.1 Purpose

The following procedure is used to create new customers. For information about discovering existing customers, see 3.1 “How does NSP discover brownfield customers?” (p. 35).

Note: Customers can also be created using either classic CLI, or MD CLI. Customers created using MD CLI will be populated into NSP, but their contact details will not. Users can populate those attributes afterwards by editing those customer instances. This is not a restriction for customers created using classic CLI.

3.2.2 Steps

1

Perform one of the following:

a. From the **Service Management, Customers** view, click **+ CREATE**.

The Create a customer form opens.

b. During service creation, click on the Customer ID field, then click **+ CREATE CUSTOMER**.

The Create a customer form opens.

2

Configure the required parameters:

Parameter	Description
ID	Specifies the ID of the customer
Bulk Associate	Specifies whether the services belonging to this customer can be bulk associated with service templates
Customer Name	Specifies the name of the customer
Description	Describes the customer
Contact	Specifies the point-of-contact for the customer
Phone Number	Specifies the phone number of the customer
Email	Specifies the E-mail address of the customer
Address	Specifies the address of the customer

3

Click **+ CREATE**.

The customer is created.

Note: The newly-created customer will only be populated within NFM-P when a service that specifies the customer is created .

END OF STEPS

3.3 How do I bulk associate a customer's services with service templates?

3.3.1 Purpose

Service management's bulk associate function can be used to simultaneously apply a specific service template to multiple services that share the same service type and customer.

3.3.2 Steps

1

Perform one of the following:

a. To create a new service template, perform 2.2 “How do I create a service template?” (p. 26), ensuring that you specify a Default Service Category in the Bulk Association panel of the Create a service template form.

b. To modify an existing service template, perform the following:

1. From the **Service Management, Service Templates** view, click ⋮ (Table row actions), **Edit** in-line with any service template. The Edit service template form opens.
2. Specify a Default Service Category in the Bulk Association panel of the service template creation form and click **UPDATE**. The Edit service template form closes.

2

Perform one of the following:

a. To create a new customer, perform 3.2 “How do I create a customer?” (p. 36), ensuring that you select the Bulk Associate check box.

b. To modify an existing customer, perform the following:

1. From the **Service Management, Customers** view, click ⋮ (Table row actions), **Edit** in-line with any customer. The Edit customer form opens.
2. Select the Bulk Associate check box and click **UPDATE**. The Edit customer form closes.

3

From the **Service Management, Services** view, click ⋮ (Table row actions), **Bulk Associate** in the top right corner.

Any services belonging to a customer that has bulk associate enabled will be associated with a service template, provided their service type matches the service template Default Service Category configuration.

END OF STEPS

3.4 How do I create a service tunnel?

3.4.1 Purpose

Use this procedure to create a new service tunnel. Brownfield service tunnels, created previously in NFM-P or on MDM-managed nodes, can be discovered by the NSP and used by services, but their properties cannot be modified from the NSP service management views. They can, however, have steering parameters applied to them, and have workflows executed on them.

The set of parameters that are available to you during service tunnel creation is dependent on the intent type that is associated with the tunnel template you select, and may differ from those described in this procedure, which assumes the Nokia-provided tunnel template is being used.

3.4.2 Steps

1

Perform 2.3 “How do I create a tunnel template?” (p. 28).

2

Perform one of the following:

a.

1. From the **Service Management, Service Tunnels** view, click **+ CREATE**.

   The Select a tunnel template to start form opens, displaying a list of tunnel templates.
2. Click on a tunnel template from the list.

   The Create Tunnel form opens with the Template Name parameter populated.

b.

1. During service creation, click on the SDP ID field, then click **+ CREATE TUNNEL**.

   The Create Tunnel form opens.
2. Click on the Template Name field and select a tunnel template from the list.

3

Configure the parameters, as required:

Parameter	Description
Source NE ID	Specifies the identifier of the source NE
SDP ID	Specifies the SDP IP
Name	Specifies the name of the tunnel
Destination NE ID	Specifies the identifier of the destination NE
Description	Describes the tunnel

Parameter	Description
Admin State	Specifies the initial administrative state of the tunnel upon deployment
Transport Type	Specifies the type of transport to be used by the tunnel, MPLS or GRE
Signaling	Specifies the signaling method to be used by the tunnel
MTU	Specifies the MTU of the tunnel
Metric	Specifies the metric of the tunnel

4

If the Transport Type parameter was set to MPLS, configure the required parameters:

Parameter	Description
Mixed LSP Mode	Specifies whether the mixed LSP mode is enabled for the tunnel
Revert Time	Specifies the revert time, when mixed LSP mode is enabled
Enable LDP	Specifies whether the LDP is enabled for the tunnel
Enable BGP Tunnel	Specifies whether the BGP tunnel is enabled for the tunnel
SR-ISIS	Specifies whether the SR-ISIS is enabled for the tunnel
SR-OSPF	Specifies whether the SR-OSPF is enabled for the tunnel
LSP	Specifies the LSP to be associated with the tunnel

5

Configure the required Hello parameters:

Parameter	Description
Keep Alive Enabled	Specifies whether the keep alive is enabled for the tunnel
Hello Time	Specifies the hello time of the tunnel
Hello Message Length	Specifies the hello message length of the tunnel

Parameter	Description
Hello Request Timeout	Specifies the hello request timeout of the tunnel
Hold Down Time	Specifies the hold down time of the tunnel
Max Drop Count	Specifies the maximum drop count of the tunnel

6

If the Transport Type parameter was set to GRE, configure the Allow Fragmentation parameter (if required), which specifies whether or not fragmentation will be allowed for the tunnel.

7

Configure the required parameters:

Parameter	Description
Steering Parameters	Specifies the steering parameter(s) to be associated with the tunnel
Tunnel Admin Group	Specifies the administrative group to which the tunnel will belong

8

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the tunnel in a Planned state.

b. Click **SAVE** to create the tunnel in a Saved state.

c. Click **DEPLOY** to create the tunnel in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

3.5 How do I audit a service tunnel?

3.5.1 Steps

1

Perform one of the following:

a. From the **Service Management, Service Tunnels** view, click ⋮ (Table row actions), **Audit config** in-line with any service tunnel.

b. From the **Service Management, Service Tunnels** view, click on a service tunnel in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

The service tunnel is audited.

2

If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

The Audit Result form closes.

3

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, perform one of the following:

a. Click ⋮ (Table row actions), **Align**, **Push To Network** in-line with the previously-audited service tunnel.

b. Click on a service in the list, then expand the Alignment State section in the info panel and click **ALIGN**.

The service tunnel is synchronized with the network.

END OF STEPS

4 Managing services

4.1 What tasks should I complete before and after service creation?

4.1.1 Service creation prerequisites

Before attempting to perform any of the service creation procedures in this chapter, the following tasks must be completed to help ensure successful service provisioning:

1. Create a service management user
   - Optionally, create a user that has specific permissions when performing service management functions. For more information, see the following procedures in the *NSP System Administrator Guide*:
     — “How do I configure a role?”
     — “How do I configure a user group?”
     — “How do I create an NSP local user?”
     For more information about the different tiers of access available to service management users, see 1.4 “How does service management implement user access control?” (p. 17).
2. Install the required artifact bundles
   - Artifact bundles contain service intent types, which are used for building service templates. Installing the required artifact bundles will make those service intent types accessible to service management via the NSP Artifacts function.
     For more information about the relationship between the NSP service management and Artifacts functions, see 2.1 “How does service management acquire intent types?” (p. 25).
3. Create a tunnel template
   - Using an existing intent type, create a template that will be used when creating service tunnels. For detailed instructions, see 2.3 “How do I create a tunnel template?” (p. 28).
4. Create a service tunnel
   - Using a created tunnel template, create a service tunnel that will be used by services. For detailed instructions, see 3.4 “How do I create a service tunnel?” (p. 39).
5. Create a service template
   - Using an existing intent type, create a template that will be used when creating services. For detailed instructions, see 2.2 “How do I create a service template?” (p. 26).
6. Verify node support
   - Before creating a service, you may want to verify that your intended service will be supported on a certain type of node. NSP provides adaptor artifact guides that can be used to obtain this information. These guides can be obtained from ALED.

When these tasks are complete, you may perform one of the service creation procedures in this chapter.

4.1.2 Post-service creation tasks

After completing any of the service creation procedures in this chapter, the following tasks can be completed, as required:

1. Generate and execute OAM test suites
   - Optionally, generate and execute OAM test suites against the objects of your service. For more information, see “How do I run an OAM test on a service?” in the *NSP Network and Service Assurance Guide* and “How do I create an OAM test suite?” in the *NSP Data Collection and Analysis Guide*.
2. Create telemetry subscriptions
   - Optionally, configure telemetry collection. The nsp-telemetry-cr-va-sros artifact bundle must be installed prior to attempting this. For more information, see “How do I install telemetry artifacts?” and “How do I manage subscriptions?” in the *NSP Data Collection and Analysis Guide*.
3. Create a telemetry chart and plot statistics
   - Optionally, chart historical telemetry data. For more information, see “How do I plot a telemetry chart?” in the *NSP Data Collection and Analysis Guide*.

4.2 How do I know which attributes my service supports?

4.2.1 Supported attributes

With the product service models (intent types) provided in the artifacts section of the Nokia Support Portal are documentation folders, which contain SR OS CLI configurations for both model and classic modes, based on the product artifact YANG model. Both raw CLI and JSON/HTML formats are included for ease of use. These files can be used to determine the attributes that may be available to you when creating services, depending on the types of nodes in your network. The contents of this folder depends on the complexity of the related service model and includes:

- intent.html — an HTML tree view of the attributes included in the product L3 VPN service intent
- payload1.NodeTypeAndVersion.mdcli.json — CLI output, in JSON format, of the attributes supported on model-driven nodes
- payload1.NodeTypeAndVersion.mdcli.txt — CLI output, in plain text, of the attributes supported on model-driven nodes
- payload1.NodeTypeAndVersion.cli.text — CLI output, in plain text, of the attributes supported on classically-managed nodes

Note: The procedures in this document assume that the Nokia-provided intent type artifacts have been used to configure service templates, and that those templates will be used to configure services. As such, the parameters and options documented in this guide are limited to what is available when using those intent types and may not allow for certain capabilities - such as mutivendor management - that may be enabled by custom intent types. Please consult Nokia for assistance when using intent types other than those described here.

4.3 How does NSP manage E-Line services?

4.3.1 E-Line services

An E-Line service connects two customer Ethernet ports over a WAN. NSP supports the creation of E-Line services over IP networks. If an existing E-Line service is modified (for example, to increase bandwidth), the service tunnel is resized to accommodate it, if permitted by the 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 NSP.

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.

4.3.2 Brownfield E-Line services

The E-Line services created within the NFM-P (brownfield E-Line services) can be managed by the NSP. Once discovered by the NSP, these services will function the same way as E-Line services created within NSP, provided that they meet NSP requirements. Any change made to these services within NFM-P after discovery will be propagated to the NSP Service Management views, 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.

4.3.3 EVPN-based E-Line services

NSP 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.

To configure an EVPN-based E-Line service, you need to start the E-Line service creation within the NSP Service Management views, 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 NEs 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 NSP:

- NSP 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.
- NSP 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 can be modified, as required. However, NSP does not support switching from the EVPN-based E-Line service (the Enable EVPN Tunnel Selection check box is selected) to a pseudowire-based E-Line service (the Enable EVPN Tunnel Selection check box is not selected).
- Each service is associated with a unique EVPN instance (EVI) number that NSP generates automatically and then sends to the NE to auto-derive the unique RD/RT for the NE. NSP 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 NSP 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. Select the appropriate Tunnel Type for an EVPN-based E-Line service in the template properties, as required.

4.4 How do I create an E-Line service?

4.4.1 Purpose

Use this procedure to create an E-Line service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided E-Line template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: The creation of E-Line services is included in Nokia NSP Use Case Catalog as UCC-12. For more information about obtaining access to the catalog and its materials, contact your Nokia sales representative.

4.4.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an E-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
NE Service ID	Specifies the NE service ID
MTU	Specifies the service MTU
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment

Parameter	Description
Job ID	Specifies the work-order number

Continue to the Site A panel.

5

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the site MTU

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

6

Click **+ ADD**.

The Add Endpoint form opens.

7

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name

8

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

9

Configure the parameters in the CPU Protection panel, as required:

Parameter	Description
Policy ID	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

10

If QoS was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue

Parameter	Description
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR

Parameter	Description
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

11

If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the endpoint.

The Add Endpoint form closes.

12

In the Site B panel, repeat Step 5 to Step 11.

13

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

14

Configure the parameters, as required:

Parameter	Description
Admin State	Specifies the desired state of the service SDP binding
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier
VC Type	Specifies the virtual circuit type, Ether or VLAN
Control Ward	Specifies whether or not to use the control ward as preferred

Click **+ ADD** to add the SDP binding.

The Add SDP form closes.

15

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.5 What are L3 VPN services?

4.5.1 L3 VPN services

NSP 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 are auto-generated as per policy direction and the topology type selected. 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 NSP.

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.

NSP allows you to configure the properties on each hub-and-spoke or full mesh 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 NSP, 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.

Note: When NFM-P discovers a VPRN service by managing nodes, an invalid service template appears within service management.

4.6 How do I create an L3 VPN service?

4.6.1 Purpose

Use this procedure to create an L3 VPN service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided L3 VPN template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: The creation of L3 VPN services is included in Nokia NSP Use Case Catalog as UCC-15. For more information about obtaining access to the catalog and its materials, contact your Nokia sales representative.

4.6.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an L3 VPN service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the assigned queue group redirect list
VRF Name	Specifies the name of the VRF
Description	Describes the VRF
MTU	Specifies the service MTU
NE Service ID	Specifies the NE service ID
Autonomous System	Specifies the AS number advertised to peers for this router
ECMP	Specifies the maximum number of ECMP routes
Router ID	Specifies the unique identifier of the router in the autonomous system
Export Inactive BGP	Specifies whether or not to export the best BGP route as a VPN-IP route, even if it is inactive due to a preferred route from another PE
Route Distinguisher Type	Specifies the route distinguisher type
Route Distinguisher	Specifies the route distinguisher
VRF Import	Specifies the name of the VRF import policy
VRF Export	Specifies the name of the VRF export policy
BGP IPVPN Admin State	Specifies the BGP IPVPN administrative state, which is only applicable on SR OS 21.x devices.
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value

7

In the Auto Bind Tunnel panel, configure the required parameters:

Parameter	Description
Resolution	Specifies the MBS of the queue
Enforce Strict Tunnel Tagging	Specifies the PIR rate of the queue
Resolution Filter	
BGP	Specifies the BGP type for the autobind tunnel
GRE	Specifies whether the GRE is enabled for the autobind tunnel
LDP	Specifies whether the LDP is enabled for the autobind tunnel
RSVP	Specifies whether the RSVP is enabled for the autobind tunnel
SR-ISIS	Specifies whether the SR-ISIS is enabled for the autobind tunnel
SR-OSPF	Specifies whether the SR-OSPF is enabled for the autobind tunnel
SR-TE	Specifies whether the SR-TE is enabled for the autobind tunnel
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether the RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether the MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether the SR policy is enabled for the autobind tunnel
SR-OSPF3	Specifies whether the segment routing OSPF3 is used for next hop resolution

8

As required, select the **Enable EVPN MPLS** check box in the BGP EVPN panel and configure the parameters:

Parameter	Description
Admin State	Specifies the administrative state of BGP-EVPN MPLS
Route Distinguisher	Specifies the route distinguisher
VRF Import Policy	Specifies the name of the VRF import policy
VRF Export Policy	Specifies the name of the VRF export policy
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
Auto Bind Tunnel	
Resolution	Specifies the MBS of the queue
Enforce Strict Tunnel Tagging	Specifies the PIR rate of the queue
Resolution Filter	
BGP	Specifies the BGP type for the autobind tunnel
GRE	Specifies whether the GRE is enabled for the autobind tunnel
LDP	Specifies whether the LDP is enabled for the autobind tunnel
RSVP	Specifies whether the RSVP is enabled for the autobind tunnel
SR-ISIS	Specifies whether the SR-ISIS is enabled for the autobind tunnel
SR-OSPF	Specifies whether the SR-OSPF is enabled for the autobind tunnel
SR-TE	Specifies whether the SR-TE is enabled for the autobind tunnel
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether the RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether the MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether the SR policy is enabled for the autobind tunnel

Parameter	Description
SR-OSPF3	Specifies whether the segment routing OSPF3 is used for next hop resolution

9

As required, select the **Enable Maximum Routes** check box in the BGP EVPN panel and configure the parameters:

Parameter	Description
Maximum IPv4 Routes	
Max Number of Routes	Specifies the maximum number of IPv4 routes that are configured on the virtual router
Log Only	Specifies whether the action is taken when the maximum number of IPv4 routes, held within a VRF context, is reached
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv4 routes that the VRF holds
Maximum IPv6 Routes	
Max Number of Routes	Specifies the maximum number of IPv6 routes that are configured on the virtual router
Log Only	Specifies whether the action is taken when the maximum number of IPv6 routes, held within a VRF context, is reached
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv6 routes that the VRF holds
MC Maximum Routes	
Max Number of MCast Routes	Specifies the maximum number of multicast routes that are configured on the virtual router
Log Only	Specifies whether the action is taken when the maximum number of multicast routes, held within a VRF context, is reached
Mid Route MCast Threshold	Specifies the mid-level water marker for the number of multicast routes that the VRF holds

10

Configure the parameters in the Route Aggregation panel, as required:

Parameter	Description
Aggregate (click **+ ADD**)	
IP Prefix	Specifies the destination IP address prefix of the aggregate route
Community	Specifies the community name that is added to the aggregate route
Summary Only	Specifies whether or not to advertise the aggregate route only
Next Hop	Specifies the address of the next hop
SNMP Community	Specifies the SNMP v1/v2c community name associated with the VPRN
Ignore NH Metric	Specifies whether or not to ignore the next hop metric

11

Configure the parameters in the BGP-VPN Backup panel, as required:

Parameter	Description
IPv4	Specifies whether or not to allow BGP-VPN to be used as a backup for IPv4 prefixes
IPv6	Specifies whether or not to allow BGP-VPN to be used as a backup for IPv6 prefixes

12

At the bottom of the form, configure the parameters, as required:

Parameter	Description
Enable eBGP	Specifies whether or not the eBGP protocol is enabled
Enable Static Route	Specifies whether or not the static route protocol is enabled
Enable IS-IS	Specifies whether or not the IS-IS protocol is enabled
Enable BGP	Specifies whether or not the BGP protocol is enabled

Parameter	Description
Enable RIP	Specifies whether or not the RIP protocol is enabled

13

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

14

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Description	Describes the interface
Administrative State	Specifies the administrative state of the interface
Loopback	Specifies whether to use the interface as a loopback interface
IP MTU	Specifies the interface IP MTU
Ingress Stats	Specifies whether or not ingress statistics will be collected
Monitor Oper Group	Specifies the operational group to monitor

15

If IS-IS was enabled in Step 12, configure the required parameters in the IS-IS panel:

Parameter	Description
IS-IS Instance	Specifies the instance ID for the IS-IS instance
Admin State	Specifies the administrative state of the IS-IS interface
Passive	Specifies the passive interface
Level Capability	Specifies the routing level for instance
Interface Type	Specifies the interface type, broadcast or point-to-point

16

If OSPF was enabled in Step 12, configure the required parameters in the OSPF panel:

Parameter	Description
Area ID	Specifies the area identifier
Interface Type	Specifies the interface type, broadcast or point-to-point
Passive	Specifies whether to allow the interface to be advertised as an OSPF interface without running the OSPF protocol
Metric	Specifies the explicit route cost metric that is applied to the interface
Authentication Key	Specifies the authentication key
Authentication Type	Specifies the authentication type used on the OSPF interface
BFD Liveliness (select the check box)	
Remain Down On Failure	Specifies whether or not to force adjacency down on failure until the session returns
Admin State	Specifies the administrative state of the OSPF interface

17

If RIP was enabled in Step 12, configure the required parameter in the RIP panel:

Parameter	Description
Group Name	Specifies the group name

18

In the IPv4 panel, configure the required parameters:

Parameter	Description
Primary	
Address	Specifies the primary IPv4 address assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary (**+ ADD**)	

Parameter	Description
Address	Specifies the secondary IPv4 address assigned to the interface
Prefix Length	Specifies the secondary IPv4 address prefix length
VRRP (**+ ADD**)	
Virtual Router ID	Specifies the virtual router identifier of the VRRP virtual router instance
Passive	Specifies whether or not to suppress the processing of VRRP advertisement messages
Admin State	Specifies the administrative state of VRRP
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
Message Interval	Specifies the interval for sending VRRP advertisement messages
Ping Reply	Specifies whether or not to allow the non-owner master to reply to ICMP echo requests
Traceroute Reply	Specifies whether or not to allow the non-owner master to reply to traceroute requests
Standby Forwarding	Specifies whether or not to allow the standby router to forward traffic
Neighbor Discovery	
Timeout	Specifies the timeout for an ARP entry learned on the interface
Retry Timer	Specifies the ARP retry interval
Learn Unsolicited	Specifies whether or not to learn new entries from any received NA message
Proactive Refresh	Specifies whether or not to send a single refresh message before the entry timeout
Populate	Specifies whether or not to allow static and dynamic hosts to be populated in the system ARP cache

Parameter	Description
Local Proxy ARP	Specifies whether or not to enable local proxy ARP on the interface
Proxy ARP Policy	Specifies the proxy ARP policy name
Populate (click **+ ADD**)	
Route Type	Specifies the type of ARP or ND entries that generate host routes
Route Tag	Specifies the tag value used with the host route from an ARP/ND entry
Limit	
Max Entries	Specifies the maximum number of entries learned on an IP interface
Log Only	Specifies whether or not to generate log entries only if the limit is reached
Threshold	Specifies the threshold value that triggers a warning message
BFD	
Admin State	Specifies the administrative state of BFD sessions
Transmit Interval	Specifies the BFD transmit interval over this interface
Receive	Specifies the BFD receive interval over this interface
Multiplier	Specifies the number of consecutive BFD messages missed from the peer
Echo Receive	Specifies the minimum echo interval over this interface
Type	Specifies the local termination point for the BFD session
ICMP - Redirects	
Admin State	Specifies the administrative state of sending ICMP redirect messages
Number	Specifies the maximum number of ICMP redirect messages to send
Seconds	Specifies the time used to limit the number of ICMP redirect messages

Parameter	Description
ICMP - Unreachables	
Admin State	Specifies the administrative state of sending unreachable messages
Number	Specifies the maximum number of unreachable messages to send
Seconds	Specifies the time used to limit the number of ICMP unreachable messages
DHCP	
Admin State	Specifies the administrative state of DHCP
Server	Specifies the IP addresses for DHCP server requests

19

In the SAP panel, configure the following parameters for both ingress and egress panels, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name

20

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

21

Configure the parameters in the CPU Protection Panel, as required:

Parameter	Description
Policy ID	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

22

If QoS was enabled in Step 21, configure the required QoS parameters in both the Ingress and Egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer

Parameter	Description
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect

Parameter	Description
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

23

If a filter was enabled in Step 21, configure the required filter parameters:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

24

In the Routed VPLS panel, configure the required parameters:

Parameter	Description
VPLS Name	Specifies the name of the VPLS service
EVPN Tunnel	Specifies whether or not to configure the interface as a VPLS EVPN tunnel
ARP	
Learn Dynamic	Specifies whether or not dynamic entries learning is enabled
Advertise Static	Specifies whether or not advertise static is enabled
Advertise Static Route Tag	Specifies the advertise static route tag
Advertise Dynamic	Specifies whether or not advertise dynamic is enabled
Advertise Dynamic Route Tag	Specifies the advertise dynamic route tag

25

In the IPv6 Details panel, configure the required parameters:

Parameter	Description
IPv6 (**+ ADD**)	
IPv6 Address	Specifies the IPv6 address assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length

Click **+ ADD** to add the interface.

The Add Interface form closes.

26

In the IP Transports panel, click **+ ADD**.

The Add IP Transport form opens.

27

Configure the parameters, as required:

Parameter	Description
Transport Port ID	Specifies the Transport Port Identifier
Admin State	Specifies the administrative state for this IP Transport entry
Description	Description of this IP Transport
Local Host	
Local Host IP Address	Specifies the IP address of the IP Transport Local Host
Local Host Port Number	Specifies the Internet socket port number
Local Host Protocol	Specifies the IP protocol of the Local Host
Session Details	
DSCP	Specifies the Differentiated Services Code Point (DSCP) for all packets sent to Remote Hosts (within the same IP Transport)
Forwarding Class	Specifies the Forwarding Class (FC) for all packets sent to Remote Hosts (within the same IP Transport)
Filter Unknown Host	Specifies whether to allow a connection/session with an unknown remote host

Parameter	Description
Profile	Specifies the profile marking for all packets sent to Remote Hosts (within the same IP Transport)
TCP	
TCP Max Retries	Specifies the maximum number of consecutive attempts to establish a TCP connection
TCP Retry Interval	Specifies the period of time between consecutive attempts to establish a TCP connection
TCP In Active Timeout	Specifies the maximum period of time a TCP connection can remain idle before tear-down is initiated
Remote Host (click **+ ADD**)	
Remote Host ID	Specifies the identifier of this IP Transport Remote Host
Name	Specifies the name assigned to this IP Transport Remote Host
Description	Specifies the description of this IP Transport Remote Host
Remote Host IP Address	Specifies the IP address of the IP Transport Remote Host
Remote Host Port Number	Specifies the number of a TCP or UDP port
Check TCP	Specifies the TCP connection test to be initiated

Click **+ ADD** to add the IP Transport.

The Add IP Transport form closes.

28

If eBGP was enabled in Step 12, configure the required parameters:

Parameter	Description
Loop Detect	Specifies the strategy for loop detection in the AS path
Peer IP Tracking	Specifies whether or not to enable BGP peer tracking

Parameter	Description
Router ID	Specifies the Router ID for the BGP instance in the AS
Local AS	
AS Number	Specifies the Local (or virtual) BGP AS number
Rapid Withdrawal	Specifies whether or not to send BGP withdrawal update messages immediately
Min Route Advertisement	Specifies the minimum time before a prefix can be advertised to peer
Next Hop Resolution	Specifies whether the BGP routes can be used to resolve the BGP next hop
Best Path Selection	
Compare Origin Validation State	Specifies whether the origin validation state is used in the BGP decision process
Deterministic MED	Specifies whether the paths will be grouped based on AS before MED attribute comparison
Origin Invalid Unusable	Specifies whether the routes that have an origin validation state of Invalid can be used
Ignore NH Metric	Specifies whether the next hop distance will be ignored during best path selection
Ignore Router ID	Specifies whether the router ID will be ignored during best path selection
Always Compare MED	
MED Value	Specifies the Always Compare MED context
Strict AS	Specifies whether the MED attributes will be compared from same-neighbor AS routes only
AS Path Ignore	
IPv4	Specifies whether the AS path length will be ignored for unlabeled unicast IPv4 routes
IPv6	Specifies whether the AS path length will be ignored for unlabeled unicast IPv6 routes
Label IPv4	Specifies whether the AS path length will be ignored for labeled unicast IPv4 routes
EBGP IBGP Equal	

Parameter	Description
IPv4	Specifies whether to consider EBGP and IBGP labeled IPv4 routes as equal
IPv6	Specifies whether to consider EBGP and IBGP labeled IPv6 routes equal
Label IPv4	Specifies whether to consider EBGP and IBGP unlabeled IPv4 routes equal
Group (**+ ADD**)	
Group Name	Specifies the group name
Damping	Specifies whether the BGP route damping is used to reduce the route flap
Authentication Key	Specifies the BGP authentication key for all peers
Peer AS	Specifies the peer AS number
Peer IP Tracking	Specifies whether the BGP peer tracking is enabled
Prefix Limit (click **+ ADD**)	
Family	Specifies the address family to which the limit applies
Maximum	Specifies the maximum number of routes to be learned from a peer
Threshold	Specifies the percentage threshold that triggers a warning message
Idle Timeout	Specifies the time which BGP peering remains idle before reconnecting
Admin State	Specifies the administrative state of the BGP group
Export (select the check box)	
Policy	Specifies the export policy name
Import (select the check box)	
Policy	Specifies the export policy name
Type	Specifies the BGP peer type
Family (select the check box)	
IPv4	Specifies whether or not to add support for the IPv4 address family

Parameter	Description
IPv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family
MCAST IPv4	Specifies whether or not to advertise support for the MCAST IPv4 address family
Flow IPv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family
Flow IPv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family
MCAST IPv6	Specifies whether or not to advertise support for the MCAST IPv6 address family
Label IPv4	Specifies whether or not to advertise support for the label-IPv4 address family
Neighbor (**+ ADD**)	
Import Policy	Specifies the import policy name
Export Policy	Specifies the export policy name
IP Address	Specifies the IP address that the neighbor uses to communicate with BGP peers
Group Name	Specifies the group name
Peer AS	Specifies the peer AS number
Admin State	Specifies the administrative state of the BGP neighbor
Split Horizon	Specifies whether to prevent routes from being reflected back to the best-route peer
Authentication Key	Specifies the BGP authentication key for the peer
Description	Describes the BGP neighbor
AS Override	Specifies whether the peer's ASN will be replaced by the local ASN in the AS Path
Type	Specifies the BGP peer type
Family (select the check box)	
IPv4	Specifies whether or not to add support for the IPv4 address family
IPv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family

Parameter	Description
MCAST IPv4	Specifies whether or not to advertise support for the MCAST IPv4 address family
Flow IPv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family
Flow IPv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family
MCAST IPv6	Specifies whether or not to advertise support for the MCAST IPv6 address family
Label IPv4	Specifies whether or not to advertise support for the label-IPv4 address family

29

If Enable Static Route was enabled in Step 12, click **+ ADD** in the Static Route Details panel.

The Add Static Route form opens.

30

Configure the parameters, as required:

Parameter	Description
IP Prefix	Specifies the IP prefix of the static route
Prefix Length	Specifies the prefix length for the static route
Route Type	Specifies the static route type
Tag	Specifies the static route tag
Is Blackhole	Specifies whether the prefix is a blackhole route
Next Hop (**+ ADD**)	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Tag	Specifies the static route tag
BFD Liveness	Specifies whether or not to use Bidirectional Forwarding Detection on this static route
Admin State	Specifies the administrative state of the next hop
Indirect (**+ ADD**)	

Parameter	Description
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Tag	Specifies the static route tag
Admin State	Specifies the administrative state of next hop

Click **+ ADD** to add the static route.

The Add Static Route form closes.

31

If Enable IS-IS was enabled in Step 12, click **+ ADD** in the IS-IS panel.

The Add IS-IS form opens.

32

Configure the parameters, as required:

Parameter	Description
IS-IS Instance	Specifies the instance ID for the IS-IS instance
Admin State	Specifies the administrative state of the IS-IS instance
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to the route table
Level Capability	Specifies the routing level for the instance
Advertise Router Capability	Specifies the router capabilities advertisement to neighbors

Click **+ ADD** to add the IS-IS instance.

The Add IS-IS form closes.

33

If Enable OSPF was enabled in Step 12, configure the parameters as required:

Parameter	Description
Compatible RFC-1583	Enables OSPF summary and external route calculations

Parameter	Description
Overload On Boot (select the check box)	
Timeout	Specifies the time during which the router operates in overload state before reestablishing normal operations
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Timers	
Incremental SPF Wait	Specifies the delay time before an incremental SPF calculation starts
LSA Accumulate	Specifies the delay to gather LSAs before advertising to neighbors
LSA Arrival	Specifies the minimum delay between the receipt of the same LSAs from neighbors
Redistribute Delay	Specifies the hold down timer for external routes into OSPF
LSA Generate	
Max LSA Wait	Specifies the maximum time between two LSAs being generated
LSA Initial Wait	Specifies the first wait period between the OSPF LSA generation
LSA Second Wait	Specifies the hold time between the first and second LSA generation
SPF Wait	
Max SPF Wait	Specifies the maximum interval between two consecutive SPF calculations
SPF Initial Wait	Specifies the initial SPF calculation delay after a topology change
SPF Second Wait	Specifies the hold time between the first and second SPF calculation
Graceful Restart (select the check box)	
Helper Mode	Enables graceful restart helper for OSPF
Strict LSA Checking	Enables strict LSA checking during graceful restart helper

34

If Enable RIP was enabled in Step 12, configure the parameters as required:

Parameter	Description
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Metric In	Specifies the metric added to routes received from a RIP neighbor
Metric Out	Specifies the metric added to routes exported into RIP
Preference	Specifies the route preference
Propagate Metric	Enables the BGP MED used to configure the RIP metric
Receive	Specifies the accepted version on received packets
Send	Specifies the RIP version and method used to send RIP updates
Admin State	Specifies the administrative state of the IS-IS instance
Timers	
Update	Specifies the timer that controls the frequency of updates
Timeout	Specifies the RIP timeout timer
Flush	Specifies the RIP flush timer
Group (click **+ ADD**)	
Group Name	Specifies the group name
Admin State	Administrative state of the RIP group
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Metric In	Specifies the metric added to routes received from a RIP neighbor
Metric Out	Specifies the metric added to routes exported into RIP

Parameter	Description
Preference	Specifies the route preference
Propagate Metric	Enables the BGP MED used to configure the RIP metric
Receive	Specifies the accepted version on received packets
Send	Specifies the RIP version and method used to send RIP updates
Timers	
Update	Specifies the timer that controls the frequency of updates
Timeout	Specifies the RIP timeout timer
Flush	Specifies the RIP flush timer

35

Click **+ ADD** to add the site.

The Add Site form closes.

36

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

37

Configure the parameters, as required:

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Interface	Specifies the name of the interface
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP

Parameter	Description
VC ID	Specifies the SDP virtual circuit identifier

Click **+ ADD** to add the SDP binding. The Add SDP form closes.

38

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.7 What are C-Line services?

4.7.1 C-Line services

C-Line services connect two SAPs that can be defined on SONET/SDH, DS3/E3,T1/E1 ports, or TDM channels. NSP 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 NSP.

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, NSP 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 NSP can auto-create channel groups as part of service creation. When channel groups are auto-created, the channel group ID will be the first time slot.

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, this 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 which states that the time slot 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 time slot, a validation error is not triggered and NSP 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, NSP 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 NSP is deleted, NSP will delete the channel groups that are in use.

4.7.2 Brownfield C-Line services

C-Line services created within NFM-P can be managed by the NSP. In order for NSP to discover these services, their "NSD-managed" flag must be enabled within NFM-P. Once discovered by the NSP, these services function the same way as C-Line services created within NSP, provided that they meet the NSP requirements. Any change made to these services within NFM-P after discovery is propagated to NSP if the change impacts the topology of the service.

Note: The C-Line services created within 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 NSP, as the “NSD-managed” flag is disabled upon service deletion, and remains even if the service is recreated and resynchronized in NSP.

4.8 How do I create a C-Line service?

4.8.1 Purpose

Use this procedure to create a C-Line service. The set parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided C-Line template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: The creation of C-Line services is included in Nokia NSP Use Case Catalog as UCC-13. For more information about obtaining access to the catalog and its materials, contact your Nokia sales representative.

4.8.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a C-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
NE Service ID	Specifies the NE service ID
VC Type	Specifies the virtual circuit type
MTU	Specifies the service MTU
Customer ID	Specifies the customer ID
Description	Describes the service

Parameter	Description
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

Continue to the Site A panel.

5

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

6

Click **+ ADD**.

The Add Endpoint form opens.

7

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Time Slots	Specifies the time slot pattern to be used
Admin State	Specifies the administrative state of the service
Description	Describes the SAP

8

In the CEM panel, configure the parameters as required:

Parameter	Description
RTP Header	Specifies whether or not an RTP header is used when packets are transmitted to the Packet Service Network
Payload Size	Specifies the payload size (in bytes) of packets transmitted to the Packet Service Network
Jitter Buffer	Specifies the jitter buffer size (in milliseconds)
Asymmetric Delay Control	
Enable	Specifies whether or not the asymmetric delay control is enabled
Samples	Specifies the number of packets that will be sampled during the sampling period
Repeat Period	Specifies the sampling period (in minutes)

9

Configure the parameters, as required:

Parameter	Description
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

10

If QoS was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy

Parameter	Description
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

11

If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and panels:

Parameter	Description
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the endpoint. The Add Endpoint form closes.

12

Configure the PW Switching parameters, as required:

Parameter	Description
Primary Hub ID	Specifies the identifier of the primary hub
Secondary Hub ID	Specifies the identifier of the secondary hub

13

In the Site B panel, specify the Device ID, then click **+ ADD**.

The Add Endpoint form opens.

14

Repeat Step 5 to Step 12 for Site B.

15

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

16

Configure the parameters, as required:

Parameter	Description
Admin State	Specifies the desired state of the service SDP binding
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier

Click **+ ADD** to add the SDP binding. The Add SDP form closes.

17

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.9 How do I create a redundant C-Line service?

4.9.1 Purpose

Use this procedure to create a redundant C-Line service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided redundant C-Line template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: The creation of C-Line services is included in Nokia NSP Use Case Catalog as UCC-13. For more information about obtaining access to the catalog and its materials, contact your Nokia sales representative.

4.9.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a redundant C-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
NE Service ID	Specifies the NE service ID
VC Type	Specifies the virtual circuit type
MTU	Specifies the service MTU
Customer ID	Specifies the customer ID
Description	Describes the service

Parameter	Description
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the site MTU

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

7

In the Service Endpoints Details panel, click **+ ADD**.

The Add Endpoint form opens.

8

Configure the parameters, as required:

Parameter	Description
Endpoint	Specifies the IP address of the endpoint
Active Multipath	Specifies whether the endpoint is the active multipath

Notes:

1. To enable Active Multipath, the service must be shut down.
2. Active Multipath must be enabled on an endpoint with two spokes
3. When Active Multipath is enabled, ICB cannot be enabled

4. When Active Multipath is enabled, asymmetric-delay cannot be enabled
5. Active Multipath is only supported on SAR devices

9

Repeat Step 7 and Step 8 as required to add additional endpoints.

10

In the SAP Details panel, click **+ ADD**.

The Add SAP form opens.

11

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Time Slots	Specifies the time slot pattern to be used
Admin State	Specifies the administrative state of the service
Description	Describes the SAP

12

In the Service Endpoint panel, specify the endpoint of the SAP.

13

In the CEM panel, configure the parameters as required:

Parameter	Description
RTP Header	Specifies whether or not an RTP header is used when packets are transmitted to the Packet Service Network
Payload Size	Specifies the payload size (in bytes) of packets transmitted to the Packet Service Network
Jitter Buffer	Specifies the jitter buffer size (in milliseconds)

14

In the Asymmetric Delay Control panel, configure the parameters as required:

Parameter	Description
Enable	Specifies whether or not asymmetric delay control is enabled
Samples	Specifies the number of packets that will be sampled during the sampling period
Repeat Period	Specifies the sampling period (in minutes)
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

15

If QoS was enabled in Step 14, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer

Parameter	Description
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	

Parameter	Description
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

16

If an IP/IPv6 filter was enabled in Step 14, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the SAP.

The Add SAP form closes.

17

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

18

Configure the parameters, as required:

Parameter	Description
Destination Device ID	Specifies the SDP destination device identifier

Parameter	Description
Steering Parameter	Specifies the steering parameter used by the NSP
Spoke SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
VC ID	Specifies the SDP virtual circuit identifier
Admin State	Specifies the desired state of the service SDP binding
Endpoint	Specifies the endpoint to associate with the SDP binding

Click **+ ADD** to add the SDP binding.

The Add SDP form closes.

19

Configure the VC Switching parameter in the PW Switching panel.

20

Click **+ ADD**.

The Site Details form closes.

21

Repeat Step 5 and Step 20 as required to add additional sites.

22

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.10 What are IES services?

4.10.1 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 must 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

NSP groups MDM IES service sites based on common Global-IDs supplied by the MDM adaptor artifacts. 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 that links the sites together is removed, the service will be divided into multiple services.

4.11 How do I create an IES service?

4.11.1 Purpose

Use this procedure to create an IES service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided IES template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: The creation of IES services is included in Nokia NSP Use Case Catalog as UCC-16. For more information about obtaining access to the catalog and its materials, contact your Nokia sales representative.

4.11.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an IES service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the first-configured site name and description taking precedence over all others. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

7

Click **+ ADD**.

The Add Interface form opens.

8

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Interface Type	Specifies the interface type (SAP, SDP, or Loopback)
Admin State	Specifies the administrative state of the interface
IP MTU	Describes the interface IP MTU
IPv4	
Address	Specifies the primary IPv4 address to be assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary (click **+ ADD**)	
Address	Specifies the secondary IPv4 address to be assigned to the interface

Parameter	Description
Prefix Length	Specifies the secondary IPv4 address prefix length
IPv6 (click **+ ADD**)	
Address	Specifies the IPv6 address to be assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length
SAP	
Port ID	Specifies the port identifier
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled
VPLS	
VPLS Name	Specifies the name of the VPLS service

9

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

10

In both the IPv4 and IPv6 panels, click **+ ADD** to configure the VRRP parameters as required:

Parameter	Description
Virtual Router ID	Specifies the virtual router identifier (VRID) for the VRRP virtual router instance
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP

Parameter	Description
MAC	Specifies a MAC address to be used by the virtual router instance, overriding the VRRP default derived from the VRID
Ping Reply	Specifies whether or not the non-owner can reply to ICMP echo requests directed to the virtual router instance IP addresses

11

If QoS was enabled in Step 8, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy

Parameter	Description
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

12

If an IP/IPv6 filter was enabled in Step 8, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the interface. The Add Interface form closes.

13

Repeat Step 6 to Step 12 to add additional interfaces.

Click **+ ADD** to add the site(s). The Add Site form closes.

14

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.12 What are Wavence L3 VPN services?

4.12.1 Wavence L3 VPN services

NSP supports L3 VPN services for Wavence nodes. With the introduction of static MPLS, Segment Routing in Shortest Path Forwarding, and static L3 VPN features, Wavence nodes can also be used to support L3 IPv4 data routing services by leveraging the capabilities of MPLS (Multi-Protocol Label Switching) networking using Label Switched Paths (LSPs).

Before extending the support for static L3 VPN, it is required to have support for L3 IPv4 data plane routing and static LSPs in Wavence. This will enable the product to create and configure static IP routes as the means of creating Network Interfaces. The MPLS static LSP feature enables the product to statically assign local labels to an IPv4 prefix. Label Switched Paths (LSPs) can be provisioned for these static labels by specifying the next hop information that is required to forward the packets containing the static label.

All the IPv4 data plane and MPLS (LSP and L3 VPN) related configuration in the Wavence shall be static-configuration provisioned by the user and by the NMS/Carrier SDN Controller; therefore, it is referred to as static MPLS or static L3 VPN.

Support for the OSPFv2 routing protocol for IPv4 and the OSPFv3 routing protocol for IPv6 is added to the IP data plane of Wavence NEs in order to avoid the use of static routes, thereby making every NE aware of the system IP addresses of the other routes, as well as the next hop to be used to reach them.

NSP supports full mesh topology with primary static route configuration, and it allows users to configure one or more SAPs on an L3 VPN service site. Also, Wavence-SR interworking scenarios with full mesh topology are supported for both IPv4 and IPv6 service configurations.

4.13 How do I create a Wavence L3 VPN service?

4.13.1 Purpose

Use this procedure to create a Wavence L3 VPN service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided Wavence L3 VPN template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

4.13.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a Wavence L3 VPN service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Site	Specifies the site to be used
VRF Name	Specifies the name of the VRF
Description	Describes the site
Auto Bind Tunnel	
Resolution	Specifies the MBS of the queue

7

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

8

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Description	Describes the interface
IPv4/IPv6	
Address	Specifies the primary IPv4/IPv6 address assigned to the interface
Prefix Length	Specifies the primary IPv4/IPv6 address prefix length
SAP	
Port ID	Specifies the port identifier
Outer VLAN Tag	Specifies the outer VLAN tag
Description	Describes the SAP

9

Click **+ ADD** to add the interface. The Add Interface form closes.

10

In the Static Route Details panel, click **+ ADD**.

The Add Static Routes form opens.

11

Configure the parameters, as required:

Parameter	Description
IP Prefix	Specifies the IP prefix of the static route
Prefix Length	Specifies the prefix length for the static route
Is Blackhole	Specifies whether the prefix is a blackhole route
Next Hop (**+ ADD**)	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources

Click **+ ADD** to add the static route. The Add Static Route form closes.

12

Click **+ ADD** to add the site.

The Add Site form closes.

13

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.14 How do I create a Wavence Backhaul service?

4.14.1 Purpose

Use this procedure to create a Wavence Backhaul service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided Wavence Backhaul template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: For Wavence Backhaul services, validations from NFM-P are not propagated to NSP. For all the validation or error messages that correspond to service failures seen in NSP, the user should refer to the NFM-P logs.

4.14.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a Wavence Backhaul service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
NE Service ID	Specifies the NE service ID
Ring Element Instance ID	Specifies the Ring Element Instance ID
Search Path	Specifies whether or not to search paths between the endpoints

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Site	Specifies the site to be used
Port ID	Specifies the port identifier
Pass Node	Specifies whether or not the endpoint is a pass through node.
Ring Site	Specifies whether or not the endpoint is part of a ring network
Outer Tag	
Outer Tag	Specifies the outer tag

7

Click **+ ADD** to add the site.

The Add Site form closes.

8

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.15 How do I create a Wavence VPRN service?

4.15.1 Purpose

Use this procedure to create a Wavence VPRN service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided Wavence VPRN template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: For Wavence VPRN services, validations from NFM-P are not propagated to NSP. For all the validation or error messages that correspond to service failures seen in NSP, the user should refer to the NFM-P logs.

4.15.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a Wavence VPRN service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Site	Specifies the site to be used
VRF Name	Specifies the name of the VRF
Description	Describes the site
MTU	Specifies the MTU of the service
Auto Bind Tunnel	
Resolution	Specifies the MBS of the queue

7

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

8

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Description	Describes the interface
IPv4/IPv6	
Address	Specifies the primary IPv4/IPv6 address assigned to the interface
Prefix Length	Specifies the primary IPv4/IPv6 address prefix length
SAP	
Port ID	Specifies the port identifier
Outer VLAN Tag	Specifies the outer VLAN tag
Description	Describes the SAP

9

Click **+ ADD** to add the interface. The Add Interface form closes.

10

In the Static Route Details panel, click **+ ADD**.

The Add Static Routes form opens.

11

Configure the parameters, as required:

Parameter	Description
IP Prefix	Specifies the IP prefix of the static route
Prefix Length	Specifies the prefix length for the static route
Is Blackhole	Specifies whether the prefix is a blackhole route

Click **+ ADD** to add the static route. The Add Static Route form closes.

12

Click **+ ADD** to add the site.

The Add Site form closes.

13

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

14

Configure the parameters, as required:

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Ingress and Egress Label	Specifies the Ingress/Egress Label used by the Wavence node
SDP ID	Specifies the SDP identifier
VC ID	Specifies the SDP virtual circuit identifier

Click **+ ADD** to add the SDP binding. The Add SDP form closes.

15

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.16 How do I create an E-Tree service?

4.16.1 Purpose

Use this procedure to create an E-Tree service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided E-Tree template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

4.16.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an E-Tree service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
NE Service ID	Specifies the NE service ID
MTU	Specifies the MTU of the service
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the first-configured site name and description taking precedence over all others. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

7

In the SAP Details panel, click **+ ADD**.

The Add SAP form opens.

8

Configure the parameters, as required:

Parameter	Description
Root Leaf Tag Value	Specifies the Root Leaf Tag Value
E-Tree Leaf	Specifies whether the E-Tree Leaf access circuit is enabled
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected

9

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.

2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

10

Configure the parameters, as required:

Parameter	Description
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

11

If QoS was enabled in Step 10, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR (kbps)	Specifies the PIR rate of the queue
CIR (kbps)	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer

Parameter	Description
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

12

If an IP/IPv6 filter was enabled in Step 10, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the SAP. The Add SAP form closes.

13

Perform one of the following:

a. If required, repeat Step 7 to Step 12 to add additional SAPs.

b. Continue to Step 14.

14

Configure the parameters in the MEP panel, as required:

Parameter	Description
MD Admin Name	Specifies the admin-assigned maintenance domain index value
MA Admin Name	Specifies the admin-assigned maintenance association index value
MEP ID	Specifies the MEP identifier
MAC Address	Specifies the MAC address of the MEP

Parameter	Description
One Way Delay Threshold	Specifies the time limit for one way delay tests
CCM	Specifies whether or not the MEP will generate CCM tests
CCM LTM Priority	Specifies the priority of CCM and LTM messages transmitted by the MEP
Admin State	Specifies the administrative state of the MEP

Click **+ ADD** to add the site(s). The Add Site form closes.

15

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

16

Configure the parameters, as required:

Parameter	Description
E-Tree Root Leaf Tag	Specifies the E-Tree root leaf tag status
E-tree Leaf	Specifies whether the E-Tree leaf access circuit is enabled
VC Type	Specifies the virtual circuit type, Ether or VLAN
SDP Type	Specifies the SDP type, mesh or spoke
Admin State	Specifies the desired state of the service SDP binding
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier

Click **+ ADD** to add the SDP binding. The Add SDP form closes.

17

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.17 How do I create a VPLS service?

4.17.1 Purpose

Use this procedure to create a VPLS service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided VPLS template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

4.17.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a VPLS service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
VPLS Type	Specifies the virtual circuit type
Management VPLS	Specifies whether or not the service will be used for management
MTU	Specifies the MTU of the service

Parameter	Description
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the MTU of the site
Routed VPLS	Specifies whether or not the VPLS will be routed
STP	
Admin State	Specifies the STP administrative state
Mode	Specifies the protocol version
Priority	Specifies the STP bridge priority
MAC Flush	
Propagate	Specifies whether or not to propagate MAC flush messages that are received from the T-LDP
Send On Failure	Specifies whether or not to send a MAC withdraw message on SAP/Spoke-SDP failure
FDB	
Discard Unknown	Specifies whether or not to discard packets with unknown destination MAC addresses
High Watermark	Specifies the high watermark for the FDB table
Low Watermark	Specifies the low watermark for the FDB table

Parameter	Description
Size	Specifies the maximum MAC entries in the FDB
Learning	Specifies whether or not to enable learning of new MAC addresses
Aging	Specifies whether or not to enable aging of MAC addresses
Local Age Time	Specifies the aging time for locally learned MAC addresses
Remote Age Time	Specifies the aging time for remotely learned MAC addresses
Split Horizon Group (click **+ ADD**)	
Name	The name of the split horizon group to which the SDP belongs
Description	Description of the split horizon group to which the SDP belongs

7

Perform one of the following:

a. If the VPLS Type parameter was set to B-VPLS in Step 4, use the Source B-MAC parameter in the PBB panel to specify the base source B-MAC address for the B-VPLS service.

b. If the VPLS Type parameter was set to I-VPLS in Step 4, configure the parameters, as required:

Parameter	Description
Backbone VPLS Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
ISID	Specifies the ISID of the service

8

In the SAP Details panel, click **+ ADD**.

The Add SAP form opens.

9

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name

10

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

11

Configure the parameters in the CPU Protection Panel, as required:

Parameter	Description
Policy ID	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled
Split Horizon Group (if neither QoS nor IP/IPv6 Filter are enabled)	Name of the split horizon group to which the SDP belongs

12

If QoS was enabled in Step 11, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	

Parameter	Description
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR (kbps)	Specifies the PIR rate of the queue
CIR (kbps)	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed

Parameter	Description
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

13

If an IP/IPv6 filter was enabled in Step 11, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues

Parameter	Description
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier
Split Horizon Group (egress only)	Name of the split horizon group to which the SDP belongs

14

Configure the parameters, as required:

Parameter	Description
FDB	
Maximum MAC Addresses	Specifies the maximum number of MAC entries in the FDB
Discard Unknown Source	Specifies whether or not to discard frames with an unknown source
MAC Pinning	Specifies whether or not to enable MAC address pinning on this SAP
Auto Learn MAC Protect	Specifies whether or not to enable the automatic update of MAC protect list
Learning	Specifies whether or not to enable learning of new MAC addresses
Aging	Specifies whether or not to enable aging of MAC addresses
Anti Spoof	Specifies the type of anti-spoof filtering to be used
Oper Group	Specifies the operational group
IGMP Snooping	
Import Policy	Specifies the import policy that filters IGMP packets
Maximum Number Groups	Specifies the maximum number of groups allowed

Parameter	Description
Send Queries	Specifies whether or not to generate IGMP general queries
Policy	Specifies the multicast CAC policy name
Total	Specifies the maximum allowed bandwidth
Mandatory	Specifies the pre-reserved bandwidth for all mandatory channels
Group (click **+ ADD**)	
Group Addresses	Specifies the group address of static IGMP multicast channel
Source or Starg	Enables adding a list entry for the source
Starg	Specifies any source address (*,G)
Source (click **+ ADD**)	
Source Address	Specifies the source IP address of multicast channel sending data

Click **+ ADD** to add the SAP.

The Add SAP form closes.

15

Perform one of the following:

a. If required, repeat Step 8 to Step 14 to add additional SAPs.

b. Continue to Step 16.

16

Configure the parameters in the MEP panel, as required:

Parameter	Description
MD Admin Name	Specifies the admin-assigned maintenance domain index value
MA Admin Name	Specifies the admin-assigned maintenance association index value
MEP ID	Specifies the MEP identifier
MAC Address	Specifies the MAC address of the MEP
One Way Delay Threshold	Specifies the time limit for one way delay tests

Parameter	Description
CCM	Specifies whether or not the MEP will generate CCM tests
CCM LTM Priority	Specifies the priority of CCM and LTM messages transmitted by the MEP
Admin State	Specifies the administrative state of the MEP

Click **+ ADD** to add the site(s).

The Add Site form closes.

17

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

18

Configure the parameters, as required:

Parameter	Description
SDP Type	Specifies the SDP type, mesh or spoke
VC Type	Specifies the virtual circuit type, ether or VLAN
Admin State	Specifies the desired state of the service SDP binding
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier
FDB	
Maximum MAC Addresses	Specifies the maximum number of MAC entries in the FDB
Discard Unknown Source	Specifies whether or not to discard packets with unknown destination MAC addresses

Parameter	Description
MAC Pinning	Specifies whether or not to enable MAC address pinning on this SAP
Auto Learn MAC Protect	Specifies whether or not to enable an automatic update of the MAC protect list
IGMP Snooping	
Maximum Number Groups	Specifies the maximum number of groups allowed
DHCP	
Snoop	Specifies whether or not to allow DHCP snooping of DHCP messages on the SAP or SDP
Force VC Forwarding	Specifies the VC forwarding action
Control Ward	Specifies whether or not to use the control word as preferred

Click **+ ADD** to add the SDP binding.

The Add SDP form closes.

19

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.18 How do I create an EVPN E-Line service?

4.18.1 Purpose

Use this procedure to create an EVPN E-Line service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided EVPN E-Line template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

4.18.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an EVPN E-Line service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
NE Service ID	Specifies the NE service ID
MTU	Specifies the service MTU
EVPN Type	Specifies the EVPN type

Continue to the Site A panel.

5

Configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the site MTU
EVI	Specifies the EVPN ID
ECMP	Specifies maximum ECMP routes information
Local AC	
Name	Specifies the attachment circuit name
Eth Tag	Specifies the Ethernet tag of the attachment circuit
Remote AC	
Name	Specifies the attachment circuit name
Eth Tag	Specifies the Ethernet tag of the attachment circuit

Note: If site names and descriptions are added, these will take precedence over any service name and description specified in Step 4, with the Site A name and description taking precedence over Site B. As such, these attributes will be displayed in various locations, such as the NSP Model Driven Configurator function and NFM-P.

6

In the SAP Details panel, click **+ ADD**.

The Add SAP form opens.

7

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag

Parameter	Description
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name

8

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

9

Configure the parameters in the CPU Protection panel, as required:

Parameter	Description
Policy ID	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

10

If QoS was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	

Parameter	Description
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

Parameter	Description
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

11

If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **+ ADD** to add the SAP.

The Add SAP form closes.

12

Configure the Multi-Homing Site Details parameters, as required:

Parameter	Description
Device ID	Specifies the device identifier
Route Distinguisher	Specifies the route distinguisher
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name

13

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

14

Configure the CPU Protection parameter, as required:

Parameter	Description
Policy ID	Specifies the CPM protection policy

15

If the EVPN Type parameter was set to MPLS in Step 4, configure the parameters, as required:

Parameter	Description
BGP Instance	
Route Distinguisher	Specifies the route distinguisher

Parameter	Description
VSI Import	Specifies the VSI import policies
VSI Export	Specifies the VSI export policies
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
Force VC Forwarding	Specifies the VC forwarding action to be taken
Auto Bind Tunnel	
Resolution	Specifies the resolution method for tunnel selection
Enforce Strict Tunnel Tagging	Specifies whether or not only LSPs marked with an admin-tag will be used for next hop resolution
Resolution Filter	
BGP	Specifies whether or not BGP type auto bind tunnels will be used
RSVP	Specifies whether or not RSVP type auto bind tunnels will be used
SR-TE	Specifies whether or not SR-TE type auto bind tunnels will be used
GRE	Specifies whether or not GRE type auto bind tunnels will be used
SR-ISIS	Specifies whether or not SR-ISIS type auto bind tunnels will be used
LDP	Specifies whether or not LDP type auto bind tunnels will be used
SR-OSPF	Specifies whether or not SR-OSPF type auto bind tunnels will be used

16

If the EVPN Type parameter was set to VXLAN in Step 4, configure the parameters, as required:

Parameter	Description
BGP Instance	

Parameter	Description
Route Distinguisher	Specifies the route distinguisher
VSI Import	Specifies the VSI import policies
VSI Export	Specifies the VSI export policies
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
VNI	Specifies the VNI of the VXLAN

17

Repeat Step 5 to Step 16 for Site B.

18

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.19 How do I create an EVPN VPLS service?

4.19.1 Purpose

Use this procedure to create an EVPN VPLS service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided EVPN VPLS template is being used.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

4.19.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on an EVPN VPLS service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
MTU	Specifies the MTU of the service
NE Service ID	Specifies the NE service ID

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
EVPN Type	Specifies the EVPN type
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the MTU of the site
EVI	Specifies the protocol version
ECPM	Specifies the STP bridge priority
Routed VPLS	Specifies whether or not the VPLS will be routed

7

Configure the parameters in the MAC Flush panel, as required:

Parameter	Description
T-LDP	
Propagate	Specifies whether or not to propagate MAC flush messages that are received from the T-LDP
Send On Failure	Specifies whether or not to send a MAC withdraw message on SAP/Spoke-SDP failure

8

Configure the parameters in the MAC Duplication panel, as required:

Parameter	Description
Retry	Specifies the BGP EVPN MAC duplication retry
Blackhole	Specifies whether or not blackhole duplication MAC configuration is enabled
Detect	

Parameter	Description
Num Moves	Specifies the BGP EVPN MAC duplication detection number of moves
Window	Specifies the BGP EVPN MAC duplication detection window

9

Select the Proxy ARP check box, as required, then configure the parameters in that panel:

Parameter	Description
Admin State	Specifies the administrative state of the proxy
Dynamic Populate	Specifies whether or not to populate proxy ARP entries from snooped GARP/ARP/ND messages on SAP/SDP-bindings

10

Configure the parameters in the FDB panel, as required:

Parameter	Description
Discard Unknown	Specifies whether or not to discard packets with unknown destination MAC addresses
Table	
High Watermark	Specifies the high watermark for the FDB table
Low Watermark	Specifies the low watermark for the FDB table
Size	Specifies the maximum MAC entries in the FDB
MAC Learning	
Learning	Specifies whether or not to enable learning of new MAC addresses
Aging	Specifies whether or not to enable aging of MAC addresses
Local Age Time	Specifies the aging time for locally learned MAC addresses
Remote Age Time	Specifies the aging time for remotely learned MAC addresses

Parameter	Description
Split Horizon Group (click **+ ADD**)	
Name	The name of the split horizon group to which the SDP belongs
Description	Description of the split horizon group to which the SDP belongs
CFM MAC (if MPLS was selected)	Specifies whether or not to enable advertisement and withdrawal of MAC address

11

If the EVPN Type parameter was set to VXLAN or Both in Step 6, configure the parameters, as required:

Parameter	Description
Tunnel Interface	Specifies the tunnel interface name
VNI	Specifies the VNI of the VXLAN
BGP Instance	
BGP Instance ID	Specifies the BGP instance identifier
Route Distinguisher	Specifies the route distinguisher
VSI Import	Specifies the VSI import policies
VSI Export	Specifies the VSI export policies
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
CFM MAC	Specifies whether or not to enable advertisement and withdrawal of MAC address

12

If the EVPN Type parameter was set to MPLS or Both in Step 6, configure the parameters, as required:

Parameter	Description
BGP Instance	
BGP Instance ID	Specifies the BGP instance identifier

Parameter	Description
Route Distinguisher	Specifies the route distinguisher
VSI Import	Specifies the VSI import policies
VSI Export	Specifies the VSI export policies
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
Admin State	Allows for administratively enabling/disabling BGP-EVPN MPLS
Force VC Forwarding	Specifies the VC forwarding action to be taken
Ingress Replication Bum Label	Specifies whether or not to use the same label as the one advertised for unicast traffic
Auto Bind Tunnel	
Resolution	Specifies the resolution method for tunnel selection
Enforce Strict Tunnel Tagging	Specifies whether or not only LSPs marked with an admin-tag will be used for next hop resolution
Resolution Filter	
BGP	Specifies whether or not BGP type auto bind tunnels will be used
RSVP	Specifies whether or not RSVP type auto bind tunnels will be used
SR-TE	Specifies whether or not SR-TE type auto bind tunnels will be used
GRE	Specifies whether or not GRE type auto bind tunnels will be used
SR-ISIS	Specifies whether or not SR-ISIS type auto bind tunnels will be used
LDP	Specifies whether or not LDP type auto bind tunnels will be used
SR-OSPF	Specifies whether or not SR-OSPF type auto bind tunnels will be used
IGMP Snooping	

Parameter	Description
Admin State	Specifies the administrative state of snooping
Report Source Address	Specifies the source IP address used when generating IGMP reports
Query Source Address	Specifies the source address for IGMP queries

13

In the SAP Details panel, click **+ ADD**.

The Add SAP form opens.

14

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected
Multi Service Site	Specifies the multi service site name
CPU Protection	
Policy ID	Specifies the CPM protection policy
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled
Split Horizon Group (if neither QoS nor IP/IPv6 Filter are enabled)	Name of the split horizon group to which the SDP belongs

15

If QoS was enabled in Step 14, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (select the check box)	
Max Rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click **+ ADD**)	
Priority Level	Specifies the priority level

Parameter	Description
MBS Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
CIR Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
VLAN QoS Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues
Split Horizon Group	Name of the split horizon group to which the SDP belongs

16

If an IP/IPv6 filter was enabled in Step 14, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
Aggregate Policer (ingress only)	
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
CIR	Specifies the aggregate policer CIR
CBS	Specifies the aggregate policer CBS
IP/IPv6 Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier
Split Horizon Group (egress only)	Name of the split horizon group to which the SDP belongs

17

Configure the parameters in the FDB panel, as required:

Parameter	Description
Maximum MAC Addresses	Specifies the maximum number of MAC entries in the FDB
Discard Unknown Source	Specifies whether or not to discard frames with an unknown source
Auto Learn MAC Protect	Specifies whether or not to enable an automatic update of the MAC protect list
MAC Learning	
Learning	Specifies whether or not to enable learning of new MAC addresses
Aging	Specifies whether or not to enable aging of MAC addresses

18

Configure the parameters in the IGMP Snooping panel, as required:

Parameter	Description
Import Policy	Specifies the import policy that filters IGMP packets
Maximum Number Groups	Specifies the maximum number of groups allowed

Parameter	Description
Send Queries	Specifies whether or not to generate IGMP general queries
MCAC	
Policy	Specifies the multicast CAC policy name
Bandwidth	
Total	Specifies the maximum allowed bandwidth
Mandatory	Specifies the pre-reserved bandwidth for all mandatory channels
Group (click **+ ADD**)	
Group Addresses	Specifies the group address of static IGMP multicast channel
Source or Starg	Enables adding a list entry for source
Starg	Specifies any source address (*,G)
Source (click **+ ADD**)	
Source Address	Specifies the source IP address of multicast channel sending data

Click **+ ADD** to add the SAP.

The Add SAP form closes.

19

Perform one of the following:

a. If required, repeat Step 13 to Step 18 to add additional SAPs.

b. Continue to Step 20.

20

Click **+ ADD** to add the Site. The Add Site form closes. Perform one of the following:

a. If required, repeat Step 5 to Step 19 to add additional sites.

b. Continue to Step 21.

21

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

4.20 How do I create a composite service?

4.20.1 Purpose

Use this procedure to create a composite service. A composite service allows users to configure multiple service types simultaneously, then execute those service types as a single service. The set of parameters that are available to you is dependent on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided composite service template is being used. The Nokia-provided composite service template allows for the configuration of both an L3 VPN and an E-Line service.

Before attempting to perform this procedure, ensure that you have read 4.1.1 “Service creation prerequisites” (p. 43).

Note: Service management does not support brownfield composite services.

4.20.2 Steps

1

Perform 2.2 “How do I create a service template?” (p. 26).

2

From the **Service Management, Composite Services** view, click **+ CREATE**.

The Select a service template to start form opens, displaying a list of service templates.

3

Click on a composite service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Customer ID	Specifies the customer ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

5

In the VPRN panel, configure the Service Name parameter, specifying a name for the VPRN service that is unique from other services created using the NSP.

6

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

7

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the assigned queue group redirect list
VRF Name	Specifies the name of the VRF
Description	Describes the VRF
NE Service ID	Specifies the NE service ID
Route Distinguisher	Specifies the route distinguisher
Route Distinguisher Type	Specifies the route distinguisher type
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value

8

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

9

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Interface Type	Specifies the interface type
Description	Describes the interface
Administrative State	Specifies the administrative state of the interface

Parameter	Description
Loopback	Specifies whether to use the interface as a loopback interface
IP MTU	Specifies the interface IP MTU
Ingress Stats	Specifies whether or not ingress statistics will be collected

10

In the IPv4 panel, configure the required parameters:

Parameter	Description
Address	Specifies the primary IPv4 address assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length

11

If the Interface Type parameter was set to SAP in Step 9, configure the parameters in the SAP panel, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected

12

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

13

Click **+ ADD**. The Add Interface form closes.

14

Click **+ ADD**. The Add Site form closes.

15

In the EPIPES panel, click **+ ADD**.

The Add EPIPES form opens.

16

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
NE Service ID	Specifies the NE service ID

17

In the Site Details panel, configure the required parameters:

Parameter	Description
Device ID	Specifies the device identifier
Site Name	Specifies the site name
Description	Describes the site
MTU	Specifies the MTU of the site
Endpoint	
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
Collect Accounting Statistics	Specifies whether or not accounting statistics will be collected

18

Perform the following to specify an accounting policy to be used:

1. Click on the Accounting Policy field. The Select Accounting Policy form opens.

2. Click on an accounting policy in the list, then click **SELECT**. The Select Accounting Policy form closes.

19

In the Site Details panel, configure the required parameters:

Parameter	Description
Enable QoS	Specifies whether or not QoS is enabled
Enable IP/IPv6 Filter	Specifies whether or not an IP/IPv6 filter is enabled

20

If QoS was enabled in Step 19, configure the parameters as required in both the ingress and egress panels:

Parameter	Description
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether the top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier of the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR (kbps)	Specifies the PIR rate of the queue
CIR (kbps)	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier of the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer

Parameter	Description
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR (kbps)	Specifies the PIR rate of the scheduler
CIR (kbps)	Specifies the CIR rate of the scheduler

21

Click **+ ADD**.

The Add EPIPES form closes.

22

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

23

Configure the parameters, as required:

Parameter	Description
Service Type	Specifies the service type
Service Name	Specifies the name of the service, which must be unique from other services created using the NSP.
Admin State	Specifies the desired state of the service SDP binding
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by the NSP
SDP ID	Specifies the SDP identifier
Description	Describes the SDP binding

Parameter	Description
Override VC ID	Specifies whether or not the VC ID will serve as the NE service ID for the SDP
VC ID	Specifies the SDP virtual circuit identifier
Interface Name (l3vpn service type only)	Species the name of the interface
VC Type	Specifies the virtual circuit type, Ether or VLAN

24

Click **+ ADD**.

The Add SDP form closes.

25

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

Note: A list of existing composite services can be viewed from the SERVICES page by choosing Composite Services from the drop-down list. Attempting to align a composite service by choosing the Pull from Network option will result in an error.

END OF STEPS

4.21 How do I audit a service?

4.21.1 Steps

1

Perform one of the following:

a. From the **Service Management, Services** view, click ⋮ (Table row actions), **Audit config** in-line with any service.

Note: Users can select up to 10 services at a time to run the Audit Config action against.

b. From the **Service Management, Services** view, click on a service in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

The service is audited.

2

If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

The Audit Result form closes.

3

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, perform one of the following:

a. Click ⋮ (Table row actions), **Align**, and then either **Push to network** or **Pull from network** in-line with the previously-audited service.

b.

1. Click on a service in the list, then expand the Alignment State section in the info panel and click **ALIGN**. The Select Alignment form opens.
2. Select the **Push to network** or **Pull from network** radio button, then click **CONTINUE**. The Select Alignment form closes.

The service is synchronized with the network.

END OF STEPS

4.22 How do I execute a service function?

4.22.1 Purpose

Use this procedure to execute a service function of an existing service.

Note: In order to execute a service function, the service must have been created from an intent type that was configured with one or more custom service functions. See the *NSP Network Automation Guide* for more information.

4.22.2 Steps

1

From the **Service Management, Services** view, click on a service in the list, then expand the Service Functions section in the info panel. A list of service functions is displayed.

2

Click **Execute service function** in-line with any service function to execute that service function.

END OF STEPS

4.23 How do I migrate a service from one service template to another?

4.23.1 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **Migrate** in-line with any service currently associated with a service template. The Migrate selected service(s) to a template form opens.

Note: Users can select up to 10 services at a time to run the Migrate action against.

Note: If two VLAN services have been created with the same Sites/Adjacencies, any attempt to migrate one of these services will cause both to be migrated, even if they have different VLAN Service IDs.

2

Click the Template Name field and, from the list, select the desired service template to which to migrate.

Note: Only service templates of the same intent type as the service's current service template are available for selection.

3

Click **CONFIRM**. The Migrate selected service(s) to a template form closes and the service is migrated to the desired service template.

END OF STEPS

4.24 How do I unassociate a service from a service template?

4.24.1 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **Unassociate** inline with any service currently associated with a service template. A dialog box appears.

Note: Users can select up to 10 services at a time to run the Unassociate action against.

Note: To be eligible for the Unassociate action, services must have at least one site and a life cycle state of Deployed

2

Click **CONFIRM**. The dialog box closes and the service is unassociated from the service template.

END OF STEPS

4.25 What brownfield services are visible from service management?

4.25.1 Visible brownfield services

When deployed in a system that includes an NFM-P, NSP is able to synchronize with the NFM-P and display any previously-created services, also known as brownfield services. If these services are of a type supported by Nokia product intents, full management of the services is possible. If the services are of another type, they will appear within NSP but with limited options for viewing. Some such services types include:

- A-Pipe
- F-Pipe
- I-Pipe
- H-Pipe
- Microwave L2 BH
- MVPLS
- VLAN

4.26 How do I lock service attributes?

4.26.1 Locking service attributes

A user can lock specific service attributes after saving their initial service configurations. This prevents those attributes from being modified again prior to the service being deployed. To lock a service attribute, the createMode parameter must be set to true within the viewConfig file in the desired service intent (this parameter is set to false by default). Once this step is completed, the attribute will become read-only. The following example demonstrates the syntax within the viewConfig file:

```
"epipe.site-a.site-name":
{
"title": "Site Name",
"required": false,
"createMode": true
}
```

4.27 How is service stitching accomplished?

4.27.1 Service stitching

When an MDM-managed NE with existing service configurations is discovered, these configurations are not auto-populated into the operational service model, but are instead placed into an alternate table space. This means that these service configurations cannot be seen by NSP functions such as service management or object troubleshooting. In order for the NSP to see these services, service stitching must be performed. NSP uses a service stitching algorithm to stitch these MDM-managed service sites into single service entities based on service type and predefined, corresponding algorithm. These services are persisted in the NSP database, making them visible (read-only) from the NSP's service management views. Users can then associate the services to a template, which would enable full lifecycle management and CRUD support. Service stitching can be triggered manually using an API, or by enabling auto-stitch.

The following service types and their predefined, corresponding algorithms are supported for service stitching:

Table 4-1 Supported service types and algorithms for stitching

Service type	Algorithms
E-Line	vcid, evi, route-target, local and service-name
E-LAN	vcid, evi, route-target, service-name
IES	service-name
L3 VPN	route-target, service-name

Note: The required artifacts for service stitching are contained in the svc-mgt-artifacts-common bundle, which can be obtained from the artifacts section of the Nokia Support Portal.

4.27.2 Service stitching API

Service stitching can be manually triggered using the POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices) API. The following is an example of the request body:

```
{
    "input":{
    "service-type": <service-type>,
    "algorithm": <name-of-algorithm>,
    "sites":["2.2.2.2","3.3.3.3]
    }
}
```

where

service-type is either eline, elan, ies, or l3vpn

name-of-algorithm is the name of a supported algorithm that corresponds to the service-type

sites is a list of one or more MDM-managed service sites

Visit the Nokia Network Developer Portal for more information.

4.27.3 Auto-stitching

By default, the automatic stitching of services is disabled. Users can either stitch a service manually using the service stitching API, or enable auto-stitching of specific service types and predefined, corresponding algorithms using the auto-stitching API. Automatic service stitching can be enabled using the POST: (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config={{service-type}} API. Setting an algorithm's admin-state to 'unlocked' enables automatic service stitching for that algorithm. The following is an example of the request body, where 'eline' was used as the service-type.

```
{
    "nsp-service-stitch:nsp-service-auto-stitch-config": [
      {
        "service-type": "eline",
        "admin-state": "unlocked",
        "algorithm-config": [
          {
            "algorithm": "evi",
            "admin-state": "locked"
          },
          {
            "algorithm": "vcid",
            "admin-state": "locked"
          },
          {
            "algorithm": "route-target",
            "admin-state": "locked"
          },
          {
            "algorithm": "service-name",
            "admin-state": "unlocked"
          },
          {
```

```
                "algorithm": "local",
                "admin-state": "locked"
            }
        }
    ]
}
```

4.27.4 Managing and unmanaging NEs

If an MDM-managed NE is unmanaged after service stitching has been successfully performed, the sites/endpoints/tunnel-bindings are deleted from the services, but empty services will persist in the operational model. If a user wants to delete these services, they must do so manually. The sites in the alternate tables are automatically deleted after the node is unmanaged. Should any remain, they must be deleted manually as well.

If the user re-manages the same node, the following behavior will occur:

- The sites will be discovered in alternate tables
- No entry will be made in operational model tables until stitching (automatic or manual) is used to stitch the services

After stitching occurs, there is no guarantee that the same number of services will stitch as when the node was previously managed. This is dependent on the stitching algorithm. The same name is also not guaranteed.

If the empty services were not deleted, there is no guarantee that the newly-stitched sites will attach with those services.

4.28 How do I create services on SDPs with multiple loopback addresses?

4.28.1 Creating services on SDPs with multiple loopback addresses

NSP 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 NFM-P or on NEs. NSP does not support the creation of new service tunnels using loopback IP addresses.

Before you start configuring a service in NSP, you must create SDP tunnels with loopback IP addresses in 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 on the Service Management, Service Tunnels view. 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.

4.29 How do I approve misalignments?

4.29.1 Approving misalignments

NSP allows the user to approve misaligned attributes, missing objects, and undesired objects that are affecting their services. In these cases, a discrepancy exists between the service management instance of an entity and the instance of the entity that exists in the network. An approved misalignment no longer contributes to a service's misaligned state. Therefore, approving all misalignments affecting a service would cause that service to be categorized as aligned.

Note: Artifacts from earlier NSP releases are supported in general, but customers must upgrade to artifacts from NSP Release 23.11 or later in order to use the approved misalignments feature. If custom artifacts are being used, customers should contact Nokia Professional Services to have these updated.

Note: When a misalignment is approved, the username of the user who provided approval is recorded, as well as a timestamp. If another user approves subsequent misalignments on the same entity, that timestamp will be overwritten, and this user's username will be applied to all historical approvals, overwriting the original.

4.29.2 Steps

1

From the **Service Management, Services** view, perform one of the following:

a. Click ⋮ (Table row actions), **Audit config** in-line with a misaligned entity. The Audit Result form opens.

b. Select a misaligned entity from the list, then expand the Alignment State section of the info panel and click **AUDIT CONFIG**. The Audit Result form opens.

2

Click on one or more of the following tabs: MISALIGNED ATTRIBUTES, MISSING OBJECTS, and/or UNDESIRED OBJECTS, then select one or more entries from the list(s) and click **APPROVE SELECTED**. The selected misaligned attributes, missing objects, or undesired objects are moved to the list of approved misalignments.

3

As required, click on the APPROVED MISALIGNMENTS tab, select one or more entries from the list, then click **REMOVE APPROVAL**. The selected entries are returned to their initial tabs/ lists.

Note: A list of misalignments that have been approved across all entities in the network is available from the **Service Management, Approved Misalignments** view.

END OF STEPS

4.30 How do I clone a service?

4.30.1 Cloning services

This procedure can be used to clone a service. Cloning services enables the operator to use a previously-created service as a starting point for service creation, retaining configuration details.

4.30.2 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **Clone** in-line with any service. The Service Creation form opens with the existing service's configured attributes populated.

2

Provide a unique name for the service instance and resolve any other conflicts with the existing service.

3

Perform one of the following:

a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.3 “What is the state of my service or tunnel?” (p. 14) for more information.

END OF STEPS

5 Workflows

5.1 How do service management and workflows interact?

5.1.1 Service management and workflows

The NSP service management and workflows functions are integrated. When installed, service management can be used as a single tool to plan and automate service life cycle operations, and execute automated workflows to support service activation and enablement.

Note: A user must have Read/execute or Read/write/execute permissions within the NSP service management function to execute workflows.

In order for workflows to be visible within the service management views, the workflow must be configured in the workflows function with the appropriate tag. These tags allow administrators to restrict workflows that are available to support service management operations without giving users access to all workflows. The *sf-service-operation* tag fetches service operation workflows, while the *sf-network-operation* tag fetches network operation workflows.

Using workflows can extend automated service operation capabilities in three ways:

1. Enforce input form validation rules during service create/modify operations.
2. Automatically perform pre/post deployment tasks and validations during service life cycle operations.
3. Use the Workflow Execution tool to perform automated actions/tasks/workflows on existing services and network objects.

Workflows to perform the validation of input forms and perform pre/post deployment tasks are configured on a service or tunnel template.

The Workflow Execution tool in service management allows you to select a workflow defined for service operations, input workflow parameters as required, monitor execution status, and view the input/output of execution results. You can also view past workflow executions and results for a selected service.

5.2 How do I execute a network operation workflow?

5.2.1 Purpose

Network operation workflows are tagged with *sf-network-operation*. This tag fetches network workflows from the NSP Workflows function. A network operation workflow allows you to perform generic tasks, such as the provisioning of ports or interfaces, and checking device or network health.

5.2.2 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **Execute Workflow** in the top right corner.

The Network Workflow Execution form opens.

2

Click on a workflow in the Select a workflow drop-down list.

A request is sent to the workflows function to retrieve a list of all workflows that have been tagged with *sf-network-operation.*

3

Configure the input parameters, as required:

The inputs are product by the user in the workflow's Input form.

You can adjust the width of the input rows using the React Schema form.

4

Click **EXECUTE.**

The execution status is displayed.

5

Click **VIEW RESULTS** to view the input/output data from the executed workflow.

6

Click **CLOSE**.

END OF STEPS

5.3 How do I execute a service operation workflow?

5.3.1 Purpose

Service operation workflows are tagged with *sf-service-operation*. This tag fetches service workflows from the workflows function. A service operation workflow allows you to perform automated tasks against an individual service.

5.3.2 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **Execute Workflow** in-line with any service.

The Service Workflow Execution form opens.

2

Click on a workflow in the Select a workflow drop-down list.

A request is sent to the workflows function to get a list of all workflows that have been tagged with *sf-service-operation*.

3

Configure the input parameters, as required:

The inputs are product by the user in the workflow's Input form.

You can adjust the width of the input rows using the React Schema form.

4

Click **EXECUTE**.

The execution status is displayed.

5

Click **VIEW RESULTS** to view the input/output data from the executed workflow.

6

Click **CLOSE**.

END OF STEPS

5.4 How do I view workflow executions on services?

5.4.1 Purpose

Use this procedure to view the workflows that were previously executed against any service.

5.4.2 Steps

1

From the **Service Management, Services** view, click ⋮ (Table row actions), **View Workflow Executions** in-line with any service.

A list of Executed Workflows is displayed.

2

Click **View Input/Output** in-line with any executed workflow.

The Quick View form opens, displaying input/output data.

Workflow execution information is stored for 90 days.

3

Click **CLOSE**.

END OF STEPS

5.5 How do I execute a tunnel operation workflow?

5.5.1 Purpose

Service operation workflows are tagged with *sf-tunnel-operation*. This tag fetches service workflows from the NSP Workflows function. A tunnel operation workflow allows you to perform automated tasks against an individual service tunnel.

5.5.2 Steps

1

From the **Service Management, Service Tunnels** view, click ⋮ (Table row actions), **Execute Workflow** in-line with any service tunnel.

The Tunnel Workflow Execution form opens.

2

Click on a workflow in the Select a workflow drop-down list.

A request is sent to the NSP Workflows function to get a list of all workflows that have been tagged with *sf-tunnel-operation*.

3

Configure the input parameters, as required:

The inputs are product by the user in the workflow's Input form.

You can adjust the width of the input rows using the React Schema form.

4

Click **EXECUTE**.

The execution status is displayed.

5

Click **VIEW RESULTS** to view the input/output data from the executed workflow.

6

Click **CLOSE**.

END OF STEPS

5.6 How do I view workflow executions on service tunnels?

5.6.1 Purpose

Use this procedure to view the workflows that were previously executed against any service tunnel.

5.6.2 Steps

1

From the **Service Management, Service Tunnels** view, click ⋮ (Table row actions), **View Workflow Executions** in-line with any service tunnel.

A list of Executed Workflows is displayed.

2

Click **View Input/Output** in-line with any executed workflow.

The Quick View form opens, displaying input/output data.

Workflow execution information is stored for 90 days.

3

Click **CLOSE**.

END OF STEPS