NOKIA

NSP
Network Services Platform

Release 22.11

User Guide

3HE-18121-AAAE-TQZZA

Issue 1

November 2022

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

The *NSP User Guide* introduces the Network Services Platform, or NSP, to technology officers and network operators by describing at a high level the NSP concepts, product offerings, and functional scope. For operators, the guide also includes general system access, application usage, and troubleshooting information.

Scope

The NSP User Guide information primarily describes elements that are common to all NSP deployments, but may also include high-level information about optional NSP functions that are separately licensed and deployed.

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 Product description

1.1 System components

1.1.1 Overview

The NSP architecture accommodates a wide variety of network management functions and interworking capabilities. In addition to the core system elements, an NSP deployment may include ancillary devices or appliances, other products, and multiple interfaces to in-house or third-party systems. For example, the NFM-P, NSP analytics servers, and the NFM-T product can be included in an NSP system that forwards statistics and other data to various types of OSS or application clients. See the *NSP System Architecture Guide* for details.

Table 1-1 NSP system component overview

Component	Description
Common nspOS components	The following components make up the base NSP platform: • Login—grants SSO access to all NSP applications, GUI clients, and other resources on the NSP Launchpad • NSP Launchpad—entry point for all NSP applications; includes Network Health Dashboard and Troubleshooting Dashboard on shared-mode NSP deployments • Central Authentication Server, or CAS—authenticates user login attempts • Session Manager—tracks and manages SSO sessions • REST API Gateway—acquires NSP REST API tokens and locates specific NSP APIs • NSP PKI Server—generates TLS certificates for system-wide NSP deployment
Web-based applications	The NSP provides an array of browser-based network management applications. The purchased feature packages, selected installation options, and operator privilege levels determine which applications are available to network operators.
VSR-NRC	The Virtual Service Router - Network Resources Controller (VSR-NRC) acts in a Virtual Network Function (VNF) capacity to perform topology discovery. The VSR-NRC is based on the SROS software, and implements the southbound protocols of the IP/MPLS Optimization application, which consist of the Path Computation Element (PCE) function, with PCEP, BGP-LS and IGP protocols, and the OpenFlow Controller (OFC).
NFM-P	The NFM-P is a network management system that functions as an NSP component. It simplifies routine operations and allows the bulk provisioning of network objects. The system is designed using industry standards such as Java, XML/SOAP, REST, and WebDAV. The NFM-P uses open-standard interfaces that allow the system to interoperate with a variety of other network monitoring and management systems. For information about transitioning from NFM-P alarm management to the NSP, see "Transitioning to alarm management and topology maps on the NSP" (p. 35).

Table 1-1 NSP system component overview (continued)

Component	Description
NFM-T	The NFM-T is a standalone optical network management product that can also function as an NSP component. The NFM-T provides end-to-end optical management functions that include service provisioning over multi-technology optical transport networks such as SDH/SONET, carrier Ethernet, WDM, ROADM, OTN, and packet. Browser-based fault management applications reduce the time and cost of network and service assurance operations, and an API enables OSS integration. For more information about the NFM-T, see the *NFM-T Getting Started Guide*.
NSP Flow Collectors and Flow Collector Controllers	An NSP Flow Collector is an optional, scalable component that collects AA Cflowd or System Cflowd statistics directly from NEs and forwards the statistics records to one or more remote target servers, or to an NFM-P database, after which they are available for processing by third-party tools or by applications such as NSP Analytics.
NSP Analytics servers	An NSP analytics server creates on-demand and scheduled reports about various network conditions and trends for display in the NSP Analytics application. An analytics server generates the reports using business intelligence software to analyze raw and aggregated NE statistics data collected by the NFM-P.
Data stores	The NSP uses various forms of persistent storage for statistics and network data model information. Depending on the deployment, the NSP can store information in the NFM-P database or auxiliary databases.

1.2 User perspectives

1.2.1 User roles and responsibilities

NSP operators typically fall into the following user categories, depending on their areas of expertise and functional roles in an organization.

Table 1-2 NSP user perspectives

User perspective	Description	NSP applications used
Developers	Application developers use the NSP REST API to provision and monitor network objects, and to subscribe to real-time network event notifications. The REST API supports service assurance, and IP/MPLS and optical network management functions.	Intent Manager Resource Administrator Model Driven Mediation Modeled Device Configurator Policy Management REST API Workflow Manager
Network engineers	A network engineer is responsible for device configuration, NE software and script management.	Device Administrator Intent Manager Resource Administrator Modeled Device Configurator

Table 1-2 NSP user perspectives (continued)

User perspective	Description	NSP applications used
Network designers	A network designer is involved in network planning work, including IP/optical network connectivity, routing management, and network optimization.	Device Administrator IP/MPLS Optimization Policy Management Modeled Device Configurator Transport Slice Controller Wireless NE Views Workflow Manager
Administrators	An NSP system administrator can manage all NSP functional areas, including system security, user access control, application setup, system component management, and database management.	Group Manager User Manager
Operators	A network operator takes care of routine tasks, including network fault detection and troubleshooting, equipment health, and service infrastructure monitoring.	Analytics Fault Management Insights Administrator IP/MPLS Optimization Network Supervision Network Health Dashboard Troubleshooting Dashboard Service Supervision Transport Slice Controller Insights Viewer Wireless Supervision
Service delivery staff	Service delivery staff are responsible for multi-layer service provisioning and assurance.	Cross Domain Coordinator Fault Management Network Supervision Network Health Dashboard Troubleshooting Dashboard Original Service Fulfillment Policy Management Service Fulfillment Service Supervision Transport Slice Controller Wireless Supervision

1.3 User interfaces

1.3.1 NSP Launchpad

The NSP Launchpad is the main access and navigation point for NSP functions and applications, and appears when you first sign in. You can return to the Launchpad from other screens anytime using the Back to Launchpad item in the grid menu. From the Launchpad, you can access NSP web applications, the NFM-P client application, the Network Health Dashboard and Troubleshooting Dashboard (in shared-mode NSP deployments), and the NSP Help Center.

1.3.2 Web applications

NSP web applications are browser-based interfaces into NSP functional areas. Some web applications are common to all NSP deployments, such as User Manager, Group Manager, and the NSP Help Center. The availability of other browser-based applications depends on your licensed feature packages and installation options.

By default, the NSP applications are available only in English. Contact Nokia for information about localization support.

See the *NSP System Architecture Guide* for more information about feature packages and installation options.

1.3.3 Client-based applications

The NFM-P GUI client provides an extensive IP/MPLS network management interface as part of the Platform feature package. See the *NSP NFM-P User Guide* for information about this application.

1.3.4 Network Health and Troubleshooting dashboards

Network Health and Troubleshooting dashboards combine information and functions from different applications into one view, providing a broad perspective on network management. You can access the dashboards using the drop-down menu at the top-left corner of the Launchpad.

The Network Health and Troubleshooting dashboards are available in shared-mode NSP deployments.

1.3.5 5G Transport Slice Controller dashboard

The 5G Transport Slice Controller dashboard provides a summary of the overall health of all transport slices in the network, as well as allowing drill-down into health views on a per-slice basis. The TSC dashboard displays details about L0/L1/L2/L3 services and tunnels/paths used during the realization of transport slices, and provides pro-active monitoring telemetry data and reports on transport slices.

1.3.6 APIs

For OSS users, NSP functions are available using the REST and RESTCONF APIs. The NSP APIs are documented on the Network Developer Portal.

1.4 Deployment flexibility

1.4.1 Compatibility

An NSP deployment can consist of multiple NSP components that interwork with separate products and interface with a variety of network elements. In order to provide specific functions, a specific NSP release supports integration with various releases of system components, integrated products, and network devices.

See the *NSP Release Notice* and *NSP and NFM-P Network Element Compatibility Guide* for specific information about the component, product and device software releases that are compatible with the NSP.

1.4.2 Network growth

NSP components can be installed in stages to allow for the growth and diversification of a given deployment. For example, an IP-only NSP deployment can be expanded to include optical network management components and products.

See the *NSP Installation and Upgrade Guide* for specific system deployment information.

1.4.3 Flexibility

NSP software is licensed and sold based on feature packages or automation packages. These packages provide the ability to fully customize an NSP deployment according to your network type, management requirements, and desired outcomes.

See the *NSP System Architecture Guide* for information about NSP feature packages. See 4.2 “Delivery” (p. 37) for information about NSP software delivery.

1.4.4 Deployment options

The NSP supports a number of recommended deployment types that address a variety of network-management scenarios. A deployment option may require the purchase of multiple feature packages, and may require the installation of various NSP components and separate products.

See the *NSP Installation and Upgrade Guide* for detailed descriptions of the supported deployment options.

1.5 NSP support for private wireless networks

1.5.1 NSP for private wireless

NSP-managed private wireless deployments are designed to meet the must-have needs of asset-intensive industries:

- Continuous operations with multiple redundancies and mission critical performance.
- Efficiency and safety that rely on coordination between multiple physical assets at work sites and in the field.
- Guaranteed security while ensuring the flexibility to react rapidly to change.

Note: Private wireless deployments apply, for example, to autonomous haulage for mining enterprises and to power utility wireless networks.

The NSP provides end-to-end management and orchestration of private wireless networks by implementing solutions that incorporate Nokia and multi-vendor equipment:

- Ready-to-use toolbox to manage the network with an integrated set of result-oriented applications.

  The NSP solution implements a flexible plug-and-play domain management system that supports the continuous evolution of all networks.
- Open automation platform that automates network operations with programmable frameworks.

  The NSP solution provides an open, model-driven, programmable set of APIs that integrate into the customer own or third-party end-to-end OSS or orchestration systems.

- Resource controller that ensures path/flow control and closed-loop optimization for IP/MPLS and optical networks.

  The NSP solution includes a comprehensive set of expert tools that allow network engineering teams to control and optimize network traffic in real-time.

Table 1-3, “NSP functions and features for private wireless” (p. 11) describes the NSP functions and features that are relevant to private wireless networks.

Table 1-3 NSP functions and features for private wireless

Function	Features
Network Configuration	Traditional wireless, IP/MPLS and optical Model-driven IP/MPLS
Service Fulfillment	Traditional IP/MPLS Traditional packet/optical Abstraction Programmable Any service (YANG defined)
Automation	Workflow management Bulk provisioning
Network Layer Control	IP/MPLS PCE with optimization Optical PCE with optimization Flow steering IP/MPLS Simulation Multi-layer coordination and cross-domain control
Network and Service Assurance	Network monitoring and visualization Service monitoring and troubleshooting Fault management and correlation Reporting Analytics
Network Mediation	Any vendor model-driven adaptation Pluggable device adaptors Continuous network upgrades

2 Concepts

2.1 MDM

2.1.1 What is model-driven mediation?

With model-driven mediation (MDM), the data objects that make up an NE and its capabilities are defined using YANG models. MDM provides the translation and abstraction required for automated applications to interact with the YANG model, allowing management of NEs without the need for the NFM-P.

An MDM server is installed as part of the NSP deployment. Within the MDM server, network protocol inputs from devices are adapted to create inputs to applications, and vice versa. Adaptation is performed by MDM adaptor files. Adaptors are installed on the MDM server according to network requirements. Nokia-provided adaptors, customer adaptor suites requested by customers, and adaptor documentation are published on the Nokia support software download site .

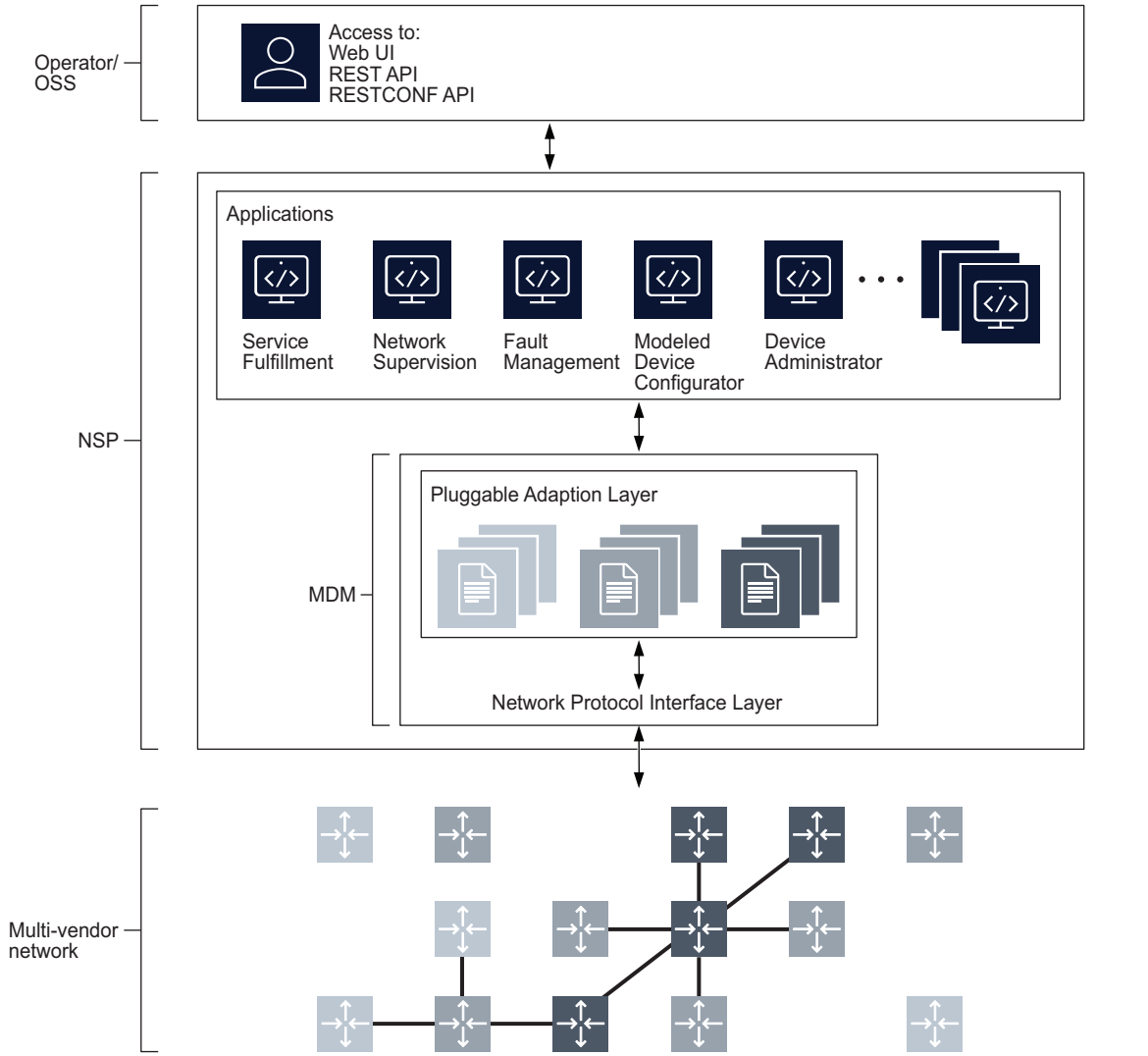
In general, an adaptor provides mapping between a specific device and an application interface. A single adaptor may only adapt one function of the application. For example, EVPN and IES functions in the Service Fulfillment application are provided by different adaptors. Therefore, managing an NE with MDM requires multiple adaptors, packaged together as an adaptor suite.

Adaptor suites are provided according to NE type and release and NSP release. For example, the package titled **sros-20-2-r1-19_11** provides adaptors for Nokia SR OS NEs, Release 20.2, for use with NSP Release 19.11.

Nokia recommends installing only the adaptor suites required for your current network, and always installing all the files in the adaptor suite. See the adaptor documentation for details.

The following figure illustrates the basic concepts of MDM. MDM incorporates a network protocol interface layer, pluggable adaptation layer, and application interface layer to allow NSP applications to manage Nokia and multi-vendor devices using Netconf/YANG.

Figure 2-1 Model-driven mediation in NSP



2.1.2 MDM in NSP

MDM is a component of NSP enabled by the following feature packages:

- Multi-layer Discover and Visualization
- Multi-layer Control Coordination

MDM is provided notably for model-driven Nokia and multi-vendor NE management.

Model-driven management interfaces are based on a common infrastructure that uses YANG models as the core definition for configuration, state, and operational actions. All model-driven interfaces take the same common underlying YANG modules and render them for the management interface.

Applications support NE discovery, management, and configuration for MDM managed NEs. The availability and level of functionality of a particular application with a particular NE type or version depends on the adaptors. Adaptors are developed continuously, and updated on the software download site regularly, meaning that application functionality can expand at any time, without the need to upgrade the NSP or the device.

2.2 Adaptors

2.2.1 Multi-vendor NE management via MDM adaptors

Adaptors enable the NSP to manage devices that include multi-vendor devices.

NSP applications can be used with multi-vendor devices, including creation of services or groups with devices from multiple vendors.

Contact your Nokia representative to obtain adaptors, and technical support for assistance with adaptor customization.

Multi-vendor devices can be managed using NETCONF, SNMP, and CLI in addition to MDM. gRPC is also supported.

2.2.2 Commercially available adaptors

Nokia-provided adaptors for various NEs, including SR OS devices, are available for download from the Nokia support software download site. The adaptor download page also provides adaptor guides. The adaptor guide lists the adaptors available in the adaptor suite, the management and application functions they support, and the application functions that are not available.

2.2.3 Custom adaptors

You can engage Nokia to build adaptors for specific NEs and feature sets. Development versions of these customer-specific adaptors are shared with the customer through the Network Developer Portal.. Once they have passed user-acceptance testing, final versions are delivered on the software download site of the Support Portal in a customer-restricted folder hierarchy: Network Services Platform/Adaptors/Customer-specific/<customername>.

2.2.4 Adaptor Designer application

You can use the Adaptor Designer to build your own adaptors or customize reference adaptors for your requirements. Contact Nokia for details.

2.2.5 Adaptor documentation

Adaptor documentation is available from the Nokia support software download site for each NE family and NSP release. For example, the Nokia SR OS Adaptor Guide for Release 22.3 lists and describes the adaptor suites delivered to support management of Nokia SR OS devices by NSP Release 22.3 over model-driven interfaces.

Adaptor guides provide information specific to the adaptor suites, including:

- lists of supported and tested software releases
- lists of files found in each suite with information about the application or function each file supports
- adaptor support of application functions, for example, whether viewing fan details is supported in Network Supervision.
- device configuration requirements for discovery and management
- limitations, recommendations, and issues

2.3 Services

2.3.1 Services overview

The NSP provides the following browser-based applications for service provisioning, activation, and monitoring:

- Original Service Fulfillment
- Service Fulfillment
- Policy Management
- Service Supervision

Original Service Fulfillment application

The Original Service Fulfillment application allows for multi-vendor service provisioning and activation across all networks accessible to the NSP. It authorizes northbound interface (NBI) service requests, executes routing algorithms that allocate network resources for these services, and then deploys the services to the network. Network deployment is performed through the mediation framework. The Original Service Fulfillment application can use existing tunnels created with the NFM-P, or it can create new tunnels to satisfy service demands. The services that can be provisioned from this application include IP VPN, L3 VPN, E Line, C-Line ,E-LAN, E-Tree, OCh, ODU, transport services and service chaining in the network with full control plane (MP-BGP and T-LDP) support.

Original Service Fulfillment and NFM-P dependencies

- Services created in the NFM-P can be managed by the Original Service Fulfillment application if the service's NSD Managed parameter is enabled in the NFM-P.
- The Original Service Fulfillment application can discover LSP and SDP tunnels created previously in the NFM-P.
- The NFM-P is used to define QoS Generic policies so that Original Service Fulfillment can handle service access QoS.

To deploy IP services to the NFM-P, the NSP uses NFM-P templates that are installed into the NFM-P during NSP installation. The templates are hard-coded in the 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 Original Service Fulfillment application. See the *NSP Original Service Fulfillment Application Help* for more information.

Service Fulfillment application

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

A library exists with a predefined set of service models (such as VPRN, EVPN, C-Line, E-LAN, E-TREE, E-Pipe and IES services) for both classic and model-mode SROS networks. These service models can be installed and utilized by the built-in, intent-based engine (NSP's Intent Manager) to provide assurance that service configuration is as planned/requested, and also easy adaptability for custom service model requests. New service models to support custom needs can also be developed with aid of the NSP's automation practice team — or, if your deployment includes the NSP's programmability suite, self-development.

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

Service Fulfilment 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 beginning the fulfilment process. Service offerings with customer-centric naming can be created by the user, thereby enabling dynamic creation of the service catalogue based on installed service models. The Service Fulfillment application supports the configuration and deployment of services on third-party devices. See the *NSP Service Fulfillment Application Help* for more information.

Policy Management application

The Policy Management application uses templates and policies to combine many lower-level network tasks into a higher-level function that shields applications from the unnecessary complexity of vendor-specific, low-level provisioning. The abstraction of low-level network functions into a standards-based, high-level "business language" (North bound API) allows SPs to innovate faster and compete better. The templates and policies allow the operator to define standard services with respect to QoS profiles, routing targets, and tunnel binding rules. When provisioning a service, the templates can be used rather than specifying each attribute, thus accelerating the process and ensuring the deployment of standard services.

Policy Management and NFM-P dependencies

The creation of Endpoint QoS templates requires QoS generic profiles created in the NFM-P.

Service Supervision application

The Service Supervision application monitors deployed services in the network. When the NSP is deployed with the Service Fulfillment application, the Service Supervision application monitors services provisioned by the Service Fulfillment application and/or other management applications, such as the NFM-P service manager.

2.3.2 Service types

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

Table 2-1 Service type naming

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

See the *NSP Original Service Fulfillment Application Help* for information about L3 VPN, C-LINE, E-LAN, and E-LINE services.

VLAN

VLANs are created to provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management. The following table lists the types of VLAN services that are supported on the NFM-P by device type:

Table 2-2 Device VLAN support

Device	Supported VLAN types
7450 ESS	• Standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN • Broadcast TV (MVR/IPMV) VLAN
All OmniSwitches	• Standard VLAN • L2 VPN (TLS/VLAN-Stacking) VLAN
All OmniSwitches except for the OS 6900 and OS 10K	• Broadcast TV (MVR/IPMV) VLAN
OS 6900 and OS 10K	• IPC VLAN • VIP VLAN
Wavence SM	• Wavence (dot1ad) VLAN • Wavence P2P (dot1q) VLAN • Wavence P2MP (dot1q) VLAN

VLL

A VLL service is an L2 point-to-point service that connects access interfaces. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this, the device performs no MAC learning in a VLL service.

The NFM-P supports the creation of the following VLL service types:

- E-Line, or Ethernet VLL service
- Apipe, or ATM VLL service
- Fpipe, or frame relay VLL service
- Hpipe, or HDLC service
- Ipipe, or IP interworking VLL service
- Cpipe, or circuit emulation VLL service

E-LAN

E-LAN is a class of virtual private network multipoint L2 service that allows multiple customer sites to be connected in a single bridged domain contained within the service provider-managed IP/MPLS network. Customer sites in the E-LAN appear to be on the same LAN, even if the sites are geographically dispersed.

E-LAN offers the following advantages:

- Ethernet interfaces on the host access side simplify provisioning.
- All routers in the E-LAN are part of the same LAN, which simplifies IP addressing and allows customers to control and simplify their routing strategies.
- E-LAN is protocol independent, which means there is no L2 protocol conversion between LAN and WAN technologies.

IES

An IES is a routed connectivity service in which the customer traffic passes through an L3 IP router interface to the Internet.

IES allows customer-facing IP interfaces in the same routing instance to be used for service network core-routing connectivity. IES requires that the IP addressing scheme that is used by the customer be unique among other provider addressing schemes and potentially the entire Internet.

L3 VPN

The NFM-P supports the creation of L3 VPN services using the 7450 ESS in mixed mode, the 7750 SR, the 7750 SR MG, the 7705 SAR, and the 7950 XRS as a PE and provider core (P) router. L3 VPNs, also called IP VPNs or BGP/MPLS VPNs, are defined in RFC 2547bis. This standard describes a method of forwarding data and distributing routing information across an IP/MPLS service provider core network.

2.4 NSP Zero Touch Provisioning

2.4.1 Zero Touch Provisioning overview

Zero Touch Provisioning (ZTP) is an SR OS feature that automatically configures a node by obtaining the required information from the network and provisioning the device with minimal manual intervention and configuration. When new devices that support ZTP are connected and boot up, the device is auto-provisioned.

For more information about ZTP and the specific devices on which it is supported, see the ZTP information in the device documentation: *Nokia 7450 Ethernet Services Switch, 7750 Service Router, 7950 Extensible Routing System, and Virtualized Service Router Basic System Configuration Guide*

RESTCONF APIs are also available for ZTP; see the API documentation on the Network Developer Portal.

NSP Zero Touch Provisioning provides tools to generate ZTP files for device provisioning, and adds device information to discovery rules, reducing manual work on the NSP required for device discovery by Device Administrator or NFM-P.

ZTP NE details can be exported from Device Administrator in JSON format. The exported data can facilitate the automation of the DHCP server configuration.

NSP uses the following intent types in Intent Manager to facilitate ZTP:

- Create_HTTP_User: creates a user identity to connect with the NSP file server

  Note: creation of an HTTP user is a one time operation. Only one HTTP user is supported.
- ZTP-Profile: saves a set of NE information and discovery information that can be applied to multiple devices. For example, you can create a profile for MDM managed 7250 IXR devices and one for classically managed 7250 IXR devices.

  Create a ZTP profile for each set of generic parameters you need.
- Day-0-ZTP: takes the parameters provided in a ZTP profile and parameters that are unique to a device and creates configuration and provisioning files for the device on the NSP file server.

  Create a Day-0 intent for each device.

When the intents have been executed, the device is added to the Zero Touch Provisioned Network Elements list in Device Administrator. The device can then be powered on and discovery can be initiated.

The Zero Touch Provisioned Network Elements list can be cleaned up using a workflow in Workflow Manager.

Important! NSP Zero Touch Provisioning has been tested with 7250 IXR-e and 7750 SR 14s NEs. Contact Nokia for assistance in using ZTP with any other NE type.

2.4.2 NSP ZTP Prerequisites

NSP ZTP requires the following prerequisites:

- Prerequisites for device ZTP must be in place; see the NE documentation.

- The ZTP intents zip files must be downloaded from Nokia central resources; contact your Nokia representative for details
- An HTTP user must be created using the Create_HTTP_User intent type; see 2.5 “How do I configure Zero Touch Provisioning?” (p. 22).
- A discovery rule for the NE must be created in Device Administrator. The administrative state of the discovery rule must be Down.

  See the Device Administrator Application Help for more information about discovery rule configuration in Device Administrator.
- For classic devices, a discovery rule for the NE must be created in NFM-P in addition to the discovery rule in Device Administrator. The administrative state of the discovery rule must be Down.

  See the *NSP NFM-P User Guide* for more information about discovery rule configuration in NFM-P.
- If you plan to upgrade your device as part of the ZTP process, for example if you purchased a device with Release 20.7 software and want to use it with Release 20.10, you must import the new software image to the NSP file server before performing ZTP. If you do this, you can configure the new target software version as part of the ZTP profile intent.

  See the procedure to import a node software image in the *NSP Device Administrator Application Help*.
- If you plan to use an IP resource pool for IP address assignment, the IP resource pool must be created in Resource Administrator.

  See the *NSP Resource Administrator Application Help* for information about using Resource Administrator. Also see the Network Programmability & Automation Frameworks tutorial on the Network Developer Portal.

2.4.3 Process

Figure 2-2, “Zero Touch Provisioning process” (p. 22) shows the ZTP process with NSP.

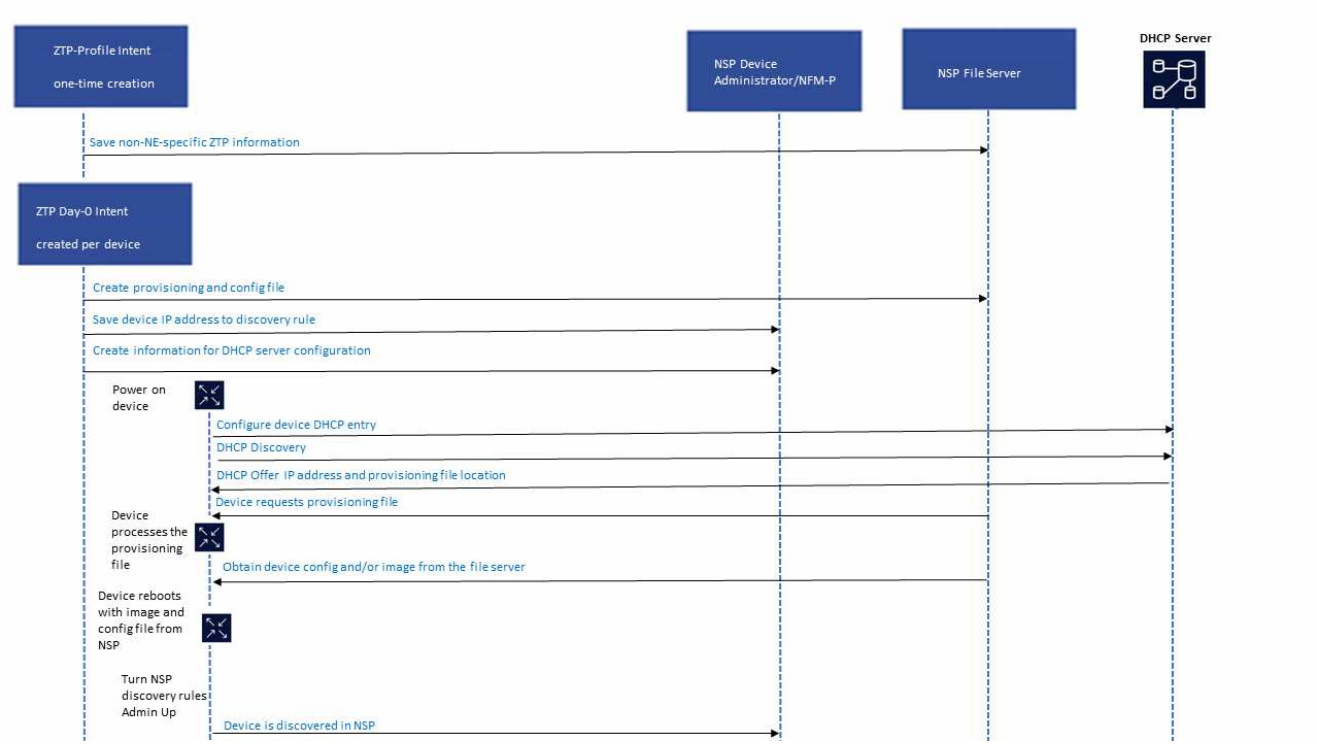
When the ZTP Day-0 intent is created and synchronized:

- Configuration and provisioning files are created and stored on the file server
- Paths and filenames for the configuration and provisioning files are saved to the database
- Device IP addresses is added to the relevant discovery rules
- The device is added to the list of Zero Touch Provisioned Network Elements in Device Administrator

If all ZTP intents are synchronized, the operator turns up the discovery rule and powers on the node. The node completes ZTP and reboots.

After rebooting, MDM managed devices are ready to manage. For classic devices, a setting must be changed in CLI to prepare the device for discovery; see 2.5 “How do I configure Zero Touch Provisioning?” (p. 22).

Figure 2-2 Zero Touch Provisioning process



2.5 How do I configure Zero Touch Provisioning?

2.5.1 Note

This procedure requires the use of the Intent Manager, Resource Administrator, Device Administrator and Workflow Manager applications, and optionally the NFM-P. For complete configuration details, you may need to consult the following documents:

- *NSP Intent Manager Application Help*
- *NSP Resource Administrator Application Help*
- *NSP Device Administrator Application Help*
- *NSP Workflow Manager Application Help*
- *NSP NFM-P User Guide*
- NE documentation: *Nokia 7450 Ethernet Services Switch, 7750 Service Router, 7950 Extensible Routing System, and Virtualized Service Router Basic System Configuration Guide*

2.5.2 Process

Import intent types in Intent Manager

1

Download the ZTP zip file to your computer.

Three intent types are included in the zip file: Create_HTTP_User, ZTP-Profile, and Day-0-ZTP.

2

Import the intent types to Intent Manager:

1. In Intent Manager, choose **Intent Types** from the drop-down list at the top left of the screen.
2. Click **Import** .
3. In the form that opens, navigate to the file you want and click Open.

3

Evaluate and update the Day 0 ZTP intent to ensure that it will generate the correct information in the provisioning and day-0 config files.

The primary image file in the bof portion of the provisioning file generated from the intent type must match the information on the compact flash of the device.

Contact Nokia for assistance with this step.

Create an HTTP user

4

An HTTP user is required to connect to the NSP file server. This step only needs to be performed once.

The file server only supports one HTTP User.

In Intent Manager, select the Create_HTTP_User intent type and click **Create Intent** + .

5

In the form that opens, configure the parameters and click **Create**.

Create at least one ZTP profile

6

A ZTP profile contains template values that can apply to multiple devices.

In Intent Manager, select the ZTP-Profile intent type and click **Create Intent** + .

7

In the form that opens, configure the required parameters:

- Choose the management mode: classic, mixed, or model driven.
- Choose the management connection, for example, in-band.
  For model-driven management, only in-band and out-of-band are available.
  For classic management, the drop-down includes in-band, out-of-band, and in-band-embedded-config. With in-band-embedded-config, the Day-0 configuration parameters will be part of the provisioning file. Embedded configuration is only available with supported releases of the 7250 IXR.
- Choose the NE Type.

8

Configure additional parameters as needed.

Attention: Static routes are only supported with the out-of-band management connection type.

9

Click **Create.**

The ZTP profile is now available.

10

Create additional ZTP profiles as needed for each set of device parameters.

Create a ZTP intent for each device you want to provision

11

The ZTP intent will create the provisioning and configuration files.

In Intent Manager, select the Day-0-ZTP intent type and click **Create Intent** + .

12

In the form that opens, configure the parameters:

- Enter the DHCP client address for the NE in the ZTP ID field
- Choose the ZTP profile to apply the template values
- Enter a unique NE name.
- Configure the System and Management IP addresses. Enter the IP addresses manually or choose IP Resource Pool for automated IP address assignment. IP resource pools can be created in the Resource Manager application.
  Note: The System IP address and Management IP address must be different.
- Choose a Device Administrator discovery rule, and, for classic NEs, an NFM-P discovery rule.

13

Click **Create**.

The provisioning and configuration files are created and a new rule element is added to the relevant discovery rule.

14

Verify and update the day0 configuration and provisioning files to match network settings, NE card type and port settings. Contact Nokia for assistance.

Verify the information in Device Administrator and discover the device

15

In Device Administrator, from the Network Elements page, choose **Zero Touch Provisioned Network Elements** from the drop-down.

Device Administrator displays the list of devices for which ZTP is configured.

16

Click on an NE to see the details.

17

Click **Export** to save the NE information to a JSON file if needed.

18

Power on the device.

The device completes ZTP and reboots. The discovery status in the **Zero Touch Provisioned Network Elements** list is updated.

19

In Device Administrator and NFM-P, turn the relevant discovery rules up.

Configure cleanup of the Zero Touch Provisioned Network Elements list

20

Import the ZTP_Purge_Workflow and ZTP_Artifacts_Cleanup workflows from the ZTP zip file into Workflow Manager.

21

In Workflow Manager, from the Workflows page, choose ZTP_Purge_Workflow.

Note: The ZTP_Purge_Workflow runs ZTP_Artifacts_Cleanup during its operation. Both workflows must be present in Workflow Manager.

22

From the menu at the end of the row, choose **More** ⋮ **Execute**.

23

Update the retentionDays parameter as needed and click **Execute**.

The cleanup removes NEs with Success status from the Zero Touch Provisioned Network Elements list that have been discovered longer than the configured number of days.

24

Schedule execution of the ZTP_Purge_Workflow for automated cleanup if needed; see the *NSP Workflow Manager Application Help*.

2.6 NSP Infrastructure Configuration Management

2.6.1 Infrastructure Configuration Management overview

Infrastructure Configuration Management (ICM) is an application to help in defining and deploying infrastructure configurations to an NSP managed network. With ICM the network engineer can easily define reusable configuration templates covering such areas as card, port, QoS, security, and routing policy configurations. ICM is found on the Configurations tab of the Device Administrator application, if Infrastructure Configuration Management is included in the deployment.

RESTCONF APIs are also available for ICM; see the API documentation on the Network Developer Portal.

ICM intent types

Device Administrator uses intent types imported from the Intent Manager application to build configuration templates, which are then used to build configurations.

The intent type defines the parameters that will be set when the configuration template is deployed. The configuration form can provide a parameter value or leave the value blank, to be set during deployment. If a parameter is not included in the configuration form, deploying the configuration template will not set that parameter on the target.

Users can create custom intent types in Intent Manager or download predefined intent types from the Artifacts directory on the NSP software download site. Nokia recommends using predefined intent types where applicable.

Predefined intent types are delivered to the software download site outside the NSP release cycle. The intent types are delivered in zip files, which include a readme file for each intent type. See the ICM Intent Types Delivery notes document in the Artifacts directory for the list and descriptions of the intent types in the collection.

Configuration templates

Operators use the configuration templates to deploy the configurations to the network either in bulk or on an individual target basis (NE or card/port). ICM provides full feedback on the success (aligned) or failure (misaligned) of the deployment request, so that the operator is aware if the defined configuration is present and running in the network. The operator can audit and monitor for

configuration drift that may occur over time and realign the network configuration back to the intended and defined configuration.

Templates can be defined with fixed or flexible attribute definitions. Certain attributes can be set with a fixed value (for example, MTU = 1500) that cannot be changed by the operator, or can be set with a default value that can be modified in the deployment phase.

2.7 ICM process

2.7.1 Purpose

This process describes the general steps of ICM. This procedure requires the use of the Intent Manager and Device Administrator applications. For complete configuration details, you may need to consult the *NSP Intent Manager Application Help*, the *NSP Device Administrator Application Help*, or the tutorials on the Network Developer Portal.

Import or create intent types in Intent Manager

1

Download the ICM intent types from the NSP software download site.

If you prefer to create your own intent types, proceed to Stage 3.

2

To import downloaded intent types to Intent Manager:

1. In Intent Manager, navigate to the **Intent Types** page.
2. Click **Import** .
3. In the form that opens, navigate to the file you want and click Open.

3

To create intent types, see the Intent Types tutorial on the Network Developer Portal for developer information.

Note the following:

- The `InfrastructureConfiguration` label must be present
- The intent type must include a resource file, `icm_descriptor.json`, that provides the category of configuration:
  - Physical (for example, port and card configuration) or
  - Logical (for example, QoS or routing)

    For intent types with the logical role, this resource file also defines whether the template can be deployed to multiple targets in one deployment, and whether it can be deployed with other templates in one deployment.
  - The intent type must include at least one schema form and viewConfig resource file.
  - Other resource files may be required depending on the operations performed by the intent type.

Import the intent types into Device Administrator

4

In Device Administrator, navigate to the **CONFIGURATIONS** tab.

5

Choose **Configuration Intent Types** from the drop-down list.

6

Click + **IMPORT**

7

Choose the intent types from the list and click **IMPORT**.

Create a configuration template

8

From the **CONFIGURATIONS** tab, choose **Configuration Templates** from the drop-down list.

9

Click + **CONFIGURATION TEMPLATE**

10

Configure the parameters and click **RELEASE**.

Deploy the configuration

11

a. From the **Configuration Deployments** list, click + **CONFIGURATION DEPLOYMENT** and choose **Logical** or **Physical**.

b. From the **Configuration Templates** list, choose a template and click ⋮ (More actions) **Deploy to Network**.

12

Configure the parameters and click **DEPLOY**.

The configuration is sent to the targets, and the deployment details are added to the **Configuration Deployments** list.

Audit and align

13

You can perform an audit at the deployment level for a single target, or at the template level for all deployments using the template.

An audit checks whether the target configuration matches the template, but does not change the target configuration.

Note: an audit at the template level checks all deployments using the template. The operation may take a long time. During the audit, you can click **VIEW DETAILS** for process information.

a.

1. From the **Configuration Templates** list, choose a template. Click ⓘ if needed to open the **Template Details** panel.

   The **Template Details** panel shows the number of deployments and the number that were aligned and misaligned after the last audit.
2. Click **AUDIT ALL CONFIG** and click **CONTINUE** to confirm. The alignment status information is updated.

b.

1. From the **Configuration Deployments** list, choose a deployment. Click ⓘ if needed to open the **Deployment Details** panel.

   Click **VIEW RESULT** in the **Deployment Details** panel to see the results of the last audit.
2. Click **AUDIT CONFIG**. The audit results and alignment status information are updated.

14

You can perform an align at the deployment or at the template level.

An align operation updates the target configuration if it does not match the configuration template.

a.

1. From the **Configuration Templates** list, choose a template. Click ⓘ if needed to open the **Template Details** panel.

   The **Template Details** panel shows the number of deployments and the number that were aligned and misaligned after the last audit.
2. Click **ALIGN ALL CONFIG** and click **CONTINUE** to confirm.

b.

1. From the **Configuration Deployments** list, choose a deployment. Click ⓘ if needed to open the **Deployment Details** panel.

   The **Deployment Details** panel shows the results of the last audit.
2. Click **ALIGN CONFIG**. The alignment is performed and the alignment status information is updated.

3 Features

3.1 Value proposition

3.1.1 Automation

NSP uses automation to provide a faster, more flexible network management solution. This automation function spans multiple components and applications, allowing for the provisioning of intelligent, adaptive services across multiple domains and use cases.

Original Service Fulfillment application

The Original Service Fulfillment application allows operators to provision a service based on service templates that are configured using the Policy Management application, which allows for faster service creation and deployment. It can also make use of operator-defined policies for dynamic network resource selection and automated provisioning. These policies utilize the application's real-time view of the network to map service connection requests to the best available tunnels/paths in order to meet the customer’s network efficiency goals.

Service Fulfillment application

The Service Fulfillment application allows operators to provision a service based on service templates that are configured using intent types imported from the Intent Manager application, which allows for faster service creation and deployment. It can also make use of operator-defined intent types for dynamic network resource selection and automated provisioning. These intent types utilize the application's real-time view of the network to map service connection requests to the best available tunnels/paths in order to meet the customer’s network efficiency goals.

IP/MPLS Optimization application

The IP/MPLS Optimization application leverages complex algorithms, applied via policies, to automate the rerouting of service paths based on operator-specified constraints. This allows for the provisioning of services that automatically respond to network changes in order to maintain optimization targets.

Intent Manager application

The Intent Manager application allows you to create and execute intent-based automation flows in NSP. With Intent Manager, you can implement planning and design at a network level. The Intent Manager application translates the high-level goal from an intent to necessary network configuration. The application generates and validates the configuration and continually verifies the state of the network

Workflow Manager application

The Workflow Manager application allows for the creation and execution of workflows within NSP. The application can be used to create automated procedures and closed loop automation.

3.1.2 Optimization

The NSP unifies service automation with network optimization, allowing network operators to deliver on demand network services cost-effectively and with scalability. Real-time network path

computation and optimization is centralized to leverage network-wide views and KPI driven to rapidly adapt to changing network conditions.

Original Service Fulfillment application

The Original Service Fulfillment application allows operators to provision a service based on constraints and on an optimization target. The service is created along with the required infrastructure to fulfill these criteria. Operators can quickly and easily deploy services in a changing environment. Operators can change the optimization objective and PIR/CIR representing the bandwidth that will be used by the service.

IP/MPLS Optimization application

The NSP supports transport network optimization through the IP/MPLS Optimization application. The IP/MPLS Optimization application provides a view of the IGP topology and PCE LSPs. It also displays the status of the IGP network and provides functionality to optimize the network resources. This can be done globally or locally e.g. optimizing the LSPs passing specific links only.

The IP/MPLS Optimization application leverages centralized, intelligent network control capabilities so that operators can rapidly adapt to changing demand and traffic patterns and run their networks more efficiently. It accepts path connection requests from the Original Service Fulfillment application, from OSS and orchestration systems, and from physical/virtual network elements. IP/MPLS Optimization calculates optimal paths through the network for a given set of business and technical constraints by leveraging centralized views of all available assets/topologies and their current state.

3.1.3 Assurance

The NSP enables operators to report, supervise, and predict issues using a suite of integrated applications that provide an end-to-end view of any network. Report generation provides full visibility of network capacity and inventory, event correlation reveals the root causes of network problems, and automated troubleshooting and dynamic scaling resolves issues in real-time. In addition, a comprehensive REST NBI allows for integration of other systems.

Fault Management application

The Fault Management application monitors alarms for IP/MPLS, Ethernet, optical, and integrated IP/optical network elements, both physical and virtual. Operators can drill down from top-level summaries of overall network health to individual element alarms, including root causes and impact analysis. Alarm information gathered by the Fault Management application is integrated across the entire NSP, creating a single assurance solution for all network domains.

Network Supervision application

The Network Supervision application supervises physical and virtual network elements, and can integrate with existing orchestration, OSS, and portal solutions, providing end-to-end visibility. Comprehensive monitoring with summarized aggregate KPIs enables fast problem detection and impact analysis; event timeline and alarm correlation focuses operator investigations on genuine root causes; and extensive troubleshooting tools resolve problems quickly.

Service Supervision application

The Network Supervision application provides monitoring and troubleshooting tools for IP/MPLS and Ethernet services. Operators can explore services through service topology maps and view details about service components such as SAPs, sites, and SDP bindings. Visualization tools combined with KPI data, alarm correlation, and event timelines help operators quickly identify problems as they emerge.

3.1.4 Monitoring

The NSP monitors realms such as the managed network, internal system processes, and user activity to provide source data for applications and utilities.

Managed network

The NSP uses SNMP and subscription-based YANG telemetry mechanisms to monitor the managed network for configuration changes and alerts.

In an NSP deployment that includes the NFM-P, the Fault Management application displays the NFM-P alarms raised in response to NE SNMP traps. For MDM-managed devices, the Fault Management application displays NE alarms if they are supported by the installed MDM adaptors.

The following NSP applications enable you to configure, manage, and review YANG-based telemetry data from NEs:

- **Insights Administrator**
  filters and stores telemetry data; can be configured to publish telemetry data to Kafka topics for subscriber notification
- **Insights Viewer** utility
  presents historical and real-time telemetry data as graphs
  Note:the Insights Viewer utility is accessed from other applications; it is not available directly from the launchpad
- **Analytics**, NSP-level reports
  provides end to end historical analytics and reporting from physical inventory to services to application-level insights for IP/MPLS, mobile and microwave networks.
  Historical data stored in an auxiliary database is presented as tables, charts, or graphs.
- **Baseline Analytics**
  provides advanced telemetry baselining with anomaly detection
  Baseline Analytics is event-driven, based on anomaly events, so it can be used for closed-loop automation or similar applications.
  Note: Baseline Analytics configuration is performed from the Insights Administrator application, and baseline and anomaly graphs are presented in the Insights Viewer utility.
- **MD-OAM**
  In the Insights Administrator application, you can create supported OAM tests on MDM-managed NEs.
  Tests can be created for any service. No additional configuration is required on the service for testing to be performed.

Internal system processes

An NSP cluster continually monitors the local server processes for errors and excessive resource consumption. The connectivity to other components and integrated systems is also checked regularly. The Fault Management application displays an alarm when a system process, resource, or connectivity fault is detected.

ACT framework

The Analyze-Calculate-Transform (ACT) framework enables NSP applications or third-party systems using the NSP API to define actions to be performed when a certain condition is met.

ACT takes Kafka notifications such as telemetry counters or gNMI updates from devices as an input and processes them into something else, for example a Kafka notification on a different stream, or an alarm.

An example of this would be to configure the ACT framework to monitor packet loss in the network. When ACT detects that packet loss is rising beyond a certain threshold, ACT can either send an email or raise an alarm. A raised alarm can be consumed either by the NSP workflow engine or by resource control, which will take an appropriate action such as optimizing the LSPs using the related network interface.

User activity

The User Manager application displays the session information for each NSP user, such as authentication success or failure, and the application actions of the user.

You can also configure an NSP or NFM-P system to export the user activity logs in syslog format to a remote server.

3.1.5 Microwave awareness (MWA)

In networks where multiple Wavence UBT-SA devices are linked to a single 7250 IXR or 7705 SAR NE, the NSP provides microwave awareness. With MWA, the NSP considers the router and its linked UBTs as a single logical site, while still providing a management path for each of the UBT-SAs.

The UBT SAs are linked to their associated routers either by LLDP links in the NFM-P, or by physical links. Physical links may be created manually in the NFM-P, or by using a Nokia-provided workflow in the Workflow Manager application. When the NSP detects MWA links, it automatically adjusts the display of the routers and their associated UBT-SA devices in the Network Supervision application; see the *Network Supervision Application Help* for more information.

Nokia also provides workflows in the Workflow Manager application that allow you to perform backup and restore, and software upgrades, on the UBT-SAs linked to a 7250 IXR or 7705 SAR. Contact your Nokia representative for more information about Nokia-provided workflows.

3.1.6 Network Slicing

End-to-end network slicing is a technology for concurrent delivery of differentiated 5G services and a key component of moving 5G use-cases toward a service-driven evolution that supports meeting SLAs deterministically across end-to-end network resources. Network slices are independent,

logical self-contained networks representing common physical or virtual network infrastructure that extends from end devices to application servers and includes all intermediate functions and domains.

See the following documents for more information about network slicing and the NSP applications that support it:

- *NSP Simplified RAN Transport Solution*
- *NSP Transport Slice Controller Application Help*

3.2 Locating NSP feature information

3.2.1 Release Descriptions

NSP feature information can be found in the release description documents. Release descriptions provide high-level feature descriptions for an NSP release, along with the schedule for delivery. Procedures or more detailed conceptual information may be located in other NSP documents.

NSP Release Description

The *NSP Release Description* lists all significant NSP features for a given release. Some but not all of the content is applicable to NFM-P-only customers.

This document is cumulative for a major release cycle, such as NSP 21.3 through 21.11, and then resets with the next release, such as NSP 22.3.

The *NSP Release Description* is delivered in the on-product NSP Help Center as well as on the Nokia Doc Center.

3.3 Feature evolution

3.3.1 Migrating to NSP applications

As NSP evolves, many of the features traditionally available in classic NFM-P deployments are being rebuilt and improved in NSP web applications. A phased deprecation plan is rolling out to ease the transition for NFM-P customers to the new feature sets and flows.

Transitioning to alarm management and topology maps on the NSP

The former alarm management and topology map functions of the NFM-P are provided by the NSP Fault Management, Service Supervision, and Network Supervision applications. You can use the Fault Management application to view, investigate, and manage alarms from the NFM-P, and the Service and Network Supervision applications to explore and manage your network.

For information about troubleshooting using the NSP, see the *NSP Troubleshooting Guide*.

4 Software

4.1 Packaging

4.1.1 Software bundle

An NSP software bundle is a set of one or more installation files that you download and use to deploy the product.

For NSP cluster deployment, a software bundle consists of a container runtime environment and the NSP software. For NSP components that are deployed outside an NSP cluster, an NSP software bundle consists of a set of RPM installation files. Each bundle type is available for download as one or more compressed archive files.

4.1.2 Feature packages

The purchase of feature packages and the associated license keys grants the right to download and use the software. “Feature packages” are not self-contained from a software-bundling or installation perspective; a feature package simply entitles you to a particular set of features. After you download and extract a software bundle, and configure your installation options during installation, the feature packages you purchased are enabled and the associated features are available for your use.

4.2 Delivery

4.2.1 Product software

As a registered customer, you can download NSP software from the Nokia Support Portal. If you are a new customer and require access, contact your sales or support representative for registration information.

The NSP software on the Electronic Delivery→Downloads portal, also called ALED, is organized by release. You navigate through the hierarchy to select and download the packages you are licensed to use according to your purchase agreement.

NFM-T and NRC-T deliver software from separate product hierarchies in the portal.

After you select items for download and click Next, you must choose a download method. Click Help for information about the available download methods.

Note: It is strongly recommended that you verify the message digest of each NSP package or file that you download from the Nokia Support Portal. The download page lists the MD5 or SHA-256 hash value of an item for comparison with the output of the RHEL md5sum or sha256sum command. See the appropriate RHEL man page for information about using a command.

4.2.2 Service packs

Service packs, or patches, are delivered on the Nokia Support Portal from the same download area as product software. Service Pack Notes bundled with the service packs describe the fixes and provide installation instructions.

4.2.3 Adaptors

Adaptors for model-driven management of multi-vendor devices are delivered on the software download site of the Nokia Support Portal. Hardened adaptors are delivered under the NSP release structure on this site. Customer-specific adaptors are delivered in their own restricted-access Adaptors directory.

Reference adaptors and trial versions of customer-specific adaptors are delivered on the Network Developer Portal .

4.2.4 Network Developer Portal

The Network Developer Portal hosts the latest NSP software in shared (free) and dedicated (paid) lab environments to allow customers to evaluate the NSP platform and develop and test NSP-enabled OSS applications. The portal is also home to API documentation, samples, and tutorials for the developer community.

4.3 Deployment mechanisms

4.3.1 Containerized NSP deployment

NSP system deployment is supported in a Kubernetes/Docker/Helm environment. The following container-based environments are supported

- the NSP container environment
- a container environment that you provide and maintain, as specified in the *NSP Planning Guide*.

You can add components that do not support deployment in containers to an NSP container deployment by installing the components using the traditional method, after which you can include the components in the NSP system.

4.3.2 Traditional deployment

Traditional NSP system deployment is performed using the open-source Ansible software-deployment tool. The tool performs the deployment based on parameters that you specify in a configuration file. You can deploy all required components in one operation from one central station.

4.3.3 Deployment documentation

See the following documents for information about the NSP system requirements, and about component installation, upgrade, and other deployment operations:

- *NSP Planning Guide*—provides information about planning an NSP deployment based on scale requirements, network environment, management scope, and the functions required; includes specific information such as firewall rules for inter-component communication

- *NSP Installation and Upgrade Guide*—describes the supported deployment types and includes all information required to preconfigure, install, upgrade, integrate and uninstall the NSP software

5 Documentation

5.1 Documentation architecture

5.1.1 Types of help

NSP documentation consists of:

- application help
- product-level guides
- component-level guides
- component-specific tools

5.1.2 Application help

Each NSP application has application help to guide operators in the use of the interface. Help for applications can be opened from a ? button in the application banner bar. Depending on the application, you may be taken directly to the Help Center, or an in-context help menu will appear offering help topics relevant to the current view.

5.1.3 Product-level guides

Information about NSP in general, as well as about shared-mode compatibility and deployments, is communicated in product-level documentation.

The following documents apply, in whole or in part, to the entire NSP product:

- *NSP User Guide* (this document)
- *NSP Installation and Upgrade Guide*
- *NSP Planning Guide*
- *NSP Release Notice**
- *NSP System Administrator Guide*
- *NSP System Architecture Guide*

With the exception of the guides marked with an asterisk (*), these product-level guides are included in the on-product NSP Help Center.

5.1.4 Component-level guides

The NFM-P is an independently deployable component of NSP which has its own user documentation and Release Notice.

Component-level user documentation is included in the on-product NSP Help Center if the component is installed in the deployment.

5.1.5 Tools

Several tools are available as part of the end user documentation; that is, they are delivered with the guides and help inside the NSP Help Center or NFM-P InfoCenter.

NSP Alarm Search Tool

NSP alarms can be searched or browsed from the NSP Alarm Search Tool in the on-product Help Center. NSP system alarms, along with alarms originating on MDM- or NFM-P-managed devices, appear in the tool and can be searched, filtered, and exported.

The alarm information displayed in the Alarm Search Tool and NSP applications is drawn from alarm dictionary files installed on the NSP. Alarm dictionaries are added automatically during component installation (for example: adaptors, feature packages, the NFM-P, and other components of the NSP), ensuring the Alarm Search Tool only contains relevant information. Some components may not yet provide an alarm dictionary. For adaptors, refer to the adaptor documentation for information about alarm dictionaries included with the adaptor. Adaptors from older NSP releases do not have alarm dictionaries.

Telemetry Search Tool

MDM telemetry statistics can be searched or browsed using the Telemetry Search Tool in the on-product Help Center. The tool displays statistics for packages and MDM adaptor files that are installed on the NSP. The content of the Telemetry Search Tool does not overlap with the Statistics Search Tool found on the NFM-P; the tools are similar, but the Telemetry Search Tool is dedicated to MDM telemetry statistics.

The Telemetry Search Tool is available if Modeled Device Configurator is included in the deployment.

Component-specific tools

NFM-P-specific developer tools and search tools for NFM-P alarms, statistics, and parameters continue to be delivered with NFM-P and are accessible under Help→Developer Tools in the NFM-P client GUI main menu. The content of these tools is not available in the NSP Help Center:

Developer tools in NFM-P:

- IPDR Reference
- JMS Example Code
- MV Metadata Navigator
- NSP Flow Collector Fields Dependencies
- Schema Reference
- SDK Navigator
- Template Development Information
- XML API Reference

Search tools in NFM-P:

- Alarm Search Tool
- Parameter Search Tool

- Statistics Search Tool

5.2 NSP Help Center

5.2.1 Content

Starting with NSP Release 19.6, NSP user documentation is delivered in an on-product application called the NSP Help Center. During NSP installation, the NSP Help Center loads the information content associated with each application and product component in your NSP deployment, providing you with end-to-end search capability across the user documentation, uncluttered by information irrelevant to your deployment.

5.2.2 Access

The Help Center can be opened from a ? button available in every NSP application banner bar, as well as the NSP Launchpad. You can also open the Help Center from the Help menu in the NFM-P client GUI. You can browse the documentation from menus on the Help Center home page, or use the searching and filtering capabilities to isolate information quickly.

5.2.3 Context-sensitive help

Many NSP applications include in-context help. When you click the ? button in an application banner bar, a “Quick Help” menu opens with suggested topics related to the current perspective. Short topics may be read in-line, whereas longer topics open in the NSP Help Center.

5.2.4 Searching

The Help Center application is centered on its robust search capabilities. When you conduct a search from the home page or search results page, the Help Center executes a global search across documentation for all installed NSP components. As shown in the tooltip on the search bar, the boolean operators AND/OR/NOT are supported, as are the wildcard characters * (any string) and ? (any character). Exact-phrase search strings enclosed in quotation marks are also supported.

Note: Common, non-technical terms such as “the,” “and,” “on,” and others are ignored in all searches, including exact-string searches.

Search history is tracked as follows:

- The Recent Searches list on the home page is per-user, and the Popular Searches list shows the trend across all users of the system.
- When a search result link is clicked on the search results page, it is captured in the Recent Searches list and considered for forming the Popular Search list. Navigating to a page in any other way (for example, by browsing from the browse menu or following links within a browsed document) does not make the page eligible for capture in the Recent/Popular Searches list.

Searched terms are not highlighted on the target page, but you can use the browser find function to see the hits within a page of content.

5.2.5 Filtering

Filters on the left of the search results page display a count beside the filter facets which contain one or more hits on your searched terms. You can refine your search results by selecting one or more filter facets and clicking APPLY FILTERS.

You can filter by either or both of these facets:

- Location
  Select one or more guides, sets, or tools to narrow your search results to those areas.
- Information Type
  Select one or more content types to narrow your search results to hits that match the content type. For example, if your search term is “LSP” and you only want to see procedural information, select “Procedure” as the content type.

The content types for filtering are:

- Use cases - use-case-based material showcasing product or feature functionality
- Description - explanatory content
- Procedure - step-by-step instructions to complete a task
- Reference - brief look-up data, such as glossary terms
- Workflow - a sequence of procedures to complete an objective

5.2.6 Browsing

From the home page, you can browse information under three menus:

- APPLICATION GUIDES - application help and component-level documentation
- NSP GUIDES - product-level guides
- TOOLS - NSP Alarm Search Tool

You can browse within a guide using the table of contents tree in the left navigation panel.

Use the breadcrumbs in the search path to return to search results or the home page. Use the browser back button to return to any previously visited page.

5.2.7 NSP Help Center notable information

The following table explains the NSP Help Center handling of exceptional circumstances.

Table 5-1 Help Center notable information

Case	Description
Recent and popular search history	To avoid accumulation of a large number of records on Recent and Popular searches, NSP triggers a purge job every week, which keeps the 5000 most recent records and deletes the rest.

Table 5-1 Help Center notable information (continued)

Case	Description
Application and help removal	If an NSP application or module is undeployed, it might take up to 24 hours before its help pages are removed from the Help Center, as this remove is done by a job which runs once nightly.
Application/module deployment	In the rare event that the Help Center does not get notification about deployment of an application or module, the help pages of the corresponding application or module will not be displayed. To address this uncommon problem, NSP includes an additional mechanism by which the Help Center tries to get information about which applications/modules are deployed, and if found, will display the corresponding help pages. Since this mechanism runs once every night, there might be a delay of up to 24 hours before help files of deployed applications/modules are seen in the Help Center.

5.3 Documentation delivery online

5.3.1 Doc Center

The on-product guides in the NSP Help Center are also available online in PDF from the Doc Center on the Nokia Support Portal. If you are a new user and require access to the service, contact your support representative.

As a registered user, you can use the following link for direct access to the NSP product documentation:

From the NSP Doc Center on the Nokia Support Portal, you can:

- filter by release, model, category, content type, and format
- sort the results by title, document number, most accessed, or issue date
- search for documents
- search inside documents
- create a downloadable collection of your filtered documents

User documentation is filed under the “Manuals and Guides” content type; Release Notices and Release Descriptions are filed under “Release Information.”

Documentation alerts

To receive an e-mail when new or reissued NSP customer documents are available, subscribe to the notification service on the Documentation Alerts Subscription page.

6 NSP Launchpad and dashboards

6.1 What is the Launchpad?

6.1.1

The NSP Launchpad is the starting point for NSP users. You open NSP applications from the Launchpad by clicking an application icon. Applications are organized by category. Depending on your NSP deployment, you may also be able to switch from the Launchpad to a dashboard view.

- Launch an application by clicking its icon. Right-click and select Open Link In New Tab to launch the application on a separate browser tab from the Launchpad. You can open multiple applications this way.
- In any NSP application window, you can switch to another application by clicking **Application Menu** and selecting an application from the list.
- Access a dashboard view (where available) from the menu in the upper left-hand corner of the Launchpad.
- Access NSP settings and URL links, or sign out of NSP from the **User** menu.

6.2 How do I change user settings?

6.2.1 Steps

NSP users can customize their application data refresh rate, GUI language, alarm list settings, and default dashboard view in the NSP Settings form. Administrative users can access a variety of global NSP settings; see the *NSP System Administrator Guide*.

1

From the NSP banner bar, click **User**, **Settings**.

2

Click **User Preferences** and configure your settings as needed.

- Global settings lets you personalize your settings when you are signed in. Here, you specify the **Polling Time** interval for application information display updates and the GUI **Language** used in your applications.
- **Row color with severity** provides the option to display the alarm severity color in your application alarm tables.
- **Set default dashboard shown on sign-in** lets you specify which NSP dashboard appears when you login to NSP.

3

Click **Save** when you have finished changing your settings.

END OF STEPS

6.3 How do I install the NFM-P client?

6.3.1 Purpose

Use this procedure to install the NFM-P client on Windows, Linux, or Macintosh systems.

6.3.2 Steps

1

Choose **User**, **Settings** from the NSP banner bar.

2

Click **NFM-P client**.

3

Click **INSTALLER INFO**.

4

Choose the zip for the binary installer package for your operating system and extract the files.

Note: The JNLP installation method is deprecated, and is to be removed in a future release.

END OF STEPS

6.4 What is the Network Health dashboard?

6.4.1

The Network Health dashboard provides a quick view of essential information relating to the proper function of your network. It presents an abbreviated view of equipment and service alarms, root cause alarms, graphical plots of service-affecting network object counts, and network object status. You can also view all of this information from the perspective of a network topology map, with NEs presented in their geographical location.

You can cross-launch from objects in the dashboard to a variety of NSP applications. The application that is launched depends on the object context. For example, you can launch the Fault Management application from an alarm object. Cross-launched applications open on a separate browser tab.

Clicking on certain objects in the Network Health dashboard takes you to a different view within the dashboard. For example, clicking on the Affected Services KPI icon in the Service Health dashlet

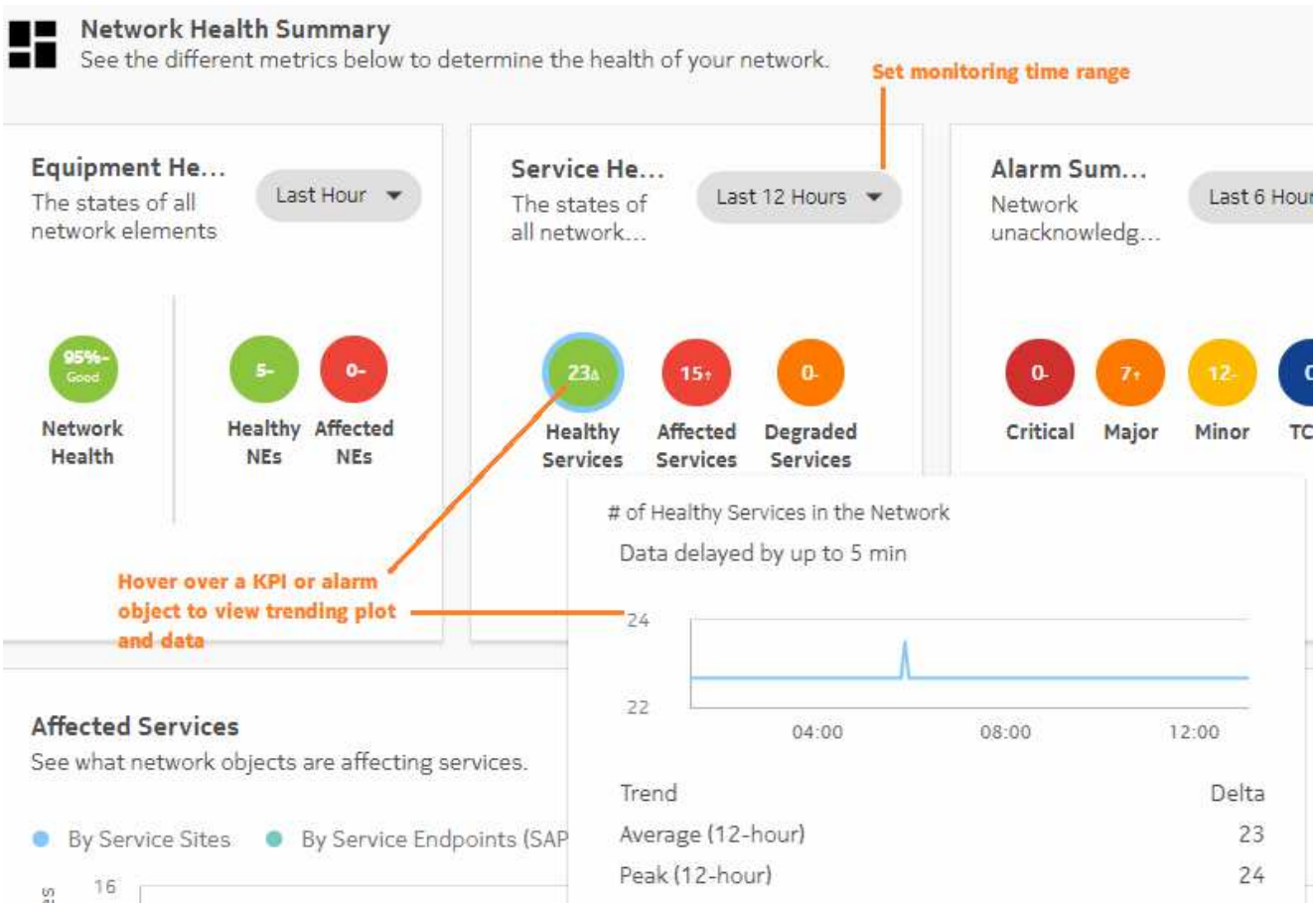
takes you to a detailed list of affected services in the Data Page. You return to the originating view by clicking the Previous View icon.

6.5 What do I see in the Network Health Summary?

6.5.1 Network Health Summary

The Network Health Summary pulls KPI and alarm information from various NSP components to show you the status of your network equipment and services.

The Network Health Summary dashlets include a cross-launch link to open an expended view of the dashlet information in the NSP application it is sourced from.



Do the following when working in the Network Health Summary:

- **Set a time range:** Click on a dashlet **Time Range** filter and select the dashlet's KPI monitor time range from the menu.

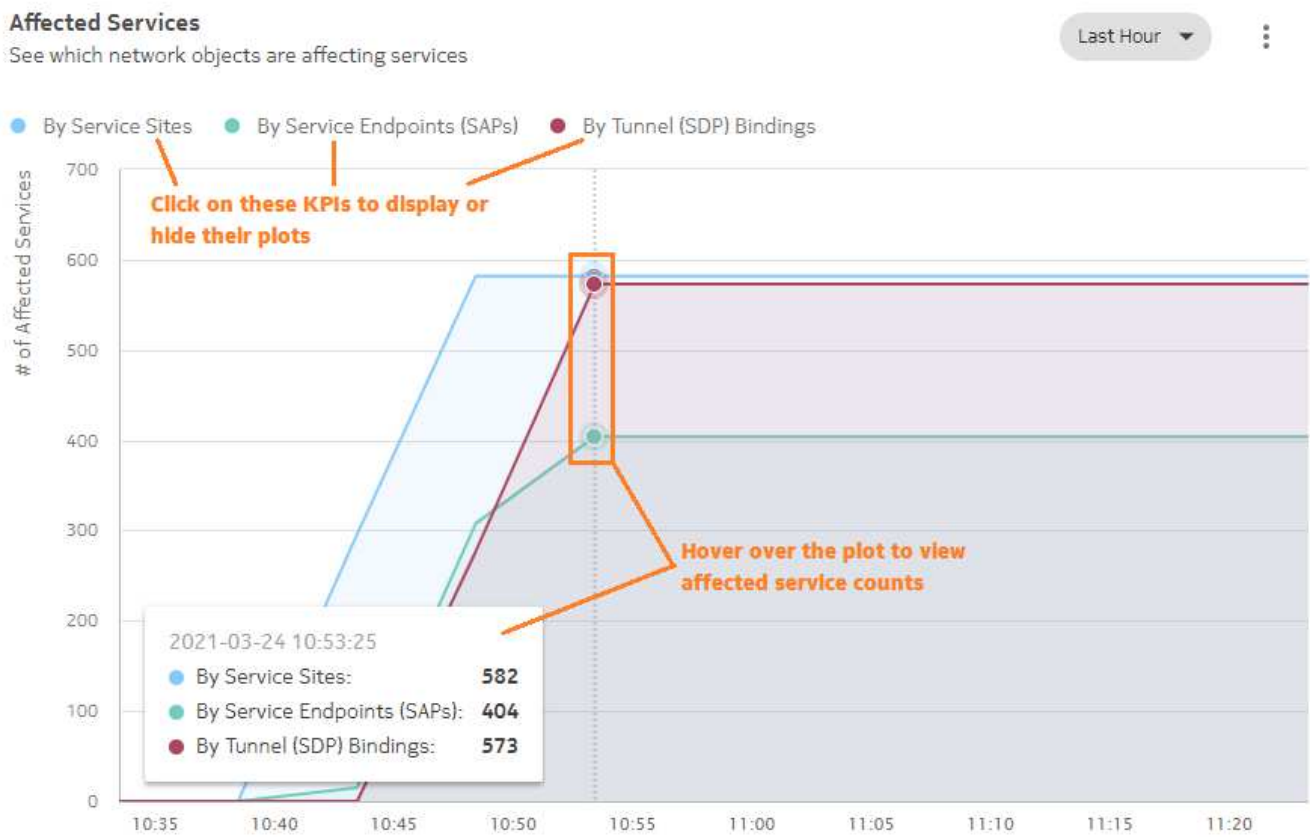
- **List NEs:** Click on a KPI icon in the Equipment Health dashlet to view an expanded Network Elements list in the Data Page.
- **List services:** Click a KPI icon in the Service Health dashlet to view an expanded Services list in the Data Page.
- **View service configuration health:** Click the Total Services icon in the Service Configuration Health dashlet to view an expanded Services list in the Data Page. Hover over the Total Services icon to see a breakdown of the different lifecycle states of the configured services.

  The Misaligned Services KPI shows a count of services whose configuration in the Service Fulfillment application is different from what is configured on the NEs. Click on this icon to cross-launch to a list of misaligned services in Service Fulfillment.
- **List alarms:** Click an alarm icon in the Alarm Summary dashlet to view the alarm list in the Fault Management application, filtered for severity, root-cause, and unacknowledged alarms.
- **View KPI trending:** Hover over a KPI icon to view a graphic plot of the KPI over the specified time range, along with KPI trend, peak and average values.

  Because the trend plot is meant to display average KPI values, the Peak value may not appear on the trend plot.

Affected Services

The Affected Services dashlet tells you which network objects are affecting the function of your services. Service sites, service endpoints, and tunnel bindings are plotted separately against the number of services they are affecting over the specified time range.



Do the following when working in the Affected Services dashlet:

- **Display or hide plots:** Click on the **By Service Sites**, **By Service Endpoints (SAPs)**, or **By Tunnel SDP Bindings** options to display or hide their plots on the graph.
- **Set a time range:** Click on the **Time Range** filter and select the KPI monitor time range from the menu.
- **Scan affected service counts:** Hover over the plot to view the affected service count by network object at a given time point. The affected service counts update as you move the cursor to the left or right along the plot.

  Because of the scale of the affected service plots, small fluctuations in affected service counts may not be visible in the plots.
- **List service-affecting objects:** Click **More** ⋮ , **Show [Service Sites|Service Endpoints|Tunnel Bindings] Affecting Services** to display a list of the selected object type in the Data Page.
- **Switch to larger view:** Click **More** ⋮ , **Expand Size** or **Full Screen** to display the list in larger formats.

  When in expanded or full screen display, you can click **More** ⋮ , **Restore Size** to return to compact display.

Simplified RAN Transport

The SRT is a solution for T-BTS management that merges management of RAN and transport components of a 4G/5G wireless network. Network monitoring components of SRT exist as a dashlet of the Network Health application to provide a single “pane of glass” view of T-BTS transport features and RAN application bindings to IP transport services.

See *Simplified RAN Transport Solution* for more information.

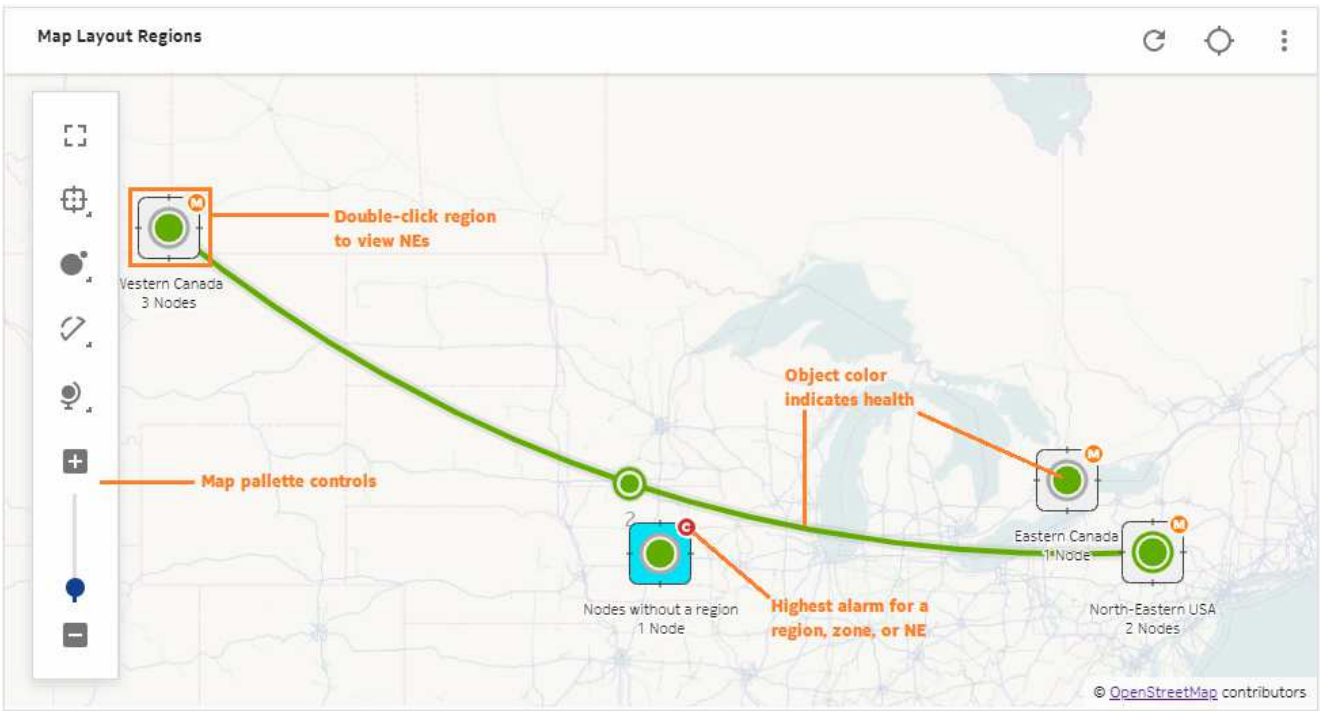
6.6 What does the Topology View show me?

6.6.1

The Topology View is a geographical map of your network equipment. NEs are grouped into geographical regions and zones. The map can be zoomed out to the regional or continental level, or zoomed in to the city street level, providing precise information about network equipment locations.

Note: Administrative users can view subnets and links to subnets as objects on the Topology map. Non-administrative users whose access rights are defined through UAC cannot view subnets and links to subnets because the Topology map is intended to display networking equipment. Subnets are not actual equipment.

Alarm and status information are automatically refreshed in the map.



If an NE does not belong to a supervision group, the alarm flag for the NE displays as Unknown.

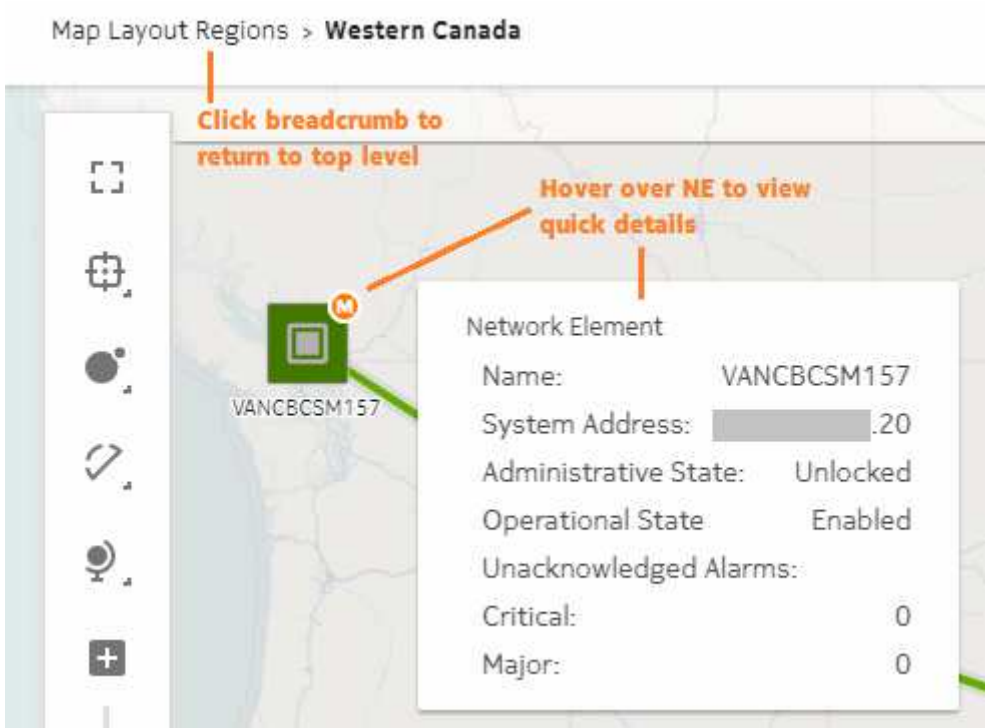
Do the following when working in the Topology Map:

- **Find a map object:** Click **Find in Map** . Select an object type from the menu and type a search string. You can click on an entry in the results list to go to the object's location in the map layout.
- **Update the map:** Click **Refresh** to update the map display.

  The Refresh command can take significant time on large networks. Use it only if there have been changes to the NSP common map layout and you want them to appear in the NH dashboard, or if the map data is stale (in which case you are prompted to refresh the map).

  Alarm and status information are automatically refreshed in the map.
- **View NEs in a region:** Double-click on a region to expand it and view its NEs.

  To return to the top-level map view, click on the left-most item in the map breadcrumb.
- **View quick information about an NE:** Hover over an NE object to display basic identification and status information for the NE in a pop-up window.

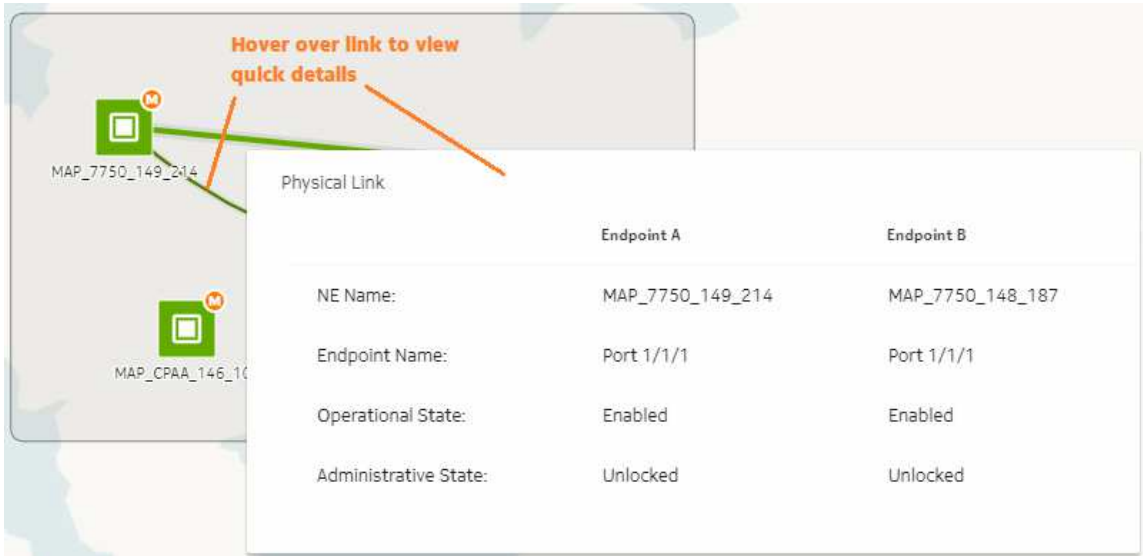


- **View detailed information about an NE:**

  Right-click on an NE object and select one of the following options to view additional information about the NE in an NSP application.
  - **Show In Current Alarm List** displays current alarms for the NE in Fault Management.
  - **Show In Network Elements List** displays the NE in the Data Page, Network Element list.
  - **Show In Equipment View** displays the NE in Network Supervision, Equipment Inventory.

- **Show in Troubleshooting Dashboard** displays the NE on the Troubleshooting dashboard with expanded performance and alarm information.
- **Plot Statistics** displays KPI plots for the NE in Insights Viewer.
- **Open NE Session** opens a CLI session on the NE.

- **View quick information about a link:** Hover over a link object to display basic identification and status information for the link in a pop-up window.



- **View detailed information about a link:**

  Right-click on a link object and select one of the following options to view additional information about the link in an NSP application.
  - **Show In Current Alarm List** displays current alarms for the link in Fault Management.
  - **Show In Links List** displays the link along with other links in the Data Page, Links list.
  - **Show in Troubleshooting Dashboard** displays the link on the Troubleshooting dashboard with expanded endpoint and alarm information.
  - **Plot Utilization Statistics** displays KPI plots for the link in Insights Viewer.
  - **Plot Error Statistics** displays KPI plots for the link in Insights Viewer.
- **Switch to a larger map display:** Click **Full Screen** to display the map in a larger format. In Full Screen view, you can click **Restore Size** to return to compact display.
- Set your own map layout view: Click **More** , **Save As My Layout** to save the map display settings as they are currently configured. The map will display the same way the next time you open the Network Health dashboard.

  If you want to return to the default map display settings, click **More** , **Restore To Common Layout**.

Map Palette Controls

Use the controls on the map palette to adjust the behaviour and appearance of the map and objects.

When objects share the same physical location, the map shows a multi-layered icon shaded in blue. To see the co-located objects individually, drag them off of the multi-layered icon.

Table 6-1 Map Palette controls

Fit to Screen	Zoom the map to fit the selected region to available screen area.
Clustering controls	Options to display NE cluster health as a pie chart or a solid circle on the cluster. Object color indicates health. Display or hide region and zone boundaries. Option to move all contained objects when moving a region or zone. Display options for connectors to any NEs that are external to a region or zone: • Group external NEs with their immediate parent zone or region; the map displays all connectors to zones or subzones that contain the external NEs. This option shows greater detail. • Group external NEs with their top-level region; the map displays a single connector to the region icon. This option shows less detail.
Adjust vertices	Show/hide text labels for map objects. Adjust icon size for NEs, zones, and regions.
Adjust Links	Show or hide links between NEs, zones, and regions. Show or hide links when the objects they connect to are outside the map view. Adjust link curvature (i.e., how deep of an arc) between objects. Adjust link grouping threshold. Options to display link group health as a pie chart or a solid circle on the group. Object color indicates health. Show or hide the number of links in a group.
Map View	Turn on Bird's-eye View (shows entire map in small inset). Adjust the opacity of the background map.
Zoom	Zoom into and out from the map.

6.7 What's in the News Feed?

6.7.1

The News Feed provides a live feed of unacknowledged root cause network alarms, as they occur in real time. Alarm severity levels of Warning, Minor, Major and Critical are displayed.

Do the following when working in the News Feed:

- **View detailed information about an alarm:** You can cross-launch from an alarm object in the News Feed to an NSP application to see more information about the alarm or the network object it originated from.

  Click More ⋮ on an alarm and select a cross-launch option. Cross-launch application availability varies depending on originating object for the alarm:
  - **Show in Current Alarm List** opens the alarm in Fault Management. For all alarms.
  - **Show in Equipment View** Opens the originating object in Network Supervision, Equipment Inventory. For NE and port alarms.
  - **Plot Utilization|Error Statistics** Opens Insights Viewer. For NE, port, and physical link alarms.
  - **Show in Map** Opens the originating object in the Network Health dashboard, Topology View. For NE and physical link alarms.
  - **Show in Troubleshooting Dashboard** Opens the originating object in a Troubleshooting dashboard summary. For NE, service, port, and physical link alarms.
- **Switch to larger view:** Click **More** ⋮ , **Expand Size** or **Full Screen** to display the News Feed in larger formats.

  When in expanded or full screen display, you can click **More** ⋮ , **Restore Size** to return to compact display.
- **Stop automatic updates:** Click **More** ⋮ , **Set To Manual Refresh** to stop automatic News Feed updates. A manual update button is added to the New Feed that you can click as needed.

  When in manual update mode, you can click **More** ⋮ , **Set To Auto Refresh** to return to automatic updates.
- **Sort the News Feed:** Click on the Sort By filter and select **By Time Reported** to list the most recent alarms first, or **By Severity** to list the most severe alarms first.

6.8 What does the Data Page show me?

6.8.1

The Data Page provides compact lists for various network object types in dashlets, with basic identification and status information for each object. You can expand a dashlet to view complete object lists with full status information.

- **Switch to larger view:** Click **More** ⋮ , **Expand Size** or **Full Screen** to display an object list dashlet in larger formats with more information.

  When in expanded or full screen display, you can click **More** ⋮ , **Restore Size** to return to compact display.

- **Stop automatic updates:** Click **More** ⋮ , **Manual Update Only** to stop automatic data updates for a dashlet. A manual update button is added to the dashlet that you can click as needed.

  When in manual update mode, you can click **More** ⋮ , **Auto Refresh** to return to automatic data updates.

Expanded and Full Screen object list

You can expand an object list dashlet to the full width or to the full size of your browser window, with expanded data displayed for each list item in columnar format. The auto-refresh function is turned off by default when you switch to expanded or full-screen display. You must refresh the object list manually or click **More** ⋮ , **Auto Refresh** to switch to automatic data updates.

Click **More** ⋮ , **Restore Size** to return to the dashlet view.

The expanded object list has a variety of tools available to help you control what you see, including sorting and filtering options:

- **View detailed information about a list item:** Click More ⋮ on a list item and select an NSP application in which to view the object; see "Cross-launching NSP applications" (p. 58). (If there is only one application available for cross-launch, the More button is replaced with ◉ .)
- **Filter the object list under a specific column:** Type a text string in the text field or select a filter option at the top of a column and press **Enter**.

  The object list automatically updates with filter results as you type your filter string if the **Auto Refresh** option is enabled.

  Where applicable, click **Filter Operator** ▼ next to the text field and select an operator from the menu.

  Click **More - List Options** ⋮ , **Clear Filters** to clear column filters.
- **Sort the object list under a specific column:** Click on a column header to sort the list under that column. Click on the header again to toggle between ascending and descending sorting.

  Click **More - List Options** ⋮ , **Clear Sorting** to clear column sorting.
- **Export the object list:** Next to the column headers, click **More - List Options** ⋮ , **Export** to export the current page or selected rows to a CSV, XLXS, or XML file.
- **Reduce white space between rows:** Next to the column headers, click **More - List Options** ⋮ , **Compact Rows**. The object list appears more condensed, allowing more visible rows.
- **Arrange object list columns:**
  - **Move a column:** Click and drag a column header to a new position.

    Re-positioned Data Page columns are saved under your login name and are maintained in future NSP sessions. User-specified column settings are only applied to expanded list views. When Data Page lists are displayed as dashlets, a default column order is maintained.
  - **Pin a column:** Click on the column header menu ☰ , and select **Pin**, **Pin Left** to pin the column to the left-most end of the list, **Pin Right** to pin the column to the right-most end of the list, or **No Pin** to return the column to its default location.

    Pinned Data Page column settings are saved under your login name and are maintained in future NSP sessions.
  - **Resize a column:** Hover between column titles until a cursor appears. Click and drag the cursor to change the column width.

- **Reset column width to automatic setting:** Click on the column header menu , and select **Autosize This Column**. Select **Autosize All Columns** to reset all columns to automatic size settings.
- **Return columns to default settings:** Click on a column header menu , and select Reset Columns to remove all column pin settings and show/hide settings.
- **Hide or display columns:** Next to the column headers, click **More - List Options** , **Manage Columns**. In the Manage Columns form, disable the check box for any column you do not want to appear in the list, or enable the check box for any column you want to appear. Click **Apply**.

Cross-launching NSP applications

You can cross-launch from objects in Expanded or Full Screen views of the Data Page to other NSP applications. Cross-launch availability varies depending on the object type. The following table lists the cross-launch commands available for various objects, and the NSP application that opens for each command.

Table 6-2 Cross-launch options from Data Page objects

Cross-launch command	Opens NSP application	Available for objects
Show In Current Alarms List	Fault Management	NEs, Links, Ports, Service Sites, Service Endpoints, Tunnel Bindings
Show In Equipment View	Network Supervision	NEs, Ports
Show In Map	Network Health dashboard	NEs and Links
Show in Troubleshooting Dashboard	Troubleshooting dashboard	NEs, Links, Ports, Service Sites, Service Endpoints, Tunnel Bindings
Open NE Session	CLI	NEs
Plot Statistics	Insights Viewer	NEs
Plot Utilization Statistics	Insights Viewer	Links and Ports
Plot Error Statistics	Insights Viewer	Links and Ports

6.9 What is the Troubleshooting dashboard?

6.9.1

The Troubleshooting dashboard provides the user with a centralized view of network equipment and service performance. The dashboard allows a network operator to view summarized

performance information, and to drill down into specific objects and view performance details, opening objects in NSP applications where necessary.

Operators can search for objects to troubleshoot under the following contexts:

- Network Elements
- Services
- Links
- Ports

Some of the dashlets on the Troubleshooting dashboard include cross-launch links to examine an object in greater detail in a separate NSP application. Cross-launch is not possible if the related object is not part of a supervision group.

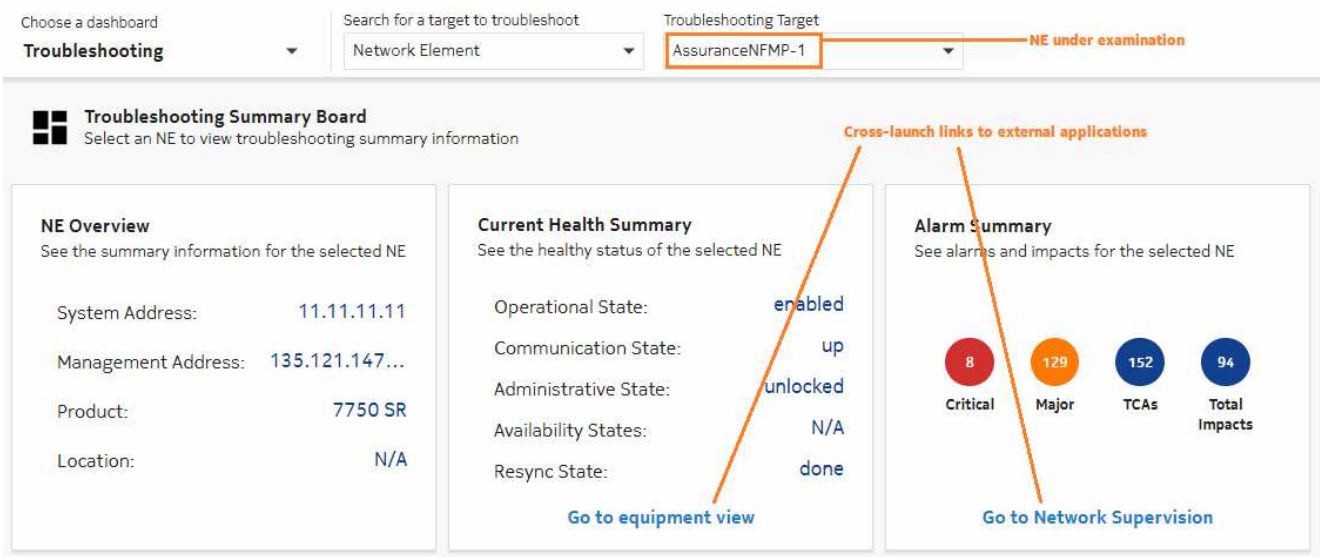
6.10 What is the Network Element Troubleshooting Summary?

6.10.1

The Network Element Summary board consists of a selection of dashlets intended to show an overall picture of a selected NE, providing the necessary information to troubleshoot it. Some dashlets include a **Go To...** link that cross-launches a separate NSP application where you can view the dashlet's information in greater detail. On alarm dashlets, you can click on an alarm counter to open the related alarms in a list view. Cross-launch to supervision applications via links or alarm circles is not possible if the related object is not part of a supervision group.

The Network Element Summary board provides information in a series of dashlets:

- NE Overview
- Current Health Summary
- Alarm Summary



To view an NE in the Troubleshooting dashboard, do the following:

1. From the **Choose a Dashboard** menu, select **Troubleshooting**.
2. From the **Search For a Target to Troubleshoot** menu, select **Network Element**.
3. From the **Troubleshooting Target** menu, select an NE.

   The dashlets are populated with information for the NE.
4. Click on a cross-launch link at the bottom of a dashlet to open the NE in an external NSP application.
5. Click on an alarm count circle to open the alarm list in the Fault Management application.

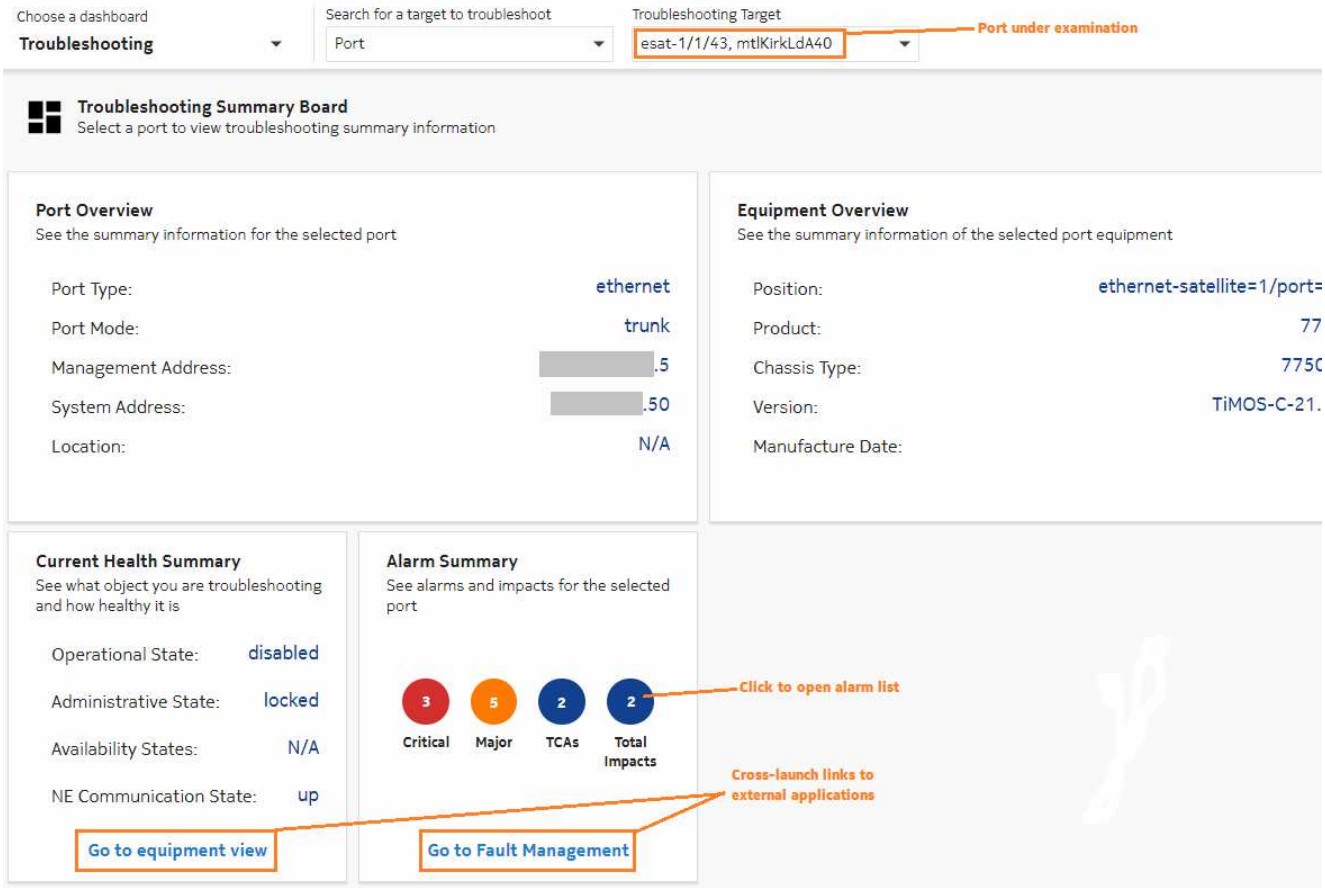
6.11 What is the Port Troubleshooting Summary?

6.11.1

The Port Summary board consists of a selection of dashlets intended to show an overall picture of a selected port, providing the necessary information to troubleshoot it. Some dashlets include a **Go To...** link that cross-launches a separate NSP application where you can view the dashlet's information in greater detail. On alarm dashlets, you can click on an alarm counter to open the related alarms in a list view. Cross-launch to supervision applications via links or alarm circles is not possible if the related object is not part of a supervision group.

The Port Summary board provides information in a series of dashlets:

- Port Overview
- Current Health Summary
- Alarm Summary
- Equipment Overview



To view a port in the Troubleshooting dashboard, do the following:

1. From the **Choose a Dashboard** menu, select **Troubleshooting**.
2. From the **Search For a Target to Troubleshoot** menu, select **Port**.
3. From the **Troubleshooting Target** menu, select a port.

   The dashlets are populated with information for the port.
4. Click on a cross-launch link at the bottom of a dashlet to open the port in an external NSP application.
5. Click on an alarm count circle to open the alarm list in the Fault Management application.

6.12 What is the Link Troubleshooting Summary?

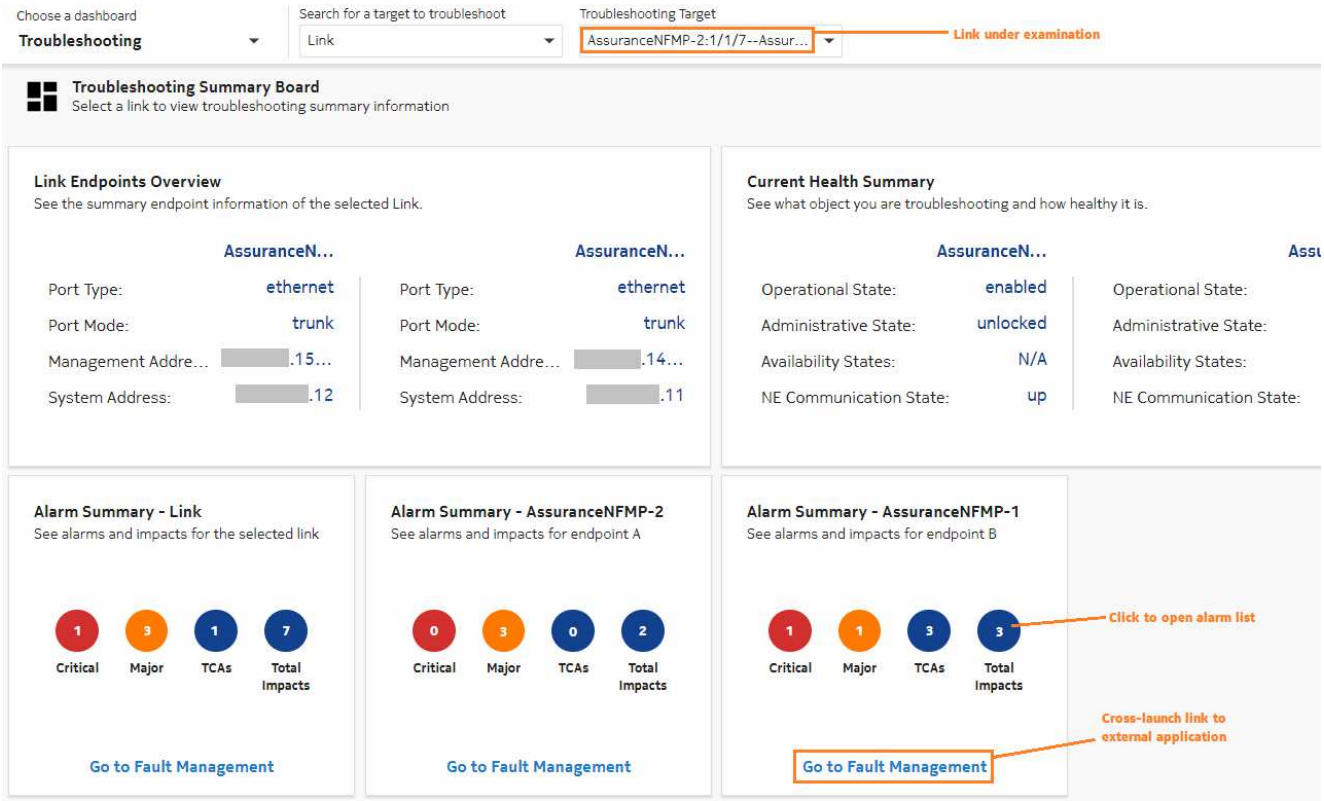
6.12.1

The Link Summary board consists of a selection of dashlets intended to show an overall picture of a selected link, providing the necessary information to troubleshoot it. Some dashlets include a **Go To...** link that cross-launches a separate NSP application where you can view the dashlet's

information in greater detail. On alarm dashlets, you can click on an alarm counter to open the related alarms in a list view. Cross-launch to supervision applications via links or alarm circles is not possible if the related object is not part of a supervision group.

The Link Summary board provides information in a series of dashlets:

- Link Endpoints Overview
- Current Health Summary
- Alarm Summary - Link
- Alarm Summary - Endpoint A
- Alarm Summary - Endpoint B



To view a link in the Troubleshooting dashboard, do the following:

1. From the **Choose a Dashboard** menu, select **Troubleshooting**.
2. From the **Search For a Target to Troubleshoot** menu, select **Link**.
3. From the **Troubleshooting Target** menu, select a link.

   The dashlets are populated with information for the link.
4. Click on a cross-launch link at the bottom of a dashlet to open the link in an external NSP application.

5. Click on an alarm count circle to open the alarm list in the Fault Management application.

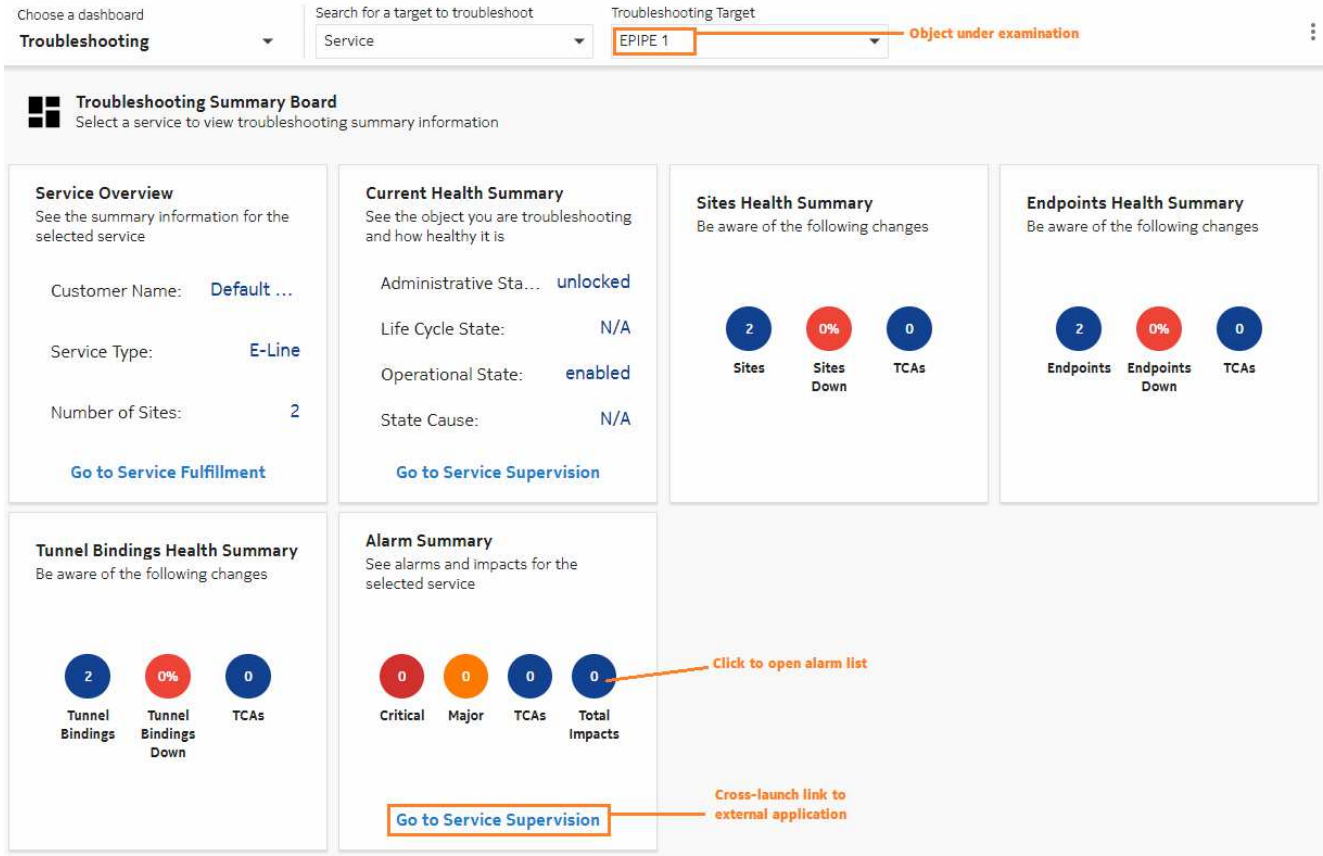
6.13 What is the Service Troubleshooting Summary?

6.13.1

The Service Summary board consists of a selection of dashlets intended to show an overall picture of a selected service, providing the necessary information to troubleshoot it. Some dashlets include a **Go To...** link that cross-launches a separate NSP application where you can view the dashlet's information in greater detail. On alarm dashlets, you can click on an alarm counter to open the related alarms in a list view. Cross-launch to supervision applications via links or alarm circles is not possible if the related object is not part of a supervision group.

The Service Summary board provides information in a series of dashlets:

- Service Overview
- Current Health Summary
- Sites Health Summary
- Endpoints Health Summary
- Tunnel Bridges Health Summary
- Alarm Summary



To view a service in the Troubleshooting dashboard, do the following:

1. From the **Choose a Dashboard** menu, select **Troubleshooting**.
2. From the **Search For a Target to Troubleshoot** menu, select **Service**.
3. From the **Troubleshooting Target** menu, select a service.

   The dashlets are populated with information for the service.
4. Click on a cross-launch link at the bottom of a dashlet to open the service in an external NSP application.
5. Click on an alarm count circle to open the alarm list in the Fault Management application.

6.14 How do I change my dashboard layout?

6.14.1

You can arrange the NSP dashboards to suit your personal requirements by rearranging and re-sizing dashlets. You can also hide dashlets you don’t need to see, with the option to re-display them later. The changes you make are saved under your login name and are maintained in future NSP sessions.

1. Click **More** , **Edit Dashboard**.

   The dashboard is placed in Edit mode. Complete any of the following tasks to change your dashboard:

   - To resize a dashlet, click and drag the **Resize** handle at the corner of the dashlet. Release the handle when the dashlet is the correct size.
   - To move a dashlet, hover the mouse pointer over the dashlet and then click and drag the dashlet to the desired position. Release the mouse button when the dashlet is in the correct position.
   - To remove a dashlet from the dashboard, click **Delete** on the dashlet you want to remove. Click **DELETE** to confirm the removal.
   - To add a currently-hidden dashlet to the dashboard, click **Add** . The Add Dashlet form opens. Select the dashlet you want to add to the dashboard and click **ADD**.

     If the Add Dashlet form is empty, all available dashlets are already displayed for this context.
   - To replace a dashlet with a currently-hidden dashlet, click **Replace** on the dashlet you want to replace. The Replace Dashlet form opens. Select the dashlet you want to add to the dashboard and click **REPLACE**.

     If the Replace Dashlet form is empty, all available dashlets are already displayed for this context.
   - To return your dashboard to default layout settings, **More** , **Reset To Default Layout**. Click **RESET** to confirm your action.

2. When you have finished changing your dashboard layout, click **SAVE**. Then click **SAVE AS DEFAULT** to confirm your changes.

6.15 Is something missing from your dashboard?

6.15.1

As an NSP user, you have access to the Network Health Dashboard, along with all of the dashlets it contains. The Network Health Dashboard is available in shared-mode NSP deployments.

This topic contains onboarding information to help you ensure that the Network Health dashboard is able to display all of the network information it is designed for. Because the Network Health dashboard pulls information from a variety of NSP applications, it is essential that those applications are configured to gather the required information, and that NSP users are assigned access rights on those applications.

The following considerations affect your data and application access in the dashboard. Most of these tasks require administrative access:

- To see network health data in the dashlets, you must have access to all network resources for which you are collecting network health data, including NEs and services; see the *User Manager Application Help*.
- To cross-launch from a dashlet to an application, you need to be assigned Read (or higher) access to the target application; see the *User Manager Application Help*.
- Your system administrator must set a background map layer URL in the NSP system settings and create a common map layout in Group Manager for a network map to appear in the Topology View; see the *Group Manager Application Help*.

- Your system administrator must configure views and supervision groups for Service Supervision in Group Manager to enable cross-launching from the dashboard to Service Supervision; see the *Group Manager Application Help*.
- Your system administrator must configure views and supervision groups for Network Supervision in Group Manager to enable cross-launching from the dashboard to Network Supervision; see the *Group Manager Application Help*.
- Your system administrator must configure a subscription in Insights Administrator with the DB Subscriptions option enabled. This makes subscription data available to Insights Viewer (Analytics) for historical statistics collection.
- You must configure a MIB policy to include the MIB file for all NE types in your network to collect statistics and KPI information from your NEs; see the *Statistics Management Guide*.

Typically, you will need access to the following applications:

- Fault Management
- Network Supervision
- Service Supervision

Note: If you are running NSP against an NFM-P user database with User Access Control turned *off* in User Manager, certain dashlets in the Network Health dashboard will not display for a user unless their user group in the NFM-P user database is also created in User Manager (with identical names and role assignments). The easiest way to accomplish this is to use the Import NFM-P User Groups function in User Manager.

7 Network Functions Interconnect

7.1 Why use Network Functions Interconnect (NF-IX)?

7.1.1 General information

Network Functions Interconnect (NF-IX) provides a unified and dynamic network fabric that seamlessly extends from connected clients in the access network cloud to distributed network functions (NFs) in the edge cloud and core data centers, thus automating connectivity across emerging mobile cloud service architectures with support for deterministic delivery requirements. NF-IX maintains the functional de-coupling between a cloud-native service overlay and network-native bearer services to rapidly compose new services with a broad range of delivery options, while automatically mapping overlay SLA policies on corresponding underlying transport SLAs and dynamically engineering the optimal bandwidth resources required in the WAN.

NF-IX leverages BGP MPLS-based Ethernet VPNs (EVPN – RFC 7432) to enable network virtualization in data centers by providing Layer 2 or Layer 3 VPN connectivity between VNFs and PNFs that are part of an end-to-end service with Segment Routing tunnels across the network.

NF-IX transport leverages Segment Routing for intra-domain routing and Segment Routing with Traffic Engineering (SR-TE) to dynamically engineer inter-domain service tunnels between NFs. SR-TE enables dynamic traffic engineering services and granular per-flow/per-application steering with various loose or strict routing constraints, including bandwidth, latency, path diversity and explicit objects to include or exclude in the route. Segment routing also implicitly supports equal-cost multi-path (ECMP) routing, which allows load-balancing traffic over available links in the path.

NF-IX provides connectivity and inter-operability for networks that do not support Segment Routing encapsulation by inter-working with Virtual Extensible LAN (VXLAN) and/or MPLS over UDP (MPLSoUDP) fabrics to Segment Routing fabrics.

For additional information on the proposed NF-IX architecture refer to the IETF draft document *draft-bookham-rtgwg-nfix-arch*.

Note: Contact your Nokia support representative before attempting to deploy or use NF-IX.

Transport tech zone algorithm

The Transport Tech Zone (TTZ) algorithm is disabled by default during IP resource control server installation, but is required for use of NF-IX. To enable TTZ, make the following changes during installation: 1. . 2. 3. St

1. In the config-yml file, set "auto_start: false".
2. In the arm-system.conf file, set:

```
arm-system {
   nrcp {
      nrcp_spf_transport_techzone {
         optimization_enabled = true
         }
```

3. Start the server. Execute:

```
nspdctl start
```

7.2 NSP as a Segment Routing Interconnect Controller

7.2.1 SRIC overview

NF-IX allows the NSP to function as a Segment Routing Interconnect Controller (SRIC) to automate the process of mapping SLA requirements for VNF and PNF connectivity within a datacenter and across the WAN. The SRIC is implemented with the IP resource control server.

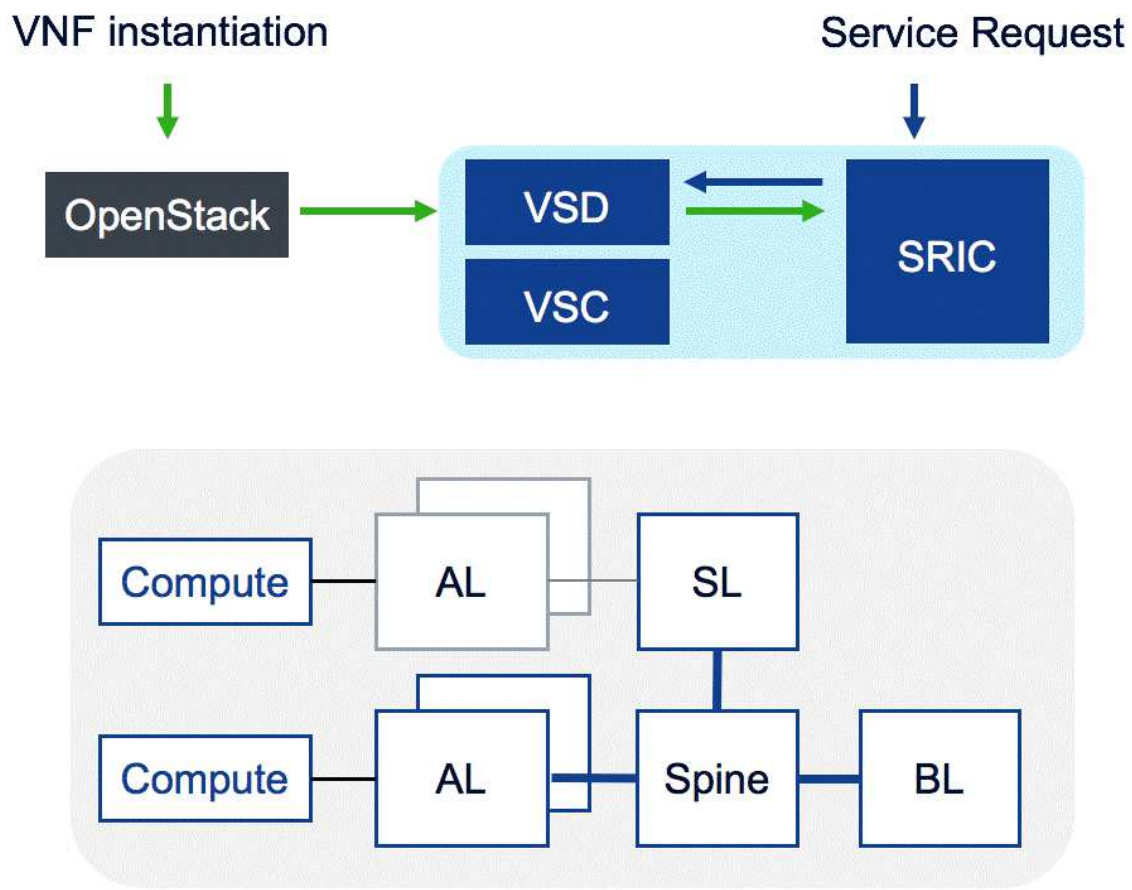
NF-IX, and NSP in an SRIC role, remain in development and the current implementation does not represent the intended, complete functionality described in IETF document *draft-bookham-rtgwg-nfix-arch*. The functionality described below is an initial feature set which provides automated inter-connectivity provisioning between VXLAN and SR fabrics for VNFs within a datacenter.

The SRIC implementation performs the following tasks:

- Integrates with the Nokia Nuage Virtualized Services Platform for an Openstack infrastructure for L3 Domains and L2 Domains that require MPLS transport
- Discovers datacenter gateway (Access Leaf) and VNF entities
- Discovers the IGP topology
- Automates provisioning of network elements for VNF connectivity while configuring the necessary EVPN service configuration
- Automatically determines and provisions network elements at stitching points (Services Leaf), providing VXLAN and SR interworking

NSP, in its SRIC role, is used to automatically provision network elements with the role of Access Leaf and Services Leaf within a datacenter that contains a mixture of Segment Routing and VXLAN transport encapsulation in the network fabric. Access Leaf entities assume the role of gateways and are connected to compute entities, running the Nokia Nuage Virtual Routing and Switching software agent which may support Virtio or SR-IOV virtualization capabilities. An Access Leaf may support VXLAN or Segment Routing transport. Access Leafs which support only VXLAN are managed and provisioned by the Nokia Nuage VSP and entities which support Segment Routing are managed and provisioned by SRIC. Services Leaf network elements support VXLAN and Segment Routing, providing the capability to perform transport stitching between VXLAN and SR transport for a given service. Certain routers are designated as stitching points between the VXLAN and SR domains - such a route is referred to as a Services Leaf. They are managed and provisioned by NSP in its SRIC role. NSP communicates with the Nuage Virtualized Service Directory (VSD), to instantiate services and discover data center entities - including but not limited to Gateways - VRS entities, and Virtual Machine and Bridge Virtual Ports. VSD provides the model and data-binding automation between Openstack and NSP, integrating with Openstack via plugins. VSD also communicates with the VRS via the Virtualized Services Controller (VSC). For more information on the VSP platform components and architecture, see the Nuage documentation suite.

Figure 7-1 High-level view of NF-IX components



A service definition includes policies and configuration for an L2 or L3 service on NSP and VSD. Within NSP, a service is instantiated as either an L2 DCI or L3 DCI service type. For L3 services, the service construct definition originates on NSP and NSP instantiates an L3 Domain on VSD. For L2 services, the construct originates on VSD and is discovered by NSP. VNFs compromised of virtual machines are instantiated on one, or many compute nodes. Through Nuage and Openstack plugin integration, Bridge virtual ports and/or Virtual Machine virtual ports (which model the VM instantiation) are created on VSD automatically, in the context of a given subnet. The virtual ports identify the compute node and gateway (Access Leaf) entity. NSP discovers this information from VSD and provisions the necessary Access Leaf under its configuration and Nuage VSD provisions the necessary Access Leaf entity under its management. If required, NSP also provisions Service Leafs to provide inter-working between the VXLAN and SR MPLS portions of the fabric. When Virtual Machine entities are disposed, cleanup of the service configuration occurs on the Access Leaf and Service Leaf entities automatically.

7.3 DCI service types

7.3.1 DCI service types overview

NF-IX services are delivered in the form of L2 and L3 DCI service types by NSP. The service model for these types provide themselves as:

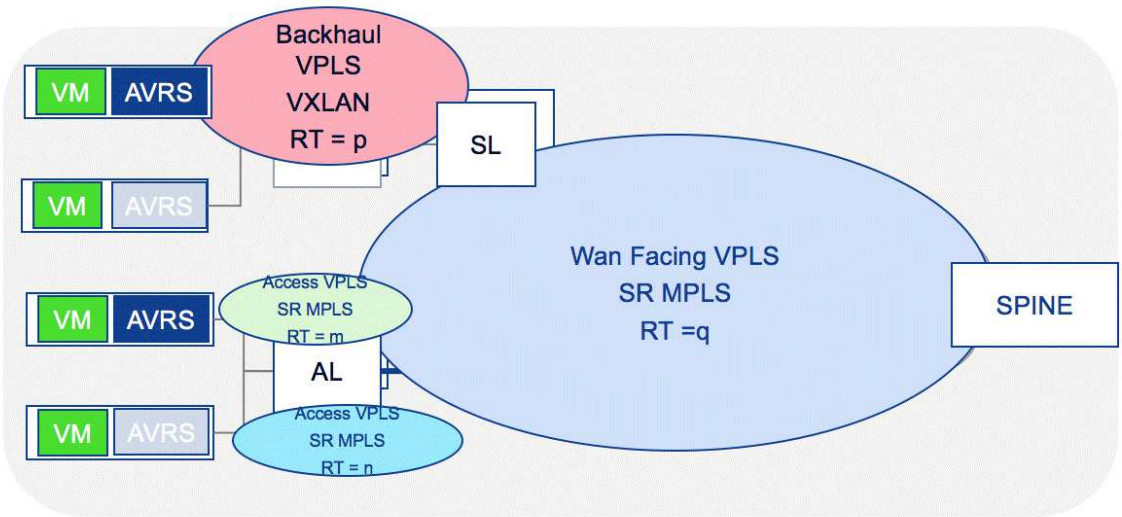
- An abstract container for the composite service requirements in various deployment types
- A binding for DC related entities, its abstractions, and network element device configurations
- A binding to invoke automatic service and tunnel differential algorithms

The concepts and use cases continue to evolve through various NF-IX phases to achieve service deployment in brownfield and greenfield networks as networks transition to an SR-based fabric. The methodology of NSP is to automatically provision only specific entities which require configuration and auto-clean the configuration when no longer required.

7.3.2 L3 DCI services

The L3 DCI service contains a Service Connectivity Type parameter to support an evolution of an NFIX service. The “VXLAN Stitched” Transport Connectivity Typeis is supported by NSP. Other connectivity types are proof-of-concept. The “VXLAN Stitched” option informs NSP that it will be performing SR MPLS and VXLAN inter-working connectivity in the topology. This section describes the “VXLAN Stitched” scenario.

Figure 7-2 L3 DCI service topology



L3 DCI with “VXLAN stitched” is a multi-subnet, layer 2 and layer 3 IP/Ethernet service realized with BGP-EVPN exchanging Type 1, Type 2, and Type 5 EVPN routes that are provisioned as Routed VPLS (R-VPLS) configuration on the network elements. Auto-bind transport encapsulation with SR-ISIS or SR-OSPF are used. EVPN service configuration is provisioned on Access Leaf nodes and

Service Leaf nodes by NSP to interconnect with Nuage VSP L3 Domain transport provisioned in the VXLAN portion of the network. VM instantiation results in the creation of a L2 EVPN service if one does not already exist. VMs that are part of the same service and attached to the same Access Leaf are connected via the access-facing L2 EVPN service. VMs that are attached to different Access Leaf nodes are connected via a (WAN-facing) L3 EVPN service that is established between those Access Leaf nodes. If a subnet has been designated as VXLAN, the Nuage VSD provisions the network elements in the VXLAN domain for each VXLAN subnet as well as a Backhaul VPLS service to provide inter-connectivity of multiple VXLAN subnets.

NSP automatically computes the appropriate service leaf nodes that require additional service configuration to fulfil the need for an entity to provide inter-working between VXLAN and SR. On the Service Leaf, NSP provisions an EVPN service configuration that exchanges routes with the VXLAN domain and the SR MPLS domain to perform route translation. The Service Leaf accepts EVPN routes from the VXLAN domain with a tunnel encapsulation of VXLAN and re-advertises those routes into the WAN Facing entities with an encapsulation of MPLS. The Service Leaf accepts EVPN routes from the SR domain with a tunnel encapsulation of MPLS and re-advertises those routes to the Backhaul service with an encapsulation of VXLAN. The routes are re-advertised with a next hop of the Service Leaf.

The L3 DCI is instantiated on the NSP via API or UI by selecting a VSD instance and Domain Template as an endpoint on the L3 DCI service. This triggers NSP to instantiate an L3 Domain on VSD, subnets on VSD model, and describe per-subnet attributes such as IP addressing. Upon the reception of Virtual Ports corresponding to a VNF from VSD, NSP provisions the access interface and Service Site configuration on the respective Access Leaf and Service Leaf nodes. Entities discovered from VSD in NSP are identified in the UI and API as having a Port Type of “Virtual Port”. The existence of a Virtual Port triggers the creation of Access Ports on the respective access element. When NSP provisions L3 Interfaces, IP addressing is provisioned based on the configurations described in VSD.

NSP auto-generates the Route Target (RT), Route Distinguisher (RD), and Ethernet VLAN Identifier (EVI) service parameters for Access Facing and Wan Facing EVPN instances. The L3 DCI will use the RT/RD Range Policy when attempting to generate the values, or if not configured, will use the default RT/RD Range Policy. When “Use Provider AS” is selected and Type 0 or Type 2 RDs are used, NSP will attempt to determine an appropriate Autonomous System number from the network elements part of the service, with a preference for the Autonomous System number configured on VSD. If possible, the system will attempt to generate RT values with a consistent numerical value as the EVI. The VXLAN Backhaul VXLAN EVPN instances parameters are auto-generated and managed by Nuage VSD.

Name generation occurs at multiple stages for various configuration objects such as service site names and interface names. Some generated names may be configured in the DCI service template. Description fields are also auto-generated and attempt to provide identifier information for the underlying entity which triggered the creation of the entity. For example, VPLS Port description fields will contain the name of the Virtual Bridge Port that was defined in VSD.

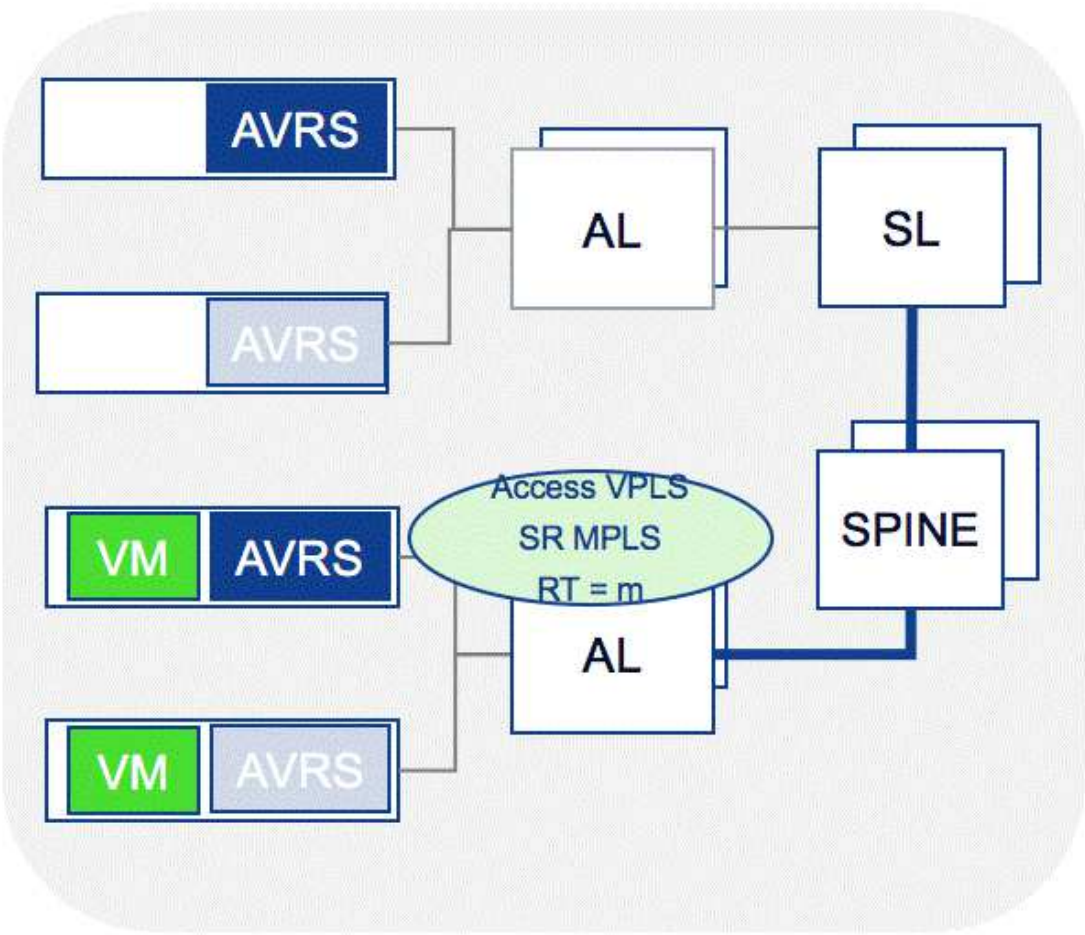
Note: In addition to a primary IP address, L3 DCI services support the configuration of one or more secondary IP addresses on loopback endpoints. The endpoints of an L3 DCI service can be added, modified, or deleted using REST APIs. For more information, see the Network Developer Portal.

See 7.10 “How do I instantiate an L3 DCI service?” (p. 80).

7.3.3 L2 DCI services

L2 DCI is a single subnet, layer 2, ethernet only service realized with BGP-EVPN exchanging Type 1 and Type 2 EVPN routes. EVPN service configuration is provisioned on Access Leaf nodes by NSP. The L2 DCI is auto-generated on NSP as a reaction to the instantiation an L2 Domain within Nuage VSD, with a transport type of MPLS. NSP auto-generates the Route Target (RT), Route Distinguisher (RD), and Ethernet VLAN Identifier (EVI) service parameters. Upon reception of Virtual Ports corresponding to a VNF from VSD, NSP provisions the access interface and Service Site configuration on the respective Access Leaf nodes.

Figure 7-3 L2 DCI service topology



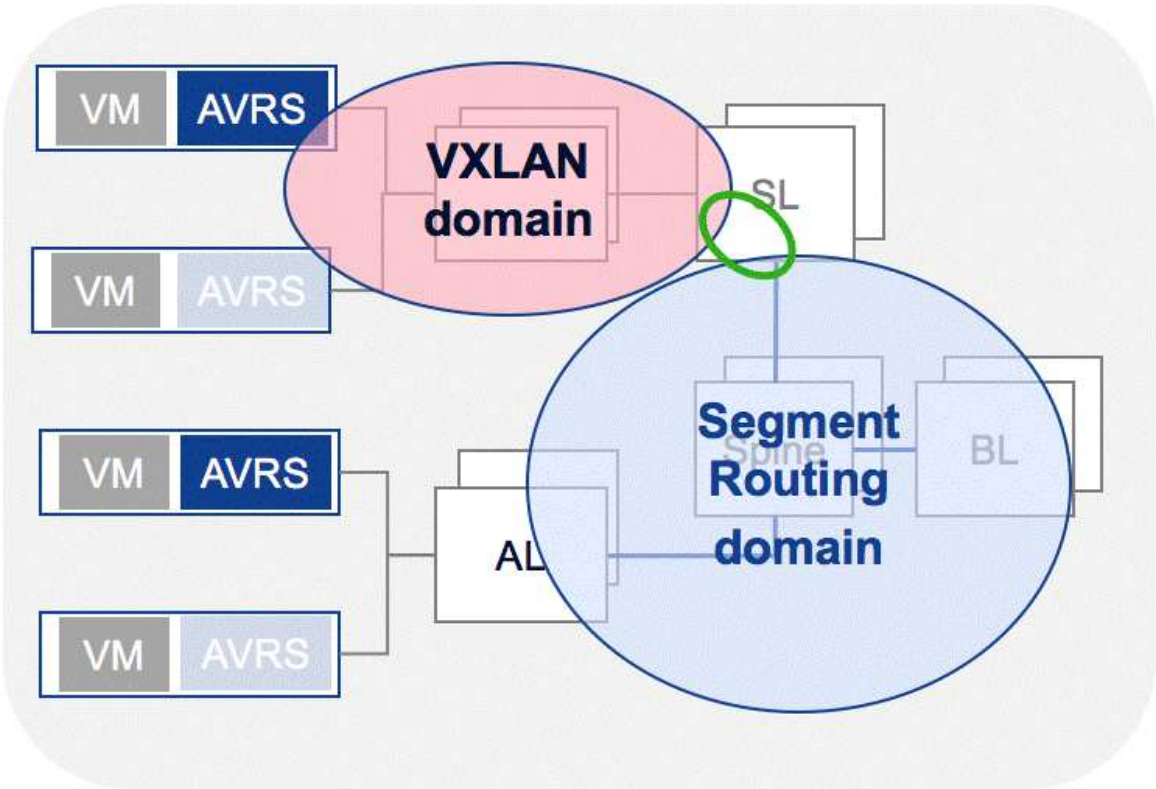
See 7.11 “How do I instantiate an L2 DCI service?” (p. 81).

7.4 Deployment assumptions

7.4.1 General information

The Nuage-managed data center network fabric is assumed to be IP/Ethernet running an IGP protocol such as ISIS or OSPF with Segment Routing extensions in a leaf spine architecture. Portions of the topology support SR MPLS, while another portion may only support native IP. A BGP-supporting EVPN address family is required for route exchange. It is assumed that BGP has been configured on the network elements with appropriate route reflector configuration, so as to permit the exchange of EVPN routes within the VXLAN and SR MPLS domains. IGP Topology must be exported to NSP (for information about importing IGP topology into NSP via BGP-LS, see the *NSP Deployment and Upgrade Guide*). It is assumed that the IGP topology represents a single administrative domain for the data center. VXLAN and Segment Routing subsections of the topology must be contiguous. The Access Leaf within the Segment Routing domain and the Service Leaf that will provide stitching must be under NSP management. For virtual ports of type “Virtual Machine” on a VRS, NSP requires the VRS to be attached into the NSP IGP topology. This can be achieved by describing the uplink Access Leaf node via metadata on VSD for the VRS. For Nuage and Openstack requirements or assumptions, see the Nuage documentation suite.

Figure 7-4 High-level view of NF-IX topology fabric



7.5 Communication

7.5.1 General information

NSP communicates with the following components:

- VSR-NRC – for IGP Topology Discovery
- NFM-P – for SNMP mediation
- VSD – For Datacenter entity integration

For more information about IP resource control server communication with VSR-NRC, see the *NSP Deployment and Upgrade Guide*. For more information about NFM-P communication for SNMP mediation, see the *NFM-P User Guide*.

NSP communicates to the VSD via its HTTPS REST API interface to fetch data during synchronization and to push data during instantiation. NSP connects to the VSD JMS event publishing system to receive notifications from VSD over SSL.

For VSD communication to the network element, see the *Nuage VSP User Guide*.

7.6 Infrastructure provisioning

7.6.1 General information

Note: For complete VSD configuration instructions, see the *Nuage VNS User Guide*.

For NSP to provide NF-IX based services, Gateways, and VRS uplink, metadata must be configured within VSD. The gateways define network elements inside of the datacenter which provide VM connectivity into the fabric.

Gateways defined within VSD may be configured as being “Managed” by VSD or as “Unmanaged”. VSDs defined as unmanaged in VSD are expected to be managed by an external entity such as NSP. NSP will discover gateways from VSD and decide whether NSP should identify the gateway management as “PASSIVE” (gateways managed by VSD) or “ACTIVE” (gateways not managed by VSD). When Virtual Ports are attached to gateways not managed by VSD, NSP will attempt to provision the network element if that network element is under its own mediation management.

Any device for which NSP is responsible must be configured with a Personality type of “Unmanaged” in VSD.

VRS entities are connected to Access Leaf ports on Access Leaf entities. For NSP to perform automatic service stitch provisioning on Service Leafs, NSP must model the connectivity of the VRS into its IP Topology Database. To achieve this, metadata must be created on the VRS inside of VSD to describe its uplink connected entity. NSP will discover this metadata and inject a link with a protocol type of “static”, representing the connection into its topology database. The key for the metadata is by default “sric_uplink_routerid” and the value of the metadata should be set to the router ID of the Access Leaf entity.

NSP contains L2 and L3 DCI service templates in the NSP Policy Management application.

The L3 DCI templates can be used during L3 DCI service creation to customize default service parameters such as autobind, mtu, and more. This includes templated descriptions and names.

RT/RD generation policy can be configured and customized. Many templates can be defined, but an L3 DCI may only refer to one template.

The L2 DCI template is used during L2 DCI service auto-generation. Only one template exists on the system and is pre-populated with default values. While these values can be edited, no new templates can be defined. The L2 DCI service template can be used to customize parameters such as autobind, mtu and more - including template descriptions and names.

7.7 How do I configure NSP to communicate with VSD?

7.7.1 Before you begin

The SRIC installer does not currently support any configuration for communicating with VSD. NSP contains a plug-in which performs all of the adaptation and communication with VSD. This plug-in supports multiple, varied, concurrent VSD instances with which NSP may communicate. This communication is accomplished via REST API with SSL and JMS with SSl. The *Nuage VNS User Guide* describes VSD REST authentication and the JMS configuration required to generate and use certificates.

NSP supports both certificate-based authentication and token-based authentication with VSD. Certificate-based authentication is recommended.

SRIC configuration is performed through the nuage.conf configuration file, located in the /opt/nsp/configure/config/ directory. This file must be created following installation. When using certificate-based authentication, the certificates must be generated in VSD and copied to the NSP system in the opt/nsp/os/ssl/certs/vsd/ directory. See the *Nuage VNS User Guide* for more information.

NSP expects the naming of the certificate file to match the name of the VSD configured in the nuage.conf file. See 7.8 “nuage.conf configuration file” (p. 76) for more information about creating and populating the nuage.conf file.

7.7.2 Steps

1

Edit the nuage.conf nuage.vsds.rest.user field to reflect the same user that made the certificate. nuage.vsds.rest.password can now be omitted.

2

As nsp user, create the nuage.conf file in the /opt/nsp/configure/config directory on your NSP system.

3

Edit /opt/nsp/server/tomcat/conf/system.conf file, adding a new “include” entry for /opt/nsp/configure/config/nuage.conf.

4

Generate the REST API certificate on VSD for a valid user that has access to root/enterprise information as intended following the *Nuage VNS User Guide*. There will be two certificate files.

5

As the nsp user, create the /opt/nsp/os/ssl/certs/vsd/ directory on the NSP system.

6

Copy the certificate to your NSP system, renaming it to match the nuage.vsds.name defined in your nuage.conf file (such as vsd1.pem, vsd1-key.pem). Ensure “-key” is lowercase.

7

Copy the certificate file to the NSP system in the directory specified by the “nuage.vsds.cert_ directory” field of the nuage.conf file (the default is /opt/nsp/os/ssl/certs/vsd/).

8

Create a user in VSD for JMS usage and assign to Root group. See the *Nuage VNS User Guide* for more information about creating a JMS user with SSL.

9

Copy the VSD .truststore file from VSD to NSP in /opt/ns/os/ssl/certrs/vsd/ and rename the file to <nuage.vsds.name>.truststore.

10

Edit nuage.conf nuage.vsds.jms.user to reflect the name of the user created in Step 8.

11

Edit the cert_truststore_password to reflect the password of the truststore. The password set on a default VSD installation is 'Alcateldc'.

END OF STEPS

7.8 nuage.conf configuration file

7.8.1 Sample nuage.conf file contents

```
nuage {
   enabled = true
   dcs = [
     {
       id = 1
       name = "myDc1"
     }
   ]
   vsds = [
```

```
        {
          name = "vsd1"
          dc_id = 1
          domain_pseudo_node_router_id = "255.255.255.251"
          rest {
            host = "138.120.150.159"
            user = "csproot"
            organization = "csp"
          }
          jms {
            password = "csproot"
            cert_truststore_password = "Alcateldc"
          }
        }
      ]
}
```

7.9 How do I create a DCI service?

Note: This procedure requires the use of multiple NSP applications, as well as Nokia's Nuage platform. For complete configuration details, you may need to consult the following documents:

- *NSP Policy Management Application Help*
- *NSP Original Service Fulfillment Application Help*
- Nuage documentation suite

7.9.1 Steps

1

From the Nuage infrastructure page, create a Data Center Gateway Template, ensuring Personality is set to “Unmanaged Gateway”.

2

Create a Data Center Gateway instance, ensuring System ID is set to the IP address of an Access Leaf that is visible on the IP/MPLS Optimization application's network map.

3

If no ports were added to the Data Center Gateway Template in Step 1, create a port to add to the new Data Center Gateway instance, specifying the Access Leaf port(s) that are connected.

4

Create one or more VLANs permitted for use on the new port.

Note: In a production environment, it is anticipated that this VLAN range is to be managed by VSD and Openstack via Nuage VSD Openstack plug-ins.

5

Create permissions for the Data Center Gateway, ensuring Permitted Action is set to “Use or Extend” for the desired enterprise.

6

VRS devices managed in VSD will be visible from the IP/MPLS Optimization application, however, they will be disconnected from the topology. In Nuage VSD, select the monitoring console and navigate to the desired VRS. Select the metadata section and click Add to create new metadata, ensuring:

- Name Field is configured as “sric_uplink_routerid”
- Metadata field is configured with the router ID that corresponds to the value visible in the IP/MPLS Optimization application

Note: Step 1 to Step 5 are considered an infrastructure setup to define the gateways in the network and may be used across multiple services.

7

Perform one of the following:

a. If creating an L2 service, continue to Step 8.

b. If creating an L3 service, go to step Step 10.

8

Using the Policy Management application, edit the default L2 DCI service template to configure desired service attributes.

9

From the Nuage Networks page, create an L2 domain instance, ensuring that Tunnel Type is set to “MPLS”.

Note: The L2 domain is created automatically when an outside system creates a subnet.

Note: When the L2 domain instance is created, the Original Service Fulfillment application creates an L2 DCI service, using the L2 DCI template to auto-populate the service parameters.

Go to step Step 13.

10

Using the Policy Management application, create or edit the default L3 DCI service template so as to contain the desired service attributes. Ensure that the DCI Connectivity is set to “VXLAN Stitched”.

11

Using the Original Service Fulfillment application, create an L3 DCI service, ensuring that:

- DCI Connectivity is set to “VXLAN Stitched”
- an enterprise belonging to a VSD instance is selected as the endpoint
- that endpoint is configured to include an L3 domain template
- optionally, add one or more PNF endpoints

Note: The enterprise and L3 domain template must be created using Nuage.

Note: When the L3 DCI service is deployed, an L3 domain instance is deployed to Nuage, and the IP/MPLS Optimization application creates the L3 DCI service.

Note: Any PNF endpoints must be configured with access-facing information, such as IPv4 addressing and BGP information. When deployed, NSP will deploy the PNF configurations that allow the endpoint to bind and exchange routes with any dynamic access leaf configuration deployment.

12

In Nuage VSD, in the domain created in Step 11, create one or more subnets with a transport type of “MPLS” or “VXLAN”. Subnets created with a transport type of “MPLS” should be used by virtual ports that are attached to network elements in the MPLS domain, while subnets created with a transport type of “VXLAN” should be used by virtual ports that are attached to network elements in the VXLAN domain.

13

From the Nuage VSD page, select the L2 domain instance created in Step 9, or the L3 domain instance created in Step 11, and create a VPort attached to a network element under NSP management, ensuring the following:

- Type is set to “Bridge” for entities connected to devices managed by NSP
- Gateway type is set to “Unmanaged gateway”
- Gateway is set to the instance created in Step 2
- Port is set to the port created in Step 3
- VLAN is set to the VLAN created in Step 4

Note: When the VPort is created, the Original Service Fulfillment application attaches the new VPort, which will serve as an endpoint with a port type of “Virtual Port”. Upon

instantiation, NSP will automatically provision the associated Access Leaf and a new port will appear within the L2 DCI or L3 DCI service in the Original Service Fulfillment application.

END OF STEPS

7.10 How do I instantiate an L3 DCI service?

7.10.1 Before you begin

The layer 3 service may contain one or more subnets distributed between one or more compute nodes. Each subnet may be of type “VXLAN” or “MPLS” and VMs must spawn on compute nodes which support the intended transport type on the uplink Access Leaf.

Note: The following is a high-level workflow.

7.10.2 Steps

1

L3 DCI service is instantiated on NSP via API or UI with a VSD and template as endpoint input criteria.

2

NSP Instantiates L3 Domain on VSD with the defined template from Step 1.

3

An orchestrator or user spawns one or more virtual machines in one or more subnets on Openstack, containing metadata which attaches the virtual machine to the domain in a subnet.

The subnet is defined with either “MPLS” or “VXLAN” transport tunnel type.

4

Nuage Openstack Plugin integration binds the virtual machine to the L3 Domain on VSD in the form of a bridge port or virtual machine.

NSP automatically discovers of the bridge port and virtual machine from VSD.

Note: For subnets with “VXLAN” transport, VSD automatically provisions the respective Access Leaf. For subnets with “MPLS” transport, NSP automatically provisions the respective Access Leaf. If there are both “MPLS” and “VXLAN” subnets, NSP automatically computes and determines the necessary Service Leaf and provisions with configuration to provide encapsulation stitching.

5

NSP cleans unnecessary service configurations that are no longer required when virtual machines are deleted.

End of steps

7.11 How do I instantiate an L2 DCI service?

7.11.1 Before you begin

The layer 2 service may contain one subnet distributed between one or more compute nodes. To instantiate a L2 DCI service, the subnet must be of type “MPLS”. VMs must spawn on computes which support “MPLS” transport type on the uplink Access Leaf.

Note: The following is a high-level workflow.

7.11.2 Steps

1

An orchestrator or user spawns an L2 domain within VSD with transport type MPLS.

2

NSP discovers the L2 Domain with a transport type of “MPLS” and automatically creates an L2 DCI service definition based on the attributes from VSD and a L2 DCI template defined in NSP.

3

An orchestrator or user spawns one or more virtual machines in the subnet on Openstack containing metadata which attaches the virtual machine to the L2 Domain.

4

Nuage Openstack Plugin integration binds the virtual machine to the L3 Domain on VSD in the form of a bridge port or virtual machine.

5

NSP automatically discovers of the bridge port and virtual machine from VSD and provisions the respective Access Leaf.

6

NSP cleans unnecessary service configurations which are no longer required when virtual machines are deleted.

End of steps