NOKIA

NSP
Network Services Platform

Release 20.11

User Guide

3HE-16045-AAAC-TQZZA

Issue 1

November 2020

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.

Nokia is a registered trademark of Nokia Corporation. Other products and company names mentioned herein may be trademarks or tradenames of their respective owners.

The information presented is subject to change without notice. No responsibility is assumed for inaccuracies contained herein.

© 2020 Nokia.

Contents

About this document **5**

1 Product description **7**
1.1 System components **7**
1.2 User perspectives **9**
1.3 Interfaces **10**
1.4 Deployment flexibility **11**
1.5 NSP support for wireless networks **12**

2 Concepts **15**
2.1 MDM **15**
2.2 Adaptors **17**
2.3 Services **18**

3 Features **23**
3.1 Value proposition **23**
3.2 NSP licensing schema **26**
3.3 Locating NSP feature information **31**

4 Software **33**
4.1 Packaging **33**
4.2 Delivery **33**
4.3 Deployment mechanisms **34**

5 Documentation **35**
5.1 Documentation architecture **35**
5.2 NSP Help Center **36**
5.3 Documentation delivery online **39**

6 Troubleshooting **41**
6.1 Troubleshooting services and connectivity **41**
6.2 Process for troubleshooting a service or connectivity problem **41**

7 Network Functions Interconnect **43**
7.1 Why use Network Functions Interconnect (NF-IX)? **43**
7.2 Segment Routing Interconnect Controller **44**
7.3 SRIC service types **46**
7.4 Deployment assumptions **48**
7.5 Communication **50**

7.6 Infrastructure provisioning 50
7.7 How do I configure NSP to communicate with VSD? 51
7.8 nuage.conf configuration file 52
7.9 How do I create a DCI service? 53
7.10 How do I instantiate an L3 DCI service? 56
7.11 How do I instantiate an L2 DCI service? 57

About this document

Purpose

This document provides an introduction to the Network Services Platform (NSP).

Intended audience

This document is intended for all audiences.

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 • 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, common to NSP	The following applications are common to all NSP deployments: • Fault Management • Group Manager • Network Supervision • Service Supervision • Telemetry Monitor • User Manager

Table 1-1 NSP system component overview (continued)

Component	Description
Additional web-based applications	The following applications can be installed with NSP, depending on deployment type: • Analytics • Cross Domain Coordinator • Device Administrator • Insights Administrator • IP/MPLS Optimization • IP/MPLS Simulation • Intent Manager • Inventory Manager • Modeled Device Configurator • Policy Management • Service Navigator • Service Fulfillment • Subscriber Manager • Telemetry Viewer • Traffic Steering Controller • Wireless NE Views • Wireless Supervision • Workflow Manager
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 standalone network management system that can also function 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. 11).
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*.

Table 1-1 NSP system component overview (continued)

Component	Description
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	Depending on the deployment, the NSP can store information in the NFM-P database, auxiliary databases, or in cloud-based data stores. See the *NSP Deployment and Installation Guide* for more information.

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 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 Inventory Management Modeled Device Configurator
Network designers	A network designer is involved in network planning work, including IP/optical network connectivity, routing management, and network optimization.	Device Administrator Inventory Management IP/MPLS Optimization Policy Management Modeled Device Configurator Subscriber Manager Wireless NE Views Workflow Manager

Table 1-2 NSP user perspectives (continued)

User perspective	Description	NSP applications used
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 Service Navigator 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 Service Supervision Telemetry Monitor Traffic Steering Controller Telemetry 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 Policy Management Service Fulfillment Service Supervision Wireless Supervision

1.3 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, and the NSP Help Center.

1.3.2 Web applications

NSP web applications are browser-based interfaces into NSP functional areas. The following web applications are common to all NSP deployments:

- Fault Management
- Network Supervision
- Service Supervision
- Telemetry Monitor
- Group Manager
- User Manager

Additional applications are available, depending on licensing and feature packages; see 3.2 “NSP licensing schema” (p. 26).

1.3.3 Client-based applications

The NFM-P GUI client provides an extensive IP/MPLS network management interface; see the *NSP NFM-P User Guide* for information.

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 6.2 “Process for troubleshooting a service or connectivity problem” (p. 41).

1.3.4 APIs

For OSS users, NSP functions are available using the REST and RESTCONF APIs. The NSP APIs are documented on the Nokia 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 Deployment and Installation Guide* for specific system deployment information.

1.4.3 Flexibility

NSP software is licensed and delivered in the form of feature packages. These feature packages provide the ability to fully customize an NSP deployment according to your network type and management requirements.

See 3.2 “NSP licensing schema” (p. 26) for specific information about NSP feature packages. See 4.2 “Delivery” (p. 33) for specific 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 inclusion of multiple feature packages, and may require the inclusion of various NSP components and separate products.

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

1.5 NSP support for wireless networks

1.5.1 NSP for wireless

The NSP consists of a set of powerful tools designed to support the deployment, configuration and management of wireless networks that support 4G and 5G equipment, technologies, and functions.

In a wireless deployment based on NSP components, you can manage network complexity consistently and perform the following sets of tasks:

- Manage the network with an integrated set of result-oriented applications. As a result, you will have a plug-and-play domain management system that supports the continuous evolution of your networks.
- Automate network operations with programmable frameworks. To achieve this, the NSP provides an open, model-driven, and programmable set of APIs that you can integrate into your own or a third-party end-to-end OSS and orchestration systems.
- Perform path/flow control and closed-loop optimization for IP/MPLS and optical networks. Backed by the NSP expert set of tools, your network engineering teams gain the ability to control and optimize network traffic in real time.

1.5.2 NSP for private wireless

The 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. 12) 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.

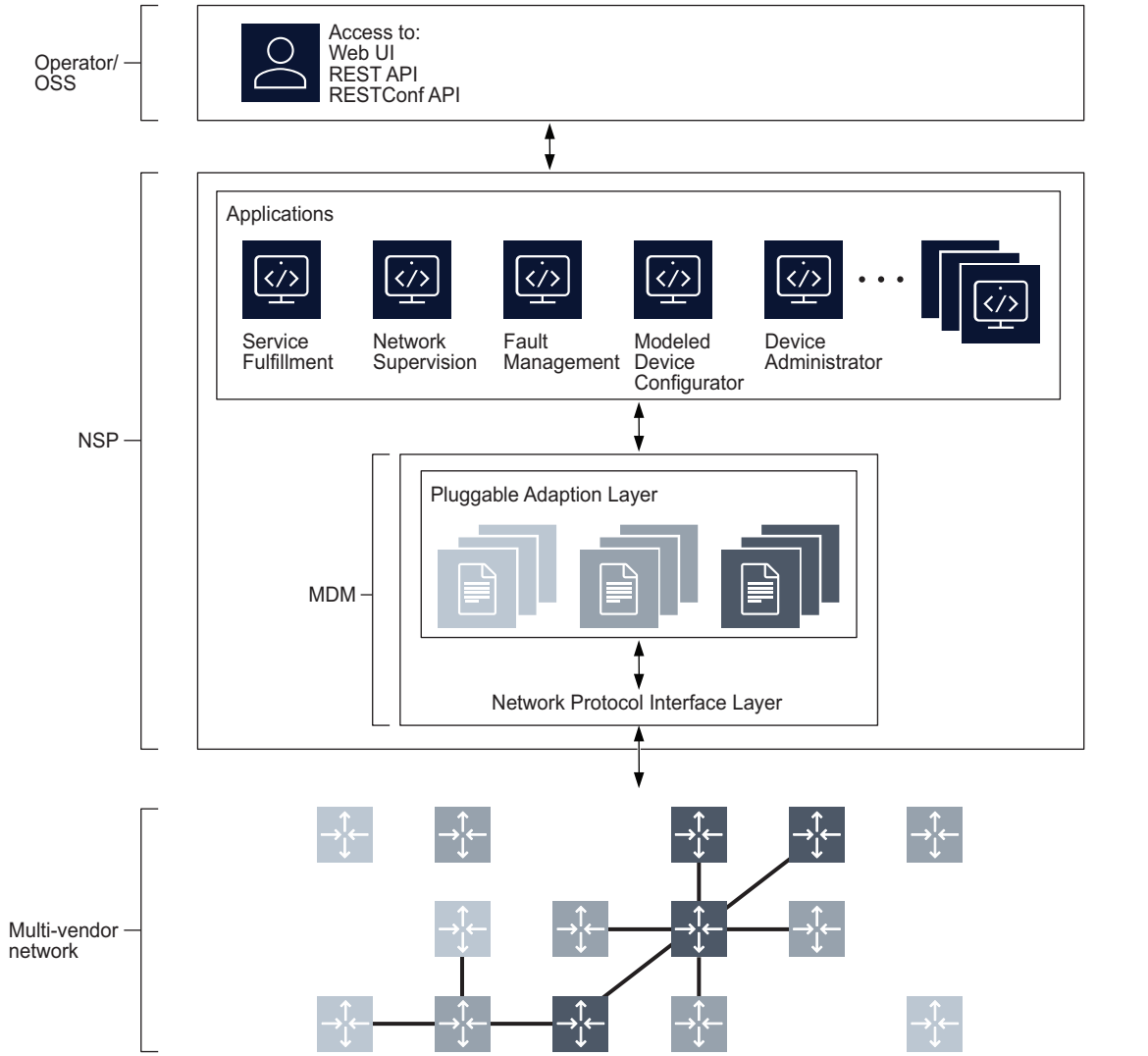
An MDM server is installed as part of the NSP deployment. Within the MDM server, network protocol inputs from devices are adapted to create inputs to applications, and vice versa. Adaptation is performed by MDM adaptor files. Adaptors are installed on the MDM server according to network requirements. SR OS adaptors and customer adaptor suites requested by customers 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:

- Pluggable Network Adaptation
- Pluggable Network Adaptation Toolkit
- Multi-layer Discover and Visualization
- Multi-layer Control Coordination

MDM is provided notably for model-driven SR OS 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, 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 SR OS adaptors

Adaptors for 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 Nokia 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.

2.3 Services

2.3.1 Services overview

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

- Service Fulfillment
- Policy Management
- Service Supervision

Service Fulfillment application

The 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 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 the NSD 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.

Service Fulfillment and NFM-P dependencies

- Services created in the NFM-P can be managed by the Service Fulfillment application if the service's NSD Managed parameter is enabled in the NFM-P.
- The 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 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 Service Fulfillment application. 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 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

Table 2-2 Device VLAN support (continued)

Device	Supported VLAN types
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 7710 SR, 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.

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.

Service Fulfillment application

The 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.

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.

Service Fulfillment application

The 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 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
- Telemetry Viewer utility

  presents historical and real-time telemetry data as graphs

  Note: the Telemetry Viewer utility is accessed from other applications; it is not available directly from the launchpad
- Analytics, NSP-level reports

  present historical data stored in an auxiliary database as tables, charts, or graphs
- Baseline Analytics

  provides advanced analytics: baselines and anomaly detection

  Note: Baseline Analytics configuration is performed from the Insights Administrator application, and baseline and anomaly graphs are presented in the Telemetry Viewer utility.

The NSP also includes the Telemetry Monitor application, which uses gRPC telemetry data to provide near-real-time NE KPIs.

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.

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 IXR Microwave Awareness (MWA)

In networks with IXR Microwave Awareness, Wavence UBT-SA devices have physical links to a 7250 IXR NE, which provides a management path for the UBT-SAs. The 7250 IXR and linked UBTs are treated as a single logical site in NSP.

Physical links between the IXR and UBT-SAs may be created manually, or by using a Nokia-provided workflow in the Workflow Manager application. When the NSP detects these physical links, it automatically makes internal system adjustments to the display of the linked 7250 IXR and UBT-SA devices in the Network Supervision application; see the Network Supervision Application Help for more information.

Additionally, Nokia 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. Contact your Nokia representative for more information about Nokia-provided workflows.

3.2 NSP licensing schema

3.2.1 What are software suites and feature packages?

Software suites are conceptual groupings of feature packages. They represent the functional pillars of the product, but they are not themselves specifically licensed or packaged. Each software suite includes a base package, the essential platform and administration aspects of NSP, and a number of feature packages.

The software suite and associated feature package model is an evolution of the former module (NSD, NRC, NFM-P) schema that used classic and premium licenses to enable use of product components. This new NSP product licensing schema has been designed to align more closely with how customers use different aspects of NSP. Existing customers have been migrated to this schema, and can add feature packages to brownfield deployments.

There are no cross-dependencies between software suites, although there are some dependencies between feature packages within some software suites.

Beginning in NSP 20.9, some NSP components and applications are supported in container environments only, while others must continue to be installed via traditional RPM files and run outside the container environment that hosts the rest of the NSP components. During container-based NSP installation, you enable the feature packages you are entitled to install in the nsp-config.yml file.

3.2.2 Network Programming software suite

The Network Programming software suite consists of feature packages aimed at developers and network architects. The feature packages in this suite leverage NSP's programmable platform, enabling automation of network operations through open, model-driven APIs that can integrate with any-vendor nodes, OSS, and orchestrators.

The following table lists and describes the feature packages available in this suite, along with the components/applications enabled through the associated license.

Table 3-1 NSP Network Programming feature packages

Feature package	Description	Software components installed	Applications enabled [1]
Base packages			
Platform	Provides essential NSP platform and administrative functions, including centralized logging. Mandatory for the deployment of any other package in a single NSP deployment	nspOS	NSP Launchpad Group Manager Insights Administrator Telemetry Monitor Telemetry Viewer User Manager
	Logging and Monitoring With the purchase of the base Platform feature package, customers can optionally enable the Logging and Monitoring feature package. This package is required by the Intent Based Networking Framework feature package. There are additional hardware requirements when this package is enabled.	efk grafana	—
High Availability	Provides high availability and disaster recovery	—	High availability
Feature packages			
Pluggable Network Adaptation Toolkit	Allows developers to manage the lifecycle of pluggable devices and application adaptors	mdm fs spark gluster act	Adaptor builder (SDK) [2] MDM Device Administrator Modeled Device Configurator
Intent Based Networking Framework	Allows developers to manage the lifecycle of network and service intents	mdt	Intent Manager
Workflow Automation Engine	Allows developers and administrators to manage the lifecycle of workflows	wfm	Workflow Manager

Notes:

1. Application availability also depends on the deployment type: some applications are tied to NSP components that must be deployed using traditional RPM files, whereas others are specific to components deployed in containers.
2. Available on the Nokia Network Developer Portal.

3.2.3 Network Operations software suite

The Network Operations software suite consists of feature packages that enable operators to manage their networks through classic SNMP and/or model-driven mediation. This suite includes feature packages that license operators to use configuration, supervision and assurance applications, as well as telemetry and analytics reporting.

The following table lists and describes the feature packages available in this suite, along with the components/applications enabled through the associated license.

Table 3-2 NSP Network Operations feature packages

Feature package	Description	Software components installed	Applications enabled [1]
Base packages			
Platform	Provides essential NSP platform and administrative functions, including centralized logging. Mandatory for the deployment of any other package in a single NSP deployment	nspOS	NSP Launchpad Group Manager Insights Administrator Telemetry Monitor Telemetry Viewer User Manager
	Logging and Monitoring With the purchase of the base Platform feature package, customers can optionally enable the Logging and Monitoring feature package. This package is required by the Intent Based Networking Framework feature package. There are additional hardware requirements when this package is enabled.	efk grafana	—
High Availability	Provides high availability and disaster recovery	—	High availability
Feature packages			
Classic Management	Provides traditional IP management capabilities for classic mode NEs Provides network discovery and adaptation for SR OS NEs using classic mode (SNMP) Includes legacy control plane management (CPAM)	NFM-P CPAM	NFM-P CPAM Inventory Management Service Navigator
Pluggable Network Adaptation	Provides SR OS MD mode and third-party device mediation Supports NE forward compatibility using application adaptors Includes programmable telemetry framework	mdm fs spark gluster act	MDM Device Administrator Modeled Device Configurator
Network Infrastructure Management	Includes network infrastructure deployment, network monitoring, IP management configuration, fault management, NGE management, troubleshooting, and IP/optical alarm correlation When combined with Pluggable Network Adaptation, provides equipment configuration and consolidated views of network objects regardless of the mediation protocol or vendor	oam	Network Supervision Fault Management Wireless NE Views Wireless Supervision
Service Activation and Configuration	Provides service fulfillment and augmentation Allows for the execution of Nokia-provided workflows and network and service provisioning intents	sdn	Service Fulfillment Policy Management Workflows and intents from Nokia Professional Services

Table 3-2 NSP Network Operations feature packages (continued)

Feature package	Description	Software components installed	Applications enabled [1]
Service Assurance	Provides service monitoring and subscriber management	sdn oam	Service Supervision Subscriber Management
Network Operations Analytics	Provides network health analysis with trending, forecasting, reporting and dashboards. Provides real-time baselining and anomaly detection	spark gluster rta	Analytics Baseline Analytics

Notes:

1. Application availability also depends on the deployment type: some applications are tied to NSP components that must be deployed using traditional RPM files, whereas others are specific to components deployed in containers.

3.2.4 Resource Control software suite

The Resource Control software suite consists of feature packages that license operators to use path control, visualization and optimization applications, as well as to perform cross-domain (IP/optical) multi-layer discovery, visualization, and coordination.

The following table lists and describes the feature packages available in this suite, along with the components/applications enabled through the associated license.

Table 3-3 NSP Resource Control feature packages

Feature package	Description	Software components installed	Applications enabled [1]
Base packages			
Platform plus High Availability	Provides essential NSP platform and administrative functions, including centralized logging. Mandatory for the deployment of any other package in a single NSP deployment	nspOS	High availability NSP Launchpad Group Manager Insights Administrator Telemetry Monitor Telemetry Viewer User Manager
	Logging and Monitoring With the purchase of the base Platform feature package, customers can optionally enable the Logging and Monitoring feature package. This package is required by the Intent Based Networking Framework feature package. There are additional hardware requirements when this package is enabled.	efk grafana	—
Feature packages			

Table 3-3 NSP Resource Control feature packages (continued)

Feature package	Description	Software components installed	Applications enabled [1]
Control and Visualization Starter	Provides for visualization of the IGP topology Provides visualization and configuration of traditional MPLS control plane and brownfield LSPs	sdn	IP/MPLS Optimization Traffic Steering Controller
Path Control and Optimization	Enables a stateful or stateless PCE to provide paths based on path profile to the requesting LSPs via PCEP/BGP Provides the ability to invoke maintenance operational practices	sdn	—
Enhanced Optimization	Provides dynamic optimization based on real-time network metrics	sdn fs mdm spark gluster act oam	—
Simulation	Provides offline simulation of operational assurance changes to assist in capacity planning	nrcpsim	IP/MPLS Simulation
Multi-layer Discovery and Visualization	Provides IP/optical topology discovery, path diversity verification, and both bottom-up and top-down navigation	nrcx fs mdm	Cross Domain Coordinator
Multi-layer Control Coordination	Supports single-step LLI establishment, maintenance coordination, cross-domain connection management, and floating port restoration	nrcx fs mdm	—

Notes:

1. Application availability also depends on the deployment type: some applications are tied to NSP components that must be deployed using traditional RPM files, whereas others are specific to components deployed in containers.

3.2.5 What are automation packages?

NSP automation packages provide end-to-end automation solutions for greenfield deployments. Automation packages are designed to deliver particular outcomes, and are sold based on a use case catalog.

3.3 Locating NSP feature information

3.3.1 NSP Release Description

The *NSP Release Description* summarizes all non-NFM-P features (such as platform, security, MDM, and common application features) delivered in each release. Some but not all of the content is applicable to NFM-P-only customers.

This document is new in NSP 20.6.

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

3.3.2 NFM-P Release Description

The *NSP NFM-P Release Description* summarizes the non-wireless NFM-P features delivered in each release

This document is cumulative for a major release cycle, such as NSP 19.3 through 19.11, and then resets with the next release, such as NSP 20.3.

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

3.3.3 NFM-P Wireless Release Description

The *NSP NFM-P Wireless Release Description* specifies the wireless NFM-P features delivered in each release

This document is cumulative for a major release cycle, such as NSP 19.3 through 19.11, and then resets with the next release, such as NSP 20.3.

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

4 Software

4.1 Packaging

4.1.1 Software bundle

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

For a traditional deployment, an NSP software bundle consists of a set of RPM installation files; a software bundle for a containerized deployment consists of a set of Docker images and Helm charts. 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 perspective; a feature package licenses a set of features that are not delivered as discrete software packages. After you download, extract and install a software bundle, the purchased feature packages 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 Nokia 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 Nokia 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 Deployment and Installation 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 Deployment and Installation Guide*
- *NSP Containerized Lab Installer Reference**
- *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.

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. Global searches conducted from the home page 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.
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 Troubleshooting

6.1 Troubleshooting services and connectivity

6.1.1 Cross-application troubleshooting

This topic covers troubleshooting at the product level, across NSP applications. See the help for each application for additional troubleshooting procedures that can be completed within an application.

NSP applications provide information about NE, network and service health.

6.2 Process for troubleshooting a service or connectivity problem

6.2.1 Before you begin

This process provides a series of tasks you can perform to identify the root cause of a problem.

See the *NSP System Administrator Guide* for information about other NSP troubleshooting actions such as displaying the system status or checking system performance.

6.2.2 Steps

Service Supervision application

1

Verify whether the administrative and operational states of each component of the service are Up:

- Sites
- Endpoints
- Tunnel Bindings

See the procedure to investigate a service in the Service Supervision help.

2

Check the Alarm List for alarms against the services in your network.

3

Check the Event Timeline to view the history of events related to alarms, configuration, OAM test failures and state change notifications.

Fault management application

4

Verify that there are no alarms associated with any component of the service:

- The Alarm List view provides high-level visibility of all alarms in the network.
- Choose the Current Alarms format to see the alarm information in a list you can filter. Select an alarm to view detailed information in an information panel.

5

From the Alarm List, check the Historical Alarms and Merged Alarms lists for further information about root causes of any current alarms.

Service Fulfillment application and/or NFM-P

6

Verify that the NFM-P service configuration aligns with the customer requirements. For example, ensure that NFM-P configuration uses the correct service type and SAP configuration, and that the circuit and site are included in the service.

7

Contact your technical support representative if the problem persists.

END OF STEPS

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 Segment Routing Interconnect Controller

7.2.1 SRIC overview

NF-IX introduces 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.

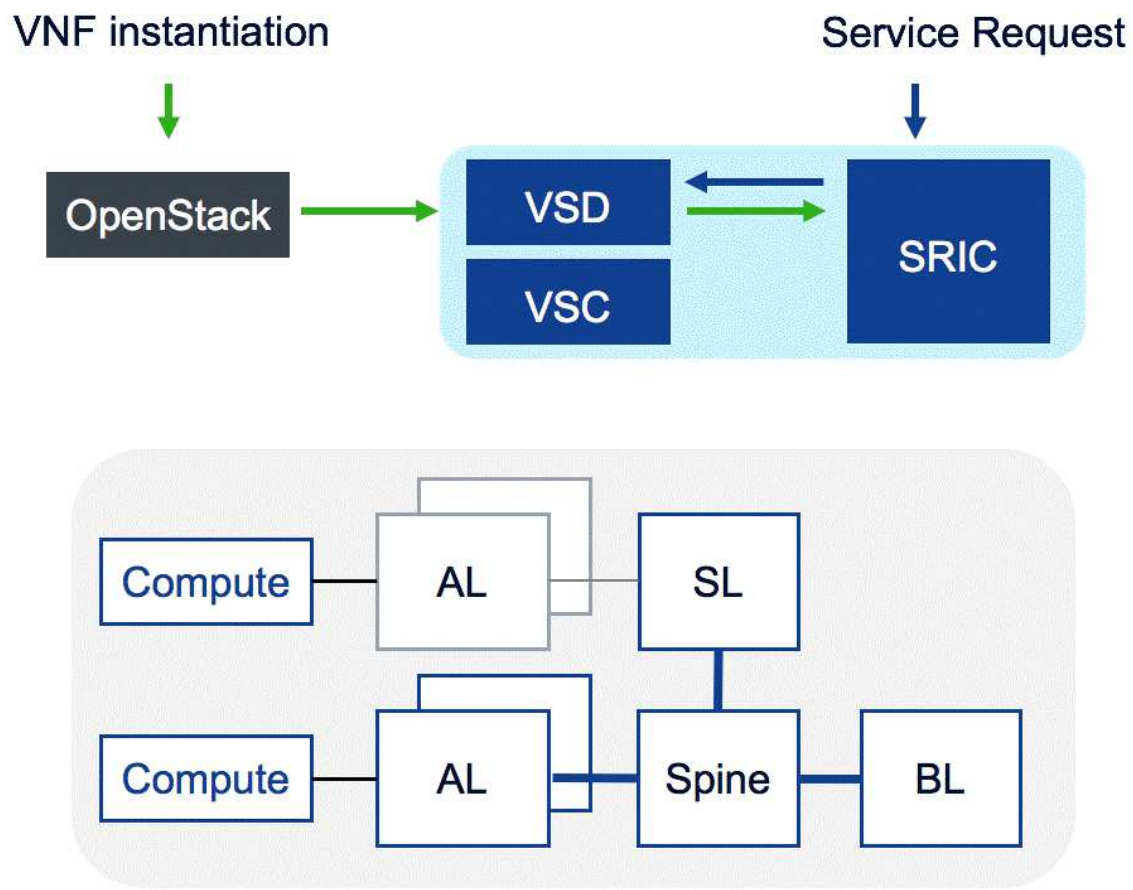
NF-IX and the SRIC remain in development and the current implementation does not represent the intended, complete functionality described in IETF document *draft-bookham-rtgwg-nfix-arch*. The functionality described below is an initial feature set which provides automated inter-connectivity provisioning 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 (Service Leaf), providing VXLAN and SR interworking

The SRIC is used to automatically provision network elements with the role of Access Leaf and Service 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. Service Leaf network elements support VXLAN and Segment Routing, providing the capability to perform transport stitching between VXLAN and SR transport for a given service. They are managed and provisioned by SRIC. SRIC 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 the SRIC, 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 SRIC and VSD. In SRIC, a service is instantiated as either an L2 DCI or L3 DCI service type. For L3 services, the service construct definition originates on SRIC and SRIC instantiates an L3 Domain on VSD. For L2 services, the construct originates on VSD and is discovered by SRIC. 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. SRIC 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, SRIC 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 SRIC service types

7.3.1 SRIC service types overview

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

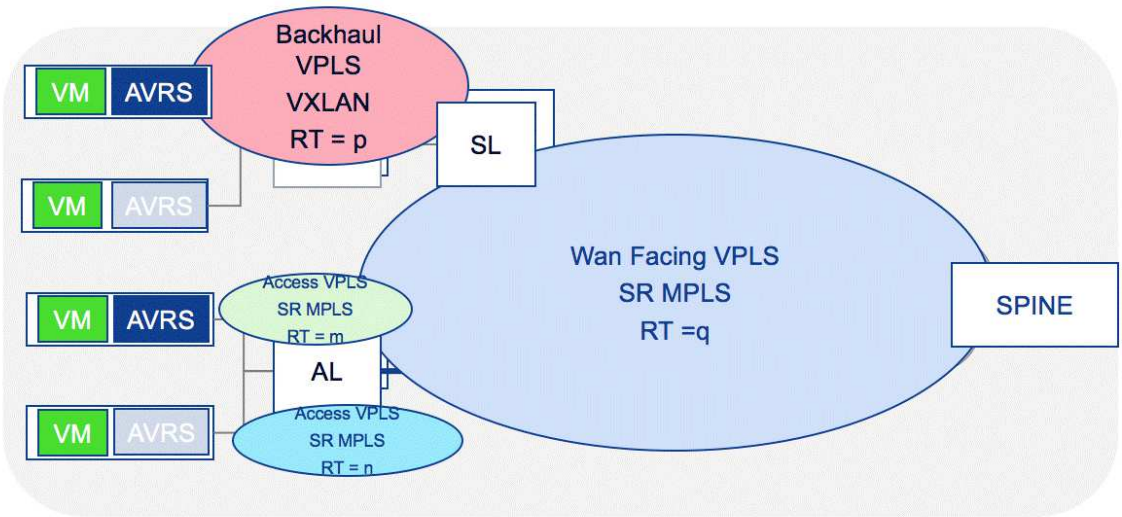
- An abstract container for the composite service requirements in various deployment types
- A binding for DC related entities, its abstractions, and network element device configurations
- A binding to invoke automatic service and tunnel differential algorithms

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 SRIC 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 SRIC. Other connectivity types are proof-of-concept. The “VXLAN Stitched” option informs SRIC 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. For each subnet described in the service, where a VNF resides, an EVPN Service is constructed and is referred to as an Access Facing service configuration. When multiple subnets exist in the service, additional configurations are provisioned to provide L3 routing to a localized node to route between multiple subnets on the same device. As well, a WAN Facing service configuration to provide L3 EVPN Tunneling transport between the network elements part of the service is provisioned. 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.

SRIC 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 SRIC via API or UI by selecting a VSD instance and Domain Template as an endpoint on the L3 DCI service. This triggers SRIC 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, SRIC provisions the access interface and Service Site configuration on the respective Access Leaf and Service Leaf nodes. Entities discovered from VSD in SRIC 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 SRIC provisions L3 Interfaces, IP addressing is provisioned based on the configurations described in VSD.

SRIC 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, SRIC 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.

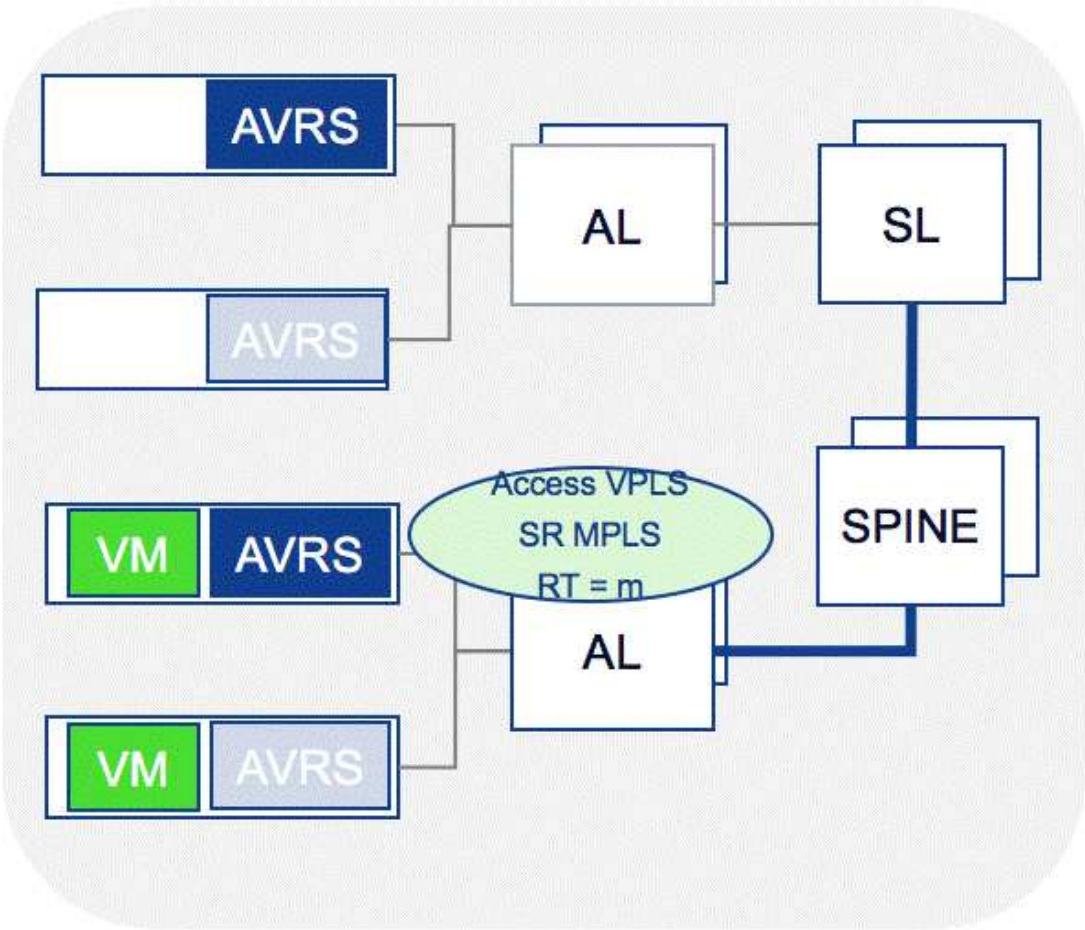
See 7.10 “How do I instantiate an L3 DCI service?” (p. 56).

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

SRIC. The L2 DCI is auto-generated on SRIC 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, SRIC 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. 57).

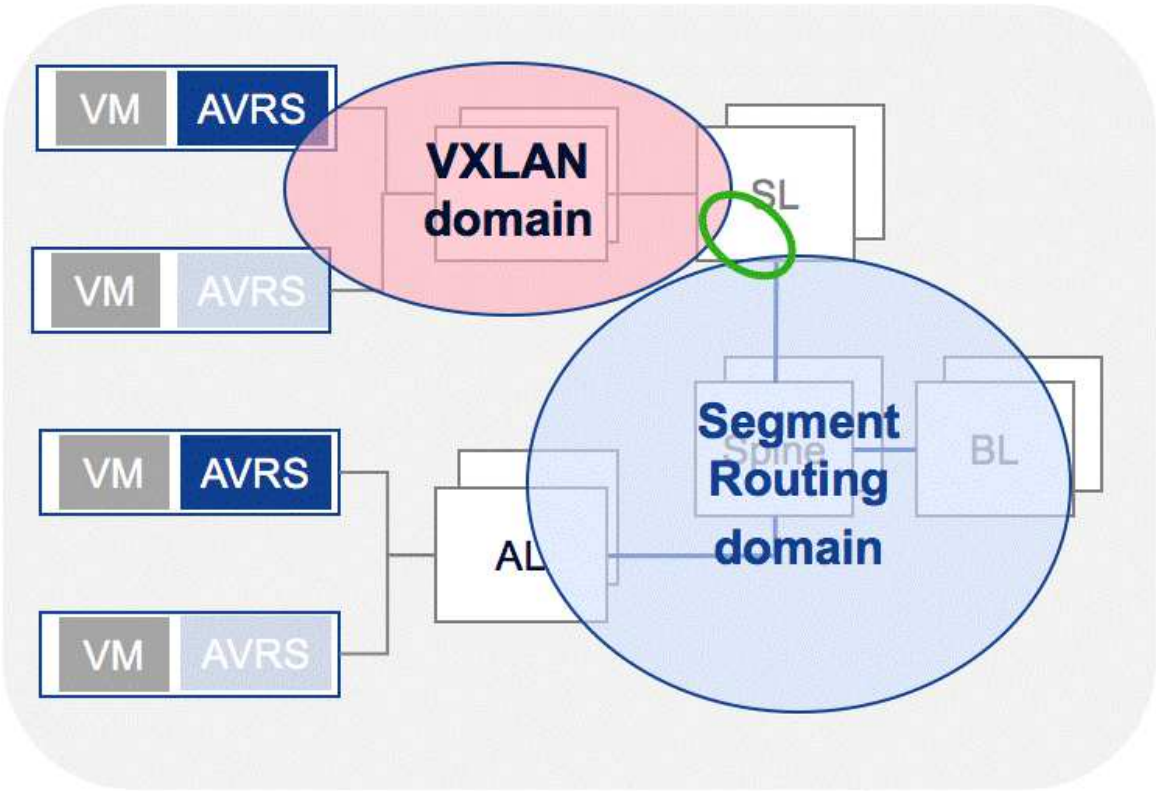
7.4 Deployment assumptions

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 SRIC (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, SRIC requires the VRS to be attached into the SRIC 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

SRIC 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*.

SRIC communicates to the VSD via its HTTPS REST API interface to fetch data during synchronization and to push data during instantiation. SRIC 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 SRIC 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 SRIC. SRIC will discover gateways from VSD and decide whether SRIC 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, SRIC will attempt to provision the network element if that network element is under its own mediation management.

Any device for which SRIC 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 SRIC to perform automatic service stitch provisioning on Service Leafs, SRIC 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. SRIC 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.

SRIC 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. SRIC 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 SRIC may communicated. This communication is accomplished via REST API with SSL and JMS with SSI. The *Nuage VNS User Guide* describes VSD REST authentication and the JMS configuration required to generate and use certificates.

SRIC 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.

SRIC 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. 52) 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 SRIC system.

6

Copy the certificate to your SRIC 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 SRIC 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 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 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 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 SRIC management, ensuring the following:

- Type is set to “Bridge” for entities connected to devices managed by SRIC
- 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 Service Fulfillment application attaches the new VPort, which will serve as an endpoint with a port type of “Virtual Port”. Upon instantiation,

SRIC will automatically provision the associated Access Leaf and a new port will appear within the L2 DCI or L3 DCI service in the 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 SRIC via API or UI with a VSD and template as endpoint input criteria.

2

SRIC 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.

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

5

SRIC 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

SRIC 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 SRIC.

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

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

6

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

END OF STEPS