NOKIA

NSP
Network Services Platform

Network Resource Controller - Packet (NRC-P)
Network Resource Controller - Cross domain (NRC-X)
Network Services Director
Release 18.9

Planning Guide

3HE-14123-AAAC-TQZZA

Issue 1

September 2018

Legal notice

Contents

List of tables

List of figures

About this document

Purpose

The *NSP NSD and NRC Planning Guide* consolidates all pre-installation information required to plan a successful deployment of the NSD and NRC modules of the Nokia NSP product.

Document support

Customer documentation and product support URLs:

- Customer Documentation Welcome Page
- Technical support

How to comment

Documentation feedback

- Documentation Feedback

1 Product overview

1.1 NSP overview

1.1.1 Introduction

This chapter provides an overview of the Network Services Director (NSD) and Network Resource Controller (NRC) modules of the Network Services Platform (NSP).

1.1.2 NSP architecture

The NSP product consists of multiple interoperating network management modules for service provisioning, automation, optimization, and element management functions for IP and optical networks. The NSD and NRC modules provide the following functionality:

- Network Resource Controller – Packet (NRC-P) – MPLS path computation and traffic flow management
- Network Services Director (NSD) – service provisioning and activation
- Network Resource Controller - Cross Domain (NRC-X)

As part of the NSP architecture, the NSD and NRC modules work with the following element management systems:

- Network Functions Manager - Packet, or NFM-P (formerly 5620 SAM)
- Network Functions Manager - Transport, or NFM-T (formerly 1830 OMS)

1.1.3 NRC-P

The NRC-P manages the creation of LSPs across IP network elements (NEs). The NRC-P maintains a network topology and a current path database synchronized with the NEs. A VSR-NRC must be deployed to interface with IP NEs to collect protocol routing data, which the NRC-P uses for path routing computations.

This release supports the migration of networks discovered by CPAM in previous NSP releases to PCE SROS-based topology.

The NRC-P is also the flow controller module of the NSP. It uses flow-based protocols to perform intelligent traffic steering and to automate policy-based redirection. The NRC-P monitors NEs discovered and statistics collected by the NFM-P. A vCPAA must be integrated with the NFM-P where the NRC-P monitors an AS.

In an NRC-P deployment, the VSR-NRC serves as an OpenFlow controller. The VSR-NRC pushes flow management information to OpenFlow switches as directed by the NRC-P.

The VSR-NRC/PCE and VSR-NRC/OFC can be deployed on virtual machine instances. Where both functions are deployed in a network, they must reside on the same VSR-NRC instance. The VSR-NRC is supported on VMWare ESXi. For platform requirements and installation instructions, see the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide*.

1.1.4 NRC-X

The NRC-X optimizes network resources across different layers and domains of IP/MPLS and optical networks.

The NRC-X is installed on a separate platform from the NSD and NRC modules. The platform requirements for an NRC-X deployment are the same as those for the deployment of NSD and NRC modules, except where indicated.

1.1.5 NSD

The NSD is the network service fulfillment module of the NSP. It provisions services using operator-defined policies across multi-domain networks. The NSD works with other NSP modules to perform service provisioning to specific elements.

1.1.6 nspOS

The nspOS is a set of platform services used by all NSP modules. The nspOS enables system-wide functions, including Single Sign On and operator access to the NSP Launchpad. The nspOS also contains common components and services that other NSP modules require.

The nspOS is installed with the NSD and NRC modules. In a shared-mode deployment, each module uses the nspOS instance on the NSD and NRC host.

See the *NSP Deployment and Installation Guide* for details about the NSP modules and their deployment options.

1.1.7 Model Driven Mediation

Model-Driven Mediation (MDM) is a component within the NSP architecture that provides mediation between model-driven NSP applications and Nokia or third-party network devices. MDM provides an adaptation layer which uses adaptors to convert NSP application requests to device specific directives using standard protocols such as NETCONF, SNMP and CLI over SSH or Telnet. MDM servers can be optionally deployed in an NSP complex with NSD and NRC. The NFM-P and NFM-T can coexist in the NSP deployment.

The MDM supports deployment in the following configurations:

- standalone instance
- 1 + 1 active/standby redundancy
- high-availability cluster
- 3 + 3 active/standby high-availability clusters

Each MDM server resides on its own virtual machine. In a redundant deployment, the primary MDM module follows the activity of the primary nspOS instance. In a high-availability cluster, the MDM provides:

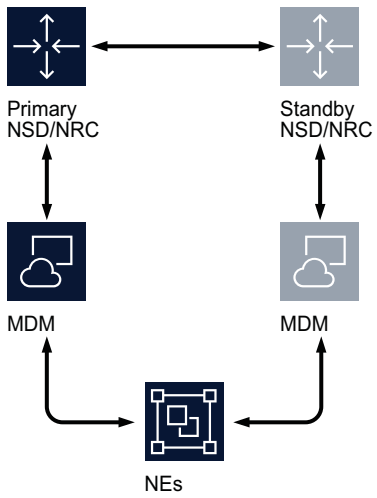
- load-balancing mediation with the NEs
- redundancy for a single MDM instance failure within the cluster

For a standalone NSD and NRC system, the MDM can be deployed as a standalone or high-availability cluster. For a redundant NSD and NRC system, the MDM can be deployed as a redundant (1 + 1) or redundant high-availability cluster (3 + 3). The MDM cannot be deployed with a

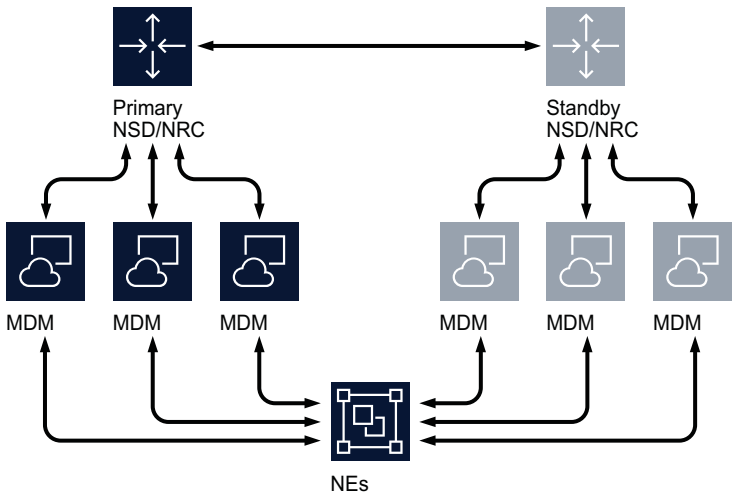
high-availability cluster deployment of NSD/NRC (either standalone or redundant).

The platform requirements for an MDM deployment are the same as the requirements for an NSD and NRC module deployment, except where indicated.

The following figure illustrates a redundant NSD and NRC system deployed with redundant MDM:



The following figure illustrates a redundant NSD and NRC system deployed with redundant, high availability MDM clusters:



1.1.8 NSD and NRC deployment overview

The NSD and NRC modules can be deployed as a standalone system, an active/standby redundant pair, a high-availability cluster, or a redundant high-availability cluster. The modules are deployed with other applications, including the NFM-P and/or the NFM-T. Both the NFM-P and the NFM-T can be deployed in standalone or redundant configurations (NFM-T with classic HA only). Nokia recommends that the NSD and NRC and Network Function Modules be all deployed as either standalone systems (for NSD and NRC, this includes standalone HA) or redundant systems (for NSD and NRC, this includes redundant HA). Mixed redundancy configuration of modules is not supported.

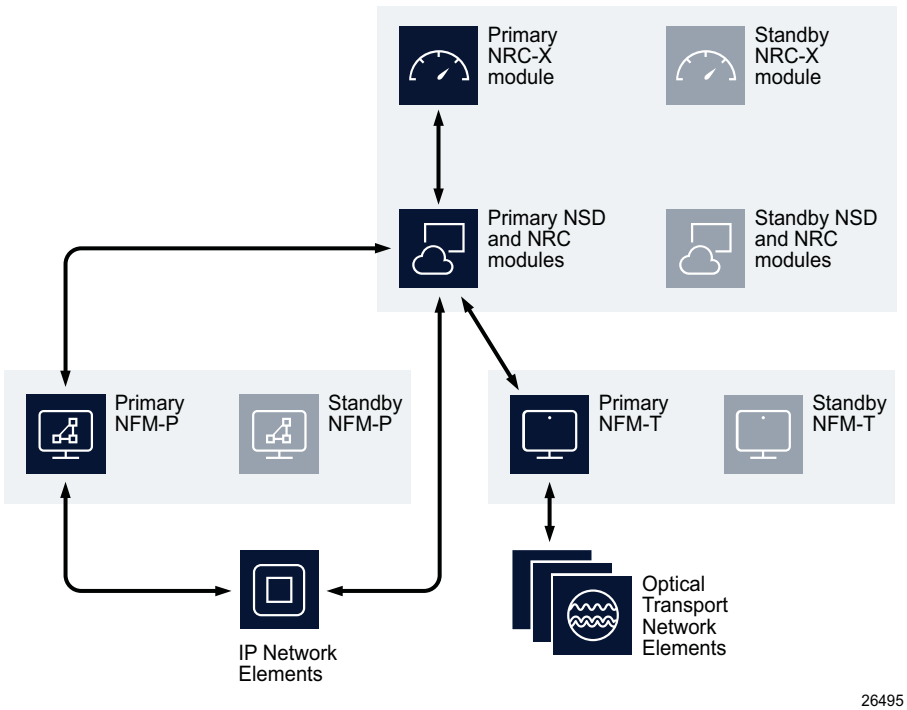
Note: The NRC-X can be deployed only as a standalone system or as an active/standby redundant pair. The NRC-X does not support high-availability clustering.

The NSD and NRC modules operate independently of the NFM-P and the NFM-T, and will automatically reconnect to the primary server if an activity switch of the NFM-P or the NFM-T takes place.

Note: A redundant deployment of the NRC-X module operates independently of the activity of the NSD and NRC modules. The primary NRC-X module will automatically reconnect to the primary NSD and NRC modules if an activity switch takes place.

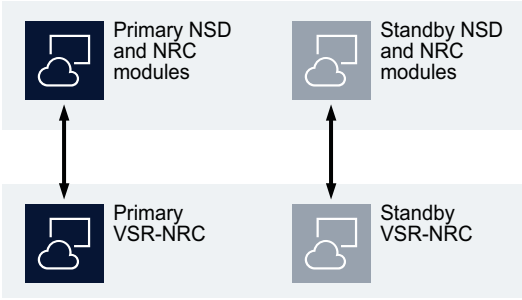
The following figure shows a fully redundant deployment of all NSP modules:

Figure 1-1 Redundant deployment of NSP modules



A redundant or redundant HA deployment of NSD and NRC modules is deployed with a redundant VSR-NRC, as described in the following figure.

Figure 1-2 Redundant NSD NRC deployment with redundant VSR-NRC



The NSD and NRC modules should be installed on a virtualized server. The NSD and NRC modules only support IPv4 connectivity with other components in the NSP architecture.

The NSD and NRC software is distributed in a tar file. An installation script will install multiple rpm packages for the NSD and NRC modules, including NRC-X and MDM. See the *NSP Deployment and Installation Guide* for full installation instructions. The *NSP Release Notice* defines compatible software releases for other applications that can be deployed with the NSD and NRC modules.

1.2 NSD and NRC key technologies

1.2.1 Java virtual machine

The NSD and NRC modules use Java technology. The installation package contains a Java Virtual Machine which is installed with the software. This is a dedicated Java Virtual Machine and does not conflict with other JVMs which may be installed on the same workstation. The NSD and NRC modules use OpenJDK 8.

1.2.2 Databases

Embedded within the NSD and NRC host server is a Neo4j database (version 3.2) for network topology information and a PostgreSQL database (version 9.6.9) for policy management.

The Neo4j database contains a graphical representation of the network topology and its elements in a multi-layer graph. The installation of the Neo4j database is customized for, and must be dedicated to, the NSD and NRC modules. Nokia will not support any configuration that deviates from the NSD and NRC installation procedure.

The PostgreSQL database contains non-topological NSD and NRC information, including policies and templates. PostgreSQL is an open source database application. Nokia will not support any PostgreSQL database configuration that deviates from the NSD and NRC installation procedure.

Note: Nokia does not support direct customer access to the Neo4j and PostgreSQL databases.

1.2.3 Browser applications

The NSD and NRC modules provide functionality using browser-based applications. The NSD and NRC modules use standard REST security mechanisms for authentication and authorization. All NSD and NRC module applications are HTML-5 based and are supported on the latest desktop version of Google Chrome. The browser applications require that WebGL be enabled.

1.2.4 API

The NSD and NRC modules provide a northbound REST API with Swagger-compliant documentation. The northbound API supports queries, service creation requests, and other functions. See the *NSP Developer portal* for more information.

1.2.5 Network mediation

The NSD and NRC modules have southbound interfaces that consist of plug-ins that interact with the NFM-P and the NFM-T, as well as standard communication protocols to interface directly with network elements. The NSD and NRC modules communicate with the NFM-P using CPROTO and HTTP protocols secured with TLS, and with the NFM-T using REST over TLS-secured HTTPS.

The NSD and NRC modules communicate with MDM using gRPC, and MDM communicates with nspOS applications of Zookeeper, Kafka and PostgreSQL. MDM communicates with network elements using NETCONF, SNMP and CLI over SSH or Telnet.

For LSP management functions of NRC-P, a VSR-NRC communicates with the PCC network elements via PCEP, IGP, and BGPLS. For flow control functions, the VSR-NRC OpenFlow Controller communicates with OpenFlow Switches using the OpenFlow protocol.

The nspOS module hosts the Telemetry application, which communicates directly with NEs using gRPC.

The NFM-P manages IP network elements using SNMP, and the NFM-T uses TL-1 and SNMP to manage optical transport network elements.

2 Operating system specifications

2.1 Red Hat Enterprise Linux (RHEL)

2.1.1 Introduction

This chapter defines the operating system requirements for the NSD and NRC modules.

2.1.2 RHEL description and recommendations

The NSD and NRC modules are supported on Red Hat Enterprise Linux Server Edition 7.3, 7.4 and 7.5 (x86-64). Previous releases, or other variants of Red Hat, and other Linux variants are not supported.

The NSD and NRC modules do not necessarily support all functionality provided in RHEL. SELinux, iptables, and Network Manager are not supported in NSD and NRC configurations. The NSD and NRC modules should use a time synchronization mechanism, such as NTP, to ensure accurate time. The NSD and NRC modules also require that the server hostname is configured in the */etc/hosts* file. RHEL must be installed in 64 bit mode where the NSD and NRC modules will be installed.

Customers are expected to purchase RHEL software and support for all platforms running RHEL Server with the NSD and NRC modules. It is strongly recommended to purchase a support package from Red Hat that provides 24x7 support.

Nokia recommends the installation of any OS, driver, or firmware updates that the hardware vendor advises for RHEL.

With the exception of documented Operating System parameter changes for NSD and NRC, all other settings must be left at the RHEL default configuration.

The *NSP Deployment and Installation Guide* provides detailed instructions for the RHEL OS installation.

2.1.3 Third-party applications

Applications that are not sanctioned by Nokia must not be running on any virtual instance running the NSD and NRC modules. Nokia reserves the right to remove any applications that are suspected of causing issues from workstations running NSD and NRC modules.

3 System resource requirements

3.1 Introduction

3.1.1 Overview

This chapter defines the system resource requirements for successfully running the NSD and NRC modules. Follow these guidelines to ensure the modules perform adequately.

3.2 Virtual machine requirements

3.2.1 Overview

Nokia recommends that the NSD and NRC modules be installed on virtual machines using VMWare ESXi or RHEL KVM, including OpenStack. The Guest Operating System for an NSD and NRC modules deployment must be a supported version of RHEL 7.3, 7.4 or 7.5 Server x86-64.

Installations of NSD and NRC are server- and vendor-agnostic, but must meet any defined hardware criteria and performance targets to be used with the NSD and NRC modules. Server class hardware must be used, not desktops. Processors must be x86-64 based with a minimum core speed of 2.4GHz.

Defined CPU and Memory resources for a virtual machine must be reserved and dedicated to that guest OS, and cannot be shared or oversubscribed. Disk and network resources should be managed appropriately to ensure that other guest OSs on the same physical server do not negatively impact the operation of the NSD and NRC modules.

Provisioned CPU resources are based upon threaded CPUs. The NSD/NRC Platform Requirements will specify a minimum number of vCPUs to be assigned to the Virtual Machine.

A guest virtual machine must use only one time synchronization protocol such as NTP. Additional time synchronization applications must be disabled to ensure the proper operation of NSP.

Nokia support personnel must be provided with the details of the provisioned Virtual Machine. These details can either be provided through read-only access to the hypervisor or must be available to Nokia support when requested. Failure to provide these details could impact support of the NSD and NRC modules.

3.3 VMware Virtualization

3.3.1 Overview

The NSD and NRC modules support using VMware vSphere ESXi 6.0, 6.1, or 6.5 only, on x86 based servers natively supported by ESXi. VMware’s Hardware Compatibility List (HCL) should be consulted to determine specific hardware support.

Not all features offered by ESXi are supported when using the NSD and NRC modules. For example, Fault Tolerant, High Availability (HA), Memory Compression, and Distributed Resource

Scheduler (DRS) features are not supported. Contact Nokia to determine if a specific ESXi feature is supported with an NSD and NRC installation.

If using NTP or a similar time synchronization protocol on the guest virtual machine, then you must disable VMwareTools time synchronization.

Virtual Machine Version 11 or above must be used. The disk must be “Thick Provisioned” with “Eager Zero” set. The SCSI controller must be set to “VMware Paravirtual” and the Disk Provisioning must be “Thick Provision Eager Zero”. The Network Adapter must be “VMXNET 3”. See the following table for additional Virtual Machine setting requirements:

Table 3-1 Additional Virtual Machine setting requirements

Resource type	Parameter	Setting
CPU	Shares	Set to High
	Reservation	Must be set to half the number of vCPUs * the CPU frequency. For example, on a 2.4 GHz 8 vCPU configuration, the reservation must be set to (1/2*8*2400) = 9600 MHz.
	Limit	Check box checked for unlimited
Advanced CPU	Hyperthreaded Core Sharing Mod	Set to None
Memory	Shares	Set to High
	Reservation	Slider set to the size of the memory allocated to the VM
	Limit	Check box checked for unlimited
Advanced Memory	NUMA Memory Affinity	No affinity
Disk	Shares	Set to High
	Limit — IOPs	Set to Unlimited

3.4 KVM virtualization

3.4.1 Overview

The NSD and NRC modules support using RHEL 6.3 through 6.7 KVM using QEMU version 0.12.1.2 and RHEL 7.2 through 7.5 KVM using QEMU version 1.5.3, 2.3.0, or 2.10.0 only, on x86 based servers natively supported by KVM. Consult the RHEL’s Hardware Compatibility List (HCL) to determine specific hardware support.

Not all features offered by KVM are supported when using the NSD and NRC modules. For example, Live Migration, Snapshots, or High Availability are not supported. Contact Nokia to determine if a specific KVM feature is supported with an installation of NSD and NRC modules.

3.4.2 Configuration

When you configure the KVM, set the parameters listed in the following table to the required values.

Table 3-2 KVM configuration parameters

Parameter	Value
Disk Controller type	virtio
Storage format	raw
Cache mode	none
I/O mode	native
I/O scheduler	deadline
NIC device model	virtio
Hypervisor type	kvm

3.5 OpenStack requirements

3.5.1 OpenStack support

The NSD and NRC modules support deployment in an OpenStack environment using Red Hat OpenStack Platform Release 8, 10, and 11. While an NSD and NRC modules installation may function in other OpenStack environments, the NSP Product Group does not commit to make the NSD and NRC modules compatible with a customer's alternate OpenStack environment.

To ensure the stability of the NSD and NRC modules and their compatibility with OpenStack, you must follow the recommendations provided in this section.

3.5.2 Hypervisor

The only hypervisor supported within an OpenStack environment is KVM. For details about the KVM hypervisor supported versions, see 3.4 “KVM virtualization” (p. 18).

3.5.3 CPU and memory resources

Defined CPU and memory resources must be reserved and dedicated to the individual Guest OSs, and cannot be shared or oversubscribed. You must set both the cpu_allocation_ratio and ram_allocation_ratio parameters to 1.0 in the OpenStack Nova configuration either on the control NE or on each individual compute node where a VM hosting the NFM-P could reside.

3.5.4 HyperThreading

The usage of CPUs with enabled HyperThreading must be consistent across all compute nodes. If there are CPUs that do not support HyperThreading, then you must disable HyperThreading at the hardware level on all compute nodes where the NSD and NRC modules could be deployed.

3.5.5 CPU pinning

Nokia does not recommend CPU pinning because it restricts the use of OpenStack migration.

3.5.6 Availability zones/affinity/placement

Nokia does not provide recommendations on configuring OpenStack for VM placement.

3.5.7 Migration

The OpenStack environment supports only the regular migration. Live migration is not supported.

3.5.8 Networking

Basic Neutron functionality using Open vSwitch with the ML2 plugin can be used in a deployment of NSD and NRC modules. The use of OpenStack floating IP addresses is supported for the NSD and NRC modules.

3.5.9 Storage

All storage must meet the performance metrics provided with the NSD and NRC modules Platform Sizing Response. Performance must meet the documented requirements for both throughput and latency.

3.5.10 VM storage

The VM storage must be persistent block (Cinder) storage and not ephemeral. For each VM to be deployed, a bootable Cinder volume must be created. The size of the volume is indicated in the NSD and NRC modules Platform Sizing Response.

3.5.11 Flavors

Flavors must be created for each “Station Type” indicated in the NSD and NRC modules Platform Sizing Response.

3.5.12 Firewalls

Firewalls can be enabled using OpenStack Security Groups, or on the VMs using the firewalld service. If firewalld is enabled, then an OpenStack Security Group that allows all incoming and outgoing traffic must be used.

3.6 Platform requirements

3.6.1 Overview

The virtual machine requirements for an NSD/NRC, NRC-X, MDM or VSR-NRC deployment depend on, but are not limited to, the following factors:

- Number of managed LSPs and services
- Number of managed elements
- Number of simultaneous user and API sessions
- Expected number of flows, monitored routers, number of ASs, number of ports with real-time statistics collection

3.6.2 Minimum and production platform requirements

The following table lists the minimum and production platform requirements for the deployment of the NSD-NRC, NRC-X, MDM and VSR-NRC based on the deployment types described in the *NSP Deployment and Installation Guide*. The minimum and production platforms support the network dimensions described in Chapter 5, “Scaling”.

Table 3-3 Platform requirements for NSD-NRC, NRC-X, MDM and VSR-NRC deployment

Deployment	Component	Minimum platform	Production platform
WAN SDN deployments	NSD-NRC	CPU: 8 vCPU Memory: minimum 30 GB, recommended 32 GB Disk space: 270 GB or more	CPU: 24 vCPU Memory: minimum 48 GB, recommended 64 GB Disk space: 540 GB or more
	MDM	CPU: 2 vCPU Memory: 8 GB Disk space: 100 GB	CPU: 4 vCPU Memory: 16 GB Disk space: 100 GB
	VSR-NRC	CPU: 4 vCPU Memory: 4 GB Disk space: 5 GB	CPU: 4 vCPU Memory: 8 GB Disk space: 5 GB
Control plane-only deployment	NRC-P	CPU: 8 vCPU Memory: 24 GB Disk space: 270 GB or more	CPU: 12 vCPU Memory: 32 GB Disk space: 540 GB or more
	VSR-NRC	CPU: 4 vCPU Memory: 4 GB Disk space: 5 GB	CPU: 4 vCPU Memory: 8 GB Disk space: 5 GB
NSD/NRC optional	NRC-X	CPU: 8 vCPU Memory: minimum 16 GB Disk space: 160 GB or more	CPU: 16 vCPU Memory: 32 GB Disk space: 270 GB

Note: Verify that the VSR-NRC platform specifications are consistent with the specifications provided in the *Virtualized 7750 SR and 7950 XRS Simulator (vSIM) Installation and Setup Guide* for this release.

3.7 Hostname requirements

3.7.1 Overview

The hostname of an NSD and NRC server must meet the following criteria:

- can contain only ASCII alphanumeric characters and hyphens
- cannot begin or end with a hyphen
- cannot end with a period followed by a digit
- if the hostname is an FQDN, period characters delimit the FQDN components
- the FQDN of the hostname cannot exceed 63 characters

4 Network requirements

4.1 Overview

4.1.1 Introduction

This chapter describes the network requirements for an NSD and NRC system and the connectivity with other applications.

4.2 NSD and NRC to OSS clients

4.2.1 Bandwidth requirements

The bandwidth requirements depend on the number of concurrent connections and on the type of transactions that are performed. For a single provisioning thread, Nokia recommends to provide 50 kbps of bandwidth from the OSS client to the NSD and NRC server. An OSS client that performs frequent query operations (for example, port or service inventory) must be provided additional bandwidth.

4.3 NSD and NRC to GUI clients

4.3.1 Bandwidth requirements

The network size drives the primary bandwidth requirement for NSD and NRC to GUI clients. More NEs and services result in more data being sent from the NSD and NRC modules to GUI clients. Optimal GUI performance is achieved with 10 Mbps of bandwidth with minimal network latency. Nokia recommends to provide a minimum of 2.5 Mbps of bandwidth.

High network latency between the NSD and NRC modules and GUI clients slows GUI performance. Nokia recommends to limit the round-trip network latency time to 100 ms.

4.4 NSD and NRC to NFM-P

4.4.1 Bandwidth requirements

The bandwidth requirements depend on the following factors:

- the number of NEs, LSPs, and services configured on the NFM-P
- the frequency of NE updates to the NSD and NRC modules

When an NSD and NRC system re-synchronizes with the NFM-P, optimal performance is achieved with 50 Mbps of bandwidth between the NSD and NRC modules and the NFM-P. Nokia recommends to provide a minimum of 25 Mbps of bandwidth.

Network latency impacts the time it takes for the NSD and NRC modules to re-synchronize a large amount of data from the NFM-P. Nokia recommends to limit the round-trip network latency time to 100 ms.

4.5 NSD and NRC to NFM-T

4.5.1 Bandwidth requirements

The bandwidth requirements between the NSD and NRC modules and the NFM-T depend on the number of optical NEs and services configured in the network. Nokia recommends to provide 10 Mbps of bandwidth between the NSD and NRC modules and the NFM-T. High round-trip network latency affects GUI performance and must be limited to 100 ms.

4.6 Network requirements for redundant and high-availability deployments

4.6.1 Redundant deployment

The network requirements between active/standby NSD and NRC servers depend on the network size (number of NEs and configured services) and the rate of service provisioning activities. The peak bandwidth requirement between redundant servers is 50 Mbps, with sustained bandwidth of 25 Mbps. Round-trip network latency between the redundant pair must be limited to 100ms.

4.6.2 High-availability deployment

The NSD and NRC modules deployed in a high-availability (HA) cluster must reside on servers in the same datacenter and on the same subnet, and share a virtual IP address. Servers in a HA cluster require connectivity with a minimum of 50 Mbps bandwidth and less than 1 ms round trip latency. The bandwidth and network latency requirements between active and standby servers in a redundant HA deployment are the same as those in a redundant deployment.

5 Scaling

5.1 Overview

5.1.1 Introduction

The following sections present the network dimension parameters for the minimum and production platforms described in section 3.6.2 “Minimum and production platform requirements” (p. 21).

5.2 Scale limits for NSD and NRC-P deployments

5.2.1 WAN SDN + IP deployment

The following tables present key dimension details for a WAN SDN + IP deployment as described in the *NSP Deployment and Installation Guide*.

Table 5-1 Dimensioning details for a WAN SDN + IP deployment

Key dimension	Minimum platform	Production platform
Number of IP services managed	3000	300 000
Number of L2 access interfaces	5000	500 000
Number of L3 access interfaces	300	30 000
Number of RSVP-TE LSPs	400	40 000
Number of service tunnels	600	60 000
Number of NFM-P managed services	17 000	1 700 000

The following table presents key dimension details for the NRC-P module (insight-driven automation).

Table 5-2 Dimensioning details for the NRC-P module (insight-driven automation)

Key dimension	Minimum platform	Production platform
Number of flows	10 000	1 000 000
Number of ASs	50	500
Number of subnets/AS	1600	32 000
Ports to collect real-time statistics from	10	200

5.2.2 Control plane-only deployment

The following table presents key dimension details for a control plane-only deployment as described in the *NSP Deployment and Installation Guide*.

Table 5-3 Dimensioning details for control plane-only deployment

Key dimension	Minimum platform	Production platform
Total Number of LSPs	5000	60 000
Number of delegated RSVP-TE or SR-TE LSPs or both (PCE-Control, PCE-Compute and PCE-Report)	2000	20 000
Number of un-delegated RSVP-TE LSPs (only PCE-Report)	3000	40 000
Number of IP NEs	1000	3000
Number of IP links	2000	6000

5.3 Scale limits for NRC-X deployments

5.3.1 NRC-X scaling within WAN SDN + IP + optical deployment

The following table presents key dimension details for NRC-X in a WAN SDN + IP + optical deployment as described in the *NSP Deployment and Installation Guide*.

Table 5-4 Dimensioning details for NRC-X in a WAN SDN + IP + optical deployment

Key dimension	Minimum platform	Production platform
IP NEs	100	2000
Optical NEs	100	2000
Ports	2400	240 000
Links	250	25 000
CDLs	100	10 000
Optical services	200	20 000
LLI	50	5000
IP-optical correlation	100	10 000

5.4 Scale limits for telemetry

5.4.1 Telemetry scaling

Telemetry has two related scaling limits:

- The maximum number of OSS subscriptions is 200. This number of OSS subscriptions includes, but is not limited to, Telemetry data.
- The maximum number of Telemetry notifications per second is 14,000, where one statistics counter update equals one Telemetry notification.

5.5 Failover performance for HA and redundant deployments

5.5.1 Overview

Redundant deployments of NSD/NRC will experience application down time when an active server switches activity to a standby server (for both High Availability cluster or single node deployments). In a High Availability cluster of NSD/NRC, when a leader switches to another member in the cluster, there will be an impact to the NSD/NRC applications.

In a WAN SDN + IP deployment, the Service Fulfillment application enables service provisioning. Operators will experience a service provisioning outage during a leader switch within a High Availability cluster, or during an activity switch in an active/standby redundant deployment. The actual down time will vary based on network size.

Service Fulfillment	
Down time for a switch of leader activity within an HA cluster	5 - 15 minutes
Down time for an activity switch from active to standby (HA cluster or single node) in a redundant deployment	20 - 60 minutes

Users and client applications that need to access NSP applications will also experience application down time during a leader switch within a High Availability cluster, and during an activity switch from active to standby (HA cluster or single node) in a redundant deployment. When the active server Launchpad application becomes available, northbound clients can authenticate and access applications.

Launchpad	
Down time for a switch of leader activity within an HA cluster	< 1s (see note)
Down time for an activity switch from active to standby (HA cluster or single node) in a redundant deployment	5 minutes

Note: The Launchpad application will remain available to users during a leader switch in an HA cluster, but some applications on the Launchpad may reload and be temporarily unavailable.

6 Security

6.1 Introduction

6.1.1 Overview

This chapter provides general information about platform security for the NSD and NRC modules.

The NSD and NRC modules implement a number of safeguards to ensure the protection of private data. Additional information can be found in the Security section of the *NSP Deployment and Installation Guide*.

6.2 Securing the NSD and NRC modules

6.2.1 Overview

Nokia recommends that you to perform the following steps to achieve workstation security for the NSD and NRC modules:

- Install the latest recommended patch cluster from Red Hat
- Implement firewall rules to control access to ports on NSD and NRC systems, as detailed below
- Use a CA signed certificate rather than a self-signed certificate.
- Use SSL certificates with strong hashing algorithms.

6.3 Operating system security for NSD and NRC workstations

6.3.1 RHEL patches

Nokia supports customers applying RHEL patches provided by Red Hat which will include security fixes as well as functional fixes. If a patch is found to be incompatible with the NSD and NRC modules, the patch may need to be removed until a solution to the incompatibility is provided by Red Hat or Nokia. See the *NSP NSD and NRC Release Notice* for up-to-date information about the recommended RHEL maintenance update and patch levels.

6.3.2 Platform hardening

Additional efforts to secure the system could impact NSD and NRC operation or future upgrades of the product. Customers must perform some level of basic testing to validate additional platform hardening does not impact the operation of the NSD and NRC modules. The NSP Product Group makes no commitment to make the NSD and NRC modules compatible with a customer's hardening requirements.

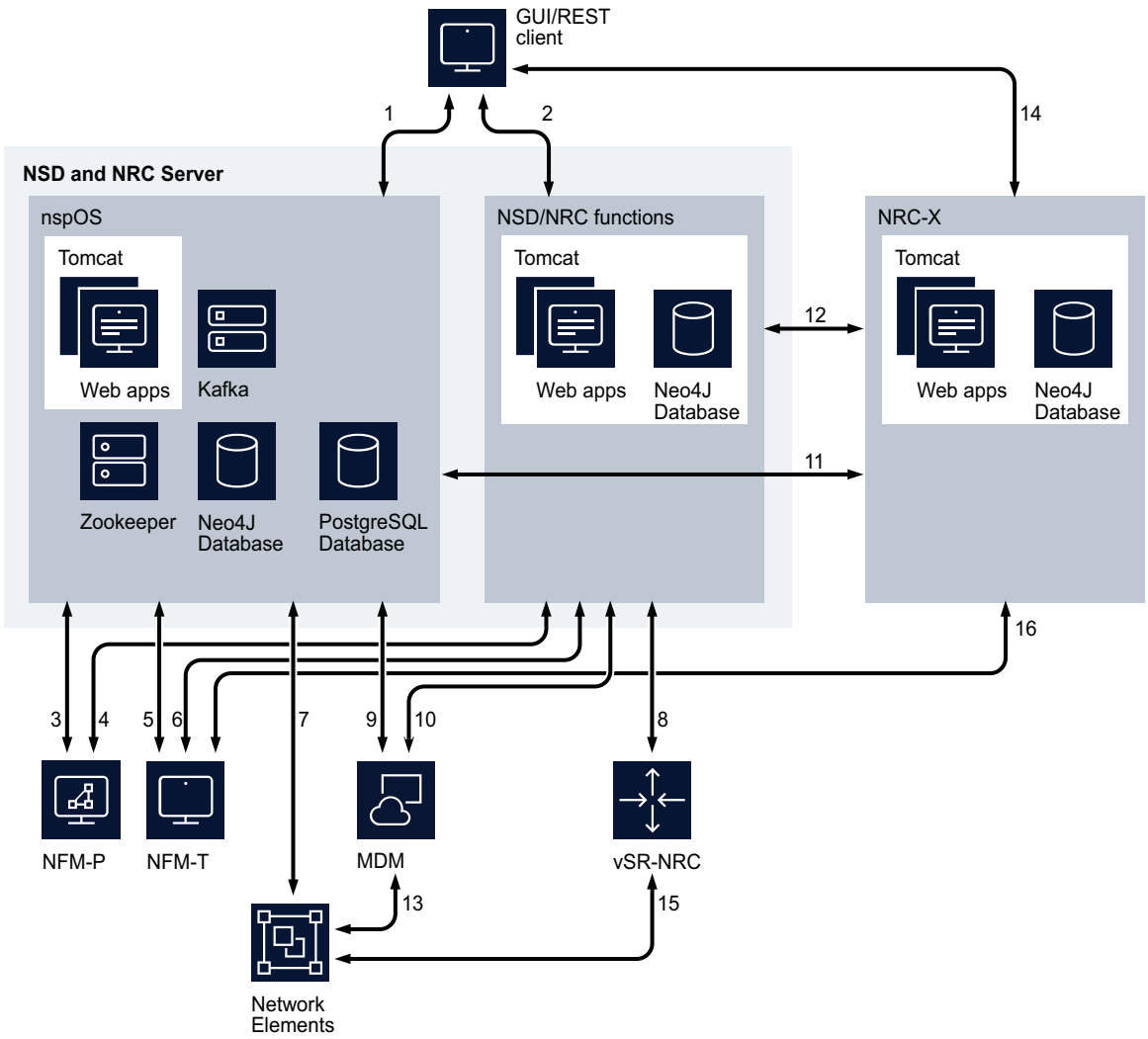
6.4 Communication between the NSD and NRC modules and external systems

6.4.1 Overview

The following diagrams illustrate the various components of the NSD and NRC modules and their internal communications, as well as communications with external systems.

The following figure shows a standalone NSD and NRC deployment and its communications with external systems.

Figure 6-1 Standalone NSD and NRC deployment



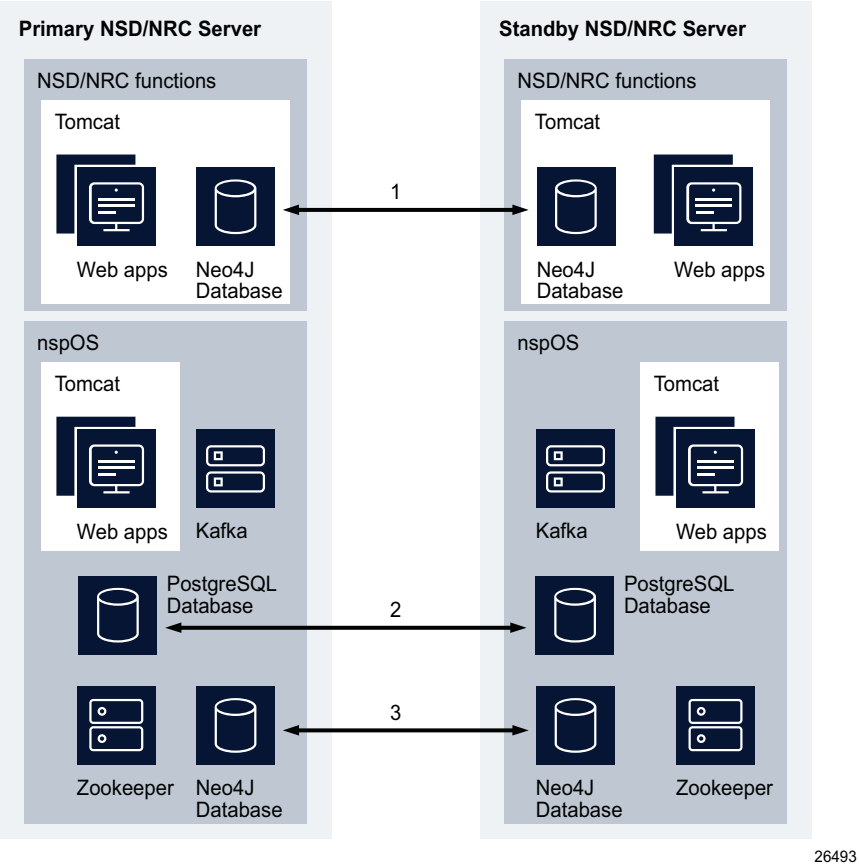
Connection	Usage
1, 2	Web Client/REST API client connections. REST over HTTPS secured with TLS
3	SSO authentication (secure), zookeeper registration (non-secure), neo4j database (non-secure), kafka (non-secure)
4	Data connection – CPROTO protocol secured with TLS
5	SSO authentication (secure), zookeeper registration (non-secure)
6	Data connection – REST over HTTPS secured with TLS
7	gRPC (for Telemetry) – secured with TLS NPN
8	Data connection – not secured
9	Zookeeper registration (non-secure), Kafka (non-secure), PostgreSQL (secure)
10	gRPC (non-secure)
11	Zookeeper registration (non-secure), Kafka (non-secure), SSO authentication (secure)
12	REST over HTTPS secured with TLS
13	NE mediation using NETCONF, SNMP, CLI (secure or non-secure)
14	Web Client connection. REST over HTTPS secured with TLS.
15	BGP,PCEP, OpenFlow communications (non-secure)
16	REST over HTTPS secured with TLS

6.5 Communication between redundant NSD and NRC server

6.5.1 Overview

The following figure shows the internal communications between redundant NSD and NRC servers:

Figure 6-2 Internal communications between redundant NSD and NRC servers



Connection	Usage
1	Neo4j data replication, not secured
2	PostgreSQL data replication, secured
3	Neo4j data replication, not secured

6.6 NSD and NRC firewalls

6.6.1 Overview

A firewall can be deployed in an NSP topology to protect the NSD and NRC modules from different networks and applications.

The NSD and NRC modules support the use of Network Address Translation (NAT) between themselves and client applications (API and GUI). The NSD and NRC modules also support NAT

between themselves and the VSR-NRC. The use of NAT is not supported between geo-redundant or HA deployments of NSD/NRC and between NSD/NRC and deployments of NFM-P or NFM-T.

Some NSD and NRC operations require idle TCP ports to remain open for long periods of time. Therefore, a customer firewall that closes idle TCP connections should adjust OS TCP keep-alives to ensure that the firewall will not close sockets that are in use by the NSD and NRC modules.

6.6.2 Firewall port requirements for NSD and NRC deployments

The tables provided in this section identify the listening ports in an NSD and NRC deployment within an NSP topology. See the respective product documentation for a complete list of firewall ports for other NSP modules.

The NSD and NRC deployment types are:

- standalone
- redundant
- standalone HA (high availability)
- redundant HA

Table 6-1 Listening ports for all communications with NSD/NRC

Default port(s)	Type	Encryption	Description	NSD/NRC deployment
All applications				
22	TCP	Dynamic Encryption	SSH/SCP/SFTP Used for remote access and secure file transfer	All
8180	TCP	None	HAProxy	HA Redundant HA
NSD and NRC				
5001	TCP	None	Neo4j database	All
5798	TCP	None	Ignite communication within cluster	HA Redundant HA
6017	TCP	None	Neo4j database	All
6018	TCP	None	Neo4j database	Redundant Redundant HA
6362	TCP	None	Neo4j database Local port to the host	All
7575	TCP	None	Neo4j database Local port to the host	All

Table 6-1 Listening ports for all communications with NSD/NRC (continued)

Default port(s)	Type	Encryption	Description	NSD/NRC deployment
7688	TCP	None	Neo4j database Local port to the host	All
8105	TCP	None	Java Tomcat Local port to the host	All
8223	TCP	None	Java Tomcat	Redundant Redundant HA
8224	TCP	Dynamic, SSL/TLS	Java Tomcat Local port to the host	All
8225	TCP	Dynamic, SSL/TLS	Java Tomcat Local port to the host	All
8543	TCP	Dynamic, SSL/TLS	Java Tomcat, secure HTTPS port for GUI and REST API	All
10800	TCP	None	Java Tomcat	All
11211	TCP	None	Ignite cache	All
11213	TCP	None	Java Tomcat	HA Redundant HA
47100–47199	TCP	None	Ignite cache	All
47500–47599	TCP	None	Ignite cache	All
48100–48199	TCP	None	Ignite cache Local port to the host	All
NRC-X application				
5001	TCP	None	Neo4j database	All
6017	TCP	None	Neo4j database	All
8105	TCP	None	Java Tomcat Local port to the host	All
8543	TCP	Dynamic, SSL/TLS	Java Tomcat, secure HTTPS port for GUI and REST API	All
nspOS				
80	TCP	None	HTTP port for nspOS common applications, redirect to 443	All
443	TCP	Dynamic, SSL/TLS	Secure HTTPS port for nspOS common applications	All

Table 6-1 Listening ports for all communications with NSD/NRC (continued)

Default port(s)	Type	Encryption	Description	NSD/NRC deployment
2181	TCP	None	Zookeeper	All
2390	TCP	Dynamic, SSL/TLS	nspdctl	All
2391	TCP	None	PKI server	only with PKI server installed and running
2888	TCP	None	Zookeeper	HA Redundant HA
3888	TCP	None	Zookeeper	HA Redundant HA
5007	TCP	None	Neo4j database	All
6007	TCP	None	Neo4j database	All
6363	TCP	None	Neo4j database Local port to the host	All
6432	TCP	SSL/TLS	PostgreSQL database	All
7473	TCP	Dynamic, SSL/TLS	Neo4j database	All
7474	TCP	None	Neo4j database Local port to the host	All
7687	TCP	None	Neo4j database	All
7889	TCP	None	Telemetry Local port to the host	All
8195	TCP	None	tomcat shutdown port Local port to the host	All
8196	TCP	None	app1-tomcat shutdown port Local port to the host	All
8197	TCP	None	Tomcat shutdown port Local port to the host	Where MDM is deployed
8544	TCP	Dynamic, SSL/TLS	HTTPS port for app1-tomcat	All
8545	TCP	Dynamic, SSL/TLS	HTTPS port for app2-tomcat (MDM apps)	Where MDM is deployed

Table 6-1 Listening ports for all communications with NSD/NRC (continued)

Default port(s)	Type	Encryption	Description	NSD/NRC deployment
9000	TCP	None	gRPC server Local port to the host.	All
9092	TCP	None	Kafka server	All
11212	TCP	None	Java Tomcat	HA Redundant HA
47100–47199	TCP	SSL/TLS	CAS ignite cache	All
47500–47599	TCP	SSL/TLS	CAS ignite cache	All
48500–48599	TCP	SSL/TLS	session-manager ignite cache	All
48600–48699	TCP	SSL/TLS	session-manager ignite cache	All
VSR-NRC				
179	TCP	None	BGP	N/A
4189	TCP	None	PCEP	N/A
4199	TCP	None	CPROTO	N/A
6653	TCP	None	OpenFlow	N/A
NFM-P application				
7879	TCP	SSL/TLS	CPROTO	N/A
8087	TCP	SSL/TLS	Web applications communications	N/A
8543	TCP	SSL/TLS	Web applications communications	N/A
NFM-T application				
80	TCP	None	Used for redirect only	N/A
8443	TCP	SSL/TLS	HTTPS-based communication	N/A

The following table lists the ports used in communication between the NSD and NRC modules and NFM-T:

Table 6-2 Ports used in communication between the NSD and NRC and the NFM-T

Protocol	From port	From module	To port	To module
TCP	80	NFM-T presentation server	>32768	NSD/NRC

Table 6-2 Ports used in communication between the NSD and NRC and the NFM-T (continued)

Protocol	From port	From module	To port	To module
TCP	>32768	NSD/NRC	80	NFM-T presentation server
TCP	443	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	443	NSD/NRC
TCP	2181	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	2181	NSD/NRC
TCP	>32768	NSD/NRC	8443	NFM-T OTNE server
TCP	8443	NFM-T OTNE server	>32768	NSD/NRC
TCP	9092	NSD/NRC	>15000	NFM-T
TCP	>15000	NFM-T	9092	NSD/NRC

The following table lists the ports used in communication between the NSD and NRC modules and the VSR-NRC:

Table 6-3 Ports used in communication between the NSD and NRC modules and the VSR-NRC

Protocol	From port	From module	To port	To module
TCP	>32768	NSD/NRC	4199	VSR-NRC
TCP	4199	VSR-NRC	>32768	NSD/NRC

The following table lists the ports used in communication between the NSD-NRC and the NFM-P:

Table 6-4 Ports used in communication between the NSD-NRC and the NFM-P

Protocol	From port	From module	To port	To module
TCP	2181	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	2181	NSD/NRC
TCP	>32768	NSD/NRC	7879	NFM-P
TCP	7879	NFM-P	>32768	NSD/NRC
TCP	>32768	NSD/NRC	8087	NFM-P
TCP	8087	NFM-P	>32768	NSD/NRC
TCP	7687	NSD/NRC	>15000	NFM-P

Table 6-4 Ports used in communication between the NSD-NRC and the NFM-P (continued)

Protocol	From port	From module	To port	To module
TCP	>15000	NFM-P	7687	NSD/NRC
TCP	9092	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	9092	NSD/NRC
TCP	>15000	NFM-P	7473	NSD/NRC
TCP	7473	NSD/NRC	>15000	NFM-P
TCP	>15000	NFM-P	443	NSD/NRC
TCP	443	NSD/NRC	>15000	NFM-P
TCP	>32768	NSD/NRC	8543	NFM-P
TCP	8543	NFM-P	>32768	NSD/NRC
TCP	>15000	NFM-P	6432	NSD/NRC
TCP	6432	NSD/NRC	>15000	NFM-P

The following table lists the ports used in communication between the NSD-NRC and the NRC-X:

Table 6-5 Ports used in communication between the NSD-NRC and the NRC-X

Protocol	From port	From module	To port	To module
TCP	>32768	NRC-X	443	NSD/NRC
TCP	443	NSD/NRC	>32768	NRC-X
TCP	>32768	NRC-X	9092	NSD/NRC
TCP	9092	NSD/NRC	>32768	NRC-X
TCP	>32768	NRC-X	2181	NSD/NRC
TCP	2181	NSD/NRC	>32768	NRC-X
TCP	>32768	NRC-X	8543	NSD/NRC
TCP	8543	NSD/NRC	>32768	NRC-X

The following table lists the ports used in communication between the NSD and NRC modules and NEs:

Table 6-6 Ports used in communication between the NSD and NRC modules and NEs

Protocol	From port	From module	To port	To module
TCP	>32768	NSD/NRC	57400	NE
TCP	57400	NE	>32768	NSD/NRC

The following table lists the ports used in communication between the active and standby NSD-NRC in a redundant deployment:

Table 6-7 Ports used in communication between the active and standby NSD-NRC in a redundant deployment

Protocol	From port	To port
TCP	>32768	22
TCP	22	>32768
TCP	>32768	2390
TCP	2390	>32768
TCP	>32768	5001
TCP	5001	>32768
TCP	>32768	5007
TCP	5007	>32768
TCP	>32768	6007
TCP	6007	>32768
TCP	>32768	6017
TCP	6017	>32768
TCP	>32768	6018
TCP	6018	>32768
TCP	>32768	6432
TCP	6432	>32768

The following table lists the ports used in communication between the active and standby NRC-X in a redundant deployment:

Table 6-8 Ports used in communication between the active and standby NRC-X in a redundant deployment

Protocol	From port	To port
TCP	>32768	22
TCP	22	>32768
TCP	>32768	5001
TCP	5001	>32768
TCP	>32768	6017

Table 6-8 Ports used in communication between the active and standby NRC-X in a redundant deployment (continued)

Protocol	From port	To port
TCP	6017	>32768

The following table lists the ports used in communication between NSD-NRC and client (GUI/REST) applications:

Table 6-9 Ports used in communication between NSD-NRC and client (GUI/REST) applications

Protocol	To port	To module	Purpose
TCP	80	NSD and NRC / nspOS	for Launchpad redirect
TCP	443	NSD and NRC / nspOS	for Launchpad
TCP	8443	NFM-T	NFM-T GUI
TCP	8543	NSD and NRC	for NSD and NRC GUI, REST API
TCP	8543	NFM-P	NFM-P web applications / REST API
TCP	8543	NRC-X	NRC-X web application, REST API
TCP	8544	NSD and NRC / nspOS	nspOS web applications
TCP	8545	NSD and NRC / nspOS	MDM applications
TCP	9092	NSD and NRC / nspOS	External notifications (messaging)

The following table lists the ports used in communication between the NSD-NRC and MDM applications

Table 6-10 Ports used in communication between the NSD-NRC modules and the MDM

Protocol	From port	From module	To port	To module
TCP	>32768	MDM	2181	NSD-NRC
TCP	2181	NSD-NRC	>32768	MDM
TCP	>32768	MDM	9092	NSD-NRC

Table 6-10 Ports used in communication between the NSD-NRC modules and the MDM (continued)

Protocol	From port	From module	To port	To module
TCP	9092	NSD-NRC	>32768	MDM
TCP	30000	MDM	>32768	NSD-NRC
TCP	>32768	NSD-NRC	30000	MDM
TCP	>32768	MDM	6432	NSD-NRC
TCP	6432	NSD-NRC	>32768	MDM

The following table lists the ports used in communication between the NRC-X and NRC-T

Table 6-11 Ports used in communication between the NRC-X and NRC-T

Protocol	From port	From module	To port	To module
TCP	8543	NRC-T	>15000	NRC-X
TCP	>15000	NRC-X	8543	NRC-T

A Standards compliance

A.1 Supported standards and open-standard interfaces

A.1.1 Industry standards and open-standard interfaces

The NSD and NRC modules incorporate industry standards and open-standard interfaces that allow them to interoperate with other network monitoring and management systems. The NSD and NRC are compliant with the standards and open-standard interfaces described in the following table.

Table A-1 Industry standards and open-standard interfaces

Standard/interface	Description
draft-alvarez-pce-path-profiles-04	PCE path profiles
draft-ietf-i2rs-yang-network-topo-20	A data model for network topologies
draft-ietf-idr-bgp-ls-segment-routing-ext-04	BGP link-state extension for segment routing
draft-ietf-isis-segment-routing-extenstions-04	IS-IS extensions for segment routing
draft-ietf-liu-netmod-yang-schedule-04	A YANG data model for configuration scheduling
draft-ietf-ospf-segment-routing-extensions-04	OSPF extensions for segment routing
draft-ietf-pce-segment-routing-08	PCEP extensions for segment routing
draft-ietf-pce-stateful-pce-14	PCEP extensions for stateful PCE
draft-ietf-teas-yang-te-10	A YANG data model for traffic engineering tunnels and interfaces
draft-ietf-teas-yang-te-topo-13	YANG data model for TE topologies
OpenFlow	OpenFlow Switch Specification version 1.3.1
REST	Representational State Transfer
RFC 4655	Path Computation Element (PCE)
RFC 5101	Specification of the IP Flow Information Export (IPFIX) Protocol for the exchange of IP traffic flow information
RFC 5102	Information model for IP flow information export
RFC 5440	Path Computation Element Communication Protocol (PCEP)

Table A-1 Industry standards and open-standard interfaces (continued)

Standard/interface	Description
RFC 5575	Dissemination of flow specification rules
RFC 6020	YANG data modelling language for NETCONF
RFC 6021	Common YANG data types
RFC 6241	Network configuration protocol (NETCONF)
RFC 6242	NETCONF over SSH
RFC 6991	Common YANG data types
RFC 7223	A YANG data model for interface management
RFC 7224	IANA interface type YANG model
RFC 7420	PCEP Management Information Base (MIB) model
RFC 7684	OSPFv2 prefix/link attribute advertisement
RFC 7752	North-bound distribution of link-state and Traffic Engineering (TE) information using BGP
RFC 7951	JSON encoding of data modelled with YANG