

NSP Network Services Platform

Use Case Catalog Sample Procedures

3HE-20932-AAAA-TQZZA Issue 4 May 2025

© 2025 Nokia. Use subject to Terms available at: www.nokia.com/terms

#### 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.

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2025 Nokia.

# Contents

Ab	out this	s document	9
1	UCC-1	I1: Brownfield Service Discovery	11
	1.1	Overview	11
	Prepa	ration	12
	1.2	Prerequisites	12
	1.3	Optional: create a restricted Service Management user	14
	1.4	Install the required artifact bundles	18
	Servio	ce Configuration	20
	1.5	Import intent types into Service Management	20
	1.6	Create a service template	22
	1.7	Stitch a brownfield service	24
	1.8	Service stitching – EPIPE/ELINE services	25
	1.9	Service stitching – ELAN services	29
	1.10	Service stitching – IES services	32
	1.11	Service stitching – L3 VPN services	34
	1.12	Auto-stitching a brownfield service	35
	1.13	Associate a brownfield service to service template	37
	1.14	Modify a brownfield service	42
	1.15	Delete a brownfield service	45
2	UCC-1	12: E-LINE/E-PIPE	49
	2.1	Overview	49
	Prepa	ration	50
	2.2	Prerequisites	50
	2.3	Optional: create a restricted Service Management user	52
	2.4	Install the required artifact bundles	56
	2.5	Configure user access to the required intent types	57
	Service Configuration		60
	2.6	Import intent types into Service Management	60
	2.7	Create a service tunnel template	61
	2.8	Create and deploy service tunnels to the network	63
	2.9	Create an EPIPE service template	65
	2.10	Create and deploy an EPIPE service to the network	67
	2.11	Modify or delete an EPIPE service	71

	Optio	nal procedures	
	2.12	Generate and execute OAM test suites	75
	2.13	Create telemetry subscriptions	77
	2.14	Create a telemetry chart and plot statistics	
3	UCC-	13: C-LINE/C-PIPE	81
	3.1	Overview	81
	Prepa	ration	83
	3.2	Prerequisites	83
	3.3	Optional: create a restricted Service Management user	85
	3.4	Install the required artifact bundles	89
	3.5	Configure user access to the required intent types	90
	Servio	ce Configuration	93
	3.6	Import intent types into Service Management	93
	3.7	Create a service tunnel template	94
	3.8	Create and deploy service tunnels to the network	96
	3.9	Create a CPIPE service template	
	3.10	Create and deploy a CPIPE service to the network	
	3.11	Modify or delete a CPIPE service	
	Optio	nal procedures	111
	3.12	Create telemetry subscriptions	111
	3.13	Create a telemetry chart and plot statistics	112
4	UCC-	14: E-LAN/EVPN	
	4.1	Overview	
	Prepa	ration	
	4.2	Prerequisites	
	4.3	Optional: create a restricted Service Management user	119
	4.4	Install the required artifact bundles	
	4.5	Configure user access to the required intent type	
	Servio	ce configuration	
	4.6	Import the intent type into Service Management	127
	4.7	Create an EVPN-VPLS service template	127
	4.8	Create an E-LAN EVPN (over MPLS) service	130
	4.9	Modify the service configuration	132
	4.10	Remove the service	132
	4.11	Delete the service	133

	Optio	nal procedures	134
	4.12	Create an OAM test suite	
	4.13	Execute an OAM test suite	136
	4.14	View OAM test results	
	4.15	Delete an OAM test suite	139
	4.16	Create a telemetry subscription	140
	4.17	Modify a telemetry subscription	142
	4.18	Plot telemetry statistics	144
	4.19	Delete a telemetry subscription	
5	UCC-	15: L3 VPN	
	5.1	Overview	149
	Prepa	ration	
	5.2	Prerequisites	
	5.3	Optional: create a restricted Service Management user	
	5.4	Install the required artifact bundles	
	5.5	Configure user access to the required intent type	
	Servio	ce configuration	
	5.6	Import the intent type into Service Management	
	5.7	Create a service tunnel template	
	5.8	Create and deploy service tunnels to the network	
	5.9	Create a VPRN service template	
	5.10	Create and deploy a VPRN service to the network	
	5.11	Modify the service configuration	
	5.12	Remove the service	
	5.13	Delete the service	
	Optio	nal procedures	
	5.14	Create an OAM test suite	
	5.15	Execute an OAM test suite	
	5.16	View OAM test results	
	5.17	Delete an OAM test suite	201
	5.18	Create a telemetry subscription	
	5.19	Modify a telemetry subscription	
	5.20	Plot telemetry statistics	
	5.21	Delete a telemetry subscription	
6	UCC-	16: IES	
	6.1	Overview	211

Р	reparatior	1	212
6.	.2 Pre	requisites	
6.	.3 Opt	ional: create a restricted Service Management user	
6.	.4 Inst	all the required artifact bundles	
6.	.5 Cor	figure user access to the required intent types	219
S	ervice Co	nfiguration	221
6.	.6 Imp	ort intent types into Service Management	221
6.	.7 Cre	ate an IES service template	
6.	.8 Cre	ate and deploy an IES service to the network	
6.	.9 Moo	lify or delete an IES service	
0	ptional pr	ocedures	231
6.	.10 Cre	ate telemetry subscriptions	231
6.	.11 Cre	ate a telemetry chart and plot statistics	
7 U	CC-20: NE	E Provisioning - Day/Phase 1 configuration	
7.	.1 Ove	erview	
Р	reparatior	۱	
7.	.2 Pre	requisites	
D	ay/Phase	1 configuration	
7.	.3 Car	ds/MDA	
7.	.4 Por	t/Connector	
7.	.5 BFD	) Templates	
7.	.6 OSI	PF/ISIS	
7.	.7 MPI	LS/RSVP Interfaces	
7.	.8 Inte	rfaces	
7.	.9 LDF	, 	
7.	.10 BGI	>	
7.	.11 Seg	ment Routing	
7.	.12 LSF		
<i>(</i> .	.13 Cus	tomers	
(.	.14 Oth	er configurations	
8 U	CC-26: NE	E Upgrades	
8.	.1 Ove	erview	
P	reparation	۱ ۱	
8.	.2 Prei	requisites	
8.	.3 Pre-	-upgrade checks	
8.	.4 Dov	vnload and upload NE software	

Upgra	des	
8.5	Upgrade prerequisites	
8.6	Backing up the node configs	40
8.7	Multi-phase upgrade: preparing the upgrade	40
8.8	Multi-phase upgrade: performing the upgrade	41
8.9	Single phase upgrade: preparing the upgrade	41
8.10	Single phase upgrade: performing the upgrade	
8.11	ISSU upgrade	
Post-	upgrade procedures	
8.12	Rollback	430
8.13	LSO reporting	
8.14	Post-upgrade checks	
8.15	Troubleshooting upgrades	430
UCC-	33: LSP Enhanced Path Control	
9.1	Overview	
Preparation		
9.2	Prerequisites	
9.3	Install the required artifact bundles	
MPLS	LSP provisioning	
9.4	Provision MPLS LSPs using Device Configuration	
Use case 1: Utilization/Bandwidth optimization		
9.5	Bandwidth optimization	
9.6	Create a bandwidth-based path profile	
9.7	Enable traffic collection parameters using an API	
9.8	Monitor bandwidth	
9.9	Bandwidth optimization	
9.10	System activity logging after bandwidth optimization	
Use case 2: Latency-based optimization		
9.11	Latency optimization	
9.12	Create a latency-based path profile	
9.13	Associate the latency-based path profile to LSPs in Device Management	
9.14	Configure OAM configuration objects using an API	
9.15	Create a TWAMP Light test session	
9.16	Execute TWAMP Light session tests	
9.17	Enable latency parameters using an API	
9.18	Monitor latency	

9.19	Latency-based optimization	485
9.20	System activity logging after latency optimization	491

# About this document

# Purpose

The *NSP Use Case Catalog Sample Procedures* document is intended for NSP operators and administrators who need to understand or perform NSP device and service management processes.

This document describes the steps required to complete use cases found in the NSP Network Automation Use Case Catalog. For more information about the use case catalog, see (https://www.nokia.com/networks/ip-networks/network-services-platform/use-case-catalog/).

This guide is a multi-release document that provides tested procedures with release-specific sample commands from different NSP releases, depending on the use case.

### Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

### **Document support**

Customer documentation and product support URLs:

- Documentation Center
- Technical support

### How to comment

Please send your feedback to Documentation Feedback.

# 1 UCC-11: Brownfield Service Discovery

# 1.1 Overview

## 1.1.1 Purpose

This chapter describes the steps that are common to discovery of all brownfield services covered in this guide (i.e., E-LINE, E-LAN, C-LINE, IES, and L3 VPN (VPRN)) in NSP.

Configuration examples in this chapter show NSP Release 24.4 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-svc-assurance-bundle-2404.zip
- nsp-svc-fulfillment-bundle-2404.zip

See the NSP and NE documentation for more information.

# 1.1.2 Contents

1.1 Overview	11
Preparation	12
1.2 Prerequisites	12
1.3 Optional: create a restricted Service Management user	14
1.4 Install the required artifact bundles	18
Service Configuration	20
1.5 Import intent types into Service Management	20
1.6 Create a service template	22
1.7 Stitch a brownfield service	24
1.8 Service stitching – EPIPE/ELINE services	25
1.9 Service stitching – ELAN services	29
1.10 Service stitching – IES services	32
1.11 Service stitching – L3 VPN services	34
1.12 Auto-stitching a brownfield service	35
1.13 Associate a brownfield service to service template	37
1.14 Modify a brownfield service	42
1.15 Delete a brownfield service	45

# Preparation

# 1.2 Prerequisites

# 1.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for Brownfield Service Discovery		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	_
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the NSP Installation and Upgrade Guide How do I enable TLS for telemetry and gNMI on_change support? in the NSP System Administrator Guide.	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>serviceActivationAndConfiguration- intentBasedServiceFulfillment</li> <li>networkInfrastructureManagement- basicManagement</li> <li>networkInfrastructureManagement- deviceConfig</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-cological-inventory</li> <li>sros-23-7-r1</li> </ul> </li> </ul>

May 2025

Issue 4

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration)	How do I install an artifact bundle? in the NSP Network Automation Guide	_
• NSP product attract bundle for Service Fulfillment		
Device discovery	Pathway for device discovery in the NSP Classic Management User Guide How do I discover devices? in the NSP Device Management Guide Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Cards and MDAs provisioning	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the NSP Device Management Guide for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	
Scheduler QoS Policies	How do I create a logical configuration deployment? in the NSP Device Management	The intent types required for this configuration are:
Network QoS Policies	Guide.	<ul> <li>icm-qos-schedulerpolicy-srqos</li> </ul>
		<ul> <li>icm-qos-network-srqos</li> </ul>
SAP QoS Policies		<ul> <li>icm-qos-sapingress-srqos</li> </ul>
		icm-qos-sapegress-srqos
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

# **1.3 Optional: create a restricted Service Management user**

# 1.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- · Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- · Configuring user access to an intent type

For example, the reference procedures in NSP Release 24.4 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- · How do I configure user access to an intent type?

### 1.3.2 Steps

### Create a role

1 —

Log in to the NSP as an administrator.

2 \_\_\_\_\_

Open Users and Security.

3 \_\_\_\_\_

Select **Roles** from the drop-down list on the toolbar.

- Click **+ Create Role**. The Create Role form opens.
- 5 -----

4

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain any spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	—
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7 —

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.
- 8

Click **Create** to save your changes and return to the Roles list.

END OF STEPS -

# **1.3.3 Create a user group**

1 —

Open Users and Security.

2 \_\_\_\_\_

Select **User Groups** from the drop-down list on the toolbar.

3 –

Click **+ Create User Group**. The Create User Group form opens.

4 \_\_\_\_\_

Specify a group name and description in the Identification panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters:  $\emptyset$  – .

The User Group Name string must not contain any spaces, including a leading or trailing space.

- 5 To assign user roles to the group, click + Add Roles on the Roles panel. The Add Roles form
- opens.

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

7 –

Click Create to save your changes and return to the User Groups list.

END OF STEPS -

# 1.3.4 Create a user

- **i** Note: This procedure describes how to create a local NSP user account in a system deployed using OAUTH2 authentication. It does not apply to users managed through external databases.
- 1 –

Open Users and Security.

2 —

Select Users from the drop-down list on the toolbar.

3 —

Click + Create User.

4

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- can be 1 to 40 characters long
- · cannot include a space
- · cannot have a leading or trailing space
- · can include only the following special characters:

- @ (at sign)
- - (hyphen)
- \_ (underscore)
- . (period)

5 —

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the Show Password option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.
- 6 —

Click Create.

END OF STEPS -

# 1.4 Install the required artifact bundles

### 1.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

### 1.4.2 Steps

### Install the artifact bundle in NSP

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open Artifacts, Artifact Bundles.

3 \_\_\_\_\_

Click IMPORT & INSTALL.

4

In the form that opens, drag and drop the artifact bundle that holds the intents provided for this use case, or click **Browse** and navigate to the files on your system.

#### 5 -

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6

To install a bundle in Imported status, choose **Install bundle** from the **(**Table row actions) menu.

END OF STEPS -

#### 1.5 Import intent types into Service Management

# 1.5.1 Purpose

Use this procedure to import the intent types you obtained in 1.4 "Install the required artifact bundles" (p. 18) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the NSP Service Management Guide.

For example, the reference procedure in NSP Release 24.4 is How do I import an intent type into Service Management?.

**i** Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are epipe, cpipe, evpn-vpls, ies, and vprn.

# 1.5.2 Steps

1

Log in to the NSP as the Service Management user.

2

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously-defined intent types is displayed.



Note: Only intent types that have the Service Fulfillment label applied will be available to import.



**i** Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the NSP Network Automation Guide. The permission needs to be granted to all applicable Intent Types.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

Depending on the service type that has to be covered, the corresponding Intent Type in the following list can be imported.

Intent types to be imported:

- epipe
- cpipe
- evpn-vpls
- ies

NSP

vprn

The intent types are imported into service management. This may take a few minutes.



**i** Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

# 1.5.3 Example configuration of user access to evpn-vpls intent type

NO <ia network="" platform<="" services="" th=""><th>í.</th><th></th><th></th><th></th><th>User: admin</th><th>1</th><th>•</th><th>0</th></ia>	í.				User: admin	1	•	0
Network Intents Intent Types	•				IMPORT -	+ INTENT TYPE	Ģ	:
Intent Type	Version				User Access			÷
T		Configure User Access Specify which users have intent type access by choosing the	teir user group(s) below.	τ				
wavencevprn	2	Selected intent type(s) (1 Intent Type(s) selected)	User Group access permissions assigned to the selected intent type(s)					1
wavencecomposite	2		Choose access 👻					
wavencebackhaul	2		Full access					÷
vprn	2		No Access 👻 admin	Admin, Ser				:
vpls	2			/iceFulfillm				-
tunnel	2			nin, Service				÷
redundant-vpls	2			viceFulfillm				÷
redundant-eline	2			<i>v</i> iceFulfillm				÷
redundant-cline	2			<i>v</i> iceFulfillm				÷
13-evpn-composite	2			<i>r</i> iceFulfillm				:
les	2			riceFulfillm				÷
evpn-epipe	2			viceFulfillm				÷
etree	2			/iceFulfillm				:
evpn-vpls	2			riceFulfillm	Service_Management_	Group		
epipe	Z			Admin, Ser	Service_Management_	Group		÷
composite	2		CANCEL SAVE	viceFulfillm				÷
cpipe	2	Released	ApprovedMisalignments, ArtifactAdmin, S	erviceFulfillm				:
* <u>.</u>							-	
Auto-refresh Last Refresh: 2024/10/14 13:2	0.21		C Page: 1 /1 > >I				Row C	ount: 64

# 1.5.4 Example importing intent types into Service Management

	Network Services Platform							User: admin	•	(?)
Service Management	Templates Intent Type Catalogue	•							IMPORT	Ģ
Intent Type	Intent Type Version		Labels	Build		Last Updated Time	:	(i) Info		
	T	Ŧ	T		T		Ť	Select an intent type		
epipe		2	ApprovedMisalignments, Ar	24.4.0-rel_2.3.0		2024-04-24 15:25:16	1	Seccontinent type		
evpn-vpls		2	ApprovedMisalignments, Ar	24.4.0-rel_2.3.0		2024-04-24 15:25:16	1			
cpipe		2	ApprovedMisalignments, Ar	24.4.0-rel_2.3.0		2024-04-24 15:25:16	:			
ies		2	ApprovedMisalignments, Ar	24.4.0-rel_2.3.0		2024-04-24 15:25:16	1			
Last Refresh : Oct 14, 2024,	, 1:27:45 PM GMT+5:30 (Local Time)					IC C Page: 1 /1 > >I			Total Ro	uw Count: 4

# **1.6 Create a service template**

# 1.6.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 24.4 is How do I create a service template?.

# 1.6.2 Steps

1 -

Log in to the NSP as the Service Management user.

2

From the **Service Management, Service Templates** view, click **+ CREATE**. The Create a service template form opens.

### 3 –

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	One of the following based on the service type: epipe, cpipe, evpn-vpls, ies, vprn
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	Specifies the interface to be used with the template

#### 4

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

#### 5 -

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

#### 6 —

### Click ADD.

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

7 \_\_\_\_\_

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

8

Click CREATE.

The service template is created.

END OF STEPS

# 1.7 Stitch a brownfield service

# 1.7.1 IBSF service stitching

IBSF provides the functionality to stitch brownfield MDM managed service sites into a single service entity and persist them in the NSP database so they are visible (read-only) by IBSF. Then, the user may associate the service to a template which would enable full lifecycle management and CRUD support. In order to achieve this, a service stitching algorithm was developed to stitch sites together into a single service entity based on service type and algorithm. This service stitching can be triggered from the IBSF API or by enabling auto-stitch.

# **1.7.2 Prerequisites**

The required artifacts for service stitching are in the svc-mgt-artifacts-common bundle. These artifacts include data-sync mapping and metadata files.

This is available on: (https://download-na.support.nokia.com/cgi-bin/Download.pl?hier\_id=197305).

# 1.7.3 Service stitching API

The service stitching API takes 3 input parameters: service-type, algorithm, and sites. Only include MDM sites. The URL and body is as follows:

(https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

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

# 1.7.4 Stitching procedures

Perform one of the following procedures to stitch a brownfield service:

- Service Stitching EPIPE Services
- Service Stitching ELAN Services
- Service Stitching IES Services
- Service Stitching L3 VPN Services

# 1.7.5 Auto-stitching

Perform the following procedure to auto-stitch a brownfield service:

· Auto-stitching a brownfield service

# **1.8 Service stitching – EPIPE/ELINE services**

# **1.8.1 Service stitching algorithm for Epipe services**

The following are the service stitching algorithm for Epipe services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	sites must have inverse matching route-target values and inverse matching local/remote ac values
service-name	matching service-name
evi	sites must have matching evi values and inverse matching local/remote ac values
local	a single site with 2 access interfaces
vcid	site's tunnel binding must have matching vcid

**i** Note: *Route-target* and *evi* algorithms are for EVPN-EPIPE and outside the scope of this document. Service stitching with the other 3 algorithms are documented below.

### 1.8.2 Service stitching with service-name algorithm

Services which are to be stitched with service-name algorithm should have same service names on the end sites.

1

Stitch the Epipe service created on MD NE using the following API:

```
POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)
BODY:
```

```
{
    "input":{
        "service-type":"eline",
        "algorithm":"service-name",
        "sites":["92.168.96.190","92.168.96.46"]
        }
    }
RESPONSE:
    {
```

```
"response": {
    "status": 0,
    "startRow": 0,
    "endRow": 0,
    "totalRows": 1,
    "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: eline_service-name-1726659802472",
    "errors": null
    }
}
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.

■ NO <ia network="" p="" service<=""></ia>	es Platform								User: epip	e-user	•	0
Service Management Services	-									+ CREATE	C,	:
Life Cycle State	Alignment State	Composite Service	Service Name		Description		Service Template	1	(i) Info			
•	-		τ.	٣.,		٣.		Τ.	States			Ĩ
<ul> <li>Unknown</li> </ul>	Unknown		EPIPE 62		Continental Rail Services Site			:				
Unknown	Unknown		EPIPE 60		TransCanadian Exploration Ltd .			:	Life Cycle State			~
Unknown	Unknown		EPIPE 12		Continental Rail Services Site			:	Unknown			
Deployed	Aligned		EPIPE 10		TransCanadian Exploration Ltd .		EPIPE Template	1	Alignment State Unknown			
<ul> <li>Unknown</li> </ul>	Unknown		Site A - Keller Construction	EPI	Keller Construction Site A - Se			:				
Unknown	Unknown		EPIPE 35		Epipe 35 - Seattle			1	General Info			
Unknown	Unknown		EPIPE 36		Site - Seattle			I				
Unknown	Unknown		EPIPE 10		TransCanadian Exploration Ltd .			:	Service ID EPIPE 36			
<ul> <li>Unknown</li> </ul>	Unknown		VPLS 103		An EVPN ELAN service betwee			:	NE Service ID			
Unknown	Unknown		VPLS 100		An EVPN ELAN service over MPL	S		:	36			
Unknown	Unknown		VPLS 101		Another EVPN ELAN service ov			:	Service Name EPIPE 36			
									Description			
									Site - Seattle			
									Service Type ELINE			
									Customer ID 12			
( )								• • •	Service Manager ID			
Last Refresh : Sep 18, 2024, 5:13:29 PM GMT+5:30	0 (Local Time)				< Page: 1 /1 >						Total Row	Count: 11
Total Service Count : 11 Deployed : 11												

END OF STEPS

# 1.8.3 Service stitching with local algorithm

1 -

Stitch the Epipe service created on MD NE using the following API: POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices) BODY:

```
{
       "input":{
       "service-type":"eline",
       "algorithm":"local",
       "sites":["92.168.96.190"]
       }
    }
RESPONSE:
    {
       "response": {
          "status": 0,
          "startRow": 0,
          "endRow": 0,
          "totalRows": 1,
          "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: "eline_local-1726669622177",
          "errors": null
       }
    }
```

2

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.

NOKIA Network Service	es Platform				_						User: epipe-user	•	0
Service Management Services	÷										+ CREATE	Ģ	:
Life Cycle State	Alignment State	Composite Service	Service Nan	ne		Description		Service Template		:	(i) Info		
			Τ.		Τ.		<b>T</b>		Τ.				
Unknown	Unknown		EPIPE 62			Continental Rail Services Site				:	Service ID		
Unknown	Unknown		EPIPE 60			TransCanadian Exploration Ltd				:	EPIPE 72		
Unknown	Unknown		EPIPE 12			Continental Rail Services Site				:	NE Service ID 72		
Deployed	Aligned		EPIPE 10			TransCanadian Exploration Ltd .		EPIPE Template		:	Service Name		
Unknown	Unknown		Site A - Kell	er Construction EPI		Keller Construction Site A - Se.				:	EPIPE 72		
Unknown	Unknown		EPIPE 35			Epipe 35 - Seattle				:	Description		
Unknown	Unknown		EPIPE 36			Site - Seattle				:			
Unknown	Unknown		EPIPE 72							:	ELINE		
Unknown	Unknown		EPIPE 10			TransCanadian Exploration Ltd				:	Customer ID		
Unknown	Unknown		VPLS 103			An EVPN ELAN service betwee				:	n		
Unknown	Unknown		VPLS 100			An EVPN ELAN service over MPL	.s			:	Service Manager ID 0		
Unknown	Unknown		VPLS 101			Another EVPN ELAN service ov.				:	Template Name		
											Service Functions		
											# of functions: 0		
											Admin State		
•										( )	Operational State Disabled		
Last Refresh : Sep 18, 2024, 7:58:27 PM GMT+5:3	0 (Local Time)					< Page: 1 / 1 >	>I.					Total Row	e Count: 12
Total Service Count : 12 Deployed : 12													

END OF STEPS

# 1.8.4 Service stitching with vcid algorithm

```
1
  Stitch the Epipe service created on MD NE using the following API.
  POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)
  BODY:
      {
          "input":{
          "service-type":"eline",
          "algorithm": "vcid",
          "sites":["92.168.96.190","92.168.96.46"]
          }
      }
  RESPONSE:
      {
          "response": {
             "status": 0,
             "startRow": 0,
             "endRow": 0,
             "totalRows": 1,
             "data": "Successfully submitted to Job Manager for Service
  Stitch processing with Job Name: eline_vcid-1725863475919",
             "errors": null
          }
      }
2 -
```

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.

■ NO <ia network="" p="" service<=""></ia>	es Platform						User: epipe-user	• ⑦
Service Management Services							+ CREATE	0 :
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Service Template		(i) Info	
•	×	Τ.			Τ.	Τ.	States	
Unknown	Unknown		EPIPE 62	Continental Rail Services Site		:	States	_
Unknown	Unknown		EPIPE 60	TransCanadian Exploration Ltd	TransCanadian Exploration Ltd			~
Unknown	Unknown		EPIPE 12	Continental Rail Services Site		1	<ul> <li>Unknown</li> </ul>	
Deployed	Aligned		EPIPE 10	EPIPE 10 TransCanadian Exploration Ltd EPIPE Template		Alignment State Unknown		
Unknown	Unknown		Site A - Keller Construction EPI	Keller Construction Site A - Se		:		
Unknown	Unknown		Site A - Keller Construction EPI	Keller Construction Site A - Se		1	General Info	
<ul> <li>Unknown</li> </ul>	Unknown		VPLS 103	An EVPN ELAN service betwee		:		_
Unknown	Unknown		VPLS 100	An EVPN ELAN service over MPLS	5	1	Service ID Site A - Keller Construction EPIPE 11	
Unknown	Unknown		VPLS 101	Another EVPN ELAN service ov		:	NE Service ID	
							11	
							Service Name	
							Site X - Keller Construction Enire 11	
							Description Keller Construction Site A - Seattle	
							Service Type	
							ELINE	
							Customer ID	
							14	
1 Last Refresh - Sen 9, 2024, 12:39:50 PM GMT+5:30	D (i ocal Time)			( Page: 1 /1 )		F 3. F	Service Manager ID	Total Row Count: 9
Deployed : 9								

END OF STEPS

# 1.9 Service stitching – ELAN services

# 1.9.1 Service stitching algorithm for Elan services

The following are the service stitching algorithm for Elan services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	sites must have inverse matching route-target values
service-name	matching service-name
evi	sites must have matching evi values and inverse matching local/remote ac values
vcid	site's tunnel binding must have matching vcid

# 1.9.2 Service stitching with service-name algorithm

1 -

Stitch the Elan service created on MD NE using the following API. POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)

NSP

```
BODY:
    {
       "input":{
       "service-type":"elan",
       "algorithm": "service-name",
       "sites":["92.168.96.190","92.168.96.46"]
       }
    }
RESPONSE:
    {
       "response": {
          "status": 0,
          "startRow": 0,
          "endRow": 0,
          "totalRows": 1,
          "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: elan service-name-1727419509598",
          "errors": null
       }
    }
```

2 -

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.

NOCIA Network Service	es Platform					User: elan-user		•	0
Service Management Service Services	•						+ CREATE	Ċ	:
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Service Templat	(i) Info			
<ul> <li>nebiolea</li> </ul>	<ul> <li>Augreo</li> </ul>	T	T			Select a service			
Unknown	Unknown		EPIPE 12	Continental Rail Services Site	:				
Unknown	Unknown		EPIPE 62	Continental Rail Services Site	:				
Deployed	<ul> <li>Aligned</li> </ul>		Site A - Keller Construction EPIPE 11	Keller Construction Site A - Se	EPIPE Template				
Unknown	Unknown		Site A - Keller Construction EPIPE 61	Keller Construction Site A - Se	:				
Unknown	Unknown		EPIPE 12	Continental Rail Services Site	:				
Unknown	Unknown		EPIPE 10	TransCanadian Exploration Ltd	:				
Unknown	Unknown		EPIPE 60	TransCanadian Exploration Ltd	:				
Unknown	Unknown		EPIPE 62	Continental Rail Services Site	:				
<ul> <li>Unknown</li> </ul>	Unknown		EVPN-VPLS-100	An EVPN ELAN service over MPLS	:				
Unknown	Unknown		EVPN-ELAN-103-Boston	An EVPN ELAN service betwee	:				
Unknown	Unknown		EVPN-VPLS-101	Another EVPN ELAN service ov	:				
Unknown	Unknown		EVPN-VPLS-102-Seattle	A new EVPN ELAN service	:				
Unknown	Unknown		EVPN-VPLS-102-Boston	A new EVPN ELAN service	:				
Deployed	Aligned		VPLS 103	An EVPN ELAN service betwee	EPVN_VPLS_Terr				
Deployed	Aligned		VPLS 101	Another EVPN ELAN service ov	EPVN_VPLS_Terr				
Deployed	Aligned		VPLS 100	An EVPN ELAN service over MPLS	EPVN_VPLS_Terr				
•					▶				
Last Refresh : Sep 27, 2024, 12:27:16 PM GMT+5:	Last Refreb : Sep 27, 2024, 12:27:16 PM GMT+53:0 (Local Time)								
Total Service Count: 17 Deployed: 17									

END OF STEPS

# 1.9.3 Service stitching with evi algorithm

```
1
  Stitch the Elan service created on MD NE using the following API:
  POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)
  BODY:
      {
          "input":{
          "service-type":"elan",
          "algorithm":"evi",
          "sites":["92.168.96.190","92.168.96.46"]
          }
      }
  RESPONSE:
      {
          "response": {
             "status": 0,
             "startRow": 0,
             "endRow": 0,
             "totalRows": 1,
             "data": "Successfully submitted to Job Manager for Service
  Stitch processing with Job Name: elan_evi-1728379514781"
             "errors": null
          }
      }
2 -
```

Ensure the service gets listed in the NSP Service Management in 'Unknown' state.

-	-										0
NOKIA Network Service	ces Platform						User: a	admin		•	0
Service Management Service Services	•							+ CR	EATE	0	:
Life Cycle State	Alignment State	Composite Service	Service Name		Description	Service Template	i 👔 Info				
•	•	T		T	Ţ		Salart a s	envice			
<ul> <li>Unknown</li> </ul>	Unknown		EVPN-ELAN-103-Boston		An EVPN ELAN service betwee		:	CI VICC			
<ul> <li>Unknown</li> </ul>	Unknown		EVPN-VPLS-100		An EVPN ELAN service over MPLS		1				
<ul> <li>Unknown</li> </ul>	Unknown		EVPN-VPLS-101		EVPN-VPLS another service de		1				
Unknown	Unknown		EVPN-VPLS-102-Boston		A new EVPN ELAN service		:				
4						▶ (	•				
Last Refresh : Oct 15, 2024, 12:05:46 PM GMT+5:	30 (Local Time)		K	< Page:	1 /1 > >1				То	tal Row I	Count: 4
Total Service Count : 4 Deployed : 4											

END OF STEPS

# 1.10 Service stitching – IES services

# 1.10.1 Service stitching algorithm for IES services

The following are the service stitching algorithm for IES services with their stitching criteria:

Algorithm	Stitching Criteria				
service-name	matching service-name				

### 1.10.2 IES service stitching with service-name algorithm

Services which are to be stitched with service-name algorithm should have same service names on the end sites.

1 –

```
Stitch the IES service created on MD NE using the following API:
POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)
BODY:
```

```
{
    "input":{
```

```
"service-type":"ies",
        "algorithm": "service-name",
        "sites":["92.168.98.97","92.168.96.215"]
    }
}
RESPONSE:
{
    "response": {
        "status": 0,
        "startRow": 0,
        "endRow": 0,
        "totalRows": 1,
        "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: ies service-name-1528357814456",
        "errors": null
    }
}
```

2 -

Once the IES service stitching is successful, ensure the service gets listed in the NSP Service Management in 'Unknown' state.

	Network Servic	es Platform					
ervice Management	Services	*					
ife Cycle State		Alignment State	Composite Service		Service Nam	:	
	•	•		<b>T</b> _+			
Deployed		O Aligned			IES 28	1	*
Unknown		Unknown			IES 77	:	

END OF STEPS

# 1.11 Service stitching – L3 VPN services

# 1.11.1 Service stitching algorithm for L3 VPN services

The following are the service stitching algorithm for L3 VPN services with their stitching criteria:

Algorithm	Stitching Criteria
route-target	Full mesh: sites must have inverse matching route-target values
	Hub and spoke: sites must have inverse matching route-target values. If the 'hub' site is stitched after the 'spoke' sites, the spoke sites will be merged to the hub site's service. When the algorithm detects the need for one site to be merged, the info will be persisted to the nsp db. In the event of a pod restart, the service merge will resume after the pod is up.
service-name	matching service-name

# 1.11.2 L3 VPN service stitching with route-target algorithm

```
1 -
```

```
Stitch the L3 VPN service created on MD NE using the following API:
POST: (https://{{server}}/restconf/data/nsp-service-intent:stitchservices)
BODY:
{
    "input":{
         "service-type":"13vpn",
         "algorithm": "route-target",
         "sites":["92.168.96.46","92.168.96.190"]
    }
}
RESPONSE:
{
    "response": {
         "status": 0,
         "startRow": 0,
         "endRow": 0,
         "totalRows": 1,
         "data": "Successfully submitted to Job Manager for Service
Stitch processing with Job Name: L3 VPN route-target-1726726571515",
         "errors": null
    }
}
```

#### 2 -

Once the L3 VPN service stitching is successful, ensure the service gets listed in the NSP Service Management in 'Unknown' state.

END OF STEPS

# 1.12 Auto-stitching a brownfield service

### 1.12.1 Auto-stitching

By default, automatic stitching of services is disabled in IBSF. Users can either stitch a service type manually by following the above procedure or enable auto-stitching in which each service type will have a predefined list of supported stitching algorithms that can be selected to run automatically.

The auto-stitching is supported for service-types Eline, Elan, IES, and L3 VPN for the algorithms mentioned in the table below:

Service Type	Algorithm
Eline	vcid, evi, route-target, local and service-name
Elan	vcid, evi, route-target and service-name
IES	service-name
L3 VPN	route-target and service-name

The auto-stitching is disabled by default. The user has to enable the auto-stitching per service-type and specific algorithm type.

The different API calls for auto-stitching are mentioned below.

# 1.12.2 fetch auto-stitch-config:

restconf GET Url: (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/ nsp-service-auto-stitch-config)

restconf GET Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-configs/nsp-service-auto-stitch-config=eline)

### 1.12.3 patch auto-stitch-config:

restconf Patch Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-config=eline)

payload:

```
{
```

```
"admin-state": "unlocked"
        },
        {
            "algorithm": "vcid",
           "admin-state": "locked"
        },
        {
            "algorithm": "route-target",
            "admin-state": "locked"
        },
        {
            "algorithm": "service-name",
            "admin-state": "locked"
        },
        {
            "algorithm": "local",
            "admin-state": "locked"
        }
      1
}
```

# 1.12.4 put auto-stitch-config:

restconf Put Url for service-type (eline): (https://{{server}}/restconf/data/nsp-service-stitch:nsp-service-auto-stitch-config=eline)

payload:

]

}

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

#### Associate a brownfield service to service template 1.13

## 1.13.1 Purpose

}

Perform this procedure to associate a brownfield service to a service template.

Brownfield services created in NFM-P can be brought under the management of NSP by associating the service to a matching service template created in NSP.

# 1.13.2 Steps

1 -

Log in to the NSP as the Service Management user.

From the Service Management, Services view, select a brownfield service.

3 -

2 -

Click **Associate template**.

#### Figure 1-1 Example 1: EPIPE 10



Figure 1-2 Example 2: VPLS 101

ervice Management Service Services ;ife Cycle State Unknown	Alignment State	Composite Service	Service Name T VPLS 101	De:	scription A	Service T	a Template	I T I	i Info States	+ SERVICE	Ģ	1
ife Cycle State ▼ ♥ Unknown	Alignment State	Composite Service	Service Name T VPLS 101	T N/A	scription	Servic	a Template	i T	i Info States			
• Unknown	Unknown		VPLS 101	T N/A	A	T		Ť	States			
Unknown	Unknown		VPLS 101	N/A	A			1	States			
							Action					
							Associate template		Life Cycle State			~
							Resync		Onknown			
							Execute workflow		Alignment State			
							View		Unkilown			
							Open in Object Troubl	ashooting				
							open in object nodo	concounty	General Info			
									Service ID VPLS 101-1-sam			
									NE Service ID 101			
									Service Name VPLS 101			
									N/A			
									Service Type ELAN			
									Customer ID 1			
ast Refresh : Dec 17, 2024, 11:55:58 AM GMT+5:3	30 (Local Time)			18	< Page: 1 /1 >	ы		/	Service Manager ID		Total Row	Count: '

4

Select the corresponding brownfield service template to associate and click CONFIRM.



NOKIA Network Service	es Platform						User: epipe-user 🔹 🕐
Service Management Services	•						+ CREATE O- :
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Service Template	I	(i) Info
•	•	Τ.	τ,	Τ.		Τ,	States
Unknown	Unknown		EPIPE 62	Continental Rail Services Site		÷	
Unknown	Unknown		EPIPE 60	TransCanadian Exploration Ltd		:	Life Cycle State
Unknown	Unknown		EPIPE 12	Continental Rail Services Site		:	• Unknown
Unknown	Unknown		EPIPE 10	TransCanadian Exploration Ltd		:	Alignment State Unknown
Unknown	Unknown					1	
Unknown	Unknown		Associate selected service(s) to	a template ×		1	General Info
Unknown	Unknown		EPIPE Template X			:	
				CANCEL CONFIRM			Service 10 EPIFE 10.2:aarn Berlie 10 Service Name EPIFE 10 Description TransCanadian Exploration Ltd Site A - Calgary Service Type ELINE Customer 10 13
Last Refresh : Aug 21, 2024, 1:51:25 PM GMT+5:30	) (Local Time)			< Page: 1 /1 > >1			Total Row Count: 7
Total Service Count : 7 Deployed : 7							

Figure 1-4 Example 2: VPLS 101

Life Cycle State	Alignment State	Composite Service Service Nam :	(i) Info
•		• T	States
Unknown	Unknown	Associate selected service(s) to a template ×	Life Cuele State
<ul> <li>Deployed</li> </ul>	Aligned	Template Name	Unknown
Unknown	Unknown	EPVN_VPLS_IEMPIATE X	Alignment State
Pull-From-Network-Failed	Aligned		Unknown
Deployed	Aligned	CANCEL CONFIRM	
Deployed	Aligned	EVPN-VPLS-	General Info
Unknown	Unknown	EVPN-VPLS-	Service ID
Unknown	Unknown	EVPN-VPLS- 🗄 👻	VPLS 101:52:sam

5

The service gets associated to the template. It may take a few minutes before it shows up as

#### Aligned and Deployed in the Services list.

Figure 1-5	Example 1:	EPIPE	10
------------	------------	-------	----





	Network Servic	es Platform								User: admin	
ervice Management	Service Services									+ SERVICE O	
ife Cycle State		Alignment State	Composite Service	Service	lame	Description		Service Template	1	(i) Info	
				T	T		т		T		
Deployed		Aligned		VPLS 10	L.	N/A		EVPN_VPLS_Template	:	States	
										Life Cycle State • DeployedDec 17, 2024, 12:10:35 PM GMT+ Alignment State Ø Aligned	5:30
										General Info	
										NE Service ID 101 Service Name	
										VPLS 101 Description N/A	
										Service Type ELAN	
										Customer ID 1	
									• • •	Service Manager ID	
t Refresh : Dec 17, 2024,	12:10:39 PM GMT+5	30 (Local Time)				< Page: 1 /1	> >1			Total	Row C

END OF STEPS -

# 1.14 Modify a brownfield service

#### 1.14.1 Purpose

The following procedure demonstrates how a brownfield Epipe service can be modified through using the example of modifying an endpoint of the service.

## 1.14.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

From the **Service Management, Services** view, select a brownfield Epipe service and choose **Edit** from the **(**Table row actions) menu.

Site A Site B SDP Details	Template Name  EPIPE Template Service Name* EPIPE 10 Customer ID* 13 Job ID	0	Current Life Cycle State Deployed NE Service ID* 10 Description TransCanadian Exploration L		Alignment State Aligned MTU Admin State			
				us site A - Calgary	unlocked	• Cx		
	Site A	×	Site Name Site A - TransCanadian Expl	vration Ltd EPIPE 10	Description TransCanadian Exploration	Ltd Site A - Calgary + ADD		
	Port ID Port 1/1/c2/1	Encep Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		

3 -

In the Edit Service form, delete the existing endpoint of Site A and add a new endpoint. Click **DEPLOY**.

	Site A							
5.arc	MTU							
ails	9208							
	Endpoint					+ ADD		
	Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		
	Port 1/1/c2/2	dot1q	-1	10	unlocked	TransCanadian E 🚦		
	4		IC C Page: 1			► < > Total: 1		
	4		IC C Page: 1	11 > >1		► 4 ► Total: 1		
	<ul> <li>Site B</li> </ul>		IC C Page: 1	II > >		► < ► Total: 1		
	<ul> <li>Site B</li> <li>Device ID</li> </ul>		IC C Page: 1	Vi > 31	Description	► < ► Total: 1		
	Site B Device ID 92.168.96.215	×	IC C Page: 1 Site Name Site 8 - TransCanadian Explo	/1 > >/	Description TransCanadian Exploratio	► < ► Total: 1 n Ltd Site 8 - Toronto		
	С Site B Ренсе 10 92.168.96.215 мти	×	IC C Page: 1 Site Name Site 8 - TransCanadian Explo	/1 > >) ration Ltd EPIPE 10	Description TransCanadian Exploratio	► < ► Total: 1 In Ltd Site B - Toronto		

Login to NFM-P and ensure the service is modified accordingly.

5 —

4 —

Login to the site NE and ensure the service is modified accordingly.

```
6 -
```

Click on the modified service and select **Service Details, Components** from the **(**Table row actions) menu. Ensure they show the modifications correctly.

3HE-20932-AAAA-TQZZA

■ NO <ia netwo<="" p=""></ia>	ork Services Platform							User: epipe-user - 🤊
Service Management >	Service Endpoints	*						0 I
Service Endpoint Name	Description	Service Name	Site Name	Site ID	Network Element	Port Name	Custome :	(i) Info
	Τ	Τ.	Τ.	Τ.	Τ.	Υ.		Name
Port 1/1/c1/1:10.0	TransCanadian Explora	EPIPE 10	Site B - TransCanad	92.168.96.215	Toronto	Port 1/1/c1/1	13	Port 1/1/c2/2:10.0
Port 1/1/c2/2:10.0	TransCanadian Explora	EPIPE 10	Site A - TransCanad	92.168.98.97	Calgary	Port 1/1/c2/2	13	Description TransCanadian Exploration Ltd - Calgary Endpoint
								Service Name EPIPE 10
								Site Name Site A - TransCanadian Exploration Ltd EPIPE 10
								Site ID 92.168.98.97
								Network Element Calgary
								Port Name Port 1/1/c2/2
								Customer ID 13
								Admin State Unlocked
								Operational State Enabled
								Outer Tag 10
4							• • •	Inner Tag
Last Refresh : Aug 23, 2024, 11:14:57	7 AM GMT+5:30 (Local Time)			K	< Page: 1 / 1 > >	4		Total Row Count: 2

END OF STEPS -

# 1.15 Delete a brownfield service

#### 1.15.1 Purpose

Use the following procedure to remove a brownfield service from the network and then delete the service permanently.

## 1.15.2 Steps

1 -

From the **Service Management**, **Services view**, select a service and click (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

2 —

Click **REMOVE** to remove the service from the network.

■ NO <ia network="" service<="" th=""><th>es Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻 🕐</th></ia>	es Platform								User: admin 👻 🕐
Service Management Service Services	•								+ SERVICE 🕞 🗄
Life Cycle State	Alignment State	Composite Service	Service Name		Description		Service Template	:	(i) Info
· ·	-	T	·	T		T	Т		
<ul> <li>Deployed</li> </ul>	Aligned		EPIPE 33		TransCanadian Exploration Lim	n	EPIPE Template		States
							Action Edit Clone View Service Definition Audit config Align	•	Life cycle State   Deployed Dec 30, 2024, 4:44:40 PM GMT+5:30  Alignment State   Aligned
							Unassociate Migrate		General Info
							Resync Execute workflow		Service ID EPIPE 33
							Remove		NE Service ID 33
							Service details Open in Object Troubleshoo	• ting	Service Name EPIPE 33
									Description TransCanadian Exploration Limited
									Service Type ELINE
									Customer ID 1
7								4 1	

The Life Cycle State of the service is changed to Removed.

3

To delete the service permanently, proceed to the next step.

**i** Note: If you prefer, you can leave the service in Removed state so that it can be deployed again later. To re-deploy the service to the network, select the service and click (Table row actions), **DEPLOY**.

4

To delete the service, select the service and click (Table row actions), **Delete**.

■ NO <ia network="" p="" services<=""></ia>	s Platform						User: admin 👻 🤅
Service Management Service Services	•						+ SERVICE 🕞 🗄
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Servi	ice Template :	(i) Info
-	•	T		T	T	Τ	States
O Removed	<ul> <li>Aligned</li> </ul>		EPIPE 33	TransCanadian Exploration Li	m EPIPE	E Template E Action Edit Clone View Service Definition Migrate Resync Execute workflow	Life cycle State   Removed Dec 30, 2024, 4:47:49 PM GMT+5:30  Alignment State   Alignment State
						Delete	General Info
						Service details   Open in Object Troubleshooting	Service ID EPIPE 33 NE Service ID 33
							Service Name EPIPE 33
							Description TransCanadian Exploration Limited
							Service Type ELINE
							Customer ID 1

The Delete Service confirmation dialog opens.

**i** Note: The Delete option only appears if the service is in Removed state.

5

Click DELETE to permanently delete the service from the NSP.

END OF STEPS -

# 2 UCC-12: E-LINE/E-PIPE

# 2.1 Overview

# 2.1.1 Purpose

This chapter describes the process required to configure an Epipe service on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

# 2.1.2 Contents

2.1 Overview	49
Preparation	50
2.2 Prerequisites	50
2.3 Optional: create a restricted Service Management user	52
2.4 Install the required artifact bundles	56
2.5 Configure user access to the required intent types	57
Service Configuration	60
2.6 Import intent types into Service Management	60
2.7 Create a service tunnel template	61
2.8 Create and deploy service tunnels to the network	63
2.9 Create an EPIPE service template	65
2.10 Create and deploy an EPIPE service to the network	67
2.11 Modify or delete an EPIPE service	71
Optional procedures	75
2.12 Generate and execute OAM test suites	75
2.13 Create telemetry subscriptions	77
2.14 Create a telemetry chart and plot statistics	78

# Preparation

# 2.2 Prerequisites

# 2.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for E-LINE/E-PIPE		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i> How do I enable TLS for telemetry and gNMI on_change support? in the <i>NSP System</i> <i>Administrator Guide</i> .	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>serviceActivationAndConfiguration- intentBasedServiceFulfillment</li> <li>networkInfrastructureManagement- basicManagement</li> <li>networkInfrastructureManagement- deviceConfig</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-co-logical-inventory</li> <li>sros-23-7-r1</li> </ul> </li> </ul>

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration)	How do I install an artifact bundle? in the NSP Network Automation Guide	_
NSP product artifact bundle for Service Fulfillment		
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Cards and MDAs provisioning	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the NSP Device Management Guide for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	_
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer
Optional	•	•

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the <i>NSP Device Management</i>	The intent types required for this configuration are:
configuration	Guide.	icm-qos-schedulerpolicy-srqos
SAP OoS Policies		ICM-qos-network-srqos     icm-gos-sepingress-srgos
configuration		<ul> <li>icm-qos-sapegress-srqos</li> </ul>
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation How do I create a logical configuration deployment? in the NSP Device Management Guide.		The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

# 2.3 Optional: create a restricted Service Management user

# 2.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

NSP

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- · Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- · How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

## 2.3.2 Steps

### Create a role

1 \_\_\_\_\_

Log in to the NSP as an administrator.

2 \_\_\_\_\_

Open Users and Security.

3 \_\_\_\_\_

Select **Roles** from the drop-down list on the toolbar.

4 \_\_\_\_\_

Click **+ Create Role**. The Create Role form opens.

5 \_\_\_\_\_

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain any spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	_
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests

7 —

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.

8

Click Create to save your changes and return to the Roles list.

## Create a user group

9 \_\_\_\_\_

Open Users and Security.

10 \_\_\_\_\_

Select **User Groups** from the drop-down list on the toolbar.

11 \_\_\_\_\_

Click **+ Create User Group**. The Create User Group form opens.

12 \_\_\_\_\_

Specify a group name and description in the Identification panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: @ - \_. The User Group Name string must not contain any spaces, including a leading or trailing space.

13 —

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14 -

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

15 —

Click Create to save your changes and return to the User Groups list.

#### Create a user

16 –

Open Users and Security.

17 –

Select **Users** from the drop-down list on the toolbar.

18 —

Click + Create User.

19

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- can be 1 to 40 characters long
- · cannot include a space
- · cannot have a leading or trailing space
- · can include only the following special characters:
  - @ (at sign)
  - - (hyphen)
  - \_ (underscore)
  - . (period)

#### 20 -

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the Show Password option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

#### 21 –

Click Create.

#### Enable user access control

22 —

Open Users and Security, User Groups.

23 —

24 –

Click More Actions, Settings.

In the Access Control Settings form, enable the NSP User Access Control option.

25 —

Click **SAVE** to enable access control.

END OF STEPS

# 2.4 Install the required artifact bundles

#### 2.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

# 2.4.2 Steps

### Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP  $\rightarrow$  23.11  $\rightarrow$  Artifacts  $\rightarrow$  Artifact\_Admin\_Import.

See the description to verify which bundle to download.

## Install the artifact bundle in NSP

2 Log in to the NSP as the Service Management user.

3

Open Artifacts, Artifact Bundles.

4

Click IMPORT & INSTALL.

5 —

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

6

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7

To install a bundle in Imported status, choose **Install bundle** from the **(**Table row actions) menu.

END OF STEPS -

# 2.5 Configure user access to the required intent types

## 2.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

# 2.5.2 Steps

1	
'	Log in to the NSP as an administrator.
2	
Z	Open Network Intents, Intent Types.
3	
-	Select the tunnel and epipe intent types.
Л	
-	Click (Table row actions), <b>User Access</b> to open the User Access form.
5	
5	In the <b>User Access</b> form, choose <b>Grant access to all user groups</b> from the drop-down list at the top right of the form.
	Choose Full access for the user group created in "Create a user group" (p. 54).

NOKIA Network Services Platform						User: -	admin		• (	3
Network Intents Intent Types +						IMPORT	+ CREATE	С I	3	:
Intent Type	User Access Specify which users have intent type ac	cess by choosing th	sir user group(s) below.		×	<u>.</u>				
wavencevprn	Selected intent type(s) (2 intent Type(s) selected)		User Group access permissions Grant access to all user gr	assigned to the se oups 👻	lected intent type(s)					: ^
wavencebackhaul vprn	✔ tunnel	Т	Full access	•	Service Management Grou					-
vpls	✓ epipe	н	Full access		Service Management Group					:
tunnel			Full access	•	admin	ce Management Group, adr				:
tbtsbackhaul										:
redundant-vpls										:
redundant-eline										:
ies										:
redundant-cline										:
evpn-epipe										:
cpipe										:
13-evpn-composite			<		>					:
epipe					CANCEL	ce Management Group, adr				:
evpn-vpls	z released App	roveamisalignme	nts, artifactadmin, Serviceruinii	ment						:
etree	2 released App	rovedMisalignme	nts, ArtifactAdmin, ServiceFulfil	ment						: ,
Auto-refresh OFF Last Refresh: 2024/2/28 12:27:11			IC C Page:	1 /1 >					Col	unt: 64

#### 6 —

Click **SAVE**. The user access is updated.

END OF STEPS -

# Service Configuration

#### 2.6 Import intent types into Service Management

# 2.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 "Install the required artifact bundles" (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the NSP Service Management Guide.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

**i** Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are tunnel and epipe.

# 2.6.2 Steps

4

Log in to the NSP as the Service Management user.

2

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously-defined intent types is displayed.



Note: Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.



**i** Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the NSP Network Automation Guide.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent types to import are:

- tunnel
- epipe

The intent types are imported into service management. This may take a few minutes.

**i** Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

#### 2.7 Create a service tunnel template

# 2.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the NSP Service Management Guide.

For example, the reference procedure in NSP 23.11 is How do I create a tunnel template?.

# 2.7.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

### From the Service Management, Tunnel Templates view, click + CREATE.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	tunnel
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

If required, click + ADD in the Workflows panel to add workflows to the tunnel template. The Add Workflows form opens.

NSP

## **5** –

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

#### 6 —

#### Click ADD.

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

7 —

### Click CREATE.

The tunnel template is created.

END OF STEPS -

NSP

# 2.7.3 Example creation form without a workflow

NO <ia network="" platform<="" services="" th=""><th>i</th><th></th><th></th><th>User: admin 🔹 🕜</th></ia>	i			User: admin 🔹 🕜
Create a tunnel template				
Basic Info	Basic Info			~
Assign Workflows	Template Name*			
	Service Tunnel			
	Description			
	Service lunnel lemplate to be used for creating servi	ce tunnels Epipe services		
	Tunnel Intent Type*	Intent Version*		
	tunner X	2	Lx	
	State*		F	
	Nelebard		-x	
	Config Form"		×	
	Gerauit		^	
	Assign Workflows			
	ASSIGN WORKHOWS			
	Workflow	+	ADD	
	Workflow Name Tunnel Life Cycle State	Tunnel Life Cycle Blocki Case	ns	
	No dat	a to display		
	<		> < >	
	IC C pages	0 /0 > >1		
				CLOSE CREATE

# 2.8 Create and deploy service tunnels to the network

## 2.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

# 2.8.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

Open the tunnel creation form:

- From the Service Management, Service Tunnels view, click + CREATE.
   The Select a tunnel template to start form opens displaying a list of tunnel templates.
- 2. Choose the template you created in 2.7 "Create a service tunnel template" (p. 61). The Create Tunnel form opens with the Template Name parameter populated.
- Configure the parameters, as required.

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

5

4

3

Configure the required Hello parameters.

6

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

7 -

Configure the required parameters.

8

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

9

Perform an audit to verify that the tunnel is deployed correctly:

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

The service tunnel is audited.

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

The Audit Result form closes.

10 -

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS -

# 2.8.3 Tunnel creation example

NO <ia network="" service<="" th=""><th>s Platform</th><th></th><th></th><th></th><th></th><th>User: a</th><th>admin</th><th></th><th>• ⑦</th></ia>	s Platform					User: a	admin		• ⑦
Create Tunnel									
MPLS	Template Name	Source NE ID*		SDP ID*					^
Hello Parameters	Service Tunnel ×	92.168.98.97 ×	0	45					
	Name*	Destination NE ID*							
	Service Tunnel Calgary to Toronto	92.168.96.215 ×	0						
	Description	Admin State		Transport Type					
	SDP for Epipe service from Calgary to Toronto	unlocked +		MPLS 👻 🗔					
	Signaling								
	TLDP * 🗔								
	MPLS								
	Mixed LSP Mode     Enable LOP     Enable BGP Turnel     SP     toTorono_1     X  MTU  9782	SR-05PF							
	Hello Parameters								
	Keep Alive Enabled Hells Request Tineout  Stearing Parameters  Turnel Admin Group  +	Helio Time 60 Kold Down Time		Hello Mesage Longth 100 Mat Drop Count					
					R	leserve Resources	CLOSE	SAVE	DEPLOY

# 2.9 Create an EPIPE service template

## 2.9.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

# 2.9.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

From the Service Management, Service Templates view, click + CREATE.

The Create a service template form opens.

## 3 —

Configure the parameters, as required.

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

#### 4

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

#### 5 –

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

#### 6

#### Click ADD.

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

#### 7 —

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

8

Click **CREATE**.

The service template is created.

END OF STEPS

NOCIA Network Services Platform		User: admin	• ⑦
Create a service template			
Basic Info	Basic Info		,
Assign Workflows	Template Rame*		
	Eppe Service lemplate Description		
	Template for creating basic Epipe services		
	Service Intent Type" Intent Version"		
	epipe X 2 - Cx		
	Released - CR		
	Config Form*		
	default ×		
	Assign Workflows		
	Workflow + ADD		
	Workflow Name Service Life Cycle Service Life Cycle Blocking State Case		
	NO Data to obplay		
	C 3,  ζ ζ pages 0 (0 5 5)		
	Bulk Association		
	Default Service Cetegory		
	ELINE-BASIC - Cx		
		CLO	SECREATE

# 2.10 Create and deploy an EPIPE service to the network

# 2.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an E-Line service?
- How do I audit a service?

## 2.10.2 Steps

1 -

Log in to the NSP as the Service Management user.

2	
-	From the Service Management Services view click + CPEATE
	The Select a service template to start form apone displaying a list of service templates
	The Select a service template to start form opens displaying a list of service templates.
3	
	Click on an E-Line service template from the list.
	The Create Service form opens with the Template Name parameter populated.
	and the second
4	
	Configure the parameters, as required.
	Continue to the Site A panel.
_	
5	
	Configure the required parameters:
	<b>i</b> Note: If site names and descriptions are added, these will take precedence over any
	service name and description specified in Step 4, with the Site A name and description
	taking precedence over Site B. As such, these attributes will be displayed in various
	locations, such as NSP's Model Driven Configurator function and NFM-P.
6	
Ŭ	
	The Add Endneint form energy
	The Add Endpoint form opens.
7	
	Configure the parameters, as required.
8	
	Deform the following to encountry an eccounting policy to be used:
	Perform the lonowing to specify an accounting policy to be used. 1. Click on the Associating Delicy field. The Select Associating Delicy form enous.
	1. Click on the Accounting Policy field. The Select Accounting Policy form opens.
	2. Click on an accounting policy in the list, then click <b>SELECT</b> . The Select Accounting Policy form closes
9	
	Configure the parameters in the Cpu Protection panel, as required.
10	
	If QoS was enabled in Step 9, configure the parameters as required in both the ingress and

egress panels:

11	
	If an IP/IPv6 filter was enabled in Step 9, configure the parameters as required in both the ingress and egress panels:
	Click ADD to add the endpoint.
	The Add Endpoint form closes.
12	
	In the Site B panel, repeat Step 5 to Step 11.
13	
	In the SDP Details panel, click <b>+ ADD</b> .
	The Add SDP form opens.
14	
	Configure the parameters, as required:
	Click <b>ADD</b> to add the SDP binding.
	The Add SDP form closes.
15	
	Click <b>DEPLOY</b> to create the service in a Deployed state.
16	Perform an audit to verify that the service is deployed correctly:
	1. From the <b>Service Management, Services</b> view, click <b>(</b> Table row actions), <b>Audit config</b> in-line with any service.
	The service is audited.
	2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click <b>OK</b> .
	The Audit Result form closes.
17	
	Click (Table row actions), <b>Align</b> , and then either <b>Push to network</b> or <b>Pull from network</b> in- line with the previously audited service.
	The service is synchronized with the network.
Eve	
	/ UF SIEPS

	Network Services Platform						User: admin	• (?
Create Service								
Site A	Template Name		Service Name*		NE Service ID*			
Site B	EPIPE Template API	×	Epipe 60 - Calgary to Toront	to - API	60			
SDP Details	мти		Customer ID*		Description			
	9208		13	× 0	Epipe 60 for TransCanadia	n Exploration Ltd created via A		
	Admin State		Job ID					
	unlocked	• Cx						
	Site A							
	Device ID		Site Name Description					
	92.168.98.97	92.168.98.97 × 0		Site A - TransCanadian Exploration Ltd EPIPE 60		on Ltd Site A - Calgary		
	мти							
	Endpoint				+ ADD			
	Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		
	Port 1/1/c2/1	dot1q	-1	60	unlocked	TransCanadian E		
	<					> < >		
			IC C Page:	1 /1 > >		Total: 1		

Site B	Device ID		Site Name		Description			
Details	92.168.96.215	× 0	Site B - TransCanadian Expl	oration Ltd EPIPE 60	TransCanadian Exploration	Ltd Site B - Toronto		
	мти							
	Endpoint					+ ADD		
	Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		
	Port 1/1/c1/1	dot1q	-1	60	unlocked	TransCanadian E		
	¢					> < >		
	<		IK K Pager 1	M > >		) ( ) Totel: 1		
	<ul> <li>SDP Details</li> </ul>		IC C Pager 1	N > >I		> C > Total: 1		
	< SDP Details 509		IC C Pager 1	N > 9I		> < > Total: 1 + ADD		
	SDP Details 50* Admin State	Source Device ID	IC C Page 1	11 > >  Steering Parameter	SDP ID	> < > Total:1 + ADD Description		
	< SDP Details 30% Admin State	Source Device ID	IC C Page 1 Destination Device 10	71 > >  Steering Parameter	SDPID	> < > Total: 1 + ADD Description		
	< SDP Details sov Admin State unlocked	Source Device ID	JC C Page 1 Destination Device 10 92.168.98.97	73 > >  Steering Parameter	SDPID 61	Total: 1 + ADD Description TransCanadian [ ]		
	< SDP Details SOP Admin State unlocked unlocked	Spurce Device ID 92.168.96.215 92.168.98.97	C C Press: 1 Destination Device 10 92.168.98.97 92.168.96.215	/1 > >1	SDP 10 61 61	Total: 1 Total: 1 + ADD Description TransCanadian I: TransCanadian I:		
	< SDP Details SDP Admin State unlocked unlocked <	Source Device ID 92.168.96.215 92.168.98.97	IC C Page: 1 Destination Device 10 92.168.98.97 92.168.96.215	/1 > >] Steering Parameter	SOPIO 61 61	ADD Description TransCanadian E TransCanadian E		

■ NO <ia network="" servi<="" th=""><th>ces Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin</th><th>•</th><th>(?)</th></ia>	ces Platform									User: admin	•	(?)
Service Management Services	•									+ CREATE	Ģ	:
Life Cycle State	Alignment State	Composite Service	Service Name	, i	Description			Ser	:	(i) Info		
•	· · · ·	T		T			τ			States		ľ
Deployed	Aligned		Epipe 60 - Calgary to Toronto - API		Epipe 60 for TransCanadian Exploration Lto	d created via API		EPI	:			
Deployed	Aligned		Epipe 61 - Seattle to Boston - API	1	Epipe 61 for Keller Construction created	Action Edit				Life Cycle State		~
Deployed	Aligned		Epipe 62 - Calgary to Boston - API		Epipe 62 for Continental Rail Services cre	Clone				<ul> <li>Deployed Apr 15, 2024, 9:50:48</li> </ul>	AM EDT	2
Deployed	Aligned		EVPN-VPLS-100		An EVPN ELAN service over MPLS	View Service Defi	inition			Alignment State		~
						Audit config				Aligned		
						Unassociate Migrate				General Info		
						Resync Execute workflov Remove	N			Service ID Epipe 60 - Calgary to Toronto - API NE Service ID		
						View Consiste dotaile				60		
						Open in Object T	roubles	hootinj	g	Service Name Epipe 60 - Calgary to Toronto - API		
								24		Epipe 60 for TransCanadian Exploration Ltd via API	created	t
Last Refresh : Apr 19, 2024, 2:07:57 PM EDT (Loca	al Time)		R	< Pa	ge: 1 /1 > >					Service Type	tal Row C	Count: 4
Total Service Count : 4 Deployed : 4												

# 2.10.4 Services Table row actions menu showing audit and align

# 2.11 Modify or delete an EPIPE service

# 2.11.1 Purpose

Use this procedure if needed to modify configured parameters for an Epipe service, or to remove a service from the network and delete it.

# 2.11.2 Steps

# Edit a service

1 –

Log in to the NSP as the Service Management user.

2

From the Service Management, Services view, select a service and choose **Edit** from the (Table row actions) menu.

### 3 —

Modify the service, site, endpoint or SDP parameters as required.

4

Perform one of the following:

- a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.
- b. Click **SAVE** to create the service in a Saved state.
- c. Click **DEPLOY** to create the service in a Deployed state.

	Services Platform						User: a	admin	• ?
Edit Service: Epipe 60 - Calgary	to Toronto - API								
Site A Site B SDP Details	Template Name  EPIPE Template API Service Name* Epipe 60 - Calgary to Toronto - API Custemer ID* 13 Job ID		Corrent Life Cycle State Deployed NE Service ID* 60 Description Epipe 60 for TransCanadian Exploration Ltd created via A		Alignment State Aligned 9208 Admin State unlocked • 2				Î
	Site A								
	Device ID 92.158.98.97 × HTU Endpoint		Site Name Site A - TransCanadian Exploration Ltd EPIPE 60		Description TransCanadian Exploration Ltd Site A - Calgary				
						+ ADD			
	Port ID	Епсар Туре	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description			
	Port 1/1/c2/1	dot1q	-1	60	unlocked	TransCanadian E			
							Reserve Resources	CLOSE MODIFY	DEPLOY

## **Delete a service**

5

From the **Service Management**, **Services view**, select a service and click (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

6 —

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.
7 If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.
8 To delete the service, select the service and click i (Table row actions), Delete. The Delete Service confirmation dialog opens.

**i** Note: The Delete option only appears if the service is in Removed state.

Click DELETE to permanently delete the service from the NSP.

END OF STEPS

9

# 2.11.3 Examples showing remove and delete

■ NOKIA Network Service	es Platform						User: admin 👻	?
Service Management Services	•						+ CREATE 📿	:
Life Cycle State	Alignment State	Composite Service	Service Name	Description		Ser 🚦	i Info	
•	•	T	Т		T		States	
<ul> <li>Deployed</li> </ul>	Aligned		Epipe 60 - Calgary to Toronto - API	Epipe 60 for TransCanadian Exploration	Ltd created via API	EPI :		
<ul> <li>Deployed</li> </ul>	<ul> <li>Aligned</li> </ul>		Epipe 61 - Seattle to Boston - API	Epipe 61 for Keller Construction created	via API	EPI 🚦	Life Cycle State	~
<ul> <li>Deployed</li> </ul>	<ul> <li>Aligned</li> </ul>		Epipe 62 - Calgary to Boston - API	Epipe 62 for Continental Rail Services cr	eated via API	EPI 🚦	<ul> <li>Deployed Apr 19, 2024, 2:21:24 PM ED</li> </ul>	T
<ul> <li>Deployed</li> </ul>	Aligned		Epipe 63 - Seattle to Toronto	Epipe 63 for Core Drilling Inc.		EPII 🚦	Alignment State	~
<ul> <li>Deployed</li> </ul>	Aligned		EVPN-VPLS-100	An EVPN ELAN service over MPLS	Action Edit		Aligned	
					Clone View Service Definition Audit config		General Info	
					Align Unassociate	•	Service ID Epipe 63 - Seattle to Toronto	
					Migrate Resync		NE Service ID 63	
					Execute workflow Remove		Service Name Epipe 63 - Seattle to Toronto	
					View Service details	,	Description Epipe 63 for Core Drilling Inc.	
<					Open in Object Trouble	shooting	Service Type	
Last Refresh : Apr 19, 2024, 2:21:25 PM EDT (Local	Time)		K K	Page: 1 /1 > >			Total Row	Count: 5
Total Service Count : 5 Deployed : 4	Removed : 1							

■ NO <ia network="" p="" serv<=""></ia>	ices Platform					User: admin - ?
Service Management Services	•					+ CREATE C+ :
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Ser	(i) Info
•	•	T	•	T	T	States
<ul> <li>Deployed</li> </ul>	Aligned		Epipe 60 - Calgary to Toronto - API	Epipe 60 for TransCanadian Exploration	Ltd created via API EPI	
<ul> <li>Deployed</li> </ul>	Aligned		Epipe 61 - Seattle to Boston - API	Epipe 61 for Keller Construction created	d via API EPII	Life Cycle State 🗸 🗸
<ul> <li>Deployed</li> </ul>	Aligned		Epipe 62 - Calgary to Boston - API	Epipe 62 for Continental Rail Services c	reated via API EPI	Deployed Apr 19, 2024, 2:17:06 PM EDT
O Removed	Aligned		Epipe 63 - Seattle to Toronto	Epipe 63 for Core Drilling Inc.	EPII 🚦	Alignment State
<ul> <li>Deployed</li> </ul>	Aligned		EVPN-VPLS-100	An EVPN ELAN service over MPLS	Action Edit	Aligned
					Clone View Service Definition Migrate Resync Execute workflow Delete View Service details Open in Object Troubleshooting	General Info Service ID Epipe 63 - Seattle to Toronto NE Service ID 63 Service Name Epipe 63 - Seattle to Toronto Description Epipe 63 for Core Drilling Inc. Service Type
Last Refresh : Apr 19, 2024, 2:19:46 PM EDT (Loc	al Time)			( Page: 1 /1 > >)	>	Total Row Count: 5
Total Service Count : 5 Deployed : 5	rvice Count : 5 Deployed : 5					

# **Optional procedures**

# 2.12 Generate and execute OAM test suites

# 2.12.1 Purpose

Use one of the procedures in this section to generate and execute an OAM test suite against objects of a service. The procedures are based on the procedures for the following:

- Configuring an OAM test suite for a service, in the NSP Network and Service Assurance Guide
- Creating an OAM test suite, in the NSP Data Collection and Analysis Guide

For example, the reference procedures in NSP Release 23.11 are:

- · How do I configure an OAM test suite for a service?
- How do I create an OAM test suite?

# 2.12.2 Steps

# Create an OAM test suite from the Object Troubleshooting dashboard

1 Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open Object Troubleshooting and select a service to test.

3 \_\_\_\_\_

### Click Create OAM Test Suite.

The Select Service Type Endpoints form opens.

4 ——

Select the endpoints you want to test and click Select.

5 \_\_\_\_\_

In the Generate OAM Tests form, specify a unique name and a description for the test suite and configure parameters as required.

6 \_\_\_\_\_

Generate the test suite.

- a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.
- b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

NSP

# Create an OAM test suite from Data Collection and Analysis Management

7 —

8 —

Open Data Collection and Analysis Management, Test Suites.

- Click + SUITE.
- 9 —

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

10 —

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

11 —

Add one or more entities:

- 1. Choose an entity type from the Entity type drop down.
- 2. Click + SELECT to open a selection form.
- 3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
- 4. Verify the list of entity objects in the Bin and click **SELECT**.
- 5. To change the list of selected entities, repeat the previous steps to re-create the list.

12 —

Click on the Service field if applicable.

- 1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
- 2. Click Tas required to add additional filter criteria.
- 3. Choose entities from the list and click **SELECT**.

13 ——

Configure the test parameters as needed.

14 \_\_\_\_\_

Generate the test suite.

- a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.
- b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

END OF STEPS

# 2.13 Create telemetry subscriptions

# 2.13.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP  $\rightarrow$  23.11  $\rightarrow$  Adaptors  $\rightarrow$  Nokia\_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-1.0. 0-rel.10.zip.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

# 2.13.2 Steps

1 -

Log in to the NSP as the Service Management user.

2

Open Data Collection and Analysis Management, Subscriptions.

3 —

To create a subscription:

1. Click **+** SUBSCRIPTION.

- 2. In the Create Subscription form that opens, configure the General parameters as needed.
  - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
  - The subscription is enabled by default: it will start running immediately. Choose **Disabled** in the **State** field if you want to enable your subscription later.
- 3. In the **Object Filter** field, enter filtering information as needed to filter the collected data. As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
- 4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type you need from the list of matches.

5. When you enter a telemetry type, all counters are enabled by default.

To customize the counters, enable the **Enable notifications and notification counters** check box.

Click **Remove i** to remove a counter.

Click + COUNTERS to add a counter that was removed.

6. Click CREATE.

The subscription begins collection when it is enabled.

END OF STEPS

# 2.14 Create a telemetry chart and plot statistics

### 2.14.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

# 2.14.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 "Create telemetry subscriptions" (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

# 2.14.3 Steps

1 -

# Create a chart

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open the New Chart window:

- From Data Collection and Analysis Visualizations, Telemetry Charts, click + CHART.
- From Data Collection and Analysis Management, Subscriptions, choose a subscription and click (Table row actions), Open in Data Collection and Analysis Visualizations.
- 3

In the window that opens, configure the parameters in the top panel:

- 1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
- 2. From the Time Range drop-down list, choose the amount of historical data to display.
- 3. Click **Combine charts** to plot data from multiple data series on the same chart.
- 4

### Click + DEFINITION.

The telemetry and resource filter definition panels are displayed.

5 -

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the Counters drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

### 8 –

If you need to save the configuration as a chart:

- 1. Click SAVE AS.
- 2. In the window that opens, enter a name for the chart and add a description if needed.
- 3. Click SAVE.

The chart is added to the list.

9 \_\_\_\_\_

Click PLOT.

END OF STEPS -

# 2.14.4 Steps

### Plot an existing chart

-	
-	

To plot an existing chart with no changes:

- 1. Open Data Collection and Analysis Visualizations, Telemetry Charts.
- 2. Choose a chart and click (Table row actions), Chart.
- 2 –

To edit a chart and plot it, choose the chart and click **(**Table row actions), **Edit**.

3 –

Edit the parameters as needed and click **PLOT**.

END OF STEPS -

# 2.14.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ()(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

# 3 UCC-13: C-LINE/C-PIPE

# 3.1 Overview

### 3.1.1 Purpose

This chapter describes the process required to configure a Cpipe service on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS (7750 SR-12) 20.10.R13 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

CPIPE/CLINE creation through NSP Service Management is supported on the following NE types:

- 7750 SR-12, version 21.2R1 or earlier, in classic mode
- 7705 SAR 8/18

See the NSP and NE documentation for more information.

# 3.1.2 Contents

3.1 Overview	81
Preparation	83
3.2 Prerequisites	83
3.3 Optional: create a restricted Service Management user	85
3.4 Install the required artifact bundles	89
3.5 Configure user access to the required intent types	90
Service Configuration	93
3.6 Import intent types into Service Management	93
3.7 Create a service tunnel template	94
3.8 Create and deploy service tunnels to the network	96
3.9 Create a CPIPE service template	98
3.10 Create and deploy a CPIPE service to the network	100
3.11 Modify or delete a CPIPE service	107
Optional procedures	111

3.12 Create telemetry subscriptions	111
3.13 Create a telemetry chart and plot statistics	112

# Preparation

# 3.2 Prerequisites

# 3.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for C-LINE/C-PIPE		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i> How do I enable TLS for telemetry and gNMI on_change support? in the <i>NSP System</i> <i>Administrator Guide</i> .	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>serviceActivationAndConfiguration- intentBasedServiceFulfillment</li> <li>networkInfrastructureManagement- basicManagement</li> <li>networkInfrastructureManagement- deviceConfig</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-oc-logical-inventory</li> <li>sros-23-7-r1</li> </ul> </li> </ul>

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the NSP Network Automation Guide	
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	
Cards and MDAs provisioning	ICM process in the NSP Device Management Guide for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the <i>NSP Device Management</i> <i>Guide</i> for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
Channel configuration on access TDM ports	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other procedures in the <i>NSP Device Management</i> <i>Guide</i> for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia. CLI Reference Guides for SR OS	For 7705 SAR-8 and 7705 SAR-18 NEs, channels can be configured using Device Configuration in NSP. The intent type required for this configuration is icm-equipment-port-access-ce. For all other NE types, the configuration must be performed using CLI.
OSPF/ISIS	CLI Reference Guides for SR OS	
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies	How do I create a logical configuration deployment? in the NSP Device Management	The intent types required for this configuration are:
Network QoS Policies	Guide.	<ul> <li>icm-qos-schedulerpolicy-srqos</li> </ul>
		<ul> <li>icm-qos-network-srqos</li> </ul>
SAP QoS Policies configuration		icm-qos-sapingress-srqos
		• icm-qos-sapegress-sirqos
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

# 3.3 Optional: create a restricted Service Management user

# 3.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- · Configuring a role
- Configuring a user group
- Creating an NSP local user

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

# 3.3.2 Steps

### Create a role

1	
	Log in to the NSP as an administrator.
ົ	
2	Open Users and Security.
2	
5	Select <b>Roles</b> from the drop-down list on the toolbar.
4	
Ĵ	Click + Create Role. The Create Role form opens.
5	
J	In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain *any* spaces, including a leading or trailing space.

6

\_.

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	_

Action permissions group item	Permissions	Notes	
Network Intents	Read: Manage Intents	Required to import intent types into Service Management	
Workflows	Read	Required to create service and tunnel templates	
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions	
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests	

7 –

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.

8

Click Create to save your changes and return to the Roles list.

### Create a user group

9 –

Open Users and Security.

10 –

Select User Groups from the drop-down list on the toolbar.

11 -

Click + Create User Group. The Create User Group form opens.

### 12 –

Specify a group name and description in the Identification panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: <sup>®</sup> – \_.

The User Group Name string must not contain any spaces, including a leading or trailing space.

#### 13 -

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

#### 14 –

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

#### 15 —

Click Create to save your changes and return to the User Groups list.

### Create a user

16 –

Open Users and Security.

#### 17 —

Select Users from the drop-down list on the toolbar.

18 —

Click + Create User.

19 -

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- can be 1 to 40 characters long
- · cannot include a space
- · cannot have a leading or trailing space
- · can include only the following special characters:
  - @ (at sign)
  - - (hyphen)
  - \_ (underscore)
  - . (period)

#### **20** –

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the Force User to Change Password option. The new user will be forced to change their password when they first login to NSP.
- Enable the Show Password option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

#### 21 –

Click Create.

### Enable user access control

22 —

Open Users and Security, User Groups.

23 —

24 –

Click More Actions, Settings.

In the Access Control Settings form, enable the NSP User Access Control option.

25 —

Click **SAVE** to enable access control.

END OF STEPS

# 3.4 Install the required artifact bundles

### 3.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

### 3.4.2 Steps

### Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP  $\rightarrow$  23.11  $\rightarrow$  Artifacts  $\rightarrow$  Artifact\_Admin\_Import.

See the description to verify which artifact bundle to download.

### Install the artifact bundle in NSP

2

Open Artifacts, Artifact Bundles.

3

Click IMPORT & INSTALL.

4

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6

To install a bundle in Imported status, choose **Install bundle** from the (Table row actions) menu.

END OF STEPS -

# 3.5 Configure user access to the required intent types

### 3.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

### 3.5.2 Steps

1

Log in to the NSP as an administrator.

### 2 —

### Open Network Intents, Intent Types.

3 \_\_\_\_\_

Select the tunnel and cpipe intent types.

4 —

Click **t** (Table row actions), **User Access** to open the User Access form.

5 \_\_\_\_\_

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose Full access for the user group created in "Create a user group" (p. 54).



6 –

Click **SAVE**. The user access is updated.

END OF STEPS

# Service Configuration

#### 3.6 Import intent types into Service Management

# 3.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 "Install the required artifact bundles" (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the NSP Service Management Guide.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

**i** Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent types required are tunnel and cpipe.

# 3.6.2 Steps

- 1		
	1	

Log in to the NSP as the Service Management user.

2

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously-defined intent types is displayed.



Note: Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.



**i** Note: For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the NSP Network Automation Guide.

3

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent types to import are:

- tunnel
- cpipe

The intent types are imported into service management. This may take a few minutes.

**i** Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

#### 3.7 Create a service tunnel template

# 3.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the NSP Service Management Guide.

For example, the reference procedure in NSP 23.11 is How do I create a tunnel template?.

# 3.7.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

### From the Service Management, Tunnel Templates view, click + CREATE.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	tunnel
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

If required, click + ADD in the Workflows panel to add workflows to the tunnel template. The Add Workflows form opens.

### **5** –

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

### 6 \_\_\_\_\_

### Click ADD.

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

7 —

### Click CREATE.

The tunnel template is created.

END OF STEPS -

# 3.7.3 Example creation form without a workflow

Create a tunnel template					
Basic Info Assign Workflows	Basic Info				
	Tunnel_Template Description				
	Service Tunnel Template				
	Tunnel Intent Type*		Intent Version*		
	tunnel State"	×	2	• Cx	
	Released			• Cx	
	Config Form*				
	default			×	4
	Assign Workflows				
	Workflow			+ ADD	
	Workflow Name	Tunnel Life Cycle State	Tunnel Life Cycle Case	Blocking	
		No data t	o display		
	4			► ( )	•
					CLOSE CREATE

# 3.8 Create and deploy service tunnels to the network

# 3.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

# 3.8.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 –

Open the tunnel creation form:

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

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

- 2. Choose the template you created in 3.7 "Create a service tunnel template" (p. 94). The Create Tunnel form opens with the Template Name parameter populated.
- 3 —

4

Configure the parameters, as required.

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

5 —

Configure the required Hello parameters.

6 –

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

7 –

Configure the required parameters.

8

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

9 –

Perform an audit to verify that the tunnel is deployed correctly:

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

The service tunnel is audited.

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

The Audit Result form closes.

10 -

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS -

# 3.8.3 Tunnel creation example

	letwork Services Platform			User: cpipe-user - (
eate Tunnel				
MPLS	Template Name 🚯	Source NE ID*	SDP ID*	
Iello Parameters	Tunnel_Template ×	92.168.98.141 × 0	31	
	Name*	Destination NE ID*		
	fromCalgaryToToronto	92.168.96.214 × 0		
	Description	Admin State	Transport Type	
	Service Tunnel from Calgary to Toronto	unlocked 👻 🗔	MPLS + E	-x
	Signaling			
	TLDP 🔹 🗔			
	MPLS			
	Mixed LSP Mode			
	Enable LDP Enable BGP Tunnel	SR-ISIS SR-OSPF		
	LSP			
	toToronto_5 ×			
	мти	Metric		
	Hello Parameters			
		Hello Time	Hello Message Length	
	Keep Alive Enabled			
	Hello Request Timeout	Hold Down Time	Max Drop Count	

# 3.9 Create a CPIPE service template

### 3.9.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

# 3.9.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

From the **Service Management, Service Templates** view, click **+ CREATE**. The Create a service template form opens.

### 3 —

Configure the parameters, as required.

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

#### 4

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

### 5 –

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

### 6

### Click ADD.

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

#### 7 —

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

### 8

Click **CREATE**.

The service template is created.

END OF STEPS

# 3.9.3 Example creation form without a workflow

Create a service template		
Basic Info	Basic Info	A
Assign Workflows	Template Name"	
Bulk Association	CPIPE Template	
	Description	
	Template for creating CPIPE services in the NSP GUI	
	Service Intent Type" Intent Version"	
	cpipe x 2 * G	
	State*	
	Released - Lx	
	Config Form*	
	default ×	
	Assign Workflows	
	Workflow Name Service Life Cycle Blocking State Case	
	No data to display	
	CLOSE	CREATE

# 3.10 Create and deploy a CPIPE service to the network

### 3.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create a C-Line service?
- How do I audit a service?

# 3.10.2 Steps

1

Log in to the NSP as the Service Management user.

### 2

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

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

3

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

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

4

Configure the parameters, as required:

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

Continue to the Site A panel.

Configure the required parameters:

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

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

<sup>5</sup> 

### 6 —

# Click + ADD.

The Add Endpoint form opens.

# 7 –

Configure the parameters, as required:

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

#### 8 \_\_\_\_\_

In the CEM panel, configure the parameters as required:

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

#### 9

Configure the parameters, as required:

Parameter	Description
Enable QoS	Specifies whether or not QoS is enabled

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

10 —

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

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

Parameter	Description				
Scheduler Name	Specifies the name of the scheduler				
PIR	Specifies the PIR rate of the scheduler				
CIR	Specifies the CIR rate of the scheduler				

### 11 –

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

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

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

### 12 -

Configure the PW Switching parameters, as required:

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

### 13 —

In the Site B panel, specify the Device ID, then click **+ ADD**. The Add Endpoint form opens.

### 14 —

Repeat Step 5 to Step 12 for Site B.

### 15 —

In the SDP Details panel, click **+ ADD**. The Add SDP form opens.

### 16 —

Configure the parameters, as required:

Parameter	Description
Admin State	Specifies the desired state of the service SDP binding

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

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

#### 17 \_\_\_\_\_

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

#### 18 -

Perform an audit to verify that the service is deployed correctly:

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

The service is audited.

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

The Audit Result form closes.

19 —

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

The service is synchronized with the network.

#### END OF STEPS -

# 3.10.3 Example of a configured service

ate Service									
e A	Template Name		Service Name*		NE Service ID*				
1	Cpipe Template	×	CPIPE-35	CPIPE-35		35			
SDP Details	VC Type*		мти		Customer ID*				
	SATOP E1	- Cx	1514		1		× 0		
	Description		Admin State		Job ID				
	Cpipe Service between Calgary	y and Toronto	unlocked	• Cx					
	Site A								
	Device ID		Site Name		Description				
	Mtu Endpoint				+ ADD				
	Endpoint						+ ADD		
	Endpoint Port Id	Time Slots	Admin State	Description	Enable QoS	Enable IP/IP	+ ADD		
	Endpoint Part Id Channel 1/1/3.e1-1.1	Time Slots	Admin State	Description	Enable QoS false	Enable IP/IP	+ ADD v6 F		



NSP

# 3.10.4 Services Table row actions menu showing audit and align

■ NO <ia network="" p="" service<=""></ia>	ces Platform							User: admin	?
Service Management Services	~							+ CREATE	:
Life Cycle State	Alignment State	Composite Service	Service Name		Description		Service Template	(i) Info	
Deployed	Aligned	T	CPIPE-35	Ŧ	Chine Service between Calgary	T	T Coine Template	States	Í
Deployed	Aligned		CPPE-35		Cpipe Service between Calgary.		Cipite Tempiate : Action Edit Cione View Service Definition Audit config Audit config Unassociate Migrate Resync Execute workflow	Life cycle State • Deployed Apr 22, 2024, 1:48:51 PM GMT+ Alignment State • Aligned General Info Service ID cycle - 35	\$
4							Remove View Service details Open in Object Troubleshooting	NE Service ID 35 Service Name CPIPE-35 Description Cpipe Service between Calgary and Toronto Service Type CLINE Customer ID	
Last Refresh : Apr 22, 2024, 2:52:42 PM GMT+5:30	) (Local Time)			1<	< Page: 1 /1 >	>1		Total I	Row Count: 1

# 3.11 Modify or delete a CPIPE service

### 3.11.1 Purpose

Use this procedure if needed to modify configured parameters for a Cpipe service, or to remove a service from the network and delete it.

# 3.11.2 Steps

# Edit a service

1 -

Log in to the NSP as the Service Management user.

2 -

From the **Service Management**, **Services** view, select a service and choose **Edit** from the (Table row actions) menu.

3

Modify the service, site, endpoint or SDP parameters as needed and click **DEPLOY**.

Edit Service: CPIPE-35							
Site A Site B SDP Details	Template Name  Cpipe Template Service Name* CPIPE-35 MT 1514 Admin State unlocked	• द	Current Life Cycle State Deployed NE Service ID* 35 Custamer ID* 1 Jeb ID	0	Alignment State Aligned VC Type* SATOP E1 Description Cipipe Service between C	algary and Toronto - API	
	Site A Device ID 92.168.98.141 Mtu		Site Name SiteA-Calgary		Description SiteA-Calgary	+ ADD	
	Pert Id Time Slots Channel 1/1/3.e1-1.1 1-32		Time Slots     Admin State     Description       1-32     unlocked		Enable QoS false	Enable IP/IPv6 F	

# **Delete a service**

From the **Service Management**, **Services view**, select a service and click **(**Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

5 –

4

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.

6 -

If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.

7 -

To delete the service, select the service and click (Table row actions), **Delete**. The Delete Service confirmation dialog opens.

**i** Note: The Delete option only appears if the service is in Removed state.
8 —

Click **DELETE** to permanently delete the service from the NSP.

END OF STEPS -

## 3.11.3 Examples showing remove and delete

rvice Management Services - t Cycle State Alignment State Composite Service Service			+ CREATE C
2 Cycle State Alignment State Composite Service Service			
	e Description Service Template	:	() Info
· · · · · ·	т	Т	Unknown
Deployed 🥥 Aligned CPIFE-3	Cpipe Service between Calgary Cpipe Templete Action Edit Cione View Service Dei Audit config Align Unassociate Migrate Resync Execute workflo Remove View Service details Open in Object T	w Troubleshooting	Operational State Disabled Blacking ~ • No VC Type SATOP E1 Job ID Deployer State Success Jub State Success Number of Endpoints 2 Number of Sites 2
		• < •	Number of Tunnel-Bindings 2
t Refresh : Apr 22, 2024, 1:32:56 PM GMT+5:30 (Local Time)	< < Page: 1 / 1 > >		Total Row Count: 1

■ NO <ia network="" p="" servi<=""></ia>	ces Platform								User: admin		0
Service Management Services	•								+ CRE	ATE 📿	:
Life Cycle State	Alignment State	Composite Service	Service Name		Description		Service Template		: i) Info		
• Removed	✓ Aligned	Ť	CPIPE-35	т	Cpipe Service between Calgary.	T	Cpipe Template	T	States		
							Action Edit Clone View Service Definitio Migrate Resync	in :	Life Cycle State O Removed Apr 22, 2024, 1:43 Alignment State Ø Aligned	07 PM GMT+5:	30
							Execute workflow Delete		General Info		
							View Service details Open in Object Troub	leshootin	Service ID CPIPE-35 I8 NE Service ID 35		
									Service Name CPIPE-35 Description Colpe Service between Calgary an	nd Toronto	
									Service Type CLINE		

## **Optional procedures**

## 3.12 Create telemetry subscriptions

## 3.12.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP  $\rightarrow$  23.11  $\rightarrow$  Adaptors  $\rightarrow$  Nokia\_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-1.0. 0-rel.10.zip.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

## 3.12.2 Steps

1 -

Log in to the NSP as the Service Management user.

2

Open Data Collection and Analysis Management, Subscriptions.

3

To create a subscription:

- 1. Click **+** SUBSCRIPTION.
- 2. In the Create Subscription form that opens, configure the General parameters as needed.
  - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.

- The subscription is enabled by default: it will start running immediately. Choose **Disabled** in the **State** field if you want to enable your subscription later.
- 3. In the **Object Filter** field, enter filtering information as needed to filter the collected data. As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
- 4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type you need from the list of matches.

5. When you enter a telemetry type, all counters are enabled by default.

To customize the counters, enable the **Enable notifications and notification counters** check box.

Click **Remove i** to remove a counter.

Click **+ COUNTERS** to add a counter that was removed.

6. Click CREATE.

The subscription begins collection when it is enabled.

END OF STEPS

## 3.13 Create a telemetry chart and plot statistics

## 3.13.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

## 3.13.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 "Create telemetry subscriptions" (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

### 3.13.3 Steps

### **Create a chart**

1 Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open the New Chart window:

- From Data Collection and Analysis Visualizations, Telemetry Charts, click + CHART.
- From Data Collection and Analysis Management, Subscriptions, choose a subscription and click (Table row actions), Open in Data Collection and Analysis Visualizations.

3

In the window that opens, configure the parameters in the top panel:

- 1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
- 2. From the Time Range drop-down list, choose the amount of historical data to display.
- 3. Click Combine charts to plot data from multiple data series on the same chart.

4

Click + DEFINITION.

The telemetry and resource filter definition panels are displayed.

5

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the Counters drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

#### 8 –

If you need to save the configuration as a chart:

- 1. Click SAVE AS.
- 2. In the window that opens, enter a name for the chart and add a description if needed.
- 3. Click SAVE.

The chart is added to the list.

9 \_\_\_\_\_

Click PLOT.

END OF STEPS -

## 3.13.4 Steps

## Plot an existing chart

4	ľ	
	I.	

To plot an existing chart with no changes:

- 1. Open Data Collection and Analysis Visualizations, Telemetry Charts.
- 2. Choose a chart and click (Table row actions), Chart.
- 2 –

To edit a chart and plot it, choose the chart and click **(**Table row actions), **Edit**.

3 –

Edit the parameters as needed and click PLOT.

END OF STEPS -

## 3.13.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ()(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

# 4 UCC-14: E-LAN/EVPN

## 4.1 Overview

### 4.1.1 Purpose

This chapter describes the process required to configure an E-LAN/EVPN service over MPLS on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

**Note:** The terms EVPN-VPLS and E-LAN EVPN are synonymous and are used interchangeably in NSP documentation.

## 4.1.2 Contents

4.1 Overview	115
Preparation	117
4.2 Prerequisites	117
4.3 Optional: create a restricted Service Management user	119
4.4 Install the required artifact bundles	123
4.5 Configure user access to the required intent type	125
Service configuration	127
4.6 Import the intent type into Service Management	127
4.7 Create an EVPN-VPLS service template	127
4.8 Create an E-LAN EVPN (over MPLS) service	130
4.9 Modify the service configuration	132
4.10 Remove the service	132
4.11 Delete the service	133
Optional procedures	134
4.12 Create an OAM test suite	134
4.13 Execute an OAM test suite	136

		_
4.14 View OAM test results	137	
4.15 Delete an OAM test suite	139	
4.16 Create a telemetry subscription	140	
4.17 Modify a telemetry subscription	142	
4.18 Plot telemetry statistics	144	
4.19 Delete a telemetry subscription	147	

## Preparation

## 4.2 Prerequisites

## 4.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this process.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for E-LAN/EVPN		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i> How do I enable TLS for telemetry and gNMI on_change support? in the <i>NSP System</i> <i>Administrator Guide</i> .	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>serviceActivationAndConfiguration- intentBasedServiceFulfillment</li> <li>networkInfrastructureManagement- basicManagement</li> <li>networkInfrastructureManagement- deviceConfig</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-oc-logical-inventory</li> <li>sros-23-7-r1</li> </ul> </li> </ul>

Prerequisite	Documentation reference	Notes
<ul> <li>Download the required artifact bundles from the NSP software delivery site:</li> <li>NSP predefined set for ICM (device configuration)</li> <li>NSP product artifact bundle for Service Fulfillment</li> </ul>	How do I install an artifact bundle? in the <i>NSP Network Automation Guide</i>	
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Cards and MDAs provisioning	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the NSP Device Management Guide for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	_
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer
Optional		

Prerequisite	Documentation reference	Notes		
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>		
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>		
Segment Routing	CLI Reference Guides for SR OS	—		
Scheduler QoS Policies Network QoS Policies configuration SAP QoS Policies	How do I create a logical configuration deployment? in the <i>NSP Device Management</i> <i>Guide</i> .	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos		
		icm-qos-sapegress-srqos		
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.		
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access		

## 4.3 Optional: create a restricted Service Management user

## 4.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide* and *NSP Network Automation Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- · Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- · How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

## 4.3.2 Steps

### Create a role

1 \_\_\_\_\_

Log in to the NSP as an administrator.

2 Open Users and Security.

3 \_\_\_\_\_

Select **Roles** from the drop-down list on the toolbar.

4 \_\_\_\_\_

Click **+ Create Role**. The Create Role form opens.

5 —

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain any spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests
Service Fulfillment	Read / Write / Execute	_
Workflows	Read	Required to create service and tunnel templates

7 —

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.

8

Click **CREATE** to save your changes and return to the Roles list.

## Create a user group

9 \_\_\_\_\_

Open Users and Security.

10 \_\_\_\_\_

Select **User Groups** from the drop-down list on the toolbar.

11 \_\_\_\_\_

Click **+ Create User Group**. The Create User Group form opens.

12 \_\_\_\_\_

Specify a group name and description in the Identification panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: @ - \_. The User Group Name string must not contain spaces, including a leading or trailing space.

13 —

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14 –

Enable the check box for the role you configured in "Create a role" (p. 120) and click **Done**. The role is added to the Selected Roles list.

15 —

Click **CREATE** to save your changes and return to the User Groups list.

### Create a user

16 -

Open Users and Security.

17 —

Select **Users** from the drop-down list on the toolbar.

18 \_\_\_\_\_

Click + Create User.

19 —

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- · can be 1 to 40 characters long
- · cannot include a space
- · cannot have a leading or trailing space
- · can include only the following special characters:
  - @ (at sign)
  - - (hyphen)
  - \_ (underscore)
  - . (period)

20 —

In the User Group field, select the user group you created in "Create a user group" (p. 54).

#### 21 –

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the Show Password option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

#### 22 -

Click CREATE.

### Enable user access control

23 —

Open Users and Security, User Groups.

24 —

Click More Actions, Settings.

25

In the Access Control Settings form, enable the NSP User Access Control option.

#### 26 —

Click **SAVE** to enable access control.

END OF STEPS

## 4.4 Install the required artifact bundles

#### 4.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

## 4.4.2 Steps

## Download the required intent type bundles

1

Download the following artifact bundles from the NSP software delivery site.

- NSP product artifact bundle for Service Fulfillment
- · NSP SR OS vendor-agnostic telemetry adaptation artifact bundle

## Install the artifact bundle in NSP

- 2 Open Artifacts, Artifact Bundles.
  - Click IMPORT & INSTALL.
- 4 –

3 —

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5 —

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6

To install a bundle in Imported status, choose **Install bundle** from the (Table row actions) menu.

END OF STEPS

## 4.4.3 Result

The bundles appear in the Artifacts, Artifact Bundles view:

Artifacts Artifact Bundles 👻											
Automatic reconcile of artifacts and artifact bundles is done every 3 mins. Next reconcile will happen in 2 min 33 sec.											
Bundle Name		Bundle Version		Status	Number of Artifacts		Author		Import Time =		:
	T		T	T		T					
nsp-svc-fulfillment-bundle-2311-v4.zip		23.11.0-SP3		Installed		26	NOKIA R&D		2024/07/29 10:35:57		:
nsp-icm-intent-types-24.0.0-rel.534-cam.zip		24.0.0-rel.534		Installed		47	NOKIA R&D		2024/06/03 08:04:08		:
nsp-mdt-intents-24.4.0-rel.73-tunnel-mapping- bundle.zip		24.4.0		<ul> <li>Installed</li> </ul>		3	NOKIA R&D		2024/05/29 08:56:27		:
nsp-telemetry-cr-va-sros-2.0.0-rel.8.zip		2.0.0		<ul> <li>Installed</li> </ul>		2	NOKIA R&D		2024/05/27 09:51:31		:

The service intent types, including the evpn-vpls intent type which is required for this use case, appear in the **Network Intents**, **Intent Types** view:

Network Intents Intent Types -					IMPORT	+ CREATE	0	:
Intent Type	Version	State	Labels	User Access				:
redundant-vpls	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
redundant-cline	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
13-evpn-composite	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
ies	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
evpn-vpls	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
evpn-epipe	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:

## 4.5 Configure user access to the required intent type

### 4.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

### 4.5.2 Steps

1 \_\_\_\_\_

Log in to the NSP as an administrator.

2 —

3 —

Open Network Intents, Intent Types.

- Select the evpn-vpls intent type.
- 4 \_\_\_\_\_

Click (Table row actions), **User Access** to open the User Access form.

5 —

In the **User Access** form, choose **Grant access to all user groups** from the drop-down list at the top right of the form.

Choose Full access for the user group created in "Create a user group" (p. 54).

#### User Access

Specify which users have intent type access by choosing their user group(s) below.

#### Selected intent type(s)

(1 Intent Type(s) selected)

✓ evpn-vpls		Full
		Full
		Full



CANCEL

SAVE

6 –

Click SAVE. The user access is updated.

END OF STEPS

×

## Service configuration

#### 4.6 Import the intent type into Service Management

## 4.6.1 Purpose

Use this procedure to import the intent types you obtained in 4.4 "Install the required artifact bundles" (p. 123) to the Service Management views. This procedure is based the procedure for importing an intent type into Service Management in the NSP Service Management Guide.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

The intent type required is evpn-vpls.

## 4.6.2 Steps

Log in to the NSP as the Service Management user.

2 -

1 -

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously defined intent types is displayed.

**i** Note: Only intent types that have the Service Fulfillment label applied will be available to import.

3 -

Select the check boxes in-line with the intent types you wish to import and click **IMPORT**.

The intent type to import is evpn-vpls.

The intent type is imported into service management. This may take a few minutes.

| i |

**Note:** Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

#### Create an EVPN-VPLS service template 4.7

## 4.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a **EVPN-VPLS** service.

This procedure is based on the procedure to create a service template in the NSP Service Management Guide.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

## 4.7.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

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

The Create a service template form opens.

3 —

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	evpn-vpls
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	default

4

Select NONE in the Default Service Category drop-down in the Bulk Association panel.

5 —

#### Click CREATE.

The service template is created.

END OF STEPS -

## 4.7.3 Example creation form

LAN (VPLS) over MPLS ser	vices Intent Version* 2		
LAN (VPLS) over MPLS ser	vices Intent Version* 2		
LAN (VPLS) over MPLS ser	vices Intent Version* 2		
×	Intent Version*	•	
×	2	•	
		•	<b>□</b> 3
		•	>
			>
			>
		+ AI	DD
Service Life Cycle State	Service Life Cycle Case	Blocking	
No data t	e display		
	Service Life Cycle State	Service Life Cycle State Service Life Cycle Case No data to display	+ Al Service Life Cycle Service Life Cycle Blocking Case No data to display

## 4.8 Create an E-LAN EVPN (over MPLS) service

## 4.8.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an EVPN VPLS service?
- How do I audit a service?

## 4.8.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 –

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

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

3

Click on the EVPN-VPLS template from the list.

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

4

Configure the parameters, as required:

- · associate sites and endpoints to the service
- · enter MPLS as the EVPN type
- · select the transport protocols to use for tunnel binding
- · associate the desired policies to the service, for example, QoS, CPU Protection

5

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

6

Verify the service details:

1. From the **Service Management, Services** view, select the new service and click (Table row actions), **Service details**, **Components**.

The list of sites in the service is displayed.

- 2. From the drop-down, select **Endpoints**.
- 3. Verify the configuration details for the endpoints.

Service Management >	Service EVPN-VPLS-100 Endpoints +										
Service Endpoint Name	Description	Service Name	Site Name	Site ID	Network Element	Port Name	Customer ID	Admin State	Operational State	Outer Tag Inner Tag	
	т	т	т	т	т	T	т	т	•	T	т
Port 1/1/c2/2:100.0	Endpoint for Service EVPN-VPLS-100	EVPN-VPLS-100	EVPN-VPLS-100	92.168.98.97	Calgary	Port 1/1/c2/2	1	Unlocked	Enabled	100	-1
Port 1/1/c1/2:100.0	Endpoint for Service EVPN-VPLS-100	EVPN-VPLS-100	EVPN-VPLS-100	92.168.96.215	Toronto	Port 1/1/c1/2	1	Unlocked	Enabled	100	-1
1/1/c2/6:100	Endpoint for Service EVPN-VPLS-100	EVPN-VPLS-100	EVPN-VPLS-100	92.168.95.190	Seattle	1/1/c2/6		Unlocked	Enabled	100	-1
1/1/c1/6:100	Endpoint for Service EVPN-VPLS-100	EVPN-VPLS-100	EVPN-VPLS-100	92.168.96.46	Boston	1/1/c1/6		Unlocked	Enabled	100	-1

- 4. From the drop-down, select Map.
- 5. Verify the details in the service map.

Service Management >	Service EVPN-VPLS-100	Мар	•			
Layer						
Service	*					
					<b>Ø</b>	
					Boston 1/1/c1/5:100	
			Ø	N.		
			Calga Port 1/1/c2	ry 12:100.0		
53						
Φ,						Ø
•						Seattle 1/1/c2/6:100
2						
<b>H</b>						
-						
				Port 1/	1/c1/2:100.0	

7

Perform an audit to verify that the service is deployed correctly:

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

The service is audited.

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

The Audit Result form closes.

8

If an object is misaligned, perform an align operation:

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

The service is synchronized with the network.

END OF STEPS

## 4.9 Modify the service configuration

## 4.9.1 Purpose

Perform this procedure to edit a service.

## 4.9.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 —

From the **Service Management, Services** view, click **(**Table row actions), **Edit** in-line with any service. The Edit service form opens.

3 \_\_\_\_\_

Update the parameters as needed and click **DEPLOY**.

4 \_\_\_\_\_

Verify the updated configuration.

END OF STEPS -

## 4.10 Remove the service

## 4.10.1 Purpose

Perform this procedure to remove a service from the network. The service remains in the NSP database and can be re-deployed from the Services view.

## 4.10.2 Steps

1 —

Log in to the NSP as the Service Management user.

2 —

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

#### 3 —

In the form that opens, click **REMOVE** to confirm.

The Life Cycle State of the service is updated to Removed.

END OF STEPS

## 4.11 Delete the service

## 4.11.1 Purpose

Perform this procedure to delete a service. Before a service can be deleted it must be removed from the network; see 4.10 "Remove the service" (p. 132).

## 4.11.2 Steps

# 1 ------

Log in to the NSP as the Service Management user.

## 2 \_\_\_\_\_

From the **Service Management, Services** view, click (Table row actions), **Delete** in-line with any service in the Removed state.

3 –

In the form that opens, click **DELETE** to confirm. The service is deleted.

END OF STEPS -

## **Optional procedures**

## 4.12 Create an OAM test suite

## 4.12.1 Purpose

Use this optional procedure to create a collection of tests that are grouped together to allow for multiple tests to be executed together or run in sequence. The suite includes both the tests and, where applicable, instructions for running tests sequentially or in parallel. Test suites can provide improved automation for OAM testing.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection and OAM testing. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP  $\rightarrow$  23.11  $\rightarrow$  Adaptors  $\rightarrow$  Nokia\_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-1.0.0-rel.10.zip.

This procedure is based on the procedure for creating a test suite in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I create an OAM test suite?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that prerequisites for testing are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?

## 4.12.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2

3

Open Data Collection and Analysis Management, Test Suites.

- Click + SUITE.
- 4 -

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

5 –

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

#### 6

Add one or more entities:

- 1. Choose an entity type from the Entity type drop down.
- 2. Click + SELECT to open a selection form.
- 3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
- 4. Verify the list of entity objects in the Bin and click **SELECT**.
- 5. To change the list of selected entities, repeat the previous steps to re-create the list.
- 7 -

Click on the Service field if applicable.

- 1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
- 2. Click  $\mathbf{T}_{\mathbf{A}}$  as required to add additional filter criteria.
- 3. Choose entities from the list and click **SELECT**.

8

Configure the test parameters as needed.

9

Generate the test suite.

- a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.
- b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

The View Test Suite Details form opens. The Generation Log reports detection or creation of the objects required to run the test against the EVPN-VPLS service onto the network. In the following example, the CFM objects required for the tests were detected, and the DMM tests were deployed.

AGGREGATED RESULTS	LIFECYCLE RESULTS	INDIVIDUAL RESULTS	GENERATION LOG	TESTS
Generation state				
<ul> <li>Generation complete</li> </ul>				
Generation logs				
2024-03-25 10:28:40				
12 Tests generated in 1.004s				
2024-03-25 10:28:39				
Detected existing MEP /nsp-eth-cfm-co name='srv:EVPN-VPLS-100']/mep[mep- id='92.168.98.97-lag-Calgary-CE_West	nfig:eth-cfm/domain[ne-id='92.168.98.9 id='4'] on /nsp-service:services/service- 100']	7'][md-admin-name='TEMP_CFM']/associa ayer/elan[service-id='EVPN-VPLS-100']/en	tion[ma-admin- dpoint[endpoint-	
2024-03-25 10:28:39				
Detected existing MEP /nsp-eth-cfm-con name='srv:EVPN-VPLS-100']/mep[mep- id='92.168.96.46-lag-Boston-CE_East:1	nfig:eth-cfm/domain[ne-id='92.168.96.4 id='3'] on /nsp-service:services/service- 00']	6'][md-admin-name='TEMP_CFM']/associa  ayer/elan[service-id='EVPN-VPLS-100']/en	tion[ma-admin- dpoint[endpoint-	
2024-03-25 10:28:39				
Detected existing MEP /nsp-eth-cfm-co name='srv:EVPN-VPLS-100']/mep[mep- id='92.168.96.215-1/1/c1/2:100']	nfig:eth-cfm/domain[ne-id='92.168.96.2 id='2'] on /nsp-service:services/service-l	15'][md-admin-name='TEMP_CFM']/associ  ayer/elan[service-id='EVPN-VPLS-100']/en	iation[ma-admin- dpoint[endpoint-	
2024-03-25 10:28:39				
Detected existing MEP /nsp-eth-cfm-co name='srv:EVPN-VPLS-100']/mep[mep- id='92.168.96.190-1/1/c2/6:100']	nfig:eth-cfm/domain[ne-id='92.168.96.1 id='1'] on /nsp-service:services/service-l	90'][md-admin-name='TEMP_CFM']/associ ayer/elan[service-id='EVPN-VPLS-100']/en	lation[ma-admin- dpoint[endpoint-	
2024-03-25 10:28:39				
Generating /nsp-oam:tests/oam-test:te 100']/endpoint[endpoint-id='92.168.96 100']/endpoint[endpoint-id='92.168.96 100']/endpoint[endpoint-id='92.168.96 100']/endpoint[endpoint-id='92.168.98	sts/cfm-dmm tests for entities : [/nsp-se i.190-1/1/c2/6:100'], /nsp-service:servic i.215-1/1/c1/2:100'], /nsp-service:servic i.64-lag-Boston-CE_East:100'], /nsp-serv 1.97-lag-Calgary-CE_West:100']]	ervice:services/service-layer/elan[service-ic es/service-layer/elan[service-id='EVPN-VPI es/service-layer/elan[service-id='EVPN-VPI ice:services/service-layer/elan[service-id='	J='EVPN-VPLS- LS- EVPN-VPLS-	

10 -

Click on the LIFECYCLE RESULTS tab to verify that the test suite was created successfully.

11 -

Click on the **TESTS** tab to view the list of tests in the suite.

12 –

Click **CLOSE** to return to the Test Suites view. The new test suite appears in the list.

END OF STEPS

## 4.13 Execute an OAM test suite

#### 4.13.1 Purpose

Use this optional procedure to start all the tests in an OAM test suite. For on-demand test suites, there is no need to manually stop the test suite. The test suite will stop automatically based on the test duration value that is assigned to the on-demand delay streaming test template.

This procedure is based on the procedure for stopping or starting a test suite in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I stop or start an OAM test suite?.

## 4.13.2 Steps

1	
'	Log in to the NSP as the Service Management user.
2	
-	Open Data Collection and Analysis Management, Test Suites.
3	
	Choose a test suite and click (Table row actions), <b>Execute</b> .
4	
-	In the form that opens, update the parameters if needed and click <b>EXECUTE</b> . The execution status is updated to Running.
	<b>Tip:</b> Disable the <b>Publish results</b> parameter if you don't need results published to kafka. This may reduce processing impact.
5	
5	To stop a test suite that is running, choose the test suite in the list and click <b>‡</b> (Table row actions), <b>Stop</b> .

The test suite and all associated tests are stopped.

END OF STEPS

#### 4.14 View OAM test results

## 4.14.1 Purpose

Use this optional procedure to view results of OAM tests. The examples in this procedure show a proactive Eth-CFM DMM test suite.

This procedure is based on the procedure to view test results in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I view OAM test suite results?.



**i** Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running, Nokia recommends that you wait a minimum of 5 s before viewing results.

## 4.14.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

Open Data Collection and Analysis Management, Test Suites.

3

2 —

Choose the test suite and click **‡** (Table row actions), **View Details**.

The View Test Suite Details page opens, showing the following:

Tab	Notes
AGGREGATED RESULTS	Each row of the aggregated results table corresponds to an execution of the test suite. Whenever the test suite is successfully started, a new aggregated results row is added. To view the individual results for a specific test suite execution, select the aggregated results row corresponding to the execution you are interested in and click <b>View individual results</b>
LIFECYCLE RESULTS	The LIFECYCLE RESULTS table shows events from the execution of the test suite, such as stop and start timestamps and error events.
INDIVIDUAL RESULTS	The page displays the results of each test executed. By default, the results from the most recent test suite execution are shown, that is, the execution ID from the first row of the aggregated results table is chosen automatically. You can view results for other test suite executions by specifying another execution ID in the <b>Test suite execution ID</b> field or by returning to the AGGREGATED RESULTS tab and clicking <b>View individual results</b> . For more detailed information about a specific test, choose an execution and click <b>View Results</b> . <b>Note:</b> If a test suite was created from the NSP, the tests will all be the same type. If the test suite was created using RESTCONF, multiple test types could be included. To view results from a different type than is currently displayed, choose the telemetry type from the drop down list. See the <b>TESTS</b> tab for a list of tests in the suite.
GENERATION LOG	The page displays log information from the generation of the suite and tests.
TESTS	<ul> <li>The page lists the test identifiers included in the suite.</li> <li>If the test suite is an on-demand suite, the TESTS tab shows the included tests grouped by stage.</li> <li>Stages are executed sequentially, but tests within each stage will be executed either sequentially or in parallel depending on how the stage is configured.</li> <li>For more detailed information about a specific test, double click on an execution or choose an execution and click View Results 2.</li> </ul>

#### UCC-14: E-LAN/EVPN Optional procedures Delete an OAM test suite

															_
EVPN-VPLS-100	CFM DMM Pro	View Test Suite Details													×
AGGREGATED	RESULTS	LIFECYCLE RESULTS	INDIVIDUAL RESULTS	GENERATION LOG		TESTS									
														Refresh Res	ults
Test suite execution ID	Result status	Start time	Finish time	Success rate	Result classifier	Tests executed	Failed executions	Te	ests kipped	Tests timed- out		Tests deleted	Successfu results	ıl	:
168	Stopped	2024-04-02 14	4:18:30 2024-04-02 14:20:49	97.50%	default	1	120	0	0		3	0		117	Ŷ

**4** ·

For more detailed information about a specific test, double click on an execution in the **TESTS** tab or choose an execution and click **View Results** 

EVPN-VPLS-100 CFM	DMM Pro View Test Suite Details											
AGGREGATED RESU	ULTS LIFECYCLE RESULTS	S INC	DIVIDUAL RESULTS	GENERATION LOG		TESTS						
Test suite execution ID 168	SET TEST SUITE EXECUT	TION ID		-								
Last 7 days	telemetry:/base/oam-pm	/eth-cfm-delay-streamin	g •	Test suite execution ID 168							Refres	h Results
Test execution ID	Session name	System ID	Result classification	Time captured	Direction	Metric ID	Delay	Service ID	Reason	Message	Test path	:
382	EVPN-VPLS-100 CFM DMM Pro-5	92.168.96.215	Passed	2024-04-02 14:20:46	Round-trip	fd-average	5722	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
382	EVPN-VPLS-100 CFM DMM Pro-4	92.168.96.215	Passed	2024-04-02 14:20:46	Round-trip	fd-average	6001	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
382	EVPN-VPLS-100 CFM DMM Pro-6	92.168.96.215	Passed	2024-04-02 14:20:40	Round-trip	fd-average	5938	EVPN-VPLS-100			/nsp-oam:tests/oa	an
383	EVPN-VPLS-100 CFM DMM Pro-8	92.168.96.46	Passed	2024-04-02 14:20:40	Round-trip	fd-average	5495	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
383	EVPN-VPLS-100 CFM DMM Pro-7	92.168.96.46	🤣 Passed	2024-04-02 14:20:40	Round-trip	fd-average	5544	EVPN-VPLS-100			/nsp-oam:tests/oi	arr
383	EVPN-VPLS-100 CFM DMM Pro-9	92.168.96.46	🔗 Passed	2024-04-02 14:20:40	Round-trip	fd-average	6296	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
381	EVPN-VPLS-100 CFM DMM Pro-3	92.168.96.190	Passed	2024-04-02 14:20:39	Round-trip	fd-average	6179	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
381	EVPN-VPLS-100 CFM DMM Pro-2	92.168.96.190	🔗 Passed	2024-04-02 14:20:39	Round-trip	fd-average	6066	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
381	EVPN-VPLS-100 CFM DMM Pro-1	92.168.96.190	Passed	2024-04-02 14:20:39	Round-trip	fd-average	6380	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
382	EVPN-VPLS-100 CFM DMM Pro-5	92.168.96.215	Passed	2024-04-02 14:20:36	Round-trip	fd-average	5836	EVPN-VPLS-100			/nsp-oam:tests/oi	arr
382	EVPN-VPLS-100 CFM DMM Pro-4	92.168.96.215	🔗 Passed	2024-04-02 14:20:36	Round-trip	fd-average	6050	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
382	EVPN-VPLS-100 CFM DMM Pro-6	92.168.96.215	Passed	2024-04-02 14:20:30	Round-trip	fd-average	5962	EVPN-VPLS-100			/nsp-oam:tests/oa	arr
383	EVPN-VPLS-100 CFM DMM Pro-9	92.168.96.46	Passed	2024-04-02 14:20:30	Round-trip	fd-average	6303	EVPN-VPLS-100			/nsp-oam:tests/oa	an
383	EVPN-VPLS-100 CFM DMM Pro-8	92.168.96.46	Passed	2024-04-02 14:20:30	Round-trip	fd-average	5503	EVPN-VPLS-100			/nsp-oam:tests/oa	an
<												F ( )

For the example shown, the tests between service endpoints are passing, showing that there are no issues with service connectivity.

END OF STEPS

## 4.15 Delete an OAM test suite

## 4.15.1 Purpose

Use this optional procedure to delete an OAM test suite and all its associated tests from the NSP UI. This action cannot be undone.



Note: Test suites cannot be edited in the NSP UI.

## 4.15.2 Steps

Log in to the NSP as the Service Management user.
 Open Data Collection and Analysis Management, Test Suites.

3 \_\_\_\_\_

Choose a test suite and click (Table row actions), **Delete**.

4 Click **DELETE** in the confirmation dialog to confirm.

The test suite and its tests are deleted from the NSP.

END OF STEPS -

## 4.16 Create a telemetry subscription

## 4.16.1 Purpose

Perform this procedure to set up telemetry collection.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

## 4.16.2 Steps

1 —

Log in to the NSP as the Service Management user.

2 -

Open Data Collection and Analysis Management, Subscriptions.

3 —

#### Click **+** SUBSCRIPTION.

4

In the Create Subscription form that opens, configure the General parameters as needed:

- Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
- The subscription is enabled by default: it will start running immediately.

Create Subscription									
General	General								
Filters & Counters	Name		Description						
	Interface_Subscription_EVPN-VPLS-100	Interface Subscription for SAPs on se							
	Collection Interval (seconds)	Sync-Time (hh:mm)	State		DB Subscriptions				
	15	00:00	Enabled +	□×	Enabled +	C <sub>x</sub>			
	File Subscriptions	Filename Prefix for File Subscriptions							
	Disabled 👻 🗔								

5 -

Configure filters and counters:

- In the **Object Filter** field, enter filtering information as needed to filter the collected data. As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
- 2. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type you need from the list of matches.

3. When you enter a telemetry type, all counters are enabled by default.

To customize the counters, enable the **Enable notifications and notification counters** check box.

Click **Remove** i to remove a counter.

Click + COUNTERS to add a counter that was removed.

This example includes the following:

- · Telemetry Type: telemetry:/base/interfaces/interface
- · Counters:
  - received-octets-periodic
  - received-octets
  - received-unicast-packets
  - received-unicast-packets-periodic
  - transmitted-octets
- Object Filter (2 port objects used by two endpoints of the service): /nsp-equipment:network/ network-element[ne-id='92.168.98.97']/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot

NSP

Create Subscription			×
General	Filters & Counters		
Filters & Counters			
	Object Filter	nent[ne-id='92.168.96.215']/hardware-component/port[component-id='shelf=1	/slot=1/card=1/slot=1/card=1/port=c1/port=2'1
	4		
	Telemetry Type		
	telemetry:/base/interfaces/interface	×	
	Enable notifications and notification counters	+ COUNTERS	
	Counter =		
	received-octets.	ii .	
	received-octets-periodic	Ĩ	
	received-unicast-packets	1	
	received-unicast-packets-periodic	T	
	transmitted-octets		
			CANCEL CREATE
6			
U			
Click	CREATE.		

The subscription appears in the subscriptions list.

Telemetry S	ubscriptions -									
State =	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	File Prefix	Description	:
•	Interface_s ×									
Enabled	Interface_Subscription_EVPN-VPLS-100	telemetry:/base/interfaces/interface	15	00:00	$\checkmark$	$\checkmark$			Interface Subscription for SAPs on service EVPN-VPLS-100	÷

Port throughput statistics from the sites and NEs found by the object filter are received and processed every 15 s (see Collection Interval value). The statistics will remain in the NSP database for a configured period of time, as defined in the ageout policy.

END OF STEPS

# 4.17 Modify a telemetry subscription

## 4.17.1 Purpose

Use this optional procedure to make changes to a telemetry subscription, for example, to change the list of counters.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

## 4.17.2 Steps

Log in to the NSP as the Service Management user.
Open Data Collection and Analysis Management, Subscriptions.
Choose a subscription and click i (Table row actions), Edit.
In the form that opens, update the parameters as needed. In this example, a new description is provided.

Edit Subscription

General	General								
Filters & Counters	Name Interface_Subscription_EVPN-VPLS-100		Description A new Interface Subscription for SAPs on service EVPN-VPLS-100						
	Collection Interval (seconds)	Sync-Time (hh:mm)	State DB Subscription		DB Subscriptions	15			
	15	00:00	Enabled 👻		Enabled -	□_x			
	File Subscriptions Disabled  Notification Topic ns-eg-53157617-3023-4561-8cc6-90fbd5c98	Filename Prefix for File Subscriptions							

5 -

Click UPDATE

The updated subscription appears in the list.

Data Collection and Analysis Management	Subscriptions •							+ SUBSCRIPTION C	:
Telemetry Subscriptions +									
Name	Telemetry Type	Collection Interval	Sync-time (UTC)	Notification Subscriptions	DB Subscrip	File Subscripti	File = Prefix	Description	:
TestSuiteEx_OAM-PM-SLM-accounting	telemetry:/base/oampm-accounting/cfm-slm	300	00:00	$\checkmark$				SLM accounting	:
Interface_Subscription_EVPN-VPLS-100	telemetry:/base/interfaces/interface	15	00:00	$\checkmark$	$\checkmark$			A new Interface Subscription for SAPs on service EVPN-VPLS-100	÷
UCC LSP Egress Path Subscription	telemetry:/base/lsps/lsp-egress-path	10	00:35	$\checkmark$	$\checkmark$			LSP Egress Path subscription for charting LSP path throughput for UCCs 12	:
UCC SAP Ingress Telemetry subscription	telemetry:/base/accounting/complete-service	10	00:10	$\checkmark$	$\checkmark$			SAP Ingress telemetry subscription for charting SAP Ingress throughput for	:
TestSulteEx_OAM-LOOPBACK-RESULT	telemetry:/base/oam-result/loopback-result	10	00:00	$\checkmark$				Loopback result	:
TestSuiteExOAM-LINK-TRACE-RESULT	telemetry:/base/oam-result/link-trace-result	10	00:00	$\checkmark$				Link-trace result	:
TestSuiteExOAM-PM-CFM-delay-streaming	telemetry:/base/oam-pm/eth-cfm-delay-stre	10	00:00	$\checkmark$				CFM DMM streaming	:
TestSuiteExOAM-PM-DMM-bin-acc	telemetry:/base/oampm-accounting/cfm-dm	300	00:00	$\checkmark$				DMM bin accounting	:
TestSuiteEx_OAM-PM-DMM-accounting	telemetry:/base/oampm-accounting/cfm-dm	300	00:00	$\checkmark$				DMM accounting	:
UCC LSP Egress subscription	telemetry:/base/lsps/lsp-egress	10	00:25	$\checkmark$	~			LSP Egress subscription for charting LSP throughput for UCCs 12 and 14 $$	:
UCC Interface Telemetry subscription - API	telemetry:/base/interfaces/interface	10	00:00	$\checkmark$	$\checkmark$			Interface telemetry subscription created via API for charting port throughput	:
UCC Interface Utilization subscription	telemetry:/base/interfaces/utilization	10	00:15	$\checkmark$	$\checkmark$			Interface utilization subscription for charting port utilization for UCCs 12 ar	:
UCC SAP Egress Telemetry subscription	telemetry:/base/accounting/complete-service	10	00:45	~	$\checkmark$			SAP Egress telemetry subscription for charting SAP Egress throughput for L	:

END OF STEPS

## 4.18 Plot telemetry statistics

## 4.18.1 Purpose

Use this optional procedure to plot a chart of telemetry statistics. The steps for charting any type of telemetry statistic are the same: the example shows port throughput statistics.

This procedure is based on the procedure to plot a telemetry chart in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.

## 4.18.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 4.16 "Create a telemetry subscription" (p. 140).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

#### **Chart limit**

Up to 10 objects can be charted at a time. The number of objects is the number of resources returned by the object filter, multiplied by the number of counters.

If your object filter returns one resource, for example, one NE, you can chart up to 10 counters for the resource.
### 4.18.3 Steps



The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

### Create a chart

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open Data Collection and Analysis Management, Subscriptions.

3 ------

Choose a subscription and click **‡** (Table row actions), **Open in Data Collection and Analysis Visualizations**.

Data Collection and Analysis	s Management Subscriptic	ins -						+	
Telemetry Subscriptions	•								
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	File Prefix	Description
•									
Enabled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	~				SLM accounting
Enabled	Interface_Subscription	telemetry:/base/interf	15	00:00	$\checkmark$	~			A new Interface Subscr
Enabled	UCC LSP Egress Path S	telemetry:/base/lsps/l	10	00:35	~	~		🖌 Edit	
<ul> <li>Enabled</li> </ul>	UCC SAP Ingress Telem	telemetry:/base/acco	10	00:10	~	~		Open in Data Collecti     Delete	on and Analysis Visualizations
Enabled	TestSulteEx_OAM-LO	telemetry:/base/oam	10	00:00	~			Delete	coopusceresure :
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-LIN	telemetry:/base/oam	10	00:00	~				Link-trace result
<ul> <li>Enabled</li> </ul>	TestSuiteEx_OAM-PM	telemetry:/base/oam	10	00:00	~				CFM DMM streaming
Enabled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	~				DMM bin accounting
<ul> <li>Enabled</li> </ul>	TestSuiteEx_OAM-PM	telemetry:/base/oamp	300	00:00	~				DMM accounting
Enabled	UCC LSP Egress subscr	telemetry:/base/lsps/l	10	00:25	~	~			LSP Egress subscriptio
Enabled	UCC Interface Telemet	telemetry:/base/interf	10	00:00	~	$\checkmark$			Interface telemetry su
Enabled	UCC Interface Utilizati	telemetry:/base/interf	10	00:15	$\checkmark$	~			Interface utilization su
Enabled	UCC SAP Egress Telem	telemetry:/base/acco	10	00:45	$\checkmark$	$\checkmark$			SAP Egress telemetry

The Data Collection and Analysis Visualizations view opens in a new browser tab.

4

In the window that opens, configure the parameters in the top panel:

- 2. From the **Time Range** drop-down list, choose the amount of historical data to display.
- 3. Click Combine charts to plot data from multiple data series on the same chart.

5		
J		

#### Click + DEFINITION.

The telemetry and resource filter definition panels are displayed.

6 —

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

7 —

Choose counters to display from the **Counters** drop-down list.

8

In the Object Filter field, enter filtering information to filter the collected data.

New Chart Configuration		×			
Collection Interval (seconds)*  15  Combine charts	Time Range Last 12 hours •				
Telemetry & Resource Filter Definitions		+ DEFINITION			
Telemetry Type telemetry (hase /interfaces/interface		×			
Counters					
receives-outes × receives-outes-period: × receives-unicast-paciets × receives-unicast-paciets-period: ×					
1 /nsp-equipment.network/network-element[ne-id="92.168.98.97"]/hardware-componen	t/port[component-id="shelf=1/slot=1/card=1/slot=1/card=1/port=c2/port=2"]/nsp-equipment.network/network-element[ne-id="92.168.96.215"]/hardware-component/port[component-id="shelf=1/slot=1/card=1/slot=1/slot=1/slot=1/card=1/slot=	t=1/c			
<		•			

SAVE AS...

CANCEL PLOT

Save the configuration as a chart:

- 1. Click SAVE AS.
- 2. In the window that opens, enter a name for the chart and add a description.
- 3. Click SAVE.

In a few seconds, the chart is added to the list.

10 -

#### Click PLOT.

NSP begins plotting data. In a few moments, data will be visualized in the chart.

eceived-octets-periodic																										
92.168.96.215 : 1/1/c1/2																										
205																				Historic	al					
****	111111	1111	1111	11111	1111	11111	1111	1111	1111	1111	11111	111	1111	1111	11111	1111	1111	1111	1111	1111	A A	11111	1111	11111	1111	1111
TAAAAAAAAAAA	VVVVVV	VVVV	10000	VVVV	JUUUU	VVVV	VVVV	VVVV	VVVL	IVVVV	VVVV	VVVV	VVVV	VVVV	VVVV	VVVV	UVVV	VVVV	UVVV	VVVV	$\Lambda \Lambda$	JVVVV	VVVV	VVVV	VVVV	VVVV
50																					V					
																					V					
14:12 14:14 14:5	14:18	14.20 1	4.22 14.2	14.26	14:28	14.30	14.32	14,34	14.36	1438	14:40	14;42	14.44	14,40	54,98	14:50	14:52	14:34	14:58	14:58	15:00	55.02	15.94	13.06	15:08	15:10
92.168.98.97 : 1/1/c2/2																										
202																				Historic	al					
A=A A A A A A A A A A A	****	1111			1111		1111	1111	1111	NAA A	1111	1111	***	1111	1111	1111	1111	****	1111	1111	1 1	****	1111	1111	1111	1111
	UVVVVV	JVVVV	VVVVV	VVVVV	VVVV	VVVV	JVVV	JVVVI	VVVV	VVVV	VVVVI	IVVV	VVVV	UVVU	VVVV	JVVVI	NVV	MM	NVV	MM	LN	NNNN	JVVV	UVVVI	WW	INNN
CARDON FOR ALL MEDICARD AND A																					V					
50																					V					
1612 1616 141	1618	14:20 1	422 14:2	1626	14-28	14-30	16.52	16.94	1636	14-35	14560	14:42	14:44	16.66	24.98	14:50	14-52	14:54	14:56	14.58		\$5.62	15:04	15:04	15.08	15:10

11 -

Close the chart window. The saved telemetry chart appears in the list, ready to be plotted again as needed.

END OF STEPS

# 4.19 Delete a telemetry subscription

### 4.19.1 Purpose

Use this optional procedure to remove a telemetry subscription from the NSP. This action cannot be undone.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

### 4.19.2 Steps

1 -

Log in to the NSP as the Service Management user.

NSP

#### Open Data Collection and Analysis Management, Subscriptions.

3 -

2 -

To delete a subscription:

Choose a subscription and click **(**Table row actions), **Delete**.

The subscription is removed immediately.



**Note:** Removing a subscription does not remove data from the database. The data collected by the subscription is retained according to the database retention policy.

END OF STEPS

# 5 UCC-15: L3 VPN

# 5.1 Overview

### 5.1.1 Purpose

This chapter describes the process required to configure an L3 VPN service over MPLS on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 24.4 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-24.4.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2404.zip

See the NSP and NE documentation for more information.

### 5.1.2 Contents

5.1 Overview	149
Preparation	151
5.2 Prerequisites	151
5.3 Optional: create a restricted Service Management user	153
5.4 Install the required artifact bundles	157
5.5 Configure user access to the required intent type	159
Service configuration	162
5.6 Import the intent type into Service Management	162
5.7 Create a service tunnel template	162
5.8 Create and deploy service tunnels to the network	164
5.9 Create a VPRN service template	166
5.10 Create and deploy a VPRN service to the network	168
5.11 Modify the service configuration	193
5.12 Remove the service	193
5.13 Delete the service	194
Optional procedures	195
5.14 Create an OAM test suite	195
5.15 Execute an OAM test suite	198

5.16 View OAM test results	199	
5.17 Delete an OAM test suite	201	
5.18 Create a telemetry subscription	202	
5.19 Modify a telemetry subscription	204	
5.20 Plot telemetry statistics	206	
5.21 Delete a telemetry subscription	209	

NSP

# Preparation

# 5.2 Prerequisites

### 5.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this process.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for L3 VPN		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the NSP Installation and Upgrade Guide How do I enable TLS for telemetry and gNMI on_change support? in the NSP System Administrator Guide.	Include the following in your deployment:

Prerequisite	Documentation reference	Notes
<ul> <li>Download the required artifact bundles from the NSP software delivery site:</li> <li>NSP predefined set for ICM (device configuration)</li> <li>NSP product artifact bundle for Service Fulfillment</li> </ul>	How do I install an artifact bundle? in the <i>NSP Network Automation Guide</i>	
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Cards and MDAs provisioning	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the NSP Device Management Guide for further detail. See the NSP Device Configuration Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet
OSPF/ISIS	CLI Reference Guides for SR OS	_
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer
Optional	•	•

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>
Segment Routing	CLI Reference Guides for SR OS	—
Scheduler QoS Policies Network QoS Policies configuration	How do I create a logical configuration deployment? in the <i>NSP Device Management</i> <i>Guide.</i>	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos • icm-qos-network-srqos • icm-qos-sapingress-srqos
configuration		<ul> <li>icm-qos-sapegress-srqos</li> </ul>
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access

# 5.3 Optional: create a restricted Service Management user

### 5.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide* and *NSP Network Automation Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- · Configuring user access to an intent type

For example, the reference procedures in NSP Release 24.4 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- · How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

### 5.3.2 Steps

### Create a role

1 \_\_\_\_\_

Log in to the NSP as an administrator.

2 \_\_\_\_\_

Open Users and Security.

3 \_\_\_\_\_

Select **Roles** from the drop-down list on the toolbar.

4 \_\_\_\_\_

Click **+ Create Role**. The Create Role form opens.

5 —

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain any spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes
Service Fulfillment	Read / Write / Execute	_
Network Intents	Read: Manage Intents	Required to import intent types into Service Management
Workflows	Read	Required to create service and tunnel templates
DCA Management	Read / Write / Execute	Optional: Only required for creating and plotting telemetry subscriptions
OAM Tests	Read / Write / Execute	Optional: Only required for generating and executing OAM tests

7

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.

8

Click **CREATE** to save your changes and return to the Roles list.

#### Create a user group

9 -

Open Users and Security.

10 -

Select **User Groups** from the drop-down list on the toolbar.

11 -

Click **+ Create User Group**. The Create User Group form opens.

**12** —

Specify a group name and description in the **Identification** panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: @ - \_\_.

The User Group Name string must not contain spaces, including a leading or trailing space.

13 -

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14 \_\_\_\_\_

Enable the check box for the role you configured in "Create a role" (p. 154) and click **Done**. The role is added to the Selected Roles list.

15 -

Click **CREATE** to save your changes and return to the User Groups list.

#### Create a user

#### 16 —

Open Users and Security.

17 —

Select **Users** from the drop-down list on the toolbar.

18 ——

Click + Create User.

19 —

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- can be 1 to 40 characters long
- cannot include a space
- cannot have a leading or trailing space
- · can include only the following special characters:
  - @ (at sign)
  - - (hyphen)
  - \_ (underscore)
  - . (period)

# 20 -In the User Group field, select the user group you created in "Create a user group" (p. 155). 21 -In the Password section, specify and confirm a password for the user account. If you want this password to be temporary, enable the Force User to Change Password option. The new user will be forced to change their password when they first login to NSP. • Enable the **Show Password** option to see the password characters as you type them. Click on the Password Requirements link to view a list of minimum security requirements for the password. 22 – Click CREATE. Enable user access control 23 — Open Users and Security, User Groups. 24 – Click More Actions, Settings. 25 -In the Access Control Settings form, enable the NSP User Access Control option. 26 – Click **SAVE** to enable access control. END OF STEPS -5.4 Install the required artifact bundles

### 5.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

# 5.4.2 Steps

1 -

# Download the required intent type bundles

Download the following artifact bundles from the NSP software delivery site.

- NSP product artifact bundle for Service Fulfillment
- NSP SR OS vendor-agnostic telemetry adaptation artifact bundle

### Install the artifact bundle in NSP

2 –

Open Artifacts, Artifact Bundles.

3 —

Click IMPORT & INSTALL.

4

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

5 —

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

6 —

To install a bundle in Imported status, choose **Install bundle** from the (Table row actions) menu.

END OF STEPS -

### 5.4.3 Result

The bundles appear in the Artifacts, Artifact Bundles view:

■ NO <ia network="" platform<="" services="" th=""><th>m</th><th></th><th></th><th></th><th></th><th></th><th>User: admin 🔹 🕜</th><th></th></ia>	m						User: admin 🔹 🕜	
Artifacts Artifact Bundles	•						IMPORT & INSTALL C+ :	
Automatic reconcile of artifacts and artifact bund	lles is done every 3 mins. Nex	xt reconcile will happen in 57 sec.						
Bundle Name	Bundle Name Bundle Version Status		Number of Artif	facts Author	Import Time =		(i) Artifact Bundle Details	
	T	T	Т	T			Select a bundle to see the details	
nsp-icm-intents-24.4.0-cam-bundle.zip	24.4.0	<ul> <li>Installed</li> </ul>		47 NOKIA R&D	2024/10/19 02:00:52	:		
nsp-svc-fulfillment-bundle-2404.zip	24.4.0	Installed		24 NOKIA R&D	2024/10/19 02:00:41	:		
nsp-telemetry-cr-va-sros-2.0.0-rel.9.zip	2.0.0	Installed		2 NOKIA R&D	2024/07/24 03:01:07	:		

The service intent types, including the tunnel and vprn intent types which are required for this use case, appear in the **Network Intents**, **Intent Types** view.

Network Intents Intent Types 🔹					IMPORT	+ CREATE	Ċ,	:
Intent Type	Version	State	Labels	User Access				:
wavencecomposite	2	released	ArtifactAdmin, ServiceFulfillment					:
wavencebackhaul	2	released	ArtifactAdmin, ServiceFulfillment					:
wavencevprn	2	released	ArtifactAdmin, ServiceFulfillment					:
vprn	2	released	$autoAudit, {\it Approved Misalignments}, {\it ArtifactAdmin}, {\it ServiceFulfillment}$	ServiceManagementGroup-API				:
vpls	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:
tunnel	2	released	ApprovedMisalignments, Tunnel, ArtifactAdmin, ServiceFulfillment	ServiceManagementGroup-API				:
redundant-vpls	2	released	ApprovedMisalignments, ArtifactAdmin, ServiceFulfillment					:

# 5.5 Configure user access to the required intent type

### 5.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I configure user access to an intent type?.

### 5.5.2 Steps

1 -

Log in to the NSP as an administrator.

2

Open Network Intents, Intent Types.

3 Ctrl+click to select the tunnel and vprn intent types.
4 Click User Access at the top right of the view to open the User Access form.
5 In the User Access form, choose Grant access to all user groups from the drop-down list at the top right of the form.

Choose Full access for the user group created in "Create a user group" (p. 155).

#### User Access

Specify which users have intent type access by choosing their user group(s) below.

Selected intent type(s) (2 Intent Type(s) selected)

✓ tunnel	

Grant access to all user group	s 🔻	
Full access	•	ServiceManagementGrou
Full access	•	admin
Full access	•	ServiceManagementUser

CANCEL

 $\times$ 

SAVE

Click **SAVE**. The user access is updated.

END OF STEPS -

# Service configuration

# 5.6 Import the intent type into Service Management

### 5.6.1 Purpose

Use this procedure to import the intent types you obtained in 5.4 "Install the required artifact bundles" (p. 157) to the Service Management views. This procedure is based the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I import an intent type into Service Management?.

The intent types required are tunnel and vprn.

### 5.6.2 Steps

Log in to the NSP as the Service Management user.

2 -

1 -

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously defined intent types is displayed.

**i** Note: Only intent types that have the Service Fulfillment label applied will be available to import.

3

Select the check boxes in-line with the intent types you wish to import and click IMPORT.

The intent types to import are tunnel and vprn.

The intent types are imported into service management. This may take a few minutes.

**i** Note: Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

# 5.7 Create a service tunnel template

### 5.7.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a service tunnel.

This procedure is based on the procedure to create a tunnel template in the NSP Service Management Guide.

For example, the reference procedure in NSP 24.4 is How do I create a tunnel template?.

### 5.7.2 Steps

1 –

Log in to the NSP as the Service Management user.

2 -

From the Service Management, Tunnel Templates view, click + CREATE.

The Create a tunnel template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Tunnel Intent Type	tunnel
Intent Version	Specifies which version of the selected tunnel intent type to associated with the template
State	Released
Config Form	Specifies the form to be used for the template

4

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

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the tunnel that will trigger workflow execution
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent tunnel life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent tunnel life cycle state changes

<sup>5</sup> 

### Click ADD.

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

7				
	Click CREATE.			

The tunnel template is created.

END OF STEPS

### 5.7.3 Example creation form without a workflow

NOKIA Network Services Platform	m	User: admin 🔹 🕐
Create a tunnel template		
Basic Info	Basic Info	
Assign Workflows	Template lange       Service Tunnel       Description       Service Tunnel Template using default tunnel intent for VPRN services       Tunnel Intent Type*       tunnel       X       Z       State*       Released       Config Form*       default	
	Assign Workflows	
	Workflow Name     Tunnel Life Cycle     Elocking       State     Case     Blocking	
		CLOSE CREATE

# 5.8 Create and deploy service tunnels to the network

#### 5.8.1 Purpose

Perform this procedure to create service tunnels. The creation of service tunnels is a prerequisite to creation of a service.

This procedure is based on the procedures for creating and auditing a service tunnel in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a service tunnel?
- How do I audit a service tunnel?

### 5.8.2 Steps

Log in to the NSP as the Service Management user.

Open the tunnel creation form:

- From the Service Management, Service Tunnels view, click + CREATE.
   The Select a tunnel template to start form opens displaying a list of tunnel templates.
- 2. Choose the template you created in 5.7 "Create a service tunnel template" (p. 162). The Create Tunnel form opens with the Template Name parameter populated.
- 3 ——

1 \_\_\_\_\_

2 —

Configure the parameters, as required.

4 —

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

5

Configure the required Hello parameters.

6

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

7 \_\_\_\_\_

Configure the required parameters.

8 \_\_\_\_\_

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

9

Perform an audit to verify that the tunnel is deployed correctly:

- From the Service Management, Service Tunnels view, click on the service tunnel in the list, then expand the Alignment State section in the info panel and click AUDIT CONFIG. The service tunnel is audited.
- 2. If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

NSP

The Audit Result form closes.

10 -

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click (Table row actions), **Align**, **Push To Network** in-line with the previously audited service tunnel.

The service tunnel is synchronized with the network.

END OF STEPS

						User: admin	• ()
Create Tunnel							
MDL C	Template Name 🛛	Source NE ID*		SDP ID*			
HIFES	Tunnel Template ×	92.168.98.97	× O	55			
Hello Parameters	Name*	Destination NE ID*					
	Service Template from Calgary to Toronto	92.168.96.215	× O				
	Description	Admin State		Transport Type			
	SDP for VPRN service Calgary to Toronto	unlocked	• 🗔	MPLS	▼ □x		
	Signaling						
	TLDP - Cx						
	MPLS						
	Mixed LSP Mode						
	Enable LDP Enable BGP Tunnel	SR-ISIS SR-OSPF					
	LSP						
	toToronto_1 ×						
	мти	Metric					
	9782						
	Hello Parameters						
		Hello Time		Hello Message Length			
	Keep Alive Enabled	60		100			
	Hello Request Timeout	Hold Down Time		Max Drop Count			
	Steering Parameters						

# 5.8.3 Tunnel creation example

# 5.9 Create a VPRN service template

### 5.9.1 Purpose

Perform this procedure to create the template that Service Management will use in the creation of a VPRN (L3 VPN) service.

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 24.4 is How do I create a service template?.

1 \_\_\_\_\_

### 5.9.2 Steps

Log in to the NSP as the Service Management user.

2 —

From the Service Management, Service Templates view, click + CREATE.

The Create a service template form opens.

3 —

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Service Intent Type	vprn
Intent Version	Specifies which version of the selected service intent type to associated with the template
State	Released
Config Form	default

4

Select L3VPN in the Default Service Category drop-down in the Bulk Association panel.

5 —

Click CREATE.

The service template is created.

END OF STEPS -

# 5.9.3 Example creation form

Basic Info       Basic Info         Assign Workflows       Images Kasan         Buik Association       Images Kasan         Default VPRN Service Template       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Template for Creating Basic VPRN Services       Images Kasan         Default Templa	
asic info asign Workflows uuk Association	
steps Workflows Jik Association  Template Name*  Default VPRN Service Template Default Template for Creating Basic VPRN services  Service Intent Typa* Intent Version*  Uprn X  Seto*  Released Config Form*  default:  X  Assign Workflows	
Default VPRN Service Template   Default VPRN Service Template   Default Template for Creating Basic VPRN services   Service Intent Type*   vpm   vpm   Released   Config Form*   default   Assign Workflows	
Description       Default Template for Creating Basic VPRN services       Service Intent Type*       vpm       x       2       State*       centers form*       default	
Default Template for Creating Basic VPRN services         Sarvice Intent Type*         vpm       2         state*         Released       •         cenfig Ferm*         default       ×	
Service Intent Type*     Intent Version*       vpm     ×       2     ~       State*     ~       Released     ~       Config Ferm*     ×       default     ×	
vpm × 2 · G	
State*       Released       config Form*       default       Assign Workflows	
Released C	
default: × Assign Workflows	
Assign Workflows	
Assign Workflows	
Workflow + ADD	
Workflow Name Service Life Cycle Service Life Cycle Blocking State Case	
No data to display	
IC C pages 0 /0 > >1	
Bulk Association	
Default Service Category	
L3VPN G	

# 5.10 Create and deploy a VPRN service to the network

### 5.10.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a L3 VPN service?
- How do I audit a service?

### 5.10.2 Steps

1 -

Log in to the NSP as the Service Management user.

#### NSP

#### 2 —

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

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

3

Click on a VPRN service template from the list, such as the one created in 5.9 "Create a VPRN service template" (p. 166).

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

4

In the Site Details panel, click **+ ADD**. The Add Site form opens.

#### 5

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the assigned queue group redirect list
VRF Name	Specifies the name of the VRF
Description	Describes the VRF
MTU	Specifies the service MTU
NE Service ID	Specifies the NE service ID
Autonomous System	Specifies the AS number advertised to peers for this router
ECMP	Specifies the maximum number of ECMP routes
Router ID	Specifies the unique identifier of the router in the autonomous system
Export Inactive BGP	Specifies whether or not to export the best BGP route as a VPN-IP route, even if inactive due to a preferred route from another PE
Route Distinguisher Type	Specifies the route distinguisher type
Route Distinguisher	Specifies the route distinguisher
VRF Import	Specifies the name of the VRF import policy
VRF Export	Specifies the name of the VRF export policy

Parameter	Description
BGP IPVPN Admin State	Specifies the BGP IPVPN administrative state. Only applicable on SROS 21.x devices.
Route Target (click + ADD)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value

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

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

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

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

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

Parameter	Description
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether SR policy is enabled for the autobind tunnel
SR OSPF3	Specifies whether segment routing OSPF3 is used for next hop resolution

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

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

Parameter	Description
Log Only	Specifies whether action is taken when the maximum number of multicast routes, held within a VRF context, is reached
Mid Route MCast Threshold	Specifies the mid-level water marker for the number of multicast routes that the VRF holds

9

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

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

10 -

Configure the parameters in the Bgp Vpn Backup panel, as required:

Parameter	Description
Ipv4	Specifies whether or not to allow BGP-VPN to be used as backup for IPv4 prefixes
Ipv6	Specifies whether or not to allow BGP-VPN to be used as backup for IPv6 prefixes

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

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

### 12 —

In the Interface Details panel, click **+ ADD**. The Add Interface form opens.

#### 13

Configure the parameters, as required:

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

#### 14 –

If IS-IS was enabled in Step 11, configure the required parameters in the IS-IS panel:

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

#### 15 —

If OSPF was enabled in Step 11, configure the required parameters in the OSPF panel:

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

If RIP was enabled in Step 11, configure the required parameter in the RIP panel:

Parameter	Description
Group Name	Specifies the group name

#### 17 \_\_\_\_\_

In the IPv4 panel, configure the required parameters:

Parameter	Description
Primary	
Address	Specifies the primary IPv4 address assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary ( <b>+ ADD</b> )	
Address	Specifies the secondary IPv4 address assigned to the interface
Prefix Length	Specifies the secondary IPv4 address prefix length
VRRP ( <b>+ ADD</b> )	
Virtual Router ID	Specifies the virtual router identifier for the VRRP virtual router instance
Passive	Specifies whether or not to suppress the processing of VRRP advertisement messages
Admin State	Specifies the administrative state of VRRP
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
Message Interval	Specifies the interval for sending VRRP advertisement messages
Ping Reply	Specifies whether or not to allow non-owner master to reply to ICMP echo requests
Traceroute Reply	Specifies whether or not to allow non-owner master to reply to traceroute requests
Standby Forwarding	Specifies whether or not to allow standby router to forward traffic

Parameter	Description
Neighbor Discovery	
Timeout	Specifies the timeout for an ARP entry learned on the interface
Retry Timer	Specifies the ARP retry interval
Learn Unsolicited	Specifies whether or not to learn new entries from any received NA message
Proactive Refresh	Specifies whether or not to send a single refresh message before entry timeout
Populate	Specifies whether or not to allow static and dynamic hosts to be populated in system ARP cache
Local Proxy Arp	Specifies whether or not to enable local proxy ARP on interface
Proxy Arp Policy	Specifies the proxy ARP policy name
Populate (click +ADD)	
Route Type	Specifies the type of ARP or ND entries that generate host routes
Route Tag	Specifies the tag value used with the host route from an ARP/ND entry
Limit	
Max Entries	Specifies the maximum number of entries learned on an IP interface
Log Only	Specifies whether or not to generate log entries only if limit is reached
Threshold	Specifies the threshold value that triggers a warning message
BFD	
Admin State	Specifies the administrative state of BFD sessions
Transmit Interval	Specifies the BFD transmit interval over this interface
Receive	Specifies the BFD receive interval over this interface
Multiplier	Specifies the number of consecutive BFD messages missed from the peer

Devenueter	Description
Parameter	Description
Echo Receive	Specifies the minimum echo interval over this interface
Туре	Specifies the local termination point for the BFD session
ICMP - Redirects	
Admin State	Specifies the administrative state of sending ICMP redirect messages
Number	Specifies the maximum number of ICMP redirect messages to send
Seconds	Specifies the time used to limit the number of ICMP redirect messages
ICMP - Unreachables	
Admin State	Specifies the administrative state of sending unreachable messages
Number	Specifies the maximum number of unreachable messages to send
Seconds	Specifies the time used to limit the number of ICMP unreachable messages
DHCP	
Admin State	Specifies the administrative state of DHCP
Server	Specifies the IP addresses for DHCP server requests

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

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

Parameter	Description
Multi Service Site	Specifies the multi service site name

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

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

20 —

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

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

#### 21 -

If QoS was enabled in Step 20, configure the required QoS parameters in both the Ingress and Egress sections:

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

Parameter	Description
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click <b>+ ADD</b> )	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Stat Mode	Specifies the mode of statistics collected by the policer
Policer Override Rate	Specifies the policer override rate
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Overrides (click check box)	
Max rate	Specifies the maximum rate
Min Thresh Separation	Specifies the minimum threshold separation
Priority (click <b>+ADD</b> )	
Priority Level	Specifies the priority level
Mbs Contribution	Specifies the minimum amount of cumulative buffer space allowed
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click + ADD)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Weight	Specifies the relative weight of the scheduler to feed the queue
Cir Weight	Specifies the weight used at the within-CIR port priority level
Aggregate Policer (ingress only)	
Parameter	Description
------------------------------------	--
Rate	Specifies the enforced aggregate rate for all queues
Burst	Specifies the aggregate policer burst
Cir	Specifies the aggregate policer CIR
Cbs	Specifies the aggregate policer CBS
Vlan Qos Policy (egress only)	
Policy Name	Specifies the Egress VLAN QoS policy name
Port Redirect	Specifies whether or not to enable Egress VLAN QoS policy port redirect
Egress Remark Policy (egress only)	
Policy Name	Specifies the Egress Remark policy name
Agg Rate or Percent Agg Rate	Specifies the enforced aggregate rate for all queues

#### 22 -

If a filter was enabled in Step 20, configure the required filter parameters:

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

#### 23

In the Routed VPLS panel, configure the required parameters:

Parameter	Description
VPLS Name	Specifies the name of the VPLS service

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

#### 24 \_\_\_\_\_

In the IPv6 Details panel, configure the required parameters:

Parameter	Description
IPv6 ( <b>+ ADD</b> )	
IPv6 Address	Specifies the IPv6 address assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length

Click **ADD** to add the interface.

The Add Interface form closes.

#### 25 —

In the IP Transports panel, click **+ADD**. The Add IP Transport form opens.

#### **26** —

Configure the parameters, as required:

Parameter	Description
Transport Port ID	Specifies the Transport Port Identifier
Admin State	Specifies the administrative state for this IP Transport entry
Description	Description of this IP Transport
Local Host	

Parameter	Description
Local Host IP Address	Specifies the IP address of the IP Transport Local Host
Local Host Port Number	Specifies the Internet socket port number
Local Host Protocol	Specifies the IP protocol that the Local Host
Session Details	
DSCP	Specifies the Differentiated Services Code Point (DSCP) for all packets sent to Remote Hosts (within the same IP Transport)
Forwarding Class	Specifies the Forwarding Class (FC) for all packets sent to Remote Hosts (within the same IP Transport)
Filter Unknown Host	Specifies whether to allow a connection/session with an unknown remote host
Profile	Specifies the profile marking for all packets sent to Remote Hosts (within the same IP Transport)
ТСР	
TCP Max Retries	Specifies the maximum number of consecutive attempts to establish a TCP connection
TCP Retry Interval	Specifies the period of time between consecutive attempts to establish a TCP connection
TCP In Active Timeout	Specifies the maximum period of time a TCP connection can remain idle before tear-down is initiated
Remote Host (click +ADD)	
Remote Host Id	Specifies the identifier for this IP Transport Remote Host
Name	Specifies the name assigned to this IP Transport Remote Host
Description	Specifies the description of this IP Transport Remote Host
Remote Host Ip Address	Specifies the IP address of the IP Transport Remote Host
Remote Host Port Number	Specifies the number of a TCP or UDP port

Parameter	Description
Check TCP	Specifies the TCP connection test to be initiated

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

The Add IP Transport form closes.

#### 27 –

If eBGP was enabled in Step 11, configure the required parameters:

Parameter	Description	
Loop Detect	Specifies the strategy for loop detection in the AS path	
Peer IP Tracking	Specifies whether or not to enable BGP peer tracking	
Router ID	Specifies the Router ID for the BGP instance in the AS	
Local AS		
As Number	Specifies the Local (or virtual) BGP AS number	
Rapid Withdrawal	Specifies whether or not to send BGP withdrawal UPDATE messages immediately	
Min Route Advertisement	Specifies the minimum time before a prefix can be advertised to peer	
Next Hop Resolution	Specifies whether BGP routes can be used to resolve BGP nexthop	
Best Path Selection		
Compare Origin Validation State	Specifies whether the origin validation state is used in the BGP decision process	
Deterministic MED	Specifies whether paths will be grouped based on AS before MED attribute comparison	
Origin Invalid Unusable	Specifies whether routes that have an origin validation state of 'Invalid' can be used	
Ignore NH Metric	Specifies whether next-hop distance will be ignored during best path selection	
Ignore Router ID	Specifies whether router ID will be ignored during best path selection	

Parameter	Description	
Always Compare MED		
MED Value	Specifies the Always Compare MED context	
Strict AS	Specifies whether MED attributes will be compared from same-neighbor AS routes only	
AS Path Ignore		
IPv4	Specifies whether AS path length will be ignored for unlabeled unicast IPv4 routes	
IPv6	Specifies whether AS path length will be ignored for unlabeled unicast IPv6 routes	
Label IPv4	Specifies whether AS path length will be ignored for labeled unicast IPv4 routes	
Ebgp Ibgp Equal		
IPv4	Specifies whether to consider EBGP and IBGP labeled IPv4 routes equal	
IPv6	Specifies whether to consider EBGP and IBGP labeled IPv6 routes equal	
Label IPv4	Specifies whether to consider EBGP and IBGP unlabeled IPv4 routes equal	
Group (+ ADD)		
Group Name	Specifies the group name	
Damping	Specifies whether BGP route damping is used to reduce route flap	
Authentication Key	Specifies the BGP authentication key for all peers	
Peer AS	Specifies the peer AS number	
Peer IP Tracking	Specifies whether BGP peer tracking is enabled	
Prefix Limit (click <b>+ADD</b> )		
Family	Specifies the address family to which the limit applies	
Maximum	Specifies the maximum number of routes to be learned from a peer	
Threshold	Specifies the percentage threshold that triggers a warning message	

Parameter	Description
Idle Timeout	Specifies the time which BGP peering remains idle before reconnecting
Admin State	Specifies the administrative state of the BGP group
Export (click check box)	
Policy	Specifies the export policy name
Import (click check box)	
Policy	Specifies the export policy name
Туре	Specifies the BGP peer type
Family (click check box)	
Ipv4	Specifies whether or not to add support for the IPv4 address family
Ipv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family
Mcast Ipv4	Specifies whether or not to advertise support for the MCAST-IPv4 address family
Flow Ipv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family
Flow Ipv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family
Mcast Ipv6	Specifies whether or not to advertise support for the MCAST-IPv6 address family
Label Ipv4	Specifies whether or not to advertise support for the label-IPv4 address family
Neighbor ( <b>+ ADD</b> )	
Import Policy	Specifies the import policy name
Export Policy	Specifies the export policy name
IP Address	Specifies the IP address that the neighbor uses to communicate with BGP peers
Group Name	Specifies the group name
Peer AS	Specifies the peer AS number
Admin State	Specifies the administrative state of the BGP neighbor

Parameter	Description	
Split Horizon	Specifies whether to prevent routes being reflected back to best-route peer	
Authentication Key	Specifies the BGP authentication key for peer	
Description	Describes the BGP neighbor	
AS Override	Specifies whether the peer's ASN will be replaced by the local ASN in AS Path	
Туре	Specifies the BGP peer type	
Family (click check box)		
lpv4	Specifies whether or not to add support for the IPv4 address family	
lpv6	Specifies whether or not to advertise MP-BGP support for the IPv6 address family	
Mcast Ipv4	Specifies whether or not to advertise support for the MCAST-IPv4 address family	
Flow Ipv4	Specifies whether or not to advertise support for the flowspec-IPv4 address family	
Flow Ipv6	Specifies whether or not to advertise support for the flowspec-IPv6 address family	
Mcast Ipv6	Specifies whether or not to advertise support for the MCAST-IPv6 address family	
Label Ipv4	Specifies whether or not to advertise support for the label-IPv4 address family	

#### 28 -

If Enable Static Route was enabled in Step 11, click **+ ADD** in the Static Route Details panel. The Add Static Route form opens.

#### 29

Configure the parameters, as required.

Parameter	Description
IP Prefix	Specifies the IP prefix for the static route
Prefix Length	Specifies the prefix length for the static route
Route Type	Specifies the static route type
Тад	Specifies the static route tag

Parameter	Description
Is Blackhole	Specifies whether the prefix is a blackhole route
Next Hop ( <b>+ ADD</b> )	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Тад	Specifies the static route tag
BFD Liveness	Specifies whether or not to use Bidirectional Forwarding Detection on this static route
Admin State	Specifies the administrative state of next hop
Indirect ( <b>+ ADD</b> )	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Тад	Specifies the static route tag
Admin State	Specifies the administrative state of next hop

Click ADD to add the static route.

The Add Static Route form closes.

#### 30 —

If Enable IS-IS was enabled in Step 11, click **+ ADD** in the IS-IS panel. The Add IS-IS form opens.

#### 31 -

Configure the parameters, as required.

Parameter	Description
IS-IS Instance	Specifies the instance ID for the IS-IS instance
Admin State	Specifies the administrative state of the IS-IS instance
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table

Parameter	Description
Level Capability	Specifies the routing level for the instance
Advertise Router Capability	Specifies the router capabilities advertisement to neighbors

Click ADD to add the IS-IS instance.

The Add IS-IS form closes.

#### 32 —

If Enable OSPF was enabled in Step 11, configure the parameters as required:

Parameter	Description
Compatible RFC-1583	Enables OSPF summary and external route calculations
Overload On Boot (click check box)	
Timeout	Specifies the time during which the router operates in overload state before reestablishing normal operations
Export Policy	Specifies the export policies that determine exported routes
Import Policy	Specifies the import policy names for routes from IGP to route table
Timers	
Incremental SPF Wait	Specifies the delay time before an incremental SPF calculation starts
LSA Accumulate	Specifies the delay to gather LSAs before advertising to neighbors
LSA Arrival	Specifies the minimum delay between receipt of same LSAs from neighbors
Redistribute Delay	Specifies the hold down timer for external routes into OSPF
LSA Generate	
Max LSA Wait	Specifies the maximum time between two LSAs being generated
LSA Initial Wait	Specifies the first wait period between OSPF LSA generation
LSA Second Wait	Specifies the hold time between the first and second LSA generation

Parameter	Description		
Spf Wait			
Max SPF Wait	Specifies the maximum interval between two consecutive SPF calculations		
SPF Initial Wait	Specifies the initial SPF calculation delay after a topology change		
SPF Second Wait	Specifies the hold time between the first and second SPF calculation		
Graceful Restart (click check box)			
Helper Mode	Enables graceful restart helper for OSPF		
Strict Lsa Checking	Enables strict LSA checking during graceful restart helper		

#### 33 ——

If Enable RIP was enabled in Step 11, configure the parameters as required:

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

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

#### 34 —

Click **ADD** to add the site.

The Add Site form closes.

#### 35 —

In the SDP Details panel, click **+ ADD**. The Add SDP form opens.

#### 36

Configure the parameters, as required:

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

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

#### 37 -

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

#### 38 -

Perform an audit to ensure that the service is properly deployed.

Perform one of the following to start the audit:

- a. From the **Service Management, Services** view, click (Table row actions), **Audit config** in-line with any service.
  - **Note:** Users can select up to 10 services at a time to run the Audit Config action against.
- b. From the **Service Management**, **Services** view, click on a service in the list, then expand the Alignment State section in the info panel and click **AUDIT CONFIG**.

The service is audited.

#### 39

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

The Audit Result form closes.

40 –

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

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

b.

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

The service is synchronized with the network.

END OF STEPS -

# 5.11 Modify the service configuration

### 5.11.1 Purpose

Perform this procedure to edit a service.

### 5.11.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2 —

From the **Service Management, Services** view, click **(**Table row actions), **Edit** in-line with any service. The Edit service form opens.

3 —

Update the parameters as needed and click **DEPLOY**.

4 \_\_\_\_\_

Verify the updated configuration.

END OF STEPS -

# 5.12 Remove the service

### 5.12.1 Purpose

Perform this procedure to remove a service from the network. The service remains in the NSP database and can be re-deployed from the Services view.

### 5.12.2 Steps

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

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

3 —

1 \_\_\_\_\_

In the form that opens, click **REMOVE** to confirm.

The Life Cycle State of the service is updated to Removed.

END OF STEPS

# 5.13 Delete the service

### 5.13.1 Purpose

Perform this procedure to delete a service. Before a service can be deleted it must be removed from the network; see 5.12 "Remove the service" (p. 193).

### 5.13.2 Steps

1 —

Log in to the NSP as the Service Management user.

2 —

From the **Service Management, Services** view, click (Table row actions), **Delete** in-line with any service in the Removed state.

3 —

In the form that opens, click **DELETE** to confirm. The service is deleted.

END OF STEPS -

NSP

# **Optional procedures**

# 5.14 Create an OAM test suite

### 5.14.1 Purpose

Use this optional procedure to create a collection of tests that are grouped together to allow for multiple tests to be executed together or run in sequence. The suite includes both the tests and, where applicable, instructions for running tests sequentially or in parallel. Test suites can provide improved automation for OAM testing.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection and OAM testing. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP  $\rightarrow$  24.4  $\rightarrow$  Adaptors  $\rightarrow$  Nokia\_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-2.0.0-rel.9.zip.

This procedure is based on the procedure for creating a test suite in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I create an OAM test suite?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that prerequisites for testing are in place. The reference procedure for this in NSP Release 24.4 is: How do I install telemetry artifacts?.

### 5.14.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2

3

Open Data Collection and Analysis Management, Test Suites.

- Click + SUITE.
- 4 -

In the Generate OAM Tests form that opens, choose a Test type.

The list of templates in the Template field is updated based on your selection.

5 –

Choose a test template if needed.

If a template is not selected, an appropriate system template is automatically selected based on the value of the execute type field. If a template is selected, the value of the execute type field is imported from the template and is read-only in the form.

#### 6 -

Add one or more entities:

- 1. Choose an entity type from the Entity type drop down.
- 2. Click **+ SELECT** to open a selection form.
- 3. Choose one or more entity objects from the list to add them to the Bin. Use the page selectors to navigate the list.
- 4. Verify the list of entity objects in the Bin and click **SELECT**.
- 5. To change the list of selected entities, repeat the previous steps to re-create the list.
- 7 –

Click on the Service field if applicable.

- 1. Select an attribute in the drop-down list, then enter values for that attribute in the field. As you type, the list is filtered for entities that match your input.
- 2. Click Tas required to add additional filter criteria.
- 3. Choose entities from the list and click **SELECT**.

8

Configure the test parameters as needed.

9

Generate the test suite.

a. To automatically execute the test suite after generation, enable Execute and click **GENERATE & EXECUTE**.

Generate OAM Tests										×
Test type										
Twamp-light		*								
Entity type										
L3 VPN Endpoint		*								
Service										
94 VPRN123										
L3 VPN Endpoints										+ SELECT
Endpoint ID	Name	Admin state	Operational state	Site name	Site ID	Service ID	IPv4 Addresses	IPv6 Addresses		1
92.168.98.97-VPRN123-VPRN	VPRN123Calgaryl	unlocked	enabled	VPRN123	92.168.98.97	VPRN123	12.30.3.1/24			н.
92.168.96.215-VPRN123-VPR	VPRN123Toronto	unlocked	enabled	VPRN123	92.168.96.215	VPRN123	12.30.2.1/24			Ŧ
Template										
Delay Streaming (proactive)		•								
Test suite name 🔘										
VPRNTwamp										
Test suite description 🔘										
VPRN Twamp Test Suite										
App ID 📵										
NSP										
Execute type										
Proactive										
Bidirectional ()										
Execute @										,
									CANCEL	GENERATE & EXECUTE

b. To create the test suite without automatically executing, disable Execute and click **GENERATE**.

The View Test Suite Details form opens. The Generation Log reports creation of the TWAMP objects required to run the test against the VPRN service onto the network were deployed.

E NOKIA Network Services Platform User: admin + 🕐					
VPRNTwamp View Test Suite Details			×		
AGGREGATED RESULTS LIFECYCLE RESULTS INDIVIDUAL RESULTS GENERATION LOG	TESTS				
Generation state					
🤣 Generation complete					
Generation logs					
2024-10-18 07:42:30					
2 Tests generated in 0.571s					
2024-10-18 074230 Generating //nsp-oam.test/oam-test.tests/wamp-light tests for entities: [/nsp-services/service-layer/l3vpn[service- id=VPRN1231]/endpoint[endpoint-id='92.168.98.97-VPRN123-VPRN123CajgaryInterface]]/msp-service-services/service-layer/l3vpn[service- id='VPRN1231]/endpoint[endpoint-id='92.168.96.215-VPRN123-VPRN123TorontoInterface]]					

10

Click on the LIFECYCLE RESULTS tab to verify that the test suite was created successfully.

11

Click on the **TESTS** tab to view the list of tests in the suite.

#### 12 –

Click **CLOSE** to return to the Test Suites view. The new test suite appears in the list.

END OF STEPS

# 5.15 Execute an OAM test suite

### 5.15.1 Purpose

Use this optional procedure to start all the tests in an OAM test suite. For on-demand test suites, there is no need to manually stop the test suite. The test suite will stop automatically based on the test duration value that is assigned to the on-demand delay streaming test template.

This procedure is based on the procedure for stopping or starting a test suite in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I stop or start an OAM test suite?.

### 5.15.2 Steps

1	
÷.	
	Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open Data Collection and Analysis Management, Test Suites.

- Choose a test suite and click (Table row actions), **Execute**.
- 4

3

In the form that opens, update the parameters if needed and click **EXECUTE**. The execution status is updated to Running.

**i Tip:** Disable the **Publish results** parameter if you don't need results published to kafka. This may reduce processing impact.

5 –

To stop a test suite that is running, choose the test suite in the list and click (Table row actions), **Stop**.

The test suite and all associated tests are stopped.

END OF STEPS -

#### 5.16 View OAM test results

### 5.16.1 Purpose

Use this optional procedure to view results of OAM tests. The examples in this procedure show a proactive Eth-CFM DMM test suite.

This procedure is based on the procedure to view test results in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I view OAM test suite results?.

**i** Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running. Nokia recommends that you wait a minimum of 5 s before viewing results.

### 5.16.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open Data Collection and Analysis Management, Test Suites.

3 —

Choose the test suite and click (Table row actions), **View Details**.

The View Test Suite Details page opens, showing the following:

Tab	Notes
AGGREGATED RESULTS	Each row of the aggregated results table corresponds to an execution of the test suite. Whenever the test suite is successfully started, a new aggregated results row is added. To view the individual results for a specific test suite execution, select the aggregated results row corresponding to the execution you are interested in and click <b>View individual results</b>
LIFECYCLE RESULTS	The LIFECYCLE RESULTS table shows events from the execution of the test suite, such as stop and start timestamps and error events.

Tab	Notes
INDIVIDUAL RESULTS	The page displays the results of each test executed. By default, the results from the most recent test suite execution are shown, that is, the execution ID from the first row of the aggregated results table is chosen automatically. You can view results for other test suite executions by specifying another execution ID in the <b>Test suite execution ID</b> field or by returning to the AGGREGATED RESULTS tab and clicking <b>View individual results</b> . For more detailed information about a specific test, choose an execution and click <b>View Results</b> . <b>Note:</b> If a test suite was created from the NSP, the tests will all be the same type. If the test suite was created using RESTCONF, multiple test types could be included. To view results from a different type than is currently displayed, choose the telemetry type from the drop down list. See the <b>TESTS</b> tab for a list of tests in the suite.
GENERATION LOG	The page displays log information from the generation of the suite and tests.
TESTS	The page lists the test identifiers included in the suite. If the test suite is an on-demand suite, the TESTS tab shows the included tests grouped by stage. Stages are executed sequentially, but tests within each stage will be executed either sequentially or in parallel depending on how the stage is configured. For more detailed information about a specific test, double click on an execution or choose an execution and click <b>View Results</b>

■ NOCIA Network Services Platform User: admin										•	0
VPRNTwamp	VPRNTwamp View Test Suite Details ×										
AGGREGATED RESULTS LIFECYCLI		LIFECYCLE RESULTS	INDIVIDUAL RESULTS	GENERATION LOG		TESTS					
									Refresh F	lesults	
Test suite execution ID	Result status	Start time	Finish time	Success rate	Result classifier	Tests executed	Failed executions	Tests skipped	Tests timed- out	Tests deleted	:
36	Stopped	2024-10-18 07:42:4	2024-10-18 07:51:45	100.00%	default	108	0		0	0	(

4 -

For more detailed information about a specific test, double click on an execution in the **TESTS** tab or choose an execution and click **View Results** 

VPRNTwamp	View Test Suite D	etails								×
AGGREGATE Test suite execution I 36	D RESULTS	LIFECYCLE RESULTS	INDIVIDUAL RESULTS	GENERATION LOG	TESTS					
Last 7 days	•)	telemetry:/base/oam-pm/twamp-light-de	lay-streaming * 36	ite execution ID						Refresh Results
Test execution ID	Session name	System ID	Result classification	Record stats	Time captured	Direction	Metric ID	Delay	Source IP address	Se į
200	VPRNTwamp -1	92.168.98.97	🥝 Passed	delay	2024-10-18 17:21:38	Round-trip	fd-average	4387	12.30,3.1	
199	VPRNTwamp -2	92.168.96.215	🕑 Passed	delay	2024-10-18 17:21:37	Round-trip	fd-average	4991	12,30.2.1	
200	VPRNTwamp -1	92.168.98.97	📀 Passed	delay	2024-10-18 17:21:28	Round-trip	fd-average	4778	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	📀 Passed	delay	2024-10-18 17:21:27	Round-trip	fd-average	\$115	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	Passed	delay	2024-10-18 17:21:18	Round-trip	fd-average	4573	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	😔 Passed	delay	2024-10-18 17:21:17	Round-trip	fd-average	4987	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	Passed	delay	2024-10-18 17:21:08	Round-trip	fd-average	4701	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	S Passed	delay	2024-10-18 17:21:07	Round-trip	fd-average	5261	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	😔 Passed	delay	2024-10-18 17:20:58	Round-trip	fd-average	4743	12.30.3.1	
199	VPRNTwamp -Z	92.168.96.215	😋 Passed	delay	2024-10-18 17:20:57	Round-trip	fd-average	5332	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	S Passed	delay	2024-10-18 17:20:48	Round-trip	fd-average	4826	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	S Passed	delay	2024-10-18 17:20:47	Round-trip	fd-average	5156	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	Passed	delay	2024-10-18 17:20:38	Round-trip	fd-average	4628	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	S Passed	delay	2024+10-18 17:20:37	Round-trip	fd-average	5081	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	S Passed	delay	2024-10-18 17:20:28	Round-trip	fd-average	4839	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	🔗 Passed	delay	2024-10-18 17:20:27	Round-trip	fd-average	5137	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	Passed	delay	2024-10-18 17:20:18	Round-trip	fd-average	4809	12.30.3.1	
199	VPRNTwamp ~2	92.168.96.215	Passed	delay	2024-10-18 17:20:17	Round-trip	fd-average	5259	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	S Passed	delay	2024-10-18 17:20:08	Round-trip	fd-average	4713	12.30.3.1	
199	VPRNTwamp -2	92.168.96.215	🥝 Passed	delay	2024-10-18 17:20:07	Round-trip	fd-average	5133	12.30.2.1	
200	VPRNTwamp -1	92.168.98.97	🙁 Passed	delay	2024-10-18 17:19:58	Round-trip	fd-average	4710	12:30.3.1	

For the example shown, the tests between service endpoints are passing, showing that there are no issues with service connectivity.

END OF STEPS

# 5.17 Delete an OAM test suite

### 5.17.1 Purpose

Use this optional procedure to delete an OAM test suite and all its associated tests from the NSP UI. This action cannot be undone.



Note: Test suites cannot be edited in the NSP UI.

### 5.17.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

3

Open Data Collection and Analysis Management, Test Suites.

\_\_\_\_\_

Choose a test suite and click **‡** (Table row actions), **Delete**.

4 –

Click **DELETE** in the confirmation dialog to confirm.

The test suite and its tests are deleted from the NSP.

END OF STEPS

# 5.18 Create a telemetry subscription

### 5.18.1 Purpose

Perform this procedure to set up telemetry collection.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

### 5.18.2 Steps

1 -

Log in to the NSP as the Service Management user.

2 -

Open Data Collection and Analysis Management, Subscriptions.

3

Click + SUBSCRIPTION.

4 -

In the Create Subscription form that opens, configure the General parameters as needed:

- Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.
- The subscription is enabled by default: it will start running immediately.

General							
Name		Description					
Interface_Subscription_VPRN_Service		Interface Subscription for ports on VPRN Service					
Collection Interval (seconds)	Sync-Time (hh:mm)	State		DB Subscriptions			
15	00:00	Enabled -	□×	Enabled -	□_x		
File Subscriptions	Filename Prefix for File Subscriptions						
Disabled 👻 🗔							

5 -

Configure filters and counters:

- 1. In the **Object Filter** field, enter filtering information as needed to filter the collected data.
- As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.
- 2. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type you need from the list of matches.

3. When you enter a telemetry type, all counters are enabled by default.

To customize the counters, enable the **Enable notifications and notification counters** check box.

Click **Remove i** to remove a counter.

Click + COUNTERS to add a counter that was removed.

This example includes the following:

- · Telemetry Type: telemetry:/base/interfaces/interface
- · Counters:
  - received-octets-periodic
  - received-octets
  - received-unicast-packets
  - received-unicast-packets-periodic
  - transmitted-octets
- Object Filter (2 port objects used by two endpoints of the service): /nsp-equipment:network/ network-element[ne-id='92.168.98.97']/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot

NSP

General	Filters & Counters	
Filters & Counters	Object Filter         1       /nsp-equipment.network/network-element[ne-id+92.168.98.971/hardware-component/portIcomponent.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+2/port+C2/port+21/insp-equipment.network/network-element[ne-id+92.168.98.971/hardware-component.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+2/port+C2/port+21/insp-equipment.network/network-element[ne-id+92.168.98.971/hardware-component.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+2/port+C2/port+21/insp-equipment.network/network-element[ne-id+92.168.98.971/hardware-component.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+2/port+C2/port+21/insp-equipment.network/network-element[ne-id+92.168.98.971/hardware-component/portIcomponent.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+2/port+C2/port+21/insp-equipment.network-id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+21/insp-equipment.network-id+92.168.98.971/hardware-component/portIcomponent.id+94elf+1/alot+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+1/adt+21/insp-equipment.network-id+92.168.98.971/hardware-component/portIcomponent.id+94elf+1/alot+1/adt+1	Jpmentr →

6 —

#### Click CREATE.

The subscription appears in the subscriptions list.

Data Collection and	nd Analysis M	anagement Subs	scriptions	•						+ SUBSCRIPTION	с :
Telemetry Subsc	criptions	•									
State		Name		Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	File Prefix	Descript 🚦
	-		×								
<ul> <li>Enabled</li> </ul>		Interface_Subscripti	ion	telemetry:/base/interf	15	00:00	$\checkmark$	$\checkmark$			Interface

Port throughput statistics from the sites and NEs found by the object filter are received and processed every 15 s (see Collection Interval value). The statistics will remain in the NSP database for a configured period of time, as defined in the ageout policy.

END OF STEPS

# 5.19 Modify a telemetry subscription

### 5.19.1 Purpose

Use this optional procedure to make changes to a telemetry subscription, for example, to change the list of counters.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

### 5.19.2 Steps

the Service Management user.
on and Analysis Management, Subscriptions.
on and click <b>(</b> Table row actions), <b>Edit</b> .
s, update the parameters as needed.
w description is provided.
×

General	General								
Filters & Counters	Name Interface_Subscription_VPRN_Service Collection Interval (seconds)	Sync-Time (hhumm)	Description A new Interface Subscription for ports on VPRN Service State DB Subscriptions Function DB Subscriptions						
	15 File Subscriptions Disabled  Notification Topic ns-eg-80c36451-63b2-48ac-9f17-60d	⊑x 2b13818	Filename Prefix for File Subscriptions	Lhauleu	, Lx	Enaureu •	Lx		

5 –

Edit Subscription

### Click UPDATE

The updated subscription appears in the list.

E NOCLA Network Services Platform User: admin - 🤅										
Data Collection and Analysis Management Subscriptions - + SUBSCRIPTION C-										
Tele	emetry Subscriptions	•								
State		Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	Description		:
	•									
• Di	sabled	Complete_Service_Ing	telemetry:/base/accou	60	00:00	$\checkmark$	$\checkmark$	UCC15_Complete_Service_Ingress_Classic		:
• Di	sabled	VPRN_Port_MD	telemetry:/base/interf	10	00:00	$\checkmark$	$\checkmark$	UCC15_VPRN_Port_MD		:
• Di	sabled	Complete_Service_Ing	telemetry:/base/accou	10	00:00	$\checkmark$	$\checkmark$	UCC15_Complete_Service_Ingress_MD		:
• Di	sabled	VPRN Queue Stats Cla	telemetry:/base/sros	60	00:00	$\checkmark$	~	UCC15 VPRN Queue Stats Classic		:
• Di	sabled	VPRN Queue Stats	telemetry:/base/sros	60	00:00	$\checkmark$	~	UCC15 VPRN Queue Stats MD		:
• Di	sabled	Complete_Service_Egr	telemetry:/base/accou	10	00:00	$\checkmark$	~	UCC15_Complete_Service_Egress_MD		:
• Di	sabled	Complete_Service_Egr	telemetry:/base/accou	60	00:00	$\checkmark$	$\checkmark$	UCC15_Complete_Service_Egress_Classic		:
• Er	abled	Interface_Subscription	telemetry:/base/interf	15	00:00	$\checkmark$	$\checkmark$	A new Interface Subscription for ports on VPRN Service		:
• Di	sabled	VPRN_PORT_CLASSIC	telemetry:/base/interf	10	00:00	$\checkmark$	$\checkmark$	UCC15_VPRN_PORT_CLASSIC		:
• Er	abled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	$\checkmark$		TWL Loss accounting		:
• Er	abled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	$\checkmark$		TWL bin accounting		:
• En	abled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	$\checkmark$		TWL accounting		:
• Er	abled	TestSuiteExOAM-PM	telemetry:/base/oam	10	00:00	$\checkmark$		TWL streaming		:

END OF STEPS

# 5.20 Plot telemetry statistics

### 5.20.1 Purpose

Use this optional procedure to plot a chart of telemetry statistics. The steps for charting any type of telemetry statistic are the same: the example shows port throughput statistics.

This procedure is based on the procedure to plot a telemetry chart in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I plot a telemetry chart?.

### 5.20.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 5.18 "Create a telemetry subscription" (p. 202).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

#### **Chart limit**

Up to 10 objects can be charted at a time. The number of objects is the number of resources returned by the object filter, multiplied by the number of counters.

If your object filter returns one resource, for example, one NE, you can chart up to 10 counters for the resource.

### 5.20.3 Steps



The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

### Create a chart

1

Log in to the NSP as the Service Management user.

2 -

Open Data Collection and Analysis Management, Subscriptions.

3

Choose a subscription and click **(**Table row actions), **Open in Data Collection and Analysis Visualizations**.

Data Collection and Analysis Management Subscriptions + SUBSCRIPTION 🕒 🗄										
Telemetry Subscripti	Telemetry Subscriptions +									
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	File Prefix	Description	
	•									
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	~				SLM accounting	
<ul> <li>Enabled</li> </ul>	Interface_Subscription	telemetry:/base/interf	15	00:00	~	$\checkmark$			A new Interface Subscr	
Enabled	UCC LSP Egress Path S	telemetry:/base/lsps/l	10	00:35	~	~		🖌 Edit		
Enabled	UCC SAP Ingress Telem	telemetry:/base/acco	10	00:10	~	$\checkmark$		Open in Data Coll	ection and Analysis Visualizations	
<ul> <li>Enabled</li> </ul>	TestSuiteEx_OAM-LO	telemetry:/base/oam	10	00:00	~			<ul> <li>Delete</li> </ul>	coopuack result	
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-LIN	telemetry:/base/oam	10	00:00	~				Link-trace result	
<ul> <li>Enabled</li> </ul>	TestSuiteEx_OAM-PM	telemetry:/base/oam	10	00:00	~				CFM DMM streaming	
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	~				DMM bin accounting	
Enabled	TestSuiteExOAM-PM	telemetry:/base/oamp	300	00:00	~				DMM accounting	
<ul> <li>Enabled</li> </ul>	UCC LSP Egress subscr	telemetry:/base/lsps/l	10	00:25	~	$\checkmark$			LSP Egress subscriptio	
<ul> <li>Enabled</li> </ul>	UCC Interface Telemet	telemetry:/base/interf	10	00:00	~	$\checkmark$			Interface telemetry su	
Enabled	UCC Interface Utilizati	telemetry:/base/interf	10	00:15	~	$\checkmark$			Interface utilization su	
Enabled	UCC SAP Egress Telem	telemetry:/base/acco	10	00:45	~	$\checkmark$			SAP Egress telemetry	

The Data Collection and Analysis Visualizations view opens in a new browser tab.

In the window that opens, configure the parameters in the top panel:

- 1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
- 2. From the Time Range drop-down list, choose the amount of historical data to display.
- 3. Click Combine charts to plot data from multiple data series on the same chart.
- 5 \_\_\_\_\_

```
Click + DEFINITION.
```

The telemetry and resource filter definition panels are displayed.

6

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

7

Choose counters to display from the Counters drop-down list.

8

In the Object Filter field, enter filtering information to filter the collected data.

New Chart Configuration		×				
Collection Interval (seconds)*           15           Combine charts	Time Range Last 12 hours					
Telemetry & Resource Filter Definitions		+ DEFINITION				
Telemetry Type telemetry://base/interfaces/interface		×				
Counters (received-octats X (received-octats-periodic X) received-uncast-periodic X) -						
Object Filer	t/port[component-id='shelf=1/slot=1/card=1/slot=1/card=1/port=c2/port=2']/nsp-equipment.network/network-element[ne-id='92.168.96.215']/hardware-component/port[component-id='shelf='	1/slot=1/t				

SAVE AS..

CANCEL PLOT

#### 9 -

Save the configuration as a chart:

- 1. Click SAVE AS.
- 2. In the window that opens, enter a name for the chart and add a description.
- 3. Click **SAVE**.

In a few seconds, the chart is added to the list.

10 -

#### Click PLOT.

NSP begins plotting data. In a few moments, data will be visualized in the chart.

eceived-octets-periodic																										
92.168.96.215 : 1/1/c1/2																										
205																				Historic	al					
****	111111	1111	1111	11111	1111	11111	1111	1111	1111	1111	11111	111	1111	1111	11111	1111	1111	1111	1111	1111	A A	11111	1111	11111	1111	1111
1710000000000	VVVVVV	VVVV	10000	VVVV	JUUUU	VVVV	VVVV	VVVV	VVVL	IVVVV	VVVV	VVVV	VVVV	VVVV	VVVV	VVVV	UVVV	VVVV	UVVV	VVVV	$\Lambda \Lambda$	JVVVV	VVVV	VVVV	VVVV	VVVV
50																					V					
																					V					
14:12 14:14 14:5	14:18	14.20 1	4.22 14.2	14.26	14:28	14.30	14.32	14,34	14.36	1438	14:40	14;42	14.44	14,40	54,98	14:50	14:52	14:34	14:58	14:58	15:00	55.02	15.94	13.06	15:08	15:10
92.168.98.97 : 1/1/c2/2																										
202																				Historic	al					
*** * * * * * * * * * * *	****	1111			1111		1111	1111	1111	NAA A	1111	1111	1111	1111	1111	1111	1111	****	1111	1111	1 1	****	1111	1111	1111	1111
$\mathbf{W}$	UVVVVV	JVVVV	VVVVV	VVVVV	VVVV	VVVV	JVVV	JVVVI	UUUU	VVVV	VVVVI	IVVV	VVVV	UVVU	VVVV	JVVVI	NVV	MM	NVV	MM	LN	NVVV	JVVV	VVVV	WW	INNN
CARDON FOR ALL MEDICARD AND A																					V					
50																					V					
1612 1616 141	1618	14:20 1	422 14:2	1626	14-28	14-30	16.52	1634	1636	14-35	14560	14:42	14:44	16.66	24.98	14:50	14-52	14:54	14:56	14.58		\$5.62	15:04	15:04	15.08	15:10

11 -

Close the chart window. The saved telemetry chart appears in the list, ready to be plotted again as needed.

END OF STEPS

# 5.21 Delete a telemetry subscription

### 5.21.1 Purpose

Use this optional procedure to remove a telemetry subscription from the NSP. This action cannot be undone.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 24.4 is How do I manage subscriptions?.

### 5.21.2 Steps

1 -

Log in to the NSP as the Service Management user.

NSP

#### Open Data Collection and Analysis Management, Subscriptions.

3 -

2 -

To delete a subscription:

Choose a subscription and click **(**Table row actions), **Delete**.

The subscription is removed immediately.



**i** Note: Removing a subscription does not remove data from the database. The data collected by the subscription is retained according to the database retention policy.

END OF STEPS

# 6 UCC-16: IES

## 6.1 Overview

### 6.1.1 Purpose

This chapter describes the process required to configure an IES on SR OS NEs using NSP Service Management.

Configuration examples in this chapter show NSP Release 23.11 and SR OS 23.7.R2 NEs.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-svc-fulfillment-bundle-2311-v3.zip

See the NSP and NE documentation for more information.

### 6.1.2 Contents

6.1 Overview	211
Preparation	212
6.2 Prerequisites	212
6.3 Optional: create a restricted Service Management user	214
6.4 Install the required artifact bundles	218
6.5 Configure user access to the required intent types	219
Service Configuration	221
6.6 Import intent types into Service Management	221
6.7 Create an IES service template	222
6.8 Create and deploy an IES service to the network	223
6.9 Modify or delete an IES service	228
Optional procedures	231
6.10 Create telemetry subscriptions	231
6.11 Create a telemetry chart and plot statistics	232

# Preparation

# 6.2 Prerequisites

### 6.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes							
Mandatory for IES									
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS								
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_							
NSP installation	Pathway for NSP system installation in the NSP Installation and Upgrade Guide How do I enable TLS for telemetry and gNMI on_change support? in the NSP System Administrator Guide.	Include the following in your deployment:   Feature packs:  platform-baseServices  platform-pluggableNetworkAdaptation  platform-loggingMonitoring  serviceActivationAndConfiguration- intentBasedServiceFulfillment  networkInfrastructureManagement- basicManagement  networkInfrastructureManagement- deviceConfig  Adaptor suites:  sros-common  sros-oc-logical-inventory  sros-23-7-r1							

Prerequisite	Documentation reference	Notes				
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the NSP Network Automation Guide					
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	_				
Cards and MDAs provisioning	ICM process in the <i>NSP Device Management</i> <i>Guide</i> for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.				
Connectors and Ports provisioning	procedures in the NSP Device Management Guide for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	The intent types required for this configuration are: • icm-equipment-port-connector • icm-equipment-port-ethernet				
OSPF/ISIS	CLI Reference Guides for SR OS	_				
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.				
Interfaces Provisioning	How do I create a physical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-network-interface				
Customer creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-service-customer				
Optional	•	•				

Prerequisite	Documentation reference	Notes						
Optional items to include in your NSP deployment	Pathway for NSP system installation in the <i>NSP Installation and Upgrade Guide</i>	<ul> <li>Optional feature packs:         <ul> <li>pathControlAndOptimization</li> <li>multilayerDiscoveryAndVisualization</li> <li>NSP Analytics: Network Operations Analytics feature package with the networkOperationsAnalytics- analyticsReporting installation option</li> <li>NSP Baseline Analytics: networkOperationsAnalytics- baselineAnalytics</li> <li>networkInfrastructureManagement- performanceIndicatorsAndAlerts</li> </ul> </li> <li>VSR/NRC</li> <li>An AuxDB</li> <li>An NFM-P instance</li> </ul>						
Telemetry/OAM	NSP Data Collection and Analysis Guide	<ul> <li>NSP SR OS vendor-agnostic telemetry adaptation artifact bundle</li> <li>networkInfrastructureManagement- gnmiTelemetry feature pack</li> </ul>						
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group						
Segment Routing	CLI Reference Guides for SR OS							
Scheduler QoS Policies	How do I create a logical configuration deployment? in the <i>NSP Device Management</i> <i>Guide</i>	The intent types required for this configuration are:						
configuration		icm-qos-schedulerpolicy-srqos     icm-qos-network-srqos						
SAP QoS Policies configuration		<ul> <li>icm-qos-sapegress-srqos</li> <li>icm-qos-sapegress-srqos</li> </ul>						
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps.						
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access						

# 6.3 Optional: create a restricted Service Management user

# 6.3.1 Purpose

Perform this optional procedure to create a user with access only to specified NSP functions.

Procedures in this chapter can be performed by the restricted user, or by an administrator.

This procedure is based on the procedures for the following in the *NSP System Administrator Guide*:

- Configuring a role
- Configuring a user group
- Creating an NSP local user
- Enabling User Access Control
- · Configuring user access to an intent type

For example, the reference procedures in NSP Release 23.11 are:

- How do I configure a role?
- How do I configure a user group?
- How do I create an NSP local user?
- How do I enable User Access Control?
- · How do I configure user access to an intent type?

If a restricted user has already been created, verify that the user has the required permissions, as shown in Step 6.

### 6.3.2 Steps

#### Create a role

1 \_\_\_\_\_

Log in to the NSP as an administrator.

2 \_\_\_\_\_

Open Users and Security.

3 \_\_\_\_\_

Select **Roles** from the drop-down list on the toolbar.

4 \_\_\_\_\_

Click **+ Create Role**. The Create Role form opens.

5 \_\_\_\_\_

In the Identification panel, specify a role name and description.

The Role Name and Description fields can employ only the following special characters: @ -

The Role Name string must not contain any spaces, including a leading or trailing space.

6

To assign NSP functional access to the role, go to the Action Permissions panel and select an access level from the drop-down list for each NSP GUI you want to include in the role.

Action permissions group item	Permissions	Notes					
Service Fulfillment	Read / Write / Execute	—					
Network Intents	Read: Manage Intents	Required to import intent types into Service Management					
Workflows	Read	Required to create service and tunnel templates					
Optional: DCA Management	Read / Write / Execute	Only required for creating and plotting telemetry subscriptions					
Optional: OAM Tests	Read / Write / Execute	Only required for generating and executing OAM tests					

7 —

To assign network resource access to the role, go to the Resource Groups Access panel. (For a detailed explanation of the Resource Groups Access panel, see How do I set network resource access levels? in the *NSP System Administrator Guide*.)

You can assign resource group access globally, to resource group categories, to individual resource groups, or a combination of these. For service management it is recommended to grant access to all equipment and all services:

- Access To All Equipment assigns full permissions on all NE resource groups and port resource groups to the role.
- Access To All Services assigns full permissions on all service resource groups to the role.

8

Click Create to save your changes and return to the Roles list.

### Create a user group

9 \_\_\_\_\_

Open Users and Security.

10 \_\_\_\_\_

Select **User Groups** from the drop-down list on the toolbar.

11 \_\_\_\_\_

Click + Create User Group. The Create User Group form opens.

12 \_\_\_\_\_

Specify a group name and description in the Identification panel.

The user group name you specify here must exactly match a corresponding user group name returned by your user repository.

The User Group Name and Description fields can employ **only** the following special characters: @ - \_.
The User Group Name string must not contain any spaces, including a leading or trailing space.

13 —

To assign user roles to the group, click **+ Add Roles** on the Roles panel. The Add Roles form opens.

14 -

Enable the check box for each role you want to assign to the group and click **Done**. The roles are added to the Selected Roles list.

To remove a role item from the Selected Roles list, click **Delete** on the item.

15 —

Click Create to save your changes and return to the User Groups list.

#### Create a user

16 —

Open Users and Security.

17 –

Select **Users** from the drop-down list on the toolbar.

18 —

Click + Create User.

19 -

In the Create User form, specify user identification information for the account in the Identification section. The **Username** and **User Group** fields are mandatory.

**i** Note: Any uppercase characters in the username are saved as lowercase.

The Username value:

- can be 1 to 40 characters long
- · cannot include a space
- · cannot have a leading or trailing space
- · can include only the following special characters:
  - @ (at sign)
  - - (hyphen)
  - \_ (underscore)
  - . (period)

217

#### 20 -

In the Password section, specify and confirm a password for the user account.

- If you want this password to be temporary, enable the **Force User to Change Password** option. The new user will be forced to change their password when they first login to NSP.
- Enable the Show Password option to see the password characters as you type them.
- Click on the **Password Requirements** link to view a list of minimum security requirements for the password.

#### 21 –

Click Create.

## Enable user access control

22 —

Open Users and Security, User Groups.

23 —

24 –

Click **More Actions**, Settings.

In the Access Control Settings form, enable the NSP User Access Control option.

25 —

Click **SAVE** to enable access control.

END OF STEPS

# 6.4 Install the required artifact bundles

## 6.4.1 Purpose

Use this procedure to make the required intent types available to Service Management in NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 23.11 is How do I install an artifact bundle?.

## 6.4.2 Steps

## Download the required intent types

1

Download the Service Fulfillment artifact bundle from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP  $\rightarrow$  23.11  $\rightarrow$  Artifacts  $\rightarrow$  Artifact Admin Import.

See the description to verify which bundle to download.

# Install the artifact bundle in NSP

Log in to the NSP as the Service Management user.

3

2 —

Open Artifacts, Artifact Bundles.

4

Click IMPORT & INSTALL.

5 —

In the form that opens, drag and drop the zip file, or click **Browse** and navigate to the files on your system.

6

To install the artifact bundle immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7

To install a bundle in Imported status, choose **Install bundle** from the (Table row actions) menu.

END OF STEPS -

# 6.5 Configure user access to the required intent types

## 6.5.1 Purpose

Use this procedure to provide the user access to intent types. If the restricted Service Management user will be performing configuration tasks, this procedure must be performed.

This procedure is based on the procedure for configuring user access to an intent type in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I configure user access to an intent type?.

# 6.5.2 Steps

1 – L	_og in to the NSP as an a	dministrator.						
2 -		atomt Turaca						
	open network intents, in	itent Types.						
3 – S	Select the ies intent type	).						
<b>4</b> –	Click (Table row action		o open the	Iser Access	form			
		b). User Access in						
5 –		b), USEI ACCESS (						
5 – Ir tł	n the User Access form, he top right of the form.	choose Grant ac	cess to all	user group	s from the	drop-dc	wn lis	st
<b>5</b> – Ir tł C	n the <b>User Access</b> form, he top right of the form. Choose <b>Full access</b> for t	choose Grant ac	ccess to all	user groups	s from the roup" (p. 5	e drop-dc 54).	wn lis	st
5 – Ir tł C	n the <b>User Access</b> form, he top right of the form. Choose <b>Full access</b> for t	choose <b>Grant ac</b>	cess to all	user groups	s from the roup" (p. 5	e drop-dc 54).	wn lis	st
5 Ir tł ⊂	n the <b>User Access</b> form, the top right of the form. Choose <b>Full access</b> for t Network Services Platform User Access Specify which users have intent type access by	choose <b>Grant ac</b> ne user group crea	ated in "Cre	user groups	s from the roup" (p. 5 <sup>User: admin</sup>	e drop-dc 54).	wn lis	st
5 li th C	n the <b>User Access</b> form, the top right of the form. Choose <b>Full access</b> for t Network Services Platform User Access Specify which users have intent type access by Selected intent type(s) (1 Intent Type(s) selected)	choose <b>Grant ac</b> ne user group crea choosing their user group(s) below. User Group access pe Grant access to a	ermissions assigned to t	user groups ate a user gr	s from the roup" (p. 5 <sup>User: admin</sup>	e drop-dc 54).	wn lis	st
5 – li tł C	n the User Access form, the top right of the form. Choose Full access for the Network Services Platform User Access Specify which users have intent type access by Selected intent type(s) (1 Intent Type(s) selected)	choose <b>Grant ac</b> ne user group creat choosing their user group(s) below. User Group access pe Grant access to a Full access	ermissions assigned to t	user groups ate a user gr he selected intent type(s)	s from the roup" (p. 5 User: admin ×	e drop-dc 54).	wn lis ¢	st

Click SAVE. The user access is updated.

released

END OF STEPS -

6 –

.

ArtifactAdmin ServiceFulfillment

:

:

:

:

•

SAVE

CANCEL

NSP

 $\equiv$ 

Network Intents

Intent Type

redundant-eline redundant-cline I3-evpn-composi

ies

cpipe

etree

evpn-vpls

evnn-enine

# **Service Configuration**

# 6.6 Import intent types into Service Management

## 6.6.1 Purpose

Use this procedure to import the intent types you obtained in 6.4 "Install the required artifact bundles" (p. 218) to the Service Management views. This procedure is based on the procedure for importing an intent type into Service Management in the *NSP Service Management Guide*.

For example, the reference procedure in NSP Release 23.11 is How do I import an intent type into Service Management?.

**i** Note: This procedure is not required in NSP 25.4 or later because intent types for Service Management will import directly into Service Management during artifact bundle installation.

The intent type required is ies.

# 6.6.2 Steps

1
-

Log in to the NSP as the Service Management user.

2

From the Service Management, Intent Type Catalogue view, click IMPORT.

A list of previously-defined intent types is displayed.

i

**Note:** Only intent types that have the Service Fulfillment label applied will be available to import. Intent types to be used for tunnel template creation must also have the Tunnel label applied.

i

**Note:** For a restricted user to be allowed to import intent types, they must have appropriate permissions configured for those intent types in Network Intents; see How do I configure user access to an intent type? in the *NSP Network Automation Guide*.

3

Select the check boxes in-line with the intent types you wish to import and click IMPORT.

The intent type to import is ies.

The intent type is imported into service management. This may take a few minutes.

**i** 1

**Note:** Selecting an imported intent type from the list opens the Info panel, which displays historical information such as the last time the intent type was updated, the last time it was imported, and the last time the modules that compose the intent type were revised.

END OF STEPS

# 6.7 Create an IES service template

# 6.7.1 Purpose

This procedure is based on the procedure to create a service template in the *NSP Service Management Guide*.

For example, the reference procedure in NSP 23.11 is How do I create a service template?.

# 6.7.2 Steps

1 \_\_\_\_\_

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

From the Service Management, Service Templates view, click + CREATE.

The Create a service template form opens.

3

\_\_\_\_\_

Configure the parameters, as required.

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

4

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

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution

<sup>5 -</sup>

Parameter	Description
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

#### 6 —

## Click ADD.

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

7 -

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

8

#### Click CREATE.

The service template is created.

END OF STEPS

# 6.8 Create and deploy an IES service to the network

## 6.8.1 Purpose

Perform this procedure to create the service.

This procedure is based on the procedures for creating and auditing a service in the *NSP Service Management Guide*.

For example, the reference procedures in NSP Release 23.11 are:

- How do I create an IES service?
- How do I audit a service?

## 6.8.2 Steps

1 –

Log in to the NSP as the Service Management user.

2 —

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

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

## 3 –

Click on an IES service template from the list.

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

#### 4

Configure the parameters, as required:

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

#### 5

In the Site Details panel, click **+ ADD**. The Add Site form opens.

#### 6

Configure the required parameters:

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

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

## 7 –

Click + ADD.

The Add Interface form opens.

## 8 -

Configure the parameters, as required:

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

#### 9 -

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

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

10 -

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

Parameter	Description
Virtual Router ID	Specifies the virtual router identifier (VRID) for the VRRP virtual router instance
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
MAC	Specifies a MAC address to be used by the virtual router instance, overriding the VRRP default derived from the VRID
Ping Reply	Specifies whether or not the non-owner can reply to ICMP echo requests directed to the virtual router instance IP addresses

#### 11 -

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

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

Parameter	Description
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click + ADD)	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click + ADD)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler

#### 12 —

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

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

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

#### 13 —

Repeat Step 6 to Step 12 to add additional interfaces.

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

14 -

Perform one of the following:

- a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.
- b. Click **SAVE** to create the service in a Saved state.
- c. Click **DEPLOY** to create the service in a Deployed state.

END OF STEPS

# 6.9 Modify or delete an IES service

## 6.9.1 Purpose

Use this procedure if needed to modify configured parameters for an IES service, or to remove a service from the network and delete it.

## 6.9.2 Steps

## Edit a service

1 –

Log in to the NSP as the Service Management user.

2 -

From the Service Management, Services view, select a service and choose **Edit** from the (Table row actions) menu.

3 \_\_\_\_\_

Modify the service, site, endpoint or SAP parameters as required.

4

Perform one of the following:

- a. Select the Reserve Resources check box and click **PLAN** to create the service in a Planned state.
- b. Click **SAVE** to create the service in a Saved state.
- c. Click **DEPLOY** to create the service in a Deployed state.

•	~ .			<b>~</b>		-
	<ia network="" p<="" services="" td=""><td>latform</td><td></td><td></td><td>User: admin</td><td>• ?</td></ia>	latform			User: admin	• ?
Service >	Edit Site 1					
Ip Transports	Device ID*			Site Name		
	92.168.96.215	×	0	100		
	Description			Mtu		
				1024		
	Interface					+ ADD
	Interface Name	Interface Type		Admin State	IP MTU	
	VPLS	sap		unlocked		0 0

# **Delete a service**

From the **Service Management**, **Services view**, select a service and click (Table row actions), **Remove**.

The Remove Service From Network confirmation dialog opens.

6

5 —

Click **REMOVE** to remove the service from the network.

The Life Cycle State of the service is changed to Removed.

7

If you prefer, you can leave the service in Removed state so that it can be deployed again later. To delete the service permanently, proceed to the next step.

8

To delete the service, select the service and click (Table row actions), **Delete**. The Delete Service confirmation dialog opens.

Note: The Delete option only appears if the service is in Removed state.

# 9 —

Click DELETE to permanently delete the service from the NSP.

END OF STEPS -

# **Optional procedures**

# 6.10 Create telemetry subscriptions

# 6.10.1 Purpose

Perform this procedure to set up telemetry collection.

The bundle of vendor agnostic custom resources must be imported and installed to support telemetry collection. The bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP  $\rightarrow$  23.11  $\rightarrow$  Adaptors  $\rightarrow$  Nokia\_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-1.0. 0-rel.10.zip.

This procedure is based on the procedure for managing subscriptions in the NSP Data Collection and Analysis Guide.

For example, the reference procedure in NSP 23.11 is How do I manage subscriptions?.

See also the procedure to install telemetry artifacts in the *NSP Data Collection and Analysis Guide* to verify that telemetry prerequisites are in place. The reference procedure for this is in NSP 24.4: How do I install telemetry artifacts?

# CAUTION Service Disruption

The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

# 6.10.2 Steps

1 -

Log in to the NSP as the Service Management user.

2

Open Data Collection and Analysis Management, Subscriptions.

3

To create a subscription:

- 1. Click **+** SUBSCRIPTION.
- 2. In the Create Subscription form that opens, configure the General parameters as needed.
  - Enable database (DB) subscriptions as needed to save subscription information to the NSP database. For subscription data to be available to Analytics, the auxiliary database must be deployed.

- The subscription is enabled by default: it will start running immediately. Choose **Disabled** in the **State** field if you want to enable your subscription later.
- 3. In the **Object Filter** field, enter filtering information as needed to filter the collected data.

As you type, the field provides suggestions for available filters to match your input and identifies incorrect syntax.

Object filter example: /nsp-equipment:network/network-element[ne-id='
<nedid>']

4. Enter information in the Telemetry Type field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type you need from the list of matches.

Telemetry type example: telemetry:/base/interfaces/interface

5. When you enter a telemetry type, all counters are enabled by default.

To customize the counters, enable the **Enable notifications and notification counters** check box.

Click **Remove** i to remove a counter.

Click + COUNTERS to add a counter that was removed.

6. Click CREATE.

The subscription begins collection when it is enabled.

END OF STEPS

# 6.11 Create a telemetry chart and plot statistics

## 6.11.1 Purpose

Use this procedure to chart historical telemetry data. This procedure is based on the procedure for plotting a telemetry chart in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP 23.11 is How do I plot a telemetry chart?.



The name of an object, including subscriptions, baselines, indicators, templates, and chart profiles, cannot contain a semicolon (;) or backslash (\).

The use of these characters in an object identifier will result in corrupted data that must be deleted by Nokia support.

## 6.11.2 Before you begin

When you create a telemetry chart, you configure a telemetry filter. For historical data to be displayed, the data must be available in the database; see 2.13 "Create telemetry subscriptions" (p. 77).

Charts are created by streaming to the plotter: historical data is queried and streamed to the plotter, then real time telemetry subscriptions are created and the data from these subscriptions is streamed to the plotter.

Data Collection and Analysis Visualizations times out if telemetry data is not received. The time-out limit is either double the collection interval or two minutes, whichever is greater.

# 6.11.3 Steps

1 -

# Create a chart

Log in to the NSP as the Service Management user.

2 \_\_\_\_\_

Open the New Chart window:

- From Data Collection and Analysis Visualizations, Telemetry Charts, click + CHART.
- From Data Collection and Analysis Management, Subscriptions, choose a subscription and click (Table row actions), Open in Data Collection and Analysis Visualizations.
- 3 —

In the window that opens, configure the parameters in the top panel:

- 1. Configure the **Collection Interval** parameter. If you are using NFM-P telemetry data, verify that the collection interval is long enough to allow time for Visualizations to receive the data before timing out.
- 2. From the Time Range drop-down list, choose the amount of historical data to display.
- 3. Click **Combine charts** to plot data from multiple data series on the same chart.
- 4

## Click + DEFINITION.

The telemetry and resource filter definition panels are displayed.

5 -

Enter information in the **Telemetry Type** field. As you type, the field filters for available telemetry types to match your input.

Choose the telemetry type from the list of matches.

6

Choose counters to display from the Counters drop-down list.

7

In the **Object Filter** field, enter filtering information to filter the collected data.

#### 8 –

If you need to save the configuration as a chart:

- 1. Click **SAVE AS**.
- 2. In the window that opens, enter a name for the chart and add a description if needed.
- 3. Click SAVE.

The chart is added to the list.

9 \_\_\_\_\_

Click PLOT.

END OF STEPS -

# 6.11.4 Steps

## Plot an existing chart

#### 1 —

To plot an existing chart with no changes:

- 1. Open Data Collection and Analysis Visualizations, Telemetry Charts.
- 2. Choose a chart and click (Table row actions), Chart.
- 2 —

To edit a chart and plot it, choose the chart and click **‡** (Table row actions), **Edit**.

3 —

Edit the parameters as needed and click **PLOT**.

END OF STEPS -

# 6.11.5 Result

Visualizations displays a chart view showing the streaming data. While data is streaming, you can configure the **Group by** parameter in the upper left of the chart view to change how the data is grouped or click **Configure** in the upper right to view or change the configuration of the chart.

Click ()(Chart Details) to open the Chart Details panel on the right side of the chart view to show details about the resources.

## Example charts:



# 7 UCC-20: NE Provisioning - Day/Phase 1 configuration

# 7.1 Overview

# 7.1.1 Purpose

This chapter describes the steps that are required to complete the Day/Phase 1 configuration on an NE that has its Day/Phase 0 configuration complete and discovered in NSP. Day/Phase 1 involves network infrastructure configuration of network interfaces, IGP, BGP and IP/MPLS, which enables the control planes to start functioning between discovered network elements.

Configuration examples in this chapter show NSP Release 24.11.

The following NE variants/versions were used to test this use case:

- 7750 SR 14s Classic [Version 23.7R2 and 23.10 R7]
- 7750 SR 14s Model Driven [Version 23.7R2 and 23.10 R7]
- 7250 IXR-6 Model Driven [Version 23.7 R2]

The following NSP device configuration artifact bundles were used to test this use case:

- NSP device configuration product artifacts for SROS (Classic) based nodes [e.g. device-configartifacts-csros-23-10-1-nsp-23-11-0-cam-v6.zip]
- NSP device configuration product artifacts for SROS Classic and Model Driven nodes with deeper attribute coverage [e.g. device-config-artifacts-gsros-23-10-1-nsp-23-11-0-cam-v4.zip]
- NSP device configuration product artifacts for SROS (Model Driven) based nodes [e.g. deviceconfig-artifacts-msros-23-10-1-nsp-23-11-0-cam-v6.zip]
- NSP device configuration product artifacts for SROS Classic and Model Driven nodes [e.g. device-config-artifacts-usros-23-10-1-nsp-23-11-0-cam-v4.zip]

**Note:** The configurations described in this guide are generic and actual user configurations might differ based on specific requirements/scenarios.

# 7.1.2 Contents

7.1 Overview	237
Preparation	239
7.2 Prerequisites	239
Day/Phase 1 configuration	241
7.3 Cards/MDA	241
7.4 Port/Connector	252
7.5 BFD Templates	285

7.6 OSPF/ISIS	293
7.7 MPLS/RSVP Interfaces	321
7.8 Interfaces	335
7.9 LDP	345
7.10 BGP	347
7.11 Segment Routing	358
7.12 LSP	360
7.13 Customers	366
7.14 Other configurations	370

# Preparation

# 7.2 Prerequisites

# 7.2.1 Network configuration prerequisites

Before services can be configured and managed in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to service use cases, and indicates whether each prerequisite is required for this use case.



**Note:** The NE must be discovered in NSP as a prerequisite to start the Day/Phase 1 configuration. NSP Intents have been used for NE configuration in Day/Phase 1 in most of the places in this chapter. Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for Brownfield Service Discovery		
GRPC configuration	See SR TLS information here in the SR OS	_
1. Generate security certificates	24.3 R1 documentation: TLS	
2. Configure security and enable GRPC on all devices		
<ol> <li>Apply security certificates on all devices</li> </ol>		
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_

Prerequisite	Documentation reference	Notes
NSP installation	Pathway for NSP system installation in the NSP Installation and Upgrade Guide How do I enable TLS for telemetry and gNMI on_change support? in the NSP System Administrator Guide.	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>serviceActivationAndConfiguration- intentBasedServiceFulfillment</li> <li>networkInfrastructureManagement- basicManagement</li> <li>networkInfrastructureManagement- deviceConfig</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-cological-inventory</li> <li>sros-23-7-r1</li> </ul> </li> </ul>
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration)	How do I install an artifact bundle? in the NSP Network Automation Guide	_
Device discovery	Pathway for device discovery in the <i>NSP</i> <i>Classic Management User Guide</i> How do I discover devices? in the <i>NSP</i> <i>Device Management Guide</i> Nokia Developer Portal for information about FTP mediation policy creation using API.	

# Day/Phase 1 configuration

# 7.3 Cards/MDA

# 7.3.1 Prerequisites:

- Users must provision power-modules in CLI on 7250 and 7750 nodes or else cards remain in booting / Lo Power state.
- Users must provision SFM in CLI; there is no intent.

# 7.3.2 To provision power in CLI:

## 7750 Classic

```
/configure system power-shelf 1 power-shelf-type "ps-al0-shelf-dc"
/configure system power-shelf 1 power-module 1 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 2 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 3 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 4 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 5 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 6 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 7 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 8 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 9 power-module-type
"ps-a-dc-6000"
/configure system power-shelf 1 power-module 10 power-module-type
"ps-a-dc-6000"
/admin save
```

```
/edit-config private
/configure chassis router chassis-number 1 power-shelf 1 power-shelf-type
ps-a10-shelf-dc
/configure chassis router chassis-number 1 power-shelf 1 power-module 1
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 2
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 3
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 4
```

```
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 5
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 6
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 7
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 8
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 9
power-module-type ps-a-dc-6000
/configure chassis router chassis-number 1 power-shelf 1 power-module 10
power-module-type ps-a-dc-6000
/commit
/admin save
/quit-config
```

A:admin@Bo	oston‡ show chassis power-s	shelf l p	ower-module			
Power Shel	f Summary					
Slot	Provisioned Type Equipped Type (if diff	Admin f) State	Operational State	Zone	Input Mode	Output
1	ps-al0-shelf-dc	up	up	1	60A	on
Power Modu	le Summary					
Slot	Provisioned Type Equipped Type (if diff	Admin f) State	Operational State	Input A B	Zone	
1	ps-a-dc-6000	up	up	ч ү	1	
2	ps-a-dc-6000	up	up	ΥY	1	
3	ps-a-dc-6000	up	up	ΥY	1	
4	ps-a-dc-6000	up	up	ΥY	1	
5	ps-a-dc-6000	up	up	ΥY	1	
6	ps-a-dc-6000	up	up	ΥY	1	
7	ps-a-dc-6000	up	up	ΥY	1	
8	ps-a-dc-6000	up	up	ΥY	1	
9	ps-a-dc-6000	up	up	ΥY	1	
10	ps-a-dc-6000	up	up	ΥΥ	1	

```
/edit-config private
/configure chassis router chassis-number 1 power-module 2
```

```
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 3
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 4
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 5
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 6
power-module-type ixr-dc-3000
/configure chassis router chassis-number 1 power-module 6
power-module-type ixr-dc-3000
/commit
/admin save
/quit-config
```

A:admin	.:admingcE_west# snow chassis power-module												
Power M	ower Module Summary												
Slot	Provisioned Type Equipped Type (if diff)	Admin State	Operational State	Input A B	Zone								
1	(not provisioned) ixr-dc-3000	up	unprovisioned	Y -	1								
2	ixr-dc-3000	up	up	Ч —	1								
3	ixr-dc-3000	up	up	У –	1								
4	ixr-dc-3000	up	up	У –	1								
5	ixr-dc-3000	up	up	У –	1								
6	ixr-dc-3000	up	up	Υ -	1								

# 7.3.3 To provision SFM:

7750 Classic

```
/configure sfm 1 sfm-type sfm-s
/configure sfm 2 sfm-type sfm-s
/configure sfm 3 sfm-type sfm-s
/configure sfm 4 sfm-type sfm-s
/configure sfm 6 sfm-type sfm-s
/configure sfm 7 sfm-type sfm-s
/configure sfm 8 sfm-type sfm-s
/admin save
```

```
/edit-config private
/configure sfm 1 sfm-type sfm-s
```

```
/configure sfm 2 sfm-type sfm-s
/configure sfm 3 sfm-type sfm-s
/configure sfm 4 sfm-type sfm-s
/configure sfm 5 sfm-type sfm-s
/configure sfm 6 sfm-type sfm-s
/configure sfm 7 sfm-type sfm-s
/configure sfm 8 sfm-type sfm-s
/commit
/admin save
/quit-config
```

#### A:admin@Boston# show sfm

SFM Summa	ry			
Slot	Provisioned Type Equipped Type (if different)	Admin State	Operational State	Comments
1	sfm-s	up	up	
2	sfm-s	up	up	
3	sfm-s	up	up	
4	sfm-s	up	up	
5	sfm-s	up	up	
6	sfm-s	up	up	
7	sfm-s	up	up	
8	sfm-s	up	up	

/edit-confi	ig pı	riv	vate	
/configure	sfm	1	sfm-type	sfm-ixr-6
/configure	sfm	2	sfm-type	sfm-ixr-6
/configure	sfm	3	sfm-type	sfm-ixr-6
/configure	sfm	4	sfm-type	sfm-ixr-6
/configure	sfm	5	sfm-type	sfm-ixr-6
/configure	sfm	6	sfm-type	sfm-ixr-6
/commit				
/admin save	Э			
/quit-confi	İg			

SFM Sum	mary			
Slot	Provisioned Type	Admin	Operational	Comments
	Equipped Type (if different)	State	State 	
1	sfm-ixr-6	up	up	
2	sfm-ixr-6	up	up	
3	sfm-ixr-6	up	up	
4	sfm-ixr-6	up	up	
5	sfm-ixr-6	up	up	
6	sfm-ixr-6	up	up	

# 7.3.4 To configure Card/MDA using icm-equipment-card\_mda intent

1 -

Import the intent type icm-equipment-card\_mda into Device Management, Configuration Intent Types.

tent Type		Version		Status	Description	R	ole	Category	Device Scope	Last Updated :	i Intent Type Details
	T		T	•		T	•	•	•	MMM d, yyyy h:mm:ss	
m-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	. Pl	hysical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 :	
											Select an intent type to view deta

#### 2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-card\_mda**.

lame		Life Cyc	le	Intent Type		Intent Type Version		Config Form		Config Fo	rm State	Role	Ca :	(i) Template Details
		T	•		T		T		T		•			<b>C</b>
Equipment-card_mda		release	ed 👻	icm-equipment-card_mda			2	default		V Up-	-to-date	Physical	Ca :	∧ General
														Name
														Equipment-card_mda
														Description
														Life Cycle released
														Target Labels
														Intent Type
														Intent Type Version
														2
														Config Form
														default
														Config Form State
														Role
														Physical
														Category
														Device Scope
														SROS Classic & Model
														Flexible
														Tes
														Nov 26, 2024 11:28:27 am
		× 4											• • •	Nov 26, 2024 11:28:27 am
Auto-refresh	Last Refresh: 2	2024/11/26 1	1:29:33			1<	< Pa	age: 1 / 1 >					Count: 1	Nov 26, 2024 11:28:27 am

3

Create configuration deployments with the above configuration template. The following example uses 7750 (SR-14s variant):

Card slot 1: card\_xcm14\_s (xcm-14s on MD)

MDA slot 1 and 2: xma\_s36\_100gb\_qsfp28 (s36-100gb-qsfp28 on MD)

Ex. 7750 Classic

Sel	ect Cards															,	¢
	NE Name			NE ID		Card (Identifier)				:	🔂 Bin (1 card)					EMP	Y
	Toronto	×	Ŧ		۲		T				NE Name		NE ID		Card (Identifier)		:
	Toronto			92.168.96.215		Card Slot - 6						T		Ŧ			
	Toronto			92.168.96.215		Card Slot - 5					Toronto		92.168.96.215		Card Slot - 1		8
	Toronto			92.168.96.215		Card Slot - 4											
	Toronto			92.168.96.215		Card Slot - 3											
	Toronto			92.168.96.215		Card Slot - 2											
	Toronto			92.168.96.215		Card Slot - 1											
						< < Page: 1 / 1	> >!		1	Count : 6	4					F	( )
															CANCEL	ADD	

Equipment-card_mda					×
Card	Card				
	Admin State		Card Type		
	enable	▼ □x	card_xcm14_s	× O	
	MDA				+ ADD
	MDA Slot	Admin State	MDA Type	Sync E	
	2	enable	xma_s36_100gb_qsfp28	B	1
	1	enable	xma_s36_100gb_qsfp28	8	1.
			IK K Page: 1	/1 > >	Total: 2
	XIOM				+ ADD
	XIOM Slot	Admin State	XIOM Type		

Deploy Physical Configuration				x
Select Template *	Select Template			REPLACE
Serect rangets and Coll Serected remplate	Yamplate Nama Equipment-card_mda Category Card	Template Description — Device Scope SROS Classic & Model	Target Labels — Flexible Yes	
	Select Targets and Edit Selected Ter	mplate		CLEAR ALL + TARGET
	Select targets. Template configurations can b	e edited after targets are selected. plates are assigned. View/Edit		EDIT TEMPLATE CONFIG
	NE Name NE ID	Card (Identifier)		
	Toronto 92.168.96.215	Card Slot - 1		1
				Count : 1
				CANCEL SAVE DEPLOY

Devic	ce Management C	Configuration Configuration	n Deployments													+ DEPLOYMENT 🕞 🚆
	Deployment Status		Configuration S	Status	NE Name		NE ID		Identifier		Template		Role	Category	r :	i Deployment Details
		-				T		T		T		T				
~	Deployed Aligned	I	<ul> <li>Modified</li> </ul>		Toronto		92.168.96.215		1		Equipment-card_mda		Physical	Card	:	NE Name Toronto
																NE ID
																92.168.96.215
																Identifier
																SLOT-NUMBER 1
																Deployment Status
																<ul> <li>Deployed Aligned</li> </ul>
																AUDIT ALIGN
																Last Audit
																Last Alignment
																Nov 26, 2024 12:14:48 pm by admin
																Equipment-card_mda
																Created
																Last Updated
																Nov 26, 2024 12:14:48 pm
																Role Physical
																Category
																card
	4													×	$\rightarrow$	Configuration Status     Modified
-	Auto-refresh	Last Refresh	: 2024/11/26 12:31:	11				1<	Page: 1 /1 >					Cou	nt : 1	

## Figure 7-1 NE CLI check after deployment

Card St	tate					
Slot/ Id	Provisioned Type Equipped Type (if different)	Admin State	Operational State	Num Ports	Num MDA	Comments
1	xcm-14s	up	up		2	
1/1	s36-100gb-qsfp28:he2400g+	up	up	36		
1/2	s36-100gb-qsfp28:he2400g+	up	up	36		
A	cpm-s	up	up			Active
В	cpm-s	up	down			Standby
	(not equipped)					

## Ex. 7750 MD

Sele	ct Cards														×	:
	NE Name			NE ID		Card (Identifier)			:	🙆 Bin (1 card)					EMPT	Y
	Boston	×	T		T		T			NE Name		NE ID		Card (Identifi	er)	:
	Boston			92.168.96.46		Card Slot-6(unassigned)					T		T			
	Boston			92.168.96.46		Card Slot-5(unassigned)				Boston		92.168.96.46		Card Slot-1(u	nassigne	1
	Boston			92.168.96.46		Card Slot-4(unassigned)									-	
	Boston			92.168.96.46		Card Slot-3(unassigned)										
	Boston			92.168.96.46		Card Slot-2(unassigned)										
$\checkmark$	Boston			92.168.96.46		Card Slot-1(unassigned)										
						< < Page: 1 / 1 >	×	c	ount : 6	4					F 4	( )÷
														CANCEL	ADD	

Card				
Admin State		Card Type		
enable	▼ □x	xcm-14s	×	
MDA				+ ADD
MDA Slot	Admin State	MDA Type	Sync E	
2	enable	s36-100gb-qsfp28		1
11	enable	s36-100gb-qsfp28		:
		Ic C Page:	1 Z1 × 21	Total: 2
хюм				+ ADD
хіом XIOM Slot	Admin State	ХІОМ Туре		+ ADD

Deploy Physical Configuration								×
Select Template *	Select Template							REPLACE
Select in gets and concerned introduce	Template Name Equipment-card_mda Category Card		Template Description — Device Scope SROS Classic & Model		Target Labels — Flexible Yes			
	Select Targets and Edit	Selected Templ	ate				CLEAR ALL	+ TARGET
	Select targets. Template cont	figurations can be ed	ited after targets are selecte are assigned. View/Edit	d.			EDIT TEMP	LATE CONFIG
	NE Name	NE ID	Card (Identifier)					
	Boston	92.168.96.46	Card Slot-1(unassigned)	T				
								Count : 1
						CANCEL	SAVE	DEPLOY

Devic	e Management	Configuration Configuration	Deployments	•													+ DEPLOYMENT 🕞 🞬
	Deployment Stat	us	Configuration	Status	NE Name		NE ID		Identifier		Template		Role		Category	:	(i) Deployment Details
		-		-		T		T		T		T		-			
	<ul> <li>Deployed Align</li> </ul>	ed	<ul> <li>Modified</li> </ul>		Boston		92.168.96.46		1		Equipment-card_mda		Physical		Card	-	Boston
																	NE ID
																	92.168.96.46
																	laentmer
																	1
																	Deployment Status
																	<ul> <li>Deployed Aligned</li> </ul>
																	AUDIT ALIGN
																	Last Audit
																	Nov 26, 2024 11:48:40 am by admin
																	Template Name
																	Equipment-card_mda
																	Nov 26, 2024 11:48:35 am
																	Last Updated Nov 26, 2024 11:48:40 am
																	Role
																	Physical
																	card
4 1 4	_														•		Configuration Status
-	Auto-refresh	Last Refresh:	2024/11/26 11:49:	:42				ĸ	Page: 1 /1	1 > >					Cour	nt : 1	<ul> <li>Moainea</li> </ul>

# Figure 7-2 NE CLI check after deployment

A:admin	n@Boston# show card state					
Card S	tate					
Slot/	Provisioned Type	Admin	Operational	Num	Num	Comments
Id	Equipped Type (if different)	State	State	Ports	MDA	
1	xcm-14s	up	up		2	
1/1	s36-100gb-qsfp28:he2400g+	up	up	36		
1/2	s36-100gb-qsfp28:he2400g+	up	up	36		
A	cpm-s	up	up			Active
В	cpm-s	up	down			Standby
	(not equipped)					

END OF STEPS

# 7.4 Port/Connector

1

# 7.4.1 To configure Port and Connectors using intent port-connector\_gsros\_23-10-1\_23-11

port-connector\_gsros\_23-10-1\_23-11 intent supports configuration of Breakout Type on connector port.

Import the intent type **port-connector\_gsros\_23-10-1\_23-11** into **Device Management**, **Configuration Intent Types**.

ent Type			Version		Status	Description		Role		Category		Device Scope	Last Updated	:	(i) Intent Type Details
		T		T		•	Т		-		*	•	MMM d, yyyy h:mm:ss		
n-equipment-card_mda				2	<ul> <li>Successful</li> </ul>	Intent-Type t	o configur	Physical		Card		SROS Classic & Model	Nov 26, 2024 11:25:43	: :	Intent Type port-connector_gsros_23-10-1_23-11
t-connector_garos_23	-10-1_23-11			1	<ul> <li>successful</li> </ul>	intent-type t	o configur	Physical		Port		SKUS Classic & Model	Nov 25, 2024 4:17:03 p	M 2	Version 1 Status Successfull Successfully imported/re-imported the intent Description Intent-type to configure connector ports Rol Physical Category Prot Device Scape SROS Classic & Model Imported Nov 26, 2024 4:15:58 pm Last Updated Nov 26, 2024 4:15:58 pm Last Updated Nov 26, 2024 4:17:09 pm Canfiguration Form default
														4.5	

2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-portconnector**.
Create Configuration Template				×
Basic Info *	Basic Info			
Configuration Intent Type *	Template Name" Equipment-port-connector Description			6
	Configuration Intent Type		0	REPLACE
	Only imported intent types will be available for selection. Go to Network Intents to view all intent types.       Intent Type     Intent Type Varsion       port-connector_gsros_23-10-1_23-11     1       Rele     Category       Physical     Port       Device Scope     SROS Classic & Model			
	Configuration Form			
	default			
	Port			
		CANCEL	SAVE AS DRAFT	RELEASE

Device Management Configuration Ter	nplates	•										+ TEMPLATE 🕞
Name	Descript	tion		Life Cycle		Target Labels	1	Intent Type	Inte	ent'	:	(i) Template Details
T		٦	T		•	T	·	Т				
Equipment-card_mda	-			released	-	-		icm-equipment-card_mda			:	C General
Equipment-port-connector	-			released	•	-		port-connector_gsros_23-10				Name Equipment-port-connector  Description  Interval of the second of th
												Created Nov 26, 2024 4:18:57 pm
Auto-refresh Last Refresh: 202	4/11/26 16:19	9:27				IC C Page: 1 /1 > >I			¢	► Coun	< → t:2	Last Updated Nov 26, 2024 4:18:57 pm

3

Create configuration deployments using the above configuration template.

For the following examples, targets are 1/1/c1 and 1/1/c2 for 7750 classic and MD nodes; selected c10-10g breakout on classic 7750 SR.



Equipment-port-connector						×
Port	Port					*
Connector	Admin State					
	enable -	□x				- 1
	Consideration (Constant)					
	Ereakout		RS FEC Mode			- 1
	c10-10g	▼ □x	none 👻	Cx		- 1
						- 1
						- 1
						- 1
						- 1
						- 1
						- 1
						-
					CANCEL	UPDATE

Deploy Physical Configuration						×
Select Template *	Select Template					REPLACE
Jeeu la gris alu Lui Jeeueu (enpare	Template Name Equipment-port-connector Category Port		Template Description  Device Scope SROS Classic & Model	Target    Plexible Yes	Labels	
	Select Targets and Edi	t Selected Tem	plate		CLI	AR ALL + TARGET
	Select targets. Template cor	figurations can be	edited after targets are select tes are assigned. View/Edit	ed.		EDIT TEMPLATE CONFIG
	NE Name	NE ID	Port (Identifier)			
	T		T	Т		
	Toronto	92.168.96.215	Port 1/1/c1			
	Toronto	92.168.96.215	Port 1/1/c2			Î
						Count : 2
					CANCEL	SAVE DEPLOY

Devi	ce Management Co Co	nfiguration Infiguration	Deployments *													+ DEPLOYMENT 🕞 🚆
	Deployment Status		Configuration Status	NE Name		NE ID		Identifier		Template		Role	Cate	gory	:	(i) Deployment Details
			-		T		T		T		T	-				
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	CE_West		92.168.99.6		1		Equipment-card_mda		Physical	Card		:	NE Name Toronto
~	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1		Equipment-port-conn		Physical	Port		+	NEID
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c2		Equipment-port-conn		Physical	Port		:	92.168.96.215
																Identifier
																Port-ID
																Port 1/1/c1
																Deployment Status
																Deployed Aligned
																AUDIT ALIGN
																Last Audit
																Nov 26, 2024 4:27:34 pm by admin
																Template Name
																Equipment-port-connector
																Created Nov 26, 2024 4:27:30 pm
																Last Updated
																Nov 26, 2024 4:27:34 pm
																Role
																Physical
																port
																Configuration Status
	4													•	4 1	Modified

Figure 7-3	NE CLI	check	after	deploy	yment
					<del>.</del>

*A:Toronto>com	nfig# /	/show	port							
Ports on Slot	1									
Port	Admin	Link	Port	Cfg	Oper	LAG/	Port	Port	Port	C/QS/S/XFP/
Id	State		State	MTU	MTU	Bndl	Mode	Encp	Type	MDIMDX
1/1/cl	Up		Link Up						conn	100GBASE-LR4*
1/1/c1/1	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/2	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/3	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/4	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/5	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/6	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/7	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/8	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/9	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/10	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c2	Up		Link Up						conn	100GBASE-LR4*
1/1/c2/1	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/2	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/3	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/4	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/5	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/6	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/7	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/8	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/9	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c2/10	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c3	Up		Down						conn	100GBASE-LR4*
1/1/c4	Up		Down						conn	100GBASE-LR4*
1/1/c5	Up		Down						conn	100GBASE-LR4*

Ex. 7750 MD

Deploy Physical Configuration									×
Select Template *	Select Template								REPLACE
Select Targets and Edit Selected Template *	Template Name Equipment-port-connect	or		Template Description		Target Labels 			
	Port			SROS Classic & Model		Yes			
	Select Targets and	d Edit Selecto	ed Templa	te			CLI	EAR ALL	+ TARGET
	Select targets. Templa	te configuration	is can be edit	ed after targets are selec	ted.			EDIT TEMPL	ATE CONFIG
	Configurations rec	uired by the select	ted templates a	are assigned. View/Edit					
	NE Name	NE ID		Port (Identifier)					
		T	T		T				
	Boston	92.168.	.96.46	1/1/c1					Î.
	Boston	92.168.	.96.46	1/1/c2					
									Count : 2
							CANCEL	SAVE	DEPLOY

Comguration	Deployments *							+ DEPLOYMENT 🕞
Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	: (i) Deployment Details
•	•		т	T	T	•		
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	1	Equipment-card_mda	Physical	Card	Boston
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1	Equipment-port-conn	Physical	Port	: NEID
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c2	Equipment-port-conn	Physical	Port	92.168.96.46
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1	Equipment-port-conn	Physical	Port	: Identifier
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2	Equipment-port-conn	Physical	Port	Port-ID
								Deployment Status © Deployment Status AUDIT ALIGN Last Audit Dec 2, 2024 11:43:22 am by admin Create Dec 2, 2024 11:43:19 am Last Updated Dec 2, 2024 11:43:22 am Refe Physical Createg Physical

A:admin@Bostor	n# show	w port	t								
Ports on Slot	1										
Port	Admin	Link	Port		Cfg	Oper	LAG/	Port	Port	Port	C/QS/S/XFP/
Id	State		State		MTU	MTU	Bndl	Mode	Encp	Type	MDIMDX
 1/1/c1	 ແບ		Link	ສປ						conn	100GBASE-LR4*
1/1/c1/1	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/2	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/3	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/4	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/5	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/6	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/7	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/8	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/9	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c1/10	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2	Up		Link	Up						conn	100GBASE-LR4*
1/1/c2/1	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/2	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/3	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/4	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/5	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/6	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/7	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/8	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/9	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c2/10	Down	No	Down		8704	8704		netw	null	xgige	
1/1/c3	Down		Down							conn	100GBASE-LR4*
1/1/c4	Down		Down							conn	100GBASE-LR4*
1/1/c5	Down		Down							conn	100GBASE-LR4*

*Figure 7-4* NE CLI check after deployment

END OF STEPS

## 7.4.2 To configure Port using intent icm-equipment-port-ethernet

icm-equipment-port-ethernet intent type deployment can be created on ethernet ports. For this use case, after connector deployment, ethernet port configuration was tested on some of the newly created ports.

1 -

## **Prerequisites:**

For Classic NE:

Accounting policy

```
/configure log accounting-policy 36 record complete-ethernet-port
/configure log accounting-policy 36 no shutdown
```

/admin save

## For MD NE:

```
    Accounting policy
```

```
/edit-config private
/configure log accounting-policy 36 record complete-ethernet-port
/commit
/quit-config
```

2 -

Import the intent type icm-equipment-port-ethernet into Device Management, Configuration Intent Types.

	Network S	ervices (	latform													User: admin 🗸 🗸
Jevice Management	Configuration Configuration	on Intent	Гур <mark>е</mark> s	•												+ IMPORT
Intent Type			Version		Status		Descriptio	n	Role		Cate	gory	Device Scope		Last Updated	: (i) Intent Type Details
		т		T					T	9	•	*		*	MMM d, yyyy h:mm:ss :	
cm-equipment-card_m	da			2	• Succes	ssful	Intent-Typ	e to configur	Phy	sical	Card		SROS Classic & Mod	el	Nov 26, 2024 11:25:43 (	: Intent Type icm-equipment-port-ethernet
port-connector_gsros_	23-10-1_23-1	1		1	• Succe	ssful	Intent-typ	e to configur	Phy	sical	Port		SROS Classic & Mod	el	Nov 26, 2024 4:17:03 pr	i Version
cm-equipment-port-et	hernet			2	<ul> <li>Succession</li> </ul>	ssful	Intent-typ	e to configur	Phy	sical	Port		SROS Classic & Mod	el	Dec 2, 2024 11:12:32 ar	1 2
																Status
																Successful     Successfully imported/re-imported the intent-t
																Description Intent-type to configure physical, breakout, xiom a satellite ports
																Role Physical
																Category Port
																Device Scope SDOS Classic & Model
																Imported
																Dec 2, 2024 11:11:59 am
																Last Updated Dec 2, 2024 11:12:32 am
																Configuration Form
																default,
																defaultIXR,
																gold,
																defaultSAR
		_		_												4 5

3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-port-ethernet**.

	1	Description		Life Cycle		Target Labels		Intent Type	Intent	1	(i) Template Details
	T		T		*		T	T			
ipment-card_mda	-	_		released	•			icm-equipment-card_mda		:	∧ General
pment-port-connector				released				port-connector_gsros_23-10		- 1	
oment-port-ethernet		_		released	-			icm-equipment-port-ethernet		:	Equipment-port-ethernet
											Description
											_
											Life Cycle
											released
											Target Labels
											Intent Tune
											icm-equipment-port-ethernet
											Intent Type Version
											2
											2 Config Form default
											2 Config Form default
											2 Config Form default Config Form State Up-to-date
											2 Config Form default Config Form State Up-to-date Role
											2 Config Form default Config Form State Up-to-date Role Physical
											2 Config Form default Config Form State Up-to-date Role Physical Chargory
											2 Config Form default Config Form State Up-to-date Rele Physical Cotegory Port
											2 config Form default Config Form State Up-to-date Rele Physical Category Port Port Device Scepe SNOS Classic & Model
											2 Config Form default Config Form State Up-to-date Rele Physical Category Port Device Scope SROS Classic & Model Fixebile
											2 Config Form default Config Form State Up-to-date Rele Physical Category Poort Device Scepe SROS Classic & Model Fluible Yes

4 -

Create configuration deployments using the above configuration template.

For the following examples, targets are 1/1/c1/1 for 7750 classic and MD nodes.

## Ex. 7750 Classic

Deployment form attribute values:

Equipment-port-ethernet							×
Port	Port						
Ethernet Hold Time	Admin State		Description				
Down When Looped	enable	• Lx	Port 1/1/cl/1				
CRC Monitor Signal Degrade Signal Failure	Ethernet Accounting Policy 36		Collect Stats				
LLDP	Autonegotiate		Dot1 Q Etype		Епсар Туре		
	Select Item	• □x	Oxffff PBB Etype		Q in Q Etype	▼ □x	
	9180						
	Speed (megabps)		Mode	• 🗔			
	Hold Time						
	Down		Units		Up		
	20		seconds	▼ □x	30		
						CANCEL	UPDATE

Equipment-port-ethernet						×
Port	Port					*
Ethernet Held Time Down When Looped SSM CRC Monitor Signal Degrade	Hold Time Down 20		units seconds - Cx		up 30	
Signal Failure	Down When Looped					
LLDP	Admin State		Keep Alive (seconds)		Retry Timeout (seconds)	
	enable	▼ □x	20		100	
	Use Broadcast Address					
	SSM					
	Admin State		Code Type			
	Select Item	• 🗔	Select Item 👻		ESMC Tunnel	
	Tx Dus					
	CRC Monitor					-
					CANCEL UP	DATE

Equipment-port-ethernet				×
Port	Port			
Ethernet Hold Time Down When Looped SSM CRC Monitor Signal Degrade Signal Degrade	CRC Monitor Window Size (seconds) 20 Signal Degrade			
LLDP	Threshold 9	Multiplier 2		
	Signal Failure Threshold 7	Multiplier 2		
	LLDP Dest MAC			+ ADD
	MAC Type Notification	Port ID Subtype Receive	Transmit	CANCEL UPDATE

Equipment-port-ethernet							×
Port	Port						-
Ethernet Hold Time Down When Looped SSM CRC Monitor Signal Degrade	Signal Failure Threshold 7		Multiplier 2				
Signal Fallure	LLDP Dest MAC MAC Type	Notification	Port ID Subtype	Receive	Transmit	+ ADD	
	nearest-bridge	true		true	true	1	
			IC C Page:	1 /1 > >1		Total: 1	
						CANCEL	UPDATE

Deploy Physical Configuration											×
Select Template *	Select Template	Select Template									REPLACE
Select Targets and Edit Selected Template *	Template Name Equipment-port-ethern Category	Template Name Equipment-port-ethernet Category			ion	- -	Target Labels — Flexible				
	Port			SROS Classic &	Model	,	Yes				
	Select Targets and Edit Selected Template							c	LEAR ALL	+ TARGET	
	Select targets. Template configurations can be edited after targets are selected.  Configurations required by the selected templates are assigned. View/Edit								EDIT TEMP	LATE CONFIG	
	NE Name	NE	ID	Port (Identifier)							
		T		T	Т						
	Toronto	92.	.168.96.215	Port 1/1/c1/1							
											Count : 1
									CANCEL	SAVE	DEPLOY

Deployment Status								
	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	(i) Deployment Details
•	•		T	т	T	-		
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	1	Equipment-card_mda	Physical	Card 1	NE Name Toronto
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1	Equipment-port-conn	Physical	Port 1	NE ID
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c2	Equipment-port-conn	Physical	Port :	92.168.96.215
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1	Equipment-port-conn	Physical	Port :	Identifier
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2	Equipment-port-conn	Physical	Port :	Port-ID
Deployed Aligned	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port :	Port 1/1/c1/1
								Last Alignment Last Alignment Dec. 2, 2024 12:18:16 pm by admin Template Name Equipment-port-ethernet Crasted Dec 2, 2024 12:18:07 pm Last Updated Dec 2, 2024 12:18:16 pm

Figure 7-5 NE CLI after deployment

```
A:Toronto>config>port# /configure port 1/1/c1/1
A:Toronto>config>port# info
        description "Port 1/1/c1/1"
        ethernet
           mode access
            encap-type dotlq
           mtu 9180
            crc-monitor
                sd-threshold 9 multiplier 2
                sf-threshold 7 multiplier 2
                window-size 20
            exit
            down-when-looped
                keep-alive 20
                retry-timeout 100
                no shutdown
            exit
            accounting-policy 36
            collect-stats
            lldp
                dest-mac nearest-bridge
                    admin-status tx-rx
                    notification
                    tx-tlvs port-desc sys-name sys-desc sys-cap
                exit
            exit
            hold-time up 30 down 20
            dotlq-etype 0xffff
        exit
        no shutdown
```

Figure 7-6	NE CLI after	deployment
------------	--------------	------------

A:Toronto# show port										
Ports on Slot	1									
Port	Admin	Link	Port	Cfg	Oper	LAG/	Port	Port	Port	C/QS/S/XFP/
Id 	State		State	MTU	MTU	Bndl	Mode	Encp	Туре	MDIMDX
1/1/cl	Up		Link Up						conn	100GBASE-LR4*
1/1/c1/1	Up	Yes	Up	1518	1518		accs	dotq	xgige	
1/1/c1/2	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/3	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/4	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/5	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/6	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/7	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/8	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/9	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/10	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c2	Up		Link Up						conn	100GBASE-LR4*
1/1/c2/1	Up	Yes	Up	1514	1514		accs	null	xgige	
1/1/c2/2	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/3	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/4	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/5	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/6	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/7	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/8	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c2/9	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c2/10	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c3	Up		Down						conn	100GBASE-LR4*
1/1/c4	Up		Down						conn	100GBASE-LR4*
1/1/c5	Up		Down						conn	100GBASE-LR4*
1/1/c6	Up		Down						conn	100GBASE-LR4*
1/1/c7	Up		Down						conn	100GBASE-LR4*
1/1/c8	Up		Down						conn	100GBASE-LR4*

## Ex. 7750 MD

Deployment form attribute values:

Equipment-port-ethernet				×
Port	Port			*
Ethernet Hold Time Down When Looped SSM CRC Monitor	Admin State enable • Cx	Description Port 1/1/c1/1		
Signal Degrade Signal Fallure LLDP	Ethernet Accounting Policy 36 Autonegotiste	Collect Stats	Encep Type	
	Select item - Cx	PSS Etypo	Dot1Q   CR Q in Q Etype	
	9180 Speed (megabpa)	Mode		
	Hold Time Down 20	Units seconds v C2	<b>Up</b> 30	
			CANCEL	UPDATE

Equipment-port-ethernet							×
Port	Port						
Ethernet. Hold Time Down When Looped SSM CRC Monitor Signal Degrade	Down When Looped Admin State enable Use Broadcast Address	* Cx	Keep Alive (seconds) 20		Retry Timeout (seconds) 100		
Signal Failure	SSM Admin State Select Item	• Ex	Code Type Select Item	• [2	ESMC Tunnel		
	CRC Monitor Window Size (seconds) 20						
	Signal Degrade						
						CANCEL	UPDATE

Equipment-port-ethernet							×
Port	Port						
Ethernet Hold Time Down When Looped SSM CRC Monitor	CRC Monitor Window Size (seconds) 20						
Signal Degrade Signal Failure LLDP	Signal Degrade Threshold 9		Multiplier 2				
	Signal Failure Threshold 7		Multiplier 2				
	LLDP Dest MAC MAC Type	Notification	Port ID Subtype	Receive	Transmit	+ ADD	
	мас туре	Notification	Porcio Subtype	Neverve	Thenen	CANCEL	UPDATE

Equipment-port-ethernet							×	
Port	Port						*	
Ethernet Hold Time Down When Looped SSM CRC Monitor Signal Degrade	Signal Failure Threshold 7	Signal Failure Threshold Multiplier 7 2						
Signal Failure LLDP	LLDP Dest MAC			- 11-100		+ ADD		
	MAC Type	Notification	Port ID Subtype	Receive	Transmit			
	nearest-bridge	true		true	true	1		
			IK K Page: 1	<i>I</i> 1 > >I		Total: 1	*	
						CANCEL	UPDATE	

Deploy Physical Configuration													×
Select Template *	Select Template												
Select largets and Loit Selected lemplate "	Template Name Equipment-port-ethernet Category Port		Template Description — Device Scope SROS Classic & Model	Template Description  Device Scope SROS Classic & Model		Target Labels — Flaxible Yes							
	Select Targets ar	nd Edit S	elected Te	empla	te								
	Select targets. Template configurations can be edited after targets are selected.  Configurations required by the selected templates are assigned. View/Edit								1	EDIT TEMPL	ATE CONFIG		
	NE Name		NE ID		Port (Identifier)								
		T		T		T							
	Boston		92.168.96.46		1/1/c1/1								
													Count : 1
												CANCEL	DEPLOY

Deployment State Ceffiguration State NE Name NE lon V Cemployment Port Cemployment Por	Device Management	evice Management Configuration Configuration Deployments + DEPLOYMENT C													
Image: Image	Deployment	t Status	Configuration Status	NE Name		NEID		Identifier		Template		Role	Categor	y :	(i) Deployment Details
Opployed Aligned Ordelind CE_Wett 02168.96.0 1 Equipment-ord_mda Physical Card 1 Biolometric Communic Opployed Aligned Ordelind Toronto 02168.96.215 Port 1/1/c1 Equipment-port.comm. Physical Port 10 Port 10 Port 10 Port 10 Port 10 Physical Ordelind Or		•	•		T		T		T		T	-			
Opployed Aligned Modified Toronto 92.168.96.215 Port 1/1/c1 Equipment-port-con Physical Port 1   Opployed Aligned Modified Toronto 92.168.96.45 1/1/c1 Equipment-port-con Physical Port 1   Opployed Aligned Modified Boston 92.168.96.45 1/1/c1 Equipment-port-con Physical Port 1   Opployed Aligned Modified Toronto 92.168.96.45 1/1/c1 Equipment-port-con Physical Port 1   Opployed Aligned Modified Toronto 92.168.96.45 Port 1/1/c1/1 Equipment-port-con Physical Port 1   Opployed Aligned Modified Boston 92.168.96.45 Port 1/1/c1/1 Equipment-port-cont Physical Port 1   Opployed Aligned Modified Boston 92.168.96.45 1/1/c1/1 Equipment-port-cont Physical Port 1   Opployed Aligned Modified Boston 92.168.96.45 1/1/c1/1 Equipment-port-cont Physical Port 1   AUDT ALIGN   AUDT ALIGN   Boston 92.168.96.45 1/1/c1/1 Equipment-port-cont Physical Port 1   AUDT ALIGN   Boston 92.168.96.46 1/1/c1/1 Equipment-port-cont Physical Port 1   AUDT ALIGN Equipment-port-cont Physical Port Equipment-port-cont Physical <td><ul> <li>Deployed A</li> </ul></td> <td>Aligned</td> <td><ul> <li>Modified</li> </ul></td> <td>CE_West</td> <td></td> <td>92.168.99.6</td> <td></td> <td>1</td> <td></td> <td>Equipment-card_mda</td> <td></td> <td>Physical</td> <td>Card</td> <td>:</td> <td>NE Name Boston</td>	<ul> <li>Deployed A</li> </ul>	Aligned	<ul> <li>Modified</li> </ul>	CE_West		92.168.99.6		1		Equipment-card_mda		Physical	Card	:	NE Name Boston
<ul> <li>Opelowed Aligned</li> <li>Modified</li> <li>South and the set of the</li></ul>	Deployed A	Aligned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1		Equipment-port-conn.		Physical	Port	:	NE ID
• Opelowed Aligned • Modified Boston 92.168.96.46 1/1/c1 Equipment-port-com Physical Port I   • Deployed Aligned • Modified Boston 92.168.96.45 Port 1/1/c1/1 Equipment-port-ether Physical Port I   • Deployed Aligned • Modified Boston 92.168.96.45 Port 1/1/c1/1 Equipment-port-ether Physical Port I   • Deployed Aligned • Modified Boston 92.168.96.45 1/1/c1/1 Equipment-port-ether Physical Port I   • Deployed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port I   • Opeloyed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port I   • Opeloyed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port I   • Opeloyed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port I   • Opeloyed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port I   • Opeloyed Aligned • Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical I I   • Opeloyed Aligned • Modified • Modified • Modified • Modified • Modified <td><ul> <li>Deployed A</li> </ul></td> <td>Aligned</td> <td><ul> <li>Modified</li> </ul></td> <td>Toronto</td> <td></td> <td>92.168.96.215</td> <td></td> <td>Port 1/1/c2</td> <td></td> <td>Equipment-port-conn.</td> <td></td> <td>Physical</td> <td>Port</td> <td>:</td> <td>92.168.96.46</td>	<ul> <li>Deployed A</li> </ul>	Aligned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c2		Equipment-port-conn.		Physical	Port	:	92.168.96.46
• Oeployed Aligned   • Modified • Boeployed Aligned   • Modified   • Tornto • 2.168.96.46 • Deployed Aligned • Modified • Boeployed Aligned • Modified • Boeployed Aligned • Modified • Modified • Boeployed Aligned • Modified • Boeployed • Modified • Boeployed Aligned • Modified • Modified • Deployed Aligned • Deployed Aligned • List Aligned • Deployed Aligned • Deployed Aligned • List Aligned • Deployed Aligned • Deployed Aligned • List Aligned • Deployed	Deployed A	Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c1		Equipment-port-conn.		Physical	Port	:	Identifier
Opeloyeed Aligned ● Modified Toronto 92.168.96.215 Port 1/1/c1/1 Equipment-port-ether Physical Port i 1     Opeloyeed Aligned ● Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ● Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Boston 92.168.96.46 1/1/c1/1 Equipment-port-ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port ether Physical Port i     Opeloyeed Aligned ■ Modified Boston 92.168.96.46 1/1/c1/1 Equipment-port ether Physical Port i     Opeloyeed Aligned ■ Port	Deployed A	Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c2		Equipment-port-conn.		Physical	Port	:	Port-ID
• Deployed Aligned         • Modified         Boston         92.168.96.46         1/1/c1/1         Equipment-port-ether         Physical         Port         E           • Deployed Aligned         • Modified         Boston         92.168.96.46         1/1/c1/1         Equipment-port-ether         Physical         Port         • Deployed Aligned           • Deployed Aligned         • V         • V         • V         • V         • V         • Deployed Aligned           • Deployed Aligned         • V         • V         • V         • V         • V         • V         • V         • Deployed Aligned           • Deployed Aligned         • V <td>Deployed A</td> <td>Aligned</td> <td><ul> <li>Modified</li> </ul></td> <td>Toronto</td> <td></td> <td>92.168.96.215</td> <td></td> <td>Port 1/1/c1/1</td> <td></td> <td>Equipment-port-ether.</td> <td></td> <td>Physical</td> <td>Port</td> <td>:</td> <td>1/1/c1/1</td>	Deployed A	Aligned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1/1		Equipment-port-ether.		Physical	Port	:	1/1/c1/1
Spelyment State       • Deplyment State         • Deplyment State       • Deplyment State         • AUDT       • ALISN         • List Audit       • International State         • Deplyment State       • International State         • International State       • International State         • International State       • International State         • International State       • Internat         • Inter	<ul> <li>Deployed A</li> </ul>	Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c1/1		Equipment-port-ether.		Physical	Port	1	
Category port															AUDIT ALIGN AUDIT ALIGN Last Audit Last Audit Dec 2, 2024 12:3 1:33 pm by admin Tomplas Name Equipment-port-ethernet Constad Dec 2, 2024 12:3 1:31 pm Last Updated Dec 2, 2024 12:3 1:33 pm Rele Physical Cotegory port Configuration Status
> < • • • • • • • • • • • • • • • • • •	→ <												+	• •	<ul> <li>Modified</li> </ul>



```
(pr) [/configure port 1/1/c1/1]
A:admin@Boston# info
    admin-state enable
    description "Port 1/1/c1/1"
    ethernet {
        accounting-policy 36
        collect-stats true
        mode access
        encap-type dotlq
        mtu 9180
        hold-time {
            units seconds
            up 30
            down 20
        crc-monitor {
            window-size 20
            signal-degrade {
                threshold 9
                multiplier 2
            signal-failure {
                threshold 7
                multiplier 2
        down-when-looped {
            admin-state enable
            keep-alive 20
            retry-timeout 100
        lldp {
            dest-mac nearest-bridge {
                notification true
                receive true
                transmit true
                tx-tlvs (
                    port-desc true
                    sys-name true
                    sys-desc true
                    sys-cap true
                tx-mgmt-address system {
                    admin-state enable
```

Figure 7-8 N	E CLI after	deployment
--------------	-------------	------------

A:admin@Bostor	n# shov	v port	t							
Ports on Slot	1									
Port Id	Admin State	Link	Port State	Cfg MTU	Oper MTU	LAG/ Bndl	Port Mode	Port Encp	Port Type	C/QS/S/XFP/ MDIMDX
1/1/cl	Up		Link Up						conn	100GBASE-LR4*
1/1/c1/1	Up	No	Down	1518	1518	-	accs	dotq	xgige	
1/1/c1/2	Up	No	Down	8704	8704	-	netw	null	xgige	
1/1/c1/3	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/4	Up	No	Down	8704	8704		netw	null	xgige	
1/1/c1/5	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/6	Up	Yes	Up	8704	8704		netw	null	xgige	
1/1/c1/7	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c1/8	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c1/9	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c1/10	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2	Up		Link Up						conn	100GBASE-LR4*
1/1/c2/1	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/2	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/3	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/4	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/5	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/6	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/7	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/8	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/9	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c2/10	Down	No	Down	8704	8704		netw	null	xgige	
1/1/c3	Down		Down						conn	100GBASE-LR4*
1/1/c4	Down		Down						conn	100GBASE-LR4*

END OF STEPS

# 7.4.3 To configure Ethernet Port using intent port-eth\_msros\_23-10-1\_24-4

port-eth\_msros\_23-10-1\_24-4 supports configuration of ethernet port on MD NE.

## 1 —

### **Pre-configuration:**

#### oper-group

• /configure service oper-group "OperGroup-1"

#### dist-cpu-protection

 /configure system security dist-cpu-protection policy "port-cpu-protect-1" type port

#### accounting-policy

• /configure log accounting-policy 20

#### port scheduler policy

• /configure qos port-scheduler-policy "port-sch-policy-1"

#### hw-agg-shaper-scheduler-policy

/configure qos hw-agg-shaper-scheduler-policy
 "hw-agg-shaper-sch-pol-1"

#### 2 -

Import intent type **port-eth\_msros\_23-10-1\_24-4** into **Device Management**, **Configuration Intent Types**.

Device Management Configuration Configuration	n Intent Types	Ŧ							+ IMPORT C-
Intent Type	Version		Status	Description	Role	Category	Device Scope	Last Updated	i Intent Type Details
	T	T	-	T	•	•	•	MMM d, yyyy h:mm:ss	
icm-equipment-card_mda		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 ;	port-eth_msros_23-10-1_24-4
port-connector_gsros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Nov 26, 2024 4:17:03 pi	Version
icm-equipment-port-ethernet		2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Dec 2, 2024 11:12:32 ar	1
icm-equipment-port-access-ce		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Dec 2, 2024 1:19:32 pm	Status
port-eth_muros_23-10-1_24-4		1	● Succesful	Intent-Type to configur	Physical	Port	SROS Model	Dec 2, 2024 1:51:20 pm 1	<ul> <li>Successful</li> <li>Successfully imported/re-imported the intent-type</li> <li>Description</li> <li>Intent-Type to configure category port and device-config port</li> <li>Rele</li> <li>Physical</li> <li>Creagery</li> <li>Port</li> <li>Device Scepe</li> <li>Serkos Model</li> <li>Imported</li> <li>Dec 2, 2024 1:51:04 pm</li> <li>Leat Upided</li> <li>Dec 2, 2024 1:51:20 pm</li> <li>Cenfiguration form</li> <li>default</li> </ul>
4								▶ ∢	Þ
Auto-refresh Last Refresh	2024/12/2 13:51:35				I< C Page:	1 /1 > >		Count : 5	

#### 3 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-port-eth-msros**.

ame		Description		Life Cycle		Target Labels		Intent Type	Intent '	:	(i) Template Details
	T		Ŧ		-		T	T			U reinplace Decans
uipment-card_mda		-		released		-		icm-equipment-card_mda		:	∧ General
uipment-port-connector		-		released		_		port-connector_gsros_23-10		:	
upment-port-ethernet		-		released				icm-equipment-port-ethernet		:	Name Equipment-port-eth-msros
ipment-port-access-ce				released		_		icm-equipment-port-access-ce		:	Description
ipment-port-eth-msros		-		released		—		port-eth_msros_23-10-1_24-4		:	
											released Torget Labels — Intent Type port-eth_msros_23-10-1_24-4 Intent Type Version 1 Config Form
											default Config Form State Up-to-date Rele Physical Category Port Device Scope SROS Model Flasible Yes Created
	þ. s								×	4 3	default Cong Fern State Up-to-date Physical Execution Port Device Scope SROS Model Fixible Yes Crasted Dec 2, 2024 1:56:47 pm

4

Create configuration deployments using the above configuration template. For the following example, targets are 1/1/c2/1 for 7750 MD nodes.

Deploy Physical Configuration						×
Select Template *	Select Template					REPLACE
Select largets and Loit Selected lemplate -	Template Name Equipment-port-eth-msros Category Port		Template Description  Device Scope SROS Model		Targot Labels — Flexible Yes	
	Select Targets and Ec	CLEAR ALL + TARGET				
	Select targets. Template co	onfigurations can b I by the selected temp	e edited after targets are s plates are assigned. View/Ed	elected.		EDIT TEMPLATE CONFIG
	NE Name	NE ID	Port (Identifier)			
	•	T	T	Т		
	Boston	92.168.96.46	1/1/c2/1			Court : 1
						CANCEL SAVE DEPLOY

Attribute values in the configuration deployment form:

Equipment-port-eth-msros							×
Port	Port						i i
Dist CPU Protection	Admin State		Description				
Percentage Of Rate	enable 👻	- Cx	Port 1/1/c2/1		DDM Events		
Scheduler			Oper Group		Monitor Oper Group		
Access	Monitor Agg Egress Queue Stats		OperGroup-1	×		×	
Egress							
Ingress	Dist CPU Protection						
DWDM							
Coherent	port-cou-protect-1	×					
Sweep	por e epo protece r						
Ethernet							
Down On Internal Error	Modify Buffer Allocation						
Hold Time							
Loopback	-						
Report Alarm	Percentage Of Rate						
CRC Monitor	Egress		Ingress				
Signal Degrade	500		500				
Dampening							
*							
						CANCEL	UPDATE

ipment-port-eth-msros					
	Port				
ist CPU Protection	Access				
odify Buffer Allocation					
Percentage Of Rate					
cheduler	Egress				
tcess	Pool				+ ADD
Egress	Name	Amber Alarm	Red Alarm Threshold	Slope Policy	
Ingress		i nresnoid (percent)	(percent)		
NDM	default	85	95	default	:
Coherent					
Sweep					
hernet					
Down On Internal Error					
Hold Time					
Loopback			1< < Page: 1	71 > >i	Total: 1
Report Alarm					
CRC Monitor					
CRC Monitor Signal Degrade	Ingress				
CRC Monitor Signal Degrade Signal Fallure	Ingress				
CRC Monitor Signal Degrade Signal Failure Dampening	Ingress				+ ADD

<i></i>	Port					
st CPU Protection odify Buffer Allocation	Ingress					
Percentage Of Rate	Pool				+ ADD	
heduler	Name	Amber Alarm Threshold (percent)	Red Alarm Threshold (percent)	Slope Policy		
ess						
gress	default	83	96	default	1	
gress						
M						
oherent						
Sweep						
Sweep						
Sweep rnet own On Internal Error			I< C Page: 1	/1 >> >X	Total: 1	
Sweep smet Iown On Internal Error Iold Time			IK K Page: 1	R X X	Totał: 1	
Sweep rnet own On Internal Error old Time oopback			IC C Page: 1	71 > 31	Total: 1	
Sweep rnet own On Internal Error ald Time aopback eport Alarm	DWDM		K C Page: 1	71 > 31	Total: 1	
Sweep rret avm On Internal Error ald Time popback aport Alarm RC Monitor	DWDM		IK < Page: 1	n x x	Total: 1	
Sweep rrret own On Internal Error old Time port Alarm RC Monitor Signal Degrade	DWDM Prequency (meguhertz)		K < Page: 1	/1 × 1	Total: 1	
Sweep vown On Internal Error old Time oopback eport Alarm RC Monitor Signal Degrade Signal Degrade	DWDM Prequency (megahertz)		K < Page: 1	n x x	Total: 1	
Sweep sweep own On Internal Error old Time oopback eport Alarm RC Monitor Signal Degrade. Signal Degrade.	DWDM Prequency (megahertz)		K C Page: 1	اد د <i>۱</i> ۱	Total: 1	

quipment-port-eth-msros								
ort	Port							
Dist CPU Protection	Ethomet							
Modify Buffer Allocation	Ethernet							
Percentage Of Rate	Accounting Policy		Autonegotiate					
Scheduler	20	×	Select Item	*	Cx	Collect Stats		
Assess	Dot1Q Etype		Duplex					
Egrare	0x600		Select Item	•		LACP Tunnel		
Ingress	Load Balancing Algorithm		MAC Address			Min Frame Length (bytes)		
DWDM	default	• 🕞	00:B0:D0:63:C2:25			64		
Coherent	Mode		Епсар Туре			MTU (bytes)		
Sweep	network	• Cx	Dot1Q	•		512		
Ithernet			PBB Etype			PTP Asymmetry (nanoseconds)		
Down On Internal Error	MTU Profile							
Hold Time	QinQ Etype		Rs FEC Mode					
Loopback			Select Item	•		Single Fiber		
Report Alarm	Speed (megabps)		Util Stats Interval (seconds)			XGIG		
CRC Monitor						Select Item	• Cx	
Signal Degrade	Discord By Davies Season							
Signal Failure	Discard RX Pause Frames							
Dampening								
	· · · · · ·							

Equipment-port-eth-msros					×
Port	Port				*
Dist CPU Protection Modify Buffer Allocation Percentage Of Rate	Hold Time Units		Up	Down	
Scheduler	seconds	▼ ⊑x	20	30	_
Access					
Egress Ingress	Loopback				
DWDM	Direction		Swan Src Dst MAC		
Coherent	Select Item	▼ Cx	0		
Sweep					
Down On Internal Error	Report Alarm				
Hold Time	Signal Fail		Remote	Local	
Report Alarm	Frame Not Locked		High Ber	Block Not Locked	
CRC Monitor	Alignment Marker Not Locked		Duplicate Lane		
Signal Degrade					
Signal Failure Dampening	CRC Monitor				
				c	ANCEL UPDATE

Equipment-port-eth-msros					×
Port	Port				
Dist CPU Protection					
Modify Buffer Allocation	CRC Monitor				
Percentage Of Rate	Window Size (seconds)				
Cabadular	60				
scheduler					
Access					
Egress	Signal Degrade				
Ingress	Threshold		Multiplier		
DWDM	9		2		
Coherent					
Sweep					
Ethernet					
Down On Internal Error	Signal Failure				
Down on Internal Error	Threshold		Multiplier		
Hold Time	8		2		
Loopback					
Report Alarm					
CRC Monitor					
Signal Degrade	Dampening				
Signal Failure	Admin State		Half Life (seconds)	Max Suppress Time (seconds)	
Dampening	enable	• Cx	70	80	
internetinetin <del>-</del> i	*				
				CANCE	L UPDATE

Equipment-port-eth-msros							×
Report Alarm	Port						
CRC Monitor	Dampening						
Signal Degrade	Admin State		Half Life (seconds)		Max Suppress Time (seconds)		
Signal Failure	enable	▼ □x	70		80		
Dampening	Reuse Threshold (penalties)		Suppress Threshold (penalties)				
Down When Looped	6		8				
ETH CFM							
Ingress							
SSM	Down When Looped						
Symbol Monitor							
Signal Degrade	Admin State		Keep Alive (seconds)		Retry Timeout (seconds)		
Signal Failure	Select Item	▼ <b></b>					
Storm Control	Use Broadcast Address						
EFM OAM							
Discovery							
Advertise Capabilities	ETH CFM						
Link Monitoring	MEP					+ ADD	
Errored Frame	MEDID	MA Admin Namo	MD Admin Namo	Admin State	Description	MAC Addross	
Errored Frame Period			Admin Name	Administate	Description	MAC AUGIESS	
Errored Frame Seconds							
						CANCEL	UPDATE

oment-port-eth-msros					
eoort Alarm	Port				
CRC Monitor	Ingress				
Signal Degrade	Parts (membra)				
Signal Failure	200				
Dampening					
Jown When Looped					
TH CFM	SSM				
ngress			- 10 - 11 - 11 - 11		
SM	Admin State		Code Type	Esmc Tunnel	
ymbol Monitor	Seleccitem	↓ L <sub>x</sub>	Select item	· Lx	
Signal Degrade	Tx Dus				
Signal Failure					
itorm Control	Cumbal Manitan				
FM OAM	Symbol Monitor				
Discovery	Admin State		Window Size (seconds)		
Advertise Capabilities	Select Item	▼ ⊑x			
Link Monitoring					
Errored Frame	Signal Degrade				
Errored Frame Period	Threshold		Multinline		
Errored Frame Seconds	*				
					CANCEL

pment-port-eth-msros				
Info Notification	* Port			
Peer RDI Rx	Port Scheduler Policy			
Dot1x	Bolizy Name			
Macsec	port-sch-policy-1	×		
Exclude Protocol				
Re Authentication				
Per Host Authentication	Overrides			
Allowed Source MACs				
Egress				
Port QOS Policy	Max Rate			
HS Scheduler Policy	Rate Or Percent Rate	Rate (kilobps)		
Overrides	Rate	- 65532	×	
Port Scheduler Policy				
Overrides	Level			+ ADD
Max Rate	Priority Lavel			
HW Agg Shaper Scheduler				
LLDP	5			:
Network	-			
Egress				
Port Queues	<b>*</b>			
				CANCEL

	* D +				
Info Notification	Port				
Peer RDI Rx	HW Agg Shaper Scheduler				
Dot1x	Policy Name				
Macsec	hw-agg-shaper-sch-pol-1	×	Monitor		
Exclude Protocol					
Re Authentication	HS Secondary Shaper			+ ADD	
Per Host Authentication	Secondary Shaper Description				
Allowed Source MACs	Name				
gress	secondary-shaper-2			:	
Port QUS Policy					
Overrides					
Port Scheduler Policy					
Overrides					
Max Rate			1/ / Barner 1 /1 > >>	Total: 1	
HW Agg Shaper Scheduler			is stroge. It is a	Total. 1	
LDP					
Network					
Network	LLDP				

LOCAL OF ALLING							
Info Notification	Port						
Peer RDI Rx	LLDP						
Dot1x							
Macsec	Dest MAC					+ ADI	D
Exclude Protocol	MAC Type	Notification	Port ID Subtype	Receive	Transmit	Tunnel Nearest Bridge	
Re Authentication							
Per Host Authentication	nearest-bridge	true	tx-local	true	true		:
Allowed Source MACs							
0000							
Bicoo							
Port OOS Policy	1						
Port QOS Policy							
Port QOS Policy HS Scheduler Policy	4					• •	Þ
Port QOS Policy HS Scheduler Policy Overrides	<		ik k Page: :	1 /1 > >I		Total:	» 1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy			ik K Page.	/1 > >I		► ∢ Total:	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides			ik < Page:	/1 5 3l		► 4 Total:	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate			ik K Page:	1 1 5 51		► ∢ Total:	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate HW Agg Shaper Scheduler	<		ik K Page:	I /1 → →I		Totak	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate HW Agg Shaper Scheduler LDP	Network Accounting Policy		K < Page:	(1 > >)		► d Total:	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate HW Agg Shaper Scheduler LDP	< Network Accounting Policy		IK K Page:			Total:	1
Port QOS Policy HS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate HW Agg Shaper Scheduler LDP Letwork Egress	Network     Accounting Policy		K C Page:			Total:	1
Port Q02 Policy MS Scheduler Policy Overrides Port Scheduler Policy Overrides Max Rate HW Agg Shaper Scheduler LDP Etwork Egress Port Queues	Network Accounting Policy	2	K Collect Stats			Total	۶ ۱

DOLTX						
Macsec	Port					
Exclude Protocol	Egress					
Re Authentication	Queue Policy					
Per Host Authentication	default	×				
Allowed Source MACs						
Egress	Queue Group					+ ADD
Port QOS Policy	Instance ID	Queue Group Name	Description	Accounting Policy	Collect Stats	HS Turbo
HS Scheduler Policy						
Overrides						
Port Scheduler Policy						
Overrides			No da	ta to display		
Max Rate						
HW Agg Shaper Scheduler						
LLDP	•					P 1 P
Network			IC C Page:	0 /0 > >		Total: 0
Egress						
Port Queues						
Overrides	Port Queues					
NSS						

## Figure 7-9 Final successful deployment

Configuratio	in Deployments										
Deployment Status	Configuration Status	NE Name	NE ID		Identifier		Template	Ro	le	:	(i) Deployment Details
•	•		T	T		T		T	•		10 No
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		1		Equipment-card_mda	Pł	iysical	:	Boston
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1		Equipment-port-connector	Pł	iysical	:	NE ID
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c2		Equipment-port-connector	Pł	iysical		92.168.96.46
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1		Equipment-port-connector	Pł	iysical	:	Identifier
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c2		Equipment-port-connector	Pł	iysical	:	PORT-ID
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1/1		Equipment-port-ethernet	Pł	iysical		1/1/02/1
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1/1		Equipment-port-ethernet	Pł	iysical	:	
											Last Audit — Last Alignment Dar 2: 2024 2:44:51 nm by admin
											Template Name Equipment-port-eth-msros Created Dec 2, 2024 2:44:47 pm
											Last Updated Dec 2, 2024 2:44:51 pm Role
											Physical Category port
						_					Configuration Status

Figure 7-10 NE CLI after deployment

```
(pr) [/configure port 1/1/c2/1]
A:admin@Boston# info
   admin-state enable
   description "Port 1/1/c2/1"
   ddm-events true
   monitor-agg-egress-queue-stats true
   oper-group "OperGroup-1"
   dist-cpu-protection {
        policy "port-cpu-protect-1"
   modify-buffer-allocation {
        percentage-of-rate {
            egress 500
            ingress 500
        3
   access {
        egress {
            pool "default" (
                amber-alarm-threshold 85
                red-alarm-threshold 95
                slope-policy "default"
                resv-cbs (
                    cbs 87
                    amber-alarm-action (
                        step 78
                        max 93
            3
        )
        ingress (
            pool "default" (
                amber-alarm-threshold 83
                red-alarm-threshold 96
                slope-policy "default"
                resv-cbs (
                    cbs 79
                    amber-alarm-action {
                        step 75
                        max 95
```

Íssue 4

Figure 7-11 NE CLI after deployment

```
ethernet {
    dotlq-etype 0x600
    lacp-tunnel true
    load-balancing-algorithm default
    mac-address 00:b0:d0:63:c2:25
    min-frame-length 64
    mode network
    encap-type dotlq
    mtu 512
    hold-time (
        units seconds
        up 20
        down 30
    report-alarm (
        signal-fail false
        remote true
        frame-not-locked false
        duplicate-lane false
    crc-monitor {
        window-size 60
        signal-degrade {
            threshold 9
            multiplier 2
        signal-failure {
            threshold 8
            multiplier 2
    dampening [
        admin-state enable
        half-life 70
        max-suppress-time 80
        reuse-threshold 6
        suppress-threshold 8
    ingress {
        rate 200
    ssm {
        tx-dus false
    з
```

Figure 7-12 NE CLI after deployment

```
egress (
    port-scheduler-policy {
        policy-name "port-sch-policy-1"
        overrides {
            max-rate {
                rate 65532
            level 5 {
                rate (
                    pir 6000
                    cir 5000
            2
    hw-agg-shaper-scheduler {
        policy-name "hw-agg-shaper-sch-pol-1"
        monitor true
11dp (
    dest-mac nearest-bridge {
        notification true
        port-id-subtype tx-local
        receive true
        transmit true
        tx-tlvs {
            port-desc true
            sys-name true
            sys-desc true
        tx-mgmt-address system {
            admin-state enable
network {
    collect-stats false
    egress {
        queue-policy "default"
```

NSP

END OF STEPS

# 7.5 BFD Templates

## 7.5.1 To configure BFD Templates using bfd-bfd-template\_gsros intent

1 -

Import intent type **bfd-bfd-template\_gsros\_23-10-1\_23-11** into **Device Management**, **Configuration Intent Types**.

Device Management Configuration Configuration Is	ntent T	ypes	•									+ IMPORT O
Intent Type		Version		Status	Description	Role	Category		Device Scope	Last Updated :		i) Intent Type Details
	T		T	-	T		-	-	•	MMM d, yyyy h:mm:ss a		
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Phy	ical Card		SROS Classic & Model	Nov 26, 2024 11:25:43 :		ntent Type ofd-bfd-template gsros 23-10-1 23-11
port-connector_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Phy	ical Port		SROS Classic & Model	Nov 26, 2024 4:17:03 pi		/ersion
icm-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Phy	ical Port		SROS Classic & Model	Dec 2, 2024 11:12:32 ar		1
icm-equipment-port-access-ce			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Phy	ical Port		SROS Classic	Dec 2, 2024 1:19:32 pm		itatus
port-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Phy	ical Port		SROS Model	Dec 2, 2024 1:51:20 pm		• Sussessful
system-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Log	cal System		SROS Model	Dec 2, 2024 3:52:48 pm		Successfully imported/re-imported the intent-type
bfd-bfd-template_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Log	cal BFD		SROS Classic & Model	Dec 3, 2024 11:01:55 ar		successionly imported the intent-type
												ntent-Tipe to configure brid brid-template logical server SFD Device Scope RSO Classic & Model mported Dec 3, 2024 11:01:48 am azt Updated Dec 3, 2024 11:01:55 am Configuration Form
Auto-refresh Last Refresh: 2	024/12	/3 11:11:14					< Page: 1 /1 >			Count: 7	P	

2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-bfd-template**.

ama										
	_	Description		Life Cycle		Target Labels		Intent Type	Intent':	i) Template Details
	T		T		•		T	T		A. Consul
upment-card_mda		-		released	•	-		icm-equipment-card_mda	1	A General
ipment-port-connector		-		released	•	-		port-connector_gsros_23-10	1	Name
pment-port-ethernet				released	٠	-		icm-equipment-port-ethernet	1	Equipment-bfd-template
pment-port-access-ce				released	*	-		icm-equipment-port-access-ce	1	Description
pment-port-eth-msros		<u></u>		released	*			port-eth_msros_23-10-1_24-4	1	
ipment-Ildp-msros		<u>1999</u>		released		-		system-Ildp_msros_23-10-1	1	Life Cycle
pment-bfd-template		-		released		-		bfd-bfd-template_gsros_23-1	1	released
										Cenfig Form default Cenfig Form State Up-to-date
										Role Logical Category
										BFD Device Scope SROS Classic & Model
										Floxible Yes Created

3

Create configuration deployments using the above configuration template. Example 1: On 7250 IXR-6 node in MD mode

Equipment-bfd-template						×
BFD Template	BFD Template					*
	Echo Receive (milliseconds)	Multiplier		Receive Interval (milliseconds)		
	400	2		400		
	Transmit Interval (milliseconds)	Туре 🕲				
	800	Select Item	▼ □x			
					CANCEL	UPDATE

Deploy Logical Configuration				×
Select Templates * Select Targets and Edit Selected Template *	Select Templates	CLEAR ALI	L + ТЕ	MPLATE
Assign identifier for Selected Template *			Cc	sunt : 1
	Select Targets and Edit Selected Template	CLEAR	ALL +	TARGET
	Select targets. Template configurations can be edited after targets are selected.  Configurations required by the selected templates are assigned. View/Edit	VIEW/EDIT	T TEMPLATE	CONFIG
	Reachability NE Name NE ID Management IP Product			
	● Up CE_West 92.168.99.6 135.249.152.19 7250 UXR			
			Co	sunt : 1
	Assign Identifier for Selected Template			
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.			
	BFD Template Name* bfd-template-A X			
		CANCEL	SAVE	DEPLOY

Devi	ce Management Configuration	Deployments •										+ DEPLOYMENT 🕞
	Deployment Status	Configuration Status	NE Name	NE ID		Identifier		Template	Role	Category	:	i Deployment Details
	-	•		T	T		T	T	-			
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		1		Equipment-card_mda	Physical	Card	:	NE Name CE West
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1		Equipment-port-conn	Physical	Port	:	NEID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c2		Equipment-port-conn	Physical	Port	:	92.168.99.6
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1		Equipment-port-conn	Physical	Port	:	Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c2		Equipment-port-conn	Physical	Port	:	BFD Template Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1/1		Equipment-port-ether	Physical	Port	:	bfd-template-A
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1/1		Equipment-port-ether	Physical	Port	:	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c2/1		Equipment-port-eth	Physical	Port	:	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		bfd-template-A		Equipment-bfd-template	Logical	BFD	1	Deployed Aligned
]	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		sbfd-reflector-A		Equipment-bfd-sbfd-r	Logical	BFD	:	AUDIT
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		0#0.0.0.0#system		Router-ospf-interface	Logical	Router	:	
]	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		0#system		Router-isis-interface	Logical	Router	:	Last Audit
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1#1.1.1.1		Router-ospf-area	Logical	Router	:	_
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		toNodeB		Router-interface-msros	Logical	Router	:	Last Alignment
												Template Name Equipment-bifd-template Dec 3, 2024 11:51:08 am Last Updated Dec 6, 2024 5:50:40 pm Rele Logical Category BFD
•	4				_						4 1	Configuration Status
	And address of the second s	2027/02/042/042/042				(						<ul> <li>Modified</li> </ul>

Figure 7-13 NE CLI after deployment



Example 2: On 7750 SR-14s node in MD mode

Equipment-bfd-template				×							
BFD Template	BFD Template										
	Echo Receive (milliseconds)	Multiplier	Receive Interval (milliseconds)								
	400	2	100000								
	Transmit Interval (milliseconds)	Туре 🕲									
	10	cpm-np 👻									
				-							
				CANCEL UPDATE							
=	NOCIA Network S	ervices Platform									User: admin 🗸 🕜
------	---------------------------------------	------------------------------	---------	---------------	---	-----------------------	------------------------	---------	----------	-----	---
Devi	ce Management Configuration	n Deployments 👻									+ DEPLOYMENT 🕞 🖀
	Deployment Status	Configuration Status	NE Name	NE ID		Identifier	Template	Role	Category	:	Deployment Details
	•	*		T	T		r	T -			
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0		TransCanadian Railway	Customer_Template	Logical	Service	:	NE Name Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		cpm	System_Security_Cpm	Logical	System	1	NEID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		cpm	System_Security_Cpm	Logical	System		92.168.96.46
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		lldp	Lldp_md_Template	Logical	System		Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		23	System_Cpu_Protectio	Logical	System	:	BFD Template Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		ptp	System_PTP_Template	Logical	PTP	:	bfd-template-A
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		ptp	System_PTP_Template	Logical	PTP	:	
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		bfd-template-A	Equipment-bfd-template	Logical	BFD	:	Deployment Status
✓	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		bfd-template-A	Equipment-bfd-template	Logical	BFD	1	<ul> <li>Deployed Aligned</li> </ul>
											AUDIT ALIGN
											Last Audit
											 Last Alignment
											Jan 7, 2025 3:45:15 pm by admin
											Template Name Equipment-bfd-template
											Created Jan 7, 2025 3:45:13 pm
											Last Updated Jan 7, 2025 3:45:15 pm
											Role Logical
											Category BFD
											Configuration Status
	4									4 1	Modified
	Auto-refresh Last Refres	h: 2025/1/7 15:47:54				< Page: 1 /1 >			Count	: 9	

Figure 7-14 NE CLI after deployment



END OF STEPS

## 7.5.2 Configure BFD Templates using bfd-sbfd-reflector-msros intent

1

Import intent type **bfd-sbfd-reflector\_msros\_23-10-1\_23-11** into **Device Management**, **Configuration Intent Types**.

Device Management Configuration	on Intent	Types	÷							+ IMPORT
Intent Type		Version		Status	Description	Role	Category	Device Scope	Last Updated	(i) Intent Type Details
	T		T	-	T	-	•	-	MMM d, yyyy h:mm:ss a	
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 ;	Intent Type hfd-shfd-reflector msros 23-10-1 23-11
port-connector_gsros_23-10-1_23-1	1		1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Nov 26, 2024 4:17:03 pi	Version
icm-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Dec 2, 2024 11:12:32 ar 🕴	1
icm-equipment-port-access-ce			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Dec 2, 2024 1:19:32 pm	Status
port-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Dec 2, 2024 1:51:20 pm 🕴	• Summe ful
system-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Dec 2, 2024 3:52:48 pm	Successfully imported/re-imported the intent type
bfd-bfd-template_gsros_23-10-1_23	-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Dec 3, 2024 11:01:55 ar	Successionly imported the interretype
bfd-sbfd-reflector_msros_23-10-1_2	3		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Dec 3, 2024 11:55:48 ar 🕴	Description
										config reflector Rele Logical Category BFD Device Scape SROS Model Imperted Dec 3, 2024 11:55:43 am Last Updated Dec 3, 2024 11:55:48 am Configuration Form default
4									$\flat \mathrel{\prec} \flat$	
Auto-refresh Last Refree	h: 2024/1	2/3 11:56:15				IC C Page: 1	/1 → →		Count : 8	

2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Equipment-bfd-sbfd-reflector-template**.

	1	Description		Life Cycle		Target Labels		Intent Type	Intent'	(i) Template Details
1	-		Ŧ				T	T		- C impact brand
uipment-card_mda	1	-		released		-		icm-equipment-card_mda	:	∧ General
upment-port-connector		-		released	-	_		port-connector_gsros_23-10	:	
uipment-port-ethernet		-		released	-	_		icm-equipment-port-ethernet	:	Name Equipment-bfd-sbfd-reflector-template
uipment-port-access-ce		-		released		-		icm-equipment-port-access-ce	:	Description
lipment-port-eth-msros		-		released	-	-		port-eth_msros_23-10-1_24-4	:	-
upment-lldp-msros		-		released	-	-		system-IIdp_msros_23-10-1	:	Life Cycle
uipment-bfd-template		-		released		-		bfd-bfd-template_gsros_23-1	:	released
upment-bfd-sbfd-reflector-template		-		released		_		bfd-sbfd-reflector_msros_23	:	Target Labels
										Centry form default Up-to-date Role Logical Category HFD
										Device Scope SROS Model
	4								<b>,</b>	Flexible Yes Created Dec 3, 2024 12:00:36 pm

Create configuration deployments using the above configuration template. The following example uses 7750 SR-14s in MD mode.

Equipment-bfd-sbfd-reflector-	template					×
Reflector	Reflector					
	Description	Admin State		Local State		
	bfd reflector	enable	• 🕞	up	⊑x	
	Discriminator					
	524288					
					CANCEL	UPDATE

Deploy Logical Configuration									×
Select Templates * Select Targets and Edit Selected Template * Assign Identifier for Selected Template *	Select Templates								Count : 1
	Select Targets and	Edit Selected Ten	nplate						
	Select targets. Template	configurations can be red by the selected temp selected for the selected	e edited afte lates are assig template	er targets are selv	ected				VIEW/EDIT TEMPLATE CONFIG
	Reachability	NE Name		NE ID		Management IP		Product	
	• Up	Boston	T	92.168.96.46	T	135.249.153	T	7750 SR	
									Count : 1
	Assign Identifier fo	r Selected Templa	ate						
	Assign unique identifiers	for templates selecte	d above to	identify the corre	espor	iding deploymen	ts. If	f content below is disabled, select targets first to enable t	iem.
	1. Equipment-bfd-sbfd-reflecto Reflector Name* sbfd-reflector-A	r-template :							
									CANCEL DEPLOY

Danlaumant Statu	Configuration Chattan	NE Nama		NEID		Identifier		Templete	Pala	Cabaa		<b>A</b>
Deployment Status	Configuration Status	NE Name	-	NEID	-	laentimer	-	Template	Kole	Category	: :	(i) Deployment Details
Deployed Aligned	Modified	CE West		92 168 99 6		1	1	Equipment-card mda	Physical	Card		NE Name
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1		Equipment-port-conn	Physical	Port	;	Boston
Deployed Aligned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c2		Equipment-port-conn	Physical	Port		NE ID 92.168.96.46
Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c1		Equipment-port-conn	Physical	Port	:	Identifier
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c2		Equipment-port-conn	Physical	Port	:	Beflecter Name
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1/1		Equipment-port-ether	Physical	Port	:	sbfd-reflector-A
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c1/1		Equipment-port-ether	Physical	Port	:	
Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c2/1		Equipment-port-eth	Physical	Port	:	Deployment Status
<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West		92.168.99.6		bfd-template-A		Equipment-bfd-template	Logical	BFD	:	<ul> <li>Deployed Aligned</li> </ul>
Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		sbfd-reflector-A		Equipment-bfd-sbfd-r	Logical	BFD	÷	AUDIT
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		0#0.0.0.0#system		Router-ospf-interface	Logical	Router	:	AUDIT
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		0#system		Router-isis-interface	Logical	Router	:	Last Audit
Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1#1.1.1.1		Router-ospf-area	Logical	Router	:	
<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		toNodeB		Router-Interface-msros	Logical	Router	:	Last Alignment
												Template Name Equipment-bif4-sbif4-reflector-template Created Dec 3, 2024 12:10:24 pm Last Updated Dec 6, 2024 5:30:27 pm Rele Logical Category BED
•										•	>	Configuration Status

Figure 7-15 NE CLI after deployment



END OF STEPS

# 7.6 OSPF/ISIS

#### 7.6.1 To configure OSPF Area on MD NEs with router-ospf-area\_msros\_23-10-1\_ 24-4 intent

router-ospf-area\_msros\_23-10-1\_24-4 intent can be used to create OSPF instance and area, and also configure the same on MD NEs.

1 -

Prerequisites:

**i** Note: The following prerequisites are unique to the example deployment below.

Configure import and export policies:

```
    /configure policy-options policy-statement "export_policy"
    /configure policy-options policy-statement "import policy"
```

Configure BIER template:

```
• /configure router "Base" bier template "BIER_Template_1"
```

2

Import the intent type router-ospf-area\_msros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

Device Management Configuration	n Intent	Types	•							+ IMPORT
Intent Type		Version		Status	Description	Role	Category	Device Scope	Last Updated :	i Intent Type Details
	T		T	-	T	-	-	•	MMM d, yyyy h:mm:ss i	
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 :	Intent Type router-osof-area msros 23-10-1 24-4
oort-connector_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Nov 26, 2024 4:17:03 pi	Version
m-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Dec 2, 2024 11:12:32 ar	1
m-equipment-port-access-ce			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Dec 2, 2024 1:19:32 pm	Status
ort-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Dec 2, 2024 1:51:20 pm	a Council I
stem-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Dec 2, 2024 3:52:48 pm	Successfully imported/re-imported the intent-type
fd-bfd-template_gsros_23-10-1_23-	11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Dec 3, 2024 11:01:55 ar	successionly imported the interrotyp
fd-sbfd-reflector_msros_23-10-1_23			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Dec 3, 2024 11:55:48 ar	Description
outer-ospf-interface_msros_23-10-1			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 1:47:43 pm	Intent-Type to configure router area
outer-isis-interface_msros_23-10-1_			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 3:11:00 pm	Role
outer-ospf-area_msros_23-10-1_24-	4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 5, 2024 12:00:13 pr	Logical
										Router Device Segee SROS Model Imported Dec 5, 2024 12:00:07 pm Last Updated Dec 5, 2024 12:00:13 pm Configuration Form default
-									▶ ∢ →	

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-ospf-area**.

lame	De	escription		Life Cycle		Target Labels		Intent Type	In	tent' :	(i) Template Details
Т			T				T		T		
quipment-card_mda	-			released	•			icm-equipment-card_mda		:	∧ General
uipment-port-connector	-			released	-	-		port-connector_gsros_23-10		1	
uipment-port-ethernet	-			released	•	-		icm-equipment-port-ethernet			Name Router-ospf-area
uipment-port-access-ce	-			released	•	-		icm-equipment-port-access-ce			Description
upment-port-eth-msros	-			released		-		port-eth_msros_23-10-1_24-4		1	-
juipment-Ildp-msros	-			released				system-lldp_msros_23-10-1		1	Life Cycle
uipment-bfd-template	-			released				bfd-bfd-template_gsros_23-1		1	released
uipment-bfd-sbfd-reflector-template	-			released	•			bfd-sbfd-reflector_msros_23		1	Target Labels
uter-ospf-interface	-			released	•			router-ospf-interface_msros		1	
uter-isis-interface	-			released	•	<del></del>		router-isis-interface_msros_2		1	router-ospf-area_msros_23-10-1_24-4
uter-ospf-area	-			released		-		router-ospf-area_msros_23-1		:	Intent Type Version
											Config Form default Config Form State Up-to-date Logical Cottgory Router Device Scepe SROS Model Flashbe Yes
											Created
	4		_							N	Dec 5, 2024 12:28:30 pm
	4										Last Undated
											cast opulated

Create configuration deployments using the above configuration template. The following example uses 7750 SR-14s MD.

Router-ospf-area				×
Area	Area			
BIER Stub	Import Policy +  Import_policy		1	
	Export Policy + export_policy			
	Advertise Router Capability     Database Export Exclude	<ul> <li>Blackhole Aggregate</li> <li>Loopfree Alternate Exclude</li> </ul>		
	IP Profix Mask Advertise			+ 400
	1.1.1/32			1
				CANCEL UPDATE

Router-ospf-area				×
Area BIER Stub	Area			
			Row Count: 1	
	BIER			_
	Template BIER_Template_1	Admin State  Enable	G	
	Stub Default Metric 2	Summaries		
	-			CANCEL UPDATE

Deploy Logical Configuration							×
Select Templates * Select Targets and Edit Selected Template * Assign Identifiar for Salertad Template *	Select Templates						
Joseph receiver to beleased rempired							Count : 1
	Select Targets and Edi	Selected Template					
	Select targets. Template cor	figurations can be edited a	fter targets are selecte	d.			VIEW/EDIT TEMPLATE CONFIG
	Configurations required b	y the selected templates are a	ssigned. View/Edit.				
	Reachability	NE Name	NE ID	Management IP	Product		
	• Up	Boston	92.168.96.46	135.249.153	7750 SR	T	
							Count : 1
	Assign Identifier for So	elected Template					
	Assign unique identifiers for	templates selected above	to identify the corresp	onding deployments.	If content b	elow is disabled, select targets first to enable them.	
	1. Router-ospf-area :						
	OSPF-INSTANCE*		AREA-ID*				
	1		1.1.1.1				
							CANCEL DEPLOY

=	NO <ia network="" ser<="" th=""><th>rvices Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻 🕜</th></ia>	rvices Platform							User: admin 👻 🕜
Devic	e Management Configuration Configuration	Deployments *							+ DEPLOYMENT C-
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	: (i) Deployment Details
	•	•	T	Ť	T	T	-		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service	Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System	NE ID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System	92.168.96.46
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System	ldentifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System	: OSPF-INSTANCE
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP	: 1
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP	AREA-ID 1111
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	bfd-template-A	Equipment-bfd-template	Logical	BFD	1
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	bfd-template-A	Equipment-bfd-template	Logical	BFD	I
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2/1	Equipment-port-eth	Physical	Port	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port	e Deployed Righted
	Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port	AUDIT ALIGN
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	bfd-template-A	Equipment-bfd-template	Logical	BFD	I
/	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1	Router-ospf-area	Logical	Router	: Last Audit
Þ. 4						_		•	Last Aligement Jan 9, 2025 12:06:10 pm by admin Tregelset Name Router-ospf-area Created Jan 9, 2025 12:05:03 pm Last Updated Jan 9, 2025 12:06:10 pm Reie Logical Category router
-	Auto-refresh Last Refresh:	2025/1/9 12:18:36			< Page: 1 /1 >>>			Count	

Figure 7-16 NE CLI after deployment

```
(pr) [/configure router "Base" ospf 1]
A:admin@Boston# info
   area 1.1.1.1 {
        advertise-router-capability true
        blackhole-aggregate true
        export-policy ["export policy"]
        import-policy ["import policy"]
        loopfree-alternate-exclude true
        database-export-exclude true
        stub {
            default-metric 2
            summaries true
        bier {
            admin-state enable
            template "BIER Template 1"
        area-range 1.1.1.1/32 {
```

END OF STEPS

## 7.6.2 To configure OSPF Area on Classic NEs with router-ospf-area\_csros\_23-10-1\_24-4 intent

router-ospf-area\_csros\_23-10-1\_24-4 intent can be used to create and configure OSPF instance and area on classic NEs.

1 \_\_\_\_\_

#### **Prerequisites:**

**i** Note: The following prerequisites are unique to the example deployment below.

Configure BIER template:

• /configure router "Base" bier template "BIER\_Template\_1"

2 -

Import the intent type router-ospf-area\_csros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

■ NO <ia network="" platform<="" services="" th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 🔹 🕐</th></ia>								User: admin 🔹 🕐
Device Management Configuration Configuration Intent Types								+ IMPORT C
Intent Type Version	s	Status	Description	Role	Category	Device Scope	Last Upr 🗄	(i) Intent Type Details
Т	T	-	T	-	-	•	MMM c	
icm-service-customer	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Service	SROS Classic & Model	Jan 3, 2) 🚦	router-ospf-area_csros_23-10-1_24-4
icm-system-ptp	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	PTP	SROS Classic & Model	Jan 6, 2) 🚦	Version
icm-system-security_cpm	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 6, 2) 🚦	1
system-lldp_msros_23-10-1_23-11	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Jan 6, 2) 🚦	Status
security-cpu-protection_gsros_23-10-1_23-11	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 6, 2) 🚦	Successful
bfd-bfd-template_gsros_23-10-1_23-11	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Jan 7, 2i 🚦	Successfully imported/re-imported the intent-type
icm-equipment-card_mda	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Jan 8, 2) 🚦	baccebrany importance important die interne type
port-eth_msros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Jan 8, 2) 🚦	Description
port-connector_gsros_23-10-1_23-11	1 (	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 8, 2) 🚦	Intent-Type to configure ospf-AreaSite for classic SROS
icm-equipment-port-ethernet	2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 8, 2) 🚦	Role
bfd-sbfd-reflector_msros_23-10-1_23-11	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Jan 9, 21 🚦	Logical
router-ospf-area_msros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 9, 21 🚦	Router
router-ospf-interface_msros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 9, 21 🚦	Device Scope
router-interface_msros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 9, 2i 🚦	SROS Classic
icm-router-network-interface	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Interface	SROS Classic & Model	Jan 9, 2i 🚦	Imported
port-eth_csros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Jan 23, 🗌	Jan 25, 2025 5:25:44 pm
router-ospf-area_csros_23-10-1_24-4	1 (	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡 🕴	Jan 23, 2025 5:25:52 pm
								Configuration Form
								default
							$\rightarrow \rightarrow$	
Auto-refresh Last Refresh: 2025/1/23 17:26:05			< < Page	1 /1 > >			Count : 17	

3 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-ospf-area-classic**.

	Network Service	es Platform								User: admin 👻 🧃
evice Management	Configuration Configuration Ten	nplates	•							+ TEMPLATE
Name		Descripti	on	Life Cycle		Target Labels		Intent Type	Intent' :	(i) Template Details
	T		T		*		т	T		
Customer_Template		-		released		-		icm-service-customer	1	∧ General
ystem_PTP_Template		-		released		-		icm-system-ptp	1	
ystem_Security_Cpm	_Template	-		released		-		icm-system-security_cpm	1	Name Router-ospf-area-classic
ldp_md_Template		-		released	*	-		system-lldp_msros_23-10-1	1	Description
ystem_Cpu_Protectio	in_Template	-		released		-		security-cpu-protection_gsros	1	-
quipment-bfd-templa	ite	-		released		-		bfd-bfd-template_gsros_23-1	1	Life Cycle
quipment-card_mda		-		released		-		icm-equipment-card_mda	1	released
quipment-port-eth-n	nsros	-		released		-		port-eth_msros_23-10-1_24-4	1	Target Labels
quipment-port-conn	ector	-		released		-		port-connector_gsros_23-10	:	
quipment-port-ether	net	-		released		-		icm-equipment-port-ethernet	:	router-ospf-area_csros_23-10-1_24-4
quipment-bfd-sbfd-r	eflector-template	-		released		-		bfd-sbfd-reflector_msros_23	:	Intent Type Version
outer-ospf-area		-		released		-		router-ospf-area_msros_23-1	:	1
outer-ospf-interface		-		released	-	-		router-ospf-interface_msros	1	Config Form
outer-interface-msrc	s	-		released	-	-		router-interface_msros_23-10	1	derault
outer-interface-unifi	ed	-		released	-	-		icm-router-network-interface	1	Config Form State
quipment-port-eth-c	sros	-		released	-	-		port-eth_csros_23-10-1_24-4	1	Bala
outer-ospf-area-clas	sic	-		released		-		router-ospf-area_csros_23-10	1	Logical
										Category
										Router
										Device Scope SROS Classic
										Flexible
										Yes
										Created
	Þ	4							• • •	Jan 23, 2025 5:27:14 pm
-										Last Updated

Create configuration deployments using the above configuration template. The following example deploys on 7750 SR-14s classic NE.

SPF Area Site	OSPF Area Site	OSPF Area Site													
	Area Type		BIER Template		BIER Administrative State										
	Backbone	▼ □ <sub>x</sub>	BIER_Template_1	×	Up	▼ □x									
	Loop-free Alternate Exclude		Blackhole Range		Enable Advertise Router Capability										
	Database Export Exclude														
	Area Range					+ ADD									
	Key ID Link St	ate DB Type	Network	Prefix Length	Effect										
			No data	to display											
			IK K Page: 0	/0 > >		Total: 0									

Deploy Logical Configuration		×
Select Templates *	Select Templates	
Select largets and bot Selected lemplate		
Assign Identifier for Selected Template *		Count : 1
	Select Targets and Edit Selected Template	
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TEMPLATE CONFIG
	Configurations required by the selected templates are assigned. View/Edit	
	Reachability NE Name NE ID Manag	ament IP Product
	Τ Τ Τ	ТТТ
	• Up Toronto 92.168.96.215 135.24	9.150.4 7750 SR
		Count : 1
	Assign Identifier for Selected Template	
	Assign unique identifiers for templates selected above to identify the corresponding d	eployments. If content below is disabled, select targets first to enable them.
	1. Router-ospf-area-classic :	
	Instance ID* Area ID*	
	0 0.0.0.0	
		CANCEL DEPLOY

=	NOKIA	Network Serv	vices Platform										User: admin 👻 🕜	
Devic	e Management	Configuration Configuration	Deployments *										+ DEPLOYMENT 📿 🖀	ì
	Deployment Sta	tus	Configuration Status	NE Name		NE ID		Identifier	Template	Role	Category	:	i Deployment Details	
		•	-		T		T	T	T	-				
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	NSP		0.0.0.0		TransCanadian Railway	Customer_Template	Logical	Service	-	NE Name Toronto	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		cpm	System_Security_Cpm	Logical	System	:	NEID	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		cpm	System_Security_Cpm	Logical	System		92.168.96.215	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		lldp	Lldp_md_Template	Logical	System	:	Identifier	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		23	System_Cpu_Protectio	Logical	System		Instance ID	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		ptp	System_PTP_Template	Logical	PTP	-	0	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		ptp	System_PTP_Template	Logical	PTP	-	Area ID 0 0 0 0	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	CE_West		92.168.99.6		bfd-template-A	Equipment-bfd-template	Logical	BFD			
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		bfd-template-A	Equipment-bfd-template	Logical	BFD	-		
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c2/1	Equipment-port-eth	Physical	Port		Deployment Status	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		Port 1/1/c1/1	Equipment-port-ether	Physical	Port	-		
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1/1/c1/1	Equipment-port-ether	Physical	Port	:	AUDIT ALIGN	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		bfd-template-A	Equipment-bfd-template	Logical	BFD	:		
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1#1.1.1.1	Router-ospf-area	Logical	Router	:	Last Audit	
	<ul> <li>Deployed Aligned</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		1#1.1.1.1#test4	Router-ospf-interface	Logical	Router	:		
	Deployment F	ailed	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		toCore_2	Router-interface-msros	Logical	Router		Jan 23, 2025 5:47:05 pm by admin	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		test7	Router-interface-unified	Logical	Interface	:	Template Name	
	Deployment F	ailed	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		test7	Router-interface-unified	Logical	Interface	:	Router-ospf-area-classic	
	Deployed Aligned	ned	<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		0#0.0.0.0	Router-ospf-area-classic	Logical	Router	- :	Created Jan 23, 2025 5:38:54 pm	
													Last Updated Jan 23, 2025 5:47:05 pm Rele Logical	
	(										•	<	Category router	
	Auto-refresh	Last Refresh: 2	2025/1/23 17:47:15					Page: 1 / 1 > 2			Count	: 19	Configuration Status	-





END OF STEPS

- 7.6.3 To configure OSPF Interface on MD NEs using router-ospf-interfacemsros intent
  - 1 -

#### Prerequisites:

**i** Note: The following prerequisites are unique to the example deployment below.

- OSPF area should be created (see 7.6.2 "To configure OSPF Area on Classic NEs with router-ospf-area\_csros\_23-10-1\_24-4 intent" (p. 298) for details)
- · Authentication keychain should be configured:

/configure system security keychains keychain "keychain-1"

NSP

2 -

Import the intent type router-ospf-interface\_msros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

Device Management Configuration Configuration Intent Types	•										+ IMPORT C
Intent Type		Version		Status	Description		Role	Category	Device Scope	La 🗄	i Intent Type Details
	T		T	•		T	•	•	•		
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Physical	Card	SROS Classic & Model	N: E	Intent Type router-ospf-interface msros 23-10-1 24-4
port-connector_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-type to configu	r	Physical	Port	SROS Classic & Model	N- I	Version
icm-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configu	r	Physical	Port	SROS Classic & Model	DI	1
icm-equipment-port-access-ce			2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Physical	Port	SROS Classic	DI	Status
port-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Physical	Port	SROS Model	DI	• Sussansful
system-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Logical	System	SROS Model	DI	Successfully imported/re-imported the intent-type
bfd-bfd-template_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Logical	BFD	SROS Classic & Model	Di	
bfd-sbfd-reflector_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ir	Logical	BFD	SROS Model	DI	Description
router-ospf-interface_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	ır	Logical	Router	SROS Model	DE	Intent-Type to configure category router and device-
											Celegory Router Davies Scope SROS Model Imperts 2024 1:47:35 pm Last Updated Dec 3, 2024 1:47:43 pm Configuration Form default
										• • •	
Auto-refresh Last Refresh: 2024/12/3 13:48:07					IC C Pas	e: 1	1 /1 5 51			Count : 9	

3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-ospf-interface**.

Device Management Configuration Configuration Te	mpl	ates 👻										+ TEMPLATE C
Name		Description		Life Cycle		Target Labels	1	Intent Type	Int	tent '	:	(i) Template Details
	r		T		•	Т	·	T				
Equipment-card_mda		-		released	-	-		icm-equipment-card_mda			:	^ General
Equipment-port-connector		-		released	-	-		port-connector_gsros_23-10			:	
Equipment-port-ethernet		-		released	-	-		icm-equipment-port-ethernet			:	Name Router-ospf-interface
Equipment-port-access-ce		-		released	-	-		icm-equipment-port-access-ce			:	Description
Equipment-port-eth-msros		-		released	-	-		port-eth_msros_23-10-1_24-4			:	-
Equipment-Ildp-msros		_		released	-	-		system-lldp_msros_23-10-1			:	Life Cycle
Equipment-bfd-template		-		released	-	-		bfd-bfd-template_gsros_23-1			:	released
Equipment-bfd-sbfd-reflector-template		_		released	-	-		bfd-sbfd-reflector_msros_23			:	Target Labels
Router-ospf-interface		-		released	-	-		router-ospf-interface_msros			- 1	-
												Intert Type Version 1 Config Form default Config Form State Up-to-date Role Logical Category Router Device Scope SKOS Model Flexible Yes Created
	4	_		_							4.1	Dec 3, 2024 1:52:02 pm
,												to state date d

Create configuration deployments using the above configuration template.

Example deployment 1: On 7750 SR-14s MD - Router Base OSPF instance 0 area 0.0.0.0

Router-ospf-interface								×
Interface	Interface							*
BFD Liveness Loopfree Alternate Policy Map Node SID	Admin State enable ~ Interface Type	⊑x	Advertise Router Capability			Advertise Subnet		
Adjacency SID	broadcast т	⊑x	none	• (	Ξ <del>x</del>	Poll Interval(seconds) 30		
	Priority 2		RIB Priority high	• (	□x	Load Balancing Weight 22		
	Hello Interval(seconds)		Dead Interval(seconds)			Retransmit Interval(seconds)		
	Transit Delay(seconds)		Authentication Keychain		~	Authentication Key	0	
	Authentication Type password	C,	SID Protection		~			
	BFD Liveness		☐ Strict			Strict Mode Holddown(seconds)		
							CANCEL	UPDATE

Deploy Logical Configuration													~
Select Templates * Select Targets and Edit Selected Template *	Select Templates										CLEAR ALL	+ TEMP	LATE
Assign Identifier for Selected Template *	Select Targets ar	d Edit Selected Templ	ate								CLEAR ALL	- + TAF	RGET
	Select targets. Templ	ate configurations can be ed quired by the selected templates	ited afte s are assi	er targets are se gned. View	electe	d.				I	VIEW/EDIT T	EMPLATE CO	NFIG
	Only 1 target can     Reachability	be selected for the selected terr NE Name	nplate	NE ID		Management	IP	Product					
	• Up	Boston	T	92.168.96.46	T	135.249.153.	<b>T</b>	7750 SR	T				
												Count	::1
	Assign Identifier	for Selected Template											
	Assign unique identif	ers for templates selected a	bove to	identify the cor	respo	nding deployn	nents. If	f content	t below is disabled, select targets first to enable ther	n.			
	OSPF-INSTANCE*		AR	REA-ID*					INTERFACE-NAME*				
	0	:	×	0.0.0.0				×	system	×			
										CA	NCEL :	SAVE	DEPLOY

		NE Name	NEID	Identifier	lemplate	Role	Category :	(i) Deployment Details
•	•		T	T	Ť	•		NEName
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	1	Equipment-card_mda	Physical	Card :	Boston
Deployed Aligned	Modified	Toronto	92.168.96.215	Port 1/1/c1	Equipment-port-conn	Physical	Port i	NE ID
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c2	Equipment-port-conn	Physical	Port i	92.168.96.46
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1	Equipment-port-conn	Physical	Port i	Identifier
Deployed Aligned	Modified	Boston	92.168.96.46	1/1/c2	Equipment-port-conn	Physical	Port :	OSPF-INSTANCE
Deployed Aligned	Modified	Ioronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port :	AREA-ID
Deployed Aligned	Modified	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port :	0.0.0
Deployed Aligned	• Modified	Boston	92.168.96.46	1/1/02/1	Equipment-port-etn	Physical	Port :	INTERFACE-NAME
Deployment Failed	Modified	Cc_west	92.168.99.6	ord-template-A	Equipment-ord-template	Logical	BED :	system
Deployment railed	• Modified	Boston	92.168.96.46	sord-reflector-A	Equipment-ord-sord-r	Logical	BrD :	
								AUDIT ALIGN Last Audit Last Audit Dec 3, 2024 2:08:40 pm by admin Template Name Router-ospf-Interface Created Dec 3, 2024 2:08:38 pm Last Audit

Figure 7-18 NE CLI after deployment



Example deployment 2: On 7750 SR-14s MD - Router Base OSPF instance 1 area 1.1.1.1 with a different set of attributes

Interface	Interface					
BFD Liveness						
Loopfree Alternate	Admin State enable	• Cx	Advertise Router Capability		Advertise Subnet	
Node SID	Interface Type		LSA Filter Out		Metric	
Adjacency SID	non-broadcast	▼ □x	none	• 🗔	65535	
	MTU				Poll Interval(seconds)	
	9182		Passive		30	
	Priority		RIB Priority		Load Balancing Weight	
	254		high	• 🗔		
	Hello Interval(seconds)		Dead Interval(seconds)		Retransmit Interval(seconds)	
	30		60		10	
	Transit Delay(seconds)		Authentication Keychain		Authentication Key	
	2		keychain-1	3	× •••••	0
	Authentication Type					
	message-digest	• 🖓				
	BFD Liveness					
					Strict Mode Holddown(seconds)	

Router-ospf-interface			×
Interface	Interface		*
ero Liveness Loopfree Alternate Policy Map Node SID Adjacency SID	Message Digest Key	+ ADD :	
	< < Page: 1 /1 > >	Total: 1	
	Neighbor	+ ADD	
	Address 192.168.96.139	I	
		c	ANCEL UPDATE

May 2025 Issue 4

Deploy Logical Configuration								×
Select Templates *	Select Templates							
Assign Identifier for Selected Template *								Count : 1
	Select Targets and Edi	t Selected Template						
	Select targets. Template cor	figurations can be edited	after targets are se	lected	J.			VIEW/EDIT TEMPLATE CONFIG
	Configurations required b	by the selected templates are	assigned. View,	/Edit				
	Only 1 target can be select	cted for the selected template	:					
	Reachability	NE Name	NE ID		Management IP	Produ	ıct	
	T		T	T	1		т	
	• Up	Boston	92.168.96.46		135.249.153	7750	SR	
								Count : 1
	Assign Identifier for So	elected Template						
	Assign unique identifiers for	templates selected above	to identify the con	respor	nding deployment	s. If conte	ent below is disabled, select targets first to enable ther	n.
	1. Router-ospf-interface :							
	OSPF-INSTANCE*		AREA-ID*				INTERFACE-NAME*	
	1		1.1.1.1				test4	
								CANCEL DEPLO

=	Notion Network Ser	vices Platform								User: admin	•	?
Devic	e Management Configuration Configuration	Deployments •								+ DEPLOYMENT	G	
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	:	Deployment Details		
	•	-	T	T	T	T	-					
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service	:	NE Name Boston		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System	:	NEID		
	Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System	:	92.168.96.46		
	Deployed Aligned	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System	:	Identifier		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System	:	OSPF-INSTANCE		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP	:	1		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP	:	AREA-ID 1 1 1 1		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	INTERFACE-NAME		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	test4		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2/1	Equipment-port-eth	Physical	Port	:			
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port	:	Deployment Status		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port	-	<ul> <li>Deployed Aligned</li> </ul>		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	411017		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1	Router-ospf-area	Logical	Router	:	AUDIT ALIGN		
$\checkmark$	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1#test4	Router-ospf-interface	Logical	Router	- 1			
										Last Audit		
										Last Alignment Jan 9, 2025 3:47:23 pm by admin		
										Template Name Router-ospf-Interface		
										Created		
										Jan 9, 2025 1:39:11 pm		
										Last Updated Jan 9, 2025 3:47:23 pm		
								×	< →	Role		
-	Auto-refresh Last Defeetby	2025/1/9 15:47:55			( Page: 1 /1 )				. 16	Logica		

Figure 7-19 NE CLI after deployment

```
(pr) [/configure router "Base" ospf 1 area 1.1.1.1 interface "test4"]
A:admin@Boston# info
   admin-state enable
   advertise-router-capability false
   advertise-subnet false
   interface-type non-broadcast
   lsa-filter-out none
   metric 65535
   poll-interval 30
   priority 254
   rib-priority high
   hello-interval 30
   dead-interval 60
   retransmit-interval 10
   transit-delay 2
   authentication-keychain "keychain-1"
   authentication-key "fDawqd7d4RnHUWWVfGycGAJSzOGT hash2"
   authentication-type message-digest
   bfd-liveness {
       remain-down-on-failure false
   message-digest-key 2 {
       md5 "ydwfsMCJlzNo0b/NVEI5yFSscWo= hash2"
   neighbor 192.168.96.139 { }
```

END OF STEPS

## 7.6.4 To configure OSPF Interface on MD NEs using router-ospf-interfacemsros intent

router-ospf-interface\_csros\_23-10-1\_24-4 intent can be used to configure OSPF interface on classic SR NEs.

1

#### **Prerequisites:**

**i** Note: The following prerequisites are unique to the example deployment below.

- OSPF area should be created (see 7.6.2 "To configure OSPF Area on Classic NEs with router-ospf-area\_csros\_23-10-1\_24-4 intent" (p. 298) for details)
- · Authentication keychain should be configured:

```
/configure system security keychain "keychain-1"
```

2 -

Import the intent type router-ospf-interface\_csros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

NO <ia network="" platform<="" services="" th=""><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻 🕜</th></ia>								User: admin 👻 🕜
Device Management Configuration Configuration Intent Types								+ IMPORT C
Intent Type Version		Status	Description	Role	Category	Device Scope	Last Upr 🗄	(i) Intent Type Details
Т	T	-	T	-	-	•	MMM c	
icm-service-customer	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Service	SROS Classic & Model	Jan 23, 🔡	Intent Type router-osof-interface csros 23-10-1 24-4
icm-system-ptp	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	PTP	SROS Classic & Model	Jan 23, 🔡	Version
icm-system-security_cpm	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🔡	1
system-lldp_msros_23-10-1_23-11	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Jan 23, 🔡	Status
security-cpu-protection_gsros_23-10-1_23-11	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🔡	• Susseenful
bfd-bfd-template_gsros_23-10-1_23-11	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Jan 23, 🔡	Successfully imported/re-imported the intent-type
icm-equipment-card_mda	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Jan 23, 🔡	Successionly imported the intent-type
port-eth_msros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Jan 23, 🔡	Description
port-connector_gsros_23-10-1_23-11	1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🔡	Intent-Type to configure ospf-Interface for classic SROS
icm-equipment-port-ethernet	2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🔡	Role
bfd-sbfd-reflector_msros_23-10-1_23-11	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Jan 23, 🔡	Logical
router-ospf-area_msros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	Router
router-ospf-interface_msros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	Device Scope
router-interface_msros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	SROS Classic
icm-router-network-interface	2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Interface	SROS Classic & Model	Jan 23, 🔡	Imported
port-eth_csros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Jan 23, 🔡	Jan 25, 2025 5:55:26 pm
router-ospf-area_csros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡	Jan 23, 2025 5:54:53 pm
router-ospf-interface_csros_23-10-1_24-4	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡 🚦	Configuration Form
								default
•							$\rightarrow \leftrightarrow$	
Auto-refresh Last Refresh: 2025/1/23 17:58:22			I< < Page	E 1 /1 → →			Count : 18	

3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-ospf-interface**classic.

NOCIA Network Servi	ces Pla	tform								User: admin 🗸
evice Management Configuration Configuration Te	emplate	s *								+ TEMPLATE
lame	D	escription		Life Cycle		Target Labels		Intent Type	Intent :	(i) Template Details
1	r		٣		*		T	T		
istomer_Template	-			released				icm-service-customer	:	∧ General
stem_PTP_Template	-			released	-	<u> </u>		icm-system-ptp	:	
stem_Security_Cpm_Template	-			released	-			icm-system-security_cpm	1	Name Router-ospf-interface-classic
dp_md_Template	-			released	-			system-Ildp_msros_23-10-1	:	Description
stem_Cpu_Protection_Template	-			released				security-cpu-protection_gsros	:	-
uipment-bfd-template	-			released	•			bfd-bfd-template_gsros_23-1	:	Life Cycle
uipment-card_mda	-			released	-			icm-equipment-card_mda	1	released
quipment-port-eth-msros	-			released	-			port-eth_msros_23-10-1_24-4	1	Target Labels
uipment-port-connector	-			released	-			port-connector_gsros_23-10	:	
quipment-port-ethernet	-			released	-			icm-equipment-port-ethernet	:	Intent Type router-ospf-interface csros 23-10-1 24-4
quipment-bfd-sbfd-reflector-template	-			released	-			bfd-sbfd-reflector_msros_23	:	Intent Type Version
outer-ospf-area	-			released	-			router-ospf-area_msros_23-1	:	1
outer-ospf-interface	-			released	-			router-ospf-interface_msros	1	Config Form
outer-Interface-msros	-			released	-			router-Interface_msros_23-10	:	default
outer-Interface-unified	-			released	-			icm-router-network-interface	:	Config Form State
ulpment-port-eth-csros	-			released	-			port-eth_csros_23-10-1_24-4	:	
uter-ospf-area-classic	-			released	-			router-ospf-area_csros_23-10	:	Logical
uter-ospf-Interface-classic	-			released	-	-		router-ospf-Interface_csros_2	:	Category
										Router
										Device Scope
										H-141-
										Yes
										Created
	4								• • •	Jan 23, 2025 5:55:46 pm
										Last Updated

Create configuration deployments using the above configuration template.

Router-ospf-interface-classic				×
OSPF Interface	OSPF Interface			*
	Description	Administrative State		
	Towards Core	Up		
	Configured MTU (bytes)			
	0			
	Interface Type			
	Broadcast 👻 🗔			
	Priority			
	1	Advertise Subnet		
	Passive			
	BFD Enabled			
	Metric			
	0			
	Loop-free Alternate Exclude	LSA Filter Out		
		None		
	Enable Advertise Router Capability			
	RIB Priority			
	None 👻 🕞			
	Load Balancing Weight			-
			CANC	CEL UPDATE

ploy Logical Configuration											
lect Templates *	Select Template	es								CLEAR ALL	+ TEMPLATE
sign identifier for Selected Template *											Count : 1
	Select Targets a	and Edit Selected	Template							CLEAR ALL	+ TARGET
	Select targets. Tem	plate configurations ca	in be edited aft	er targets are se	electe	d.				VIEW/EDIT TEM	4PLATE CONFIG
	Oconfigurations	required by the selected t	emplates are ass	igned. View	/Edit.						
	Only 1 target ca	an be selected for the sele	cted template								
	Reachability	NE Name		NE ID		Management IP	Pro	oduct			
		T	Ŧ		T	1		T			
	• Up	Toronto		92.168.96.215		135.249.150.4	77	50 SR			I.
											Count : 1
	Assign Identifie	er for Selected Ten	nplate								
	Assign unique ident	ifiers for templates se	lected above to	identify the cor	respo	onding deployment	s. If co	ntent below is disabled, select	targets first to enable them.		
	1. Router-ospf-interface-	classic :									
	Instance ID*		A	rea ID*				Interface Name*			
	0		×	0.0.0.0				× test1	×		
											7

=	NOCIA Network Ser	vices Platform								User: admin 👻 🕜
Devi	ce Management Configuration Configuration	Deployments *								+ DEPLOYMENT
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	:	i Deployment Details Refresh
	•	-	T	T	T	T	-			
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service	:	NE Name Toronto
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System		NEID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System		92.168.96.215
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System		Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System		Instance ID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP	-	0
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP	:	Area ID 0 0 0 0
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	Interface Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	test7
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2/1	Equipment-port-eth	Physical	Port	:	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port	:	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port	:	Deployed Aligned
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	bfd-template-A	Equipment-bfd-template	Logical	BFD	:	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1	Router-ospf-area	Logical	Router	:	AUDIT
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1#test4	Router-ospf-interface	Logical	Router	:	
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	toCore_2	Router-interface-msros	Logical	Router	:	Last Audit
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	test7	Router-interface-unified	Logical	Interface	:	Last Alignment
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	test7	Router-Interface-unified	Logical	Interface	:	Jan 23, 2025 6:15:20 pm by admin
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	0#0.0.0.0	Router-ospf-area-classic	Logical	Router	:	Template Name Router-osof-interface-classic
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	0#0.0.0.0#test7	Router-ospf-Interface	Logical	Router	1	Created
										Jan 23, 2025 6:11:59 pm
										Last Updated Jan 23, 2025 6:15:20 pm
4 1	4							۱.	4 1	Role
-	Auto-refersh Last Prévale	2025/1/22 19:15:40			/ Dage: 1 /1			Court	20	Logical
-	Auto-rerresh Last Refresh: .	2020/1/20 10:15:49		15	( Page: 71 > >			Count :	20	Category

Figure 7-20 NE CLI after deployment

```
A:Toronto>config>router>ospf# info
            traffic-engineering
            advertise-router-capability area
            segment-routing
                prefix-sid-range global
                no shutdown
            exit
            area 0.0.0.0
                no advertise-router-capability
                no blackhole-aggregate
                bier
                    template "BIER Template 1"
                    no shutdown
                exit
                interface "system"
                    node-sid label 20000
                    no shutdown
                exit
                interface "test7"
                    no shutdown
                exit
                interface "test1"
                    interface-type broadcast
                    no shutdown
                exit
            exit
            no shutdown
```

END OF STEPS

1

7.6.5 To configure ISIS Interface on MD NEs using router-isis-interfacemsros intent

Prerequisites:

**i** Note: The following prerequisites are unique to the example deployment below.

• ISIS instance and area should be created. This has to be done via NE CLI as there is no intent for this:

```
/edit-config private
/configure router isis 0 admin-state enable
/configure router isis 0 area-address 49.0001
/configure router isis 0 level-capability 2
/configure router isis 0 advertise-router-capability as
/commit
/quit-config
```

2

Import the intent type router-isis-interface\_msros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

Device Management Configuration Configuration	n Intent Types	•							+ IMPORT C
Intent Type	Version		Status	Description	Role	Category	Device Scope	Last Updated :	(i) Intent Type Details
	T	T	-	T	-	-	-	MMM d, yyyy h:mm:ss i	
icm-equipment-card_mda		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 ;	Intent Type router-isis-interface msros 23-10-1 24-4
port-connector_gsros_23-10-1_23-1	1	1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Nov 26, 2024 4:17:03 pi	Version
icm-equipment-port-ethernet		2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Dec 2, 2024 11:12:32 ar	1
icm-equipment-port-access-ce		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Dec 2, 2024 1:19:32 pm	Status
port-eth_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Dec 2, 2024 1:51:20 pm	• Summed
system-lldp_msros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Dec 2, 2024 3:52:48 pm	Successfully imported/re-imported the intent-type
bfd-bfd-template_gsros_23-10-1_23-	-11	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Dec 3, 2024 11:01:55 ar	baccobiany important to important the interior ope
bfd-sbfd-reflector_msros_23-10-1_2	3	1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Dec 3, 2024 11:55:48 ar	Description
router-ospf-interface_msros_23-10-1		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 1:47:43 pm	Intent-Type to configure category router and device-
router-isis-interface_msros_23-10-1_		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 3:11:00 pm	and a set
									Category Router Bovice Scope SKOS Model Imported Dec 3, 2024 3:10:53 pm Last Updated Dec 3, 2024 3:11:00 pm Cenfiguration Ferm default
4								$\rightarrow$	
Auto-refresh Last Refresh	1: 2024/12/3 15:12:28			K	< Page: 1 /	more > >		Count: 10	

3

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as Router-isis-interface.

		Description		Life Cycle		Target Labels		Intent Type	Intent '	1	(i) Template Details
	Ŧ		Ŧ		-		T	T			• • • • • • • • • • • • • • • • • • • •
ipment-card_mda		_		released		_		icm-equipment-card_mda		:	∧ General
ipment-port-connector		-		released	•	-		port-connector_gsros_23-10		:	
ipment-port-ethernet		-		released	•	-		icm-equipment-port-ethernet		:	Name Router-Isis-Interface
ipment-port-access-ce		-		released	•	-		icm-equipment-port-access-ce		:	Description
pment-port-eth-msros		-		released	•	-		port-eth_msros_23-10-1_24-4		:	_
pment-lldp-msros		_		released	•	-		system-lldp_msros_23-10-1		:	Life Cycle
pment-bfd-template		-		released	•	-		bfd-bfd-template_gsros_23-1		:	released
ipment-bfd-sbfd-reflector-template		-		released	•	-		bfd-sbfd-reflector_msros_23		:	Target Labels
ter-ospf-interface		-		released	•	-		router-ospf-interface_msros		:	Intent Type
er-IsIs-Interface		-		released	•	_		router-isis-interface_msros_2		1	router-isis-interface_msros_23-10-1_24-4
											Config Form default Up-to-date Rele Logical Category Router Device Scope SROS Model
											Ver

Create configuration deployments using the above configuration template. The following example uses 7750 SR-14s MD.

Router-isis-interface						×
Interface	Interface					*
IPv4 Adjacency SID	Admin State		Hello Authentication Key		Hello Authentication Keychain	_
Loonfree Alternate	enable 🗸	C,x		0	×	
Policy Map	Hello Authentication Type		Hello Padding			
Mesh Group	password 🗸	□,x	adaptive 👻	Cx.	Passive	
BFD Liveness	CSNP Interval (seconds)					
IPv4	2		Default Instance		Hello Authentication	
IPv6	Interface Type					
IPv4 Node SID	broadcast 👻	C,x	IPv4 Multicast		IPv6 Multicast	
IPv6 Node SID			Level Capability		Load Balancing Weight	
	IPv6 Unicast		2	Cx.		
	LSP Pacing Interval (milliseconds)		Retransmit Interval (seconds)			
	200		3		SID Protection	
	Tag					
	IPv4 Adjacency SID					
	iype					-
					C/	ANCEL UPDATE

Deploy Logical Configuration					×
Select Templates * Select Targets and Edit Selected Template *	Select Templates			CLEAR ALL	+ TEMPLATE
Assign identiner for Selected template	Select Targets and Edit Selected Template			CLEAR ALL	+ TARGET
	Select targets. Template configurations can be edited at Configurations required by the selected templates are as O Only 1 target can be selected for the selected template	fter targets are selected. signed. View/Edit		VIEW/EDIT TEM	IPLATE CONFIG
	Reachability NE Name	NE ID Management IP Produ	ict T		
	• Up Boston	92.168.96.46 135.249.153 7750	SR		ii.
					Count : 1
	Assign Identifier for Selected Template				
	Assign unique identifiers for templates selected above t	to identify the corresponding deployments. If conte	ent below is disabled, select targets first to enable them.		
	1. Router-isis-interface : ISIS-INSTANCE* 0 ×	INTERFACE-NAME* system X			
				CANCEL SA	VE DEPLOY

Devi	ce Management Configuration Configuration	Deployments •										+ DEPLOYMENT 🕞 🚆
	Deployment Status	Configuration Status	NE Name	NE ID		Identifier		Template	Role	Category	/ :	(i) Deployment Details
	-	•		T	T		T	T	•			
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		1		Equipment-card_mda	Physical	Card	:	NE Name Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1		Equipment-port-conn	Physical	Port	:	NE ID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c2		Equipment-port-conn	Physical	Port	:	92.168.96.46
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1		Equipment-port-conn	Physical	Port	:	Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c2		Equipment-port-conn	Physical	Port	:	ISIS-INSTANCE
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215		Port 1/1/c1/1		Equipment-port-ether	Physical	Port	:	0
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c1/1		Equipment-port-ether	Physical	Port	:	INTERFACE-NAME
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		1/1/c2/1		Equipment-port-eth	Physical	Port	:	system
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6		bfd-template-A		Equipment-bfd-template	Logical	BFD	:	
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		sbfd-reflector-A		Equipment-bfd-sbfd-r	Logical	BFD	:	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		0#0.0.0.0#system		Router-ospf-interface	Logical	Router	:	<ul> <li>Deployed Aligned</li> </ul>
~	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46		0#system		Router-isis-interface	Logical	Router	1	AUDIT ALIGN
												Last Audit Last Audit Lest Alignment Dec 3, 2024 3:24:53 pm by admin Template Name Router-sise-interface Created Dec 3, 2024 3:23:35 pm Last Updated Dec 3, 2024 3:24:53 pm Role
+	•				-					Þ		Category router
	Auto-refresh Last Refresh:	2024/12/3 15:24:55				< Page: 1 / 1 >				Coun	t:12	Configuration Status

Figure 7-21 NE CLI after deloyment



END OF STEPS

#### 7.6.6 To configure ISIS Interface on classic NEs using router-isis-interfacecsros intent

1

Import the intent type router-isis-interface\_csros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

Nersting       Version       Status       Description       Role       Category       Device Scope       Last Up:       East Up:       Control (MMMC)         Icm-service-customer       2       Successful       Intent-Type to configur       Logical       Service       SROS Classic & Model       Jan 23.       E         Icm-service-customer       2       Successful       Intent-Type to configur       Logical       System       SROS Classic & Model       Jan 23.       E         icm-system-security-cpm       2       Successful       Intent-Type to configur       Logical       System       SROS Classic & Model       Jan 23.       E         system-lidp_msros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       System       SROS Classic & Model       Jan 23.       E         bfd-bfd-template geros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       System       SROS Classic & Model       Jan 23.       E         opt-cetty_msros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       BPD       SROS Classic & Model       Jan 23.       E         opt-cetty_msros_23-10-1_24-4       1       Successful       Intent-Type to configur       Physical	Trose Version Status Description Role Category Device Scope Last Upr 🗄 🔿 Industry Type Device	
T       T	U interit type Details	
cm-service-customer       2       Successful       Intent-Type to configur       Logical       Service       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       PTP       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       PTP       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model       Jan 2, 1       Intent-Type to configur       Logical       SROS Classic & Model	T T T T MMM C	
con-system-sptp       2       Successful       Intent-Type to configur       Logical       PTP       SROS Classic & Model       Jan 23. cl       Maintent Configur       Variant         jum-system-security_cpm       2       Successful       Intent-Type to configur       Logical       System       SROS Classic & Model       Jan 23. cl       Image: State Sta	nvice-customer 2 • Successful Intent-Type to configur Logical Service SROS Classic & Model Jan 23, it Intent-Type to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 23, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Service SROS Classic & Model Jan 24, it Intent-Stype to configur Logical Servic	4.4
cm-system-security_cpm         2         Successful         Intent-Type to configur         Logical         System         SROS Classic & Model         Jan 23. it         Image: State	stem-ptp 2 • Successful Intent-Type to configur Logical PTP SROS Classic & Model Jan 23.: i Version	
yystem-lidp_maros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       System       SR0S Model       Jan 23.       Istain         uecurity-cpu-protection_gros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       B7D       SR0S Classic & Model       Jan 23.       Istain         ofd-bif-translate_gros_23-10-1_23-11       1       Successful       Intent-Type to configur       Logical       B7D       SR0S Classic & Model       Jan 23.       Istain         orn-equipment-card_mda       2       Successful       Intent-Type to configur       Physical       Card       SR0S Classic & Model       Jan 23.       Istain         orn-equipment-card_mda       1       Successful       Intent-Type to configur       Physical       Port       SR0S Classic & Model       Jan 23.       Istain         orn-equipment-card_mda       1       Successful       Intent-Type to configur       Physical       Port       SR0S Classic & Model       Jan 23.       Istain         orn-equipment-card_mda       1       Successful       Intent-Type to configur       Physical       Port       SR0S Classic & Model       Jan 23.       Istain       Intent-Type to configur       SR0S       SR0S Model       Jan 23.       Istain       So	stem-security_cpm 2 • Successful Intent-Type to configur Logical System SROS Classic & Model Jan 23,: 1	
security-cpu-protection_gsros_23-10-1_23-11 1 Successful Intent-Type to configur Logical BrD SROS Classic & Model Jan 23, 1 profe-bfd-bfd-template_gsros_23-10-1_23-11 1 Successful Intent-Type to configur Physical Card SROS Classic & Model Jan 23, 1 profe-bfd-bfd-template_gsros_23-10-1_23-11 1 Successful Intent-Type to configur Physical Physical Port SROS Model Jan 23, 1 Sort-eth_marso_23-10-1_23-11 1 Successful Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Classic & Model Jan 23, 1 Intent-Type to configur Physical Physical Physical Port SROS Classic & Model Jan 23, 1 Successful Intent-Type to configur Physical Physical Port SROS Model Jan 23, 1 Successful Intent-Type to configur Clgical Router SROS Model Jan 23, 1 SROS Model Jan 23, 1 Logical Physical Physica Physical Ph	-s-lldp_msros_23-10-1_23-11 1 © Successful Intent-Type to configur Logical System SROS Model Jan 23.: : Status	
pickbfd-template_gsros_23-10-1_23-11       1       • Successful       intent-Type to configur       Logical       BFD       SROS Classic & Model       Jan 23. []       • Successful         cm-equipment-card_mda       2       • Successful       Intent-Type to configur       Physical       Card       SROS Classic & Model       Jan 23. []       • Successful       Successful       Successful       Jan 23. []       • Successful       Successful       Jan 23. []       • Successful<	y-cpu-protection_geros_23-10-1_23-11 1   Successful Intent-Type to configur Logical System SROS Classic & Model Jan 23, : :	
m-equipment-card_mda       2       9 Successful       Intent.Type to configur       Physical       Cad       SROS Classic & Model       Jan 23, 1       1       Successful       Intent.Type to configur       Physical       Port       SROS Classic & Model       Jan 23, 1       1       Successful       Intent.Type to configur       Physical       Port       SROS Classic & Model       Jan 23, 1       1       Successful       Intent.Type to configur       Physical       Port       SROS Classic & Model       Jan 23, 1       Intent.Type to configur       Physical       Port       SROS Classic & Model       Jan 23, 1       Intent.Type to configur       Port       SROS Classic & Model       Jan 23, 1       Intent.Type to configur       Port       SROS Classic & Model       Jan 23, 1       Intent.Type to configur       Port       SROS Classic & Model       Jan 23, 1       Intent.Type to configur       Intent.Type to configur       Logical       Port       SROS Model       Jan 23, 1       Intent.Type to configur       Logical       Router       SROS Model       Jan 23, 1       Intent.Type to configur       Logical       Router       SROS Model       Jan 23, 1       Intent.Type to configur       Logical       Router       SROS Model       Jan 23, 1       Intent.Type to configur       Logical       Router       SROS Model       <	d-template_garos_23-10-1_23-11 1 © Successful Intent-Type to configur Logical BFD SROS Classic & Model Jan 23, : :	ha intent to
sourcessful       intent-Type to configur       Physical       Port       SROS Model       Jan 23, if       Intent-Type to configur       Physical       Port       SROS Model       Jan 23, if       Intent-Type to configur       Physical       Port       SROS Classic & Model       Jan 23, if       Intent-Type to configur       Physical       Port       SROS Classic & Model       Jan 23, if       Intent-Type to configur       Physical       Port       SROS Classic & Model       Jan 23, if       Intent-Type to configur       Logical       BFD       SROS Model       Jan 23, if       Intent-Type to configur       Logical       BFD       SROS Model       Jan 23, if       Intent-Type to configur       Logical       BFD       SROS Model       Jan 23, if       Ref       Logical         outer-cospf-interface_marcs_23-10-1_24-4       1       Successful       Intent-Type to configur       Logical       Router       SROS Model       Jan 23, if       Router       Category       Router       Category       Router       SROS Model       Jan 23, if       Router       SRO	pipment-card_mda 2 • Successful Intent-Type to configur Physical Card SROS Classic & Model Jan 23, : i	ie intent-ty
ort-connector_gsros_23-10-1_23-11       1          Successful Intent-type to configur           Physical Physical           Port           SROS Classic & Model           Jan 23, if           Intent-Type to configureis             mequipment-port-ethermet           2         Successful         Intent-type to configur           Physical           Port           SROS Classic & Model           Jan 23, if              df-sbfd-reflector_msros_23-10-1_23-11           1           Successful           Intent-Type to configur           BFD           SROS Model           Jan 23, if            Cogical          outer-ospf-area_msros_23-10-1_23-11           1           Successful           Intent-Type to configur           Logical           Router           Cogical           Logical           Logical           Logical           Logical           Router           Cogical           Logical           Logical           Logical           Logical           Logical           Logical           Logical           Router	th_msros_23-10-1_24-4 1 • Successful Intent-Type to configur Physical Port SROS Model Jan 23.: : Description	
m-equipment-port-ethemet     2     • Successful     Intent-type to configur     Physical     Port     SROS Classic & Model     Jan 23, 1     Ref       fds-bfd-reflector_msros_23-10-1_23-11     1     • Successful     Intent-Type to configur     Logical     BFD     SROS Model     Jan 23, 1     Category       outler-ospf-area_msros_23-10-1_23-11     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Category       outler-ospf-area_msros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Monter       outler-ospf-area_msros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Monter       outler-interface_msros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Monter       outler-interface_msros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Monter       outler-interface_msros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Monter       moutle	onnector_gsros_23-10-1_23-11 1   Successful Intent-type to configure. Physical Port SROS Classic & Model Jan 23, : : Intent-Type to configure isis-interface	or classic SR
Indextd-reflector_maros_23-10-1_23-11     I        • Successful     Intent-Type to configur     Logical        BFD        SROS Model     Jan 23, II     Logical        Logical       outer-ospf-area_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        Category       Router       outer-ospf-farea_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        Router       outer-ospf-farea_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        Device Stepse       outer-interface_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        Device Stepse       outer-interface_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        SROS Stepse       outer-interface_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, II        SROS Stepse       outer-interface_maros_23-10-1_24-4     1     • Successful     Intent-Type to configur	uppment-port-ethernet 2 • Successful Intent-type to configur Physical Port SROS Classic & Model Jan 23.: : Role	
cuter-copf-area_msroa_23-10-1_24-4     1     Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Category Router       outer-copf-interface_msroa_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Parket Stepp       outer-copf-interface_msroa_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Stocessful       outer-interface_msroa_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Stocessful       monter-interview/interface_msroa_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Stocessful       monter-interview/interface_msroa_23-10-1_24-4     1     • Successful     Intent-Type to configur     Logical     Router     SROS Model     Jan 23, 1     Stocessful	fd+reflector_msros_23-10-1_23-11 1 • Successful Intent-Type to configur Logical BFD SROS Model Jan 23.: : Logical	
puter-ospf-interface_msros_23-10-1_24-4     1 <ul> <li>Successful</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Model</li> <li>Jan 23, 1</li> <li>Device Scope</li> <li>SROS Classic</li> <li>SROS Classic</li> <li>SROS Classic</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Model</li> <li>Jan 23, 1</li> <li>Device Scope</li> <li>SROS Classic</li> <li>SROS Classic</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Model</li> <li>Jan 23, 1</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Model</li> <li>Jan 23, 1</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Model</li> <li>Jan 23, 1</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Classic</li> <li>SROS Classic</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Router</li> <li>SROS Classic</li> <li>Model</li> <li>Jan 23, 1</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Logical</li> <li>Router</li> <li>SROS Classic</li> <li>Intent-Type to configur</li> <li>Logical</li> <li>Logical</li> <li>Router</li> <li>SROS Classic</li> <li>SROS Classic</li> <li>Intent-Type to configur</li> <li>Logical</li> /ul>	-ospF-area_msros_23-10-1_24-4 1 © Successful Intent-Type to configur Logical Router SROS Model Jan 23.: i Rester r	
puter-interface_msros_23-10-1_24-4 1 © Successful Intent-Type to configur Logical Router SR05 Model Jan 23, : SR05 Classic	-ospF-interface_msros_23-10-1_24-4 1   SROS Model Jan 23,   Device Scose	
rm-muter-network-interfane 2 Osurressful Intent-Type to configur Logical Interfane SPDS Classic & Model Lan 23 : Imported	-interface_msros_23-10-1_24-4 1 • Successful Intent-Type to configur Logical Router SROS Model Jan 23.: : SROS Classic	
	uter-network-interface 2 • Successful Intent-Type to configur Logical Interface SROS Classic & Model Jan 23, : : Imported	
ort-eth_csros_23-10-1_24-4 1    Successful Intent-Type to configur Physical Port SROS Classic Jan 23, 1  Jan 23, 2025 b:2/38 pm	th_coros_23-10-1_24-4 1 • Successful Intent-Type to configur Physical Port SROS Classic Jan 23, :	
outer-ospf-area_csros_23-10-1_24-4 1 © Successful Intent-Type to configur Logical Router SROS Classic Jan 23, 1: Jan 23, 2: Jan 24, 3: Jan 2	-ospF-area_esros_23-10-1_24-4 1 • Successful Intent-Type to configur Logical Router SROS Classic Jan 23. : i Jan 23. 2025 662.60 pm	
outer-ospf-Interface_csros_23-10-1_24-4 1   Successful Intent-Type to configur Logical Router SROS Classic Jan 23.: :  Configuration Form	-ospF-interface_csros_23-10-1_24-4 1     Successful Intent-Type to configur Logical Router SROS Classic Jan 23.: :   Configuration Form	
outer-isis-interface_csros_23-10-1_24-4 1   Successful Intent-Type to configur Logical Router SROS Classic Jan 23, i default default	isis-interface_csros_23-10-1_24-4 1 O Successful Intent-Type to configur Logical Router SROS Classic Jan 23, i default	

#### 2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-isis-interface**classic.

NSP

NOCIA     Network Service	es Platform					User: admin 🔹 🕥
Device Management Configuration Configuration Terr	nplates 👻					+ TEMPLATE C-
Name	Description	Life Cycle	Target Labels	Intent Type	Intent :	(i) Template Details
T	T	-		Т		
Customer_Template	-	released 👻	-	icm-service-customer	:	∧ General
System_PTP_Template	-	released 👻	-	icm-system-ptp	:	Name
System_Security_Cpm_Template	-	released 👻	-	icm-system-security_cpm	:	Router-isis-interface-classic
Lldp_md_Template	-	released 👻	-	system-IIdp_msros_23-10-1	:	Description
System_Cpu_Protection_Template	-	released 👻	-	security-cpu-protection_gsros	:	- '
Equipment-bfd-template	-	released 👻	-	bfd-bfd-template_gsros_23-1	:	Life Cycle
Equipment-card_mda	-	released -	-	icm-equipment-card_mda	:	released
Equipment-port-eth-msros	-	released 🗸	-	port-eth_msros_23-10-1_24-4	:	Target Labels
Equipment-port-connector	-	released -	-	port-connector_gsros_23-10	:	-
Equipment-port-ethernet	-	released -	-	icm-equipment-port-ethernet	:	Intent Type router-isis-interface csros 23-10-1 24-4
Equipment-bfd-sbfd-reflector-template	-	released -	-	bfd-sbfd-reflector_msros_23	:	Intent Type Version
Router-ospf-area	-	released -	-	router-ospf-area_msros_23-1	:	1
Router-ospf-interface	-	released -	_	router-ospf-Interface_msros	:	Config Form
Router-Interface-msros	-	released -	_	router-interface_msros_23-10	:	detault
Router-Interface-unified	-	released -	_	icm-router-network-interface	:	Config Form State
Equipment-port-eth-csros	-	released -	-	port-eth_csros_23-10-1_24-4	:	
Router-ospf-area-classic	-	released -	_	router-ospf-area_csros_23-10	:	Role Logical
Router-ospf-interface-classic	-	released -	_	router-ospf-interface_csros_2	:	Category
Router-isis-interface-classic	-	released -	-	router-isis-interface_csros_23	:	Router
						Device Scope SROS Classic
						Flexible Yes
						Created
b.	4				<b>b</b> d b	Jan 23, 2025 6:29:25 pm
Auto-refresh Last Refresh: 202	5/1/23 18:29:30		<pre></pre>		Count: 19	Last Updated Jan 23, 2025 6:29:25 pm

Create configuration deployments using the above configuration template. The following example deploys on 7750 SR-14s classic NE.

Router-isis-interface-classic						×
ISIS Interface	ISIS Interface					
Level 1 Authentication	Description		Administrative State		Туре	
Level 2	Towards Core1		Up .	r Cx	broadcast	Cx
Authentication Authentication	Level Capability level_1_and_2	□x	IPv4 BFD Enabled		IPv6 BFD Enabled	
	CSNP Interval		LSP Pacing Interval		Retransmit Interval	
	10		100		5	
	Mesh Group Status		Mesh Group		Passive	
	disabled 🗸		1		false	
	IPv6 Unicast Enabled		Route Tag		_	
	false 🔹	□x	0		Loop-free Alternate Exclude	
	IPv4 Multicast Enabled		IPv6 Multicast Enabled		Load Balancing Weight	
	true 👻	$\Box_{\mathbf{x}}$	true -	r 🗔	0	
	Hello Padding		Route Next-Hop Policy		IPv4 SID Type	
	disable 👻	Cx.		×	none	⊂x
	IPv6 SID Type		SID Protection		Default Instance ()	
	none 👻	$\Box_{\mathbf{x}}$	enabled -	r 🗔	false	⊂ <sub>x</sub>
	Flexible Algorithm					+ ADD
						CANCEL UPDATE

Deploy Logical Configuration				×
Select Templates *	Select Templates	CLEAR ALL	+ TEMPLATE	
Select largets and Edit Selected lemplate *			Count : 1	
	Select Targets and Edit Selected Template	CLEAR ALL	+ TARGET	Ì
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TE	MPLATE CONFIG	
	Configurations required by the selected templates are assigned. View/Edit			
	Only 1 target can be selected for the selected template			
	Reachability NE Name NE ID Management IP Product			
	T T T T			
	Up Toronto 92.168.96.215 135.249.150.4 7750.5R			
			Count : 1	
	Assign Identifier for Selected Template			ľ
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.			
	1. Router-Isis-Interface-classic :			
	ISIS Instance" Interface Name"			
	0 X IsisIntf-1 X			
		CANCEL S	AVE DEPL	ογ

=	NOKIA	Network Serv	vices Platform										User: admin	-	0
Devic	e Management	Configuration Configuration	Deployments •										+ DEPLOYMENT	Ċ,	
	Deployment Stat	tus	Configuration Status	NE Name	N	NE ID		Identifier	Template	Role	Category	:	Deployment Details		
		•	-		T		T	T	T	-					
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	NSP	0	0.0.0		TransCanadian Railway	Customer_Template	Logical	Service	-	NE Name Toronto		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		cpm	System_Security_Cpm	Logical	System		NE ID		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		cpm	System_Security_Cpm	Logical	System	:	92.168.96.215		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		lldp	Lldp_md_Template	Logical	System	:	Identifier		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		23	System_Cpu_Protectio	Logical	System	:	ISIS Instance		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		ptp	System_PTP_Template	Logical	PTP	:	0		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		ptp	System_PTP_Template	Logical	PTP	:	Interface Name		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	CE_West	9	92.168.99.6		bfd-template-A	Equipment-bfd-template	Logical	BFD	:			
	<ul> <li>Deployed Aligr</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		bfd-template-A	Equipment-bfd-template	Logical	BFD	:			
	<ul> <li>Deployed Aligr</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		1/1/c2/1	Equipment-port-eth	Physical	Port	:	Deployment Status		
	<ul> <li>Deployed Aligr</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		Port 1/1/c1/1	Equipment-port-ether	Physical	Port	:	Deployed Highed		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		1/1/c1/1	Equipment-port-ether	Physical	Port	:	AUDIT ALIGN		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		bfd-template-A	Equipment-bfd-template	Logical	BFD	:			- 1
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		1#1.1.1.1	Router-ospf-area	Logical	Router	:	Last Audit		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		1#1.1.1.1#test4	Router-ospf-interface	Logical	Router	:	-		
	Deployment Fa	ailed	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		toCore_2	Router-interface-msros	Logical	Router	:	Jan 23, 2025 6:37:03 pm by admin		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Boston	9	92.168.96.46		test7	Router-interface-unified	Logical	Interface	:	Template Name		
	<ul> <li>Deployment Fa</li> </ul>	ailed	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		test7	Router-interface-unified	Logical	Interface	:	Router-isis-interface-classic		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		0#0.0.0.0	Router-ospf-area-classic	Logical	Router	:	Created Jan 23, 2025 6-37-00 nm		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		0#0.0.0.0#test1	Router-ospf-interface	Logical	Router	:	Last Updated		
	<ul> <li>Deployed Align</li> </ul>	ned	<ul> <li>Modified</li> </ul>	Toronto	9	92.168.96.215		0#isisIntf-1	Router-isis-interface-c	Logical	Router	-	Jan 23, 2025 6:37:03 pm		
													Role Logical		
< > ·	C.										×	$\leftrightarrow$	Category router		
	Auto-refresh	Last Refresh: 2	2025/1/23 18:37:08					Page: 1 / 1 >			Count	: 21	Configuration Status		

NSP

Figure 7-22 NE CLI after deployment



END OF STEPS -

# 7.7 MPLS/RSVP Interfaces

## 7.7.1 To configure MPLS interface on MD NEs using router-mpls-interface-msros

1

Import the intent type router-mpls-interface\_msros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

Device Management Configuration Configuration Intent Types												+ IMPORT C
Intent Type		Version		Status	Description		Role	Category		Device Scope	Last Upr 🗄	i Intent Type Details
	T		T	-		T	•		-	•	MMM c	
icm-router-network-interface			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical	Interface		SROS Classic & Model	Dec 10, 🗄	Intent Type router-mpls-interface_msros_23-10-1_24-4
router-mpls-interface_maros_23-10-1_24-4			1	• Successful	Intent-Type to configur		Logical	Router		SROS Model	Dec 12, i	Version 1 State Successful Successful Successful Successful Successful Configure category router and device- config interface Rele Logical Category Router Device Sege SROS Model Imparted Dec 12, 2024 4:49:57 pm Last Updated Dec 12, 2024 4:50:04 pm Configures From default
4 Auto-refresh Last Refresh: 2024/12/12 16:5	0-57	_		_	14 4	Page		ы			▶ ( )> Count : 2	

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-mpls-msros**.

Configuratio	iem	210.023										
ame		Description		Life Cycle		Target Labels		Intent Type		Intent '	:	(i) Template Details
	T		T		•		T		T			an anna la
uter-interface-unified		-		released	÷	-		icm-router-network-in	terface		÷	∧ General
user-in poetinsros				1999594				Touer injuer iterate				Name Router-mpls-maros Pascription Pascription Treleased Treleased Treleased Touter-mpls-interface_maros_23-10-1_24-4 Intent Type Version I Config Form default Config Form default Config Form State Up-to-date Role Logical Conter Role SKOS Model Fissible Yes Constate Versible Constate Versible Constate Conter
	$\rightarrow \cdot$	•								•	4 >	Dec re, 2024 4:50:17 pm
		(12/12/16/16/22)				1/1 / Dans 1 /1						Last opened

Create configuration deployments using the above configuration template. The following example uses 7750 MD.

Router-mpls-msros				×										
Interface	Interface	Interface												
			Row Count: 0											
	Label Map		+ ADD											
	Ingress Label	Admin State												
	222	enable	:											
			Row Count: 1											
			,	CANCEL UPDATE										

Deploy Logical Configuration			×	:
Select Templates * Select Targets and Edit Selected Template *	Select Templates	CLEAR ALL	+ TEMPLATE	•
Assign Identifier for Selected Template *			Count : 1	
	Select Targets and Edit Selected Template	CLEAR ALL	+ TARGET	l
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TE	EMPLATE CONFIG	l
	Configurations required by the selected templates are assigned. Wew/Edit			I
	Only 1 target can be selected for the selected template			I
	Reachability NE Name NE ID Management IP Product			I
	T         T         T         T         T           •Ib         Boston         92 168 96 46         135 249 153         7750 58			I
			-	1
			Count : 1	1
	Assign Identifier for Selected Template			
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.			l
	1. Router-mpli-msras : INTERFACE-NAME"			
	test4 X			
		CANCEL S	SAVE DEPLOY	Y

Figure 7-23 NE CLI after deployment



END OF STEPS
# 7.7.2 To configure MPLS interface on Classic NEs using router-mpls-interfacecsros

router-mpls-interface\_csros\_23-10-1\_24-4 intent can be used for MPLS interface configuration on classic NEs.

1

Import the intent type router-mpls-interface\_csros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

■ NO <ia network="" p="" platform<="" services=""></ia>	ı								User: admin 👻 📀
Device Management Configuration Configuration Intent Types	•								+ IMPORT C
Intent Type	Version		Status	Description	Role	Category	Device Scope	Last Upr 🚦	i) Intent Type Details
	T	T	-	T	-	-	•	MMM c	
icm-service-customer		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Service	SROS Classic & Model	Jan 23, 🔡	Intent Type router-mols-interface csros 23-10-1 24-4
icm-system-ptp		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	PTP	SROS Classic & Model	Jan 23, 🔡	Version
icm-system-security_cpm		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🖂	1
system-lldp_msros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Jan 23, 🖂	Status
security-cpu-protection_gsros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🔡 🚦	• Current d
bfd-bfd-template_gsros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Jan 23, 🖂 🛙	Successful
icm-equipment-card_mda		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Jan 23, 🔡	Successionly imported neimported the interic-type
port-eth_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Jan 23, 🔡	Description
port-connector_gsros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🔡	Intent-Type to configure mpls-Interface for classic
icm-equipment-port-ethernet		2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🔡	SRUS
bfd-sbfd-reflector_msros_23-10-1_23-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Jan 23, 🔡	Role
router-ospf-area_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	Category
router-ospf-interface_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	Router
router-interface_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🗌	Device Scope
icm-router-network-interface		2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Interface	SROS Classic & Model	Jan 23, 🔡	SRUS Classic
port-eth_csros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Jan 23, 🗌	Jan 23, 2025 6:43:25 pm
router-ospf-area_csros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🖂	Last Updated
router-ospf-interface_csros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡 🕴	Jan 23, 2025 6:43:32 pm
router-isis-interface_csros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🖂	Configuration Form
router-mpls-interface_csros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🖂	default
Auto-refresh Last Refresh: 2025/1/23 18:43:	51			I< < Page:	: 1 /1 > ⊃l			Count : 20	

2

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as Router-mpls-csros.

■ NO <ia network="" s<="" th=""><th>Service</th><th>s Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻 🕐</th></ia>	Service	s Platform								User: admin 👻 🕐
evice Management Configuration	n Ion Terr	plates	-							+ TEMPLATE
lame		Description		Life Cycle		Target Labels		Intent Type	Intent' :	(i) Template Details
	۲		T		*		T	т		
Customer_Template		-		released	-			icm-service-customer	:	∧ General
ystem_PTP_Template				released	-			icm-system-ptp	:	
ystem_Security_Cpm_Template		-		released	-	1		icm-system-security_cpm	:	Name Router-mpls-csros
ldp_md_Template				released		<u></u>		system-Ildp_msros_23-10-1	:	Description
ystem_Cpu_Protection_Template				released				security-cpu-protection_gsros	:	_
quipment-bfd-template				released				bfd-bfd-template_gsros_23-1	:	Life Cycle
quipment-card_mda				released				icm-equipment-card_mda	:	released
quipment-port-eth-msros				released				port-eth_msros_23-10-1_24-4	:	Target Labels
quipment-port-connector				released				port-connector_gsros_23-10	:	_
quipment-port-ethernet				released				icm-equipment-port-ethernet	:	Intent Type router-mpls-interface csros 23-10-1 24-4
quipment-bfd-sbfd-reflector-temp	ate			released				bfd-sbfd-reflector_msros_23	:	Intent Type Version
outer-ospf-area				released				router-ospf-area_msros_23-1	:	1
outer-ospf-Interface		-		released				router-ospf-interface_msros	:	Config Form
uter-Interface-msros		-		released				router-Interface_msros_23-10	:	default
outer-Interface-unified		-		released		_		icm-router-network-Interface	:	Config Form State
ulpment-port-eth-csros		-		released				port-eth_csros_23-10-1_24-4	:	op-to-date
outer-ospf-area-classic		-		released		_		router-ospf-area_csros_23-10	:	Logical
outer-ospf-Interface-classic		-		released	*			router-ospf-Interface_csros_2	:	Category
outer-IsIs-Interface-classic		-		released				router-Isis-Interface_csros_23	:	Router
outer-mpls-csros		_		released	*	-		router-mpls-Interface_csros_2	:	Device Scope SROS Classic
										Flexible Yes Created Jan 23, 2025 6:45:10 pm
	- F	4								Last Updated
Auto-refresh Last Refre	sh: 202!	5/1/23 18:45:15				IC C Page: 1 / 1 > >1			Count: 20	Jan 23, 2025 6:45:10 pm

Create configuration deployments using the above configuration template.

Router-mpls-csros													
MPLS Interface	MPLS Interface												
TP MEP Interface		No data to display											
		<: < Page: 0 /0; ≥	Total: 0										
	TE Metric 32												
	Static Label Maps	+ ADD											
	Label Action Admir	istrative State Ingress Label											
	pop mplsX	cUp 222	1										
		<pre> &lt; Page: 1 /1 &gt; &gt;)</pre>	Total: 1										
			CANCEL UPDAT										

Figure 7-24 NE CLI after deployment



END OF STEPS -

# 7.7.3 To configure RSVP interface on MD NEs using router-rsvp-interface\_msros\_ 23-10-1\_24-4



```
(pr)[/configure router "Base" rsvp diffserv-te]
A:admin@Boston# info
admission-control-model rdm
```

2 -

Import the intent type router-rsvp-interface\_msros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

evice Management Configuration Configuration Intent Types		•										+ IMPORT
itent Type		Version		Status	Description	Role		Category		Device Scope	Last Upr 🗄	i Intent Type Details
	T		T	•	T		*		*	•	MMM c	
m-router-network-interface			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		Interface		SROS Classic & Model	Dec 10, 🗄	router-rsvp-interface_msros_23-10-1_24-4
uter-mpls-interface_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		Router		SROS Model	Dec 12, 🗄	Version
uter-rsvp-interface_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		Router		SROS Model	Dec 12, 🗄	1
												Statu Successfull Successfully imported/re-imported the intent-ty Description Intent-Type to configure category router and device config interface Rele Logical Category Router Device Scope SRO5 Model Imported Dec 12, 2024 5:21:37 pm Last Updated Dec 12, 2024 5:21:37 pm Last Updated Dec 12, 2024 5:21:43 pm Configuration Form default
											$\bullet \to \bullet$	
<ul> <li></li></ul>												

3 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-rsvp-interface**.

Device Management Configuration Configuration Te	emp	lates •									+ TEMPLATE
Name		Description		Life Cycle		Target Labels		Intent Type		Intent :	i Template Details
	T		T		•		Ŧ		T		
Router-Interface-unified		-		released	•	-		icm-router-network-interface		:	∧ General
Router-mpls-msros		-		released	•	-		router-mpls-interface_msros		:	Name
Router-rsvp-Interface		-		released		-		router-rsvp-interface_msros		:	Router-rsvp-interface
											Description
											Life Cycle
											Target Labels
											Intent Type router-rsvp-interface_msros_23-10-1_24-4
											Intent Type Version 1
											Config Form default
											Config Form State Up-to-date
											Role Logical
											Category Router
											Device Scope SROS Model
											Flexible Yes
,										<b>F</b> (	Created Dec 12, 2024 5:26:24 pm
Auto-refresh Last Refresh: 20	024/	12/12 17:26:30				IC C Page:	1 /1 > >1			Count : 3	Last Updated Dec 12, 2024 5:26:24 pm

Create configuration deployments using the above configuration template. The following example uses 7750 MD.

Router-rsvp-interface				×
Interface	Interface			*
Class Type BW Refresh Reduction TE DOWN Threshold TE UP Threshold	Admin State enable • SFD Liveness Hello Interval (seconds) 20	Authentication Keychain X	Authentication Key           Image: Craceful Shutdown           Implicit Null Label	
	Class Type 0 BW Class Type 0 BW Percent 10 Class Type 3 BW Percent	Class Type 1 BW Percent 30 Class Type 4 BW Percent	Class Type 2 BW Percent 5 Class Type 5 BW Percent	
	15 Class Type 6 BW Percent 10	20 Closs Type 7 BW Percent 5	5	
	Refresh Reduction			
			c	ANCEL UPDATE

Deploy Logical Configuration			×
Select Templates * Select Targets and Edit Selected Template * Assign identifier for Selected Template *	Select Templates	CLEAR ALL + TE	MPLATE
		C	sunt : 1
	Select Targets and Edit Selected Template	CLEAR ALL +	TARGET
	Select targets. Template configurations can be edited after targets are selected.  Configurations required by the selected templates are assigned. View/Edit	VIEW/EDIT TEMPLATE	CONFIG
	Reschability NE Name NE ID Management IP Product		
	T T T T		
	● Up Boston 92,168,96,46 135,249,153 7750 SR		-
		C	ount of the
	Assign Identifier for Selected Template		
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.		
	1. Router-resp-interface : INTERFACE-NUME*		
	test4 X		
		CANCEL SAVE	DEPLOY

Figure 7-25 NE CLI after deployment



END OF STEPS

# 7.7.4 To configure RSVP interface on Classic NEs using router-rsvp-interface\_ msros\_23-10-1\_24-4

router-rsvp-interface\_csros\_23-10-1\_24-4 intent can used for the configuration of RSVP on classic NEs.

1

Import the intent type router-rsvp-interface\_csros\_23-10-1\_24-4 into Device Management, Configuration Intent Types.

■ NO <ia network="" platform<="" services="" th=""><th>n</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻 🕜</th></ia>	n									User: admin 👻 🕜		
Device Management Configuration Configuration Intent Types		•								+ IMPORT 📿		
Intent Type	Version			Status	Description	Role	Category	Device Scope	Last Upr 🗄	(i) Intent Type Details		
	T		T	-	T	-	-	•	MMM c			
icm-service-customer			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Service	SROS Classic & Model	Jan 23, 🔡	Intent Type router-rsvp-interface_csros_23-10-1_24-4		
icm-system-ptp			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	PTP	SROS Classic & Model	Jan 23, 🔡	Version		
icm-system-security_cpm			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🔡	1		
system-Ildp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Jan 23, 🗌	Status		
security-cpu-protection_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Classic & Model	Jan 23, 🔡	• Current 1		
bfd-bfd-template_gsros_23-10-1_23-11	_23-11				1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Jan 23, 🗌	Successful
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Jan 23, 🗌	Successionly imported the intent-type		
port-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Jan 23, 🔡	Description		
port-connector_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🗌	Intent-Type to configure rsvp-Interface for classic SROS		
icm-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Jan 23, 🗌	Role		
bfd-sbfd-reflector_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Jan 23, 🔡	Logical		
router-ospf-area_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🗌	Category Router		
router-ospf-interface_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🗌 🕴	Device Scope		
router-interface_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Jan 23, 🔡	SROS Classic		
icm-router-network-interface			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Interface	SROS Classic & Model	Jan 23, 🗌 🕴	Imported		
port-eth_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Jan 23, 🔡	Jan 23, 2025 7:12:02 pm		
router-ospf-area_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡	Jan 23, 2025 7:12:08 pm		
router-ospf-interface_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🗌 🕴	Configuration Form		
router-isis-interface_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡	default		
router-mpls-interface_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🗌 🕴			
router-rsvp-interface_csros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Classic	Jan 23, 🔡			
Auto-refresh Last Refresh: 2025/1/23 19:12:	25				I< < Page	: 1 <b>/1</b> → →			Count : 21			

#### 2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-rsvp-interface**classic.

	Network Service	es Platfor	m								User: admin 👻 I
evice Management	Configuration Configuration Ten	nplates									+ TEMPLATE
ame		Descri	ption		Life Cycle		Target Labels		Intent Type	Intent' :	(i) Template Details
	т			T		*		T	T		
ustomer_Template		-			released				icm-service-customer	:	∧ General
stem_PTP_Template		-			released		-		icm-system-ptp	:	
stem_Security_Cpm_	_Template	-			released	-	_		icm-system-security_cpm	:	Name Router-rsvo-interface-classic
dp_md_Template		-			released	-	_		system-lldp_msros_23-10-1	:	
stem_Cpu_Protectio	n_Template	-			released	-	-		security-cpu-protection_gsros	:	-
juipment-bfd-templa	ite				released	-	_		bfd-bfd-template_gsros_23-1	:	Life Cycle
uipment-card_mda					released	-	-		icm-equipment-card_mda	:	released
uipment-port-eth-m	isros	-			released	-	_		port-eth_msros_23-10-1_24-4	:	Target Labels
uipment-port-conne	ector	-			released	-	_		port-connector_gsros_23-10	:	-
uipment-port-etherr	net	-			released	-	_		icm-equipment-port-ethernet	:	Intent Type
uipment-bfd-sbfd-re	eflector-template	-			released	-	_		bfd-sbfd-reflector_msros_23	:	Intent Type Version
uter-ospf-area		-			released	-	_		router-ospf-area_msros_23-1	:	1
uter-ospf-interface		-			released	-	_		router-ospf-interface_msros	:	Config Form
uter-interface-msro:	s	-			released	-	_		router-interface_msros_23-10	:	default
uter-interface-unifie	ed	-			released	-	_		icm-router-network-interface	:	Config Form State
uipment-port-eth-cs	sros	-			released	-	_		port-eth_csros_23-10-1_24-4	:	op-to-date
uter-ospf-area-class	sic	-			released	-	_		router-ospf-area_csros_23-10	:	Logical
uter-ospf-interface-	classic	-			released	-	_		router-ospf-interface_csros_2	:	Category
uter-isis-interface-cl	lassic	-			released	-	_		router-isis-interface_csros_23	:	Router
uter-mpls-csros					released	-	_		router-mpls-interface_csros_2		Device Scope
uter-rsvp-interface-	classic	_			released	+	_		router-rsvp-interface_csros_2	:	SRUS Classic
											Yes
											Created
	•	4								• • •	Jan 23, 2025 7:13:50 pm
-											Last Updated

Create configuration deployments using the above configuration template. The following example uses 7750 MD.

Router-rsvp-interface-classic			x
RSVP Interface	RSVP Interface		i i i i i i i i i i i i i i i i i i i
RSVP Authentication Key RSVP TE Thresholds	Description Inherit NFM-P Class Type BW Enable Implicit Null Label Hello Interval 3000	Administrative State Up   Subscription Ratio 100 Graceful Restart Helper Mode	Enable Graceful Shutdown     BFD Enabled     Enable Refresh Reduction
	RSVP Authentication Key Key	RSVP Keychain keychain-1	x
	RSVP TE Thresholds           Inherit TE Up Thresholds	✓ Inherit TE Down Thresholds	
			CANCEL UPDATE

Deploy Logical Configuration												×
Select Templates *	Select Templates	3								CLEAR ALL	+ TEMPLATE	e
Assign Identifier for Selected Template *											Count : 1	
	Select Targets ar	nd Edit Selected T	emplate							CLEAR ALL	+ TARGET	
	Select targets. Templ	VIEW/EDIT TE	MPLATE CONFIG									
	Configurations re	quired by the selected te	mplates are ass	igned. View,	/Edit							
	<ul> <li>Only 1 target can</li> </ul>	be selected for the selec	ted template									
	Reachability	NE Name		NE ID		Management IP	1	Product				
		Ť	Ť		T	1	r	Ť				11
	• Up	Ioronto		92.168.96.215		135.249.150.4		7/50 SR				
											Count : 1	
	Assign Identifier	for Selected Tem	plate									
	Assign unique identif	iers for templates sele	cted above to	identify the corr	respo	nding deployment	s. If (	content below is disabled, select targets first to	enable them.			
	1. Router-rsvp-interface-cla	ssic :										
	test7		×									
										CANCEL S	AVE DEF	PLOY

=	NOKIA Network S	ervices Platform							User: admin 🔹 🕜
Devi	e Management Configuratio	on Deployments							+ DEPLOYMENT 🔿 🖀
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	i Deployment Details
	•	-	Ť	T	T	T	-		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service :	NE Name Toronto
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System :	NE ID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System :	92.168.96.215
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System :	Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System :	Interface Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP :	test7
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	bfd-template-A	Equipment-bfd-template	Logical	BFD :	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	bfd-template-A	Equipment-bfd-template	Logical	BFD :	<ul> <li>Deployed Aligned</li> </ul>
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2/1	Equipment-port-eth	Physical	Port :	AUDIT ALIGN
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port :	Last Audit
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	bfd-template-A	Equipment-bfd-template	Logical	BFD :	_
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1	Router-ospf-area	Logical	Router :	Last Alignment
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1#test4	Router-ospf-interface	Logical	Router :	Jan 25, 2025 6:29:25 pm by admin
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	toCore_2	Router-interface-msros	Logical	Router :	Router-rsvp-interface-classic
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	test7	Router-Interface-unified	Logical	Interface	Created
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	test7	Router-Interface-unified	Logical	Interface	Jan 23, 2025 8:29:17 pm
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	0#0.0.0.0	Router-ospf-area-classic	Logical	Router :	Last Updated
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	0#0.0.0.0#test1	Router-ospf-interface	Logical	Router :	Role
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	O#isisIntf-1	Router-isis-interface-c	Logical	Router :	Logical
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	test7	Router-mpls-csros	Logical	Router :	Category
	Deployed Aligned	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	test7	Router-rsvp-interface	Logical	Router :	router
< ►								$\rightarrow \rightarrow$	Configuration Status <ul> <li>Modified</li> </ul>
	Auto-refresh Last Refre	nh: 2025/1/23 20:32:56		K	< Page: 1 / 1 > >			Count : 23	





END OF STEPS -

# 7.8 Interfaces

### 7.8.1 To configure router interface with icm-router-network-interface intent

1 -

Import the intent type icm-router-network-interface into Device Management, Configuration Intent Types.

Device Management Configuration	n on Intent Ty	bes	•							+ IMPORT
Intent Type	V	ersion		Status	Description	Role	Category	Device Scope	Last Updated :	i Intent Type Details
	T		T	•	T	-	•	•	MMM d, yyyy h:mm:ss	
icm-equipment-card_mda			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Card	SROS Classic & Model	Nov 26, 2024 11:25:43 :	Intent Type icm-router-network-interface
port-connector_gsros_23-10-1_23-	11		1	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Nov 26, 2024 4:17:03 pr	Version
icm-equipment-port-ethernet			2	<ul> <li>Successful</li> </ul>	Intent-type to configur	Physical	Port	SROS Classic & Model	Dec 2, 2024 11:12:32 ar	2
icm-equipment-port-access-ce			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Classic	Dec 2, 2024 1:19:32 pm	Status
port-eth_msros_23-10-1_24-4			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Physical	Port	SROS Model	Dec 2, 2024 1:51:20 pm	
system-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	System	SROS Model	Dec 2, 2024 3:52:48 pm	Successfully imported/re-imported the intent-tup
bfd-bfd-template_gsros_23-10-1_2	3-11		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Classic & Model	Dec 3, 2024 11:01:55 ar	Successionly imported/re-imported the interne-type
bfd-sbfd-reflector_msros_23-10-1_	23		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	BFD	SROS Model	Dec 3, 2024 11:55:48 ar	Description
router-ospf-interface_msros_23-10	1		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 1:47:43 pm	Intent-Type to configure network interface
router-isis-interface_msros_23-10-1			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 3, 2024 3:11:00 pm	Role
router-ospf-area_msros_23-10-1_2	-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 5, 2024 12:00:13 pr	Logical
router-interface_msros_23-10-1_24	-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Router	SROS Model	Dec 6, 2024 3:37:50 pm	Category Interface
icm-router-network-interface			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical	Interface	SROS Classic & Model	Dec 9, 2024 1:48:58 pm 🚦	Device Scope SROS Classic & Model
										Imported Dec 9, 2024 1:48:41 pm
										Last Updated Dec 9, 2024 1:48:58 pm
										Configuration Form
										default, defaultIXR
									▶ < >	

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Router-interface-unified**.

Device Management Configuration Configuration Te	empl	lates •									+ TEMPLATE 📿
Name		Description		Life Cycle		Target Labels	1	Intent Type	Inter	nt'i	(i) Template Details
1	T		T		-	Т		T			
Equipment-card_mda		-		released	•	-	i	icm-equipment-card_mda		:	∧ General
Equipment-port-connector		-		released	*	-	1	port-connector_gsros_23-10		:	Name
Equipment-port-ethernet		-		released	*	-	i	icm-equipment-port-ethernet		:	Router-interface-unified
Equipment-port-access-ce		-		released	*	-	i	icm-equipment-port-access-ce		:	Description
Equipment-port-eth-msros		-		released	*	-	1	port-eth_msros_23-10-1_24-4		:	- '
Equipment-Ildp-msros		-		released	•	-	1	system-lldp_msros_23-10-1		:	Life Cycle
Equipment-bfd-template		-		released	•	-	1	bfd-bfd-template_gsros_23-1		:	released
Equipment-bfd-sbfd-reflector-template		-		released	•	-	1	bfd-sbfd-reflector_msros_23		:	Target Labels
Router-ospf-interface		-		released	•	-		router-ospf-interface_msros		:	
Router-isis-interface		-		released	•	-		router-isis-interface_msros_2		:	icm-router-network-interface
Router-ospf-area		-		released	•	-		router-ospf-area_msros_23-1		:	Intent Type Version
Router-interface-msros		-		released	•	-		router-interface_msros_23-10		:	2
Router-interface-unified		-		released	•	-	i	icm-router-network-interface		- 1	Config Form default
											Cenfig Form State Up-to-date Role Logical Category Interface Device Scope
( ) Auto-refresh Last Refresh: 20	→ 4 024/1	12/9 13:50:44		_		K < Pege 1 /1 > >			Cou	▶ ( int:13	SROS Classic & Model Flexible Yes Crested De 5, 2024 1:50:38 pm Last Upided Dec 9, 2024 1:50:38 pm

Create configuration deployments using the above configuration template. Example 1: 7750 SR-14s MD

Router-interface-unified				×
Interface	Interface			*
LDP Sync Timer				
IPv4	Description	Admin State	Port Binding	
BFD	Interface to Core node	enable 👻	Cx port	▼ Cx
Primary	Port	Outer Tag	Inner Tag	
IPv6	1/1/c2/1 × 0	2		
BFD				
Egress				
QoS	LDP Sync Timer			
VLAN QoS Policy	Seconds			
Egress Remark Policy	100			
Ingress				
QoS				
Network Ingress	IPv4			
108				
Interface Parameters				
MDLC	BFD			
MPL5	Admin State	Transmit Interval (Milli Seconds)	Receive (Milli Seconds)	
RSVP	enable 👻 🗔	100	100	
	Multiplier	Туре		
	2	auto		-
				CANCEL

Router-interface-unified				×
Interface	Interface			*
LDP Sync Timer IPv4 BPD Primary	BFD Admin State enable • C2	Transmit Interval (Milli Seconds) 100 Tune	Receive (Milli Seconds) 100	
IPv6 BPD Egress QoS	2	auto 👻 🖂		
VLAN QoS Policy Egress Remark Policy Ingress	Primary Address 10.10.10.2	Prefix Length 24		
QoS Network Ingress	Secondary		+ ADD	
LDP Interface Parameters MPLS RSVP	Address Prefix Length	No data to display		
			CAN	CEL UPDATE

Router-interface-unified				×
Interface	LDP			*
LDP Sync Timer				
IPv4-				
BFD	Interface Parameters			
Primary	Interface		+ ADD	
IPv6				
BFD	Interface Name	Admin State		
Egress				
QoS	test7	enable	1	
VLAN QoS Policy				
Egress Remark Policy				
Ingress				
QoS				
Network Ingress		I< < Page: 1 / 1 > >I	Total: 1	
LDP				
Interface Parameters	NOL C			
MPLS	MPLS			
RSVP	Interface		+ ADD	
	Interface Name	Admin State		•
			CANCEL	UPDATE

couter-interface-unified						~
nterface	MPLS					
LDP Sync Timer						
IPv4	Interface				+ ADD	
BFD	Interface Name	Admin State				
Primary						
IPv6	test7	enable				
BFD						
Egress						
QoS						
VLAN QoS Policy						
Egress Remark Policy						
Ingress			IC C Page:	1 /1 > >	Total: 1	
QoS						
Network Ingress	DSV/D					
DP	KJVF-					
Interface Parameters	Interface				+ ADD	
MPLS	and the second second	New IN ADDA	Hello Interval	LI DUC WORKSY		
SVP	Interface Name	Admin State	(seconds)	BFD Liveness		
	test7	enable	30	true	1	

Router-interface-unified						×
Interface	RSVP					1
LDP Sync Timer						
IPv4	Interface				+ ADD	
BFD	Interface Name	Admin State	Hello Interval (seconds)	BFD Liveness		
Primary						
IPv6	test7	enable	30	true	1	
BFD						
Egress						
QoS						
VLAN QoS Policy						
Egress Remark Policy						
Ingress			IC C Page:	1 /1 > >1	Total: 1	
QoS	1515				+ ADD	
Network Ingress						
LDP	ISIS Instance					
Interface Parameters						
MPLS			-			
251/2						
RSVP			No data	a to display		
					CANC	EL UPDATE

eploy Logical Configuration										
elect Templates * elect Targets and Edit Selected Template *	Select Template	es								Count : 1
ssign identifier for Selected Template *	Select Targets a									
	Select targets. Tem	plate configurations can b	e edited af	ter targets are se	electe	d.				VIEW/EDIT TEMPLATE CONF
	<ul><li>Configurations</li><li>Only 1 target ca</li></ul>	required by the selected tem	plates are ass d template	signed. View	v/Edit.					
	Reachability	NE Name		NE ID		Management IP	Product	t		
	• Up	Boston	Ť	92.168.96.46	T	135.249.153	7750 SI	R		
										Count : 1
	Assign Identifie	er for Selected Temp	late							
	Assign unique ident	ifiers for templates select	ed above to	o identify the cor	rrespo	nding deployment:	s. If conten	nt below is disabled, select tar	gets first to enable the	:m.
	1. Router-interface-unifie	ed :								
	test/									

=	NO <ia network="" ser<="" th=""><th>vices Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 🔹 🕜</th></ia>	vices Platform							User: admin 🔹 🕜
Devi	e Management Configuration Configuration	Deployments •							+ DEPLOYMENT 🔿 🖀
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	(i) Deployment Details
	-	-	T	T	T	T	-		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service :	NE Name Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System :	NE ID
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System :	92.168.96.46
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System :	Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System :	INTERFACE NAME
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP :	test7
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	CE_West	92.168.99.6	bfd-template-A	Equipment-bfd-template	Logical	BFD :	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	bfd-template-A	Equipment-bfd-template	Logical	BFD :	<ul> <li>Deployed Aligned</li> </ul>
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2/1	Equipment-port-eth	Physical	Port :	AUDIT ALIGN
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	Port 1/1/c1/1	Equipment-port-ether	Physical	Port :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/1	Equipment-port-ether	Physical	Port :	Last Audit
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	bfd-template-A	Equipment-bfd-template	Logical	BFD :	-
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1	Router-ospf-area	Logical	Router :	Last Alignment Jan 9, 2025 5-25-07 nm by admin
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1#1.1.1.1#test4	Router-ospf-interface	Logical	Router :	Template Name
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	toCore_2	Router-interface-msros	Logical	Router :	Router-interface-unified
	<ul> <li>Deployment Failed</li> </ul>	<ul> <li>Modified</li> </ul>	Boston2	92.168.99.50	test5	Router-interface-msros	Logical	Router :	Created
	Deployed Aligned	Modified	Boston	92.168.96.46	test7	Router-interface-unified	Logical	Interface :	Jan 9, 2025 5:10:28 pm
									Last Updated Jan 9, 2025 5:25:07 pm
									Role
									Logical
									Category interface
4 F -	C								Configuration Status Modified
	Auto-refresh Last Refresh:	2025/1/9 17:25:08		K	< Page: 1 /1 > >			Count : 18	

Figure 7-27 NE CLI after deployment



Example 2: 7750 SR-14s Classic

Router-interface-unified							×
Interface	Interface						
LDP Sync Timer							
IPv4	Description		Admin State		Port Binding		
BFD	Interface to Core NE		enable	• Cx	port	▼ □x	
Primary	Port		Outer Tag		Inner Tag		
IPv6	1/1/c1/9	× O	4				
BFD							
Egress							
QoS	LDP Sync Timer						
VLAN QoS Policy	Seconds						
Egress Remark Policy	100						
Ingress							
QoS							
Network Ingress	IPv4						
LDP							
Interface Parameters							
MPLS	BFD						
11 20	Admin State		Transmit Interval (Milli Seconds)		Receive (Milli Seconds)		
RSVP	enable	• Cx	100		100		
	Multiplier		Туре				
	2		auto				

Router-interface-unified					×
Interface	Interface				*
LDP Sync Timer	BFD				
IPv4					
BFD	Admin State		Transmit Interval (Milli Seconds)	Receive (Milli Seconds)	
Primary	enable	• Lx	100	100	-
IPv6	Multiplier		Туре		
BFD	2		auto 👻 🕞		
Egress					
QoS					
VLAN QoS Policy	Primary				
Egress Remark Policy	Address		Prefix Length		
Ingress	10.10.10.2		30		
QoS					
Network Ingress	Secondary			+ ADD	
LDP	Address	Prefix Length			
Interface Parameters					
MPLS					
RSVP					
			No data ta dicalay		
			ing apple of display		
				CA.	OPDATE

Router-interface-unified			×
Interface	LDP		
LDP Sync Timer			
IPv4			
BFD	Interface Parameters		
Primary	Interface	1.1	DD
IPv6			
BFD	Interface Name Admin	State	
Egress			
QoS	test1 enable		1
VLAN QoS Policy			
Egress Remark Policy			
Ingress			
QoS			
Network Ingress		IC C Page: 1 /1 > >I Tot	al: 1
LDP			_
Interface Parameters			
MPLS	MPLS		
RSVP			
	Interface	+ AD	D
	Interface Name Admin St	tate	

Router-interface-unified						×
Interface	MPLS					*
LDP Sync Timer	Interface				+ 4DD	
BFD	Interface Name	Admin State			T ADD	
Primary						
IPv6	test1	enable			1	
BFD						
QoS						
VLAN QoS Policy						
Egress Remark Policy						
Ingress			IC C Page:	1 /1 > >1	Total: 1	
QoS						
LDP	RSVP					
Interface Parameters	Interface				+ ADD	
MPLS	Interface Name	Admin State	Hello Interval	BFD Liveness		
RSVP			(2000)			
	test1	enable	60	true	1	
					c	ANCEL UPDATE

Router-interface-unified						×
Interface	RSVP					*
LDP Sync Timer						
IPv4	Interface				+ ADD	
BFD	Interface Name	Admin State	Hello Interval (seconds)	BFD Liveness		
Primary						
IPv6	test1	enable	60	true	1	
BFD						
Egress						
QoS						
VLAN QoS Policy						
Egress Remark Policy						
Ingress			IC < Page:	1 /1 > >	Total: 1	
QoS	ISIS					
Network Ingress					1.000	
LDP	ISIS Instance					
Interface Parameters						
MPLS						
RSVP						
			No dat	ta to display		
					CANCEL	LUPDATE

**i** Note: The deployment works without the primary IPv4 address, MPLS, and RSVP configurations on the 7750 SR-14s classic NE, and the interface is created on the classic NE.

Figure 7-28 NE CLI after deployment



END OF STEPS

# 7.9 LDP

# 7.9.1 LDP protocol

LDP (Label Distribution Protocol) is a protocol used in Multiprotocol Label Switching (MPLS) networks to establish label-switched paths (LSPs).

Configuration must be performed in CLI because there is no intent to enable or configure LDP. The CLI commands below are the minimum required to enable this protocol.

# 7.9.2 Configuring LDP

1	
•	Configure LDP on nodes.
	Classic nodes:
	/configure router ldp
	MD nodes:
	/edit-config private
	/configure router ldp admin-state enable
	/commit
	/admin save
	/exit all
	/quit-config



Check the status of the protocols on all nodes:

/show router ldp status

**Note:** For LDP to be operational, users need to configure the IPv4 and IPv6 bindings manually via CLI. The bindings are not attributes users can select/configure via the intent type.

3

Log in to each router via CLI.

```
4
```

Add the IPv4 and/or IPv6 bindings to the protocol traffic-engineering on OSPF, IS-IS, or both via CLI since it cannot be done through NSP via an ICM pre-defined intent:

#### Classic:

```
/configure router ldp interface-parameters interface "<interface_
name>" ipv4 no shutdown
```

```
/configure router ldp interface-parameters interface "<interface_
name>" ipv6 no shutdown
```

#### MD:

```
/configure router ldp interface-parameters interface "<interface</pre>
name>" ipv4
/configure router ldp interface-parameters interface "<interface</pre>
name>" ipv6
```

5 —

Repeat Step 4 for all interfaces under the LDP context.

Figure 7-29 Ex. Classic





**i** Note: The IPv4 binding should be configured by default even though this attribute is not part of the intent type for classic NEs only.

END OF STEPS

# 7.10 BGP

## 7.10.1 BGP-EVPN

1 -

**i** Note: The following configurations must be done manually on a router before BGP can be configured.

- Log in to the router via CLI.
- 2 Configure the autonomous system parameter on the routers:

Classic:

/configure router autonomous-system <ID>

```
Example: /configure router autonomous-system 65100
```

### MD:

/configure router autonomous-system <ID>

Example: /configure router autonomous-system 65100

3

For classic NEs, the BGP context or instance must be created first. This is not necessary for model-driven NEs.

### Classic:

/configure router bgp

4

Log in to NSP.

5

Import the intent type icm-router-bgp\_group into Device Management, Configuration Intent Types.

6

Navigate to **Device Management**, **Configuration Templates**.

7

Create a configuration template (ex. Router-bgp-group) and associate **icm-router-bgp\_group** intent type. Use the default schema form.

8

Release the BGP group template.

e Management Configuration	Temp	olates *											+ TEMPLATE
		Description		Life Cycle		Target Labels		1	Intent Type	Inf	tent '	:	i Template Details
	Ŧ		T		*		T		T				
er-Interface-unified		1777 S		released		-		ł	icm-router-network-Interface			£.	∧ General
er-mpls-msros				released	•			ŕ	router-mpls-interface_msros			:	News
er-rsvp-Interface		1		released		-		ŕ	router-rsvp-Interface_msros			£.,	Router-bgp-group
er-bgp-group		-		released	•	_		1	icm-router-bgp_group			:	Description
													Life cycle released Target Labels — Intent Type Kcm-outer-bgp_group Intent Type Version 2 Config Form default Config Form State Up-to-date Rele Logical Category Rooter Device Scope SROS Classic & Model Peakle Yes Cented De-15, 2024 11:05:50 am
	÷	(									- F - (	•	Last Indated

Navigate to Device Management, Configuration Deployments.

10

9

Create a logical deployment and select the BGP group template.

11 -

Select the target NE.

For the following example, both 7750 SR-14s classic and MD NEs were selected as deployment targets.

Sele	ect NEs														×
0	Multiple targets selected. Ter	mplate list will not be f	iltered	d based on targe	t produ	ct or type.					🛆 Bin (2 NEs)				EMPTY
	NE Name	NE ID		Management II	Þ	Product			1	:	NE Name		NE ID		:
		r	T		T		T					T		T	
$\checkmark$	Toronto	92.168.96.215		135.249.150.4		7750 SR					Toronto		92.168.96.215		ii.
	Seattle	92.168.96.190		135.249.151		7750 SR					Boston		92.168.96.46		Ĩ
	Core_2	92.168.96.93		135.249.150.5	5	7950 XRS									
	Core_1	92.168.97.250		135.249.151		7950 XRS									
	CE_West	92.168.99.6		135.249.152.1	9	7250 IXR									
	Calgary	92.168.98.97		135.249.151.2	1	7750 SR									
	Boston2	92.168.99.50		135.249.155.6	7	7750 SR									
	Boston	92.168.96.46		135.249.153		7750 SR									
			k	C C Page:	1	/1 >			Count : 8	3				CANCEL	ADD

Deploy Logical Configuration										×
Select Templates *	Select Templates								CLEAR ALL	+ TEMPLATE
Assign Identifier for Selected Template *										Count : 1
	Select Targets and	Edit Selected Templ	ate						CLEAR ALL	+ TARGET
	Select targets. Template	e configurations can be ec	lited after targets are s	elected.		1.			VIEW/EDIT TE	MPLATE CONFIG
	Awarting user input:	View/Edit Template Config to	assign configurations req	uired by tr	ne selected ten	nplates	Deschurt			
	Reachability	NE Name	NE ID	۹ ۳	Management IP	, T	Product	<b>Y</b>		
	• Up	Toronto	92.168.96.215	1	135.249.150.4		7750 SR			
	• Up	Boston	92.168.96.46	1	135.249.153		7750 SR			E.
										Count : 2
	Assign Identifier fo	or Selected Template	1							
	Assign unique identifier	s for templates selected a	bove to identify the co	respond	ding deployme	ents. If	content be	low is disabled, select targets first to enable them.		
	1. Router-bgp-group :									
	BGP-EVPN		×							
									CANCEL S	DEPLOY

#### 12 -

Click on VIEW/EDIT TEMPLATE CONFIG and enter the BGP group parameters that are common to all targets. At minimum, select the family.



**i** Note: For BGP-EVPN, EVPN must be selected.

Router-bgp-group			×
Group	Group		· · · · · · · · · · · · · · · · · · ·
Hold Time (Seconds) Family Remove Private Cluster Local AS	Seconds	Minimum Hold Time (Seconda)	
Import Export Graceful Restart Outbound Route Filtering Extended Community Send ORF	IPv4     Mcast IPv4     MVPN lpv4     Flow lpv4     MVPN IPv6     Mcast IPv6     BGP LS     SR Policy lpv6	VPN IPv4 VPN IPv6 MDT Saft Route Target Ifow IPv6 Label IPv4 Kcast VPN IPv6 Ifow VPN IPv6 Ifow VPN IPv4	<ul> <li>IPv6</li> <li>L2 VPN</li> <li>MS PW</li> <li>Mcast VPN IPv4</li> <li>✓ EVPN</li> <li>Label IPv6</li> <li>SR Policy IPv4</li> <li>Flow VPN IPv5</li> </ul>
	Remove Private Unvited	Skip Peer AS	CANCEL UPDATE

13

Deploy the configurations and verify that all the deployments have been successful.

Dev	ice Management Configu	ration uration D	Deployments •												
2 0	Deployments Selected	DESEL	LECT ALL												:
	Deployment Status		Configuration Status	NE Name		NE ID		Identifier		Template	R	ole	Category	. :	Deployment Details
		•	-		T		T		T	T	r	-			
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Boston2		92.168.99.50		test1		Router-interface-unified	L	ogical	Interface	:	
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		test4		Router-mpls-msros	L	ogical	Router	:	
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		test4		Router-rsvp-interface	L	ogical	Router	:	
	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Boston		92.168.96.46		BGP-EVPN		Router-bgp-group	L	ogical	Router	1	
$\checkmark$	<ul> <li>Deployed Aligned</li> </ul>		<ul> <li>Modified</li> </ul>	Toronto		92.168.96.215		BGP-EVPN		Router-bgp-group	L	ogical	Router	:	
															Multiple deployments selected
													•	<.>	
	Auto-refresh Last R	efresh: 20	024/12/16 11:23:40					< Page: 1 /1 >					Cou	nt : 5	

After deployment:





Figure 7-31 MD NE



14 -

Add the peers to each BGP group instance (and add the corresponding attributes):

- 1. Select the first BGP group deployment and click View/Edit....
- 2. On the Deploy Logical Configuration form, click VIEW/EDIT TEMPLATE CONFIG.
- 3. In the "Neighbor" section, add all neighbors (i.e other PE routers) to that particular group and configure the "peer" as attribute (which should be equal to the autonomous system ID).

+ ADD					hbor
Keepalive (Seco	Connect Retry (Seconds)	Peer Creation Type	Admin State	IP Address	Peer AS
:			enable	92.168.96.215	65100
:			enable	92.168.96.190	65100
$\blacktriangleright \   \bullet \   \circ \   \bullet \   \circ \   \bullet \   \circ \   \bullet \   \circ \   \bullet \ \   \circ \  \  \  \  \  \  \  \  \  \  \  \  \$				▶ ◀	
Total: 2		1 > >	< < Page:		

Figure 7-32 Classic NE

```
A:Toronto>config>router>bgp# info
            group "BGP-EVPN"
                family evpn
                disable-client-reflect
                disable-4byte-asn
                neighbor 92.168.96.46
                    disable-client-reflect
                    disable-4byte-asn
                    peer-as 65100
                    disable-capability-negotiation
                exit
                neighbor 92.168.96.190
                    disable-client-reflect
                    disable-4byte-asn
                    peer-as 65100
                    disable-capability-negotiation
                exit
            exit
            no shutdown
```

```
Figure 7-33 MD NE
```

```
(pr) [/configure router "Base" bgp]
A:admin@Boston# info
    group "BGP-EVPN" {
        admin-state enable
        family {
            evpn true
    neighbor "92.168.96.190" {
        admin-state enable
        group "BGP-EVPN"
        peer-as 65100
        family {
            evpn true
    neighbor "92.168.96.215" {
        admin-state enable
        group "BGP-EVPN"
        peer-as 65100
        family {
            evpn true
    )
(pr) [/configure router "Base" bgp]
```

END OF STEPS

# 7.10.2 BGP-LS

A different router BGP group can be configured with the same **icm-router-bgp\_group** intent type. The following procedure describes this process. The same configuration template **Router-bgp-group** can be used for this configuration deployment.

1

The following attribute can be filled for the **Router-bgp-group** template deployment form for configuring BGP-LS.

NSP

Router-bgp-group							×
Group	Group						
Hold Time (Seconds)	Admin State		Connect Retry (Seconds)		Keepalive (Seconds)		
Family	enable 👻	□x	30		10		
Remove Private			Local Preference		Loop Detect		
Cluster	Damping				off -	Γ×	
Local AS	Min Route Advertisement				Preference		
Import			Aggregator ID Zero				
Export	Multihop		Authentication Key				
Graceful Restart	-		-	0	✓ Client Reflect		
Outbound Route Filtering							
Extended Community	VPN Apply Export		VPN Apply Import		ASN 4 Byte		
Send ORF	Path MTU Discovery						
	Hold Time (Seconds)						
	Seconds		Minimum Hold Time (Seconds)				
	Family						
							_
							_
						CANCEL	UPDATE

Router-bgp-group				×
Group Hold Time (Seconds)	Group			A
Remove Private Cluster Local AS Import Export Graceful Restart Outbound Route Filtering Extended Community Send ORF	<ul> <li>IPv4</li> <li>Mcast IPv4</li> <li>MVPN jpv4</li> <li>Flow ipv4</li> <li>MVPN IPv6</li> <li>Mcast IPv6</li> <li>GEP LS</li> <li>SR Policy Ipv6</li> </ul>	<ul> <li>VPN IPv4</li> <li>VPN IPv6</li> <li>MDT Safi</li> <li>Route Target</li> <li>Flow IPv6</li> <li>Label IPv4</li> <li>Flow VPN IPv6</li> <li>Flow VPN IPv4</li> </ul>	IPV6 L2 VPN MS PW Mcast VPN IPv4 VPN Label IPv6 SR Policy IPv6 Flow VPN IPv6	
	Cluster ID	Skip Peer AS		CANCEL LIEDATE

Deploy Logical Configuration			×
Select Templates *	Select Templates	CLEAR ALL	+ TEMPLATE
Assign identifier for selected template			Count : 1
	Select Targets and Edit Selected Template	CLEAR ALL	+ TARGET
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TE	MPLATE CONFIG
	Configurations required by the selected templates are assigned. View/Edit		
	Reachability NE Name NE ID Management IP Product		
	T T T T T		
	● Up Toronto 92.168.96.215 135.249.150.4 7750 SR		1
			Count : 1
	Assign Identifier for Selected Template		
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.		
	1. Router-bgp-group :		
	GROUP_NAME*		
	BGP-LS X		
		CANCEL S	AVE DEPLOY

NE CLI after successful deployment of BGP-LS group configuration:



NSP

Configuring neighbors in the BGP-LS group can be done through a re-deployment of the same template by adding the neighbor to the deployment form.

Router-bgp-group							×	ĸ
Group	Group   Extended Community  Accept DBF  Send ORF  Neighber + ADC							*
Hold Time (Seconds) Family Remove Private Cluster Local AS								
Import Export								
Graceful Restart Outbound Route Filtering	IP Address	Admin State	Peer Creation Type	Connect Retry (Seconds)	Keepalive (Seconds)	Damping		
Extended Community	92.168.98.97	enable				1		
	4		IC C Page: 1	/1 > >		► ◀ ► Total: 1		
							CANCEL UPDATE	E

NE CLI after addition of neighbor to the "BGP-LS" group through the above deployment:

A:Toronto>config>router>bgp# info						
group "BGP-LS"						
family bgp-ls						
connect-retry 30						
keepalive 10						
loop-detect off						
neighbor 92.168.98.97						
exit						
exit						
group "BGP-EVPN"						
family amon						
ramity evpn						
neighbor 92.168.96.46						
peer-as 65100						
exit						
neighbor 92.168.96.190						
peer-as 65100						
exit						
exit						
no shutdown						

END OF STEPS

# 7.11 Segment Routing

**i** Note: To enable and configure Segment Routing (SR) on the NEs, users need to use CLI as there is no NSP ICM intent type that can provision or configure SR on the NEs in the network. Segment Routing is a prerequisite for creating SR-TE LSPs.

# 7.11.1 Steps

1 -

Log in to the router via CLI.

2 -

Configure the IGP instance (OSPF, IS-IS, or both) to signal the router capability TLVs (advertisements). "Area" should be used for OSPF and "AS" should be used for IS-IS.

#### Classic:

```
/configure router ospf advertise-router-capability area
/configure router isis advertise-router-capability as
MD:
/configure router ospf advertise-router-capability area
/configure router isis advertise-router-capability as
/commit
```

3

Through CLI, define the Segment Routing Global Block (SRGB) to reserve a range of labels to Prefix-SIDs:

**i** Note: In the following example, the range used is [20000, 30000].

**Classic:** 

```
/configure router mpls-labels sr-labels start 20000 end 30000 MD:
```

```
/configure router mpls-labels sr-labels start 20000 end 30000
/commit
```

4

If not already done, enable traffic engineering using CLI. This is also not configurable through the use of the pre-defined intent types.

**i** Note: If RSVP has already been configured on the network, this step can be skipped. **Classic:** 

```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
MD:
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
/commit
```

5

Through CLI, enable Segment Routing in the IGP instance (OSPF, IS-IS, or both). Also define the "start-label" for the "Prefix-SID" range as well as the "index-range". Here, if the user chooses "global" as the value, the "start-label" is equal to the lowest label value in the SRGB and max-index is equal to the range size of the SRGB.

#### Classic:

```
/configure router ospf segment-routing prefix-sid-range global
/configure router ospf segment-routing no shutdown
```

/configure router isis segment-routing prefix-sid-range global /configure router isis segment-routing no shutdown MD: /configure router ospf segment-routing prefix-sid-range global /configure router ospf segment-routing admin-state enable /configure router isis segment-routing prefix-sid-range global /configure router isis segment-routing admin-state enable /commit.

6 —

A node-SID index or label value is normally assigned to the NE's primary address (such as a "system" or "loopback" address). The address must be in the GRT (Global Routing Table). Use CLI to configure the index or label to the interface in the IGP instance (OSPF, IS-IS, or both). If both IGP instances are to be configured, a different label/index value must be used as the same value cannot be used. Each router must have a unique label/index value.

Example: Defined SRGB: [20000, 30000]

### Classic NE (e.g. 'Calgary NE'):

/configure router ospf 0 area 0.0.0.0 interface "system" node-sid label 20000

/configure router isis 0 interface "system" ipv4-node-sid label 20006

#### MD NE (e.g. 'Seattle NE'):

/configure router ospf 0 area 0.0.0.0 interface "system" node-sid label 20005

/configure router isis 0 interface "system" ipv4-node-sid label 20011 /commit

**i** Note: The label/index node-SID value assignment must be different and unique. The chosen value must be a value within the SRGB.

END OF STEPS

#### 7.12 LSP

# 7.12.1 To configure RSVP-TE LSPs and Paths onto the network

Log in to the router via CLI.

2 —

1

Configure traffic-engineering on OSPF, IS-IS, or both via CLI since it cannot be done through NSP via an ICM pre-defined intent:
#### Classic:

```
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
MD:
/configure router ospf traffic-engineering
/configure router isis traffic-engineering
/commit
```

3 -

Log in to NSP.

4

Import the intent type icm-te-tunnel into Device Management, Configuration Intent Types.

Device Management Configuration Configuration Intent Types	•									+ IMPORT
Intent Type	Version		Status	Description		Role	Category	Device Scope	Last Upr 🗄	i Intent Type Details
T		T	-		T	-	-	-	MMM c	
icm-router-network-interface		2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical	Interface	SROS Classic & Model	Dec 10, 🕴	Intent Type icm-te-tunnel
router-mpls-interface_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical	Router	SROS Model	Dec 12, 🕴	Version
router-rsvp-interface_msros_23-10-1_24-4		1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical	Router	SROS Model	Dec 12, 🕴	2
icm-router-bgp_group		2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical	Router	SROS Classic & Model	Dec 16, 🕴	Status
im-te-tunnel		2	• Successful	Intent-Type to configu	F	Logical	LSP	SROS Classic & Model	Dec 24, i	Successful     Successfully imported/re-imported the intent-type      Description     Intent-Type to configure LSP     Rele     Logical     Contegery     LSP     Device Segie     SROS Classic & Model     Imported     Dec 24, 2024 4:10:19 pm     List updated     Dec 24, 2024 4:10:26 pm     Configuration Form     default
4									▶	
Auto-refresh Last Refresh: 2024/12/24 16:10:36				K <	Page:	1 /1 > >>	I		Count : 5	

5 –

Navigate to Device Management, Configuration Templates.

6

Create a configuration template and associate the **icm-te-tunnel** intent type. For example, the configuration template created below is named as **icm-te-tunnel-template**.

lame	Description		Life Cycle		Target Labels		Intent Type		Intent '	(i) Template Details	
	T	T				T		T			
uter-Interface-unified			released	-			icm-router-network-inte	rface		∧ General	
iter-mpls-msros			released		-		router-mpls-interface_m	nsros			
ter-rsvp-Interface			released	•	-		router-rsvp-interface_m	sros		icm-te-tunnel-template	
ter-bgp-group	-		released				icm-router-bgp_group			Description	
-te-tunnel-template	-		released	-	-		icm-te-tunnel			-	
										Life Cycle released	
										Target Labels	
										Target Labels —	
										Target Labels — Intent Type	
										Target Labels — Intent Type icm-te-tunnel	
										Target Labels — Intent Type icrm-te-tunnel Intent Type Version 2	
										Target Labels — Intent Type Icm-te-tunnel Intent Type Version 2 Config Form	
										Target Labels intent Type icm-te-tunnel intent Type Version 2 Config Form default	
										Target Labels — Intent Type Intent Type Version 2 Config Form default Config Form State In the data	
										Target Labels — intent Type Intent Type Varian 2 Config Form default Config Form State Up-to-date	
										Target Labels — Intent Type Intent Type Version 2 Config Form default Config Form State Up-to-date Rele Logical	
										Target Labels — Intent Type Intent Type Varian 2 Config Form State Up-to-date Rele Logical Category	
										Target Labels — Instent Type Instent Type Version 2 Config Form State Up-to-date Role Logical Category LSP	
										Target Labels — Intent Type Intent Type Version 2 Config Form default Config Form State Up to-date Role Logical Category LSP Device Scope SROS Classic & Model	
										Trajet Labels — intent Type Intent Type Version 2 Config Form default Config Form State Up to -date Role Logical Category LSP Drvice Scope SROS Classic & Model Ficible	
										Trapel Labels — intent Type Intent Type Version 2 Config Form default Config Form State Up-to-date Role Logical Chaptory LSP Device Scope SROS Classic & Model Fleaible Yes	

Navigate to Device Management, Configuration Deployments.

8

7 -

Create a logical deployment and select the TE tunnel (LSP) template.

Templates *	Select Templates															CLEAR AL	L + TEI	MPLA
Targets and Edit Selected Template *	The selected temp	late can	not be deployed wi	th other tem	plates													
	Template Name		Description	Targe	rt Labels						Categor	Y	Device S	icope	Flexib	ole		
		T		T						т		-		•				
	icm-te-tunnel-templa	ite	-	-							LSP		SROS CI	assic & Model	Yes			
																	Co	ount :
	Select Targets and	<b>d Edit</b> te conf	Selected Ten	<b>nplate</b> e edited aft	er targets are s	elected	42									CLEAR VIEW/EDI	ALL +	TAR
	Awaiting user input	t: View/I	Edit Template Conf	ig to assign o	configurations req	uired by	, the selected ten	nplate	5									
	Only 1 target can be	e select	ted for the selected	i template														
			NE Name		NE ID		Management IP	(	Product									
	Reachability					*		T		T								
	Reachability	T		T		a.												
	Reachability • Up	T	Boston	Ť	92.168.96.46	1	135.249.153		7750 SR									

Click on **VIEW/EDIT TEMPLATE CONFIG** and enter the LSP and LSP path parameters (source, destination, signaling-type (RSVP vs. SR-TE) path-computation method, primary and secondary paths, hop limits and conditions, etc.).

xplicit Route Objects Always	Name*	Path Computation Method	
ath Metric Bounds	usingCore1_1	path-locally-computed 🗸 🔽 Use Path Computation	
e Bandwidth ath Affinity Names	Explicit Route Objects Always		
	Route Object Include Exclude		+ ADD
	Explicit Route Usage Index		
	route-include-object 2		:
	route-include-object 1		:
			Total: 2
		IX X Page. 1 / 1 / 21	10001.2
	Path Metric Bounds		
	Path Metric Bound		+ ADD

NSP

icm-te-tunnel-template > Create Second	dary Path						×
Restoration	Restoration						
Explicit Route Objects Always			Restoration Scheme				
Path Metric Bounds	Enable		restoration-scheme-presignaled	• Cx			
Te Bandwidth	Name*		Path Computation Method				
Path Affinity Names	usingCore2_1		path-locally-computed	• 🗔 🗹	Use Path Computation		
	Disjointness						
	Select a value	•					
	Explicit Route Object	ts Always				+ ADD	
	Explicit Route Usage	Index					
	route-include-object	2				1	
	Toute-Include-object	- <u>I</u>					
						CA	NCEL ADD

	Source*		Destination*		Color	
	92.168.96.46	×	92.168.96.190	×		
	Description		Admin State			
s	None		Up	• Ex		
	Primary Paths					
	Primary Path					+ ADD
	Name	Path Computation Method	Use Path Computation	Setup Priority	Hold Priority	
		(and facely second and				
	usingcore r_r	pati-locally-computed	uue	1	0	
			I< < Page:	1 /1 > >1		Total: 1
	Secondary Paths					

10 -

Click UPDATE.

NSP

11 -

	uration       Select Templates         ted Template *       Select Targets and Edit Selected Template         Select Targets. Template configurations can be edited after targets.       Select targets. Template configurations can be edited after targets.         © Configurations required by the selected templates are assigned.       Only 1 target can be selected for the selected templates         Reachability       NE Name       NE ID         Up       Boston       92.168.3         Assign Identifier for Selected Templates selected above to identify to       Assign unique identifiers for templates selected above to identify to											
Deploy Logical Configuration											>	
elect Templates *	Select Templates									CLEAR ALL	+ TEMPLATE	*
elect largets and colt selected lemplate "											Count : 1	
	Select Targets an	d Edit Selected Ter	nplate							CLEAR ALL	+ TARGET	ļ,
	Select targets. Templa	ate configurations can b	e edited after targ	ets are selecte	ł.					VIEW/EDIT TEM	IPLATE CONFIG	
	<ul> <li>Configurations red</li> </ul>	quired by the selected temp	lates are assigned.	View/Edit								
	Only 1 target can l	be selected for the selecter	l template									
	Reachability	NE Name	NE ID	)	Management II	Product						
		T	T	T		T	T					
	• Up	Boston	92.1	68.96.46	135.249.153	. 7750 SF	2				Ĩ	
											Count : 1	l
	Assign Identifier	for Selected Temp	ate									
	Assign unique identifi	ers for templates select	ed above to identi	fy the correspo	nding deploym	ents. If conten	t below is disable	d, select targets first to ena	ble them.			
	1. icm-te-tunnel-template :											
	TunnelName*											
	toSeattle_1											Ŧ

#### Give LSP Tunnel a name and click **DEPLOY**.

CANCEL

SAVE DEPLOY

Figure 7-34 NE CLI after deployment

```
A:admin@Boston# configure router mpls lsp "toSeattle l"
(pr) [/configure router "Base" mpls lsp "toSeattle_1"]
A:admin@Boston# info
   admin-state enable
   type p2p-rsvp
   from 92.168.96.46
   to 92.168.96.190
   pce-control true
   pce-report true
   path-computation-method pce
   egress-statistics {
        admin-state enable
   primary "toSeattle_l_usingCorel_l" {
        bandwidth 0
       priority {
            setup-priority 7
            hold-priority 0
    secondary "toSeattle_1_secondary_usingCore2_1" {
       bandwidth 0
        srlg false
        standby false
        priority {
            setup-priority 7
            hold-priority 0
(pr) [/configure router "Base" mpls lsp "toSeattle_1"]
```

END OF STEPS ----

# 7.13 Customers

1

### 7.13.1 To configure customers using service customer intent

Log in to NSP.

NSP

2 -

Import the intent type **icm-service-customer** into **Device Management**, **Configuration Intent Types**.

	Network Services Platform	n												User: admin 🔹 🕜
Device Management	Configuration Configuration Intent Types		•											+ IMPORT
Intent Type			Version		Status	Description		Role		Category		Device Scope	Last Upr	(i) Intent Type Details Refresh
		T		т	•		Т		*		*	×	MMM c	112-01420002000 I
icm-service-customer				2	Successful	Intent-Type to configu	ur	Logical		Service		SROS Classic & Model	Jan 3, 21 🚦	Intent Type icm-service-customer
														Version 2
														Status
														Successful     Successfully imported/re-imported the intent-type
														Description Intent-Type to configure service customer
														Role
														Category
														Device Scope
														SROS Classic & Model
														Imported Jan 3, 2025 11:28:19 am
														Last Updated Jan 3, 2025 11:28:26 am
														Configuration Form
														default
													• • •	
Auto-refresh	Last Refresh: 2025/1/3 11:28:3	88				14	Page	e: 1 /1	> >				Count : 1	

3 -

Navigate to Device Management, Configuration Templates.

4

Create a configuration template and associate the **icm-service-customer** intent type. For example, the configuration template created below is named as **Customer\_Template**.

■ NO <ia network="" service<="" th=""><th>es Platform</th><th></th><th></th><th></th><th></th><th>User: admin 🔹 🕐</th></ia>	es Platform					User: admin 🔹 🕐
Device Management Configuration Configuration Ter	mplates *					+ TEMPLATE C-
Name	Description	Life Cycle	Target Labels	Intent Type	Intent :	i Template Details
T	Ť	-		T	T	∧ General
Customer_Template	-	released 👻		icm-service-customer	I	
						Name Customer_Template
						Description —
						Life Cycle released
						Target Labels —
						Intent Type icm-service-customer
						Intent Type Version 2
						Config Form default
						Config Form State Up-to-date
						Role Logical
						Category Service
						Device Scope SROS Classic & Model
						Flexible Yes
						Created Jan 3, 2025 11:31:57 am
Auto-refresh Last Refresh: 207	25/1/3 11:32:01		< < Page: 1 /1 >	я	•	Last Updated Jan 3, 2025 11:31:57 am

| i |

#### Navigate to Device Management, Configuration Deployments.

**Note:** NSP is always the target for this deployment. While configuring the customer, users can choose to deploy it to one or more sites or leave it to Service Management to configure the customer on the requisite sites when a service is provisioned.

Customer_Template				×
Customer	Customer			A
	Description	Contact	Phone	
	TransCanadian Railways	Ottawa, Canada	+1-0123-4567	
	Sites			+ ADD
	Site Id			
	92.168.96.215			T
				Rows: 1
				CANCEL

Deploy Logical Configuration									×
Select Templates *	Select Templates							CLEAR ALL	+ TEMPLATE
Assign Identifier for Selected Template *	The selected template cannot be deployed with other to	templates							
	Template Name Description Ta	arget Labels			Category	Device Scope	Flexible		
	Т			T	•	-		÷	
	Customer_Template — –	-			Service	SROS Classic & Model	Yes		Î
									Count : 1
	Review target and edit the template configurations.           Image: NSP has been set as target           Configurations required by the selected templates are	assigned. View/Edit						VIEW/EDIT	TEMPLATE CONFIG
	Assign Identifier for Selected Template								
	Assign unique identifiers for templates selected above	e to identify the correspondir	g deployments. If content below i	is disa	abled, select targets	s first to enable them.			
	1. Customer_Template :								
	Customer Name*	Customer Id*							
	IransCanadian Railways X	2	X						
							CA	NCEL S	AVE DEPLOY

	Network Se	ervices Platform											User: admin		•	?
evice Management	Configuration Configuration	n Deployments 🔹											+ DEPLOYME	σ	G	
Deployment S	itatus	Configuration Status	NE Name	NE ID		Identifier		Template		Role		Category :	(i) Deployment Details			
	-	•		Т	T		T		T		-					
Deployed Al	ligned	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0		TransCanadian Railway.		Customer_Template		Logical		Service :	NE Name NSP			
• Deployed A	igned	Modified	ΝSP	0000		TransCanadan Railway,		Customer_Tempiate		Logical		Service :	NSP NE D 0.0.0 Identifier Customer Name TransCanadian Railways Customer Id 2 Deployment Status 0 Deployed Aligned AUDIT ALIGN Last Alignment Jan 3, 2025 11:42:03 am by admin Froeplate Customer_Template Created Jan 3, 2025 11:45:57 am Last Updated Jan 3, 2025 11:42:03 am Last Updated Logical			
4												• • •	Category service			
Auto-refresh	Last Refres	h: 2025/1/3 11:43:58			K	< Page: 1 / 1 >						Count : 1	Configuration Status			
	6	Check th	e NE:													
:Toroi :Toroi	nto>c nto>c	onfig>se onfig>se	ervice>( ervice>(	cust# /c cust# in	onfi fo	gure se	rv	ice cus	to	omer	2					
		descrip	tion "	TransCan va. Cana	adia da"	n Railw	ay	s"								

phone "+1-0123-4567"

END OF STEPS -

# 7.14 Other configurations

### 7.14.1 To configure using icm-system-security-cpm intent type

1

Import the intent type icm-system-security-cpm into Device Management, Configuration Intent Types.

Device Management Configuration Configuration Intent Types		•											+ IMPORT Q
Intent Type		Version		Status	Description		Role		Category		Device Scope	Last Upr 🗄	i Intent Type Details
	T		T	-		T				•	-	MMM c	
icm-service-customer			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical		Service		SROS Classic & Model	Jan 3, 21 🚦	Intent Type icm-system-security_com
icm-system-ptp			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical		PTP		SROS Classic & Model	Jan 6, 21 🚦	Version
icm-system-security_cpm			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical		System		SROS Classic & Model	Jan 6, 21 🚦	2
													Status
													Successful     Successfully imported/re-imported the intent-type     Intent-Type to configure system cpm-filter     Rele     Logical     Cregery     System     Device Scope     SKOS Classic & Model     Imported     Jan 6, 2025 11:59:03 am     Lest Updated     Jan 6, 2025 11:59:10 am     default
4												▶ ∢ >	
Auto-refresh Last Refresh: 2025/1/6 12:15:	13				IC C	Page	E 1 /1 →	>				Count : 3	

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **System\_Security\_Cpm\_ Template**.

Y conservations											
Device Management Configuration	Temp	plates 🔹									+ TEMPLATE C
Name		Description		Life Cycle		Target Labels		Intent Type		Intent'	(j) Template Details
	٣		Ŧ		*		T		T		o General
Customer_Template	_			released	•	-		icm-service-customer		1	A General
System_PTP_Template		-		released	•			icm-system-ptp			Name
System_Security_Cpm_Template				released		-		icm-system-security_cpn	n	1	System_Security_Cpm_Template
											Description
											_
											released
											Target Labels
											-
											Intent Type
											Intent Type Version
											2
											Config Form default
											Up-to-date
											Role
											Logical
											Category System
											Device Scope
											SROS Classic & Model
											Flexible Yes
											Created
(		4								• • •	Jan 6, 2025 12:00:05 pm
Auto-refresh Last Refresh:	2025,	/1/6 12:16:37				IC C Page: 1	1 /1 > >I			Count : 3	Last Updated Jan 6, 2025 12:00:05 pm

Create configuration deployments using the above configuration template.

System_Security_Cpm_Template > Create E	ntry			×
Match	Match			l l
IP Option Source IP	IP Option			
Destination IP	Туре	Mask		
Action				
	Source IP			
	Match Address Choice	Address	Mask 🕲	
	Address And Prefix Or Mask 👻	10.10.10.1	10.10.10.1	
	Destination IP			
	Match Address Choice			
	Select Item 👻			
	Action			
	Action Choice	Drop		
	Case Drop 👻			
				CANCEL ADD

#### Successful deployment:

System_Security_Cpm_Template > Edit Entry	1				×
Match IP Option	Entry ID* 2		Description		*
Source IP Destination IP Action	Match				
	Pretocol igmp ~	□x	Fragment Select Item 🗸	G	l
	☐ IP Option		Mask		l
	Source IP				
	Match Address Choice Select Item	•			
-	Destination IP			CANCEL LIDDA	Ŧ
				CANCEL UPDAT	E

System_Security_Cpm_Template		×
CPM Filter	CPM Filter	
IPv6 Filter CPM Queue	drop	
	IP Filter Admin State enable T	
	Entry	+ ADD
	Entry ID Description	
	2	I
	IC C Page: 1 /1 > >I	Total: 1
		CANCEL UPDATE

Deploy Logical Configuration		×
Select Templates *	Select Templates	
Select Targets and Edit Selected Template *		
Assign Identifier for Selected Template *		
		Count : 1
	Select Targets and Edit Selected Template	
	Challense Territor Complete and a Parl Declaration and de	
	Select targets. lemplate configurations can be edited after targets are selected.	VIEW/EDIT TEMPLATE CONFIG
	Configurations required by the selected templates are assigned. View/Edit	
	Keachability NE Name NE ID Management IP Product	
	Up Toronto 92.168.96.215 135.249.150.4 7750 SR	
		Count : 1
	Assign Identifier for Selected Template	
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.	
	1. System_Security_Cpm_Template :	
	CPM"	
	cpm	
		CANCEL DEPLOY

	eeningaration of	uarus.	Nu Name		NEID		Identiner		Template	n	COLE	Cate	igory :	(i) Deployment Details
				T		Ŧ		T	Т			-		
Deployed Aligned	<ul> <li>Modified</li> </ul>		NSP		0.0.0.0		TransCanadian Railway	3	Customer_Template	L	ogical	Sen	rice I	NE Name Toronto
Deployed Aligned	Modified		Toronto		92.168.96.215		¢pm		System_Security_Cpm	L	ogical	Syst	em i	NE IO 92.1639.6215 Identifier CPH cpm Deployment Status Opployment Status Deployment Status Deployment Status Deployment Status ALIGN Last Audit Template Alignment Jan 6, 2025 12:39:43 pm by admin Template Alignment Jan 6, 2025 12:39:43 pm Status Data Status Last Audit Last A
														system

Figure 7-35 On Classic NE:



Figure 7-36 On MD NE:



END OF STEPS

# 7.14.2 To configure using system-IIdp-msros intent type

1

Import the intent type system-Ildp-msros into Device Management, Configuration Intent Types.

Configuration												
Device Management Configuration Inter	nt Types	•										+ IMPORT Q
Intent Type		Version		Status	Description	Role		Category		Device Scope	Last Up(	: (i) Intent Type Details
	T		T	•		T	•		•	•	MMM c	
icm-service-customer			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		Service		SROS Classic & Model	Jan 3, 2	system-Ildp_msros_23-10-1_23-11
icm-system-ptp			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		PTP		SROS Classic & Model	Jan 6, 2	Version
icm-system-security_cpm			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		System		SROS Classic & Model	Jan 6, 2	1
system-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur	Logical		System		SROS Model	Jan 6, 21	: Status
												<ul> <li>Successful Successfully imported/re-imported the intent-type</li> <li>Description Intent-Type to configure category system and device- configure category system and device- configure category system</li> <li>Rele Logical</li> <li>Cogical</li> <li>System</li> <li>Device Sege</li> <li>SNOS Model</li> <li>Imported</li> <li>Jan 6, 2025 1:01:01 pm</li> <li>Last Updated</li> <li>Jan 6, 2025 1:01:01 pm</li> <li>Configuration Form</li> <li>default</li> </ul>
•												4 <b>&gt;</b>
Auto-refresh Last Refresh: 2025/	/1/6 13:07:18				I< < 1	Page: 1 / 1	> >				Count : 4	1:4

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **Lldp\_md\_Template**.

vanie		Description		Life Cycle	Target Labels		Intent Type	Intent' :	(i) Template Details	
	T		T		•	T		T	-	
ustomer_Template		-		released	• -		icm-service-customer	:	^ Deployments ALL	
stem_PTP_Template				released	• —		icm-system-ptp	:	Configuration Deployments 1	
stem_Security_Cpm_Template				released	•		icm-system-security_cpm	1		
Jp_md_Template		-		released	• —		system-IIdp_msros_23-10-1	:	1 Deployed Aligned	
									AUDIT ALL CONFIG ALIGN CONFIG Last Audit — Last Alignment —	
									∧ General	
									Name Lidp_md_Template Description — Life Cycle released	
									Target Labels	
									Target Labels — Instant Type system-Ildp_msros_23-10-1_23-11 Instant Type Version 1	

Create configuration deployments using the above configuration template.

Lldp_md_Template					×
LLDP	LLDP				
	Admin State		Tx Credit Max	Message Fast Tx (seconds)	
	Enable	▼ □x	10	20	
	Message Fast Tx Init		Tx Interval (seconds)	Tx Hold Multiplier	
	2		30	3	
	Reinit Delay (seconds)		Notification Interval (seconds)		
	2		20		

Deploy Logical Configuration							
Select Templates * Select Targets and Edit Selected Template *	Select Templates						,
Assign Identifier for Selected Template *							Count : 1
	Select Targets and Edit	Selected Template					
	Select targets. Template conf	figurations can be edited afte	r targets are selecter ned. View/Edit	d.			VIEW/EDIT TEMPLATE CONFIG
	Reachability	NE Name	NE ID	Management IP	Product	T	
	• Up	Boston	92.168.96.46	135.249.153	7750 SR		
							Count: 1
	Assign Identifier for Se	elected Template					
	Assign unique identifiers for t	templates selected above to i	dentify the correspo	nding deployments	. If content b	elow is disabled, select targets first to enable them.	
	1. Lidp_md_Template : LLDP* Ildp						
							CANCEL DEPLO

Devi	Device Management Configuration Deployments • • • • • • • • • • • • • • • • • • •									
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	:	(i) Deployment Details
	Deployed Aligned	• Modified	T	T	Trans Canadian Railway	Customer Template	•	Samira		NE Name
	Deployed Aligned	Modified	Toronto	0.0.0.0	rranscanadian Kaliway	Sustem Security Com	Logical	Service		Boston
	Deployed Alighed	Modified	Toronto	92 168 96 215	oto	System_Security_opin	Logical	PTP		NE ID
	Deployed Aligned	Modified	Boston	92 168 96 46	com	System_Project	Logical	System	÷	Identifier
	Deployed Aligned	Modified	Boston	92.168.96.46	lldo	Lido md Template	Logical	System		
								-,		lldp
										Deployment Status
										Deployed Aligned
										AUDIT ALIGN
										Last Audit
										-
										Last Alignment Jan 6, 2025 1:03:58 pm by admin
										Template Name
										Lldp_md_Template
										Created Jan 6, 2025 1:03:56 pm
										Last Updated
										Jan 6, 2025 1:03:58 pm
										Role
										Category
										system
<								<b>F</b> - 1	< →	Configuration Status
	Auto-refresh Last Refresh	2025/1/6 13:10:04			< Page: 1 /1 > >			Count	• 5	<ul> <li>Moamea</li> </ul>
_	cost the rest							coone.		

Figure 7-37 NE CLI after deployment:



END OF STEPS

### 7.14.3 To configure using security-cpu-protection-gsros intent type

1

Import the intent type **security-cpu-protection-gsros** into **Device Management**, **Configuration Intent Types**.

Intent Type		Version		Status	Description		Role	Category	Device Scope	Last Upc 🚦	(i) Intent Type Details
	T		T	•		Ŧ	•		-	MMM c	0
m-service-customer			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical	Service	SROS Classic & Model	Jan 3, 2) 🚦	Intent Type
m-system-ptp			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur.		Logical	PTP	SROS Classic & Model	Jan 6, 21 🚦	Version
m-system-security_cpm			2	<ul> <li>Successful</li> </ul>	Intent-Type to configur.		Logical	System	SROS Classic & Model	Jan 6, 21 🚦	1
stem-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configur		Logical	System	SROS Model	Jan 6, 21 🚦	Status
											Successful     Successful     Successful     Successful     Successful     Successful     Successful     repr     su     Intent-Type to configure CPU Protection     Rels     Logical     Cotegory     System     Device Scepe     SROS Classic & Model     Imported     Jan 6, 2025 1:17:25 pm     Lest Updated     Jan 6, 2025 1:17:32 pm     Configuration Form     default
										$\rightarrow \rightarrow \rightarrow$	

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **System\_Cpu\_Protection\_ Template**.

	1										
me	_	Description		Life Cycle		Target Labels		Intent Type		Intent :	(i) Template Details
	T		T		-		T		T		A Conoral
stomer_Template		-		released	•	-		icm-service-customer		:	General
tem_PTP_Template	_	-		released	•	-		icm-system-ptp		:	Name
tem_Security_Cpm_Template		-		released	•	-		icm-system-security_cpm		1	System_Cpu_Protection_Template
o_md_Template		-		released	*	-		system-lldp_msros_23-10	ŀ1		Description
em_Cpu_Protection_Template		-		released	*	-		security-cpu-protection_g	sros	:	-
											Intent Type
											security-cpu-protection_garos_23-10-1_23-11 Intent Type Version 1 Config Form default Config Form State Up-to-date Rele Logical Cabegory

Create configuration deployments using the above configuration template.

System_Cpu_Protection_Template				×
Policy	Policy			د.
Out Profile Rate Per Source Parameters IP Src Monitoring ETH CFM	Description System Cpu Protection Per Source Rate (packets) 32000	Alarm	Overall Rate (packets) 64000	×
	Out Profile Rate PIR 64400	× Log Events		
	Per Source Parameters			
	IP Src Monitoring			
				CANCEL UPDATE

System_Cpu_Protection_Templa	te	;
Policy	Policy	
Out Profile Rate Per Source Parameters	Per Source Parameters	
IP Sice Monitoring ETH CFM	IP Src Monitoring	
	ETH CFM	+ ADD
	ID PIR	
	23 64000	I,
	I< < Page: 1 /1 > >I	Total: 1

Deploy Logical Configuration			>	×
Select Templates * Select Targets and Edit Selected Template *	Select Templates	CLEAR ALL	+ TEMPLATE	*
Assign Identifier for Selected Template *			Count : 1	Ì
	Select Targets and Edit Selected Template	CLEAR ALL	+ TARGET	
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TE	MPLATE CONFIG	
	Configurations required by the selected templates are assigned. View/Edit			1
	Reachability NE Name NE ID Management IP Product			
	● Up Boston 92.168.96.46 135.249.153 7750 SR			1
				1
			Count : 1	
	Assign Identifier for Selected Template			
	Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.			1
	1. System_Cpu_Protection_Template :			
	23			
		CANCEL S	AVE DEPLO	9Y

Device Management Configuration Deploym	Figuration Status         NE Name           oddfred         NSP           oddfred         Toronto           oddfred         Toronto           oddfred         Boston           oddfred         Boston           oddfred         Boston           oddfred         Boston	NE ID 0.0.00 92.168.94 92.168.94 92.168.94 92.168.94	Identifie           ▼           TransCa           6.215         cpm           6.215         ptp           6.46         cpm           6.46         IIdp           6.46         23	r Templa nadian Railway Custor System System Lido_m System	e Role T Role Security_Cpm Logic PTP_Template Logic Security_Cpm Logic I_Template Logic Cpu_Protectio Logic	Categor Categor Categor Categor System Categor Categor System System Categor System	Y I Deployment N Name Boston NE ID 92.168.96.46 I identifier POLICY-ID 23 Deployment Status Deployed Align	+ DEPLOYMENT () (
Deployment Status     Config       ● Deployed Aligned     ● Mod       ● Deployed Aligned     ● Mod	Figuration Status         NE Name           odified         NSP           odified         Toronto           odified         Boston           odified         Boston           odified         Boston	NE ID 0.0.0.0 92.168.94 92.168.94 92.168.94 92.168.94 92.168.94	Y         Identifie           TransCa         FransCa           6.215         ptp           6.46         cpm           6.46         Idp           6.46         23	r Templa nadian Railway Custor System System Lidg_m System	e Role T Constant Security_Com Cogic Security_Com Cogic Security_Com Cogic Security_Com Cogic Copu_Protectio Cogic	Categor al Service al System al System al System	Y i Deployment Status Deployment Status Deployment Status	ent Details
Deployed Aligned     Mod	odified NSP dodified Toronto odified Toronto odified Boston odified Boston	92.168.94 92.168.94 92.168.94 92.168.94 92.168.94	T           TransCa           6.215         cpm           6.215         ptp           6.46         cpm           6.46         lidp           6.46         23	nadian Railway Custor System System Lidor System	er_Template Logic Security_Cpm Logic (PTP_Template Logic Security_Cpm Logic J_Template Logic (Cpu_Protectio Logic	al Service al System al System al System al System	NR Name Boston NE 10 92158.96.46 identifier 23 Deployment Status • Deployed Align	ned
Obepopy Aligned	odified Toronto odified Toronto odified Boston odified Boston odified Boston	92.168.9 92.168.9 92.168.9 92.168.9 92.168.9	6.215 cpm 6.215 ptp 6.46 cpm 6.46 lldp 6.46 23	System System Lidg_m System	county_Con. Security_Con. PP_Template Logic Security_Com Logic J_Template Logic (Cpu_Protectio Logic	al System al PTP al System al System al System	Boston NE ID 92.158.96.46 1 dettilfer POLICY-ID 23 Deployment Status Deployed Align	ned
Deployment Failed Mod     Deployed Aligned Mod     Deployed Aligned Mod     Deployed Aligned Mod     Deployed Aligned Mod	odified Toronto odified Boston odified Boston odified Boston	92.168.9 92.168.9 92.168.9	2.15 ptp 6.46 cpm 6.46 lldp 6.46 23	System System Lidp_m System	PTP_Template Logic Security_Cpm Logic j_Template Logic (Cpu_Protectio Logic	al PTP al System al System	NE ID 92.168.96.46 i Identifier 23 Deployment Status © Deployed Align	a ned
Ozploved Aligned     Mod     Ozploved Aligned     Mod     Ozploved Aligned     Mod     Ozploved Aligned     Mod	odified Boston odified Boston odified Boston	92.168.9 92.168.9 92.168.9	6.46 cpm 6.46 lldp 6.46 23	System Lidp_m System	Security_Cpm Logic j_Template Logic Cpu_Protectio Logic	al System al System al System	identifier POLICY-ID 23 Deployment Status © Deployed Align	a ned
Opejoyed Aligned Mod     Opejoyed Aligned Mod     Opejoyed Aligned Mod	odified Boston Boston	92.168.90 92.168.90	6.46 Ildp 6.46 23	Lldp_m System	g_Template Logic	al System al System	POLICY-ID     23  Deployment Status  Deployed Align	ned
<ul> <li>Deployed Aligned</li> <li>Mod</li> </ul>	odified Boston	92,168.94	6.46 23	System	Cpu_Protectio Logic	al System	23 Deployment Status • Deployed Align	s ned
							Deployment Status Deployed Align	ned
> 4							AUDIT	ALION k-25 pm by admin btection_Template k-21 pm k-25 pm

Figure 7-38 NE CLI after deployment:



END OF STEPS

### 7.14.4 To configure using icm-system-ptp intent type

1

Import the intent type **icm-system-ptp** into **Device Management**, **Configuration Intent Types**.

evice Management Configuration Configuration Intent Types		•										+ IMPORT
ntent Type		Version		Status	Description		Role		Category	Device Scope	Last Upr 🗄	i Intent Type Details
	T		T	•		T		•	-	•	MMM c	
cm-service-customer			2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical		Service	SROS Classic & Model	Jan 3, 2) 🚦	Intent Type icm-system-ptp
cm-system-ptp			2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical		PTP	SROS Classic & Model	Jan 6, 2) 🚦	Version
rm-system-security_cpm			2	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical		System	SROS Classic & Model	Jan 6, 2i 🚦	2
ystem-lldp_msros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical		System	SROS Model	Jan 6, 2i 🚦	Status
ecurity-cpu-protection_gsros_23-10-1_23-11			1	<ul> <li>Successful</li> </ul>	Intent-Type to configu	r	Logical		System	SROS Classic & Model	Jan 6, 21 🚦	• Summer la
												Successfully imported/re-imported the intent-ty
												Description Intern-Type to configure system ptp Role Logical Category PTP Device Scope SKOS Classic & Model Imported Jan 6, 2025 10:32:00 am Last 06, 2025 10:32:00 am Last 06, 2025 10:32:00 am default
-												

2 -

Create a configuration template in **Device Management**, **Configuration Templates** and set to released state.

For example, the configuration template created below is named as **System\_PTP\_Template**.

■ NO <ia network="" p="" servio<=""></ia>	ices Platform							User: admin 🔹 🕜
Device Management Configuration Configuration Te	emplates -							+ TEMPLATE O
Name	Description	Life Cycle	Ta	rget Labels		Intent Type	Intent' :	(i) Template Details
	T	T	•		T	T		VIEW
Customer_Template	_	released	· -			icm-service-customer	1	^ Deployments ALL
System_PTP_Template	-	released	· -			icm-system-ptp	:	Cauffornation Danlayments
System_Security_Cpm_Template	-	released	• –			icm-system-security_cpm	:	2
Lldp_md_Template		released	· -			system-IIdp_msros_23-10-1	:	• 2 Destand thread
System_Cpu_Protection_Template		released	· ·			security-cpu-protection_gsros	:	<ul> <li>z Deployed Aligned</li> </ul>
								Last Alignment 
								A General
								Name System_PTP_Template Description —
								Life Cycle
								released
								Target Labels
								_
								icm-system-ptp
								Intent Type Version
								2
	× *						• • •	2 Config Form

Create configuration deployments using the above configuration template.

РТР						
Admin State		Announce Receipt Timeout		Log Announce Interval		
disable	•	3		1		
Clock Type		Network Type		Domain		
slave-only	•	sdh	✓ □x	0		
Profile		Priority1		Priority2		
ieee1588-2008	•	128		128		
Port ID Admin State		Address	Local Priority	Log Delay Interval	Log Sync Inter	rva
1/1/c2/1 enable		01:1b:19:00:00:00	128	-6	-6	:
Port ID Admin State           Image: Port ID         Admin State           1/1/c2/1         enable		Address 01:1b:19:00:00:00	Local Priority	Log Delay Interval	Log Sync Inter	rvi
- C						• • •

Deploy Logical Configuration											×
Select Templates *	Select Templates										
Select Targets and Edit Selected Template * Assign Identifier for Selected Template *										c	ount:1
	Select Targets and	l Edit Selected Templ	ate								
	Select targets. Templat	te configurations can be ec	lited af	ter targets are s	electe	d.				VIEW/EDIT TEMPLATE	CONFIG
	Configurations requ	uired by the selected template	s are ass	igned. Viev	w/Edit						
	Only 1 target can be	e selected for the selected ter	nplate								
	Reachability	NE Name		NE ID	_	Management I	P	Product			
	• Up	Toronto	Ť	92.168.96.215	T	135.249.150.4	т f	7750 SR	T		
										c	ount : 1
	Assign Identifier fo	or Selected Template	2								
	Assign unique identifier	rs for templates selected a	bove to	identify the co	rrespo	nding deploym	nents. I	If content b	elow is disabled, select targets first to enable them.		
	1. System_PTP_Template :										
	ptp										
										CANCEL	DEPLOY

=	Notwork Ser	vices Platform							User: admin 👻 🕜
Devic	e Management Configuration Configuration	Deployments •							
2 De	ployments Selected DES	ELECT ALL							1
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	(i) Deployment Details
	-	-	T	r	T T	T	-		
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	NSP	0.0.0.0	TransCanadian Railway	Customer_Template	Logical	Service 1	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	cpm	System_Security_Cpm	Logical	System :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	cpm	System_Security_Cpm	Logical	System I	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	lldp	Lldp_md_Template	Logical	System :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	23	System_Cpu_Protectio	Logical	System :	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Toronto	92.168.96.215	ptp	System_PTP_Template	Logical	PTP I	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	ptp	System_PTP_Template	Logical	PTP E	
									Multiple deployments selected
<									•
	Auto-refresh Last Refresh:	2025/1/7 13:53:20		K	< Page: 1 / 1 >	К		Count : 7	

NSP





Figure 7-40 MD NE CLI after deployment:

```
A:admin@Boston# /configure system ptp
(pr) [/configure system ptp]
A:admin@Boston# info
    admin-state enable
    announce-receipt-timeout 4
    clock-type slave-only
    domain 1
    profile ieee1588-2008
    log-announce-interval 4
    network-type sonet
   priorityl 23
   priority2 34
    tx-while-sync-uncertain true
    port 1/1/c1/3 {
        address 01:80:c2:00:00:0e
(pr) [/configure system ptp]
```

END OF STEPS

# 8 UCC-26: NE Upgrades

## 8.1 Overview

#### 8.1.1 Purpose

This chapter describes the process required to perform and manage NE software upgrades on both classic and model-driven SR nodes.

Testing for this chapter was completed on NSP Release 24.8 GA load and NFM-P Openstack setup.

The NE upgrades for this use case were done using the following nodes:

- 7750 SR-2se dual cpm
- 7250 IXR-R6dl dual cpm

The NE was upgraded from version 23.10 R2 to 24.7 R2 using both classic node (7750) and modeldriven (7250).

### 8.1.2 Artifact bundles

Upgrade artifacts included in the NSP installation are shown below. All default artifacts are certified and cannot be modified.

The following node upgrade artifacts are included with the installation of the networkInfrastructureManagement-basicManagement feature pack:

- nsp-ne-upgrade-with-phases
- nsp-ne-upgrade

The **nsp-ne-upgrade-with-phases** is used for multi-phase of SR OS, SR OS 7210, SR OS 7705, SR Linux.

The **nsp-ne-upgrade** is used for single phase upgrade of SR OS, SR OS 7210, SR OS 7705, SR Linux.

**Note:** Nokia recommends using the **nsp-ne-upgrade-with-phases** operation type to upgrade a 7750 SR.

Phase	Workflow	Process
-------	----------	---------

Pre-check	SR OS 7x50: • LSO_7x50_Pre_Checks • LSO_7x50_Upgrade_ Cleanup_Redundant_CPM • LSO_7x50_Upgrade_ Cleanup_Single_CPM SR OS 7210: • LSO_7210_PreChecks • LSO_7210_Upgrade_	<ul> <li>Checks current software version: if the update is already done, no workflow is called</li> <li>Checks the BOF</li> <li>Checks on CPM redundancy</li> <li>Checks availability of adaptors and supported equipment for md nodes</li> </ul>
	Cleanup_Redundant_CPM <ul> <li>LSO_7210_Upgrade_</li> <li>Cleanup_Single_CPM</li> </ul>	<ul> <li>Checks for deprecated cards and MDAs on the node</li> </ul>
	SR OS 7705: • LSO_7705_PreChecks • LSO_7705_Upgrade_ Cleanup_Redundant_CPM • LSO_7705_Upgrade_ Cleanup_Single_CPM	<ul> <li>Retrieves details of the target software image</li> <li>Runs a cleanup of stale images on the /images/ folder is autoCleanup option is set to True</li> </ul>
	LSO_SRLinux_Pre_Checks	
Download	SR OS 7x50: • LSO_7x50_Download	Reads and processes the BOF
	SR OS 7210: • LSO_7210_Download	<ul> <li>Creates a directory on the NE and transfers the image files</li> </ul>
	SR OS 7705: • LSO_7705_Download	<ul> <li>Confirms the file integrity and sends a success message</li> </ul>
	SR Linux: • LSO_SRLinux_Download	

Activate	SR OS 7x50: • LSO_7x50_Activate • LSO_7x50_Upgrade_ Rollback_ActivatePhase SR OS 7210: • LSO_7210_Activate • LSO_7210_Upgrade_ Rollback_ActivatePhase	<ul> <li>Saves the updated configuration on the NE and performs an admin save</li> <li>Updates the Bof</li> <li>Synchronizes the CPM</li> <li>Resets redundancy settings as needed and sends a success message</li> </ul>
	SR OS 7705: • LSO_7705_Activate • LSO_7705_Upgrade_ Rollback_ActivatePhase	
	SR Linux: • LSO_SRLinux_Activate	
Reboot	SR OS 7x50: • LSO_7x50_Reboot • LSO_7x50_ISSU • LSO_7x50_Upgrade_ Rollback_RebootPhase	<ul> <li>Checks BOF instructions for reboot and CPM redundancy requirements</li> <li>Processes redundancy</li> <li>Triggers a reboot and</li> </ul>
	SR OS 7210: • LSO_7210_Reboot • LSO_7210_ISSU • LSO_7210_Upgrade_ Rollback_RebootPhase	<ul> <li>checks the device version</li> <li>Sends a success message</li> </ul>
	SR OS 7705: • LSO_7705_Reboot • LSO_7705_ISSU • LSO_7705_Upgrade_ Rollback_RebootPhase	
	SR Linux: • LSO_SRLinux_Reboot	

## 8.1.3 Contents

8.1 Overview	389
Preparation	393

8.2 Prerequisites	393
8.3 Pre-upgrade checks	393
8.4 Download and upload NE software	400
Upgrades	404
8.5 Upgrade prerequisites	404
8.6 Backing up the node configs	405
8.7 Multi-phase upgrade: preparing the upgrade	408
8.8 Multi-phase upgrade: performing the upgrade	415
8.9 Single phase upgrade: preparing the upgrade	419
8.10 Single phase upgrade: performing the upgrade	422
8.11 ISSU upgrade	424
Post-upgrade procedures	430
8.12 Rollback	430
8.13 LSO reporting	431
8.14 Post-upgrade checks	434
8.15 Troubleshooting upgrades	436

# Preparation

# 8.2 Prerequisites

### 8.2.1 Network configuration prerequisites

Before NE upgrades can be configured and managed in NSP, the network configuration prerequisites must be met.

Prerequisite	Documentation reference	Notes
Mandatory for NE Upgrades		
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the NSP Installation and Upgrade Guide	<ul><li>Include the following in your deployment:</li><li>Feature packs:</li><li>networkInfrastructureManagement- basicManagement</li></ul>
Device discovery	Pathway for device discovery in the NSP Classic Management User Guide How do I discover devices? in the NSP Device Management Guide Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Check SR OS Software Release Notes	Check the SR OS Software Release Notes for the node type and version you are upgrading to.	—

# 8.3 Pre-upgrade checks

### 8.3.1 Node pre-checks

Users can run some show commands on the routers to compare with the node post-upgrade.

The following is an example of suggested commands users can run on a node before an upgrade. Users can run any additional commands needed. Save the output in a file for comparison post-upgrade.

```
show card
show chassis
show mda
show version
show bof
show service service-using
show service sdp-using
show oam-pm tests
```

```
show system lldp neighbor
show router interface
show router rsvp neighbor
show router ospf neighbor
show system netconf connection
show system grpc connection
show port
show system information
```

Check node version in the Device Management and Network Health dashboard.

Device Management Devices Managed Network Elements											
NE Name	Reachability	Management State	Product	NE Mode	Software Version	Manag :					
T	<b>.</b>	•	T	-		T					
IXRR6D_245	Reachable	-	7250 IXR	MDM	TiMOS-C-23.10.R2	100.12					
N87_20	Reachable	Managed	7750 SR	Classic	TiMOS-C-23.10.R2	100.12					

Network Elements 2 <sup>v</sup>														
Name		Operational State	# Affected Objects		Version	1	System Address		Product		Chassis Type		Manager :	
	T	•		T		T		T		T		T		
N87_20		enabled		7	TiMOS-C-23.10.R2		92.168.96.170		7750 SR		7750 SR-2se		100.127	
IXRR6D_24	5	enabled		3	TiMOS-C-23.10.R2		92.168.96.175		7250 IXR		7250 IXR-R6dl		100.127	

[/] A:admin@IXRR6D\_245# show version TiMOS-C-23.10.R2 cpm/x86hops64 Nokia 7250 IXR Copyright (c) 2000-2023 Nokia. All rights reserved. All use subject to applicable license agreements. Built on Mon Dec 11 23:45:58 UTC 2023 by builder in /builds/2310B/R2/panos/main/sros [/]

A:admin@IXRR6D\_245#

### 8.3.2 NSP pre-configs and checks

See the following for a list of services and checks:

#### **Service Management**

The following is a created L3VPN service through Service Management using intents and an associated brownfield epipe service with an intent.

B:admin@IXRR6D 245# show service service-using

		=====			
Services					
ServiceId	Туре	Adm	Opr	CustomerId	Service Name
10	Epipe	Up	Up	13	Site B - TransCanadian
Exploration*	VPRN	Up	Up	12	L3VPN_Test
Matching Serv	vices : 2				

\* indicates that the corresponding row element may have been truncated.

#### [/]

B:admin@IXRR6D\_245#

= NO <ia netw<="" th=""><th>ork Services Platform</th><th></th><th></th><th></th><th></th><th>User: admin</th><th>×</th><th>0</th></ia>	ork Services Platform					User: admin	×	0
Service Management Servi Servi	ce .					+ CREATE	G	:
Life Cycle State	Alignment State	Composite Service	Service Name	Description	Ser 🗄	(i) Info		
	•	T		T		Select a service		
• Deployed	() Misaligned		EPIPE 10	TransCanadian Exploration Ltd	epi 🚦			
Deployed	Aligned		Site B - TransCanadian Explora	TransCanadian Exploration Ltd	epi 🚦			
<ul> <li>Deployed</li> </ul>	Aligned		L3VPN_Test	Pre upgrade service	vpr 🚦			
	DM FOT ( J TANA)			1 1 1 1 1			Tetal Day	C
Last Kerresh : Uct 31, 2024, 1:07:26	PM EDT (Local Time)		IS S Page:	1 /1 2 21			Iotal Row	r count: 3
Total Service Count : 3 Dep	oloyed : 3							

#### ICM

The following objects were configured through ICM:

- · Classic 7750 Node using device specific intents
  - Logical router interface
  - Logical router mpls interface
  - Logical router rsvp interface
  - Logical ospf interface

MD Node IXR - using md device specific intents, except for router interface which was not supported on IXR

- Logical router interface
- Logical router mpls interface
- Logical ospf interface

Associate to network (Brownfield Discovery)

- Classic Physical port
- MD Physical port

=	NOCIA Network Se	rvices Platform								User: admin 🔹 📀
Devi	e Management Configuration Configuration	Deployments •								+ DEPLOYMENT 🕞 🚆
	Deployment Status	Configuration Status	NE Name	NE ID		Identifier	Template	Role	Category	i Deployment Details
	•	•		T	т	Т	т	•		NE Name
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		toIXR-2	interfaceConfigClassic	Logical	Router	N87_20
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		toIXR-2	classicMPLSInt	Logical	Router	92.168.96.170
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		toIXR-2	classicRSVP-Int	Logical	Router	Identifier
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		toIXR-1	InterfaceConfigClassic	Logical	Router	toIXR-2
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		toIXR-1	classicMPLSInt	Logical	Router	
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		0#0.0.0.0#toIXR-1	classicOSPF_Int	Logical	Router	Deployment Status
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		0#0.0.0.0#toIXR-2	classicOSPF_Int	Logical	Router	Deployed Aligned
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	IXRR6D_245	92.168.96.175		toSR7750-2	unifiedNetworkInterface	Logical	Interface	AUDIT ALIGN
	Deployed Aligned	<ul> <li>Modified</li> </ul>	IXRR6D_245	92.168.96.175		toSR7750-2	mplsInterfaceMD	Logical	Router	Last Audit
	Deployed Aligned	<ul> <li>Modified</li> </ul>	IXRR6D_245	92.168.96.175		0#0.0.0.0#toSR7750-2	MDospfinterface	Logical	Router	Nov 6, 2024 2:49:02 pm by admin
	Deployed Aligned	<ul> <li>Modified</li> </ul>	N87_20	92.168.96.170		Port 2/1/c2/1	physicalPortClassic	Physical	Port	VIEW RESULT
	Deployed Aligned	<ul> <li>Modified</li> </ul>	IXRR6D_245	92.168.96.175		1/2/c2/1	unifiedPhysicalPort	Physical	Port	Last Alignment Oct 24, 2024 4:20:27 pm by admin
										Template Name interfaceConfigClassic
										Created Oct 2, 2024 1-39-33 pm
										Last Updated
										Oct 24, 2024 4:20:27 pm
0	4								•	Role Logical
	Auto-refresh Last Refresh	2024/11/7 15:53:22			14	< Page: 1 /1 >			Count : 12	Category

#### **OAM/Telemetry**

Created Twamp light interface tests on both nodes:

$\leftrightarrow \rightarrow C$ S Not secure	https://135.121.151.243/web/c	lca-managemen	t/oam-test		Q	☆ 📀 💠	ି 🕼 🖸 🗌 📵	Relaunch to updat	te :
🦚 Home - Nokiacentral 🛛 NSP	🗅 Nokia 🗅 Docs 🚊 Regn	ession results	Regression Scheduler	🔀 Eman Al Disi (Nol	kia 🔇 NSP Sar	nity KPI Das OS P	atch Information	» 🗋 All Book	marks
■ NO <ia network="" p="" service<=""></ia>	es Platform						User: admin	Ť	0
Data Collection and Analysis Management	OAM Test Tests							+ TEST O	÷
Filter	Test name	Admin state	Execution status	NE ID	Test type	Execute type	Service ID	:	0
Test type	systemInterfaceTwampLightTe	Enable	Running	92.168.96.170	Twamp-light	Proactive		1	:=
Twamp-light 👻	systemInterfaceTwampLightTe	Enable	Running	92.168.96.175	Twamp-light	Proactive		:	
Name	twampLightInterface_1-1	Enable	Running	92.168.96.170	Twamp-light	Proactive	~	:	
	twampLightInterface_1-2	Enable	Running	92.168.96.175	Twamp-light	Proactive		:	
NE ID									
Execute types									
•									
Service ID									
Test suite									
	4								Þ
RETRIEVE	Last Refresh: 2024-10-31 12:59:32 (Local T	ime)		IC C Page: 1 /	/1 > >			Row Count: 4	

$\leftarrow \rightarrow G$	Not secure https://135.1	121.151.243/web/dca-manager	ment/oam-test-suite/det	ails/individual-results?suiteNa	🔍 🛧 🕺 🔶	B 🗅   🗉	Relaunch to update
🏟 Home - Nokiace	entral 🗀 NSP 🗅 Nokia	🗀 Docs 🙀 Regression results	S Regression Scheduler	🔀 Eman Al Disi (Nokia 🔇	NSP Sanity KPI Das OS Patch	Information »	• 🗋 All Bookmarks
	Network Services Platform					User: admin	• ③
systemInterfaceTw	vampLightTest View Test Suit	te Details					×
AGGREGATED R	ESULTS LIFECYCLE	RESULTS INDIVIDU	AL RESULTS	GENERATION LOG	TESTS		
Test suite execution ID	SET TEST SUITE	EXECUTION ID					
Last 7 days	▼ telemetry:/base/o	pam-pm/twamp-light-delay-streaming	▼ Test suite es	xecution ID			Refresh Results
Test execution ID	Session name	System ID	Result classification	Record stats	Time captured	Direction	Metric ID
45	systemInterfaceTwampLightTe	92.168.96.170	Passed	delay	2024-10-31 13:01:01	Round-trip	fd-average
46	systemInterfaceTwampLightTe	92.168.96.175	Passed	delay	2024-10-31 13:00:59	Round-trip	fd-average
45	systemInterfaceTwampLightTe	92.168.96.170	Passed	delay	2024-10-31 13:00:51	Round-trip	fd-average
46	systemInterfaceTwampLightTe	92.168.96.175	Passed	delay	2024-10-31 13:00:49	Round-trip	fd-average
45	systemInterfaceTwampLightTe	92.168.96.170	Passed	delay	2024-10-31 13:00:41	Round-trip	fd-average
46	systemInterfaceTwampLightTe	92.168.96.175	Passed	delay	2024-10-31 13:00:39	Round-trip	fd-average
4	eustamistarfaarTurmelishtTa	03 459 06 470	- Dasad	dalar	2024 40 24 42:00:24	Darred trip	€4
			I< < Page: 1	/ more > >I			
							CLOSE

$\leftarrow \rightarrow $ G	8 Not secure https://135.	121.151.243/web/dca-manager	ment/oam-test-suite/de	tails/individual-results?suite	eNa 🍳 🛧 🥺 📀	<b>同 口 日</b>	Relaunch to update
🏟 Home - Nokiace	entral 🗅 NSP 🗅 Nokia	🗅 Docs 🚊 Regression results	S Regression Scheduler	💢 Eman Al Disi (Nokia	S NSP Sanity KPI Das OS Pate	h Information X	All Bookmarks
	Network Services Platform					User: admin	• ⑦
twampLightInterfa	ace_1 View Test Suite Details						×
AGGREGATED RE	ESULTS LIFECYCLE	RESULTS INDIVIDU	AL RESULTS	GENERATION LOG	TESTS		
Test suite execution ID	SET TEST SUIT						
20							
Last 7 days	← telemetry:/base/	oam-pm/twamp-light-delay-streaming	<ul> <li>Test suite e</li> <li>26</li> </ul>	xecution ID			Refresh Results
Test execution ID	Session name	System ID	Result classification	Record stats	Time captured	Direction	Metric ID
48	twampLightInterface_1-2	92.168.96.175	😔 Passed	delay	2024-10-31 13:01:58	Round-trip	fd-average
47	twampLightInterface_1-1	92.168.96.170	🕑 Passed	delay	2024-10-31 13:01:52	Round-trip	fd-average
48	twampLightInterface_1-2	92.168.96.175	✓ Passed	delay	2024-10-31 13:01:48	Round-trip	fd-average
47	twampLightInterface_1-1	92.168.96.170	🕑 Passed	delay	2024-10-31 13:01:42	Round-trip	fd-average
48	twampLightInterface_1-2	92.168.96.175	Passed	delay	2024-10-31 13:01:38	Round-trip	fd-average
47	twampLightInterface_1-1	92.168.96.170	✓ Passed	delay	2024-10-31 13:01:32	Round-trip	fd-average
< ×0	kunnalishtetarfana 4.9	03 460 06 475	Decend	dalar.	2024 40 24 42.04.20	Darred Ivia	
			I< < Page: 1	/more > >I			

CLOSE





## 8.4 Download and upload NE software

### 8.4.1 Steps

1

NE software images can be downloaded from the Nokia Support Portal for the NE type and release.

2 -

Specify the image name, the product type, and version for the software image. The md5 checksum for an image is displayed on the Nokia support page where the file was downloaded.

#### 7750 SR (Service Router) > 24.7 > R2 > Nokia-7750\_SR-TiMOS-24.7.R2

When using:	Browserdownload	Please verify the file(s) you have downloaded by generating either an MD5 hash value or an SHA-256 hash value and compare your generated values with the values provided here:
File	Size	Hash Values
Nokia-7750_SR- TiMOS-24.7.R2.zip	2,422,840,510	MD5: 387cc350eb07c53419039357a8f7583a SHA-256: 502c00db5ab3b4eed06040c1cbdd7bfdf603572a20939d745b0f92a61129e6a6

May 2025

Issue 4

#### 3 –

Import the image to NSP:

**i** Note: For 7x50 image import, the software bundle name and contents must not be modified after downloading it from the Nokia support page.

- 1. Open Device Management, Node Images.
- 2. Click Import. The Import Node Software Images form opens.
- Specify the image name, the product type, and the md5 checksum for the software image. The md5 checksum for an image is displayed on the Nokia support page where the file was downloaded.
- 4. Drag and drop the node software image file into the Software Bundle field, or click browse to select the file in a file browser.
- 5. Click Import to upload the node software image to the NSP.

Image Name			_
7750_SR-TiMOS-24.7.R2			- 10
SR OS			•
Checksum (md5sum)			
207CC250EB07C52/10020257A0E7	583A		
Software Bundle Select Software Bundle from directory			
Software Bundle Select Software Bundle from directory File Name			
Software Bundle Select Software Bundle from directory File Name File Name Nokia-7750_SR-TiMOS	S-24.7.R2.zip	Ĩ	
Software Bundle Select Software Bundle from directory File Name File Name Nokia-7750_SR-TiMOS	S-24.7.R2.zip	Ĩ	
Software Bundle Select Software Bundle from directory File Name File Name Nokia-7750_SR-TiMOS	S-24.7.R2.zip	1	

Images can be viewed from **Node Images**, with the content displayed in the info panel on the right.

4

	etwork Services Platform				User: admin 🔹 🕥
Device Management No	eration ode Images	÷			+ IMPORT
MAG-c Appliance	SR OS				¢
SR Linux	Name =	Platform	Software Version	Validation	i (i) Info
	T	T	T	•	2024/10/04 13:36:54
SR OS	Nokia-7750_SR-TiMOS	7750-SR, 7950-XRS, 7	TiMOS-24.7.R2	Yes	End Time 2024/10/04 13:37:14
SR OS 7210	Nokia-7250_IXR-TiMO	7750-SR, 7950-XRS, 7	TiMOS-23.10.R6	Yes	Package Nokia, 7750, SP_TMOS_24,7,P2 zin
SR OS 7705 Wavence					Additional Infe Image files processed successfully Filepath /isom/neSoftware/Nokia/7x50/TIMOS-24.7.R2/
					▲ File Name kernel. tim isa-aa tim com. tim signatures-isa-aa.txt both.tim signatures.txt support.tim boot.ldr hypervisors. tim
	Auto-refresh	Last Refresh: 2024/11/14 15:12:36		Row Co	yang.tim
	Failure 0 Validated 2				

5 —

Images can also be viewed from the File Server application.

File Server										Q () 🏟
Root Directory List	+	lsom > neSoftware > Nokia	> 7x50 > TiMOS	-24.7	R2			+	+	(i) Info
		Directory/File Name	File Type		Creation Time	Last Modified Time	Last Access Time		:	4
som Isom	÷	τ		T	DD/MM/YYY = DD/MM/YYY 🖬	DD/MM/YYY - DD/MM/YYY 🖬	DD/MM/YY1 - DD/MM/YY1 🖬			Select Directory or File
nokia	:	🖺 signatures.txt	txt		2024/10/04 13:37:11	2024/10/04 13:37:11	2024/11/10 19:10:35		:	
	·	liom.tim	tim		2024/10/04 13:37:11	2024/10/04 13:37:11	2024/11/10 19:10:32		:	
		🖺 signatures-isa-aa.txt	txt		2024/10/04 13:37:07	2024/10/04 13:37:07	2024/11/10 19:10:35		:	
		🖺 both.tim	tim		2024/10/04 13:37:07	2024/10/04 13:37:07	2024/11/11 19:10:24		:	
		🖺 isa-aa.tim	tim		2024/10/04 13:37:06	2024/10/04 13:37:06	2024/11/10 19:10:33		:	
		🖹 yang.tim	tim		2024/10/04 13:37:06	2024/10/04 13:37:06	2024/11/10 19:10:40		:	
		🖹 kernel.tim	tim		2024/10/04 13:37:06	2024/10/04 13:37:06	2024/11/10 19:10:34		:	
		hypervisors.tim	tim		2024/10/04 13:37:05	2024/10/04 13:37:05	2024/11/10 19:10:31		:	
		Support.tim	tim		2024/10/04 13:37:02	2024/10/04 13:37:02	2024/11/11 19:10:35		:	
		🖹 boot.ldr	ldr		2024/10/04 13:36:57	2024/10/04 13:36:57	2024/11/10 19:10:24		:	
		E cpm.tim	tim		2024/10/04 13:36:57	2024/10/04 13:36:57	2024/11/10 19:10:29		:	
					IC C Page: 1 / 1	> >1		Row Co	unt: 11	

# Upgrades

## 8.5 Upgrade prerequisites

## 8.5.1 For classic nodes upgrade

Complete the following prior to running a classic node upgrade:

• Verify that the classic mediation policy is correctly set in NSP.

Modification of a cla	assic policy can take a few seconds.			
Edit Mediation Policy				
General	Classic CLI			
Classic SNMP Classic CLI Classic FTP	Communication Protocol SSH2 User	• G		
	admin Pre Login User Name Cli	CHANGE USER PASSWORD		
	Timeout 30000	Idle Timeout (seconds) 3600	Port 22	
	Classic FTP			
	File Transfer Type SFTP	* Cx		
	Connect Timeout (seconds)	Read Timeout (seconds) 50		
				CANCEL UPDATE

## 8.5.2 For MD nodes upgrade

Complete the following prior to running an MD node upgrade:

- 1. Install adaptors for the new node version; Pre-check will fail if adaptors are not installed. See "How do I install adaptor artifacts that are not supported in the Artifacts view?" in the *NSP System Administrator Guide* for more information.
- 2. Configure FTP policy:

An FTP mediation policy must be assigned to the NE before you can perform a backup. FTP mediation policies are created and assigned using a REST API. See the Device Management tutorials on the Network Developer Portal.

### 8.5.3 Additional requirements

The following additional general requirements apply to all upgrades:

- Make sure there is enough space on the node for the upgrade.
- Do not delete NE software images from the NSP during an upgrade operation.

Issue 4

- Both primary and secondary images should be stored on the same flash drive number (for example, cf3 or cf1).
- bof.cfg should be stored on the same cf where the primary image is stored.
- Backout files are stored locally on the NE, and are required if an upgrade fails.
- Pre-check removes images not referenced in the BOF configuration. If insufficient space is freed up, the upgrade cannot proceed.
- Tertiary images are not supported.

An upgrade operation can fail if a workflow task times out; for example, fetching upgrade status or validating downloads and CPM synchronization. You may need to customize the upgrade workflow for your network; see the *NSP Network Automation Guide* for information about modifying workflows.

## 8.5.4 ISSU upgrade path limitations

Before performing an upgrade operation, consult the NE documentation to confirm that the upgrade you need to perform is supported on that NE. For example, a 7750 NE only supports upgrades to releases one or two major releases later than the current release: from Release 21.x to Release 22.x or 23.x, but not to Release 24.x or later.

Nokia recommends using the **nsp-ne-upgrade-with-phases** operation type to upgrade all nodes that support upgrade with phases. When you create an operation with this operation type and NE type, the parameter values are provided as input for the upgrade workflow. NSP monitors the status of workflow executions.

**i** Note: Scale limits apply for number of concurrent executions and number of targets per operation; see Scale limits for large-scale operations in the *NSP Planning Guide*.

## 8.6 Backing up the node configs



Note: Perform this step prior to the upgrade.

### 8.6.1 To backup configs:

1 -

Log in to the NSP.

2 -

Open Device Management, All Operations.

3 \_\_\_\_\_

Select Create an Operation.

4 —

Select the right backup for your nodes: i.e. "nsp-ne-backup" for SR OS, SR OS 7210, SR.

**i** Note: An NDX file is required to perform a backup on nodes configured in classic or mixed mode. The backup operation fails if an NDX file with the same name as the configuration file defined in the bof file is not present in the same folder. You can configure a backup to include debug files located on the same cf as the configuration file.

NO <ia network="" platform<="" services="" th=""><th></th><th></th><th></th><th></th><th>User: admin + 🕥</th></ia>					User: admin + 🕥
Create Operation					×
Select an Operation Type	1.5	elect an Operation Type			+ OPERATION TYPE
General					
Select Targets	Select an Oper	ration Type			×
Operation Inputs	Category	Name	Description	Tags	
View/Edit Schedule	T	T	т	Ť	
	upgrade	nsp-magc-appl-upgrade-phases	Operation for Multi-Ph	LSO, MAGCa2	
	backup	nsp-ne-backup	Operation for NE Backup	LSO, Backup, SR OS, SR OS 7210, SR	
	other	nsp-ne-backup-audit	Operation for NE Back	LSO, All	
	upgrade	nsp-ne-upgrade-eth-sat	Operation for Ethernet	LSO, Upgrade, SR OS 7210	
	backup	nsp-ne-wavence-backup	Operation for Wavenc	LSO, Wavence	+ TARGETS
	other	nsp-ne-wavence-file-retrieval	Operation for Wavenc	LSO, Wavence	
	other	nsp-ne-wavence-password-upd	Operation for Wavenc	LSO, Wavence	
	upgrade	nsp-ne-wavence-upgrade	Operation for Wavenc	LSO, Wavence	
	other	nsp-wavence-service-migration	Operation for Wavenc	LSO, Wavence	
	upgrade	nsp-ne-upgrade-all-normal	nsp-ne-upgrade-all-no	LSO, SR OS, SR Linux	
	upgrade	nsp-ne-upgrade-with-phases	Operation for Multi-Ph	LSO, Upgrade, SR OS, SR OS 7210, S	
				Row Co	unt: 11
				CANCEL	
	5. V	/iew/Edit Schedule			
					Create Another CANCEL SAVE RUN

5

Select + TARGETS and select either NEs or Predefined NE groups.

6

Select all options required.

Under View/Edit Schedule, select either "Run immediately" or "Setup up the schedule".

Create Operation										×
Select an Operation Type	1. Select an Operation	туре								REPLACE
General	Operation Type		Description		Cat	igery		Tags		
Devict largets Operation inputs	nsp-ne-backup (Default)		Operation for NE Ba	kup	bac	(cup		LSO, Backup, SR OS, SR OS 7210, SR OS 7705, SR Linux, Cisco, MAG-c Appliance		
Vew/tot schedule	2. General									
	Operation Name*		Description							
	badrup									
	3. Select Targets								CLEAR	+ TARGETS
	Status	NE Name	NE ID	Management 19	Product	Chassis	Software Version			
	Rescheble	0XRR6D_245	92.168.95.175	100.127.87.245	7250 0KR	7250 IXR-R6d	TIM05-C-23.10.R1			
							< Page 1 21 ->			Row Count: 1
	4. Operation Inputs									
	Debug Fileneme ()	Backup Certificates	Beckup Roll	ack Firs 0	Endage T.S. Files					
		ns	* no	٠	no	•				- 1
	~ Advanced Inputs									
	5. View/Edit Schedule									
	Beckup									
	Single phase backup									
	<ul> <li>Set up the schedule</li> </ul>									
								E	Create Another CANCEL	NE RUN

7 -

You can view the backup status from Device Management, All Operations.

	All Upe	erations	•																+ OPERATIO	N C
ation Name	5	Status	Completion Success	,	waiting Action	Operation T	pe	Category	Operation Control	Scheduled	Scheduled Phase	4	Start Time	Last Modified Time =	Duration	Repeats	1	τ.	0	4
	Ŧ			T		backup	× 1					т	ралим/уу - ралимлуу 🗖	DD/MM/Yr + DD/MM/Yr 🖬				Operation Progr	155	
_backup_lat		Completed	1/1			nsp-ne-bad	up	badtup	Per phase	-		٥	2024/10/31 16:12:30	2024/11/01 10:05:30	17h 53m 332ms	None	3			
_backup_lat		Completed	1/1			nsp-ne-badi	up	backup	Per phase	22		0	2024/10/31 16:11:52	2024/11/01 10:03:53	17h 52m 1s 78ms	None		Total NEs		
																		e 1 Success	ed executions for r	nore deta
																		=		

8 -

Backup files can be viewed from **Device Management**, **Managed Network Elements**. Click on the NE and then select **Review backups**, **View all backup files**.

NSP

Parchability	Muchaniment State	NE Mode	Management ID		NE ID	Broduct		Oracia		Coffware Marriso		Report Status	Die	rounted Du		Domaio Controllor			0	B	
 T	riangement State	in room	rangement o	Ŧ	T T	Freedoct	Ŧ	Cinada	*	Joint Contract	+	nasjin Status	0.4		Ŧ	Contrain Contraine	<b>T</b>			60	
Reachable	-	MDM	100.127.87.245		92.165.96.175	7250 IXR		7250 IXR-R6d		TM05-C-24.7.82		done	five	e nodes		-		^ Summa	ry .		
• Reachable	Managed	Classic	100.127.87.144		92.168.96.160	7250 IXR		7250 (XR-R5		TM05-8-23.10.R6		done	clas	ssic-disc-rule-1		-		I NE Norre			
Reschable	Managed	Classic	100.127.87.20		92.168.96.170	7750 SR		7750 5R-2se		TM05-0-24.7.82		done	clas	issic-disc-rule-1		-		I Hanagemen	e IP		
																	Open NE Inventory	NE ID			
																	Operation	NE Type	170		
																	Review backups	y SR-7750-1	dassic n history		
																	Create an operation	* View all bac	iup files		
																	Manage	, TIMOS-C-	24.7.R2		
																		Product 7750 SH Charlos 7750 SH-2 Version 242-750 SH-2 Version 242-750 SH Responder 23274 Managener Manage	es Banyon OS OP 50:03 (H Silon fera) A Sinte re	89 (Local time	and the second se

END OF STEPS

## 8.7 Multi-phase upgrade: preparing the upgrade

### 8.7.1 Steps

The following example shows a 7250 IXR model-driven node multi-phase upgrade from 23.10 to 24.7 R2.

1 -

Node upgrade can be created from two different locations: **Device Management, All Operations** or **Device Management, Node Images**. Navigate to either location to begin this procedure.

2

If you navigated to **All Operations**, select **Operation**, **Operation Type** and choose "nsp-ne-upgrade-with-phases" from the list.

1 Select a	on Operation Type			
Select an Opera	ition Type			×
Category	Name	Description	Tags	
T	T	T	Ť	
upgrade	nsp-magc-appl-upgrade-phases	Operation for Multi-Ph	LSO, MAGCa2	
backup	nsp-ne-backup	Operation for NE Backup	LSO, Backup, SR OS, SR OS 7210, SR	
other	nsp-ne-backup-audit	Operation for NE Back	LSO, All	
upgrade	nsp-ne-upgrade-eth-sat	Operation for Ethernet	LSO, Upgrade, SR OS 7210	
backup	nsp-ne-wavence-backup	Operation for Wavence	LSO, Wavence	
other	nsp-ne-wavence-file-retrieval	Operation for Wavence	LSO, Wavence	
other	nsp-ne-wavence-password-upd	Operation for Wavence	LSO, Wavence	
upgrade	nsp-ne-wavence-upgrade	Operation for Wavence	LSO, Wavence	
other	nsp-wavence-service-migration	Operation for Wavence	LSO, Wavence	
upgrade	nsp-ne-upgrade-all-normal	nsp-ne-upgrade-all-no	LSO, SR OS, SR Linux	
upgrade	nsp-ne-upgrade-with-phases	Operation for Multi-Ph	LSO, Upgrade, SR OS, SR OS 7210, S	
				Row Count: 1

3 -

If you navigated to **Node Images**, locate the **SR OS** tab and click **‡**, **Upgrade...** 

Device Management No	peration ode Images	•					+ IMPORT
MAG-c Appliance	SR OS						C-
SR Linux	Name =	Platform	Software Version	Validation		:	(i) Info
	T	T	T		•		
SR OS	Nokia-7750_SR-TiMOS	7750-SR, 7950-XRS, 7	TIMOS-24.7.R2	Yes		:	Start Time 2024/10/04 13:36:54
SR OS 7210	Nokia-7250_IXR-TiMO	7750-SR, 7950-XRS, 7	TiMOS-23.10.R6	Yes		Upgrade	End Time 2024/10/04 13:37:14
						Open in Workflows	Package Nokia-7750 SR-TiMOS-24.7.R2.zip
SR OS 7705						Derete	Additional Info
Wavence							Image files processed successfully Filepath
							/lsom/neSoftware/Nokia/7x50/TiMOS-24.7.R2/
							✓ File Name
	Auto-refresh	Last Refresh: 2024/11/14 15:03:57				Row Count: 2	
	Failure 0 Validated 2						

Select Operation, Operation Type and choose "nsp-ne-upgrade-with-phases" from the list.

Create Operation	Select an O	Operat	ion Type						×		
Select an Operation Type	Category		Name	Description	Tags					+ 0	PERATION TYPE
General		T	T	T			T				
Select Targets	upgrade		nsp-ne-upgrade	Operation for Upgrade	LSO	, Upgrade, SR OS, SR OS 72	10, S				
Operation Inputs	upgrade		nsp-ne-upgrade-with-phases	Operation for Multi-Ph	LSO	, Upgrade, SR OS, SR OS 72	10, S				
View/Edit Schedule											
											+ TARGETS
									Row Count: 2		
								CANCEL	ADD		
										Create Another CANCEL S	AVE RUN

4

Select Target family product and all other options:

Operation Control: When upgrading multiple NEs at the same time, users can select "Per Phase" if targets (nodes) proceed as a group - which means all nodes must complete the current phase before proceeding to the next - OR "Per target" target and proceed to the next phase immediately regardless if the other targets are complete or not.

Rollback Type: Applicable for phases that support rollback - Activate and Reboot.

Operation Name*	Description	Targeted Product Family* 👔
Insertion Control		
	Manual	
Per target - targets proceed as a group	O Automatic	
5		
5Select + TARGE	ETS, NEs or Predefined NE groups	- + TAR
5 Select + TARGE	ETS, NEs or Predefined NE groups	+ TAR
5 Select + TARGE	ETS, NEs or Predefined NE groups	+ TAR NEs Predefined NE groups

#### 6

Select Operation Inputs:

Target Software Version: Select the version of the image from the list; the images that show in the drop down are the ones imported to Node Images.

Is ISSU: Defaulted to False, set to True only for nodes that support ISSU. Check the "SR OS Software Release Notes" documentation for the node chassis types that support ISSU.

Auto Cleanup: Defaulted to True. When set to True, it will auto-delete all images in the images directory that are not referenced in the bof.

Free Space Post Upgrade: The expected free disk space % after upgrade, and only used when autoCleanup is set to True.

4. Operation Inputs						
Target Software Version*	Is I S S U* 🚺	Auto Cleanup* 🕕		Free Space Post Upgrade* (Enter a Number)	0	
Sel Target software version of node for	False	True	•	10		
the target product family chosen						
the software itself needs to be						
imported first in Node Images						

7

Users can select any of these optional Advanced Inputs for each of the phases:

Advanced Inputs			
heck to enable options			
Window Size 🌘	🗌 Failure Threshold (%) 🌘		
Pre-Checks			
Pre-Checks for NE upgrade			
Concurrency Count	🗌 Phase Timeout (minutes) 🚯	Average Execution Threshold (minutes)	
- 20 +			
Download Software image download to N	E		
Concurrency Count	Phase Timeout (minutes) 🕕	Average Execution Threshold (minutes)	
- 20 +			
1. el e.			
Activate	IF		
Concurrency Count	Phase Timeout (minutes)	Average Execution Threshold (minutes)	
- 20 +			
Reboot			
Reboot NE or perform CPM swi	tchover to complete upgrade		
Concurrency Count	Phase Timeout (minutes) 🚯	Average Execution Threshold (minutes)	
- 20 +			

Configure the Advanced Inputs as needed:

Parameter	Description
Window Size Failure Threshold	These two parameters work together to define an automatic stopping point for the operation due to failed workflow executions:
	<ul> <li>Window size specifies the sample size to use when calculating whether a threshold has been crossed.</li> </ul>
	• Failure threshold specifies the percentage of executions failed that will trigger the automatic stop.
	For example, with a window size of 200 and a failure threshold of 50%, the operation will automatically stop after 100 failed executions. The phase and operation are paused and any not-started executions remain in not-started status.
The following parameters can be configured s pre-checks, software download, software activ	eparately for each phase of the operation: vation, and NE reboot or CMP switchover.
<ul> <li>Concurrency Count</li> <li>Phase Timeout (minutes)</li> <li>Average Execution Threshold (minutes)</li> </ul>	These parameters specify how the workflow executions will be managed. The pre-check steps themselves are defined in the applicable workflow.
	Concurrency Count: maximum number of executions to run concurrently.
	Phase Timeout and Average Execution Threshold: if these parameters are configured, the operation automatically stops after the specified time. The phase and operation are paused and any not-started executions remain in not-started status.

8

View/Edit Schedule:

If the user selected Operational Control - "Per phase" in Step 3, the phases will only have the option to run manually.

View/Edit Schedule				
Pre-Checks				
Pre-Checks for NE upgrade				
Run immediately				
Download				
Software image download to NE				
Run manually				
Activate				
Software image activation on NE				
Run manually				
Reboot				
Reboot NE or perform CPM switchover to complete upgrade				
Run manually				

If the user selected Operation Control - "Per target" in Step 3, they can select to run each phase manually, immediately, or after a delay (min).

5. View/Edit Schedule
Pre-Checks
Pre-Checks for NE upgrade
Run manually
Download
Software image download to NE
R Bin manually
Ruinmadata/
Run after a delay (min)
Activate
Software Image activation on NE
Run manually
O Run Immediately
Run after a delay (min)
nectori i
Report N2 or perform CFM surchover to complete upgrade
Run manually
O Run immediately
() Run atter a delay (min)

9

After selecting all the options for an upgrade, users can Run or Save. A saved operation can be viewed from **Device Management**, **All Operations** with Saved status. Users can start operation at any time.

ice Management	Operation All Operations														+ OPERATION	0
eration Name	Status	Completion Success		Awaiting Action	Operation Type	Category		Operation Control	Scheduled	Scheduled Phases		Start Time	Last (	₹,	0	4
	T	-	т	•	т		*	•			т	DD/MM/YYY - DD/MM/YYY 🖬	DD	Operation Progress		
ved_operation	• Saved	-			nsp-ne-upgrade-with	upgrade		Per phase	-		2	2024/11/13 12:01:49	2024			
_Upgrade_reporting	Paused	-		-	nsp-ne-upgrade-with	upgrade		Per phase	-		0	2024/11/12 09:10:53	Run	1 1		
50_backup_lat	Completed	1/1			nsp-ne-backup	backup		Per phase	-		0	2024/10/31 16:12:30	Edit	1 Pre-Checks		
50_backup_lat	Completed	1/1			nsp-ne-backup	backup		Per phase	-		0	2024/10/31 16:11:52	Delete	immediate		
VormalUpgrade	Paused	-		-	nsp-ne-upgrade-all-no	upgrade		Per phase	-	0	5	2024/10/28 08:55:02	2024 1	ninfo:-		
														2. Download Manual Phase not started     1 Info :		

END OF STEPS

## 8.8 Multi-phase upgrade: performing the upgrade

### 8.8.1 Encountering failures

In the event of a failure at any phase in the upgrade process, troubleshoot and complete the necessary tasks based on the failure message, then re-run the phase. To re-run the phase, click and select **Rerun**.

### 8.8.2 Phase 1: Pre-check

In the Pre-check phase, the node is assessed to verify it is prepared and ready for upgrade.



**Note:** Pre-check will fail if Cleanup is set to True and there is not enough space on the node. Users can manually delete old files on the node and rerun the phase.

Device Management	> Operation XR_Upgrade_24_7_R2	Execu	itions												0- i
Manual start "D	ownload" phase to proceed w	ith the op	eration												(i) Execution Summary
• 1. Pre-Checks	0 2. Download 🚦 0 3.	Activate	O 4. Reboot												2025/03/31 19:57:34
Status	NE Name		NE ID		Product		Current Software		Target Software		Upgrade State		Magu In	:	Duration 3m 19s 22ms
	•	T		T		T		T		T		Ŧ			Workflow
Success	IXRR6D_245		92.168.96.175		7250 IXR		TIMOS-C-23.10.R2		TiMOS-24.7.R2		PreChecks Complete		N/A	:	LSO_7x50_Pre_Checks
															Total Rerun N/A
															Additional Info
															PreChecks Complete
															∧ Execution Progress
															✓ Initial Run: ReadBof
															✓ Initial Run: CheckTargetImageOnNSP
															Initial Run: CheckPrimaryImageValidity
															✓ Initial Run: CheckAdaptorsCompatibility
															Initial Run: CheckDeprecatedCards
															Initial Run: CleanUpDiskSpaceRedundantCPM
•							-						Þ	$\leftrightarrow$	✓ Initial Run: preChecksSuccess
Auto-refresh	Last Refresh: 2025/3/31	20:07:26			I< < Page: 1	/1	$\rightarrow$ $\rightarrow$ 1						Row Cor	unt : 1	
Failed 0 In Progres	ss 0 Not Started 0 Si	ccessful 1													

## 8.8.3 Phase 2: Download

After Pre-check passes, click "Start download".

In the download phase, the image is downloaded from NSP to the node cf images directory. If the image is already downloaded, it will run the checks and let the user know that the image is already downloaded.

The files will be transferred as shown below if they are not already on the node.

**i** Note: Download can fail for many reasons, such as if there is not enough space on the node and the Auto cleanup was set to False. If this occurs, users can free up space manually and re-run the phase.

Device Management	t > D	Operation XR_Upgrade_24_7_R2	Execu	itions												с :
Manual star	Manual start *Activate* phase to proceed with the operation										(i) Execution Summary					
• 1. Pre-Checks	• 2. D	ownload O 3. Activat	te 🕴	O 4. Reboot												∧ General
Status		NE Name		NE ID		Product		Current Software Version		Target Software Version		Upgrade State		Magu In	:	
	•		T		T		T		T		T		T			Start Time 2025/03/31 20:10:48
Success		IXRR6D_245		92.168.96.175		7250 IXR		TiMOS-C-23.10.R2		TiMOS-24.7.R2		Download Complete		N/A	:	End Time
																2025/03/31 20:17:52
																Duration
																Workflow
																LSO_7x50_Download
																Total Rerun
																Additional Info
																Download Complete
																. Franking Branner
																Execution Progress
																Initial Run: ReadBof
																Initial Run: CheckTargetImageOnNSP
																✓ Initial Run: TransferImageFiles
(							_	-						+	$\leftrightarrow$	Initial Run: imageDownloadSuccess
Auto-refre	esh	Last Refresh: 2025/3/31 20	0:24:22			I< < Page:	1 /1							Row Co	unt : 1	
Failed 0 In Pro	ogress O	Not Started 0 Suc	cessful 1													

## 8.8.4 Phase 3: Activate

After Download is successful, users can start the Activate phase.

In the activate phase, the boot image will be copied to cf3, and update bof primary image and bootenv synch command will run on the node (admin redundancy synchronize boot-env).



**Note:** The Activate phase will fail if any of the previous phases fail.

Device Management > Cperatian IXR_Upgrade_24_7_R2 Executions	Q :
Manual start "Reboot" phase to proceed with the operation	(i) Execution Summary
1. Pre-Checka     2. Download     0.1. Activates     0.4. Reboot	∧ General
Status NE Name NE ID Product Current Software Target Software Upgrade State Magu In :	
- T T T T T T T	Start Time
Success IX.RR60_245 92.168.96.175 7250 IX.R TIMOS-C-23.10.R2 TIMOS-24.7.R2 Activation Complete 01,Fa :	2025/03/31 20:25:12
	End Time 2025/03/31 20:34:17
	Duration
	9m 5s 421ms
	Workflow
	Tetal Perus
	N/A
	Additional Info
	Activation Complete
	∧ Execution Progress
	Initial Run: readBofForActivation
	✓ Initial Run: setBofConfig
	✓ Initial Run: softwareActivationSuccess
Auto-refresh     Last Refresh: 2025/7/31 210734     IC ( Page: 1 / 1 ) )     Rev Count: 1	
Failed 0 In Progress 0 Not Started 0 Successful 1	

## 8.8.5 Phase 4: Reboot

After the Activate phase is successful, users can begin the Reboot phase.

In the reboot phase, the node will either be rebooted or ISSU switchover. When the upgrade is complete, the NE reboots and raises a reboot alarm. The reboot alarm triggers an NE-specific discovery scan. When the discovery scan detects a version change, the NE information is updated.

Device Management	> Operation IXR_upgrade_24_7 E	xecutio	ns												C
• 1. Pre-Checks	• 2. Download • 3. Activa	ite	• 4. Reboot												(i) Execution Summary
Status	NE Name		NE ID		Product		Current Software Version		Target Software Version		Upgrade State	N	Magu In	:	∧ General
Success	VRR6D_245	T	92.168.96.175	T	7250 IXR	T	TIMOS-C-23.10.R2	T	TIMOS-24.7.R2	T	Upgrade Successful	c	D,,,-1,Fa	:	Start Time 2025/03/31 15:53:23 End Time 2025/03/31 16:00:28 Duration 7m 45 7877m s Werkflew LSO_7x50_Reboot Tetal Rervin N/A A Additional Infe
															<ul> <li>Execution Progress</li> </ul>
															Initial Run: ReadBofForReboot Initial Run: RebootDevice IdditionalInfo-[An I/O error occurred while try Ing to send a EL request on RR-725023.10.8 e <sup>R</sup>
•													•		Initial Run: SoftwareRebootSuccess
Auto-refresh Failed 0 In Progre	Last Refresh: 2025/3/31 1 ss 0 Not Started 0 Suc	6:27:11 ccessful 1			I< < Page: 1	/1	> >I						Row Cour	nt:1	

**i** Note: The RebootDevice incorrectly shows that it failed, as connectivity to the node was lost, even though it successfully passed. There is an active PTS to address this issue.

Alarms raised after reboot:

-				., , .	
•	netw.NetworkElement	N87_20	NodeRebooted	nodeReboot	
0	netw.NetworkElement	N87_20	NodeUpgraded	upgradedNodeVersion	

### 8.8.6 ISSU

See 8.11 "ISSU upgrade" (p. 424) for the steps to perform an ISSU upgrade.

## 8.9 Single phase upgrade: preparing the upgrade

#### 8.9.1 Steps

Upgrade is completed in one single phase with no pauses. The maintenance window will run before the start of the upgrade until it is complete.

#### 1

Navigate to Device Management, All operations.

NSP

2 -

Select Operation, Operation Type and choose "nsp-ne-upgrade" from the list.

ork pervices Platform							User:	aamin
	Select an Ope	ration Type				×		
1.	Category	Name	Description		Tags			
	1	·	T	T		T		
	upgrade	nsp-magc-appl-upgrade-phases	Operation for Multi-	Ph	LSO, MAGCa2			
	backup	nsp-ne-backup	Operation for NE Ba	ckup	LSO, Backup, SR OS, SR OS 72	10, SR		
	other	nsp-ne-backup-audit	Operation for NE Ba	ck	LSO, All			
	upgrade	nsp-ne-upgrade	Operation for Upgra	ide	LSO, Upgrade, SR OS, SR OS 7	210, S		
	upgrade	nsp-ne-upgrade-eth-sat	Operation for Ether	net	LSO, Upgrade, SR OS 7210			
2.	upgrade	nsp-ne-upgrade-with-phases	Operation for Multi-	Ph	LSO, Upgrade, SR OS, SR OS 7	210, S		
	backup	nsp-ne-wavence-backup	Operation for Waver	nce	LSO, Wavence			
Op	other	nsp-ne-wavence-file-retrieval	Operation for Waver	nce	LSO, Wavence			
	other	nsp-ne-wavence-password-upd	Operation for Waver	nce	LSO, Wavence			
	upgrade	nsp-ne-wavence-upgrade	Operation for Waver	nce	LSO, Wavence			
3.	other	nsp-wavence-service-migration	Operation for Waver	nce	LSO, Wavence			
						Row Count: 11		
4.					CANCEL	ADD		
							Create Another	CANCEL

3

Under General, fill out the Operation Name and select the Operation Control.

Operation Name*	Description	Targeted Product Family* 🚯
Control per phase: All targets must complete the currer phase before any target can proceed the next phase. Control per target: Per target - targets pr Per target - targets pr of other targets.	it to se ess	SR OS

4

#### Select **+ TARGETS**, **NEs** or **Predefined NE groups**.

3. Select Targets	+ TARGETS
	NEs
	Predefined NE groups
No targets selected	

5 -

Select Operation Inputs:

With single phase upgrades, users can select to enable or disable any of the phases. Below are the default options:

4. Operation Inputs							
Target Software Version* 🚺		Is I S S U* 🚺		Is Download* 🚺		Is Activate* 🚺	
SR OS: 7750-SR, 7950-XRS,	7450- ×	False	•	True	•	True	•
Is Reboot* 🚺	Auto Cleanup	• •	Free Space Po Number)	st Upgrade* (Enter a	0		
True	True	•	10				

6

**i** Note: Users cannot set both isISSU and isReboot to True.

Users can select any of these optional Advanced Inputs for each of the phases:

True 👻	10		
^ Advanced Inputs			
Check to enable options			
🔲 Window Size 📵	🔲 Failure Threshold (%) 🔞		
Upgrade			
Single phase node upgrade			
Concurrency Count	Phase Timeout (minutes) 1	Average Execution Threshold (minutes)	

END OF STEPS -

## 8.10 Single phase upgrade: performing the upgrade

### 8.10.1 Steps

1

View/Edit Schedule: Choose to Run or Save.

/iew/Edit Schedule					
Upgrade					
Single phase node upgrade					
Run immediately					
			CANCEL		
		Create Another	CANCEL	SAVE	

If you select "Run immediately" the upgrade will run in one phase and show the status as running.

2 -

If the upgrade fails, it can be re-run.

	Network Services Platform	1										User: admin 👻	0
Device Management >	Operation SinglePhaseUpgradeWDow	nload Executions											Ċ
• 1. Upgrade											i	Execution Summary	
Status	NE Name	Product	Cu Ve	urrent Software ersion	Target Software Version		Upgrade State		Last Updated	: 1		Software activation failed. Backout to current vers	i Î
•		T	T	T		T		T	DD/MM/YY1 - DD/MM/YY1 🖬				
Success	IXRR6D_245	7250 IXR	TI	MOS-C-23.10.R1	TIMOS-24.7.R1		Activate Successful		2024/10/15 13:58:52	: :	×	Rerun: PreChecks	
												Failed	
											~	Rerun: PreChecks	
											~	Rerun: Download	
											×	Rerun: Activate	1
												Software activation failed. Backout to current vers on has not worked	i
											~	Rerun: PreChecks	
											~	Rerun: Download	
•										• •	~	Rerun: Activate	
Auto-refresh	Last Refresh: 2024/10/15 14	k:40:23		< < Page: 1 / 1	> >1				Ro	w Count : 1			
Failed 0 In Progress 0	Not Started 0 Succe	rssful 1											

3 \_\_\_\_\_

See 8.11 "ISSU upgrade" (p. 424) for the steps to perform an ISSU upgrade.

End of steps

## 8.11 ISSU upgrade

### 8.11.1 Introduction

ISSU (In service software upgrade) is supported on specific chassis types. See "ISSU upgrade procedure" in the *SR OS Software Release Notes* for the specific release you are upgrading to.

### 8.11.2 Multi-phase ISSU upgrade

Fill out the upgrade operation options. Set the ISSU to "True". If the ISSU is not supported for the node, the Pre-check will fail.

NSP



Create Operation								×
Select an Operation Type	3. Select Targets					CLEAR	+ TARGETS	4
General			IC C Page: 1 / 1				Row Count: 1	
Select Targets	6 Operation Inputs							
Operation Inputs	4. Operation inputs							
View/Edit Schedule	Target Software Version* 🕕	Is I S S U* 🚯	Auto Cleanup* 🚯	Free Space Post Upgrade* (Enter a Number)	0			
	SR OS: 7750-SR, 7950-XRS, 7450- ×	True 👻	True 👻	10				1
	✓ Advanced Inputs							
	5. View/Edit Schedule							Į
	Pre-Checks							
	<ul> <li>Run immediately</li> </ul>							
	Download Software image download to NE							
	Run manually							
					Create Another	CANCEL SAVE	E RUN	

Figure 8-2 Successful ISSU upgrade:

• 1. Pre-Checks	• 2. Do	wnload • 3. Activate	• 4. Reboot											
Status		NE Name	Product		Current Software Version		Target Software Version		Upgrade State		Last Updated	Start Time	:	∧ General
	¥		т	T		٣		Т		T	DD/MM/YY - DD/MM/YY	DD/MM/YY - DD,		
• Success		live-144	7250 IXR		TIMOS-8-23.10.81		TMOS-23.10.86		Starting Upgrade		2024/10/28 11:30:16	2024/10/28 11:14:5		Jour India 2024/10/28 11:14:55 Eed Time 2024/10/28 11:30:16 Duration 15m 20:664ms Wurkflow USQ, 750, Reboot Total Rem N/A Additional Info Upgrade Successful
C												•	< >	
Auto-refre	esh aress 0	Last Refresh: 2024/10/28 14	i:30:25			Page:	1 /1 > >1					Row Co	unt : 1	



#### Example IXR node show card command during ISSU upgrade:

Before reboot:

A:live-14	4# show card		
Card Summa	ary		
	-		
Slot Comments	Provisioned Type	Admin	Operational
	Equipped Type (if different)	State	State
1	iom-ixr-r6	up	up
2	iom-ixr-r6	up	up
A	cpiom-ixr-r6	up	up/active
B =========	cpiom-ixr-r6	up ======	up/standby ====================================

#### Reboot phase:

A:live-144# show card \_\_\_\_\_ Card Summary \_\_\_\_\_ Slot Provisioned Type Admin Operational Comments Equipped Type (if different) State State \_\_\_\_\_ \_\_\_\_\_ iom-ixr-r6 1 up up 2 iom-ixr-r6 up provisioned (not equipped) А cpiom-ixr-r6 up up/active В cpiom-ixr-r6 down/standby up (not equipped) A:live-144# show card \_\_\_\_\_ Card Summary \_\_\_\_\_ Slot Provisioned Type Admin Operational Comments Equipped Type (if different) State State \_\_\_\_\_ \_\_\_\_\_

		======	
В	cpiom-ixr-r6	up	ISSU/standby
A	cpiom-ixr-r6	up	up/active
2	iom-ixr-r6	up	booting
1	iom-ixr-r6	up	up

\_\_\_\_\_

A:live-144#

B:live-144# show card

Card Summary \_\_\_\_\_ Slot Provisioned Type Admin Operational Comments Equipped Type (if different) State State \_\_\_\_\_ \_\_\_\_\_ iom-ixr-r6 up provisioned 1 (not equipped) 2 iom-ixr-r6 up up A cpiom-ixr-r6 up down/standby (not equipped) В cpiom-ixr-r6 up up/active \_\_\_\_\_ B:live-144# B:live-144# show card \_\_\_\_\_ Card Summary \_\_\_\_\_ Slot Provisioned Type Admin Operational Comments Equipped Type (if different) State State \_\_\_\_\_ 1 iom-ixr-r6 up up 2 iom-ixr-r6 up up up up/standby А cpiom-ixr-r6 В cpiom-ixr-r6 up up/active

### 8.11.3 Single phase ISSU upgrade

To complete an ISSU upgrade, users need to set the ISSU to "True" and Reboot to "False". Both cannot be set to "True" at the same time. The Pre-check will fail if both are set to "True".

\_\_\_\_\_

arget Software Version* 🕕		Is I S S U* 🕕		ls Download* 🕚		Is Activate* 🚺	
SR OS: 7750-SR, 7950-XRS, 7450-	· ×	True	•	True	•	True	•
s Reboot*	Auto Cleanup*	Ð	Free Space Po Number)	st Upgrade* (Enter a 🕕			
sReboot flag is used to	True	•	10				



	Network Servi	ces Platform														User: admin 🗸 🕥
Device Management	> Operation ISSU_IXR	Executions														0
• 1. Upgrade																(i) Execution Summary
Status	NE Name		5	Product		Current Software Version		Target Software Version		Upgrade State		Last Updated	Star	t Time	:	∧ General
,	-		T		т		٣		Ŧ		Ŧ	DD/MM/YY • DD/MM/YY 🖬	D	р/мм/үү <sup>,</sup> - DD,		Caust Time
Success	IXRR6D_2	245	1	7250 IXR		TIMOS-C-23.10.R1		TIMOS-24.7.R2		Upgrade Successful		2024/11/01 17:27:55	202	4/11/01 16:52:1	÷	2024/11/01 16:52:17
															•	Led Time 2024/11/01/12/2:55 Duration 35m 38s 21mms Workflow LSQ_7:XSQ_Upgrade Train Rarms N/A Additional Infe Successfully done 7:50 node upgrade operation Additional Infe Successfully done 7:50 node upgrade operation Execution Progress initial Run: PreChecks initial Run: Download initial Run: Activate initial Run: ISSU initial Run: SoftwareUpgradeSuccess
														•		
Auto-refresh	Last Refresh	2024/11/1 17:	30:57			€ € P	age:	1 71 2 31						Row Cou	nt:1	
Failed 0 In Progres	s 0 Not Starte	d 0 Succe	essful 1													

# **Post-upgrade procedures**

## 8.12 Rollback

### 8.12.1 Introduction

Rollback is the process of switching the node version back to its original pre-upgrade version. It is only supported in multi-phase upgrade/upgrade with phases and can be done from the Activate or Reboot state. It is not supported with single phase upgrade or ISSU.

### 8.12.2 Activate phase

To begin Rollback, click on **Rollback**.



**Note:** Rollback is an option regardless of if the phase passed or failed. After running the rollback, the phase will be in the failed state. All phases will be complete and cannot be re-run.

	tions did n	ot succeed in pha	se(s): Activa	te										(i) Execution Summary
1. Pre-Checks	• 2. Do	wnload 💽 3.	Activate	O 4. Reboot										∧ General
us		NE Name		Product		Current Software Version		Target Software Version		Upgrade State		Last Updated	Start Time :	Software Rollback Complete. Node has be
			T		T		٣		Т		Т	DD/MM/YY' - DD/MM/YY'	DD/MM/YY' - DD,	rolledback to original version
or		N87_20		7750 SR		TIMOS-C-23.10.R2		TIMOS-C-23 10 R2		Starting Upgrade		2024/11/0117:09:52	2024/11/01 17:09:4	Surt Time 2024/11/01 17:09:52 2024/11/01 17:09:52 Duration 9 817/ms Workflow Kollback Tatal Reren N/A

## 8.12.3 Reboot Rollback

Following the completion of the Rollback procedure, reboot the Rollback.

• 1. Pre-Checks	• 2. Download • 3. Active	ate . Reboot						(i) Execution Summary
tatus	NE Name	Product	Current Software Version	Target Software Version	Upgrade State	Last Updated		∧ General
,	•	T	T	T	T	DD/MM/YY) - DD/MM/YY		
Success	IXRR6D_245	7250 IXR	TIMOS-C-23.10.R1	TIMOS-24.7.R1	Upgrade Successful	2024/10/10 10:49:10	:	Start Time 2024/10/10 10:38:25
			Changes made by the	rollback action cannot be u	ndone. Do you want to perfo	rm a rollback?		10m 44s 800ms Warkflaw LSQ_7X50_Reboot Tatal Revue N/A Additional Infe Upgrade Successful

Device Management	> Opera	ion pgrade_NoCleanu	Exe	outions													0
Some execut	tions did not s	cceed in phase(s)	: Reboot														() Execution Summary
• 1, Pre-Checks	• 2. Downie	ad 💿 3. Activ	ate 🤇	4. Reboot													∧ General
Status	N	Name		Product		Current Software Version		Target Software Version		Upgrade State		Last Updated	Start Time	End Time	Duration	1	Software Rollback Complete. Node has been
	•		т		T,		T		т		T	DD/MM/YY - DD/MM/YY	DD/MM/111 - DD/MM/111 🖬	DD/MM/YYr - DD/MM/YYr 🖬			rolledback to original version
€ erer	0	R60_245		7250 XXX		TM05-C-23 1081		THOS-031081		Santing Upprofe		2024/10/19 11:2029	2024/10/1011/1331	2024/10/1011/2029	6m35k436ms	2	Sen Ties 2024/10/01/11:331 Leaf Ties 3024/10/01/11:3029 Barais Ministra 226ms Ministra 226ms Mi
4																• •	
Auto-refre	sh Last	Refresh: 2024/10/1	0 14:05:19					14	Page:	3 14 > >0					Ro	/ Count : 1	

# 8.13 LSO reporting

## 8.13.1 Reports

Reports are not published as out of the box with NSP, but LSO framework does support a way to generate and publish reports as part of the upgrade operation. The content of the report can be customized to include running config/show commands.

**i** Note: There is a limitation on the size of the generated file: 15Mb.

This needs to be requested and customized per customer need. Please contact the Nokia support team for more information.

For this use case, the Pre-check and Reboot workflows are customized to enable report generation and collect the following show commands pre and post-upgrade:

cmds:

- show card
- show system grpc connection
- show system netconf connection
- show router interface
- show system lldp neighbor
- show version

After enabling reporting for Pre-check and Reboot phases, users will see the new option "For detailed information, **view report**" in the info panel for these phases when they select **\*** "View log". Users can pick any supported file format in the workflow: csv, yaml, json, txt.

ence management 2	> 77	50_mPhase_Report Exec	ottu	8												0
Manual start "Do	ownload	" phase to proceed with the	oper	stion												(i) Execution Summary
1. Fre-Checks	O 2. Dow	vnload   0 3. Activate	) (	O 4. Reboot												∧ General
itatus		NE Name	1	voduct	1	Current Software Version		Target Software Version	_	Upgrade State		Last Updated	Start Time	End Time	1	6 For detailed information, view report
	•	т		т			т	т			T	DD/MM/YY - DD/MM/YY 🖬	DD/MM/YYY - DD/MM/YYY 🖬	DD/MM/YYY	- DD/MM/YY 🖬	Start Time
Success		N87_20		750 SR	1	TIMOS-C-23.10.R2		TIMOS-24.7.R2		PreChecks Complete		2024/11/14 16:36:12	2024/11/14 16:34:49	2024/11/14 1	6:36:12	2024/11/14 16:34:49
															Rerun View log Open in Workflows	End Time 2024/11/14 16:36:12 Duration 1m 23s 273ms
																Workflow LSQ_7x50_Pre_Checks Tatal Ranan N/A Mddional Info PreChecks Complete
																<ul> <li>Execution Progress</li> </ul>
																🗸 initial Run: ResdBof
																🗸 Initial Run: CheckTargetImageOnNSP
																Initial Run: preChecksSuccess
atus •	NE Name	Product														
-----------	---------	---------	---	-----------------------------	---	----------------------------	---	---------------	---	-------------------------------	--					
•				Current Software Version		Target Software Version		Upgrade State		Last U 🚦	∧ General					
	T		Ŧ		т		T		T	t/dd	For detailed information, view report or comparent or comparent.					
									Rerun Rollbac View log Compai Open in	k g re log Workflows	Surt Time 2024/11/17 22:48:03 End Time 2024/11/17 22:58:31 Durstion 10m 275 170ms Workflow LSO_7X50_Reboot Total Rerun N/A Additional Info Upgrade Successful					

#### Compare the reports:

^ .	6	
	<u>I</u> 10 unche	inged
11	,	
12	gRPC Server connections	
13		
3.4	Address : 135.121.151.226	
15	- Port : 6835	
36	Router Instance : management	
17	- Establishment Time : 2024/11/18 12:01:00	
18	Active RPC Count : 2	
19	Total RPC Count : 2	
20	- Rx Bytes : 20642	
21	- Tx Bytes : 416268	
22		
23	No. of connections : 1	
24		
25	NETCONF Server connections	
26		
27	Connection Username Session Status Session Running Candidate	
28	Id Type Locked? Locked?	
	<u><u><u></u></u> 25 uncha</u>	inged
	Number of neighbors - 2 TMOS-C- 28 10 P2 cmm/v86bons64 Nikia 750 SP Convrist/ (/ 2000, 2028 Nikia	
100		
36	- policion man podritti da tagi and o concerna na policide un concernativos	
4		

^∎6 ■6	All Unchanged Sections: 🗄 🌲	
10 unchang	ed lines collapsed	*
	12 gRPC Server connections	
	1)	
	14 Address :135.121.151.226	
	15 + Port : 34053	
	16 Router Instance : management	
	17 + Establishment Time : 2024/11/18 13 :18 :08	
	18 Active RPC Count : 2	
	19 Total RPC Count : 2	
	28 + RX Bytes : 7219	
	21 + Tx Bytes : 109739	
	12	_
	21 No. of connections : 1	
	- 24	
	25 NETCONF Server connections	
	26	
	27 Connection Username Session Status Session Running Candidate	
	28 Id Type Locked? Locked?	
1 25 unchang	red lines collapsed	
	<ul> <li>+ Number of neighbors : 2,TIMOS-C- 24. 7. R2 cpm/x86hops64 Nokia 7750 SR Copyright (c) 2000- 2024 Nokia.</li> </ul>	
	55 All rights reserved. All use subject to applicable license agreements.	
	<ul> <li>Built on Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/ 247B /R2/panos/main/sros</li> </ul>	*
4		•

# 8.14 Post-upgrade checks

### 8.14.1 Checks

For this use case, post-upgrade checks, show commands, and node configs are run on the nodes and compared to pre-upgrade.

NSP post-upgrade checks:

- · Node version in Device Management is updated to the new version
- Network Health View, Network Map View, and Inventory View are updated as expected

Additional NSP checks depend on NSP-enabled features. Some possible checks include:

- · Service Management all services are in the same state pre-upgrade
- Configuration Deployments (ICM) deployment status is the same pre-upgrade
- Telemetry stats collection works as expected post-upgrade
- · OAM tests continue to pass post-node upgrade

The following are examples of commands run during Pre-check. Run the commands again, then save the output to a file and compare it to the pre-upgrade output.

NSP

```
show card
show chassis
show mda
show version
show bof
show service service-using
show service sdp-using
show oam-pm tests
show system lldp neighbor
show router interface
show router rsvp neighbor
show router ospf neighbor
show system netconf connection
show system grpc connection
show port
show system information
```

The following 7750 SR example shows some default config changes occurred when upgrading from 23.10 R2 to 24.7 R2:



Users can check that the software version is successfully updated in Device Management and in the Network Elements dashboard:

	Network Services Plat	tform												User: admir			÷
Device Management	Devices Managed Network Eleme	ents •															
NE Name		Reachability	Mar	nagement State		Product	NE	Mode		Software Version		Management IP		NE ID		Chassis	:
	T	-			•	T			*		T		T		T		
IXRR6D_245		Reachable	-			7250 IXR	MC	м		TiMOS-C-24.7.R2		100.127.87.243		92.168.96.175		7250 IXR-R{	:
N87_20		Reachable	Mar	naged		7750 SR	Cla	ssic		TIMOS-C-24.7.R2		100.127.87.20		92.168.96.170		7750 SR-2s	:
Network Elements	25/03/31 16:10:56 (Click t	o update)														:	7 <sup>2</sup>
Name	Operational State	# Affected Objects		System Address		Management Address		Product	c	Chassis Type		Version			Commur	ication State	:
T		•	T		T		T		T		٦	r		T			
N87_20	enabled		14	92.168.96.170		100.127.87.20		7750 SR	7	7750 SR-2se		TIMOS-C-24.7.R2			up		
IXRR6D_245	enabled		12	92.168.96.175		100.127.87.243		7250 IXR	7	7250 IXR-R6dl		TIMOS-C-24.7.R2			up		

[/] A:admin@IXRR6D\_245# show version TiMOS-C-24.7.R2 cpm/x86hops64 Nokia 7250 IXR Copyright (c) 2000-2024 Nokia. All rights reserved. All use subject to applicable license agreements. Built on Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/247B/R2/panos/main/sros

[/] A:admin@IXRR6D\_245# <mark>|</mark>

### 8.15 Troubleshooting upgrades

### 8.15.1 Fail scenarios

When an upgrade operation fails, users can click on the failed operation and select **Open in Workflows**. A new window will open.



**Note:** If auto cleanup is set to False, and there is not enough space on the node, the Activate will fail but will not show the accurate reason.

Device Management	t > Operation EstActivate7750	xecutions									0-
Some execut	itions did not succeed in phase(s)	: Activate									(i) Execution Summary
• 1. Pre-Checks	• 2. Download • 3. Activ	ate O 4. Reboot									∧ General
Status	NE Name	Product	Current Software Version	T V	Target Software /ersion		Upgrade State		Last Updated	Start Time :	Error: One of the activation task failed. Bof
	•	T	Ŧ	T		т		Ţ	DD/MM/YY - DD/MM/YY	DD/MM/YY' - DD,	<ul> <li>updates were not performed. Node remains in current version</li> </ul>
• Error	N87_20	7750 SR	TIMOS-C-23.10.R2	Т	FIMOS-24.7.R2		Activation Failed		2024/11/04 13:39:28	2024/11/04 13:39:2	Start Time
										Rerun	2024/11/04 13:39:24
										Rollback	2024/11/04 13:39:28
										Open in Workflows	Duration 3s 767ms
											Workflow
											LSO_7x50_Activate
											N/A
										Q	<u>)</u>
											<ul> <li>Execution Progress</li> </ul>
											Initial Run: readBofForActivation
4										• • •	
Auto-refre	esh Last Refresh: 2024/11/4	13:46:01		Page: 1	71 > >I					Row Count : 1	
Failed 1 In Pro	ogress 0 Not Started 0 S	uccessful 0									

ce Management	> Operation testActivate7750 Ex	ecutions						
Some execut	ions did not succeed in phase[s]:	Activate						(i) Execution Summary
1. Pre-Checks	• 2. Download • 3. Activa	te O 4. Reboot						∧ General
us	NE Name	Product	Current Software Version	Target Software Version	Upgrade State	Last Updated	Start Time	Error: Software activation failed. Backout to
	•	Τ.	<b>T</b>	T	r T	DD/MM/YY - DD/MM/YY	DD/MM/YY - DD,	<ul> <li>current version has not worked</li> </ul>
ır	N87_20	7750 SR	TIMOS-C-23.10.R2	TIMOS-24.7.R2	Activation Failed	2024/11/04 13:51:19	2024/11/04 13:46:4	Start Time 2024/11/04 13:46:47
							Rerun Rollback Open in Workflows	End Time 2024/10/13:51:19 Duration 4m 315 438ms Workflow LSO_7/SO_ACtIvate Total Berun
								1      Execution Progress      Initial Run: readBofForActivation
								Rerun: readBofForActivation     Rerun: setBofForActivation
								Rerun: softwareActivationAndBackoutFailed     Software activation failed. Backout to current version
							• < •	as not worked
Auto-refres	sh Last Refresh: 2024/11/4	13:52:29	IC C Pa	ge: 1 /1 > >1			Row Count : 1	

```
A:N87 20# show bof
_____
BOF (Memory)
_____
   primary-image cf3:\images\TiMOS-24.7.R2
   primary-config cf3:\7750SR2SE.cfg
   secondary-image cf3:\images\TiMOS-SR-23.10.R2
                100.127.87.20/24 active
   address
   address
                100.127.87.21/24 standby
   primary-dns
                138.120.252.56
   dns-domain
                labs.ca.alcatel-lucent.com
   static-route
                10.0.0/8 next-hop 100.127.87.1
   static-route
                100.127.0.0/16 next-hop 100.127.87.1
   static-route
                135.0.0.0/8 next-hop 100.127.87.1
   static-route
                138.0.0/8 next-hop 100.127.87.1
   autonegotiate
   duplex
                full
                100
   speed
                3
   wait
   persist
                on
   no li-local-save
   no li-separate
```

\_\_\_\_\_

A:N87\_20#

\_\_\_\_\_



NSP

A:N87\_20# show redundancy synchronization

Synchronization Inform	mation							
=========================								
Standby Status	: standby ready							
Last Standby Failure	: N/A							
Standby Up Time	: 2024/09/30 10:03:42							
Standby Version	: TiMOS-C-23.10.R2 cpm/x86hops64 Nokia 7750 SR							
Сору	right (c) 2000-2023 Nokia.							
All ri	rights reserved. All use subject to							
appl	plicable license agreements.							
Built	lt on Mon Dec 11 23:45:58 UTC 2023 by							
build	ler in /builds/2310B/R2/panos/main/sros							
Failover Time	: N/A							
Failover Reason	: N/A							
Boot/Config Sync Mod	de : Configuration							
Boot/Config Sync Stat	us Boot environment synchronize failed							
Last Config File Sync T	ime : 10/08/2024 10:13:10							
Last Boot Env Sync Tir	ne : Never							
Rollback Sync Mode	: None							
Rollback Sync Status	: No Rollback synchronization							
Last Rollback Sync Tim	ne : Never							
Certificate Sync	: Enabled							
Cert Sync Status	: unknown							
Last Cert Sync Time	: Never							

A:N87\_20#

admin redundancy synchronize boot-env on the node manually

NSP

A:N87\_20# admin redundancy synchronize boot-env Syncing Boot environment boot option file : cf3:\bof.cfg.1 ... OK nvsvs file : cf3:\nvsys.info ... OK primary config : cf3:\7750SR2SE.cfg.2 ... OK persistent index : cf3:\7750SR2SE.ndx.2 ... OK primary image : ...ges\TiMOS-24.7.R2\cpm.tim ... Failed

MINOR: CLI Boot environment sync failed - Compact flash full or has no capacity on standby.

### 8.15.2 Solution

Delete some old files on the node and re-run the Activate phase.



### 8.15.3 Some useful node commands:

A:admin@IXRR6D\_245# show redundancy synchronization admin redundancy synchronize boot-env show card B detail | match expression cf3 post-lines 10 show card A detail | match expression cf3 post-lines 10 A:N87\_20# file version cf3-a:\boot.ldr TiMOS-L-24.7.R2 Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/247B/R2/panos/main/sros A:N87\_20# file version cf3-b:\boot.ldr TiMOS-L-24.7.R2 Thu Sep 5 20:04:26 UTC 2024 by builder in /builds/247B/R2/panos/main/sros A:N87\_20#

# 9 UCC-33: LSP Enhanced Path Control

### 9.1 Overview

#### 9.1.1 Purpose

This chapter describes the process required to configure LSP Enhanced Path Control on SR OS NEs using NSP. Two options for telemetry-based optimization, also called enhanced optimization, are presented.

Configuration examples in this chapter show NSP Release 24.4, SR OS 23.7.R2 NEs, and a VSR-NRC 24.3.R3 NE.

The following artifact bundles were used to test this use case:

- nsp-icm-intents-23.11.0-cam-bundle.zip
- nsp-telemetry-cr-va-sros-2.0.0-rel.8

See the NSP and NE documentation for more information.

### 9.1.2 Contents

9.1 Overview	443
Preparation	445
9.2 Prerequisites	445
9.3 Install the required artifact bundles	448
MPLS LSP provisioning	450
9.4 Provision MPLS LSPs using Device Configuration	450
Use case 1: Utilization/Bandwidth optimization	455
9.5 Bandwidth optimization	455
9.6 Create a bandwidth-based path profile	455
9.7 Enable traffic collection parameters using an API	458
9.8 Monitor bandwidth	459
9.9 Bandwidth optimization	462
9.10 System activity logging after bandwidth optimization	465
Use case 2: Latency-based optimization	467
9.11 Latency optimization	467
9.12 Create a latency-based path profile	467

9.13 Associate the latency-based path profile to LSPs in Device Management	470
9.14 Configure OAM configuration objects using an API	472
9.15 Create a TWAMP Light test session	474
9.16 Execute TWAMP Light session tests	479
9.17 Enable latency parameters using an API	480
9.18 Monitor latency	482
9.19 Latency-based optimization	485
9.20 System activity logging after latency optimization	491

# Preparation

### 9.2 Prerequisites

### 9.2.1 Network configuration prerequisites

Before enhanced path control can be configured in NSP, the network configuration prerequisites must be met. The following table describes the requirements that can apply to similar use cases, and indicates whether each prerequisite is required for this use case.

Where an NSP intent type is not available, CLI or MD-CLI must be used to perform configuration on the device.

Prerequisite	Documentation reference	Notes
Mandatory for LSP Enhanced Path Control		
<ul> <li>GRPC configuration</li> <li>1. Generate security certificates</li> <li>2. Configure security and enable GRPC on all devices</li> <li>3. Apply security certificates on all devices</li> </ul>	See SR TLS information here in the SR OS 24.3 R1 documentation: TLS	
Netconf/SNMP provisioning: enable NETCONF and SNMP protocols on all devices	For more information about SNMP and NETCONF with SR OS, see SNMP and NETCONF in the SR OS 24.3 R1 System Management Guide.	_
NSP installation	Pathway for NSP system installation in the <i>NSP Installation and Upgrade</i> <i>Guide</i> How do I enable TLS for telemetry and gNMI on_change support? in the <i>NSP System Administrator Guide</i> .	<ul> <li>Include the following in your deployment:</li> <li>Feature packs: <ul> <li>platform-baseServices</li> <li>platform-pluggableNetworkAdaptation</li> <li>platform-loggingMonitoring</li> <li>networkInfrastructureManagement-basicManagement</li> <li>networkInfrastructureManagement-deviceConfig</li> <li>enhancedOptimization</li> </ul> </li> <li>Adaptor suites: <ul> <li>sros-common</li> <li>sros-cological-inventory</li> <li>sros-23-7-r1</li> </ul> </li> <li>Additional required components: <ul> <li>VSR-NRC NE</li> </ul> </li> </ul>

Prerequisite	Documentation reference	Notes
Download the required artifact bundles from the NSP software delivery site: • NSP predefined set for ICM (device configuration) • vendor agnostic custom resources to support telemetry collection.	How do I install an artifact bundle? in the NSP Network Automation Guide	The vendor agnostic custom resources bundle is found on the NSP software delivery site, in the Adaptors folder along with your NE adaptor suite, for example, NSP $\rightarrow$ 23.11 $\rightarrow$ Adaptors $\rightarrow$ Nokia_SROS. Choose the zip file with va and cr in the filename, for example, nsp-telemetry-cr-va-sros-1.0.0-rel. 10.zip.
Device discovery	Pathway for device discovery in the NSP Classic Management User Guide How do I discover devices? in the NSP Device Management Guide Nokia Developer Portal for information about FTP mediation policy creation using API.	_
Cards and MDAs provisioning	ICM process in the NSP Device Management Guide for more information about using the Device Configuration views, and the other	The intent type required for this configuration is icm-equipment-card-mda.
Connectors and Ports provisioning	procedures in the <i>NSP Device</i> <i>Management Guide</i> for further detail. See the NSP ICM Intent Type Catalog for information about this and other device configuration intent types developed by Nokia.	<ul><li>The intent types required for this configuration are:</li><li>icm-equipment-port-connector</li><li>icm-equipment-port-ethernet</li></ul>
OSPF/ISIS	CLI Reference Guides for SR OS	—
LDPs, MPLS and RSVP configuration	CLI Reference Guides for SR OS	For LDP to be operational, the IPv4 and IPv6 bindings must be configured manually using CLI.
Interfaces Provisioning	How do I create a physical configuration deployment? in the NSP Device Management Guide.	The intent type required for this configuration is icm-router-network-interface
PCEP configuration	CLI Reference Guides for VSR-NRC	Most of the connections required for PCEP are established during previous configuration steps. For this use case, the VSR-NRC component must be correctly integrated with the setup. PCEP sessions between the routers in the network and the VSR-NRC component (VSR-I NE) must be established.

Prerequisite	Documentation reference	Notes
Optional items to include in your NSP deployment	Pathway for NSP system installation in the NSP Installation and Upgrade Guide SR OS Router Configuration Guide for information about configuring Cflowd sampling on NEs.	<ul> <li>Optional feature packs: <ul> <li>An AuxDB</li> <li>serviceActivationAndConfiguration-intentBasedServiceFulfillment</li> </ul> </li> <li>To force incoming traffic to use a particular LSP path, the easiest way is to configure a service between the edge routers. The service can be provisioned using CLI, but if the user wishes to use NSP, the serviceActivationAndConfiguration-intentBasedServiceFulfillment feature pack must be included. The service fulfillment artifact bundle is also required for this option.</li> <li>If you choose to provision a service via NSP, a customer will also have to be provisioned via NSP's Device Management, Device Configuration views.</li> <li>A Flow Collector (FC) and Flow Collector Controller (FCC)</li> <li>FC and FCC components are required if the older generation of 7250 IXRs are part of the Nokia SR OS network. For such devices, there is no gNMI telemetry support for collecting LSP/path statistics. Therefore, Cflowd sampling was used to collect interface/MPLS statistics.</li> <li>Cflowd sampling can be used for other NE types if preferred, however, this document assumes that gNMI telemetry will be used whenever possible.</li> <li>Older generation 7250 IXRs: <ul> <li>7250 IXR-6</li> <li>7250 IXR-R6</li> <li>7250 IXR-R6</li> <li>7250 IXR-Re</li> </ul> </li> <li>An NFM-P instance NFM-P is required if classically managed NEs are part of the network</li> </ul>
Download the following artifact bundle from the NSP software delivery site: • NSP product artifact bundle for Service Fulfillment	How do I install an artifact bundle? in the NSP Network Automation Guide	
BGP/EVPN	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent type required for this configuration is icm-router-bgp_group

Prerequisite	Documentation reference	Notes		
Segment Routing	CLI Reference Guides for SR OS	The examples in this use case use RSVP/MPLS LSPs. If SR-TE LSPs are used instead, segment routing configuration is mandatory.		
Scheduler QoS Policies	How do I create a logical configuration deployment? in the <i>NSP Device</i>	The intent types required for this configuration are: • icm-qos-schedulerpolicy-srqos		
Network QoS Policies configuration		<ul> <li>icm-qos-network-srqos</li> <li>icm-qos-sapingress-srqos</li> <li>icm-qos-sapegress-srqos</li> </ul>		
LAGs and MC-LAG creation	How do I create a logical configuration deployment? in the <i>NSP Device Management Guide</i> .	The intent types required for this configuration are: • icm-logical-lag-access • icm-logical-mc_lag-access		

# 9.3 Install the required artifact bundles

### 9.3.1 Purpose

Use this procedure to make the required artifacts, intent types and telemetry files, available to NSP. This procedure is based on the procedure for installing an artifact bundle in the *NSP Network Automation Guide*.

For example, the reference procedure in NSP 24.4 is How do I install an artifact bundle?.

### 9.3.2 Steps

### Download the required intent types

1 -

Download the ICM and CN telemetry artifact bundles from the NSP software delivery site.

Navigate through the hierarchy to the folder of artifacts that can be imported using the Artifacts views, for example: NSP  $\rightarrow$  24.4  $\rightarrow$  Artifacts  $\rightarrow$  Artifact\_Admin\_Import.

See the description to verify which bundles to download.

### Install an artifact bundle in NSP

2 \_\_\_\_\_

Log in to the NSP.

3

Open Artifacts, Artifact Bundles.

4 -

Click IMPORT & INSTALL.

#### 5 –

6

In the form that opens, drag and drop the zip files, or click **Browse** and navigate to the files on your system.

To install the artifact bundles immediately, click **IMPORT & INSTALL**. To import without installing, click **IMPORT**.

The chosen operation is triggered immediately. The artifact bundle status is updated to Imported or Installed when NSP has confirmed the status of all artifacts in the artifact bundle.

7 -

To install a bundle in Imported status, choose **Install bundle** from the **(**Table row actions) menu.

#### END OF STEPS -

# MPLS LSP provisioning

### 9.4 Provision MPLS LSPs using Device Configuration

### 9.4.1 Purpose

Use this procedure to configure MPLS LSPs using the Device Management views. This procedure is based on the overall device configuration procedure in the *NSP Device Management Guide*.

For example, the reference procedure in NSP Release 24.4 is ICM Process

The intent type required is icm-te-tunnel.

### 9.4.2 Prerequisites

Intent types must be installed and imported to NSP; see 9.3 "Install the required artifact bundles" (p. 448).

For this use case, the following parameters must be configured:

- egress-statistics must be enabled on the LSPs of the NE. This parameter may be enabled by default upon provisioning, depending on the NE type.
- pce-report this parameter must be enabled for the LSP to appear in Path Control in NSP. This attribute is enabled by default upon provisioning.

### 9.4.3 Steps

#### Import the intent type

1 \_\_\_\_\_

Log in the NSP.

2 \_\_\_\_\_

Open Device Management, Configuration Intent Types.

- Click + IMPORT
- 4 —

3 ——

Choose the icm-te-tunnel intent type from the list and click IMPORT.

### Create a configuration template

5 –

Open Device Management, Configuration Templates.

Click + TEMPLATE
In the form that opens, enter a name for the template.
<b>Note:</b> Template names cannot start or end with a space, or contain special characters other than spaces, underscores, or hyphens.
Click + INTENT TYPE and choose the icm-te-tunnel intent type.
Choose a configuration form from the drop-down list.
Click <b>RELEASE</b> to create the template in released state.

basic into	Basic Info			
Configuration Intent Type *	Template Name*			
Configuration Form	TE-Tunnel Template			
	Description			
	Tunnel Template that can be used for L	SP Provisioning. Based on definitions mentioned in icm-te-tur	inel intent type	6.
	Configuration Intent Type			REPLACE
	Only imported intent types will be a	vilable for selection. Go to Network Intents to view all	intent types.	
	Intent Type	Intent Type Version		
	icm-te-tunnel	2		
	Role	Category		
	Logical	LSP		
	Device Scope			
	SROS Classic & Model			
	Configuration Form			
	default			
	Source*	Destination*	Color	
	Description	Admin State		
	None	Up		
	Primary Paths			
	Primary Path			
		Path Computation Use Path		

The configuration template is added to the list.

Create Configuration Template

### Deploy the configuration

11 –

- a. Open Device Management, Configuration Templates.
- b. From the list, choose a template you created in the previous steps and click (More actions) **Deploy to Network**.

The form opens with the template already selected.

12 —

Choose the target NE:

- 1. Click **+ TARGET** and choose **NEs** from the drop-down list.
- 2. Choose an NE from the list to add to the Bin.
- 3. Verify that the correct NE is shown in the Bin and click **ADD**.

13 —

- 1. Click VIEW/EDIT TEMPLATE CONFIG.
- 2. In the form that opens, configure the template parameters. The following parameters are required:
  - A primary path must be added:
     Use Path Computation must be enabled
     path-computation-method must be path-locally-computed
  - Signaling Type must be RSVP.
  - An association object must be created, with the path profile associated to the LSP. The path profile is created in Path Control; see 9.6 "Create a bandwidth-based path profile" (p. 455) and 9.12 "Create a latency-based path profile" (p. 467)

It is not necessary to create path profiles before performing this procedure.

3. Click UPDATE.

In this example, no secondary path is provisioned.

14 -

Identifier fields appear in the form for each selected template. Enter information in each field.

**i** Attention: Your input can't contain the hash symbol (#).

15 -

Click **DEPLOY** to apply the configuration to the targets.

#### Audit the configuration

16

Perform an audit to verify that the configuration has deployed correctly:

- 1. Open Device Management, Configuration Deployments.
- 2. Choose a deployment.
- 3. Click () if needed to open the **Deployment Details** panel.
- 4. Click AUDIT CONFIG. The audit results and alignment status information are updated.

#### Repeat to deploy other LSPs

17 -

Repeat this procedure to deploy all other LSPs. Ensure that the correct path profile is assigned to each LSP.

END OF STEPS

### 9.4.4 LSP creation example, template parameters

TE-Tunnel Template						×			
Primary Paths	Protection								
Secondary Paths Protection Association Objects	Enable								
	Association Objects								
	Association Object Extended		-		+ ADD				
	Association Key	Id (Path Profile Id)	Extended Id (Path Group Id)						
	Utilization-based Optimization Profile	2			I	I			
	L		-						
			< Page: 1 /1 > >		Total: 1				
	Setup Priority	Hold Priority		Signaling Type		I			
	7	0		RSVP	<b>▼</b> □x				
						CANCEL UPDATE			

securet     pestission*     color       92.168.99.6     ×     92.168.97.241     ×       securitien Objects     0     0         Primary Paths       Primary Paths           Primary Path	-lunnel lemplate						
econdary Paths.  Potection  Permary Paths  Primary Path  Path Computation  Ver Path  Path Computation  Path-locally-computed  Ver Path  Path  Path Computed  Ver Path  ath	imary Paths	Source*		Destination*		Color	
Administrate None Up CR Primary Paths Primary Path Path Computation Use Path Computation Discuss Primary Dath Path-Computation Use Path Computation Discuss Primary Dath Path-Computation Use Path Computation Discuss Primary Dath Path-Computation Use Path Computation Discuss Primary Dath Path-Computation Discuss Primary Dath Path-Path Path-Computation Discuss Primary Dath Path Path-Path Path	condary Paths	92.168.99.6	×	92.168.97.241	×		
ssociation Objects  None  Up	otection	Description		Admin State			
Primary Paths         + ADD         Name       Path Computation       Use Path Computation       Setup Priority       Hold Priority         Iose       path-locally-computed       true       7       0       ::	sociation Objects	None		Up	• Cx		
loose path-locally-computed true 7 0 :		Primary Path Name	Path Computation Method	Use Path Computation	Setup Priority	Hold Priority	+ ADD
		loose	path-locally-computed	true	7	0	I

### Use case 1: Utilization/Bandwidth optimization

### 9.5 Bandwidth optimization

### 9.5.1 Overview

This use case demonstrates NSP's Path Control Bandwidth optimization. With bandwidth optimization, optimization is triggered when link utilization exceeds a configured threshold.

To perform bandwidth optimization, create a path profile to optimize on Cost, with Telemetry as the bandwidth strategy.

### 9.6 Create a bandwidth-based path profile

### 9.6.1 Purpose

Use this procedure to configure a path profile for bandwidth optimization, using the Path Control view.

This procedure is based on the following:

- the procedure to configure a path profile policy in the NSP Path Control and Simulation Guide
- an API call using the NSP Path Control API

For example, the reference procedures in NSP Release 24.4 are:

- · How do I create a path profile policy?
- Swagger documentation for the NSP Path Control API on the Nokia Developer Portal

**Note:** If LSPs were created with path profile IDs before the creation of path profiles, an error message is displayed showing that a path profile or association policy is configured on the path but missing on NSP. This is expected and will resolve when the profiles are created.

	2	B	[≡]	A
8	Operati associa missing	ion Down with p tion policy is co g on NSP	ath error: Path p nfigured on the p	rofile or path, but

### 9.6.2 Steps

### Create a path profile policy

Log in to the NSP.

2 -

1

From the **Path Control, Path Profiles** view, click **Create Policy** (). The Create Path Profile policy form opens.

3 —

Configure the required parameters:

- the Profile ID parameter must match the profile ID number configured for the LSPs in Step 13 of 9.4 "Provision MPLS LSPs using Device Configuration" (p. 450).
- · Optimize on (Objective) must be Cost
- Bandwidth Strategy must be Telemetry
- 4

As required, Exclude Route Objects by adding the IP address(es) of the object(s) to be excluded.

5

As required, Include Route Objects by adding the IP address(es) of the object(s) to be included. You must also specify Hop Type.

6

Click **CREATE**. The Path Profile policy is created.

Issue 4

Create	Path	Profile	Policy
--------	------	---------	--------

Reserved Profile ID
Name
BW-based_Path_Profile
Profile ID
2
Description
A BW or utilization-based optimization path profile
Bi-directional
No
Disjoint
No
No   Optimize On (Objective)
No   Optimize On (Objective)  Cost
No <ul> <li>Optimize On (Objective)</li> <li>Cost</li> <li>Bandwidth Strategy</li> <li>Eandwidth Strategy</li> <li>Image: /li></ul>
No <ul> <li>Optimize On (Objective)</li> <li>Cost</li> <li>Bandwidth Strategy</li> <li>Telemetry</li> <li> </li></ul>
No <ul> <li>Optimize On (Objective)</li> <li>Cost</li> <li>Bandwidth Strategy</li> </ul> Telemetry <ul> <li>Keep Bandwidth Reservation on Failure</li> </ul>
No   Optimize On (Objective)   Cost   Bandwidth Strategy   Telemetry   Telemetry   Keep Bandwidth Reservation on Failure   Explicit Route Strategy
No <ul> <li>Optimize On (Objective)</li> <li>Cost</li> <li>Gost</li> <li>Bandwidth Strategy</li> <li>Telemetry</li> <li>Telemetry</li> <li>Keep Bandwidth Reservation on Failure</li> </ul> <li>Explicit Route Strategy</li> <li>Standard</li> <li> <ul> <li>Standard</li> </ul> </li>
No       ▼         Optimize On (Objective)       ▼         Cost       ▼         Bandwidth Strategy       ▼         Telemetry       ▼         ▲ Keep Bandwidth Reservation on Failure       ▼         Explicit Route Strategy       ▼         Standard       ▼         Control Route Strategy       ▼

#### **Re-signal LSPs**

7

Now that the path profile policy is in place, the LSPs assigned to the profile can be brought up:

- 1. Open the **Path Control, LSPs** view.
- 2. Select an LSP and click (Table row actions), **Resignal**.

END OF STEPS

### 9.7 Enable traffic collection parameters using an API

#### 9.7.1 Allow Path Control to receive the bandwidth measurements from the network

The next step is to configure specific parameters and subscriptions to enable collection and set thresholds. There is no UI support for this: the pre-requisites can be configured via a specific NSP Path Control API call. See the following example:

PATCH	<ul> <li>✓ https</li> </ul>	s://{(server))/sdn/a	pi/v4/nsp/c	onfiguratio	on/traffic-da	ata-collection		
Params	Authorization	Headers (11)	Body •	Scripts	Tests	Settings		
⊖ none	⊖ form-data	⊖ x-www-form-	urlencoded	O raw	) binary	⊖ GraphQL	JSON	V
1 {								
2	"data": {							
3 -	"enabled":	true,						
4	"flowColle	ction": {						
5	"mplsLab	elStackQueryRa	te": 60,					
6 .	"srTeLsp	Enabled": true	,					
7 -	"staleSt	atsWipeInterva	1": 60,					
8	statsTi	meToLive": 360						
9 -	····},							
10	"linkBwTar	getThreshold":	10,					
11 -	"linkBwTri	ggerThreshold"	: 10,					
12	"neLevelFi	lteringEnabled	": true,					
13	"source":	"mdm"						
14	- }							
15 2								

In this example, the BW link threshold values were set to 10, which means 10%. Therefore, if a particular link has a utilization value exceeding 10%, NSP's Path Control module will attempt to re-

route one or more LSPs, avoiding that link. It is important to note that for this use case to work, the 'source' value must also be set to 'mdm'.

When the call is successful, real-time BW measurements in Path Control for both LSP and link objects are displayed. The measurements are updated approximately every minute.

Following the API call, streaming telemetry subscriptions for reporting link and LSP bandwidth are automatically created, as shown in the following figure.

	Network Services Platform					User: admin	• ⑦
Data Collection	and Analysis Management Subscriptions	•				+ SUBSCRI	IPTION C :
Telemetry Sub	oscriptions -						
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions
•							
Enabled	combined-interface-streaming	telemetry:/base/interfaces/combined-mpls-ip-interface	60	00:00	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	mpls-interface-streaming	telemetry:/base/mpls-interfaces/mpls-interface	60	00:00	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	router-interface-streaming	telemetry:/base/router-interfaces/router-interface	60	00:00	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	lsp-egress-path-stats-streaming	telemetry:/base/lsps/lsp-egress-path	60	00:00	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	lsp-egress-stats-streaming	telemetry:/base/lsps/lsp-egress	60	00:00	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	lsp-egress-summation-stats-streaming	telemetry:/base/lsps/lsp-egress	60	00:00	$\checkmark$		:

# 9.8 Monitor bandwidth

### 9.8.1 Monitoring links in Path Control

Open the Path Control, Links view and select a link.

You can click LSPS in the Info panel to see LSPs on the selected link.

The following columns show bandwidth data:

- Utilization/Reservation (%)
- Available Bandwidth

Note: Available Bandwidth is Total Link Bandwidth — Consumed Bandwidth. Bandwidth can be reserved for another LSP using the same link.

- Bandwidth
- Measured IP BW: pure IP traffic on the link
- Measured MPLS BW: MPLS traffic over the link (the sum of all LSPs using the link)
- Measured MPLS & IP BW: this value is only used for 7250 IXR NEs. These NEs do not split MPLS and IP traffic.

Path Control Link	3	Ŧ									
Reservation = (%)	Source	IP Address	Operation	Admin =	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW Measured (Mbps) (Mbps)	MPLS BW Measure BW (Mb	red MPLS & IP ops)	Latency (microse	ec i
			•	•	т	Т	Т	т	T		
• 9	CE_East	20.20.23.5	Up	Up	9051	10000	0	0	0.001		÷ ^
• 9	Seattle	20.20.22.6	Up	Up	9050.999	10000	0.001	0	0		-
• 9	CE_West	20.20.20.1	Up	Up	9051	10000	0	0	0.001		-
• 9	Core_2	10.10.16.10	Up	Up	9050.999	10000	0.001	0	0		-
• 9	Boston	20.20.23.6	Up	Up	9050.999	10000	0.001	0	0		-
• 9	Boston	10.10.17.13	Up	Up	9050.999	10000	0.001	0	0		-
• 9	Core_1	10.10.15.2	Up	Up	9050.999	10000	0.001	0	0		- 1
• 9	Calgary	10.10.10.1	Up	Up	9050.999	10000	0.001	0	0		- 1
• 0	Core_1	10.10.14.14	Up	Up	9999.999	10000	0.001	0	0		
• 0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Seattle	10.10.16.1	Up	Up	9999.998	10000	0.002	0	0	-	:
• 0	Calgary	10.10.12.9	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Toronto	10.10.13.13	Up	Up	9999.999	10000	0.001	0	0		
• 0	92.168.99.38	10.10.40.2	Up	Up	0	0	0	0	0		-
• 0	Core_1	10.10.11.6	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Core_1	10.10.10.2	Up	Up	9999.999	10000	0.001	0	0		
• 0	Toronto	20.20.21.2	Up	Up	9999.999	10000	0.001	0	0		
• 0	Core_2	10.10.12.10	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Core_2	10.10.16.14	Up	Up	9999.999	10000	0.001	0	0		-
• 0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Boston	10.10.15.1	Up	Up	9999.999	10000	0.001	0	0	-	:
• 0	CE_East	20.20.23.1	Up	Up	9999.999	10000	0	0	0.001	-	
• 0	CE_East	20.20.21.5	Up	Up	10000	10000	0	0	0	-	
• 0	Core_1	10.10.30.1	Up	Up	9999.999	10000	0.001	0	0	-	
• 0	Core_2	10.10.30.6	Up	Up	10000	10000	0	0	0		

Click **(**Table row actions), **Show on map** to display the link in a network map format.

Click on the highlighted link to display link information in the Info panel.



### 9.8.2 Monitoring LSPs in Path Control

Open the Path Control, LSPs and select an LSP.

- The Hops panel in the Info panel shows the LSP paths.
- The following columns show bandwidth data:
  - Bandwidth
  - Telemetry Measured BW

Click [(Table row actions), **Show on map** to display the LSP in a network map format.

May 2025

Issue 4



Click on a link to display link information in the Info panel.

# 9.9 Bandwidth optimization

### 9.9.1 Link rerouting

After injecting some traffic, we can check the Path Control, Links view to see that at least one LSP has been rerouted to bypass links where utilization exceeds the configured threshold value of 10%.

**i** Note: To demonstrate this particular use case, the iPerf3 tool was used to inject traffic (i.e. to simulate real-live traffic).

#### Example, before optimization:

	Network Service	es Platform							
Path Control Lin	ks	•							
Reservation = (%)	Source	IP Address	Operati	Admin	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW (Mbps)	Measured MPLS BW (Mbps)	:
			-	•	T	T	T	T	
• 10	Core_1	10.10.15.2	Up	Up	8994.082	10000	0.001	3.872	:
• 10	Core_2	10.10.16.10	Up	Up	9003.649	10000	0.001	0.127	:
• 10	Boston	10.10.17.13	Up	Up	9003.649	10000	0.001	0.13	:
• 10	CE_West	20.20.20.1	Up	Up	8994.083	10000	0	0	:
• 10	Boston	20.20.23.6	Up	Up	8994.082	10000	0.001	3.849	:
• 10	Calgary	10.10.10.1	Up	Up	8994.082	10000	0.001	3.785	:
• 10	Seattle	20.20.22.6	Up	Up	9003.649	10000	0.001	0.133	:
• 10	CE_East	20.20.23.5	Up	Up	9003.65	10000	0	0	:
• 0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0	:
• 0	Toronto	10.10.11.13	Up	Up	9999.999	10000	0.001	0	:
• 0	Core_2	10.10.30.2	Up	Up	9999.999	10000	0.001	0	:
• 0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0	:
• 0	Core_2	10.10.16.2	Up	Up	9999.998	10000	0.002	0	:
• 0	Calgary	10.10.10.13	Up	Up	9999.999	10000	0.001	0	:
• 0	Boston	10.10.15.5	Up	Up	9999.999	10000	0.001	0	:
• 0	Core_1	10.10.10.10	Up	Up	9999.999	10000	0.001	0	:

#### Example, after optimization:

Path Control Links		•									
Reservation =	Source	IP Address	Operati	Admin	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured IP BW (Mbps)	Measured MPLS BW (Mbps)	Measured MPLS & IP BW (Mbps)	Latency (microseconds)	:
			•	· · · ·	т	Т	T	T	T		
• 10	Core_1	10.10.15.2	Up	Up	9003.999	10000	0.001	0	0	-	: 1
• 10	Core_2	10.10.16.10	Up	Up	9003.722	10000	0.001	0.335	0		:
• 10	Boston	10.10.17.13	Up	Up	9003.722	10000	0.001	0.328	0	-	:
• 10	CE_West	20.20.20.1	Up	Up	9004	10000	0	0	0.001	10	:
• 10	Boston	20.20.23.6	Up	Up	9003.999	10000	0.001	0	0	-	:
• 10	Calgary	10.10.10.1	Up	Up	9003.999	10000	0.001	0	0		:
• 10	Seattle	20.20.22.6	Up	Up	9003.722	10000	0.001	0.349	0	т <u>е</u>	:
• 10	CE_East	20.20.23.5	Up	Up	9003.723	10000	0	0	0.328		:
• 0	Core_2	10.10.40.1	Up	Up	9999.999	10000	0.001	0	0		:
• 0	Toronto	10.10.11.13	Up	Up	9999.999	10000	0.001	0	0		:
• 0	Core_2	10.10.30.2	Up	Up	9999.999	10000	0.001	0	0	12	:
• 0	Calgary	10.10.12.13	Up	Up	9999.999	10000	0.001	0	0		:
• 0	Core_2	10.10.16.2	Up	Up	9999.998	10000	0.002	0	0		:
• 0	Calgary	10.10.10.13	Up	Up	9999.999	10000	0.001	0	0	-	:
• 0	Boston	10.10.15.5	Up	Up	9999.999	10000	0.001	0	0	с <u>и</u>	:

None of the links has available bandwidth lower than 9 000 Mbps. The network has optimized itself; redirecting LSPs to other links.

#### 9.9.2 Network map views

The change to the path is clear in the network map.

Network map example, before optimization:



Network map example, after optimization:



# 9.10 System activity logging after bandwidth optimization

### 9.10.1 Monitor events in real time

To view system event logs, open the Path Control, System Activity Logging view.

The logs show the bandwidth optimization operation on the links, as seen in the following example:

#### UCC-33: LSP Enhanced Path Control Use case 1: Utilization/Bandwidth optimization System activity logging after bandwidth optimization

Path Control System Activity Logging •						
Creation Date & Time ≡	Category	Source	Target	Log message		
Jul 04, 2024 02:43:59 PM-Jul 05, 2024 02:43:59	•					
Jul 05, 2024 02:32:09 PM	LSP	92.168.98.97	toSeattle_5::toSeattle	Calculation found path same as existing, no update required. Trigger: RESIGNAL_TIMER. +		
Jul 05, 2024 02:32:09 PM	ALGO	92.168.98.97	toSeattle_5::toSeattle	Path calculation success		
Jul 05, 2024 02:31:24 PM	LSP	92.168.96.46	toToronto_4::toToront	Calculation found path same as existing, no update required. Trigger: RESIGNAL_TIMER.		
Jul 05, 2024 02:31:24 PM	ALGO	92.168.96.46	toToronto_4::toToront	Path calculation success		
Jul 05, 2024 02:31:12 PM	LINK	92.168.99.6	92.168.99.6::92.168.9	Link bandwidth utilization dropped below the target threshold of 10. Bandwidth optimi.		
Jul 05, 2024 02:31:12 PM	LINK	92:168.96.46	92.168.96.46::92.168	Link bandwidth utilization dropped below the target threshold of 10. Bandwidth optimi.		
Jul 05, 2024 02:31:12 PM	LINK	92.168.97.250	92.168.97.250::92.16	Link bandwidth utilization dropped below the target threshold of 10. Bandwidth optimi.		
Jul 05, 2024 02:31:12 PM	LINK	92.168.98.97	92.168.98.97::92.168	Link bandwidth utilization dropped below the target threshold of 10. Bandwidth optimi.		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state set to [REGISTERED]		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state set to [REGISTERED]		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state change notified cause by [KPI_STATE_CHANGED];		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state change notified cause by [KPI_STATE_CHANGED];		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state set to [PENDING]		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state set to [UNKNOWN]		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI is deregistered for LSP [toCE_East::toCE_East_loose]		
Jul 05, 2024 02:31:11 PM	LSP	92.168.99.6	toCE_East::toCE_East	KPI state change notified cause by [REQUESTED_BW_DIFF, CURRENT_PATH_CHANGE];		

# Use case 2: Latency-based optimization

### 9.11 Latency optimization

### 9.11.1 Overview

This use case demonstrates NSP's Path Control latency-based optimization. With latency-based optimization, optimization is triggered when latency exceeds a configured threshold.

To perform latency-based optimization, create a path profile to optimize on Latency, with Telemetry as the bandwidth strategy.

# 9.12 Create a latency-based path profile

### 9.12.1 Purpose

Use this procedure to configure a path profile for latency-based optimization, using the Path Control view.

This procedure is based on the following:

• the procedure to configure a path profile policy in the NSP Path Control and Simulation Guide

For example, the reference procedures in NSP Release 24.4 are:

- How do I create a path profile policy?
- Swagger documentation for the NSP Path Control API on the Nokia Developer Portal

**i** Note: If LSPs were created with path profile IDs before the creation of path profiles, an error message is displayed showing that a path profile or association policy is configured on the path but missing on NSP. This is expected and will resolve when the profiles are created.

	2		[=]	1				
8	Operation Down with path error: Path profile or association policy is configured on the path, but missing on NSP							

### 9.12.2 Steps

1 -

Log in to the NSP.

#### 2 -

From the **Path Control, Path Profiles** view, click **Create Policy**  $\bigoplus$ . The Create Path Profile policy form opens.

3

Configure the required parameters:

- the Profile ID parameter must match the profile ID number configured for the LSPs in Step 13 of 9.4 "Provision MPLS LSPs using Device Configuration" (p. 450).
- · Optimize on (Objective) must be Latency
- · Bandwidth Strategy must be Telemetry
- the Max Latency and Latency Threshold parameters must be configured.

In this example, the latency threshold value is set to 90,000 microseconds (90 milliseconds). Therefore, if a particular link latency exceeds this value (i.e. 90,000 microseconds, NSP's Path Control will attempt to re-route the LSPs which are using the link.

4

Click **CREATE**. The Path Profile policy is created.
Reserved Profile ID   Name   Latency-based_Path_Profile   Profile ID   4   Description   A latency-based optimization path profile   Bi-directional   No   Disjoint   No   Optimize On (Objective)   Latency (microseconds)   Sandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure	Reserved Profile ID   Name   Latency-based_Path_Profile   Profile ID   4   Description   A latency-based optimization path profile   Bi-directional   No   Disjoint   No   Optimize On (Objective)   Latency (microseconds)   Bandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure   Explicit Route Strategy		
Name Latency-based_Path_Profile  Profile ID  4  Description A latency-based optimization path profile  Bi-directional  No  Disjoint  No  Optimize On (Objective) Latency (microseconds)  Bandwidth Strategy  Telemetry  Keep Bandwidth Reservation on Failure	Name Latency-based_Path_Profile  Profile ID  4  Description A latency-based optimization path profile  Bi-directional No  Disjoint No  Optimize On (Objective) Latency (microseconds)  Bandwidth Strategy  Telemetry  Keep Bandwidth Reservation on Failure  Explicit Route Strategy	Reserved Profile ID	
Latency-based_Path_Profile  Profile ID  4  Description  A latency-based optimization path profile  Bi-directional  No  Disjoint  No  Optimize On (Objective)  Latency (microseconds)  Catency (microseconds)  Eandwidth Strategy  Telemetry  Keep Bandwidth Reservation on Failure	Latency-based_Path_Profile  Profile ID  4  Description  A latency-based optimization path profile  Bi-directional  No  Disjoint  No  Optimize On (Objective)  Latency (microseconds)  Bandwidth Strategy  Telemetry  Keep Bandwidth Reservation on Failure  Explicit Route Strategy	Name	
Profile ID 4 4 Description A latency-based optimization path profile Bi-directional No  Disjoint No  Optimize On (Objective) Latency (microseconds)  Fandwidth Strategy Telemetry  Keep Bandwidth Reservation on Failure	Profile ID 4 4 Description A latency-based optimization path profile Bi-directional No Disjoint No Optimize On (Objective) Latency (microseconds) Catency (micro	Latency-based_Path_Profile	
4 Description A latency-based optimization path profile Bi-directional No ▼ Disjoint No ▼ Optimize On (Objective) Latency (microseconds) ▼ Bandwidth Strategy Telemetry ▼	4 Description A latency-based optimization path profile Bi-directional No Disjoint No Coptimize On (Objective) Latency (microseconds) Catency (microseconds) Cat	Profile ID	
Description   A latency-based optimization path profile   Bi-directional   No   Disjoint   No   Optimize On (Objective)   Latency (microseconds)   Bandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure	Description   A latency-based optimization path profile   Bi-directional   No   Disjoint   No   Optimize On (Objective)   Latency (microseconds)   Eandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure   Explicit Route Strategy	4	
A latency-based optimization path profile  Bi-directional  No  Disjoint  No  Optimize On (Objective)  Latency (microseconds)  Telemetry  Keep Bandwidth Reservation on Failure	A latency-based optimization path profile  Bi-directional  No  Disjoint  No  Optimize On (Objective)  Latency (microseconds)  Bandwidth Strategy  Telemetry  Keep Bandwidth Reservation on Failure  Explicit Route Strategy	Description	
Bi-directional   No ▼   Disjoint No   No ▼   Optimize On (Objective)   Latency (microseconds)   ▼   Bandwidth Strategy   Telemetry   ▼   Keep Bandwidth Reservation on Failure	Bi-directional No No Disjoint No Optimize On (Objective) Latency (microseconds)  Bandwidth Strategy Telemetry Keep Bandwidth Reservation on Failure Explicit Route Strategy	A latency-based optimization path profile	
No   Disjoint   No   Optimize On (Objective)   Latency (microseconds)   Bandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure	No   Disjoint  No   Optimize On (Objective)  Latency (microseconds)  Telemetry  Keep Bandwidth Reservation on Failure  Explicit Route Strategy	Si-directional	
Disjoint No Optimize On (Objective) Latency (microseconds) Bandwidth Strategy Telemetry Keep Bandwidth Reservation on Failure	Disjoint No Optimize On (Objective) Latency (microseconds)  Bandwidth Strategy Telemetry Keep Bandwidth Reservation on Failure Explicit Route Strategy	No	•
No   Optimize On (Objective)   Latency (microseconds)   Bandwidth Strategy   Telemetry   Keep Bandwidth Reservation on Failure	No   Optimize On (Objective)   Latency (microseconds)   Bandwidth Strategy   Telemetry   Telemetry   Keep Bandwidth Reservation on Failure   Explicit Route Strategy	Disjoint	
Optimize On (Objective)         Latency (microseconds)         Bandwidth Strategy         Telemetry         Telemetry         Keep Bandwidth Reservation on Failure	Optimize On (Objective) Latency (microseconds)   Bandwidth Strategy Telemetry Keep Bandwidth Reservation on Failure Explicit Route Strategy	No	•
Latency (microseconds) <ul> <li>Bandwidth Strategy</li> <li>Telemetry</li> <li>Keep Bandwidth Reservation on Failure</li> </ul>	Latency (microseconds)       ▼         Bandwidth Strategy       ▼         Telemetry       ▼         ▲ Keep Bandwidth Reservation on Failure       ■         Explicit Route Strategy       ■	Optimize On (Objective)	
Bandwidth Strategy Telemetry Keep Bandwidth Reservation on Failure	Bandwidth Strategy         Telemetry         Keep Bandwidth Reservation on Failure         Explicit Route Strategy	Latency (microseconds)	<b>*</b>
Telemetry   Keep Bandwidth Reservation on Failure	Telemetry  Keep Bandwidth Reservation on Failure  Explicit Route Strategy	Sandwidth Strategy	
Keep Bandwidth Reservation on Failure	Keep Bandwidth Reservation on Failure Explicit Route Strategy	Telemetry	<b>.</b>
Keep Bandwidth Reservation on Failure	Keep Bandwidth Reservation on Failure  Explicit Route Strategy		
	Explicit Route Strategy	Keep Bandwidth Reservation on Failure	

Standard	•
SID Protection Strategy	
Standard (Protected Preferred)	-
Max Hops (Span)	
0	
Max Cost	
0	
Max TE Metric	
0	
Max Latency (microseconds)	
90000	
······	
Latency Threshold (microseconds)	
90000	
Exclude Route Objects	+ ADD

# 9.13 Associate the latency-based path profile to LSPs in Device Management

# 9.13.1 Purpose

Use this procedure to assign the newly created latency-based path profile to the LSPs. Perform this procedure for each LSP.

To perform this procedure, the LSPs must be configured using Device Configuration; see 9.4 "Provision MPLS LSPs using Device Configuration" (p. 450).

This procedure is based on the procedure to edit a deployment in the *NSP Device Management Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I edit a deployment?.

# 9.13.2 Steps

1	
•	Log in to the NSP.
~	
2	Open Device Management, Configuration Deployments.
3	
	Choose an LSP deployment and click (Table row actions), View/Edit.
٨	
-	In the <b>Deploy Logical Configuration</b> form, click <b>VIEW/EDIT TEMPLATE CONFIG</b> to change the parameters.
_	
5	
	In the Association Objects panel, click + ADD.
	Enter an association key to describe the path profile, and the path profile ID. The path profile ID

LSP Template					
Primary Paths	Setup Priority		Hold Priority	Signaling Type	
Secondary Paths	7		0	RSVP	- Cx
Protection Association Objects	Association Object	S			
	Association Object Extended				+ ADD
	Association Key	Id (Path Profile Id)	Extended Id (Path Group Id)		
	Latency-based Optimi	4			1
			IK K Page: 1 /1 3	> >1	Total: 1

must match the ID provided in 9.12 "Create a latency-based path profile" (p. 467).

# 6 Click DEPLOY.

7 –

Verify that the path profile has been assigned:

- 1. Open the Path Control, LSPs view.
- 2. Select the LSP and view the Association Groups and Profiles panel.
- 3. Verify the profile ID.

= NOKIA Ne	twork Services Platform								Use	r: admin		• ⑦
Path Control LSPs	*											÷ ÷
LSP Name	Administration	Operation	Path Type	Delegated	NSP Initiated	Active	Source N	:	2	٨	[=]	A
toCE_East ×		· ·							Assigned Pro	files		
toCE_East::toCE_East	Up	Up	RSVP		а. С		92.168.5	:	Profile details o	an be seen in Path	Profiles	
toCE_East_2::toCE_Ea	Up	Up	RSVP	$\checkmark$		$\checkmark$	92.168.5	:	Profile 4 Group 0			:≡ ^
toCE_East_IETF::toCE	Up	Up	RSVP	$\checkmark$	~	$\checkmark$	92.168.5	:	Name	9	1	
									Latency-ba	ised_Path_Profile		
									Profile ID 4			
									Description A latency-b	pased optimization	n path profil	e

END OF STEPS

# 9.14 Configure OAM configuration objects using an API

# 9.14.1 Purpose

Use this procedure to create configuration objects that are required prerequisites for TWAMP Light session tests. There is no UI support for this: the pre-requisites can be configured via NSP OAM configuration API calls.

See the Swagger documentation for the NSP OAM configuration API on the Nokia Developer Portal for more information.

# 9.14.2 Steps

1

Configure an OAM-PM bin group for each NE. Note the bin-group-id attribute. Example API call

POST	8	Ŷ	http	s://{{server}}/restc	conf/data/nsp	o-oam-cor	nfig:oam-pm			
Params		Author	ization	Headers (11)	Body •	Scripts	Settings			
⊖ nor	ne	⊖ for	m-data	○ x-www-form	-urlencoded	o raw	🔿 binary	🔿 Graph <mark>Q</mark> L	JSON	~
1	Ł									
2	÷	"bin	n-group	)s"•∶•[•{						
з	-+		··· "bin	-group-id":2						
4	+		··· "ne-	id" : "92.168.	99.6",					
5	+	6.4.8.4	· · "adm	in-state" : "e	nable",					
6	4	1.1.1.1	- "dep	loyment-asynch	ronous" :	false,				
7	-+	1454	des"	cription" : "0	AM-PM Bin	Group us	sed for TW	AMP-Light Te	sts".	
8			"bin	-type".:.[	aste tel televition		and also here	ne stelledi	100	
0				E						
10			2	"bio matria"	1					
10				"big" . F	. 10 ,					
11				DIU						
12	1			1	10 I I					
13	1			bin-numbe	r"•:•1,					
14	Ť			"lower-bou	nd" : 5500	1				
15	1		-p 1 - p	3,						
16	1	11111	+ . +	£						
17	7			···· bin-numbe	r"•:•2,					
18	4		1.1.1.1.1.1	lower-bou	nd" : 1100	0				
19	4.1	21,222	and the	3-]						
20	4									
21										
22	1			"bin-metric"	"fdr"					
22				"bin"	. 101 /					
20				DTU . L						
24	1			2	W					
25	1			bin-numbe	r"•:•1,					
26	T.			lower-bou	nd" : 5500	)				
27	1			3-]						
28	+		····},	11. CS						
29	÷		1.0.0	E						
30	+		(1,1,2,2,2,2)	"bin-metric"	·: "ifdv",					
31	-+			"bin" : [						
32	+			ξ.						
33	-+			bin-numbe	r"-:-1.					
34				"lower-bou	nd" : 5500					
35		101210	41	3-1	10000					
36				<b>۲</b> ډ						
20			5							
37	1		1							
38	ţ,	3 ]								
39	3									
4.63	1.0									

Repeat this step for all NEs, updating the ne-id attribute.

2 Configure a TWAMP-Light reflector for each NE. Note the udp-port attribute. Example API call

POST	r v https://{{server}}/restconf/data/nsp-oam-config:oam-pm
Params	s Authorization Headers (11) Body Scripts Settings
() noi	ne 🔿 form-data 🔿 x-www-form-urlencoded 🧿 raw 🔿 binary 🔿 GraphQL 🛛 JSON 🗸
1	Ę
2	"twamp-light-reflector-rtr": [
з	
4	""""""""""""""""""""""""""""""""""""""
5	"admin-state": "enable",
6	"description": "OAM TWL Base Routing Instance Reflector",
7	"udp-port": 64372,
8	"prefix": [
9	
10	·····"ip-prefix": "0.0.0.0/0",
11	"description": "Reflector for all prefixes"
12	n n n n n n n n n n n n n n n n n n n
13	
14	
15	eos]
16	3

Repeat this step for all NEs, updating the ne-id attribute.

END OF STEPS

# 9.15 Create a TWAMP Light test session

# 9.15.1 Purpose

Use this procedure to provision TWAMP Light tests for each link in the network, where the source of the latency information is OAM.

This procedure is based on the procedure to configure an OAM test in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedure in NSP Release 24.4 is How do I create an OAM test?.

# 9.15.2 Steps

Log in to the NSP.
Open Data Collection and Analysis Management, Tests.
Click + TEST.
In the Create OAM Test form that opens, select Twamp-light in the Test type field. Enter the link details in the entity identification parameters.
Choose a the Delay Streaming (proactive) test template. The test parameters are displayed.
<ul> <li>Configure the required test parameters:</li> <li>The Destination UDP port must match the UDP port used when the TWAMP Light reflector was created in Step 2 of 9.14 "Configure OAM configuration objects using an API" (p. 472).</li> <li>The Bin group must match the bin group ID created in Step 1 of 9.14 "Configure OAM configuration objects using an API" (p. 472).</li> <li>The Execute type parameter must be Proactive.</li> <li>The Record stats parameter must be Delay.</li> <li>In Note: If the required parameters are not visible or configurable in the form on the UI, you can edit the proactive system template to customize the test creation form; see How do I edit an OAM test template?</li> </ul>
Click <b>CREATE</b> . The test appears in the list of tests.
Repeat this procedure to create additional TWAMP Light session tests for other links in the network

END OF STEPS

### Example test configuration

Create OAM Test	TWL_Test_CE_West_Seattle_1
Test type	
Twamp-light	•
Entity type	
Network Interface Ad	dress 👻
Entity reference type	
ipv4	•
Source test entity	
Q 92.168.99.6 toSe	eattleInt1
Destination test entity	
Q 92.168.96.190 to	bCE_WestInt1
Template	
Delay Streaming (pro	active) 👻
Name*	
TWL_Test_CE_West_S	Seattle_1
Test ID 🚯	
Destination UDP port 🚯	
64372	
Bin group 🚯	
2	

∧ Advanced	
Admin state	
Disable	
App ID	
NSP	
Bin group	
2	
Bulk result	
True	
CHLI threshold	
5	
Consecutive delta-T	
10	
Deployment asynchronous	
True	
Destination UDP port	
64372	
<b>Execute type</b> Proactive	

F	LR threshold
5	50
F	rames per delta-T
1	I
h	nterval
1	1000
Ν	1easurement interval
5	5
N	Name
٦	<pre>FWL_Test_CE_West_Seattle_1</pre>
N	Notify target NE
Ν	Vever
_	
R	Record stats
	Delay
L	
F	Router instance
E	Base
S	Sample window
6	50
S	Streaming template
c	default

# 9.16.1 Purpose

Use this procedure to execute the TWAMP Light tests created in 9.15 "Create a TWAMP Light test session " (p. 474).

This procedure is based on the procedures to execute an OAM test and view results of an OAM test, in the *NSP Data Collection and Analysis Guide*.

For example, the reference procedures in NSP Release 24.4 are:

- How do I execute an OAM test?
- How do I view OAM test results?

# 9.16.2 Steps

1 \_\_\_\_\_

Log in to the NSP.

2 -

Open Data Collection and Analysis Management, Tests.

3 -

In the **Filter** column at the left of the view, select Twamp-Light in the Test type field and click **RETRIEVE**. The list of TWAMP-Light tests is populated.

4

Choose a test and click **‡** (Table row actions), **Execute**. The Execute dialogue opens.

5 \_\_\_\_\_

Configure the required parameters and click **EXECUTE**.

- The Sync mode parameter specifies whether or not execution requests generate notifications in the UI. The **Sync-execute** option (default) provides a notification if the execution fails.
- The Result Classifier parameter specifies the name of the result classifier used to determine test success or failure. Result classifiers are configurable using a REST API.
   Check the **Perform result classification** check box to apply the classifications.
- The **Publish results** check box publishes results to Kafka.

**i** Note: The execution of a test auto-generates telemetry subscriptions. Auto-generated subscriptions can be identified in the Data Collection and Analysis Management, Subscriptions view by their names. The subscription name format is TestSuiteEx\_ OAM-PM-test\_type-statistic-type; for example, the subscription for Twamp-light delay streaming statistics would be named TestSuiteEx\_OAM-PM-TWAMP-streaming. Do not edit or delete these subscriptions.

 The Save results to database check box makes results available to the NSP UI. If this box is not checked, the UI does not display results of the test.

6

To view results of a test, select the test and click (Table row actions), **View Results**.

The Test executions page opens, showing the executions and their results.



**i** Note: After a test has executed, there is a brief processing delay before results are available. For tests that have just finished running, Nokia recommends that you wait a minimum of 5 s before viewing results.

### **Results example**

|--|

Last 1 day	▼ telemetr	y:/base/oam-pm/twamp-light-i			Refresh Results				
Test execution ID	Result classification	Record stats	Time captured	Direction	Metric ID	Delay	Service ID	Rease :	
5	Passed	delay	2024-07-15 15:14:55	Round-trip	fd-average	7202		A	
5	Passed	delay	2024-07-15 15:14:45	Round-trip	fd-average	9799			
5	🤣 Passed	delay	2024-07-15 15:14:35	Round-trip	fd-average	10066			
5	Passed	delay	2024-07-15 15:14:25	Round-trip	fd-average	28181			
5	Passed	delay	2024-07-15 15:14:15	Round-trip	fd-average	19146			
5	Passed	delay	2024-07-15 15:14:05	Round-trip	fd-average	23198			
5	Passed	delay	2024-07-15 15:13:55	Round-trip	fd-average	27919			
5	Passed	delay	2024-07-15 15:13:45	Round-trip	fd-average	14905			
5	Passed	delay	2024-07-15 15:13:35	Round-trip	fd-average	28557			
5	Passed	delay	2024-07-15 15:13:25	Round-trip	fd-average	38794			
5	Passed	delay	2024-07-15 15:13:15	Round-trip	fd-average	31855			
5	Passed	delay	2024-07-15 15:13:05	Round-trip	fd-average	7678			
5	Passed	delay	2024-07-15 15:12:55	Round-trip	fd-average	25179			
5	Passed	delay	2024-07-15 15:12:45	Round-trip	fd-average	27784			
5	Passed	delay	2024-07-15 15:12:35	Round-trip	fd-average	12040			

END OF STEPS

#### Enable latency parameters using an API 9.17

# 9.17.1 Allow Path Control to receive the bandwidth measurements from the network

Now that the tests are running, the next step is to allow latency collection in NSP's Path Control module. By default, Path Control's latency configuration is displayed. To enable latency collection in Path Control, a specific NSP Path Control API call is used.

For more information about the API, see the Swagger documentation for the NSP Path Control API on the Nokia Developer Portal.

See the following example:

Params	Authorization	Headers (11)	Body •	Scripts	Settings			
Granna	- Hattencoulon	11000010 (11)		oonpro	ootnigo			
O nor	ne 🔘 form-data	○ x-www-form-	-urlencoded	O raw	🔿 binary	🔿 GraphQL	JSON	Y
1	ş							
2	"data": {							
з	"classic":	false,						
4	"modelDriv	en": true,						
5	"neat": fa	lse,						
6	"timeout":	- {						
7	"enabled	": false,						
8	"expired	Ttl": 1800,						
9	"staleTt	1": 300						
	2							
10	5							
10 11	- }							

In this example, the "modelDriven" parameter is the parameter to be enabled. That is because we need Path Control to report link latency based on the measurements coming from Data Collection and Analysis Management.

When the call is successful, real-time latency measurements in Path Control for both LSP and link objects are displayed. The measurements are updated approximately every minute.

Path Control Links	•									
Reservation (%) =	Source	IP Address	Operation	Admin	Latency (microseconds)	1	Available Bandwidth (Mbps)	Bandwidth (Mbps)	Measured (Mbps)	IP BW
	CE_West ×		•	•		T	· · · · · · · · · · · · · · · · · · ·		T	
• 0	CE_West	20.20.22.5	Up	Up	• 14829		10000	10000		:
• 0	CE_West	20.20.20.1	Up	Up	1408		10000	10000		:
• 0	CE_West	20.20.20.5	Up	Up	• 1692		10000	10000		:
• 0	CE_West	20.20.22.1	Up	Up	• 3417		10000	10000		:

Path Control LSPs

LSP Name	Administration	Operation	Path Type	Source NE Name	Destination NE Name	Latency (microseconds)	Delegated :
toCE ×	•	-	•			T	•
toCE_East::toCE_East_loose	Up	Up	RSVP	CE_West	CE_East	1601	✓ :
toCE_West::toCE_West_loose	Up	Up	RSVP	CE_East	CE_West	20277	✓ :
toCE_East_2::toCE_East_2_loose	Up	Up	RSVP	CE_West	CE_East	1601	× :
toCE_East_IETF::toCE_East_IETF_loose	Up	Up	RSVP	CE_West	CE_East	1376	✓ :
toCE_West_2::toCE_West_2_loose	Up	Up	RSVP	CE_East	CE_West	20277	× :
toCE_West_IETF::toCE_West_IETF_loose	Up	Up	RSVP	CE_East	CE_West	20277	✓ :

#### **Monitor latency** 9.18

# 9.18.1 Monitoring LSPs in Path Control

Open the Path Control, LSPs and select an LSP.

- The Hops panel in the Info panel shows the LSP paths. Pay close attention to the current path the LSPs of interest are taking to reach the destination.
- · The Latency column shows the measured latency in microseconds.

Click (Table row actions), **Show on map** to display the LSP in a network map format.



Click on a link to display link information in the Info panel.

NSP

# 9.18.2 Monitoring links in Path Control

From the network map view of the LSP, click on a highlighted link to display link information in the Info panel.



Open the **Path Control**, **Links** view and select a link.

The Latency column shows the measured latency in microseconds. The Latency information in the Info panel provides further details about recorded latency measurements. Path Control considers three possible sources (API, OAM, and NFM-P). The measurements shown in this example are coming from MD-OAM, as expected.

Furthermore, as shown here, latency values can be configured manually via APIs. If latency values are coming from both API and OAM/NFM-P sources, latency values or measurements from API calls will take precedence over OAM and NFM-P.

Latency (OAM) 1385 microseconds	
API O microseconds OAM • 1385 microseconds Last updated: Jul 19, 2024 10:57:48 AM NFM-P O microseconds	

From the selected link, click (Table row actions), **LSPs on Link** to see the list of LSPs on the selected link.

Path Control > Link 20.20.20.5 LSPs of	n Link								
LSP Name	Administration	Operation	Path Type	Delegated	NSP Initiated	Active	Source NE IP = Address	Source NE Name	:
		•	•	•	•	•			
toCE_East::toCE_East_loose	Up	Up	RSVP	$\checkmark$	-	$\checkmark$	92.168.99.6	CE_West	:
toCE_East_2::toCE_East_2_loose	Up	Up	RSVP	$\checkmark$	-	$\checkmark$	92.168.99.6	CE_West	:
toCE_East_IETF::toCE_East_IETF_loose	Up	Up	RSVP	$\checkmark$		$\checkmark$	92.168.99.6	CE_West	:

# 9.19 Latency-based optimization

# 9.19.1 Link rerouting

After injecting latency on a particular link beyond the configured threshold (i.e. 90,000 microseconds in this example), we can see that the LSPs that were using the link have been rerouted, bypassing the link with the high latency value.

**i** Note: To demonstrate this particular use case on a lab setup, the link latency was manually configured on a link via API, overriding the value obtained from the OAM tests. In a real network, if there is congestion or network-related performance problems, the latency measurements coming from the OAM source are expected to fluctuate, sometimes exceeding the configured link threshold values.

### Example, before optimization:

≡ NO <ia ne<="" th=""><th>twork Services Platf</th><th>form</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></ia>	twork Services Platf	form													
Path Control Links		÷													
Reservation (%) ==	Source		IP Address	Operation		Admin	Latency (microseconds)	Available Ban (Mbps)	dwidth	Bandwidth (Mbps)	Measured IP BW (Mbps)		Measured MPLS BW (Mbps)		Measured MPL ; BW (Mbps) ;
	CE_West	×			•	•	Т		Т	Т		T		Ŧ	
• 0	CE_West		20.20.22.5	Up		Up	• 10460		10000	10000		0		0	;
• 0	CE_West		20.20.20.1	Up		Up	• 1767		10000	10000		0		0	:
• 0	CE_West		20.20.20.5	Up		Up	120000		10000	10000		0		0	:
• 0	CE_West		20.20.22.1	Up		Up	• 11841		10000	10000		0		0	:



The latency measurement from the API, 120000 microseconds, is taking precedence over the OAM measurement of 1608 microseconds.

### Example, after optimization:

	etwork Services Platform						
Path Control > 20.20	LSPs on Link						
LSP Name	Administration =	Operation	Path Type	Delegated	NSP Initiated	Active	Source N
	•	•	•	•	•	•	

The LSPs are no longer using this link to reach the destination.

View the LSP in the **Path Control**, **LSPs** view to see the new set of hops. For reference, the previous hops were:

- Hop 1: 20.20.20.5
- Hop 2: 20.20.20.6
- Hop 3: 10.10.12.2
- Hop 4: 10.10.17.5
- Hop 5: 20.20.23.1

May 2025

Issue 4

Hops	
20.20.20.1 Hop 1	^
Router 92.168.99.6	
Admin Domain TopologyId-0:0:0	
Local Protection Available None	
Local Protection In Use False	
20.20.20.2 Hop 2	^
Label 524251	
Router 92.168.98.97	
Admin Domain TopologyId-0:0:0	
Local Protection Available None	
Local Protection In Use False	
10.10.12.14 Hop 3	^
Label 524264	
Router 92.168.96.93	
Admin Domain TopologyId-0:0:0	
Local Protection Available None	
Local Protection In Use False	



# 9.19.2 Network map views

The change to the path is clear in the network map.

Network map example, before optimization:

Issue 4



Network map example, after optimization:



# 9.20 System activity logging after latency optimization

# 9.20.1 Monitor events in real time

To view system event logs, open the Path Control, System Activity Logging view.

The logs show the latency optimization operation on the links, as seen in the following example:

### UCC-33: LSP Enhanced Path Control Use case 2: Latency-based optimization System activity logging after latency optimization

Path Control System Activity Logging	•			
Creation Date & Time =	Category	Source	Target	Log message
Jul 21, 2024 08:44:16 AM-Jul 22, 2024 08:44:16	-		toCE_East ×	
Jul 22, 2024 08:42:29 AM	LSP	92.168.99.6	toCE_East_IETF::toCE	Received PCEP Report, LSP parameters updated
Jul 22, 2024 08:42:29 AM	LSP	92.168.99.6	toCE_East::toCE_East	Received PCEP Report, LSP parameters updated
Jul 22, 2024 08:42:29 AM	LSP	92.168.99.6	toCE_East_2::toCE_Ea	Received PCEP Report, LSP parameters updated
Jul 22, 2024 08:42:28 AM	LSP	92.168.99.6	toCE_East_2::toCE_Ea	Calculation found new path, sending PCEP update. Reason: [PathChanged], Trigger: SE
Jul 22, 2024 08:42:28 AM	LSP	92.168.99.6	toCE_East_IETF::toCE	Calculation found new path, sending PCEP update. Reason: [PathChanged], Trigger: SE
Jul 22, 2024 08:42:28 AM	LSP	92.168.99.6	toCE_East::toCE_East	Calculation found new path, sending PCEP update. Reason: [PathChanged], Trigger: SE
Jul 22, 2024 08:42:28 AM	ALGO	92.168.99.6	toCE_East_2::toCE_Ea	Path calculation success
Jul 22, 2024 08:42:28 AM	ALGO	92.168.99.6	toCE_East_IETF::toCE	Path calculation success
Jul 22, 2024 08:42:28 AM	ALGO	92.168.99.6	toCE_East::toCE_East	Path calculation success
Jul 22, 2024 08:42:27 AM	LSP	92.168.99.6	toCE_East_IETF::toCE	LSP reroute initiated due to [[LATENCY_INC]]
Jul 22, 2024 08:42:27 AM	LSP	92.168.99.6	toCE_East_2::toCE_Ea	LSP reroute initiated due to [[LATENCY_INC]]
Jul 22, 2024 08:42:27 AM	LSP	92.168.99.6	toCE_East::toCE_East	LSP reroute initiated due to [[LATENCY_INC]]
Jul 22, 2024 08:41:46 AM	LSP	92.168.99.6	toCE_East_2::toCE_Ea	Received PCEP Report, LSP parameters updated