

# NSP Network Services Platform Release 24.8

# **Troubleshooting Guide**

3HE-20033-AAAB-TQZZA Issue 2 July 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

out this	document	9
rt I: Tro	ubleshooting overview	11
NSP tr	oubleshooting overview	13
1.1	Overview	13
1.2	The troubleshooting process	14
1.3	NSP and NFM-P troubleshooting tools	17
1.4	Process to troubleshoot a problem in the NSP	19
Obtain	ing Technical Assistance	
2.1	Before you call support	25
rt II: Tro	publeshooting the system	27
Troubl	eshooting the NSP platform	
3.1	To collect NSP log files	29
3.2	To retrieve a list of pods	30
3.3	To retrieve pod information	30
3.4	To recover pods	30
3.5	To recover executor pods	31
3.6	To retrieve a list of cluster members	
3.7	To retrieve cluster member information	
3.8	To retrieve detailed information about MDM servers	
3.9	To rebalance NE load on MDM servers	
3.10	To verify disk performance for etcd	35
3.11	To verify disk performance for NSP	
3.12	Problem: NSP data synchronization is not 100%	
3.13	Problem: Alarms not appearing for rapidly reoccurring faults	
Troubl	eshooting the NFM-P platform	41
4.1	Overview	41
Troubl	eshooting the NFM-P	
4.2	To collect NFM-P log files	44
4.3	Problem: Poor performance on a RHEL station	46
4.4	Problem: Device discovery fails because of exceeded ARP cache	48
	rt I: Tro NSP tr 1.1 1.2 1.3 1.4 Obtain 2.1 rt II: Tro Troubl 3.1 3.2 3.3 3.4 3.5 3.6 3.7 3.8 3.9 3.10 3.11 3.12 3.13 Troubl 4.1 Troubl 4.1 Troubl 4.2 4.3	1.2       The troubleshooting process.         1.3       NSP and NFM-P troubleshooting tools.         1.4       Process to troubleshoot a problem in the NSP.         Obtaining Technical Assistance

Troubles	shooting using the LogViewer	.51
4.5	LogViewer overview	.51
4.6	LogViewer GUI and Quick Links panel	.52
4.7	LogViewer CLI	.53
4.8	To display logs using the LogViewer GUI	.53
4.9	To configure the LogViewer using the GUI	.58
4.10	To search log files in a path	.61
4.11	To show or hide buttons from the LogViewer main tool bar	.62
4.12	To set highlight colors and fonts for LogViewer components and levels	.63
4.13	To automatically show or hide log messages	.64
4.14	To manage filters using the GUI Filter Manager	.65
4.15	To specify a plug-in using the LogViewer GUI	.67
4.16	To display logs using the LogViewer CLI	.68
4.17	To configure the LogViewer CLI	.72
4.18	To specify plug-ins using the CLI	.74
Troubles	shooting the NFM-P database	.75
4.19	Database troubleshooting overview	.75
4.20	Problem: NFM-P database corruption or failure	.75
4.21	Problem: The database is running out of disk space	.76
4.22	Problem: Frequent database backups create performance issues	.77
4.23	Problem: An NFM-P database restore fails and generates a No backup sets error	
4.24	Problem: NFM-P database redundancy failure	
4.25	Problem: Primary or standby NFM-P database is down	.79
4.26	Problem: Need to verify that Oracle database and listener services are started	
4.27	Problem: Need to determine status or version of NFM-P database or Oracle proxy	
	shooting NFM-P server issues	
4.28	NFM-P server troubleshooting overview	
4.29	Problem: Cannot start an NFM-P server, or unsure of NFM-P server status	
4.30	Problem: NFM-P server and database not communicating	
4.31	Problem: An NFM-P server starts up, and then quickly shuts down	
4.32	Problem: Client not receiving server heartbeat messages	
4.33	Problem: Main server unreachable from RHEL client station	
4.34	Problem: Excessive NFM-P server-to-client response time	
4.35	Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded	
4.36	Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP	
4.07	traps are arriving	
4.37	Cannot manage new devices	.92

NSP

	4.38	Problem: Cannot discover more than one device, or device resynchronization fails	93
	4.39	Problem: Slow or failed resynchronization with network devices	94
	4.40	Problem: Statistics are rolling over too quickly	95
	4.41	Problem: Y.1564 service test results not published to Kafka	96
	Trouble	eshooting NFM-P clients	98
	4.42	Problem: Cannot start NFM-P client, or error message during client startup	98
	4.43	Problem: NFM-P client unable to communicate with NFM-P server	99
	4.44	Problem: Delayed server response to client activity	100
	4.45	Problem: Cannot place newly discovered device in managed state	101
	4.46	Problem: User performs action, such as saving a configuration, but cannot see any results	102
	4.47	Problem: Device configuration backup not occurring	104
	4.48	Problem: NFM-P client GUI shuts down regularly	105
	4.49	Problem: Configuration change not displayed on NFM-P client GUI	106
	4.50	Problem: List or search function takes too long to complete	106
	4.51	Problem: Cannot select some menu options or save some configurations	107
	4.52	Problem: The NFM-P client GUI does not display NE user accounts created, modified, or del	eted
		using the CLI	107
Pa	rt III: Tro	ubleshooting the network	109
5	Networ	k troubleshooting using NSP functions	111
	5.1	Overview	111
	Trouble	eshooting using NSP assurance functions	112
	5.2	Troubleshooting services and connectivity	112
	5.3	Onboarding an NE into NSP	113
	5.4	Onboarding a service into NSP	155
	5.5	LSP Throughput with Forecast reporting scenario	175
	5.6	SAP Throughput reporting scenario	<b>194</b>
	5.7	End-to-end NE troubleshooting scenario	215
	5.8	End-to-end service troubleshooting scenario	240
	5.9	End-to-end link troubleshooting scenario	<b>268</b>
	5.10	End-to-end port troubleshooting scenario	289
	Trouble	eshooting using Analytics	319
	5.11	Analytics troubleshooting overview	319
	5.12	Troubleshooting data collection	319
	5.13	Troubleshooting data storage	322
	5.14	Troubleshooting Analytics reporting	322

	Troubleshooting using NSP workflows		
	5.15	Evaluating failed or slow workflow executions	324
6	Netwo	rk troubleshooting using NFM-P	331
	6.1	Overview	
	Troubl	eshooting services and connectivity	333
	6.2	Service and connectivity diagnostics	333
	6.3	Workflow to troubleshoot a service or connectivity problem	333
	6.4	To identify whether a VPLS is part of an H-VPLS	335
	6.5	To verify the operational and administrative states of service components	336
	6.6	To verify the FIB configuration	337
	6.7	To verify connectivity for all egress points in a service using MAC Ping and MAC Trace	338
	6.8	To verify connectivity for all egress points in a service using MEF MAC Ping	340
	6.9	To measure frame transmission size on a service using MTU Ping	342
	6.10	To verify the end-to-end connectivity of a service using Service Site Ping	343
	6.11	To verify the end-to-end connectivity of a service tunnel using Tunnel Ping	345
	6.12	To verify end-to-end connectivity of an MPLS LSP using LSP Ping	347
	6.13	To review the route for an MPLS LSP using LSP Trace	349
	6.14	To review ACL filter properties	350
	6.15	To view anti-spoof filters	351
	6.16	To retrieve MIB information from a GNE using the snmpDump utility	352
	Troubl	eshooting using the NE resync audit function	354
	6.17	NE resync auditing overview	354
	6.18	Workflow for NE resync auditing	355
	6.19	To clear a Frame Size Problem (MTU Mismatch) alarm	355
	6.20	To perform an NE resync audit	356
	6.21	To view NE resync audit results using the NE audit manager	357
	Troubl	eshooting network management LAN issues	359
	6.22	Problem: All network management domain stations experience performance degradation	359
	6.23	Problem: Lost connectivity to one or more network management domain stations	359
	6.24	Problem: Another station can be pinged, but some functions are unavailable	
	6.25	Problem: Packet size and fragmentation issues	361
	Troubl	eshooting using NFM-P client GUI warning messages	
	6.26	Client GUI warning message overview	363
	6.27	To respond to a GUI warning message	364

Trouble	shooting with Problems Encountered forms	
6.28	Overview	
6.29	To view additional problem information	
6.30	To collect problem information for technical support	
Trouble	shooting using the NFM-P user activity log	
6.31	User activity log overview	
6.32	To identify the user activity for a network object	
6.33	To identify the user activity for an NFM-P object	
6.34	To navigate to the object of a user action	
6.35	To view the user activity records of an object	
6.36	To view the user activity performed during a user session	

# About this document

## Purpose

The *NSP Troubleshooting Guide* provides information about using NSP, NFM-P tools, and other functions to troubleshoot customer services and the NSP network management domain.

## Scope

The scope of this document is limited to the NSP application and the NFM-P. Many configuration, monitoring, and assurance functions are delivered by NSP. Help for all of these NSP functions is available in the NSP Help Center. The content in this document is divided by relevance to the NSP and NFM-P.

## 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.

# Part I: Troubleshooting overview

## Overview

## Purpose

This part provides an overview of NSP troubleshooting.

## Contents

Chapter 1, NSP troubleshooting overview	13
Chapter 2, Obtaining Technical Assistance	25

# **1** NSP troubleshooting overview

## 1.1 Overview

## **1.1.1 General information**

This chapter provides information about the troubleshooting process, guidelines, and tools, along with a process for troubleshooting a problem in the NSP.

The *NSP Troubleshooting Guide* is intended for NOC operators and engineers who are responsible for identifying and resolving NSP performance issues. The guide contains troubleshooting information for the following domains:

- managed network
- NSP functions
- NSP platform
- NFM-P platform

## 1.1.2 Managed network troubleshooting

The NSP has a number of powerful troubleshooting functions and dashboards that help to quickly pinpoint the root cause of network and service management problems to speed resolution.

You can use the NSP alarm and service monitoring functions to help you troubleshoot the network of managed NEs.

#### Alarms for network objects

The NSP raises alarms against network objects in response to received SNMP traps from managed NEs. You can then use the alarms function to correlate the events and alarms to the managed object, configured services and policies. A correlated event or alarm can cause fault conditions on multiple network objects and services. For example, an alarm raised for a port failure causes alarms on all services that use the port. You can view the alarm notification from the Network Health dashboard.

## 1.1.3 Platform troubleshooting

You can troubleshoot NSP platform issues that include the following:

- slow system response, poor performance, or excessive disk activity
- database failure, corruption, disk capacity, or performance degradation
- server communication problems, slow response, system alarms or statistics of concern, or inability to manage new devices

## 1.2 The troubleshooting process

### 1.2.1 Identifying network performance issues

The troubleshooting process identifies and resolves performance issues related to a network service or component. The performance issue can result in service degradation, or in a complete network failure.

The first step in problem resolution is to identify the problem. Problem identification can include an alarm received from a network component, an analysis of network capacity and performance data, or a customer problem report.

The personnel responsible for troubleshooting the problem must:

- understand the designed state and behavior of the network, and the services that use the network
- recognize and identify symptoms that impact the intended function and performance of the product

#### 1.2.2 Network maintenance

The most effective method to prevent problems is to schedule and perform routine maintenance on your network. Major networking problems often start as minor performance issues. See the *NSP System Administrator Guide* for more information about how to perform routine maintenance on your network.

## 1.2.3 Troubleshooting problem-solving model

An effective troubleshooting problem-solving model includes the following tasks:

- 1. "Establish a performance baseline" (p. 14).
- 2. "Categorize the problem" (p. 15).
- 3. "Identify the root cause of the problem" (p. 15).
- 4. "Plan corrective action and resolve the problem" (p. 16).
- 5. "Verify the solution to the problem" (p. 16).

See 1.4 "Process to troubleshoot a problem in the NSP" (p. 19) for information about how the problem-solving model aligns with using the NSP to troubleshoot a network or network management problem.

#### Establish a performance baseline

You must have a thorough knowledge of your network and how it operates under normal conditions to troubleshoot problems effectively. This knowledge facilitates the identification of fault conditions in your network. You must establish and maintain baseline information for your network and services. The maintenance of the baseline information is critical because a network is not a static environment.

See the *NSP System Administrator Guide* for more information on how to generate NSP system baseline information.

#### Categorize the problem

When you categorize a problem, you must differentiate between total failures and problems that result in a degradation in performance. For example, the failure of an access switch results in a total failure for a customer who has one DS3 link into a network. A core router that operates at over 80% average utilization can start to discard packets, which results in a degradation of performance for services that use the device. Performance degradations exhibit different symptoms from total failures and may not generate alarms or significant network events.

Multiple problems can simultaneously occur and create related or unique symptoms. Detailed information about the symptoms that are associated with the problem helps the NOC or engineering operational staff diagnose and fix the problem. The following information can help you assess the scope of the problem:

- alarm files
- error logs
- network statistics
- network analyzer traces

- output of CLI show commands
- accounting logs
- customer problem reports

Use the following guidelines to help you categorize the problem:

- · Is the problem intermittent or static?
- · Is there a pattern associated with intermittent problems?
- · Is there an alarm or network event that is associated with the problem?
- · Is there congestion in the routers or network links?
- · Has there been a change in the network since proper function?

#### Identify the root cause of the problem

A symptom for a problem can be the result of more than one network issue. You can resolve multiple, related problems by resolving the root cause of the problem.

Use the following guidelines to help you implement a systematic approach to resolve the root cause of the problem:

- · Identify common symptoms across different areas of the network.
- · Focus on the resolution of a specific problem.
- Divide the problem based on network segments and try to isolate the problem to one of the segments.

Examples of network segments are:

- LAN switching (edge access)
- LAN routing (distribution, core)
- metropolitan area
- WAN (national backbone)
- partner services (extranet)
- remote access services
- Determine the network state before the problem appeared.

• Extrapolate from network alarms and network events the cause of the symptoms. Try to reproduce the problem.

#### Plan corrective action and resolve the problem

The corrective action required to resolve a problem depends on the problem type. The problem severity and associated QoS commitments affect the approach to resolving the problem. You must balance the risk of creating further service interruptions against restoring service in the shortest possible time.

Corrective action should:

- 1. Document each step of the corrective action.
- 2. Test the corrective action.
- 3. Use the CLI to verify behavior changes in each step.
- 4. Apply the corrective action to the live network.
- 5. Test to verify that the corrective action resolved the problem.

#### Verify the solution to the problem

You must make sure that the corrective action associated with the resolution of the problem did not introduce new symptoms in your network. If new symptoms are detected, or if the problem has only recently been mitigated, you need to repeat the troubleshooting process.

### 1.2.4 Checklist for identifying problems

When a problem is identified in the network management domain, track and store data to use for troubleshooting purposes:

• Determine the type of problem.

Review the sequence of events before the problem occurred:

- Trace the actions that were performed to see where the problem occurred.
- Identify what changed before the problem occurred.
- Determine whether the problem happened before under similar conditions.
- Check the documentation or your procedural information to verify that the steps you performed followed documented standards and procedures.
- Check the alarm log for any generated alarms that are related to the problem.
- Record any system-generated messages, such as error dialog boxes, for future troubleshooting.
- If you receive an error message, perform the actions recommended in the error dialog box, client GUI dialog box, SOAP exception response, or event notification.

During troubleshooting:

- · Keep both the Nokia documentation and your company policies and procedures nearby.
- Check the appropriate release notice from the Nokia Support Documentation Service for any release-specific problems, restrictions, or usage recommendations that relate to your problem.

- If you need help, confirmation, or advice, contact your TAC or technical support representative. See Table 1-1, "General NSP problem types" (p. 20) to collect the appropriate information before you call support.
- Contact your TAC or technical support representative if your company guidelines conflict with Nokia documentation recommendations or procedures.
- Perform troubleshooting based on your network requirements.

## 1.3 NSP and NFM-P troubleshooting tools

## 1.3.1 NSP troubleshooting tools

NSP provides various functions and dashboards that can help your troubleshoot network, provide various alarm details, and see the network health.

#### Network Health dashboard

The Network Health dashboard provides a quick view of essential information relating to the proper function of your network. It presents an abbreviated view of equipment and service alarms, root cause alarms, graphical plots of service-affecting network object counts, and network object status.

#### **Troubleshooting dashboard**

The Troubleshooting dashboard provides the user with a centralized view of network equipment and service performance. The dashboard allows a network operator to view summarized performance information, and to drill down into specific objects and view performance details, opening objects in NSP functions where necessary. See the *NSP User Guide* for more information.

#### Assurance functions

Various NSP assurance and analysis functions are available..

#### **Current Alarms**

The alarms management function provides alarm monitoring, correlation, and troubleshooting for the most unhealthy network elements (NE) in the network. You can diagnose problems using various alarm management tools. See the *NSP Network and Service Assurance Guide*.

#### **Data Collection and Analysis**

NSP Analytics uses business intelligence software to generate graphical and tabular reports, based on the aggregate statistical data and telemetry collected from NEs. There are four categories of reports available to you: Network and service, Application assurance, Administration, and NSP. See the *NSP Analytics Report Catalog* for more information.

### Network and service assurance

The network and service assurance functions help you to monitor the health of core, access, transport, and optical NEs and virtual NFs using a combined NE matrix, pre-defined KPIs, alarms, event timeline, and network map. See the *NSP Network and Service Assurance Guide* for more information.

## 1.3.2 NFM-P troubleshooting tools

The NFM-P supports a number of troubleshooting tools and event logs to help identify the root cause of a network or network management problem.

#### **OAM** diagnostics

The NFM-P supports configurable in-band and out-of-band, packet-based OAM diagnostic tools for network troubleshooting and for verifying compliance with SLAs. See 6.2.1 "STM OAM diagnostics for troubleshooting" (p. 333) for more information.

#### **Ethernet CFM diagnostics**

Ethernet CFM diagnostic tests detect connectivity failures between pairs of local and remote maintenance end points, or MEPs, in a MEG. Each MEP is a reference point that can initiate or terminate one of the following diagnostic tests:

- CFM continuity check
- CFM loopback
- CFM link trace
- CFM Eth test
- CFM two-way delay

- CFM one-way delay
- CFM single-ended loss (7705 SAR only)
- CFM two-way SLM

See the NSP NFM-P Classic Management User Guide for more information about Ethernet CFM diagnostic.

#### **RCA** audit tool

The NFM-P RCA audit tool allows you to perform on-demand or scheduled verifications of the configuration of services and physical links to identify possible configuration problems. Except for physical links, the NFM-P provides a solution, which, at your request, can automatically be implemented to make all the required configuration changes.

You can perform RCA audits of the following objects:

- VLL services
- VPLSs
- VPRN services
- physical links
- OSPF interfaces, areas, and area sites (NFM-P/CPAM integration only)
- IS-IS interfaces and sites (NFM-P/CPAM integration only)

See the NSP NFM-P Classic Management User Guide for more information about the RCA audit tool.

#### **NFM-P** log files

You can use NFM-P log files to help troubleshoot your network. The log files can consume a large amount of disk space during a long period of significant activity. Ensure that the contents of the various log directories are backed up on a regular basis. See the *NSP System Administrator Guide* for more information about how to perform routine NFM-P system maintenance.

**i** Note: The event log files may be overwritten or removed when you restart an NFM-P server.

#### **NFM-P LogViewer**

The NFM-P LogViewer is a system monitoring and troubleshooting utility that parses, formats, and displays the contents of NFM-P log files.

You can use LogViewer to perform the following:

- · View and filter real-time log updates.
- View, filter, and sort the entries in a static log view.
- Open compressed or uncompressed log files.
- Compare active logs in real time.
- Automatically send a notification when a specified type of entry is logged.

#### User activity log

The NFM-P records each NFM-P GUI and OSS user action. The NFM-P User Activity form allows an operator with the appropriate privilege level to list and view the NFM-P GUI and OSS client user activity, and to navigate directly to the object of a user action. You can also open a pre-filtered list of the recent activity for an object from the object properties form.

See the NSP NFM-P Classic Management User Guide for detailed information about the user activity log.

## 1.4 Process to troubleshoot a problem in the NSP

#### 1.4.1 Purpose

Perform the following high-level sequence of actions with respect to the problem-solving model described in 1.2 "The troubleshooting process" (p. 14).

## 1.4.2 Stages

#### 1

Establish an operational baseline for your network. See the *NSP System Administrator Guide* for more information.

2

When a problem occurs, identify the type of problem. The table below lists some general NSP problem types.

NSP

Table 1-1	General NSP	problem types
-----------	-------------	---------------

Туре	Example problems
Managed network	<ul> <li>alarms raised against network objects</li> <li>service degradation with no associated alarms</li> <li>problem indications on topology maps</li> </ul>
Service and network health	<ul> <li>network health issues</li> <li>error or warning messages related to configuration</li> <li>problem encountered during diagnose</li> </ul>
NSP platform	<ul> <li>pod failure</li> <li>errored cluster member</li> <li>disk capacity or performance issues</li> <li>MDM server issues</li> </ul>

3

Identify the root cause of the problem using NSP or NFM-P procedures in the document

- a. Use Table 1-2, "NSP functions and dashboards problems or tasks" (p. 20) to identify the appropriate NSP function troubleshooting procedure for the problem.
- b. Use Table 1-3, "NSP platform problems or tasks" (p. 21) to identify the appropriate NSP platform troubleshooting procedure for the problem.
- c. Use Table 1-4, "NFM-P managed NE network problems or tasks" (p. 21) to identify the appropriate NFM-P managed NE network troubleshooting procedure for the problem.
- d. Use Table 1-5, "NFM-P network management domain problems or tasks" (p. 22) to identify the appropriate NFM-P network management domain troubleshooting procedure for the problem.
- e. Use Table 1-6, "NFM-P platform problems or tasks" (p. 22) to identify the appropriate NFM-P platform troubleshooting procedure for the problem.

Table 1-2 NSP functions and dashboards problems or tasks

Problem or task		
Troubleshooting using alarms		
5.2 "Troubleshooting services and connectivity" (p. 112)		
5.4 "Onboarding a service into NSP" (p. 155)		
Troubleshooting NSP Analytics		
5.12 "Troubleshooting data collection" (p. 319)		
5.13 "Troubleshooting data storage" (p. 322)		
5.14 "Troubleshooting Analytics reporting" (p. 322)		

#### Table 1-3 NSP platform problems or tasks

Problem or task
Troubleshooting NFM-P platform problems
3.1 "To collect NSP log files" (p. 29)
3.2 "To retrieve a list of pods" (p. 30)
3.3 "To retrieve pod information" (p. 30)
3.4 "To recover pods" (p. 30)
3.5 "To recover executor pods" (p. 31)
3.6 "To retrieve a list of cluster members" (p. 32)
3.7 "To retrieve cluster member information" (p. 32)
3.8 "To retrieve detailed information about MDM servers" (p. 33)
3.9 "To rebalance NE load on MDM servers" (p. 34)
3.10 "To verify disk performance for etcd" (p. 35)
3.11 "To verify disk performance for NSP" (p. 36)
3.12 "Problem: NSP data synchronization is not 100%" (p. 38)
3.13 "Problem: Alarms not appearing for rapidly reoccurring faults" (p. 38)

#### Table 1-4 NFM-P managed NE network problems or tasks

Problem or tasks
Troubleshooting services and connectivity
6.4 "To identify whether a VPLS is part of an H-VPLS" (p. 335)
6.5 "To verify the operational and administrative states of service components" (p. 336)
6.6 "To verify the FIB configuration" (p. 337)
6.7 "To verify connectivity for all egress points in a service using MAC Ping and MAC Trace" (p. 338)
6.8 "To verify connectivity for all egress points in a service using MEF MAC Ping" (p. 340)
6.9 "To measure frame transmission size on a service using MTU Ping" (p. 342)
6.10 "To verify the end-to-end connectivity of a service using Service Site Ping" (p. 343)
6.11 "To verify the end-to-end connectivity of a service tunnel using Tunnel Ping" (p. 345)
6.12 "To verify end-to-end connectivity of an MPLS LSP using LSP Ping" (p. 347)
6.13 "To review the route for an MPLS LSP using LSP Trace" (p. 349)
6.14 "To review ACL filter properties" (p. 350)
6.15 "To view anti-spoof filters" (p. 351)
6.16 "To retrieve MIB information from a GNE using the snmpDump utility" (p. 352)

#### Table 1-5 NFM-P network management domain problems or tasks

Problem or task		
Troubleshooting network management LAN issues		
6.22 "Problem: All network management domain stations experience performance degradation" (p. 359)		
6.23 "Problem: Lost connectivity to one or more network management domain stations" (p. 359)		
6.24 "Problem: Another station can be pinged, but some functions are unavailable" (p. 360)		
6.25 "Problem: Packet size and fragmentation issues" (p. 361)		
Troubleshooting using NFM-P client GUI warning messages		
6.27 "To respond to a GUI warning message" (p. 364)		
Troubleshooting with Problem Encountered forms		
6.29 "To view additional problem information" (p. 366)		
6.30 "To collect problem information for technical support" (p. 367)		
Troubleshooting with the client activity log		
6.32 "To identify the user activity for a network object" (p. 368)		
6.33 "To identify the user activity for an NFM-P object" (p. 369)		
6.34 "To navigate to the object of a user action" (p. 370)		
6.35 "To view the user activity records of an object" (p. 371)		

#### Table 1-6 NFM-P platform problems or tasks

Problem or task
Troubleshooting NFM-P platform problems
4.2 "To collect NFM-P log files" (p. 44)
4.3 "Problem: Poor performance on a RHEL station" (p. 46)
4.4 "Problem: Device discovery fails because of exceeded ARP cache" (p. 48)
Troubleshooting with the NFM-P LogViewer
4.8 "To display logs using the LogViewer GUI" (p. 53)
4.9 "To configure the LogViewer using the GUI" (p. 58)
4.11 "To show or hide buttons from the LogViewer main tool bar" (p. 62)
4.12 "To set highlight colors and fonts for LogViewer components and levels" (p. 63)
4.13 "To automatically show or hide log messages" (p. 64)
4.14 "To manage filters using the GUI Filter Manager" (p. 65)
4.15 "To specify a plug-in using the LogViewer GUI" (p. 67)
4.16 "To display logs using the LogViewer CLI" (p. 68)
4.17 "To configure the LogViewer CLI" (p. 72)

#### *Table 1-6* NFM-P platform problems or tasks (continued)

Problem or task	
4.18 "To specify plug-ins using the CLI" (p. 74)	
Troubleshooting the NFM-P database	
4.20 "Problem: NFM-P database corruption or failure" (p. 75)	
4.21 "Problem: The database is running out of disk space" (p. 76)	
4.22 "Problem: Frequent database backups create performance issues" (p. 77)	
4.23 "Problem: An NFM-P database restore fails and generates a No backup sets error" (p. 78)	
4.24 "Problem: NFM-P database redundancy failure" (p. 78)	
4.25 "Problem: Primary or standby NFM-P database is down" (p. 79)	
4.26 "Problem: Need to verify that Oracle database and listener services are started" (p. 79)	
4.27 "Problem: Need to determine status or version of NFM-P database or Oracle proxy" (p. 80)	
Troubleshooting NFM-P server issues	
4.29 "Problem: Cannot start an NFM-P server, or unsure of NFM-P server status" (p. 82)	
4.30 "Problem: NFM-P server and database not communicating" (p. 86)	
4.31 "Problem: An NFM-P server starts up, and then quickly shuts down" (p. 87)	
4.32 "Problem: Client not receiving server heartbeat messages" (p. 87)	
4.33 "Problem: Main server unreachable from RHEL client station" (p. 88)	
4.34 "Problem: Excessive NFM-P server-to-client response time" (p. 89)	
4.35 "Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded" (p. 90)	
4.36 "Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving" (p. 91)	
4.37 "Cannot manage new devices" (p. 92)	
4.38 "Problem: Cannot discover more than one device, or device resynchronization fails" (p. 93)	
4.39 "Problem: Slow or failed resynchronization with network devices" (p. 94)	
4.40 "Problem: Statistics are rolling over too quickly" (p. 95)	
Troubleshooting NFM-P GUI and OSS clients	
4.42 "Problem: Cannot start NFM-P client, or error message during client startup" (p. 98)	
4.43 "Problem: NFM-P client unable to communicate with NFM-P server" (p. 99)	
4.44 "Problem: Delayed server response to client activity" (p. 100)	
4.45 "Problem: Cannot place newly discovered device in managed state" (p. 101)	
4.46 "Problem: User performs action, such as saving a configuration, but cannot see any results" (p. 102)	
4.47 "Problem: Device configuration backup not occurring" (p. 104)	
4.48 "Problem: NFM-P client GUI shuts down regularly" (p. 105)	

#### Table 1-6 NFM-P platform problems or tasks (continued)

4.50 "Problem: List or search function takes too long to complete" (p. 106)		
. 107)		

4 –

Plan corrective action using information in the NSP User Guide and NSP System Administrator Guide.

5

Verify the solution.

# 2 Obtaining Technical Assistance

## 2.1 Before you call support

## 2.1.1 Monitor NSP KPIs

You can use the NSP logging and monitoring functions to view the current system status using a wide variety of KPIs; see "NSP logging and monitoring" in the *NSP System Administrator Guide* for information.

## 2.1.2 Gather information

Collect the following information before you contact technical support.

Table 2-1	Required technical-support Information

Information type	Description
Issue description	<ul> <li>recent GUI or XML API operations</li> <li>screen captures or text versions of error or information messages</li> <li>actions performed in response to the issue</li> </ul>
Platform specifications	<ul> <li>NSP software Release and patch level</li> <li>NFM-P software release ID</li> <li>OS type, release, and patch level</li> <li>hardware information such as: <ul> <li>CPU type</li> <li>number of CPUs</li> <li>disk sizes, partition layouts, and RAID configuration</li> <li>amount of RAM</li> </ul> </li> </ul>
System logs	System logs are crucial for system troubleshooting; see th appropriate topic in this chapter for specific log-collection information.

## 2.1.3 To collect NSP system logs

You can run the following script to collect the log files required by technical support:

• on the deployer

/opt/nsp/NSP-CN-DEP-releaseID/NSP-CN-releaseID/tools/support/systemDebugInfo/bin/get-debug-info.bash

where releaseID is the NSP load name in the format N.n.n-rel.n, for example, 23.4.0-rel.2994

 on an NSP auxiliary database station: /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles

## 2.1.4 To collect NFM-P system logs

You can run the following scripts to collect the log files required by technical support:

- on a main server station: /opt/nsp/nfmp/server/nms/bin/getDebugFiles.bash
- on an auxiliary server station: /opt/nsp/nfmp/auxserver/nms/bin/getDebugFiles.bash
- on a main database station: /opt/nsp/nfmp/db/install/getDebugFiles.bash

## 2.1.5 Check the disk space on your deployer

A common cause of failures during patch upgrades, such as images failing to import, is due to the deployer having run out of disk space. If you experience a failure such as "Error: patch.yml experienced an error" while performing an upgrade, check your deployer's disk space.

# Part II: Troubleshooting the system

## Overview

## Purpose

This part provides information about NSP and NFM-P platform troubleshooting.

## Contents

Chapter 3, Troubleshooting the NSP platform	29
Chapter 4, Troubleshooting the NFM-P platform	41

# **3** Troubleshooting the NSP platform

# 3.1 To collect NSP log files

## 3.1.1 NSP auxiliary database

If required, use a script to collect a comprehensive set of log files.

```
1 _____
  Log in to the station as the root user.
2 —
  Open a console window.
3 —
  Enter the following:
  · On an auxiliary database station:
     # /opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh
    getDebugFiles output dir days 4
    where
    output dir is a local directory that is to contain the output files
    days is the optional number of days for which to collect log files
   i Note: You cannot specify /tmp, or any directory below /tmp, as the output directory.
  Collect the output files:

    hostname date.WsInfoFiles.checksum.tar.gz

    Contains station-specific information such as the hardware and network configuration

    hostname date.ServerLogFiles.checksum.tar.gz

    Contains server and JBoss logs, and configuration information

    hostname date.DBLogFiles.checksum.tar.gz

    Contains NFM-P database logs and configuration information
```

END OF STEPS -

## 3.2 To retrieve a list of pods

### 3.2.1 Steps

1

Enter the following command to view a list of pods in the NSP cluster:

```
# kubectl get pods -A 🗸
```

END OF STEPS

## 3.3 To retrieve pod information

### 3.3.1 Steps

1 -

Enter the following to view information about a specific pod:

```
# kubectl describe pod --namespace pod namespace pod name 4
```

where *pod\_namespace* is the name of the pod's namespace and *pod\_name* is the name of the pod

**I** Note: Ensure the full name of the pod is entered for *pod\_name*. To find the full name of a pod, see the procedure 3.2 "To retrieve a list of pods" (p. 30).

2 –

The command output includes many parameters, including any events associated with the pod. For example:

```
TypeReasonAgeFromMessage--------------------WarningFailedScheduling <unknown>default-scheduler0/1 nodes areavailable:1 Insufficient memory.--------
```

END OF STEPS -

## 3.4 To recover pods

#### 3.4.1 Steps

1 -

Enter the following command to recover a pod:

# kubectl delete pod --namespace pod\_namespace pod\_name +

where *pod\_namespace* is the name of the pod's namespace and *pod\_name* is the name of the pod

**i** Note: Ensure the full name of the pod is entered for *pod\_name*. To find the full name of a pod, see the procedure 3.2 "To retrieve a list of pods" (p. 30).

2

The pod is automatically redeployed. You can use the command to recover a pod in an errored state.

END OF STEPS

#### To recover executor pods 3.5

## 3.5.1 Executor pods

The following applications use executor and driver pods:

- act-pipeline-app
- rta-anomaly-detector-app
- rta-trainer-app
- rta-windower-app

An executor pod name has the following format:

app name-instance-exec-executor ID

where

app name is the application name

instance is the pod instance ID

executor\_ID is a number that identifies the executor instance

## 3.5.2 Steps

1 -

Enter the following to recover an executor pod, where pod namespace is the name of the pod's namespace and app name is the application name:

# kubectl delete pod --namespace pod namespace app-name-driver 4

2

The driver pod is automatically redeployed, thereby recovering any associated errored executor pods.

END OF STEPS

## 3.6 To retrieve a list of cluster members

### 3.6.1 Steps

1

Enter the following to list the NSP cluster members:

```
# kubectl get nodes 4
```

END OF STEPS -

# 3.7 To retrieve cluster member information

## 3.7.1 Steps

1

Enter the following to view information about a specific member:

```
# kubectl describe nodes node_name +
```

where node\_name is the name of the member to view

```
2
```

The command output includes member information such as the following:

• member status; for example:

Type Status LastHeartbeatTime LastTransitionTime Reason Message

NetworkUnavailable False Wed, 30 Sep 2020 12:19:23 -0400 Wed, 30 Sep 2020 12:19:23 -0400 CalicoIsUp Calico is running on this node

• member resource capacity; for example:

Capacity:

cpu:	24
ephemeral-storage:	67092472Ki
hugepages-1Gi:	0
hugepages-2Mi:	0
memory:	64381888Ki
pods:	110

• running pods on the member; for example:

· resources allocated to the member; for example:

```
      Resource
      Requests
      Limits

      ------
      ------
      ------

      cpu
      22870m (71%)
      41150m (129%)

      memory
      42120228Ki (32%)
      44290630912 (33%)

      ephemeral-storage
      0 (0%)
      0 (0%)
```

END OF STEPS

# 3.8 To retrieve detailed information about MDM servers

Note: The NSP system must be operational before these operations can be performed.

## 3.8.1 Steps

1

From the NSP deployer host software directory, enter the following to show the MDM server roles, the number of NEs managed using MDM, and which MDM server is hosting which NE:

```
# tools/mdm/bin/server-load.bash --user username --pass
password--detail
where
username is the NSP username
password is the NSP password
```

2

The command output includes information such as the following:

```
{
    "mdmInstanceInfos": [
    {
        "name": mdm-server-0,
        "ipAddress": mdm-server-0.mdm-server-svc-headless.default.
svc.cluster.local,
        "grpcPort": 30000,
        "status": Up,
        "neCount": 0,
        "neIds": null,
        "active": False
        "groupIds": [1, 2],
    },
    {
}
```

```
"name": mdm-server-1,
           "ipAddress": mdm-server-1.mdm-server-svc-headless.default.
svc.cluster.local,
           "grpcPort": 30000,
           "status": Up,
           "neCount": 2,
           "neIds": ["1.1.1.1", "1.1.1.2"],
           "active": True
           "groupId": 1,
      },
      {
           "name": mdm-server-2,
           "ipAddress": mdm-server-2.mdm-server-svc-headless.default.
svc.cluster.local,
           "grpcPort": 30000,
           "status": Up,
           "neCount": 2,
           "neIds": ["1.1.1.3", "1.1.1.4"],
           "active": True
           "groupId": 2,
      }
    1
}
```

END OF STEPS

## 3.9 To rebalance NE load on MDM servers

**i** Note: The NSP system must be operational before these operations can be performed.

#### 3.9.1 Steps

From the NSP deployer host software directory, enter the following to rebalance the NE load on the MDM servers:

```
1
```

```
# tools/mdm/bin/server-load.bash --user username --pass
password--rebalance
where
username is the NSP username
```

NSP

password is the NSP password

END OF STEPS

## 3.10 To verify disk performance for etcd

### 3.10.1 Steps

1 -

```
As the root user, enter the following:
  # mkdir /var/lib/test
  # fio --rw=write --ioengine=sync --fdatasync=1 --directory=
  /var/lib/test --size=22m --bs=3200 --name=mytest 4
2 -
  The command produces output like the following:
  Starting 1 process
  mytest: Laying out IO file (1 file / 22MiB)
  Jobs: 1 (f=1)
  mytest: (groupid=0, jobs=1): err= 0: pid=40944: Mon Jun 15 10:23:23
  2020
    write: IOPS=7574, BW=16.6MiB/s (17.4MB/s) (21.0MiB/1324msec)
      clat (usec): min=4, max=261, avg= 9.50, stdev= 4.11
       lat (usec): min=4, max=262, avg= 9.67, stdev= 4.12
      clat percentiles (nsec):
       | 1.00th=[ 5536], 5.00th=[ 5728], 10.00th=[ 5920], 20.00th=[
  6176],
       | 30.00th=[ 7584], 40.00th=[ 8896], 50.00th=[ 9408], 60.00th=[
  97921,
       70.00th=[10432], 80.00th=[11584], 90.00th=[12864], 95.00th=
  [14528],
       99.00th=[20352], 99.50th=[23168], 99.90th=[28800], 99.95th=
  [42752],
       | 99.99th=[60672]
     bw ( KiB/s): min=16868, max=17258, per=100.00%, avg=17063.00,
  stdev=275.77, samples=2
                 : min= 7510, max= 7684, avg=7597.00, stdev=123.04,
     iops
  samples=2
    lat (usec) : 10=64.21%, 20=34.68%, 50=1.08%, 100=0.02%, 500=0.01%
```

3 -

In the second block of output, which is shown below, the 99th percentile durations must be less than 10ms. In this block, each durations is less than 1ms.

```
fsync/fdatasync/sync file range:
   sync (usec): min=39, max=1174, avg=120.71, stdev=63.89
   sync percentiles (usec):
    | 1.00th=[
                  42], 5.00th=[ 45], 10.00th=[ 46], 20.00th=[
48],
                  52], 40.00th=[ 71], 50.00th=[ 153], 60.00th=[
    | 30.00th=[
159],
    | 70.00th=[ 167], 80.00th=[ 178], 90.00th=[ 192], 95.00th=[
2061,
    | 99.00th=[ 229], 99.50th=[ 239], 99.90th=[ 355], 99.95th=[
416],
    | 99.99th=[ 445]
               : usr=2.95%, sys=29.93%, ctx=15663, majf=0, minf=35
 сри
 IO depths
               : 1=200.0%, 2=0.0%, 4=0.0%, 8=0.0%, 16=0.0%, 32=0.0%,
>=64=0.0%
    submit
              : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
    complete : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
    issued rwts: total=0,10029,0,0 short=10029,0,0,0 dropped=0,0,0,0
    latency : target=0, window=0, percentile=100.00%, depth=1
```

END OF STEPS

# 3.11 To verify disk performance for NSP

## 3.11.1 Steps

```
1 –
```

Enter the following as the root user in the /opt/nsp directory to create a file called 'test' in the directory:

```
# fio --randrepeat=1 --ioengine=libaio --direct=1 --gtod_reduce=1
--name=test --filename=random_read_write.fio --bs=4k --iodepth=64
--size=4G --readwrite=randrw --rwmixread=50
```

2 -

The command produces output like the following:

```
test: (g=0): rw=randrw, bs=(R) 4096B-4096B, (W) 4096B-4096B, (T) 4096B-4096B, ioengine=libaio, iodepth=64
```
```
fio-3.7
Starting 1 process
test: Laying out IO file (1 file / 4096MiB)
Jobs: 1 (f=1): [m(1)][100.0%][r=22.1MiB/s,w=22.2MiB/s][r=5645,w=5674
IOPS][eta 00m:00s]
test: (groupid=0, jobs=1): err= 0: pid=32439: Mon Sep 21 10:25:11 2020
read: IOPS=6301, BW=24.6MiB/s (25.8MB/s) (2049MiB/83252msec)
  bw ( KiB/s): min=13824, max=39088, per=99.57%, avg=25098.60,
stdev=5316.27, samples=166
   iops
               : min= 3456, max= 9772, avg=6274.49, stdev=1329.11,
samples=166
write: IOPS=6293, BW=24.6MiB/s (25.8MB/s) (2047MiB/83252msec)
  bw ( KiB/s): min=13464, max=40024, per=99.56%, avg=25062.73,
stdev=5334.65, samples=166
               : min= 3366, max=10006, avg=6265.57, stdev=1333.67,
   iops
samples=166
               : usr=5.13%, sys=18.63%, ctx=202387, majf=0, minf=26
  cpu
 IO depths
               : 1=0.1%, 2=0.1%, 4=0.1%, 8=0.1%, 16=0.1%, 32=0.1%,
>=64=100.0%
     submit
               : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.0%,
>=64=0.0%
     complete : 0=0.0%, 4=100.0%, 8=0.0%, 16=0.0%, 32=0.0%, 64=0.1%,
>=64=0.0%
     issued rwts: total=524625,523951,0,0 short=0,0,0,0 dropped=0,0,
0,0
     latency : target=0, window=0, percentile=100.00%, depth=64
Run status group 0 (all jobs):
  READ: bw=24.6MiB/s (25.8MB/s), 24.6MiB/s-24.6MiB/s (25.8MB/s-25.
8MB/s), io=2049MiB (2149MB), run=83252-83252msec
 WRITE: bw=24.6MiB/s (25.8MB/s), 24.6MiB/s-24.6MiB/s (25.8MB/s-25.
8MB/s), io=2047MiB (2146MB), run=83252-83252msec
Disk stats (read/write):
  vda: ios=523989/526042, merge=0/2218, ticks=3346204/1622070,
in_queue=4658999, util=96.06%
```

```
END OF STEPS
```

## 3.12 Problem: NSP data synchronization is not 100%

### 3.12.1 Issue

If you run the procedure "How do I check NSP database synchronization?" in the *NSP System Administrator Guide* and do not get a 100% synchronized result, this indicates that a switchover occurred before the system had stabilized and nsp-tomcat on the standby site had caught up with the active site. The following workaround describes how to synchronize the data.

### 3.12.2 Steps

Perform a switchover to go back to the previous active site.

2

1 -

Wait for database instances to sync up.

3 —

Perform another switchover.

4

Run the procedure "How do I check NSP database synchronization?" again to verify the active and standby databases are 100% synchronized.

END OF STEPS

## 3.13 Problem: Alarms not appearing for rapidly reoccurring faults

### 3.13.1 Issue

Alarms are not generated under certain circumstances when the underlying fault is occurring and resolving faster than the duration of the NSP alarm flush interval. This only applies to alarms created by NSP alarm rules, and not to alarms received from other sources, for example using NETCONF. By default, the flush interval is four seconds, and the NSP may not capture events that occur and resolve faster than that, such as an ISIS interface that is flapping once every second.

You can configure the duration of the flush interval to capture rapidly flapping events. However, this impairs the performance of the NSP, as it increases how often the NSP writes to the alarm database. The following procedure describes how to configure the NSP alarm flush interval.

## 3.13.2 Steps

**i** Note: Performing this procedure involves restarting a component of the NSP, and should not be performed outside of a maintenance window. In the event that resync-fw is upgraded, this procedure must be repeated to change the alarm flush interval again.

Log in as the root user on the NSP cluster host. For information about logging in to the NSP, see the NSP System Administrator Guide.

Open a console window.

3

1 -

2 -

In the **nspos-resync-fw** Kubernetes pod, open the following file in a text editor:

/opt/nsp/os/resync-fw/config/resync-fw-overrides.conf

4

The file contains parameter settings in nested declarations. The existing parameters depend on your current NSP configuration. Find or add the flush-buffer-interval-in-second parameter, which is nested under resync-fw > mdm > notification, as shown below:

```
resync-fw
{
    mdm
    {
        notification
        {
           flush-buffer-interval-in-second = 1
        }
    }
}
```

Configure the value of the parameter to the required duration of the NSP alarm flush interval, in seconds.

5

Save the configuration file, and enter the following to restart the **nspos-resync-fw** pod:

```
# kubectl delete pod --namespace pod namespace pod name 4
```

where *pod\_namespace* is the name of the pod's namespace and *pod\_name* is the name of the pod

**Note:** Ensure the full name of the pod is entered for *pod\_name*. To find the full name of a pod, see the procedure 3.2 "To retrieve a list of pods" (p. 30).

END OF STEPS

i

# 4 Troubleshooting the NFM-P platform

## 4.1 Overview

## 4.1.1 Purpose

This chapter provides information about troubleshooting the NFM-P platform, database, server, or clients.

## 4.1.2 Contents

4.1 Overview	41
Troubleshooting the NFM-P	44
4.2 To collect NFM-P log files	44
4.3 Problem: Poor performance on a RHEL station	46
4.4 Problem: Device discovery fails because of exceeded ARP cache	48
Troubleshooting using the LogViewer	51
4.5 LogViewer overview	51
4.6 LogViewer GUI and Quick Links panel	52
4.7 LogViewer CLI	53
4.8 To display logs using the LogViewer GUI	53
4.9 To configure the LogViewer using the GUI	58
4.10 To search log files in a path	61
4.11 To show or hide buttons from the LogViewer main tool bar	62
4.12 To set highlight colors and fonts for LogViewer components and levels	63
4.13 To automatically show or hide log messages	64
4.14 To manage filters using the GUI Filter Manager	65
4.15 To specify a plug-in using the LogViewer GUI	67
4.16 To display logs using the LogViewer CLI	68
4.17 To configure the LogViewer CLI	72
4.18 To specify plug-ins using the CLI	74
Troubleshooting the NFM-P database	75
4.19 Database troubleshooting overview	75

4.20 Problem: NFM-P database corruption or failure	75
4.21 Problem: The database is running out of disk space	76
4.22 Problem: Frequent database backups create performance issues	77
4.23 Problem: An NFM-P database restore fails and generates a No backup sets error	78
4.24 Problem: NFM-P database redundancy failure	78
4.25 Problem: Primary or standby NFM-P database is down	79
4.26 Problem: Need to verify that Oracle database and listener services are started	79
4.27 Problem: Need to determine status or version of NFM-P database or Oracle proxy	80
Troubleshooting NFM-P server issues	82
4.28 NFM-P server troubleshooting overview	82
4.29 Problem: Cannot start an NFM-P server, or unsure of NFM-P server status	82
4.30 Problem: NFM-P server and database not communicating	86
4.31 Problem: An NFM-P server starts up, and then quickly shuts down	87
4.32 Problem: Client not receiving server heartbeat messages	87
4.33 Problem: Main server unreachable from RHEL client station	88
4.34 Problem: Excessive NFM-P server-to-client response time	89
4.35 Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded	90
4.36 Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving	91
4.37 Cannot manage new devices	92
4.38 Problem: Cannot discover more than one device, or device resynchronization fails	93
4.39 Problem: Slow or failed resynchronization with network devices	94
4.40 Problem: Statistics are rolling over too quickly	95
4.41 Problem: Y.1564 service test results not published to Kafka	96
Troubleshooting NFM-P clients	98
4.42 Problem: Cannot start NFM-P client, or error message during client startup	98
4.43 Problem: NFM-P client unable to communicate with NFM-P server	99

4.44 Problem: Delayed server response to client activity	100
4.45 Problem: Cannot place newly discovered device in managed state	101
4.46 Problem: User performs action, such as saving a configuration, but cannot see any results	102
4.47 Problem: Device configuration backup not occurring	104
4.48 Problem: NFM-P client GUI shuts down regularly	105
4.49 Problem: Configuration change not displayed on NFM-P client GUI	106
4.50 Problem: List or search function takes too long to complete	106
4.51 Problem: Cannot select some menu options or save some configurations	107
4.52 Problem: The NFM-P client GUI does not display NE user accounts created, modified, or deleted using the CLI	107

## **Troubleshooting the NFM-P**

## 4.2 To collect NFM-P log files

### 4.2.1 Purpose

Perform this procedure to collect the relevant log files for troubleshooting an NFM-P database, server, single-user client or client delegate server station.



**Note:** When an NFM-P log file reaches a predetermined size, the NFM-P closes, compresses, and renames the file to include a timestamp and sequence number in the following format:

EmsServer.yyyy-mm-dd\_hh-mm-ss.n.log

During a system restart, NFM-P log files are backed up to directories that are named using a timestamp. A component that runs for a long time can generate multiple log files. Before you restart an NFM-P component, ensure that there is sufficient disk space to store the backup log files.

## 4.2.2 Steps

1 -

To collect the logs for a problem specifically related to installation, perform the following steps.

- 1. Navigate to the installation directory, which is one of the following:
  - NFM-P database—/opt/nsp/nfmp/db/install
  - main server—/opt/nsp/nfmp/server
  - auxiliary server—/opt/nsp/nfmp/auxserver
  - single-user client— typically /opt/nsp/client on RHEL, and C:\nsp\client on Windows
  - client delegate server-typically /opt/nsp/client on RHEL, and C:\nsp\client on Windows
- 2. Collect the following files:
  - NFM-P\_component.install.time.stderr.txt
  - NFM-P\_component.install.time.stdout.txt
  - NFM-P\_*component*\_InstallLog.log where

*component* is the NFM-P component type, such as Main\_Server or Main\_Database *time* is the installation start time

3. Go to Step 7.

2 -

If required, collect the NFM-P database logs.

- 1. Log on to the NFM-P database station as the Oracle management user.
- 2. Collect the following files:
  - /opt/nsp/nfmp/db/install/config/dbconfig.properties
  - all files in /opt/nsp/nfmp/db/install/admin/diag/rdbms/instance/instance/alert

NSP

- all files in /opt/nsp/nfmp/db/install/admin/diag/rdbms/instance/instance/trace
- all files in /opt/nsp/nfmp/db/install/admin/diag/proxy
- all files with a .log extension in the following directories:
  - /opt/nsp/nfmp/db/install
  - /opt/nsp/nfmp/db/install/config

where *instance* is the database instance name, which is maindb1 in a standalone deployment, or maindb1 or maindb2 in a redundant deployment

3

If required, collect the main or auxiliary server logs; the log files have a .log extension and are in the following directories:

- main server—/opt/nsp/nfmp/server/nms/log
- auxiliary server—/opt/nsp/nfmp/auxserver/nms/log

4

If required, collect the RHEL single-user client or client delegate server log files:

- install\_dir/nms/config/nms-client.xml
- all files and subdirectories in the install\_dir/nms/log/client directory

where *install\_dir* is the client software installation location, typically /opt/nsp/client

5

If required, collect the Windows single-user client or client delegate server log files:

- install\_dir\nms\config\nms-client.xml
- all files and subdirectories in the install\_dir\nms\log\client directory

where install\_dir is the client software installation location, typically C:\nsp\client

6

If required, use a script to collect a comprehensive set of log files.

- 1. Log in to the station as the root user.
- 2. Open a console window.
- 3. Enter one of the following:
  - On a main server station:
    - # /opt/nsp/nfmp/server/nms/bin/getDebugFiles.bash output\_dir days
      4
  - On an auxiliary server station:
     # /opt/nsp/nfmp/auxserver/nms/bin/getDebugFiles.bash output\_ dir days
  - On an NFM-P database station:
    - # /opt/nsp/nfmp/db/install/getSAMDebugFiles.bash output\_dir days 4

4. Collect the output files:

#### Note:

On a station that hosts a collocated NFM-P database and main server, all files are present. On a station in a distributed deployment, only two files are present.

- hostname\_date.WsInfoFiles.checksum.tar.gz
   Contains station-specific information such as the hardware and network configuration
- hostname\_date.ServerLogFiles.checksum.tar.gz
   Contains server and JBoss logs, and configuration information
- hostname\_date.DBLogFiles.checksum.tar.gz
   Contains NFM-P database logs and configuration information
- 7 -

Store the files in a secure location to ensure that the files are not overwritten. For example, if two NFM-P clients have problems, rename the files to identify each client and to prevent the overwrite of one file with another of the same name.

8

Send the files to technical support, as required.

END OF STEPS

## 4.3 Problem: Poor performance on a RHEL station

### 4.3.1 Checking CPU performance

When a RHEL station is taking too long to perform a task, you can check the CPU status to ensure that one process is not using most of the CPU resources, and then use commands to review the CPU usage.

Perform this procedure when CPU usage remains high and performance degrades.

You can also perform other procedures to monitor performance: If you are you performing a large listing operation using the NFM-P client GUI or OSS, check the LAN throughput using the netstat command, as described in 4.44 "Problem: Delayed server response to client activity" (p. 100).

### 4.3.2 Steps

1

Log on to the station as the root user.

2

Open a console window.

#### 3 —

Perform the following steps to check for processes that are consuming excessive CPU cycles:

1. To list the top CPU processes using the UNIX utility prstat, type:

# top ↓

Depending on your system configuration, approximately the top 20 processes are displayed.

2. Review the output.

The top NFM-P process in the CPU column should be the Java process. However, the Java process should not consume too much CPU time. Some Oracle processes may also consume CPU time, depending on the database load.

3. Press Ctrl-C to stop the command.

4

Perform the following steps to view a CPU activity summary.

1. Enter the following command:

# mpstat time 4

where *time* is the interval, in seconds, between CPU polls; a value between 10 and 60 is recommended

2. Review the command output.

mpst	at output	example						
CPU	%usr	%nice	%sys	%iowait	%irq	%soft	%steal	ବ
gues	t %idle							
all	0.25	0.00	0.17	0.00	0.00	0.00	0.00	0.
00	99.58							
all	0.50	0.00	0.08	0.08	0.00	0.00	0.00	0.
00	99.33							
all	0.17	0.00	0.08	0.00	0.00	0.00	0.00	0.
00	99.75							
all	0.25	0.00	0.17	0.08	0.00	0.00	0.00	0.
00	99.50							

mpstat field descriptions

Field	Description (events per second unless noted)	
CPU	Processor number; the keyword all indicates that statistics are calculated as averages imong all processors	
%usr	Percentage of CPU utilization at the user application level	
%nice	Percentage of CPU utilization at the user level with nice priority	
%sys	Percentage of CPU utilization at the system level; does not include time spent servicing hardware and software interrupts	
%iowait	Percentage of CPU idle time during which the system had an outstanding disk I/O request	

Field	Description (events per second unless noted)	
%irq	Percentage of CPU time spent servicing hardware interrupts	
%soft	Percentage of CPU time spent servicing software interrupts	
%steal	Percentage of time spent in involuntary wait by the virtual CPU or CPUs during hypervisor servicing of another virtual processor	
%guest	Percentage of CPU time spent running a virtual processor	
%idle	Percentage of CPU idle time without an outstanding disk I/O request	

Review the %usr, %sys and %idle statistics, which together indicate the level of CPU saturation. A Java application that fully uses the CPUs typically falls within 80 to 90 percent of the %usr value, and 20 to 10 percent of the %sys value. A smaller percentage for the %sys value indicates that more time is being spent running user code, which generally results in better execution of the application.

3. Press Ctrl-C to stop the command.

#### 5

If processes are competing for CPU resources, perform the following steps to isolate the information about a single process.

1. Check the state of CPUs by typing:

ps -aux 🗸

A list of processes is displayed.

2. Review the command output.

For CPU troubleshooting, the important data is listed in the %CPU row. If a process is taking 90% or more of the CPU resources, there may be a problem with the process. Contact your account or technical support representative for more information.

- 3. Press Ctrl-C to stop the command.
- 6

Contact technical support and provide the data obtained in the previous procedure steps.

END OF STEPS

## 4.4 Problem: Device discovery fails because of exceeded ARP cache

#### 4.4.1 ARP cache and /var/log/messages

When an NFM-P system manages a large number of NEs in a broadcast domain, the ARP cache on a main server station may fill and prevent the discovery of additional devices. When this happens, the /var/log/messages file contains entries like the following:

Jan 21 09:37:40 hostname kernel: Neighbour table overflow

Jan 21 09:37:40 hostname kernel: Neighbour table overflow
Jan 21 09:37:40 hostname kernel: Neighbour table overflow
Jan 21 09:38:00 hostname kernel: ratelimit:190 callbacks suppressed

Perform this procedure when one of the following occurs:

- The /var/log/messages file contains more than 1024 entries like the example entries above.
- You need to increase the ARP cache size to accommodate the network.

The default ARP cache threshold values are the following:

- Threshold 1—128
- Threshold 2—512
- Threshold 3—1024

### 4.4.2 Steps

1 -

Log in to the main server station as the root user.

2 –

Open a console window.

3

Perform one of the following to increase the ARP cache thresholds.

a. To temporarily increase the thresholds, type the following:

- # echo 8096 > /proc/sys/net/ipv4/neigh/default/gc\_thresh1 4
- # echo 25600 > /proc/sys/net/ipv4/neigh/default/gc\_thresh2 4
- # echo 32384 > /proc/sys/net/ipv4/neigh/default/gc\_thresh3 4
- b. To permanently override the default thresholds, perform the following steps.
  - 1. Open the /etc/sysctl.conf file using a plain-text editor such as vi.
  - 2. Add the following lines to the end of the file:

```
net.ipv4.neigh.default.gc_thresh1 = 8096
net.ipv4.neigh.default.gc_thresh2 = 25600
net.ipv4.neigh.default.gc_thresh3 = 32384
```

- 3. Save and close the file.
- 4. Enter the following:
  - # sysctl -p ↓

4 –

Close the console window.

END OF STEPS -

## Troubleshooting using the LogViewer

## 4.5 LogViewer overview

### 4.5.1 Managing log files

The LogViewer is a system monitoring and troubleshooting utility that parses, formats, and displays the contents of log files.

You can use LogViewer to perform the following:

- View and filter real-time log updates.
- View, filter, and sort the entries in a static log view.
- · Open compressed or uncompressed log files.
- Compare active logs in real time.
- Automatically send a notification when a specified type of entry is logged.

LogViewer is available on NFM-P main or auxiliary server stations, and on single-user client and client delegate server stations as separate GUI and CLI utilities. The GUI has more functions than the CLI, which is designed for use on a character-based console over a low-bandwidth connection such as a Telnet session.

LogViewer can interpret various log formats. The log files must be local server or database logs.

### 4.5.2 Configuration

The LogViewer GUI and CLI utilities share a set of configuration options; an option change by one utility affects the other utility. Some options apply only to the GUI.

You can customize LogViewer by creating and saving log filters and log profiles that are available to all GUI and CLI users, and can save the GUI configuration, or workspace, to have LogViewer display the currently open logs the next time it starts. LogViewer does not save the current filter and display configuration for a log when you close the log unless you export the configuration to a log profile.

Your operating configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set such as location, size and splitter location, are used the next time you start the utility.

For multiple instances of LogViewer running on the same server, you can set the system environment variable LOGV\_HOME to make all instances use the same properties file. In this way, properties such as filters, window location, and window size are common to all instances.

## 4.5.3 Filters

You can use the LogViewer CLI or GUI to create multiple filters that define the log entries that are displayed in a log view. A filter uses Java regular expressions as match criteria to specify which entries to display and optionally uses colors to identify the filtered entries.

### 4.5.4 Plug-ins

LogViewer supports the use of plug-ins to provide additional functionality. You can specify a plug-in for use with a specific log, or assign a default plug-in configuration that applies to the subsequently opened logs.

LogViewer has default plug-ins that can send notifications, such as e-mail messages and GUI popups, when a new log entry matches a set of filter criteria. The LogViewer e-mail plug-in uses SMTP as the transport.

## 4.6 LogViewer GUI and Quick Links panel

## 4.6.1 Accessing log entries

The LogViewer GUI opens to display a Quick Links panel that has shortcuts to the logs that are present on the local file system. When you click on a log shortcut, LogViewer opens a tab that displays the most recent log entries.



**Note:** If you hover your mouse cursor over a GUI tab, toolbar button, or field, a description or configuration instruction specific to that object appears.

## 4.6.2 LogViewer GUI and log tabs

Each log that you open using the LogViewer GUI is displayed on a separate tab whose label contains the name of the log profile and an icon that indicates the log type. The log entries are highlighted using the colors configured for the log debug levels. A log tab that displays dynamic log updates also has a tool bar for common operations.

The lower panel of a log tab contains the following sub-tabs:

- · Preview—displays the unparsed log-file text for the currently selected log entries
- · Filter—lists and permits management of the currently active filters for the log
- · Status—displays status information about the current log
- Plugin—displays information about the plug-ins associated with the log
- Legend—displays a legend that correlates log file names to the numbers in the File column on a log tab that contains multiple open logs, for example, merged logs; is not shown for log comparisons

The LogViewer GUI allows you to drag and drop a log file into the GUI window. If you drop a file onto an open log tab, LogViewer provides options such as merging or comparing the log with another.

You can open a tab to list static log entries, such as the contents of an archived log or a snapshot of entries from an active log, and can pause the updates to active logs. The GUI also includes a text-search function.

### GUI-based log filtering

The GUI provides a Filter Manager applet that lists the filters defined using the CLI or GUI and allows filter creation, modification, and deletion. A GUI operator can also use Filter Manager to test the regular expressions as filter match criteria.

To rapidly isolate a specific log entry or type of entry, you can create a temporary filter, or quick filter, by entering a regular expression in the field below a column header on a log tab. You can convert a quick filter to a saved filter for later use. A drop-down menu above the Level column allows the immediate filtering of log entries based on the debug level.

You can also create and use simple filters. These filters do not require the use of regular expressions, but instead, perform a case insensitive "contains" filtration of a string you specify. The use of simple filters must be enabled using the Preferences→Options menu option.

A color that is specified as the highlight color for a filter is saved with the filter and applies to all logs that use the filter.

## 4.7 LogViewer CLI

## 4.7.1 Accessing log entries using the CLI

The CLI-based LogViewer works like the UNIX tail command when in display mode. The command mode has a multiple-level menu that you can display at any time. You can specify a command or log file using the minimum number of unique characters in the name, and can quickly toggle between the command and display modes. LogViewer buffers new log entries while in command mode and displays them when it returns to display mode.

The LogViewer CLI assigns a different color to each logging level, for example, WARN or INFO, using standard ANSI color attributes that can be specified as CLI startup options or configured through the GUI. The CLI also supports the use of filters, plugins, and quick links.

## 4.8 To display logs using the LogViewer GUI

### 4.8.1 Purpose

Perform this procedure to start the LogViewer GUI utility and view one or more logs. Move the mouse cursor over a GUI object to view a description of the object, for example, a tool bar button.

## 4.8.2 Steps

1 —

Log in to a station as the nsp user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

Enter the following:

bash\$ /opt/nsp/nfmp/server/nms/bin/logviewerui.bash 4

The LogViewer GUI opens with the Quick Links panel or the log tabs in the saved workspace displayed.

#### 4 -

To open a log file, perform one of the following:

- a. If the Quick Links panel is displayed, click on a link to view the associated log file.
- b. Choose Quick Links→log\_name from the LogViewer main menu.
- c. To open a recently viewed log, choose File→Recent Logs→*log\_file\_name* from the LogViewer main menu.
- d. To browse for a log file, perform the following steps:
  - 1. Choose File→Local Log File from the LogViewer main menu or click Open log in the main tool bar. The Local Log File form opens.
  - 2. Use the form to navigate to the log-file location.
  - 3. Select a log file and click Add between the form panels. The log is listed in the panel on the right.

#### Note:

The log file can be in compressed or uncompressed format.

- 4. If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.
- 5. Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.
- 6. Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.
- 7. Click OK. The Local Log File form closes.
- e. Drag and drop a log file into a section of the LogViewer main window that does not contain a log tab.
- f. Drag and drop a log file onto a log tab in the LogViewer main window. The Add File form opens.

Perform the following steps:

- 1. Choose one of the following options:
  - · New View—specifies that the log is displayed on a new log tab
  - Replace Existing File—specifies that the log tab displays the new log instead of the current log
  - Add to View—specifies that the entries in the new log and the entries in the current log are merged into one list on the same log tab
  - Add to Compare View—specifies that the new log is to be displayed on the same log tab as the current log in a separate panel for comparison
- 2. Click OK. The new log is displayed as specified.

A log tab opens to display the most recent entries in a log. If the log is active and the Auto-Tail parameter is enabled, the list scrolls upward to display new log entries as they are generated. **i** Note: The Auto-Tail parameter for a log is enabled by default.

### **Common display operations**

5

To specify which columns are displayed on a log tab, right-click on a column header, and select or deselect the column names in the contextual menu, as required.

6

To reposition a column, drag the column title bar to the desired position, or right-click on the column header and choose Move Left or Move Right.

7

To view the raw log-file text of one or more entries, select the entries. The entry text is displayed on the Preview sub-tab.

8 -

To restrict the list of displayed entries to a specific debug level, choose a debug level from the drop-down menu under the Level column header.

9

To find log entries that contain a specific text string:

- 1. Choose  $Edit \rightarrow Find$  from the LogViewer main menu. The Find form opens.
- 2. Specify a text string to search for using the text field and search options on the form. **Note:**

The LogViewer Find function does not support the use of regular expressions. To perform a search using a regular expression, use the Find In Path function, as described in 4.10 "To search log files in a path" (p. 61).

- 3. Click Find, as required, to find the next list entry that contains the text string.
- 4. To find all list entries that contain the text string, click Find All. The Find form closes and a new log tab opens to display the result of the search.
- 5. Close the Find form if it is open.

#### Note:

After you close the Find form, you can use the F3 key or the Find next button on the main tool bar to perform repeated find operations for the same text string on the same log tab.

10

To remove one or more log entries from the current view, perform one of the following.

- a. To clear all listed log entries, choose Log→Clear All Events from the LogViewer main menu, or click Clear all in the main tool bar.
- b. To clear the currently selected log entries, choose Log→Clear Selected Events from the

LogViewer main menu, or click Clear Selected in the main tool bar.

- c. To clear all log entries that match the currently selected cell, select a cell and choose Log→Hide All Like Selected from the LogViewer main menu, or click Hide All Like Selected in the main tool bar.
- d. To show only log entries that match the currently selected cell, select a cell and choose Log→Show All Like Selected from the LogViewer main menu, or click Show All Like Selected in the main tool bar.
- 11 -

To apply a quick filter, enter a regular expression as a match criterion in the field below a column header and press 4. The list is cleared, and only subsequent log entries that match the criterion are displayed; see 4.14 "To manage filters using the GUI Filter Manager" (p. 65).

12 -

Repeat Step 11 to apply an additional quick filter, if required.

13 —

To apply a saved filter:

- 1. Choose Log→Add Filter from the LogViewer main menu, or click Add filter in the main tool bar. The Select Filters form opens.
- 2. Select one or more filters in the list and click OK. The filters are applied to the log view and are listed on the Filters sub-tab of the log tab.

See 4.14 "To manage filters using the GUI Filter Manager" (p. 65) for information about creating saved filters.

14 —

To remove a filter from the log, select the filter in the Filter sub-tab and choose  $Log \rightarrow Remove$ Selected Filters, or click Remove filter in the main tool bar.

15

If the log display is static, such as for an archived log or the result of a Find All operation, go to Step 22.

#### **Dynamic view operations**

16

To edit the log display properties, choose  $Edit \rightarrow Edit Log$  from the LogViewer main menu, or click Edit log in the log tab tool bar, and perform the following steps.

1. Configure the Max. Messages parameter to specify the maximum number of entries that are listed on the log tab. LogViewer removes the oldest entries as required to keep the number of entries at or below this value.

- 2. Configure the Auto-Tail parameter to specify whether the log tab dynamically displays the log updates.
- 3. Click OK to close the Local Log File form.
- 17 -

To pause the display of log-file updates, choose  $Log \rightarrow Pause$  from the LogViewer main menu, or click Pause log updates in the log tab tool bar.

18 -

To resume the display of log-file updates, choose Log $\rightarrow$ Initialize Connection from the LogViewer main menu, or click Initialize log updates in the log tab tool bar.

19

By default, a dynamic log view focuses on a new log entry. To focus the display on an earlier log entry and prevent the display from automatically focusing on a new log update, click Follow latest updates in the log tab tool bar. Click on the button again to enable the default behavior.

#### 20

To compare logs in real time:

- 1. Choose Log→Specify Compare from the LogViewer main menu, or click Add log to compare on the log tab tool bar. The Compare Files form opens.
- 2. Use the form to navigate to the log-file location.
- 3. Select a log file and click Add between the form panels. The log is listed in the panel on the right.

Note:

The log file can be in compressed or uncompressed format.

- 4. If LogViewer cannot determine the type of log that the file contains, for example, if a log file is renamed, it sets the Type to Other. Use the Type drop-down menu to specify the log type, if required.
- 5. Click OK. The Compare Files form closes, and a second panel opens on the log tab to display the specified log.

The log entry lines are synchronized by timestamp. Dynamic log updates to each log are displayed as they occur. Blank entry lines serve as spacers to preserve the chronological order of the combined log entries.

- 6. By default, the scroll bars in the two panels are synchronized; when you scroll in the right panel, the display in the left panel scrolls by the same amount. Click Synchronize scroll bars between views in the log tab tool bar to disable or re-enable this behavior, as required.
- 7. To remove the added log from the comparison, choose Log→Clear Compare from the LogViewer main menu, or click Clear compared logs on the log tab tool bar. The right panel is removed from the log tab form.

#### 21 -

To capture one or more log entries for display in a static view on a separate tab:

- a. To capture all listed log entries, choose Log→Full Snapshot from the LogViewer main menu, or click Snap all in the main tool bar.
- b. To capture the currently selected log entries, choose Log→Snapshot from the LogViewer main menu, or click Snap selected in the main tool bar.

A new tab opens to display the captured log entries in a static view.

#### Static view operations

22 –

To sort a list of log entries in a static view, right-click on a column header and choose Sort Ascending, Sort Descending, or No Sort. The log entries are sorted accordingly.

| i |

**Note:** You cannot sort the log entries in a dynamic view, but you can sort the entries in a snapshot of a dynamic log view.

#### 23 –

To copy the text of selected log entries to the clipboard, select one or more log entries in a log tab and choose  $Edit \rightarrow Copy$  from the LogViewer main menu, or click Copy in the main tool bar.

**24** —

To save selected log entries to a file, select one or more log entries in a log tab and click Save Selected in the main tool bar.

#### 25 -

To save the current workspace for subsequent sessions, choose File $\rightarrow$ Save Workspace from the LogViewer main menu, or click Save configuration in the main tool bar.

26 -

Choose File $\rightarrow$ Exit from the LogViewer main menu to close the LogViewer GUI.

END OF STEPS -

## 4.9 To configure the LogViewer using the GUI

#### 4.9.1 Purpose

Perform this procedure to use the LogViewer GUI to configure general options for the LogViewer GUI and CLI.

### 4.9.2 Steps

Open the LogViewer GUI.

2 -

1

Choose Edit $\rightarrow$ Options $\rightarrow$ General from the LogViewer main menu, or click Application options in the main tool bar. The Options form opens.

3

Configure the required parameters:

- Last Directory—Click in the parameter field and use the browser form that opens to specify where to save exported log profiles.
- Base File Messages Directory—Click in the parameter field and use the browser form that opens to specify the base log directory.
- Default Character Set—Edit this parameter to specify the character set that LogViewer uses to display the log-file contents.
- Default Log Pattern—Edit this parameter to specify a regular expression that LogViewer uses to interpret log-file contents.
- Default Date Format—Enter a colon-separated string to specify the LogViewer date format using y for year digits, M for month digits, d for date digits, H for hour digits, m for minute digits, s for second digits, and S for millisecond digits, for example, yyyy:MM:dd HH:mm:ss:SSS.
- Regular Expression Help URL—Enter a value to specify the location of the Java regularexpression help web page that opens when you click Help while testing a regular expression for a filter.
- Web Browser Location—Enter a value to specify the location of the local file browser used to open the Java regular-expression help web page.
- Quick Links Refresh Time (ms)—Enter a value to specify how often LogViewer refreshes the Quick Links list.
- Rollover Remove Size—Enter a value to specify the number of log entries to remove from the LogViewer display when the maximum number of displayed log entries is reached.
- Delay for local file polling (ms)—Enter a value to specify, in ms, how long LogViewer waits before it checks local log files for updates.
- Hide Table Tooltips—Select this parameter to suppress the display of tool tips when the mouse pointer moves over log entries in a log tab.
- Use Simple Filters—Select this parameter to allow the use of simple filters.
- Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on log tabs.
- Display Advanced Quick Filter—Select this parameter to display the advanced Quick Filter table header on the log tab when a log file is opened.
- Include Host in Title—Select this parameter to display the hostname in the log title.

- Show Memory Monitor—Select this parameter to display the memory monitor at the bottom right corner of the LogViewer window.
- Memory Monitor Clear Messages—Select this parameter to allow the memory monitor to attempt recovery by clearing some messages from live event logs when the memory threshold is exceeded.
- Clear Log on Rollover—Select this parameter to clear the events from the logs when a Style View file rolls over or is moved.
- Style View—Select this parameter to display the styled preview pane.
- Memory Monitor Threshold (%)—Enter a value to specify the percentage of available memory that LogViewer uses before it stops displaying log updates.
- Max. Recent Files—Enter a value to specify the number of files that LogViewer keeps in the list of recently opened files.
- Max. Profile Files—Enter a value to specify the number of profile files that LogViewer keeps in the list of recently opened files.
- LogViewer Log Level—Choose a logging level from the drop-down menu to specify the minimum log level of the LogViewer-specific log messages.
- Enable Viewer Performance Stats—Select this parameter to enable the display of LogViewer performance statistics.
- Stats Timer (seconds)—Enter a value to specify the number of seconds that LogViewer waits between log statistics updates.

4

Click on the Command Line tab to configure the LogViewer CLI.

5

Configure the following parameter:

- Command line buffer size—Enter a value to specify the number of log messages that LogViewer buffers when the CLI is in command mode.
- 6

Choose an ANSI display attribute from the drop-down menu beside each of the following parameters to specify how the CLI displays the corresponding text.

- Normal Display—for normal text
- · Trace Level Display-for trace-level log entries
- Debug Level Display—for debug-level log entries
- · Info Level Display-for info-level log entries
- · Warning Level Display-for warning-level log entries
- · Error Level Display-for error-level log entries
- · Fatal Level Display-for fatal-level log entries
- · Filter Display-for filtered log entries

NSP

#### 7 -

Configure the Always Use ANSI Display parameter, as required.

#### 8

Click on the NFM-P tab to configure the required parameters that are specific to the NFM-P.

9

Configure the required parameters by clicking in the parameter field and using the browser form that opens to specify a directory:

- Database Location—specifies the base NFM-P database installation directory
- Oracle Location—specifies the base NFM-P Oracle installation directory
- NMS Root—specifies the nms directory under the base NFM-P server installation directory Note:

Your configuration of LogViewer is stored in the user directory. Any filters, fonts, colors, or other preferences you have set are preserved when you install a newer version.

```
10
```



The parameters on the Advanced tab typically require configuration only when LogViewer has performance problems.

Consult technical support before you attempt to modify a parameter on the Advanced tab, as it may affect server performance.

Click on the Advanced tab to configure the required parameters related to LogViewer performance.

END OF STEPS -

## 4.10 To search log files in a path

### 4.10.1 Purpose

Use this procedure to perform a search on all log files in a specified path using a plain text search or a regular expression.



**Note:** You can test regular expressions in the Find In Path window by clicking Test beside the expression. Enter sample text in the Example box, and an expression in the Expression box, then click on the green Execute button to test the results of the expression.

## 4.10.2 Steps

1	
	Open the LogViewer GUI.
2	
L	Choose Edit $\rightarrow$ Find In Path from the LogViewer main menu, or click Search all files. The Find In Path window opens.
3	
	Perform one of the following:
	a. To perform a text search, specify the text string to search for in the Text to find parameter and deselect the Regular expression option.
	b. To perform a search using a regular expression, enter a regular expression in the Text to find parameter and select the Regular expression option.
4	
·	In the Directory parameter, enter the directory path you need to search, or click Browse and select a directory. To search subdirectories, select the Recursive option.
5	
Ū	To restrict the search to logs with certain filenames, enter a regular expression in the File Mask parameter. To search all logs in the specified path, leave this parameter blank.
6	
	Click Find. The log entries matching the search parameters are displayed in a new tab.
	<b>i</b> Note: A new search using the Find In Path function cannot be performed until the search tab is closed.
END	OF STEPS

## 4.11 To show or hide buttons from the LogViewer main tool bar

## 4.11.1 Purpose

Perform this procedure to show or hide specific buttons from the LogViewer main tool bar.

## 4.11.2 Steps

1

Open the LogViewer GUI.

Choose Edit $\rightarrow$ Preferences $\rightarrow$ Manage Toolbar from the LogViewer main menu. The Manage Toolbar page opens divided into a Palette and Toolbar section.

Use the directional arrows to manage which buttons appear in the main tool bar, and the order in which the buttons appear.

4 Click OK to save your settings.

END OF STEPS -

4.12 To set highlight colors and fonts for LogViewer components and levels

### 4.12.1 Purpose

2 —

3

Perform this procedure to set highlight colors and fonts for the various LogViewer components and levels.

### 4.12.2 Steps

1 -

Open the LogViewer GUI.

2 –

Choose Edit $\rightarrow$ Preferences $\rightarrow$ Highlight Colors from the LogViewer main menu. The Highlight Color Selection form opens.

3 —

Set the item for which you want to specify colors and/or fonts by choosing it from the Component/Level drop-down menu.

4

For the item that you want to change, choose the foreground or background plane as required, by clicking on the appropriate tab. The foreground is the text contained in a field. The background is the fill color of the field behind the text.

5 \_\_\_\_\_

For foreground text items, set the font type, style, and size, as required.

NSP

#### 6 -

For either foreground or background items, set the color as required. You can choose a color from the samples shown on the Swatch tab, or you can specify a color by entering its red, green, and blue values in the RGB tab.

Previews of your choices appear in the sample fields at the bottom of the form.

7 —

Click OK to save your settings.

END OF STEPS

## 4.13 To automatically show or hide log messages

#### 4.13.1 Purpose

Perform this procedure to automatically filter (show or hide) log messages based on the current selected cell in the message table.

#### 4.13.2 Steps

1 -

Open the LogViewer GUI.

2 –

To automatically show or hide log messages:

- 1. Select a log entry.
- 2. To hide log messages based on a selected cell in the message table, perform one of the following:
  - Right-click on the cell and choose Hide All Like Selected.
  - Choose Log $\rightarrow$ Hide All Like Selected from the LogViewer main menu.
  - Click the Hide All Like Selected button in the main tool bar.

LogViewer hides all messages that contain the selected cell. For example, if you have selected the cell in the "Logger" column that contains the word "samConsole", all messages that have the logger set to "samConsole" are hidden.

- Perform one of the following to show log messages based on a selected cell in the message table.
  - Right-click on the cell and choose Show All Like Selected.
  - Choose Log $\rightarrow$ Show All Like Selected from the LogViewer main menu.
  - Click the Show All Like Selected button in the main tool bar.

This shows all messages that contain the selected cell. For example, if you have selected the cell in the "Logger" column containing the word "samConsole", all messages that have the logger set to "samConsole" are displayed.

END OF STEPS

## 4.14 To manage filters using the GUI Filter Manager

### 4.14.1 Purpose

Perform this procedure to create, modify, assign or delete a LogViewer filter.



**Note:** The Filter Manager is opened from within LogViewer, but runs as a separate applet. This enables the dragging and dropping of filters between Filter Manager and the Filters subtab of a lob tab.

## 4.14.2 Steps

1 -

Choose Log $\rightarrow$ Filter Manager from the LogViewer main menu. The Filter Manager applet opens.

2 —

To add a regular filter or a simple filter:

- 1. Click Add or Add Simple, as required. The Add Filter form opens.
- 2. Configure the Name parameter by specifying a unique name for the filter.
- 3. Configure the required parameters that correspond to the fields in a log entry by entering regular expressions for regular filters, or just strings for simple filters as a filter criterion for each:
  - Level
  - Message
  - Thread
  - Logger
  - Timestamp
  - Platform
- 4. If you are configuring a simple filter, go to Step 2 11 .
- 5. Test a regular expression that you enter by clicking Test beside the regular expression. The Regular Expression form opens.
- 6. Paste an example log entry that you want to match using the regular expression into the Example field.
- 7. Click on the green right-pointing arrow to test the expression. If the expression is invalid, a message is displayed to indicate the error in the expression.
- 8. Correct the errors in the expression.
- 9. Repeat Step 2 7 and Step 2 8 until no error message is displayed.
- 10. Repeat Step 2 5 to Step 2 9 to test additional regular expressions, if required.
- 11. Enable the Color parameter and click in the field beside the parameter to specify a highlight color for the matching log entries. A standard color chooser form opens.
- 12. Use the form to specify a color and click OK. The color chooser form closes and the Add Filter form reappears.

13. Click OK. The Add Filter form closes and the Filter Manager form lists the new filter.

3

To create a saved filter based on the current quick filter, perform the following steps:

- Choose Log→Create from Quick Filter from the LogViewer main menu, or click Create from quick in the main tool bar. The Add Filter form opens and is populated with the quick filter match criteria.
- 2. Modify the match criteria as required.
- 3. Click OK to save the filter.
- 4

To create a saved filter using a log entry as a template:

- 1. Select a log entry.
- Choose Log→Create from Selected from the LogViewer main menu, or click Create from entry in the main tool bar. The Add Filter form opens and is populated with the current logentry field values as match criteria.
- 3. Modify the match criteria as required.
- 4. Click OK to save the filter.
- 5 —

To move a filter to other instances of the LogViewer:

- To export a filter, click Export in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Export form opens, and allows you to export a filter to a specified file.
- To import a filter, click Import in the main tool bar, or choose Log→Filter Manager from the LogViewer main menu. The Import form opens, and allows you to import a filter from a specified file.
- 3. Click OK to save the filter.
- 6

To make a copy of a filter, select the filter and click Copy. A copy of the filter is listed on the Filter Manager form.

7

To edit a filter, select the filter and click Edit. Configure the required parameters described in Step 2.

8

To delete a filter, select the filter and click Delete.

END OF STEPS -

## 4.15 To specify a plug-in using the LogViewer GUI

### 4.15.1 Purpose

Perform this procedure to configure and enable plug-ins for a log file.

### 4.15.2 Steps

Choose File $\rightarrow$ Local Log File from the LogViewer main menu, or click Open log in the log tab tool bar. The Local Log File form opens.
Use the form to navigate to the log-file location.
Select a log file and click on the Add object icon button between the form panels. The log is listed in the panel on the right.
<b>i</b> Note: The log file can be in compressed or uncompressed format.
Click on the Plugins tab.
Choose a plug-in from the Plugin drop-down menu.
<ol> <li>If you choose the Bring to Front plug-in, perform the following steps:</li> <li>Specify a regular expression as a match criterion in the Message Filter field.</li> <li>Go to Step 8.</li> </ol>
<ul> <li>If you choose the E-Mail plug-in, perform the following steps:</li> <li>Specify a regular expression as a match criterion in the Message Filter field.</li> <li>Configure the required parameters: <ul> <li>Message Filter—specifies a regular expression that is used as a filter to identify the log entries that invoke the plug-in</li> <li>Subject—specifies the e-mail message subject line</li> <li>Body Prefix—specifies the text that precedes the log-entry text in an e-mail message</li> </ul> </li> </ul>
<ul> <li>Authenticate? —specifies whether or not authentication is enabled</li> <li>User—specifies a user name associated with the plug-in</li> </ul>

- Password—specifies an SMTP password
- · Host—specifies the name of an SMTP server
- Use TLS? —specifies whether the mail server uses Transport Layer Security (TLS) encryption
- Use SSL? —specifies whether the mail server uses Secure Sockets Layer (SSL) encryption
- · To-specifies the e-mail address of the recipient
- · From—specifies the sender e-mail address used by the plug-in
- Minimum E-mail Time (minutes)—specifies the minimum time between messages that the plug-in sends, to prevent e-mail flooding

8 -

Click OK. The Local Log File form closes.

END OF STEPS -

## 4.16 To display logs using the LogViewer CLI

#### 4.16.1 Purpose

Perform this procedure to start the LogViewer CLI and view one or more logs.

### 4.16.2 Steps

1 -

Log in to a station as the nsp user.

2 –

Open a console window.

3 —

Enter the following:

bash\$ /opt/nsp/nfmp/server/nms/bin/logviewer.bash argument options parameter 4

where

*argument* is an argument listed in Table 4-1, "LogViewer CLI startup arguments" (p. 68) *options* is one or more of the options listed in Table 4-2, "LogViewer CLI startup options" (p. 69) *parameter* is a parameter listed in Table 4-3, "LogViewer CLI startup parameters" (p. 69)

Table 4-1 LogViewer CLI startup arguments

Argument	Meaning
version	Display LogViewer version information.

Tahlo 4-1	LogViewer CLI startup arguments	(continued)
		(continucu)

Argument	Meaning
help	Display LogViewer CLI help text.

#### Table 4-2 LogViewer CLI startup options

Option	Meaning	
-counter	Prepend a counter number to each displayed log entry.	
-parseAll	Parses and display the entire contents of a file before displaying the real-time updates.	
-ansi level attribute	Display events and filters using ANSI-specified colors where <i>level</i> is a logging level, such as debug <i>attribute</i> is an ANSI color attribute, such as 42m to specify the color green	
-quit	Quit LogViewer after parsing the log files.	

*Table 4-3* LogViewer CLI startup parameters

Parameter	Meaning
-xml file_name	Read information such as log file, plug-in and filter specifications from the XML file specified by <i>file_name</i> . The LogViewer GUI can export this information to an XML file.
file name	Display the specified file when LogViewer starts.

The LogViewer CLI opens in display mode. If a log file is specified as a startup parameter, the most recent entries in the log file are displayed as they are written to the log file. Otherwise, a cursor is displayed.

Enter command mode by pressing 4. The following prompt is displayed:

#### log>

This prompt is called the root prompt. The table below describes the options that are available at the root prompt.

Table 4-4	LogViewer	CLI root	menu	options
	LOGVICWCI	OLITOOL	monu	options

Option	Function
open	opens a submenu for choosing the logs to view
include	opens a submenu for specifying which log files to list in the open submenu
filter	opens a submenu for adding, listing or deleting filters
plugin	opens a submenu for adding, listing or delete plugins

<sup>4</sup> 

#### Table 4-4 LogViewer CLI root menu options (continued)

Option	Function	
options	opens a submenu for configuring LogViewer CLI and GUI options	
list	lists the files in the open submenu file list	
reset	resets the log message counts	
stats	displays LogViewer statistics for the current log	
The following options are also available in submenus:		
back	goes to the previous menu	
root	goes to the root menu	
quit	quits LogViewer	
return	returns to display mode	

#### 5

Enter the following:

open 🚽

The following prompt is displayed:

log-open>

6

Press  $\checkmark$  to display the list of available logs.

#### 7 -

Perform one of the following:

- b. To view a log that is not listed, perform the following steps.
  - 1. Enter the following:

other  $\prec$ 

The following prompt is displayed:

```
File Name (full path)?
```

2. Enter the absolute or relative path of the log file that you want to open and press 4. LogViewer opens the file.

8

Enter the following to enter display mode and view the real-time log updates:

return 🗸

LogViewer enters display mode. Log updates are displayed as they occur.

#### 9 –

To add a filter that restricts the types of log entries that are displayed during the current LogViewer session, perform the following steps:

- 1. Press ↓ to enter command mode.
- 2. Enter the following to return to the root menu:

```
root 4
```

The following prompt is displayed:

log>

3. Enter the following:

filter 4

The following prompt is displayed:

log-filter>

Note:

You can also use commands at this menu level to list and delete filters.

4. Enter the following:

add 🗸

The following prompt is displayed:

Filter name:

- 5. Enter a name for the filter and press  $\triangleleft$ .
- 6. The following prompts are displayed in sequence:

```
Level:
Logger:
Thread:
Timestamp:
Message:
```

At each prompt, enter a regular expression to use as a match criterion, if required, and press 4.

7. The following prompt is displayed:

```
Display Filter? (Y/N):
```

Enter y 4 to apply the filter to the current log display. LogViewer applies the filter.

8. Enter the following to return to display mode:

```
return 🗸
```

LogViewer enters display mode. The log updates are filtered before they are displayed.

10 -

To list the available log files, perform the following steps:

1. Press ↓ to enter command mode.

2. Enter the following:

```
list ↓
```

LogViewer lists the available log files.

3. Enter the following to return to display mode:

```
11
```

To display statistics about the current LogViewer session, perform the following steps:

- 1. Press 4 to enter command mode.
- 2. Enter the following:
  - stats  $\downarrow$

LogViewer displays statistics about the current session.

3. Enter the following to return to display mode:

return 4

12 –

To reset the statistics counters for the current LogViewer session, perform the following steps:

- 1. Press ↓ to enter command mode.
- 2. Enter the following:

reset 🗸

LogViewer resets the counters.

- 3. Enter the following to return to display mode: return 4
- 13 –

Enter the following to close LogViewer:

quit ↓

END OF STEPS

## 4.17 To configure the LogViewer CLI

### 4.17.1 Purpose

Perform this procedure to use the LogViewer CLI to configure general CLI options.



**Note:** The options configured in this procedure apply only to the current LogViewer CLI session.
## 4.17.2 Steps

```
Open the LogViewer CLI.
```

2 –

1

To add a file to the list of files in the open menu, perform the following steps:

- 1. Press  $\leftarrow$  to enter command mode.
- 2. Enter the following at the root prompt:
  - include 🚽

The following prompt is displayed:

log-include>

3. Enter the following:

add 4

The following prompt is displayed:

File Name (full path)?

4. Enter the absolute or relative path of the log file that you want to add and press 4. LogViewer adds the file to the list in the *open* menu.

Note:

The LogViewer CLI supports file drag-and-drop functionality.

5. Enter the following to return to the root prompt:

root 4

```
3
```

To configure LogViewer file parsing, perform the following steps:

- 1. Press ↓ to enter command mode.
- 2. Enter the following at the root prompt:

options 🗸

The following prompt is displayed:

log-options>

- 3. Enter  $y \leftarrow to$  confirm the action.
- 4. To specify whether LogViewer parses the entire log file, enter the following:

#### parseAll 🚽

A confirmation prompt is displayed.

- 5. To force LogViewer to reparse the current log file, enter the following: **reparse**  $\prec^{1}$
- 6. If you are prompted to enable parsing of the entire log file, enter y 4.

7. Enter the following to return to the root prompt:

root 4

END OF STEPS -

# 4.18 To specify plug-ins using the CLI

#### 4.18.1 Purpose

Perform this procedure to specify a plug-in for the current LogViewer CLI session.

### 4.18.2 Steps

1 -

Open the LogViewer CLI.

```
2 -
```

Press  $\prec$  to enter command mode.

3

Enter the following at the root prompt:

```
plugin 🗸
```

The following prompt is displayed:

log-plugin>

4

Enter the following:

add 4

LogViewer displays a list of the available plug-ins and the following prompt:

Which plugin would you like to specify? (name)

5 \_\_\_\_\_

Enter the name of a plug-in from the list and press  $\triangleleft$ .

6

You may be prompted for plug-in configuration information. Supply the information, as required.

**i** Note: The currently available plug-ins and the associated configuration options are described in 4.15 "To specify a plug-in using the LogViewer GUI" (p. 67).

END OF STEPS

# Troubleshooting the NFM-P database

## 4.19 Database troubleshooting overview

### 4.19.1 Database status

The NFM-P monitors the primary and standby database status and displays a colored status based on the primary and standby database connection and availability states. The following describes the conditions that determine database status color. These conditions also cause the NFM-P to raise database alarms.

#### Clear

The database status panel changes to clear status (gray) when the database connection, proxy, and applicable standby entities are up and all database error conditions are cleared.

#### Yellow

The following conditions cause the panel to change to yellow status:

- A database switchover or failover is complete.
- The database connection is partially down.
- The primary database is up and the standby database is down.
- A problem is detected with synchronization or archiving.

#### Red

The following conditions cause the panel to change to red status:

- A database switchover or failover is starting.
- The database connection is down.
- The primary database is down.

# 4.20 Problem: NFM-P database corruption or failure

### 4.20.1 Solution

You can restore an NFM-P database using a backup copy.



**Note:** Before you perform a database restore operation, you must shut down the databases and main servers in the NFM-P system. Contact technical support before you attempt to perform a database restore.

In a redundant NFM-P system, you must perform one or both of the following to regain database function and redundancy:

- Restore the primary NFM-P database.
- Reinstantiate the standby NFM-P database.

Both operations are required after a primary database failure. After a standby database failure, no restore operation is required, but you must reinstantiate the standby database to restore redundancy. You can use the NFM-P client GUI or a CLI script to reinstantiate a database.

**Note:** In a redundant NFM-P system, you can restore a database backup only on a primary database station. To restore a database backup on a station other than the primary station, you must do the following on the station before you attempt the restore:

- Uninstall the NFM-P database, if it is installed.
- Install a primary NFM-P database on the station.

**i** Note: In a redundant NFM-P system, you can reinstantiate a database only on a standby database station. To reinstantiate a database on a station other than the standby station, you must do the following on the station before you attempt the reinstantiation:

- Uninstall the NFM-P database, if it is installed.
- Install a standby NFM-P database on the station.

See the *NSP System Administrator Guide* for information about restoring or reinstantiating an NFM-P main database.

## 4.21 Problem: The database is running out of disk space

#### 4.21.1 Database disk space

Sufficient database disk space is essential for efficient NFM-P database operation. You can also check whether your database backup schedule is adequate. Underscheduling backups while the database is in ARCHIVELOG mode creates numerous log files.

### 4.21.2 Steps

1

Verify that the database platform is adequately sized. See the *NSP Planning Guide* or consult technical support.

2 -

Verify that the thresholds for disk space and archive logs are sufficient for your network, and determine how the disk space is being used. Contact your technical support representative for more information.

3

Check the root database backup directory or partition to ensure that:

- · the size of the assigned disk space or slice is sufficient
- · the disk directory or slice is sufficient to hold the configured number of database backups

NSP

#### 4 —

If the disk directory has many archived log files due to underscheduling of database backups, contact your technical-support representative for information about deleting archived log files.

5 —

Back up the NFM-P database, as described in the NSP System Administrator Guide.

END OF STEPS

## 4.22 Problem: Frequent database backups create performance issues

#### 4.22.1 Overscheduling database backups

Overscheduling the number of database backups can affect database performance by consuming excessive system resources.

#### 4.22.2 Steps

1 -

Choose Administration  $\rightarrow$  Database from the NFM-P main menu. The Database Manager form appears.

2 –

Click on the Backup tab.

3 —

Check the Backup Interval and Interval Unit parameters. For example, setting the Backup Interval parameter to 6 and setting the Interval Unit parameter to hour means a backup is performed every 6 hours, or four times a day. Such frequent backups can cause performance issues.

**i** Note: Nokia recommends scheduling database backups to occur once daily.

4

Modify other parameters as required to improve performance.

5 —

Save your changes and close the Database Manager form.

END OF STEPS -

# 4.23 Problem: An NFM-P database restore fails and generates a No backup sets error

### 4.23.1 Solution



Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

Database backup sets expire based on a retention period. After the retention period passes, the database backup sets are set to expired. You cannot restore databases from expired backup sets. Contact your technical support representative for assistance with an NFM-P database restore failure.

## 4.24 Problem: NFM-P database redundancy failure

## 4.24.1 Steps



Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

1

Ensure that the database redundancy configuration is correct, as specified in the *NSP Installation and Upgrade Guide*:

- The primary and standby database directory structures and disk partition configurations are identical.
- The same OS version and patch level, and the same NFM-P software release and patch level, are installed on the primary and standby database stations.

2

Ensure that there are no network communication problems between the primary and standby database stations; see Chapter 3, "Troubleshooting the NSP platform".

END OF STEPS

# 4.25 Problem: Primary or standby NFM-P database is down

### 4.25.1 Primary or standby database is down

The status bar of the NFM-P client GUI indicates that the primary or standby database is down.

## 4.25.2 Steps

# WARNING Equipment Damage

Performing NFM-P database modifications using Oracle database tools can cause irreparable harm to the NFM-P database and the network management data, and can void your warranty or support agreement.

Contact your technical support representative for assistance with database troubleshooting.

1

Verify the correct IP address and instance name of the database. From the NFM-P main menu, select Administration→Database to open the Database Manager. Verify the information in the Instance Name and DB Server fields.

2 -

Verify the network connectivity between the NFM-P primary server and the primary or standby database by ensuring that the primary server and the primary or standby database can ping each other; see Chapter 3, "Troubleshooting the NSP platform".

END OF STEPS

# 4.26 Problem: Need to verify that Oracle database and listener services are started

## 4.26.1 Purpose

Perform the following procedure to determine the status of the Oracle database and listener services, each of which starts automatically during NFM-P database station initialization.

## 4.26.2 Steps

1

Open an NFM-P GUI client.

#### 2 —

View the status bar at the bottom of the GUI. The background of the NFM-P database section of the status bar is yellow or red when there is a problem with a service. The status bar text indicates the database service status.

END OF STEPS

## 4.27 Problem: Need to determine status or version of NFM-P database or Oracle proxy

#### 4.27.1 Purpose

Perform the following procedure to determine the status of the NFM-P database or Oracle proxy, each of which starts automatically during NFM-P database station initialization.

#### 4.27.2 Steps

1 -

Log in as the Oracle management user on the database station.

2 —

Open a console window.

3

Navigate to the /opt/nsp/nfmp/db/install/config/db directory

4 —

Enter the following command.

```
bash$ ./oracleproxy.sh option 4
```

where option is one of the options in the table below.

Table 4-5 oracleproxy.\* flag options

Flag option	Description
start	Starts the Oracle proxy
no option, or help	Lists the available options
proxy_version	Displays Oracle proxy version information
proxy_status	Displays Oracle proxy status information
db_version	Displays NFM-P database version information
db_status	Displays NFM-P database status information

5 \_\_\_\_\_

Review the command output.

The following sample shows the output of the proxy\_status option.

Proxy is UP The following sample shows the output of the db\_version option.

NSP Version Release - Built on Wed Mar 27 03:14:15 EST 20XX

6

Close the console window.

END OF STEPS

# **Troubleshooting NFM-P server issues**

## 4.28 NFM-P server troubleshooting overview

#### 4.28.1 Problems associated with the NFM-P server

NFM-P server statistics collection is a useful troubleshooting tool for memory, alarm, and SNMP issues on an NFM-P main or auxiliary server. See the *NSP NFM-P Statistics Management Guide* for more information.

When no NE is associated with an NFM-P alarm, the alarm Site ID and Site Name properties are populated with the IP address and hostname, respectively, of the NFM-P main or auxiliary server that raised the alarm.

# 4.29 Problem: Cannot start an NFM-P server, or unsure of NFM-P server status

### 4.29.1 Server status indicators

The NFM-P main or auxiliary server startup script provides server status indicators that include the following:

- · how long the server has been running
- the used and available memory
- the NFM-P database connectivity status
- NFM-P license capacity

### 4.29.2 Steps

1 -

Log in to the NFM-P server as the nsp user.

2 \_\_\_\_\_

Open a console window.

3 \_\_\_\_\_

To check the status of an NFM-P main server, perform the following steps.

1. Enter the following:

/opt/nsp/nfmp/server/nms/bin/nmsserver.bash appserver\_status +
The general server status is displayed.

2. Enter the following at the CLI prompt:

/opt/nsp/nfmp/server/nms/bin/nmsserver.bash nms\_status +
Detailed NFM-P server information is displayed.

3. To obtain more specific server status information, run the nmsserver script in step 3 using the appropriate option from the following table in place of the nms\_status or appserver\_status option.

Option	Description
start	Starts the NFM-P main server in a non-interactive mode
stop	Stops the NFM-P main server
debug	Starts the NFM-P server in an interactive mode. <b>Note:</b> The server shuts down if the console is closed or if Ctrl-C is pressed.
appserver_status	Returns information about the status of the NFM-P main server (both active and standby servers when the NFM-P is configured for redundancy)
appserver_version	Returns NFM-P software release information that includes the start time of the current NFM-P main server instance
nms_status	Returns the following information: <ul> <li>NFM-P standalone, primary, or standby server start time and running time</li> </ul>
	<ul> <li>total used and available memory</li> </ul>
	NFM-P database connectivity status
	<ul> <li>redundancy configuration and status</li> </ul>
	NFM-P license information
	JVM memory-usage information
	alarm forwarding information
	basic auxiliary server information
	number and status of current process threads
-v nms_status	Verbose version of the nms_status option that returns the following additional information:
	<ul> <li>ID and status of the current process threads</li> </ul>
	general JMS server information
	<ul> <li>currently connected JMS subscribers, by topic</li> </ul>
-s nms_status	Short version of the nms_status option that returns the following information:
	system information
	• IP address
	NFM-P database information
	installation information

#### NFM-P main-server startup script options

Option	Description
nms_info	Returns the following information from the NFM-P database: • number of managed devices by device type; for example, 7750 SR • number of MDA ports by type • number of equipped ports by type • number of services by type; for example, IES or VLL • number of access interfaces, connection termination points, and channels, by type
	<ul> <li>number of alarms, listed in order of severity</li> <li>lists of enabled statistics, file, and accounting policies, including the counts and the polling frequency for different types of objects</li> </ul>
nms_version	Returns NFM-P software release information
jvm_version	Returns version information about the currently running Java Virtual Machine environment
script_env	Returns main server script environment information
read_config	Rereads the nms-server.xml server configuration file while the server is running in order to put configuration file updates into effect
force_restart	Forces the NFM-P main server to restart
force_stop	Forces the NFM-P main server to stop
passwd <username> <current> <new> where username is the NFM-P database username, for example, samuser current is the current password new is the new password</new></current></username>	Changes the NFM-P database user password
read_metrics_config	Reads the server metrics configuration file
import_license	Imports a new license zip file for the server
threaddump	Prints a thread dump for every SAM java process running on the station
webstart	Starts the web server
webstop	Stops the web server
webstatus	Prints web server status
webforce_restart	Forces the web server to restart
webforce_stop	Forces the web server to stop and not restart
jmsstart	Starts the JMS server in interactive mode
jmsstop	Stops the JMS server

Option	Description
jmsstatus	<ul><li>Returns information that includes the following:</li><li>general JMS server information</li><li>currently connected JMS subscribers, by topic</li></ul>
jmsread_config	Rereads the JMS server configuration file while the JMS server is running
jmsforce_restart	Forces the JMS server to restart
jmsforce_stop	Forces the JMS server to stop
jmsjvm_version	Returns version information about the currently running Java Virtual Machine environment
jmsappserver_status	Returns the JMS server status
jmsscript_env	Returns the JMS script environment
no keyword, help, or ?	Lists the available command options

4

To check the status of an NFM-P auxiliary server, perform the following steps.

1. Enter the following at the CLI prompt:

/opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash aux\_status + The general server status is displayed.

2. Enter the following at the CLI prompt:

/opt/nsp/nfmp/auxserver/nms/bin/auxnmsserver.bash auxappserver\_ status ↓

Detailed NFM-P server information is displayed.

3. To obtain more specific server status information, run the nmsserver script using the appropriate option from the following table in place of the aux\_status or appserver\_status option.

#### NFM-P auxiliary-server startup script options

Option	Description
auxappserver_status	Returns information about the operational status of the auxiliary server
auxdebug	Starts the auxiliary server in interactive mode
auxforce_restart	Forces the auxiliary server to restart
auxforce_stop	Forces the auxiliary server to stop
auxjvm_version	Returns the auxiliary server JVM version
auxread_config	Directs the auxiliary server to read and apply the settings in the general configuration file

Option	Description
auxread_metrics_config	Directs the auxiliary server to read and apply the settings in the metrics configuration file
auxscript_env	Returns auxiliary server script environment information
auxstart	Starts the NFM-P auxiliary server
auxstatus	Returns information about the auxiliary server that includes the following:
	• IP address
	port number
	NFM-P database connections
	installed server software release ID
auxstop	Stops the NFM-P auxiliary server
aux_version	Returns auxiliary server software release information
auxthreaddump	Returns a thread dump for every auxiliary server process currently running on the station
auxhelp, no keyword, or ?	Lists the available command options

#### 5 -

Review and record the displayed information for technical support, if required.

#### 6 —

Close the console window.

#### 7 —

View the NFM-P server logs for error messages using the LogViewer utility, as described in Chapter 5, "Network troubleshooting using NSP functions".

8

Report the error messages that you find to a technical support representative.

END OF STEPS -

## 4.30 Problem: NFM-P server and database not communicating

#### 4.30.1 Purpose

Perform this procedure when an NFM-P server cannot connect to an NFM-P database.

### 4.30.2 Steps

#### 1

Verify network connectivity between both the primary and standby servers and the primary and standby NFM-P databases by ensuring that both the primary and standby servers and the primary database can ping each other. See Chapter 3, "Troubleshooting the NSP platform".

2

Ensure that the ports specified at installation time are available and not being blocked by firewalls; see Chapter 3, "Troubleshooting the NSP platform".

3

Perform the following troubleshooting activities for the primary NFM-P database, as described in 4.25 "Problem: Primary or standby NFM-P database is down" (p. 79).

- Verify the NFM-P database IP address and instance name.
- Verify that the database instance is running.
- Verify that the database is running in the correct mode.

END OF STEPS

## 4.31 Problem: An NFM-P server starts up, and then quickly shuts down

#### 4.31.1 Solution

When a server starts then stops, collect the logs identified in 4.2 "To collect NFM-P log files" (p. 44) and contact your technical support representative.

## 4.32 Problem: Client not receiving server heartbeat messages

### 4.32.1 Purpose

Perform this procedure when an NFM-P client is not receiving heartbeat messages.

### 4.32.2 Steps

1

Verify network connectivity between both the primary and standby servers and the clients by ensuring that both the primary and standby servers and the clients can ping each other. See Chapter 3, "Troubleshooting the NSP platform".

#### 2 -

Verify that the NFM-P server and client clocks are synchronized. To set the date and time for NFM-P server and client clocks, see the *NSP System Administrator Guide*.

END OF STEPS

## 4.33 Problem: Main server unreachable from RHEL client station

#### 4.33.1 Purpose

Perform this procedure to check the IP connectivity between an NFM-P client and main server using ping commands. When the ping commands indicate that IP communication is active but there are still IP reachability issues, the problem could be poor LAN performance.

#### 4.33.2 Steps

#### 1

Perform a ping test to measure reachability, as described in 6.23 "Problem: Lost connectivity to one or more network management domain stations" (p. 359).

2 -

If you cannot ping the main server from a RHEL single-user client or client delegate server station, ensure that the server hostname is in the /etc/hosts file on the client station.

- 1. Log on to the client station as the root user.
- 2. Enter the following:
  - # cd /etc ↓
- 3. Open the hosts file with a plain-text editor such as vi.
- 4. Edit the file, as required, to contain the following:

```
server_IP server_hostname
```

where

*server\_IP* is the IP address of the main server

server\_hostname is the hostname of the main server

5. Save the changes and close the file.

#### END OF STEPS -

# 4.34 Problem: Excessive NFM-P server-to-client response time

### 4.34.1 Increasing available server network management resources

As the number of managed devices grows and as more GUI or OSS clients are brought online, the processing load on the NFM-P system increases. For optimum NFM-P performance, you must ensure that the NFM-P configuration meets the requirements in the *NSP Planning Guide* as your network expands.

You can do the following to increase the available NFM-P server network management resources:

- Deploy the NFM-P system in a distributed configuration.
- Deploy the NFM-P system in a redundant configuration.
- Deploy NFM-P auxiliary servers.
- Reallocate the NFM-P server resources that are assigned to groups of managed devices.

See the NSP NFM-P Classic Management User Guide, , and the NSP Installation and Upgrade Guide for information about a particular option. Contact technical support for reconfiguration assistance.

Perform this procedure to check the following:

• NFM-P auxiliary server status

System performance may degrade if the number of available Preferred and Reserved auxiliary servers drops below the number of configured Preferred auxiliary servers.

• NFM-P main server status

Alarms raised against the NFM-P main server may provide information about the performance degradation.

### 4.34.2 Steps

## CAUTION

### Service Disruption

Only Nokia support staff are qualified to assess and reconfigure an NFM-P deployment.

Contact your technical support representative for assistance.

1 –

Open an NFM-P client GUI.

2 —

 $\label{eq:choose} Choose \ Administration \rightarrow System \ Information. \ The \ System \ Information \ form \ opens.$ 

3

Click on the Faults tab to view auxiliary server and general NFM-P system alarm information, if required.

#### 4 –

If your NFM-P deployment includes one or more auxiliary servers, perform the following steps to check the status of each auxiliary server.

- 1. Click on the Auxiliary Servers tab.
- 2. Review the list of auxiliary servers.
- 3. Select an auxiliary server in the list and click Properties. The properties form for the auxiliary server is displayed.
- 4. Review the information, which includes:
  - · the auxiliary server IP address
  - the auxiliary server hostname
  - the auxiliary server port number
  - the auxiliary server type (Reserved or Preferred)
  - the auxiliary server status (Unknown, Down, Up, or Unused)
- 5. If the auxiliary server status is Down, perform 4.29 "Problem: Cannot start an NFM-P server, or unsure of NFM-P server status" (p. 82) on the auxiliary server.
- 6. If the auxiliary server status is Unknown, perform 4.39 "Problem: Slow or failed resynchronization with network devices" (p. 94) to check the connectivity between the managed network and the main and auxiliary servers.
- 5 –

Close the System Information form.

END OF STEPS -

# 4.35 Problem: Unable to receive alarms on the NFM-P, or alarm performance is degraded

#### 4.35.1 General information

By default, the system begins purging alarms when the outstanding alarm count reaches 50 000, unless historical alarm record logging and purging alarm policies are configured to keep the outstanding alarm count below that level.

#### 4.35.2 Steps

# CAUTION Service Disruption

Exceeding the alarm limit configured in the nms-server.xml file may cause system performance problems.

Contact your technical support representative for assistance.

Check the status bar of the NFM-P client GUI status bar for indications that the maximum number of alarms for the system is reached.

2 -

If required, clear outstanding alarms or delete them to the alarm history record log, as described in the NSP NFM-P Classic Management User Guide.

3

1 -

If the NFM-P system includes one or more auxiliary servers, perform 4.34 "Problem: Excessive NFM-P server-to-client response time" (p. 89) to ensure that system performance is not degraded because of auxiliary-server unavailability.

4

Contact your technical support representative for more information.

END OF STEPS -

#### 4.36 Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving

### 4.36.1 Configuration for SNMP trap notifications

When you install the NFM-P, you specify the port on which SNMP traps arrive.

In addition, the following configuration is required for SNMP trap notifications to work:

- · Enable the SNMP parameters on the devices before managing them.
- Ensure that a unique trapLogId is specified for each router to communicate with the NFM-P.



**i** Note: You must have sufficient user permissions, for example, admin permissions, to configure SNMP on a device.

## 4.36.2 Steps

1

See the commissioning chapter of the NSP NFM-P Classic Management User Guide for more information about configuring devices for NFM-P management.

2 -

Configure SNMP on the device using CLI.

END OF STEPS -

## 4.37 Cannot manage new devices

### 4.37.1 New devices cannot be managed

The possible causes are:

- The number of managed devices or MDAs exceeds the licensed quantity.
- Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU, causing resynchronizations to fail.

Additional devices cannot be managed, but can be discovered, when the licensed MDA limit is exceeded.

4.37.2 Steps



Do not modify other nms-server.xml parameters. Modifying the file can seriously affect network management and performance of the NFM-P.

Consult technical support before you attempt to modify parameters.

1 -

Check the license key status.

- 1. The NFM-P generates an alarm when a license limit is exceeded or nearly exceeded. View the NFM-P alarm list in the client GUI, or use an OSS client to monitor the JMS alarm event stream for license alarms.
- 2. Choose Help→NFM-P License Information from the NFM-P main menu. The NFM-P License (Edit) form opens.
- 3. Click on the Devices and Quantities Licensed tab.
- 4. View the information to ensure that the required Remaining quantity is not equal to zero. **Note:**

If you have a new license that supports a greater number of managed objects, you can dynamically update the license without restarting the main server. See the *NSP NFM-P Classic Management User Guide* for information about updating an NFM-P license.

5. Close the NFM-P License (Edit) form.

Ensure that the new devices are configured to send SNMP packets of up to 9216 bytes. Check the MTU size, as described in 6.25 "Problem: Packet size and fragmentation issues" (p. 361).

END OF STEPS

<sup>2 -</sup>

# 4.38 Problem: Cannot discover more than one device, or device resynchronization fails

## 4.38.1 General information

Consider the following:

- When using SNMPv3 encryption, the engine ID of the managed device must be unique. As well, SNMP issues may result in Polling Problem alarms. Otherwise, the following issues may occur:
  - unreliable or slow discovery of network devices
  - resynchronization during scheduled polling fails
  - slow communication and synchronization times
  - polling fails completely
- When NFM-P resynchronizes some functions on an NE, for example, BGP configurations for the 7750 SR, the SNMP packets may be broken into two or more smaller packets, when the maximum PDU size of 9216 bytes is exceeded.
- Each MIB entry policy has its own polling interval. When there is insufficient time in a polling interval for a resynchronization to occur, the interval may need to be changed to ensure proper resynchronization.

## 4.38.2 Steps

1 -

For resynchronization issues that may be caused due to insufficient MIB polling intervals.

2

Choose Administration  $\rightarrow$  Mediation from the NFM-P main menu. The Mediation (Edit) form opens with the General tab selected.

3

Ensure that the Polling Admin State is Up.

**Note:** Polling and scanning use system resources, and can increase the amount of management traffic. Consider your network needs and network management domain capabilities before setting these parameters.

4 -

i

Check the MIB polling intervals for different managed devices, as required, by clicking on the MIB Entry Policies tab.

A list of MIBs appears, organized by managed device type.

- 1. Select a MIB in the list and click Properties.
- 2. Configure the Polling Interval parameter to ensure that sufficient time is configured for the polling to occur.
- 3. Configure the Administrative State of polling for the MIB entry, if required.

4. Click OK to save the changes and close the form, or click Cancel to close the form without saving changes, as required.

END OF STEPS

## 4.39 Problem: Slow or failed resynchronization with network devices

#### 4.39.1 General information

When NFM-P performance is slow, especially when performing network device resynchronizations, SNMP and IP performance along the in-band or out-of-band interfaces between the network device and the NFM-P server may be the problem.

Check the following:

- configuration of the LAN switch port and the NFM-P station port match
- · configuration of the LAN switch port and the network device management ports match
- mediation policy SNMP timeout and retry values are sufficient to allow the transfer of data between network devices and the NFM-P

#### 4.39.2 Steps

1 -

Ensure that port configurations are compatible for the NFM-P server, the network device management ports, and the LAN switch. This is normally done by configuring auto-negotiation between the platforms, but your network may require more specific configuration.

2

Check whether all data is being transferred between the network device in-band management port and the NFM-P server.

- 1. Open a Telnet or SSH session to the device from the NFM-P.
- 2. Check statistics on the in-band management port of the device:

```
# monitor port 1/2/3
```

Check the output for the following.

- errors that may indicate a communication problem with the a LAN switch.
- Over each time interval, is the number of input and output packets constant? This may indicate intermittent traffic.
- Are there more input packets or octets being transferred than output packets or octets? This may indicate a unidirectional traffic problem.

The types of error messages displayed determine the action to take.

- · For failure errors, consider increasing the SNMP timeout value
- For collision errors, consider increasing the SNMP retry value
- 3. Check the mediation policy for the device using the NFM-P client GUI. Check the SNMP timeout and retry value for the mediation policy.

If the output of step 2 indicates failures, consider increasing the default SNMP timeout value and perform step 2 again.

When the output of step 2 indicates frequent collisions, consider increasing the default SNMP number of retries value, then retest to see if resynchronizations are more reliable. Increasing the number of retries increases the likelihood that an SNMP packet is not dropped due to collisions.

You can check SNMP timeout and retry values from the Administration $\rightarrow$ Mediation menu. Click on the Mediation Security tab.

#### CAUTION:

When LAN performance is poor, increasing timeout values may mask an underlying problem. Increasing the SNMP timeout value in an environment where collisions are frequent reduces performance. Timeout values should be based on typical network response times

Check LAN communication issues, as specified in Chapter 3, "Troubleshooting the NSP platform". If problems persist, collect the logs as specified in 2.1 "Before you call support" (p. 25) and contact your technical support representative.

END OF STEPS

# 4.40 Problem: Statistics are rolling over too quickly

#### 4.40.1 Problem

Statistics database tables roll over, or lose statistics during an interval, if the tables fill before all statistics are collected or the next collection interval starts.

#### Solution

To ensure sufficient statistics collection, consider the following:

- the statistics table size, depending on the configuration specified in the NSP Installation and Upgrade Guide
- the number of statistics collected, the number of objects with statistics collection enabled, and the frequency of statistics collection, as specified in the NSP NFM-P Classic Management User Guide
- the OSS requests data from the statistics tables less frequently than the configured rollover interval
- FTP must be enabled on the managed device in order for the NFM-P to retrieve statistics.

Nokia recommends that statistics collection planning includes the following considerations to prevent the loss of statistics data.

- · measure the rate of statistics collection over a sufficient time interval
- determine the appropriate collection interval and statistics database table size based on individual network configurations
- ensure that the polling interval is sufficient for polled statistics

# 4.41 Problem: Y.1564 service test results not published to Kafka

## 4.41.1 General information

Y.1564 service test results are not published to Kafka if the test has timed out.

When this situation occurs, the **staleTestTime** duration must be updated to prevent timeouts.

## 4.41.2 Steps

# CAUTION Service Disruption

Modifying the nms-server.xml file can have serious consequences that can include service disruption.

Contact technical support before you attempt to modify the nms-server.xml file.

1 Log in to the main server station as the nsp user.

2 \_\_\_\_\_

Open a console window.

3

4

Navigate to the /opt/nsp/nfmp/server/nms/config directory.

Create a backup copy of the nms-server.xml file.

5

Open the nms-server.xml file using a plain-text editor such as vi.

6

Edit the following line:

staleTestTime="value"

Update the value to reflect the required test duration interval to avoid timeout.

7 ——

Save and close the nms-server.xml file.

8

On a standalone main server, or the primary main server in a redundant system, enter the following:

bash\$ /opt/nsp/nfmp/server/nms/bin/nmsserver.bash read\_sync 4
The NFM-P puts the configuration change into effect.

Close the console window.

10 -

9

Re-run the Y.1564 service tests, with the **Publish to Kafka** parameter enabled.

END OF STEPS

# **Troubleshooting NFM-P clients**

# 4.42 Problem: Cannot start NFM-P client, or error message during client startup

## 4.42.1 Prerequisites

Before you proceed, ensure that the following conditions are present:

- the NFM-P client and server have the same software versions and compatible patch sets
- the login name and password of the user are correct
- there are no OS errors
- a local firewall is running on the client station

### 4.42.2 Steps

#### 1 –

If the NFM-P client is installed on RHEL and you receive a "Cannot execute" message when you try to run the client, the client executable file permission may have been reset by an event such as an auto-client update failure. You must ensure that the correct file permissions are assigned.

- 1. Log in as root, or as the user that installed the client, on the client station.
- 2. Open a console window.
- 3. Enter the following:

```
# chmod +x path/nms/bin/nmsclient.bash
```

where path is the NFM-P client installation location, typically /opt/nsp/client

#### 2 -

Review the login messages that are displayed when a client GUI attempts to connect to a server. Messages that state things like the server is starting or the server is not running indicate the type of problem.

#### 3

Ensure that the user name and password are correct.

#### 4

To check that the NFM-P server is up and to view additional server configuration information, perform the following steps.

- 1. Log on to the NFM-P server station as the nsp user.
- 2. Open a console window.
- 3. Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4. Enter the following:

```
./nmsserver.bash appserver_status 🗸
```

Server status and configuration information are displayed.

5. To check additional server status conditions, perform 4.29 "Problem: Cannot start an NFM-P server, or unsure of NFM-P server status" (p. 82).

5 —

Check the client GUI login error message.

When a firewall is running locally on the client station, a login error message may appear indicating that the server is not available. Ensure that a local firewall is not preventing a connection to the server, and that the NFM-P server IP address is in the client host-lookup file.

END OF STEPS -

## 4.43 Problem: NFM-P client unable to communicate with NFM-P server

#### 4.43.1 Prerequisites

Before you proceed, ensure that the following conditions are present:

- The NFM-P client points to the correct IP address and port of the server.
- The problem is not a network management domain LAN issue. See Chapter 3, "Troubleshooting the NSP platform" for more information.
- · Firewalls between the NFM-P clients and the server are correctly configured

#### 4.43.2 Steps

1 –

To check that the NFM-P client points to the correct IP address and port of the server, open the nms-client.xml file using a text editor. The default file location is *installation\_directory*/nms/ config.

where *installation\_directory* is the directory in which the NFM-P client software is installed, for example, /opt/nsp/client

2 —

Verify the IP address of the server as specified by the ejbServerHost parameter.

3 —

Verify the server port as specified by the ejbServerPort parameter.

4 —

Modify the IP address and port values, if required.

#### 5 —

Save the file, if required.

6

Perform 4.29 "Problem: Cannot start an NFM-P server, or unsure of NFM-P server status" (p. 82) to check the server status. A client cannot connect to an NFM-P server that is not started.

7 —

If the server is started, compare the firewall and network configuration guidelines in the *NSP Planning Guide* with your network configuration to ensure that it complies with the guidelines.

8

Contact your technical support representative if the problem persists.

END OF STEPS -

## 4.44 Problem: Delayed server response to client activity

## 4.44.1 Causes

Possible causes are:

- a congested LAN
- improperly sized platforms

Using the netstat command on the client may help troubleshoot network throughput problems. When an Ethernet LAN is highly congested, the actual throughput slows down. This is caused by packets colliding on the LAN as multiple machines begin to transmit at approximately the same time, for example, when multiple GUI or OSS clients are performing tasks simultaneously.

#### 4.44.2 Steps

Client GUIs may respond more slowly than normal during resynchronizations of managed devices. Repeat the client GUI action when the resynchronization is complete.

2 —

Check for LAN throughput issues.

- 1. Open a shell console window.
- 2. Enter the following at the console prompt to display local network-interface transmission data over a period of time:
  - # netstat -i *s* ↓

<sup>1 -</sup>

where *s* is the time, in seconds, over which you want to collect data. Nokia recommends that you start with 50 s

3. Review the output. The following is sample netstat output:

```
netstat -i 5
input le0
                  output
                                   input (Total)
                                                      output
packets errs packets errs colls packets errs packets
errs colls
                             49998 6454787 41
6428555 41
              541360 80
                                                  567592 80
49998
        0
22
                       0
                             Ο
                                   22
                                            Ω
                                                  \cap
                                                           0
                                                                 0
              \cap
71
        0
              7
                       0
                             3
                                   71
                                            0
                                                  7
                                                           0
                                                                 3
```

This sample displays the number of input and output packets, errors and collisions on the le0 interface. One column displays the totals for all interfaces. This sample only has one interface, so both sets of columns display the same data.

Calculate the number of collisions as a percentage of the number of output packets. For example, according to the last line of output, there were three collisions and seven output packets resulting in a 42% rate.

This number is high, but the time in which the sampling was obtained (5 s), was low. Change the sample rate to, for example, 50 s for an accurate sampling of the network throughput.

When collisions are between 2% and 5%, congestion on the interface is within the normal operating range.

In a typical network, when collisions are greater than 5%, you may have a serious congestion problem on the interface. Review your LAN topology and design to reduce the number of network bottlenecks.

- 4. To stop the command, press Ctrl-C.
- 3

Check that the server and client platforms are appropriately sized. See the *NSP Planning Guide* for more information.

END OF STEPS

## 4.45 Problem: Cannot place newly discovered device in managed state

#### 4.45.1 Solution

If the newly discovered device cannot be placed in a managed state, ensure that the number of managed MDAs do not exceed the NFM-P license. Also, check for resynchronization problems between the managed network and the NFM-P. See 4.37 "Cannot manage new devices" (p. 92).

# 4.46 Problem: User performs action, such as saving a configuration, but cannot see any results

### 4.46.1 Causes

Possible causes are:

- Failed SNMP communication between the server and managed device; see 4.36 "Problem: All SNMP traps from managed devices are arriving at one NFM-P server, or no SNMP traps are arriving" (p. 91).
- Failed deployment of the configuration request.

## 4.46.2 Steps

1 —

For the NFM-P client, perform the following:

1. Choose Administration  $\rightarrow$  NE Maintenance  $\rightarrow$  Deployment from the NFM-P main menu.

The Deployment form opens. Incomplete deployments are listed, and deployer, tag, state and other information is displayed.

The possible states for a deployment are:

- Deployed
- Not Deployed
- Pending
- Failed Resource Unavailable. Failure occurred because one of the resources required to apply the configuration is not present in the NFM-P database
- Failed Configuration. Failure occurred because the configuration could not be applied to the specified objects
- Failed Partial. Failure occurred at deployment and some of the configuration can been sent to the network
- Failed Internal Error. Failure a occurred due to general error conditions. Code is intended as a catch-all code for all other possible errors
- Cancelled
- Postponed

You can also suspend or resume deployment retries by clicking Suspend Retries or Resume Retries. You can clear a deployment by clicking Clear. When you clear a deployer, no further attempt is made to reconcile the network device status with the NFM-P database. Affected objects should be resynchronized.

If a deployment is not sent to a managed device, the intended configuration change is not made on the device.

2. Choose a failed deployment and click Properties to view additional information. The deployment properties form opens.

2 -

When a deployment fails and you receive a deployment alarm, check the following steps:

- 1. Using CLI, check on the device whether the deployment change is on the device.
- 2. If the change is on the device, the deployment alarm was likely raised because the configuration already exists on the device. Clear the failed deployment and resynchronize the device with the NFM-P.

If the change is not on the device, collect the information from the deployment properties form and contact your technical support representative.

```
3
```

**Note:** These steps describe how to troubleshoot asynchronous deployment requests only. Nokia recommends that deployment requests be made in asynchronous mode.

For OSS clients, perform the following steps:

1. Browse real-time alarms received via JMS. An alarm denoting a deployment failure contains the following text:

Attribute: alarmClassTag Value: generic.DeploymentFailure

The alarm also contains additional information, including the object affected by the alarm and the severity of the alarm. See the *NSP NFM-P XML API Developer Guide* for more information.

2. Find the following text in the alarm:

Attribute: requestID=requestID

The parameter specifies the request id sent with the original request. The request id should be unique per request.

- 3. Determine the original request using the request id.
- 4. Troubleshoot the original request. If there are problems with the original request, clear the deployer, fix the request, and send the new request. See the *NSP NFM-P XML API Developer Guide* for more information.
- 5. If there are no problems with the original request, the failure may be caused by a network communication or device failure, or by packet collisions caused by conflicting configurations.

You can:

- · resend the request
- · troubleshoot your network or device

END OF STEPS

# 4.47 Problem: Device configuration backup not occurring

### 4.47.1 Steps

1

- Use the NFM-P client to check the device database backup settings. Choose Administration→NE Maintenance→Backup/Restore from the NFM-P main menu. The Backup/ Restore form opens.
- Click on the Backup/Restore Status tab. The managed devices are listed and backup and restore status information is displayed.
- 3

2 -

Select the device and click Properties. The NE Backup/Restore Status form opens.

4

View the information in the Backup Status panel. A Backup State other than Successful may indicate a communication problem or a backup policy configuration error.

5

Ensure that the device configuration file and the associated index file are saved on the device and available for backup. Click on the Configuration Saves tab, and ensure that the Config Save State indicator reads Success.

See the appropriate device OS documentation for more information.

6 —

Click on the Backups tab to view a list of backup operations that are currently in progress. A backup operation disappears from the list after it completes.

7

Click on the Faults tab to view additional troubleshooting information.

8

Close the NE Backup/Restore Status form. The Backup/Restore form is displayed.

9

Use the information obtained from the NE Backup/Restore Status form to check the backup policy configuration, if required. Click on the Backup/Restore Policy tab.

10 —

Select the backup policy for the device and click Properties. The Backup Policy (Edit) form opens.

#### 11 —

Ensure that the policy is assigned to the device.

- 1. Click on the Backup/Restore Policy Assignment tab.
- 2. If required, configure a filter and click OK.
- 3. Move the device to the Assigned Sites list if it is not there by selecting the site from the Unassigned Sites list and clicking on the right-arrow button.
- 4. Click Apply to save changes, as required.

12 \_\_\_\_\_

Click on the General tab.

13 \_\_\_\_\_

Verify the parameter settings and modify, if required.

14 \_\_\_\_\_

Save the changes and close the form.

END OF STEPS -

## 4.48 Problem: NFM-P client GUI shuts down regularly

#### 4.48.1 Causes

The NFM-P client GUI automatically shuts down under the following conditions:

- · no activity on the GUI for a specified amount of time
- no communication between the GUI and the server for a specified amount of time.
- · when there is an communication error that causes problems between the server and the client

**i** Note: Changing the OS clock setting on the server station can cause communication problems on the client. If the server clock setting changes significantly, the clients must log off and the server must be restarted. Nokia recommends that the server OS clock be tied to a synchronous timing source to eliminate time shifts that may lead to polling and communication problems.

### 4.48.2 Steps

1 –

Disable the GUI activity check, if required. Choose Administration→Security→NFM-P User Security from the NFM-P main menu. The Security Management (Edit) form appears with the General tab selected.

NSP

#### 2

Set the Client Timeout (minutes) parameter to 0 to disable the GUI inactivity check. Alternately, you can configure a higher value for the parameter, to increase the time that must pass before the client GUI is shut down due to inactivity.

3

Click Apply and close the form.

END OF STEPS

# 4.49 Problem: Configuration change not displayed on NFM-P client GUI

### 4.49.1 Solution

The NFM-P supports the configuration of complex objects, for example, services, using configuration forms or templates. Additional configuration forms and steps may be contained by main, or parent, configuration form. For example, when you configure a VLL service, a site configuration form is contained within the main configuration form. In turn, an L2 interface configuration form is contained within the site configuration form. Alternatively, when you use service templates, parent templates for site configuration must also be configured.

Objects configured in contained configuration forms are not saved until the parent configuration form is saved. For example, when you configure a VLL service, sites or L2 interfaces that you configure are not saved during service creation until the parent configuration form is saved. You cannot view new objects or new object configurations in other parts of the GUI, such as the navigation tree, until the service is saved. The NFM-P displays a dialog box to indicate that configured objects in a configuration form are not saved until the parent configuration forms are saved.

## 4.50 Problem: List or search function takes too long to complete

### 4.50.1 Solution

You can perform simple listings or complex searches using the Manage menu on the NFM-P main menu to query the database for information about services, customers, and other managed entities.

Depending on the type of information and the number of entries returned, a list or search operation may take considerable time to complete. As a general rule, Nokia recommends that you use filters to restrict the number of items in a list or search operation to 10 000 or fewer.

See the NSP NFM-P Classic Management User Guide for information about the NFM-P client GUI list and search functionality. See the NSP Planning Guide for information about NFM-P scalability and system capacity guidelines.

# 4.51 Problem: Cannot select some menu options or save some configurations

### 4.51.1 Solution

An NFM-P administrator can restrict user access to GUI functions, and limit the ability of a user to configure objects. See your administrator for information about your general user permissions, scope of command, and span of control.

The NFM-P license may also affect user access to functions or objects; see the *NSP System Administrator Guide* for information.

An administrative change to a user or group permission takes effect immediately, and determines which actions are available to the user or user group.

See 4.37 "Cannot manage new devices" (p. 92) to identify which NEs are licensed for NFM-P management.

# 4.52 Problem: The NFM-P client GUI does not display NE user accounts created, modified, or deleted using the CLI

### 4.52.1 Cause

When an NE user account is created, modified, or deleted using the CLI, the NFM-P client GUI does not update the user list in the NE User Profiles form. For increased security, the NE does not send a trap for changes made to NE user accounts. You can update the NFM-P with the NE user account changes by resynchronizing the NE.

## 4.52.2 Steps

1 -

On the Equipment tree, navigate to the NE. The path is Network $\rightarrow$ NE.

2

Right-click on the NE and choose Resync.

The Resync menu option specifies that SNMP MIB and CLI information bases are reread to resynchronize them with the NFM-P, which also resynchronizes the network management settings with the router. Resynchronization does not impact the contents of the historical statistics database.

END OF STEPS
# Part III: Troubleshooting the network

# **Overview**

## Purpose

This part provides information about network troubleshooting using NSP functions and NFM-P.

## Contents

Chapter 5, Network troubleshooting using NSP functions	111	
Chapter 6, Network troubleshooting using NFM-P	331	

# 5 Network troubleshooting using NSP functions

## 5.1 Overview

## 5.1.1 Purpose

This chapter provides information about troubleshooting using various NSP functions and dashboards.

For more information on alarm management, see the NSP Network Service and Assurance Guide.

## 5.1.2 Contents

5.1 Overview111Troubleshooting using NSP assurance functions1125.2 Troubleshooting services and connectivity1125.3 Onboarding an NE into NSP1135.4 Onboarding a service into NSP1555.5 LSP Throughput with Forecast reporting scenario1755.6 SAP Throughput reporting scenario2165.7 End-to-end NE troubleshooting scenario2405.9 End-to-end service troubleshooting scenario2895.10 End-to-end port troubleshooting scenario2895.10 End-to-end port troubleshooting scenario3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3225.14 Troubleshooting Analytics reporting3225.15 Troubleshooting analytics reporting3245.15 Troubleshooting at a storage3225.14 Troubleshooting at a storage3245.15 Evaluating failed or slow workflow executions324		
5.2 Troubleshooting services and connectivity1125.3 Onboarding an NE into NSP1135.4 Onboarding a service into NSP1555.5 LSP Throughput with Forecast reporting scenario1755.6 SAP Throughput reporting scenario1945.7 End-to-end NE troubleshooting scenario2155.8 End-to-end NE troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.1 Overview	111
5.3 Onboarding an NE into NSP1135.4 Onboarding a service into NSP1555.5 LSP Throughput with Forecast reporting scenario1755.6 SAP Throughput reporting scenario1945.7 End-to-end NE troubleshooting scenario2155.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting Analytics reporting324	Troubleshooting using NSP assurance functions	112
5.4 Onboarding a service into NSP1555.5 LSP Throughput with Forecast reporting scenario1755.6 SAP Throughput reporting scenario1945.7 End-to-end NE troubleshooting scenario2155.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting324	5.2 Troubleshooting services and connectivity	112
5.5 LSP Throughput with Forecast reporting scenario1755.6 SAP Throughput reporting scenario1945.7 End-to-end NE troubleshooting scenario2155.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.3 Onboarding an NE into NSP	113
5.6 SAP Throughput reporting scenario1945.7 End-to-end NE troubleshooting scenario2155.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.4 Onboarding a service into NSP	155
5.7 End-to-end NE troubleshooting scenario2155.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting3225.14 Troubleshooting NSP workflows324	5.5 LSP Throughput with Forecast reporting scenario	175
5.8 End-to-end service troubleshooting scenario2405.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.6 SAP Throughput reporting scenario	194
5.9 End-to-end link troubleshooting scenario2685.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.7 End-to-end NE troubleshooting scenario	215
5.10 End-to-end port troubleshooting scenario289Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.8 End-to-end service troubleshooting scenario	240
Troubleshooting using Analytics3195.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.9 End-to-end link troubleshooting scenario	268
5.11 Analytics troubleshooting overview3195.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.10 End-to-end port troubleshooting scenario	289
5.12 Troubleshooting data collection3195.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	Troubleshooting using Analytics	319
5.13 Troubleshooting data storage3225.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.11 Analytics troubleshooting overview	319
5.14 Troubleshooting Analytics reporting322Troubleshooting using NSP workflows324	5.12 Troubleshooting data collection	319
Troubleshooting using NSP workflows 324	5.13 Troubleshooting data storage	322
	5.14 Troubleshooting Analytics reporting	322
5.15 Evaluating failed or slow workflow executions324	Troubleshooting using NSP workflows	324
	5.15 Evaluating failed or slow workflow executions	324

# Troubleshooting using NSP assurance functions

# 5.2 Troubleshooting services and connectivity

## 5.2.1 Before you begin

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

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

## 5.2.2 Steps

## Assurance supervision function

1 -

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

- Sites
- Endpoints
- Tunnel Bindings

See the NSP Network and Service Assurance Guide for more information about each component.

2 -

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

3

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

## Alarms function

4

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

- The Current Alarm List view provides high-level visibility of all alarms in the network.
- Choose the Current Alarms format to see the alarm information in a list you can filter. Select an alarm to view detailed information in an information panel.
- 5 —

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

### NFM-P

#### 6

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

7 -

Contact your technical support representative if the problem persists.

END OF STEPS

# 5.3 Onboarding an NE into NSP

## 5.3.1 Purpose

This process shows you how to use the NSP to manage an NE, configure attributes, verify component health, and confirm that the NE is up, running, and ready for further configuration.

#### Prerequisites

This process assumes that the following prerequisites are in place:

- The intent type artifact bundles required for device configuration have been installed:
  - icm-equipment-card\_mda
  - icm-equipment-port-connector
  - icm-equipment-port-ethernet
  - icm-router-network-interface
- The NE has been discovered in the NSP.
- Required templates and telemetry subscriptions have been created.
- Power modules and SFMs have been configured on the NE using CLI.

For details about intent type installation, see the *NSP Network Automation Guide*. For device discovery and template creation, see the *NSP Device Management Guide*. For telemetry subscriptions, see the *NSP Data Collection and Analysis Guide*. For CLI, see the NE documentation.

## 5.3.2 Resync the NE in Device Management

#### 1

First, we'll perform a resync, to ensure that the configuration on the NE is aligned with the NSP. This step is performed immediately after the NE is discovered.

View the NE in **Device Management**, **Managed Network Elements**. A green icon indicates that the NE is reachable.

T         T         T         T         T         T         T         Select an NE to see the details           attle              • Partially reachable               • Partially reachable               • MOM          135,121,147,210          92,168,96,190          7750 SR               • Select an NE to see the details            ston              • Reachable               -          MOM          135,121,158,12          92,168,96,49               7750 SR               •               •                            •                                •  135,121,158,121               92,168,96.93	E Name		Reachability	Management State	NE Mode	Management IP	NE ID	Product	:	0	Ą	艮	E
Attel       Partially reachable       —       MDM       155.121.147.210       92.168.96.190       775.0 SR       E         Atton       MDM       155.121.147.210       92.168.96.46       775.0 SR       E         e_2       Reachable       —       MDM       155.121.158.32       92.168.96.46       775.0 SR       E         gary       Beachable       Managed       Classic       155.121.149.11       92.168.99.37       775.0 SR       E         e_1       Managed       Classic       155.121.149.11       92.168.99.38       775.0 SR       E         e_1       Managed       Classic       155.121.149.11       92.168.99.38       775.0 SR       E         e_1       Managed       Classic       155.121.149.11       92.168.99.38       755.0 SR       E		Ŧ	- T	- T	•			T	]	Coloritore MC	·		
e_2         Reachable         -         MDM         135.121.158.121         92.168.96.93         7950.XRS         1           gary         Reachable         Managed         Classic         135.121.149.11         92.168.99.93         7750.5R         1           k-NRC         Reachable         Managed         Classic         135.121.148.123         92.168.99.38         7750.5R         1           e_1         Managed         Classic         135.121.147.128         92.168.97.250         7950.XRS         1	eattle		<ul> <li>Partially reachable</li> </ul>	-	MDM	135.121.147.210	92.168.96.190	7750 SR	:	Select an NE	to see the de	etans	
Constraint         Managed         Classic         135.121.149.11         92.168.98.97         7750 SR         1           R-NRC         Reachable         Managed         Classic         135.121.149.13         92.168.99.93         7750 SR         1           e_1         Managed         Classic         135.121.147.122         92.168.97.250         7950 XRS         1	oston		Reachable	-	MDM	135.121.158.32	92.168.96.46	7750 SR	:				
ANRC         Reachable         Managed         Classic         135.121.148.123         92.168.99.38         7750 SR         #           e_1         Reachable         Managed         Classic         135.121.147.162         92.168.97.250         7950 XRS         #	ore_2		Reachable	-	MDM	135.121.158.121	92.168.96.93	7950 XRS	:				
re_1 • Reachable Managed Classic 135.121.147.182 92.168.97.250 7950 XRS :	algary		Reachable	Managed	Classic	135.121.149.11	92.168.98.97	7750 SR	:				
	R-NRC		Reachable	Managed	Classic	135.121.148.123	92.168.99.38	7750 SR	:				
onto         • Reachable         Managed         Classic         135.121.147.235         92.168.96.215         7750 SR         !	ore_1		Reachable	Managed	Classic	135.121.147.182	92.168.97.250	7950 XRS	:				
	ronto		Reachable	Managed	Classic	135 121 147 235	02 169 06 215	7750.00					
			<ul> <li>Reaching the</li> </ul>	ronogen		100112-11147-200	92.100.30.213	7730.SK	I				

2 –

Select the NE and choose Manage, Resync from the table row actions menu (

## 5.3.3 Verify the NE inventory pre configuration

1 -

Select the NE and choose **Open in NE Inventory** from the table row actions menu ( .).

vice Management Managed	Network Eler	nents 👻						
Name		Reachability	Management State	NE Mode	Management IP	NE ID	Product	। 🕕 २ 見
	T	- T	- T	•		T		^ Summary
attle		<ul> <li>Partially reachable</li> </ul>	-	MDM	135.121.147.210	92.168.96.190	7750 SR	1
ston		Reachable	-	MDM	135.121.158.32	92.168.96.46	7750 SR	Boston
re_2		Reachable	-	MDM	135.121.158.121	92.168.96.93	Open NE Inventory	Management IP 135.121.158.32
gary		Reachable	Managed	Classic	135.121.149.11	92.168.98.97	View applicable adapt	NEID
R-NRC		Reachable	Managed	Classic	135.121.148.123	92.168.99.38	Operation View operation histor	92.168.96.46 NE Type
re_1		Reachable	Managed	Classic	135.121.147.182	92.168.97.250	Review backups	SR-7750
onto		Reachable	Managed	Classic	135.121.147.235	92.168.96.215	Create an operation	
								Nokia Product 7750 SR Chassis 7750 SR-14s Version 23.7.R2 Resync Status done Last Manual Resync 2024/06/21 14:36:50 501 (Local time) Resync Davisio (ma) 5430 Management State —
2.0	Þ						Þ. (	✓ Software

The NE inventory tree view opens in a new browser tab, displaying the components that are already configured using CLI.

Expand the Equipment group to show the status of the power shelf and power modules.

NOCIA Network Services Platform		User: admin	•	0
NE Inventory Boston				C
Equipment type filters • T, Any of:	^	0	έΞ	
Operational State: All + Administrative State: All + APPLY FILTERS		∧ Properties		
<ul> <li>Boston (7750 SR-14s), Operational State: enabled, Administrative State: unlocked</li> </ul>	÷	Name Power Shelf-1(ps-a10-shelf-dc)		
Equipment Group (Last Refresh: 2024-7-22 01:14:34)	v	Description —		
Power Shelf Slot-1(ps-a10-shelf-dc) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:	Operational State enabled		
Power Shelf-1(ps-a10-shelf-dc), Operational State: enabled, Administrative State: unlocked	:	Administrative State unlocked		
Power Module Slot-1/1(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Standby State providingService		
Power Module Slot-1/Z(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Position powerShelfSlot=1/powerShelf=1		
Power Module Slot-1/3(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	State Reasons		
Ower Module Slot-1/4(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Ower Module Slot-1/5(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	✓ Manufacture Details		
Ower Module Slot-1/5(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Power Module Slot-1/7/ps-a-dc-60001 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Tower Module Slot-1/8(ps-a-dc-6000) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Power Module Slot-1/9(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Power Module Slot-1/10(ps-a-dc-6000) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Power Shelf Slot-Zlunassigned) [installedNotExpected], Operational State: disabled, Administrative State: unlocked				
	<ul> <li>Back to top</li> </ul>			
Auto-refresh equipment group     Dia	splayed Count: 17			

Expand the shelf to show the status of the SFMs.

NOCIA Network Services Platform	User: admin		0
NE Inventory Boston			0
Equipment type filters	0	ŧΞ	
Operational State: All + Administrative State: All + APPLY FILTERS	∧ Properties		
Power Shelf-2(ps-a 10-shelf-dc), Operational State: disabled, Administrative State: unlocked	Name Shelf-1		
Shelf-1, Operational State: enabled, Administrative State: unlocked :	Description		
Card Slot-1 (unassigned) (installedNotExpected), Operational State: disabled, Administrative State: unlocked	MAC Address		
Card Slot-2(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	Operational State enabled		
Card Slot-3(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked	Administrative State unlocked		
Card Slot-4(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	Standby State providingService		
Card Slot-S(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	Position shelf=1		
Card Slot-S(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	State Reasons		
CPM Slot-A(cpm-e) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	Hardware Mac Address c2:7c:ff:00:00:00		
CPM Slot-Blunassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked			
> 🧧 SFM Slot-11sfm-s) (installedAndExpected), Operational State: enabled, Administrative State: unlocked :	✓ Manufacture Details		
SFM Slot-2[sfm-s] (installedAndExpected), Operational State: enabled, Administrative State: unlocked			
> 📕 SFM Slot-3(sfm-s) (installedAndExpected), Operational State: enabled, Administrative State: unlocked 🚦			
> 🧧 SFM Slot-4(sfm-a) (installedAndExpected), Operational State: enabled, Administrative State: unlocked			
SFM Slot-Slafm-a) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	*		
A Back to top			
💶 Aub-refesh equipment group Displayed Court: 42			

## 5.3.4 Create device configuration deployments for NE components

1 –

Next, we'll configure NE components. This can be done by deploying a series of templates in the **Device Management**, **Configuration Deployments** view.

2 -

From the **Device Management**, **Configuration Deployments** view, click **+ DEPLOYMENT**. We'll start by configuring Cards and MDAs, which are physical components: select **Physical** from the drop-down.

≡ NOKIA Net	work Services Platform							User: admin		-	0
Device Management Cor	figuration Deployments 🔹 👻							-	- DEPLOYMENT	Ċ	
Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Catego :	i Deployment (	Logical		
	•		Т	T	Т	T	•		Physical		

3

In the form that opens, click **+ TEMPLATE** and choose the template for Card and MDA configuration.

elect Template *	Select Physical Template	• • • • • •									+ TEMPL
lect Targets and Edit Selected	Template Name	Description	Role		Category	Dev	vice Scope	Flexible		×	
	T		T	•		•	•				
	Equipment-port-ether	-	Physica	iî.	Port	SRC	OS Classic & Model	Yes		Ð	
	Equipment-port-conn	<u>—:</u>	Physica	el.	Port	SRC	OS Classic & Model	Yes			
	Card MDA	-	Physica	al .	Card	SRC	OS Classic & Model	Yes		Đ	
											VIEW/EDIT TEMPLATE COI
											VIEW/EDIT TEMPLATE COL
					51	< Page:	1 /1 > 31			Count : 3	VIEW/EDIT TEMPLATE CO

Choose a card to add as the target:

- 1. Click **+ TARGET** and select **Cards** as the target type.
- 2. Choose a card slot from the list to add it to the Bin and click ADD

Targets a Sele	ect Cards								,		REPL
	NE Name	NE ID	Card (Identifier)	1	合 Bin (1 card)				EMP	Y	
		т	T		NE Name		NE ID		Card (Identifier)	:	
	Core_2	92.168.96.93	Card Slot-9(unassigned)	i		т		T			
	Core_1	92.168.97.250	Card Slot - 9		Boston		92.168.96.46		Card Slot-6(unassigne	î	
	Core_2	92.168.96.93	Card Slot-8(unassigned)								
	Core_1	92.168.97.250	Card Slot - 8							+	+ TAI
	Core_2	92.168.96.93	Card Slot-7(unassigned)								
	Core_1	92.168.97.250	Card Slot - 7							PLAT	ATE CO
	Boston	92.168.96.46	Card Slot-6(unassigned)								
	Seattle	92.168.96.190	Card Slot-6(unassigned)								
	Core_2	92.168.96.93	Card Slot-6(unassigned)								
	Core_1	92.168.97.250	Card Slot - 6								
	Toronto	92.168.96.215	Card Slot - 6								
	Calgary	92.168.98.97	Card Slot - 6								
	Seattle	92.168.96.190	Card Slot-5(unassigned)								
			IC C Page: 1 /1 > >1	Count:74						$\rightarrow$	

Click VIEW/EDIT TEMPLATE CONFIG. In the form that opens, configure the card parameters:

- 1. Choose a card type.
- 2. In the MDA panel, click + ADD and configure the parameters to create an MDA.
- 3. Click UPDATE.

NOCIA     Network Services Platform			User: admin	• 7
Deploy Physical Configuration				×
Select Template Card MDA			×	REPLACE
Select Targets a Card	Card			Î
	Admin State	Card Type		
	enable 👻 🗔	xcm-14s-b X		
	MDA		+ ADD	
	MDA Slot Admin State	MDA Type Sync E		
	1 enable	s36-100gb-qsfp28-3.6t	1	+ TARGET
	2 enable	s36-100gb-qsfp28	I	PLATE CONFIG
		$ \langle \langle Page: 1 /1 \rangle \rangle $	Total: 2	
	XIDM		+ ADD	
	XIOM Slot Admin State	ХІОМ Туре		Count: 1
		No data to display		
		Wo data to display	CANCEL UPDATE	×
_				
			CANCEL SAVI	E DEPLOY

Click **DEPLOY** to deploy the configuration.

7

Create physical deployments for additional connectors and ports, using their templates. The overall steps are very similar to creation of a Card and MDA deployment, but the parameters vary by template.

- 1. Configure deployments for port connectors if applicable, using the template created from the icm-equipment-port-connector intent type.
- 2. Configure deployments for ports, using the template created from the icm-equipment-portethernet intent type.
- 8

After the port configurations have been deployed, configure OSPF and ISIS routing on the NE using CLI.

9

Now we can create a logical deployment to configure a router interface.

Click **+ DEPLOYMENT** and select **Logical** from the drop-down.

10											
NOCIA     Network Ser Device Management     Configuration     Configuration	vices Platform Deployments							User: admin	+ DEPLOYMENT	G	7
Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	i Deployment	Logical Physical		

In the form that opens, click **+ TEMPLATE** and choose the template for router interface configuration. Click **ADD**.

t Templates	*				10.20										+ TEMI
t Targets a	Sele	ct Logical Templates													×
n Identifie		Template Name		Description =		Role		Category		Device Scope	Flexible		:	🕒 Bin (1 Template)	EMPTY
			T		Ŧ		•		•			•		Template Name Category	1
	~	Router-network-interface		-		Logical		Interface		SROS Classic & Model	Yes		۵	т	
		Service-customer		-		Logical		Service		SROS Classic & Model	Yes		Ð	Router-network-interf interface	Т
															PLATE CO
						< Page:	1 /1					Count			

12 -

Choose a target:

- 1. Click **+ TARGET** and choose **NEs** from the drop-down list.
- 2. Choose an NE from the list to add it to the Bin and click **ADD**.

eploy Logica	l Confi	iguration													
lect Template	e *														
lect Targets a		ect NEs												×	TEMPLATE
sign Identifie	0	Only 1 target can be	selected fo	r the selected templa	ite					合 Bin (1 NE)				EMPTY	
	-	NE Name		NEID	Manage	ment IP	Product		:	NE Name		NE ID		:	
			T	т		Ŧ		T			T		т		
		VSR-NRC		92.168.99.38	135.12		7750 SR			Core_2		92.168.96.93		î	1
		Toronto		92.168.96.215	135.12	.147	7750 SR								
		Seattle		92.168.96.190	135.12	.147	7750 SR								Count : 1
		Core_2		92.168.96.93	135.12	.158	7950 XRS								+ TARGET
		Core_1		92.168.97.250	135.12	.147	7950 XRS								
		Calgary		92.168.98.97	135.12	.149.11	7750 SR								ATE CONFIG
		Boston		92.168.96.46	135.12	.158.32	7750 SR								
															_
					IC S	Page:	/1 >		Count:7						
													CANCEL	ADD	
				1. Router-network-	interferer .								_		
				INTERFACE NAME*											

- 1. Click **VIEW/EDIT TEMPLATE CONFIG**. In the form that opens, configure the interface parameters. Scroll through the form to update parameters as needed.
- 2. Click UPDATE.

BFO Inner Tog QoS LDP Vitarface Parameters LDP Sync Timer TARGS Seconds CONTROL CONTRO	TE
Select Targy Interface Int	TE
Assign Idn LDP Sync Timer  Assign Idn LDP Sync Timer  Inter Table  Inter Table Inter Table Inter Table Inter Table Inter Table Inter Table Inter Table Inter Table Inter Table Inter Table	
Private Peer spiton   Private Peer spit	
Br0     Pert outer Tig       Primary     Pert outer Tig       Prid     prit       Prid	
Pr6     port     C2     1/1/ct/2     X     22       BP0     Inner Tag       QoS     Inner Tag       LDP       Interface Parameters       MPLS   LDP Sync Timer	
EFO Inner Trg  GoS LDP ViteFace Parameters LDP Sync Timer TARGE MPLS Sacods	
Apple and a series a	1
LDP Interface Parameters MPLS Seconds	
Interface Parameters MPLS Seconds Seconds CONS	
MPLS LDP Sync Timer	
Saranda Com	
	IG
RSVP	
IPv4	
BFD	
Admin State Transmit Interval (Mill Seconds) Receive (Mill Seconds)	Î
Select Item - CR	
Multiplier Type	
CANCEL UPDATE	
Assign unique identifiers for templates selected above to identify the corresponding deployments. If content below is disabled, select targets first to enable them.	-
CANCEL SAVE DE	

Enter a name for the interface in the **INTERFACE NAME** field.

#### 15 —

Click **DEPLOY** to deploy the configuration.

Deploy Logical Configuration			×
Select Templates *	Select Templates	CLEAR ALL	+ TEMPLATE
Select Targets and Edit Selected Template * Assign Identifier for Selected Template *	Router-network-Interf — Logical Interface SROS Classic & Model Yes		×
			Count : 1
	Select Targets and Edit Selected Template	CLEAR ALL	+ TARGET
	Select targets. Template configurations can be edited after targets are selected.	VIEW/EDIT TEI	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		
	• Up Core_2 92.168.96.93 135.121.158 7950 XRS		н
			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. Rovter-sotuario-interface : INTERFACE NAME*		
	to_Bos_Int1		
		CANCEL SA	DEPLOY

#### 16 —

Audit and align each deployment:

1. For each of the deployments we created, select the deployment and click **AUDIT**.

=	NOCIA Network Ser	vices Platform							User: admin 👻 🛞
Device	e Management Configuration	Deployments +							+ DEPLOYMENT 🕞 🖀
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Catego :	(i) Deployment Details
	•			T	Т	т	•		NE Name
	Deployed Aligned	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1	Card MDA	Physical	Card 1	Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1/1/c1	Equipment-port-conn	Physical	Port	NE ID 92.168.96.46
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1/1/c2	Equipment-port-conn	Physical	Port 🚦	Identifier
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1	Equipment-port-conn	Physical	Port 🕴	Port-ID 1/1/c1
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c2	Equipment-port-conn	Physical	Port	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1/1/c1/1	Equipment-port-ether	Physical	Port 🕴	Deployment Status Deployed Aligned
	<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 I	
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1/1/c1/2	Equipment-port-ether	Physical	Port 1	AUDIT ALIGN

2. Click **ALIGN** to ensure that the NE configuration is aligned with the templates.

=	No <ia network="" set<="" th=""><th>rvices Platform</th><th></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	Deployments +								+ DEPLOYMENT C
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier =	Template	Role	Catego	:	(i) Deployment Details
	•	•		T	т	T	•			NE Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1	Card MDA	Physical	Card	֔	Boston
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1	Card MDA	Physical	Card	-	92.168.96.46
	<ul> <li>Aligning</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>	Core_2	92.168.96.93	1/1/c1	Equipment-port-conn	Physical	Port	:	Port-ID 1/1/c1
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	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	-	Deployment Status
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Core_2	92.168.96.93	1/1/c1/2	Equipment-port-ether	Physical	Port		• Aligning
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	Boston	92.168.96.46	1/1/c1/2	Equipment-port-ether	Physical	Port	-	AUDIT ALIGN

## 5.3.5 Back up the NE configuration

1 -

Returning to the Managed Network Elements list, we'll take a backup of the NE. Select the NE and choose **Create an operation**, **Backup** from the table row actions menu ( ).

vice Management Managed Net	work Elem	nents -										
E Name		Reachability		Management State	NE Mode	Management IP	NE ID	Product			X 🔋	Ę
	Ŧ	•	T	- T	•		T		^ Su	mmary		
attle		Reachable		-	MDM	135.121.147.210	92.168.96.190	7750 SR	i NE N			
oston		Reachable		-	MDM	135.121.158.32	92.168.96.46	7750 SR	Bost			
pre_2		Reachable		-	MDM	135.121.158.121	92.168.96.93	Open NE Inventory		gement IP 121.158.32		
lgary		Reachable		Managed	Classic	135.121.149.11	92.168.98.97	View applicable adapto	NE IL	68.96.46		
R-NRC		Reachable		Managed	Classic	135.121.148.123	92.168.99.38	Operation View operation history				
re_1		<ul> <li>Reachable</li> </ul>		Managed	Classic	135.121.147.182	92.168.97.250	Review backups	SR-7	750		
ronto		Reachable		Managed	Classic	135.121.147.235	92.168.96.215	Create an operation	Back			
									Versi 23.7 Resyn donu Last 202 Resyn 374	ret ) SR ) SR-14s on .R2 re Status Manual Resync %/07/06 10:20: re Duration (ms)	03 497 (Local time)	
										ftware		

2 –

We can check the status of the backup by clicking **‡** (Table row actions), **Review backups**, **View all backup files** to view the list of completed backups.

■ NO <ia network="" p="" platform<="" services=""></ia>				User: admin	• ⑦
Boston Backup Files for Boston					×
Name	Size(in bytes)	File Type	Last Modified Time =		:
	T	T	▼ DD/MM/YY) - DD/MM/YY)		
/lsom/neBackup/Nokia/7750_SR/Boston/TiMOS-23.7.R2	4096	directory	2024/07/15 13:01:19		:=

## 5.3.6 Verify the NE inventory post configuration

Return to the list of devices in **Device Management**, **Managed Network Elements**.

2 \_\_\_\_\_

1 —

Select the NE and choose **Open in NE Inventory** from the table row actions menu ( **‡** ).

	Services Plat											030	: admin		•
	letwork Eleme											_			
EName		Reachability		Management State		NE Mode	Management IP	NE ID		Product	-	0	Ą	₽,	Ę
	T	•	Ŧ		- 1	•			T			^ Summary			
attle		<ul> <li>Partially reachable</li> </ul>		-		MDM	135.121.147.210	92.168.96.190	7	7750 SR	:				
oston		Reachable				MDM	135.121.158.32	92.168.96.46	7	7750 SR	•	NE Name Boston			
re_2		Reachable		-		MDM	135.121.158.121	92.168.96.93		Open NE Inventory		Management IP 135.121.158.			
ilgary		Reachable		Managed		Classic	135.121.149.11	92.168.98.97	2	View applicable ada	otors	NE ID			
R-NRC		Reachable		Managed		Classic	135.121.148.123	92.168.99.38		Operation		92.168.96.46			
ore_1		Reachable		Managed		Classic	135.121.147.182	92.168.97.250		View operation histo Review backups	bry	SR-7750			
ronto		Reachable		Managed		Classic	135.121.147.235	92.168.96.215		Create an operation	,	NE Mode MDM			
												Software Versio			
										Manage	•	TIMOS-C-23.	.R2		
												Nokia			
												Product 7750 SR			
												Chassis			
												7750 SR-14s Version			
												23.7.R2			
												Resync Status done			
												Last Manual Res 2024/06/21		li a and Alaza b	
												Resync Duration		(Local time)	
												5430			
												Management St	ate		
	•	(								×	< >	✓ Software			
Auto-refresh Last Refre	sh: 2024/6/21					/1 > >				Row Cou					

The NE inventory tree view opens in a new browser tab, displaying the components that are configured.

Expand the Equipment group to show the status of the shelves, slots, and cards.

Inventory Boston			
quipment type filters 🔹 👻 T <sub>e</sub> Any of:	^	0	ê =
perational State: All + Administrative State: All + APPLY FILTERS	-	Properties	
Boston (7750 SR-14s), Operational State: enabled, Administrative State: unlocked		Name Shelf-1	
Equipment Group (Last Refresh: 2024-7-15 01:52:49)		Description	
Power Shelf Slot-1[ps-a10-shelf-dc] (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked		MAC Address	
Power Shelf Slot-2 (unassigned) (InstalledNotExpected), Operational State: disabled, Administrative State: unlocked		Dperational State enabled	
- 🚆 Shelf-1, Operational State: enabled, Administrative State: unlocked		Administrative State unlocked	
Card Slot-1(xcm-14s-b) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked		Standby State providingService	
Card Slot-2(xcm-14s-b) (expectedNotInstalled), Operational State: disabled, Administrative State: unlocked		Position shelf=1	
Card Slot-3(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked	1	State Reasons —	
Card Slot-4(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked		Hardware Mac Address c2:89:ff:00:00:00	
Card Slot-S(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	:		
Card Slot-6(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	1	<sup>,</sup> Manufacture Details	
CPM Slot-Alcpm2-s) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:		
CFM Slot-Blumassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked	:		
SPM Slot-1(sfm2-s) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	I		
SFM Slot-2(sfm2-s) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	A Back to top		
Auto-refresh equipment group	Displayed Count: 30		

4

We can also verify configuration details in Modeled Device Configurator. From the top of the inventory tree, select **Open object** from the More menu ( :).

■ NO <ia network="" platform<="" services="" th=""><th></th><th>User: admin</th><th></th><th>0</th></ia>		User: admin		0
NE Inventory Boston				Ċ,
Equipment type filters	^	0	ŧΞ	
Operational State: All + Administrative State: All + APPLY FILTERS		No data available		
👻 🧧 Boston (7750 SR-14s), Operational State: enabled, Administrative State: unlocked	1			
- 🛃 Equipment Group (Last Refresh: 2024-7-15 01:56:50)	Open in Current Alarms			
Power Shelf Slot-1 (ps-a10-shelf-dc) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	Open object			
	Open NE Session			
Power Shelf Slot-2(unassigned) (installedNotExpected), Operational State: disabled, Administrative State: unlocked	Plot utilization statistics			
🔹 🚆 Shelf-1, Operational State: enabled, Administrative State: unlocked	Show in Event Timeline			
Card Slot-11xcm-14s-b) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	1			
👻 📴 Card-11xcm-14s-b), Operational State: enabled, Administrative State: unlocked	:			
Card Slot-1/x1(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked	1			
Card Slot-1/1(s36-100gb-qsfp28-3.6t) (Installed AndExpected), Operational State: enabled, Administrative State: unlocked	1			
Card Slot-1/x2(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked	1			
Card Slot 1/2[s36-100gb-qsfp28] [installedAndExpected], Operational State: enabled, Administrative State: unlocked	I			
Card-1/2(s36-100gb-qsfp28), Operational State: enabled, Administrative State: unlocked	I			
Card Slot-2(xcm-14s-b) (expectedNotinstalled), Operational State: disabled, Administrative State: unlocked	:			
Card Slot-3(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	:			
Card Slot-4(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked				
	A Back to top			
Auto-refresh equipment group	Displayed Count: 36			

Modeled Device Configurator opens in a new tab, showing the configuration and state trees for the NE.

■ NO <ia network="" platform<="" services="" th=""><th></th><th></th><th>User: admin - 🧿</th></ia>			User: admin - 🧿
Model Driven Configurator > Router   SR-7750 23.7.R2 Boston (92.168.96.46)			Configured Attributes View  CONFIG BASKET
	Root		Î
	Nokia-conf:/configure	>	
	Nokia-state:/state	>	
	Nokia-oper-global-/global-operations	>	
	Nokia-oper-file:/file	>	
	Nokia-oper-admin:/admin	>	
	Nokia-oper-reset/reset	>	
	Nokia-oper-perform:/perform	>	
	Openconfig-act:/acl	>	
	Openconfig-bfd:/bfd	>	
	Openconfig-bgp./bgp	>	
	Openconfig-interfaces:/interfaces	>	
	Openconfig-keychain:/keychains	>	
	Openconfig-lacp://acp	>	
	Openconfig-Ildp://ldp	>	
	Openconfig-local-routing:/local-routes	>	
	Openconfig-mpls:/mpls	>	

Click the **Nokia-conf:/configure** row to open the configuration tree.

■ NO <ia network="" platform<="" services="" th=""><th></th><th></th><th>User: admin + ⑦</th></ia>			User: admin + ⑦
Model Driven Configurator > Boston (92.168.96.46)			Configured Attributes View   CONFIG BASKET
	Root		í
	Nokia-conf./configure	>	
	Nokia-state:/state	>	
	Nokia-oper-global:/global-operations	>	
	Nokia-oper-file/file	>	
	Nokia-oper-admin:/admin	>	
	Nokia-oper-reset/reset	>	
	Nokia-oper-perform:/perform	>	
	Openconfig-acl:/acl	>	
	Openconfig-bfd:/bfd	>	
	Openconfig-bgp://bgp	>	
	Openconfig-interfaces:/interfaces	>	
	Openconfig-keychain:/keychains	>	
	Openconfig-lacp:/lacp	>	
	Openconfig-Ildp://ldp	>	
	Openconfig-local-routing:/local-routes	>	
	Openconfig-mpls:/mpls	>	

Scroll down to see information about the objects we configured. For example, we'll click Port List to see the configured ports.

del Driven Configurator > Router   SR-7750 23.7.R2 Boston (92.168.96.46)						T	Configured Attributes Vi	ew 👻	CONFIG BASKET
	Root > Nokia-conf:/configure > Port List			CREATE PORT	Ð				
	Port-id	Admin-state	Description	Ddm-events	:				
	1/1/c1	enable	Network Port		_				
	1/1/c1/2	enable	Network Port						
	1/1/c1/3	enable	Access port						
	1/1/c1/4	enable	Access port						
	1/1/c1/5	enable	Hybrid ports		_				
	1/1/c1/6	enable	Hybrid ports		_				
	1/1/c2/1	enable							
	1/1/c2/2	enable							
					♦ ► bunt: 10				

7 –

We can also verify our logical configurations from the NE Inventory tab.

Return to the NE Inventory tab and expand the Logical Group. To see interfaces, expand, Routers and Interfaces. Green icons show normal operation.

■ NO <ia network="" platform<="" services="" th=""><th></th></ia>	
NE Inventory Boston	
Equipment type filters - T <sub>+</sub> Any of:	^
Operational State: All + Administrative State: All + APPLY FILTERS	
<ul> <li>Boston (7750 SR-14s), Operational State: enabled, Administrative State: unlocked</li> </ul>	1
Equipment Group (Last Refresh: 2024-7-18 10:35:28)	~
✓ Im Logical Group (Last Refresh: 2024-7-18 10:21:12)	
Link Aggregation Groups	
✓ Routing Instances	
✓ ■ Routers	
Router - default, Operational State: true, Administrative State: true	
Interfaces	ļ
Interface - 1, system, Operational State: UP, Administrative State: true	
Interface - 2, to_core2_int1, Operational State: UP, Administrative State: true	
Interface - 3, to_Core2_Int2, Operational State: UP, Administrative State: true	
BGP Instances	
OSPFv2 Instances	
OSPFv3 Instances	
ISIS Instances	-
	A Back to top
Auto-refresh equipment group	Displayed Count: 22

## 5.3.7 View the NE in the Network Health dashboard

1 -

The Network Health dashboard is the home screen of the NSP. It provides a quick view of essential information relating to the function of your network and its components.

Choose Network Health View from the NSP main menu to open the dashboard.

■ NO <ia network="" platform<="" services="" th=""><th></th><th>User: admin</th><th></th><th>0</th></ia>		User: admin		0
NETWORK FUNCTIONS				Ċ.
✓ Network Map and Health				
Network Health View	*	(j)	ŧΞ	
Network Map View				
Network Inventory View	APPLY FILTERS	No data available		
Object Troubleshooting				
Current Alarms	d, Administrative State: unlocked			
OAM Tests	.41:17)			
Device Management				
Model Driven Configurator	44)			
Device Discovery				
IP/Optical Coordination				
> Data Collection and Analysis				
Service Management				
Path Control				
PROGRAMMING				
Developer Portal				
Network Intents				
Workflows				
NSP ADMINISTRATION				
System Health				
Map Layouts and Groups				
File Server				
Users and Security				
Artifacts				
	A Back to top			
	Displayed Count: 3			

The Equipment Health dashlet shows that six affected NEs are present in the network.

work Map and Health	Overview -				E
Network Health Vie Determine the overall	<b>w</b> health of your network using the metric	s below			
<b>quipment Health</b> he status of all network ele	ments	Service Health The status of all network services	Last Hour 👻	Service Configuration Health The configuration status of all network services	Alarm Summary Unacknowledged root cause alarms
0%- Poor Network Healthy I	6- 1- RES Affected Unreachable NES NES	0 0 Healthy Affected Services	0- Degraded Services	0 0 Total Milailgned Services	6: 2201 15. 0. Critical Major Minor TCAs
nearn	NES NES	Services Services	Services	View in Service Management	View in Current Alarms
ffected Services	re affecting services			Last Hour 👻	: News Feed View unacknowledged root cause alarms as they occur
By Service Sites 🏾 🔹	By Service Endpoints • By Tu	nnel Bindings			
	A A A				▼ Alarms → 🖶 By Time Reported →
1					Y Alarms      ▼ By Time Reported      NodeConfigurationProblem     Seattle     Impact:0     Seattle     Impact:0     Seattle     Impact:0     Seattle     Impact:0     Seattle     S
1		9-			NodeConfigurationProblem Seattle 32 seconds ago
					NodeConfigurationProblem 32 seconds ago filmpact.0 32 seconds ago film
1					NodeConfigurationProblem     Seatte     Impact: 0     MisconfiguredNode     topology     MisconfiguredNode     MisconfiguredNode     MisconfiguredNode     MisconfiguredNode     S7 seconds ago     S7 seconds     S7 seco

Scroll down to see the Map View. Double-click on **Pre-Provisioned NEs** to show our NE, with the link that we created by configuring the router interface.

NOCIA Network Services Platform		User: admin	• ?
etwork Map and Health Overview -			E. :
View Operational -		(rend)	·
			Ū
	<b>O</b>		ŧΞ
	Pre-Provisioned NEs 3 Nodes		ti.
Φ,			
•			
9.			
e).			
<b>†</b>			
-	NEs without a region 4 Nodes		



Scroll further down to see further information provided by the dashlets.

Expand the Network Elements dashlet to see the list of NEs. The Table row actions menu shows options. We'll choose **Open in Current Alarms**.

	d Health Overview	•													E	
etwork Eler Content up	ments odated on 2024/06/25 13:42:05 (C	ick to update)														:
ame	Operational State	# Affected Objects		System Address		Management Address		Product	Chassis Type		Version		Communication State	Managed State	Adminis	
т	•		T		T		т	T		т		۲		•		
SR-NRC	enabled		59	92.168.99.38		135.121.148.123		7750 SR	VSR-I		TIMOS-B-2		up	managed	unlocke	8
ore_1	enabled		50	92.168.97.250		135.121.147.182		7950 XRS	7950-XRS20e		TIMOS-C-2		up	managed	unlocke	ŝ
one_Z	enabled		19	92.168.96.93		135.121.158.121		7950 XRS	7950 XRS-20e		TIMOS-C-2		up	managed	unlocke	K.
ston	enabled		12	92.168.96.46		135.121.158.32		7750 SR	7750 SR-14s		TIMOS-C-2		up	managed	unlocke	(
attle	enabled		5	92.168.96.190		135.121.147.210		7750 SR	7750 SR-14s		TiMOS-C-2		partial	View in Current	Alarms	
ronto	enabled		3	92.168.96.215		135.121.147.235		7750 SR	7750 SR-14s		TiMOS-C-2		up	🖧 Show in Netwo	0000000000	
lgary	enabled		3	92.168.98.97		135.121.149.11		7750 SR	7750 SR-14s		TiMOS-C-2		up	<ul> <li>Open in NE Inv</li> <li>View in Object</li> </ul>		oti
														Open in NE See     Plot statistics     Add to Watchlis		
ervice Sites		с <sup>Я</sup>	Link	5			e <sup>n</sup>	Ports				ĸ	7 Services			Ľ
	Operatio	al State	Name	e i		Operational State		Name		Operat	ional State		Name	Operational	State	
me			Bost	on:1/1/c2/1Core_2:1.		enabled		Port 1/3/4		disable	d		Î			
me																
me								1/2/c19		disable	d					

The Current Alarms view opens, filtered to show the alarms on the NE of interest. We can further filter the list if needed.

etwork Map and Health	> Network Element 92.168.96.46 (Boston)	Current Alarms												Ģ	
+						C (			0	0	0	G	) Details		
everity	Impact	Last Time Detected	Site ID		Site Name			Alarmed Object Type	-		an i	~	General		
- T	Т	YYYY - YYYY 🖬		Т			T			T					
	0	2024/06/25 11:55:23	92.168.96.46		Boston			/openconfig-net	work-i	le	ve :	~	Severity		
	0	2024/06/25 11:55:23	92.168.96.46		Boston			/openconfig-net	work-i	in	tei :	~	Acknowledgement		
<b>.</b>	0	2024/06/25 11:49:39	92.168.96.46		Boston			equipment.Equi	oment	P	ow :				
3	0	2024/06/11 11:37:16	92.168.96.46		Boston			equipment.Equi	oment	p	ort :	~	Acknowledgement Notes		
<b>D</b>	0	2024/06/11 11:37:16	92.168.96.46		Boston			equipment.Equip	oment	P	ort :	~	Statistics		
3	0	2024/06/11 11:37:16	92.168.96.46		Boston			equipment.Equi	oment	P	ort :				
2	0	2024/06/11 11:37:16	92.168.96.46		Boston			equipment.Equi	oment	p	ort :	^	Description		
0	0	2024/06/25 11:55:23	92.168.96.46		Boston			equipment.Netv	orkEle	sy	/st i				
0	0	2024/06/25 11:49:38	92.168.96.46		Boston			equipment.Netv	orkEle	sy	/st :				
0	0	2024/06/25 11:49:38	92.168.96.46		Boston			equipment.Netv	orkEle	S	/st :				
<b>—</b>	0	2024/06/25 11:49:38	92.168.96.46		Boston			equipment.Netv	orkEle	sy	/st :	^	Remedial Action		
	0	2024/06/25 11:49:38	92.168.96.46		Boston			equipment.Netv	orkEle	S	/st :				
0	0	2024/06/24 8:28:41 8	92.168.96.46		Boston			equipment.Netv	orkEle	sy	/st :				
3	0	2024/06/25 11:50:16	92.168.96.46		Boston			necontrol.Disco	veredNe	B	ost I				
•	0	2024/06/25 11:50:15	92.168.96.46		Boston			necontrol.Disco	veredNe	В	ost I		Public Condition		
	0	2024/06/25 11:50:02	92.168.96.46		Boston			necontrol.Disco	veredNe	В	ost I	~	Raising Condition		
												~	Clearing Condition		
												~	Additional Text		
												~	Custom Text		
Live Data	4 @										▶ 4 ▶	~	Specific Problem		

Returning to the Network Elements dashlet, we can also view the NE in the Object Troubleshooting dashboard. The Object Troubleshooting dashboard provides specific performance information about the selected NE.

work map and	d Health Overview														E	
etwork Eler Content up	ments odated on 2024/06/25 13:46:56 (Cl	ick to update)													1	1
ame	Operational State	# Affected Objects		System Address		Management Address		Product	Chassis Type		Version	Co	mmunication State	Managed State	Adminis	
т	•		۲		T		т	T		т			*	•		
SR-NRC	enabled		59	92.168.99.38		135.121.148.123		7750 SR	VSR-I		TIMOS-B-2	up		managed	unlocke	
ore_1	enabled		50	92.168.97.250		135.121.147.182		7950 XRS	7950-XRS20e		TIMOS-C-2	up		managed	unlocke	
ne_2	enabled		19	92.168.96.93		135.121.158.121		7950 XRS	7950 XRS-20e		TIMOS-C-2	up	5	managed	unlocke	
ston	enabled		12	92.168.96.46		135.121.158.32		7750 SR	7750 SR-14s		TIMOS-C-2	up	1	managed	unlocke	
attle	enabled		5	92.168.96.190		135.121.147.210		7750 SR	7750 SR-14s		TiMOS-C-2	pa	rtial	View in Current		
ronto	enabled		3	92.168.96.215		135.121.147.235		7750 SR	7750 SR-14s		TiMOS-C-2	up		<ul> <li>Show in Networ</li> <li>Open in NE Inve</li> </ul>		
lgary	enabled		3	92.168.98.97		135.121.149.11		7750 SR	7750 SR-14s		TiMOS-C-2	up	•	View in Object		oti
														<ul> <li>Open in NE Ses</li> <li>Plot statistics</li> <li>Add to Watchlis</li> </ul>		4
rvice Sites	5	л 2	Link	s			u <sup>3</sup>	Ports				ĸ	Services			ĸ
me	Operation	nal State	Nam	e		Operational State		Name		Operat	ional State		Name	Operational S	itate	
			Bost	on:1/1/c2/1Core_2:1		enabled		Port 1/3/4		disable	d	í	i			
								1/2/c19		disable	d					
												_				

Troubleshooting Summary Board View troubleshooting summary inform	<b>d</b> nation								
Overview mmary information for the selected NE		Current Health Summary Health status for the selected NE		Alarm Summar Alarms and impac		ted NE		Analytics Reports Run Analytics Reports	
System Address:	92.168.96.46	Operational State:	enabled					Inventory Reports	
Management Address:	135.121.158.32	Communication State:	up	2	8		0	Card Inventory (NSP)	•
Product:	7750 SR	Administrative State:	unlocked					Port Details (NSP)	Þ
.ocation:	N/A	Availability State:	N/A	Critical	Major	TCAs	Total Impacts	Port Inventory (NSP)	Þ
		Resync State:	done					Utilization Reports	
		Open in NE Inventory			View in Curr	rent Alarms		Temperature CPU Memory Utilization Summary (NSP)	Þ
								Temperature CPU Memory Utilization Details (NSP)	Þ
KPIs portant KPIs for the selected NE								OAM Reports	
								OAM-PM Latency (NSP)	•
# Affected Components:	12 (60%)	# Affected LAGs:	0 (0%)					OAM-PM Loss (NSP)	•
# Alarms:	14	# Affected Links:	0 (0%)					OAM-PM Network Site Summary (NSP)	•
# Unacknowledged Critical Alarms:	2							OAM-PM Network Summary (NSP)	
# Affected Cards:	6 (67%)							OAPPER Retwork Summary (NSI)	
# Affected Ports:	6 (60%)								

Returning again to the Network Elements dashlet, we can add the NE to the Watchlist to navigate to it easily in future. Choose Add to Watchlist from the Table row actions menu.

work Map and	l Health Overview	•													E	
etwork Elen Content up	nents dated on 2024/06/25 13:48:14	(Click to update)														:
ame	Operational State	# Affected Objects		System Address		Management Address		Product	Chassis Type		Version		Communication State	Managed State	Adminis	,
Ŧ			۲		T		т	T		т		T		•		
R-NRC	enabled		59	92.168.99.38		135.121.148.123		7750 SR	VSR-I		TIMOS-B-2		up	managed	unlocke	8
ore_1	enabled		50	92.168.97.250		135.121.147.182		7950 XRS	7950-XRS20e		TIMOS-C-2		up	managed	unlocke	i.
re_2	enabled		19	92.168.96.93		135.121.158.121		7950 XRS	7950 XRS-20e		TIMOS-C-2		up	managed	unlocke	R.
ston	enabled		12	92.168.96.46		135.121.158.32		7750 SR	7750 SR-14s		TIMOS-C-2		up	managed	unlocke	
attle	enabled		5	92.168.96.190		135.121.147.210		7750 SR	7750 SR-14s		TiMOS-C-2		partial	View in Current	t Alarms	
ronto	enabled		3	92.168.96.215		135.121.147.235		7750 SR	7750 SR-14s		TiMOS-C-2		up	🖧 Show in Netwo	100000000000	
lgary	enabled		3	92.168.98.97		135.121.149.11		7750 SR	7750 SR-14s		TiMOS-C-2		up	<ul> <li>Open in NE Inv</li> <li>View in Object</li> </ul>		oti
														Ø Open in NE Se		
														Plot statistics		
										_				Add to Watchl	st	
rvice Sites		с <sup>л</sup>	Link	s			к <sup>л</sup>	Ports				ĸ	* Services			ĸ
me	Operat	ional State	Nam	1		Operational State		Name		Operat	ional State		Name	Operational	State	
			Bost	on:1/1/c2/1Core_2:1.		enabled		Port 1/3/4		disable	d		î			
								1/2/c19		disable	d					
								1/1/c2/10		disable	d			No data to display		
	No data to display							17 17 667 10		Gibbble	<sup>l</sup> u					

Click Watchlist at the top of the page to navigate to the watchlist.

NSP

work Map and H	Health Overview														R	
letwork Eleme															Watchlis	st
Content upda	ated on 2024/06/25 13:48:14 (Click Operational State	# Affected Objects		System Address		Management Address		Product	Chassis Type		Version	Commu	nication State	Managed State	Adminis	
т	•		T		T		т	1		т	T					
SR-NRC	enabled		59	92.168.99.38		135.121.148.123		7750 SR	VSR-I		TIMOS-B-2	up		managed	unlocke	
ore_1	enabled		50	92.168.97.250		135.121.147.182		7950 XRS	7950-XRS20e		TIMOS-C-2	up		managed	unlocke	
ne_2	enabled		19	92.168.96.93		135.121.158.121		7950 XR5	7950 XRS-20e		TIMOS-C-2	up		managed	unlocke	
ston	enabled		12	92.168.96.46		135.121.158.32		7750 SR	7750 SR-14s		TIMOS-C-2	up		managed	unlocke	
attle	enabled		5	92.168.96.190		135.121.147.210		7750 SR	7750 SR-14s		TiMOS-C-2	partial		managed	unlocke	
ronto	enabled		3	92.168.96.215		135.121.147.235		7750 SR	7750 SR-14s		TiMOS-C-2	up		managed	unlocke	
lgary	enabled		3	92.168.98.97		135.121.149.11		7750 SR	7750 SR-14s		TiMOS-C-2	up		managed	unlocke	
			·									. 1			•	
rvice Sites		× <sup>3</sup>	Link				e <sup>3</sup>	Ports				K 3	Services			ĸ
rvice Sites	Operationa		Nam	•		Operational State	¥.	Name			ional State	к <sup>7</sup>	Services Name	Operationa		×
rvice Sites	Operationa		Nam			Operational State	κ <sup>3</sup>	Name Port 1/3/4		disable	ional State	κ <sup>π</sup>		Operationa		E.
ervice Sites			Nam	•			к Л	Name			ional State d	×*				*

■ NOKIA Network Services Platform	User: admin 🗸	0
Watchlist		۵
Services & Network elements Monitor and navigate to most important Services & Network elements Y Service & NE + ) = Object type +		*
Boston (92.168.96.46)           7750 58-146           Components affected: 12 (60%), Trending: —           Affected: Cardis 6 (67%), Ports 6 (60%), Linka 0 (0%), UnAck Critical Alarms 2		

Let's take a look at other information available on the Network Health dashboard. The Links dashlet shows a list of links configured on the system, showing their attributes.

NO <ia netwo<="" th=""><th>rk Services Platforn</th><th>1</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th></ia>	rk Services Platforn	1										
work Map and Health Ov	erview	-										
inks												
Content updated on 2024/06	i/25 13:49:17 (Click to up											
me	Ŧ	Operational S		ly Created	Link Type	Туре	Latency	Description	Er	ndPoint A Source	EndPoint A	EndPoint A
ston:1/1/c2/1Core_2:1/1/		enabled	• No	•	IP/IGP/CUPS	pointToPoint		N/A		ore_2	1/1/c2/1	10000
vice Sites		× <sup>n</sup>	Service Endpoints			e <sup>n</sup> Ports			x <sup>א</sup>	Services		
	Operational Stat		Service Endpoints Name		erational State	ر م <sup>a</sup> Ports Name	01	erational State	x <sup>3</sup>	Services Name	Opera	> tional State
e .				Ope			di	abled	×*			
ne				Ope	erational State	Name Port 1/3/4 1/2/c19	di	abled	x*			
				Ope	erational State	Name Port 1/3/4	di di di	abled	x <sup>2</sup>			

We can access more information from the Ports dashlet.

Expand the Ports dashlet and filter the list to show a port of interest.

July 2025

Issue 2

twork Map and Health	Overview									e	
orts											:
Content updated on 2024	4/06/25 14:19:43 (Click to update)										
lame		Operational State	NE ID	NE Name	Description	Administrative State	Stan	dby State	Position	Port Index	1
1/1/c2/1	× T	•		т	T	т	*	•	T		T
/1/c2/10		disabled	92.168.96.46	Boston		locked	prov	IdingService	shelf=1/car	1610899594	
1/c2/10		disabled	92.168.96.93	Core_2		locked	prov	idingService	shelf=1/car	1610899594	
/1/c2/1		enabled	92.168.96.46	Boston		unlocked	prov	idingService	shelf=1/car	1610899585	
1/c2/1		enabled	92.168.96.93	Core_2		unlocked	prov	idingService	shelf=1/car	1610899585	
		ر م Links		v×	Tunnel Bindings		×۶	Services			
etwork Elements	Operational State	ي <sup>×</sup> Links Name	Operational Stat		Tunnel Bindings Name	Operational State	× <sup>n</sup>	Services		Operational State	
etwork Elements	Operational State enabled	Name	Operational Stat /1Core_2:1 enabled			Operational State	u <sup>N</sup>			Operational State	
etwork Elements Ime IR-NRC		Name	-			Operational State	2			Operational State	
letwork Elements lame SR-NRC iore_1 iore_2	enabled	Name	-			Operational State	~			]	<u>که ۲</u>

Select the port and choose **Open in NE Inventory** from the Table row actions menu ( . An NE Inventory view opens in a new tab, filtered to show the selected port.
■ NOKIA Network Services Platform		User: admin	• ⑦
NE Inventory Boston			G
Equipment type filters • T <sub>e</sub> Any of: Port: 1/1/c2/1 x	^	0	ê=
Operational State: All   Administrative State: All   AppLy FILTERS		∧ Properties	
Boston (7750 SR-14a), Operational State: enabled, Administrative State: unlocked	:	NE Name Boston	
Equipment Group (Last Refresh: 2024-6-25 02:19:59)	~	NE Description —	
Shelf-1, Operational State: enabled, Administrative State: unlocked	:	Site ID 92.168.96.46	
Card Slot-1(xcm-14s-b) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Management IP 135.121.158.32	
Card-11xcm-14s-b), Operational State: enabled, Administrative State: unlocked	:	MAC Address C2:89:FF:00:00:00	
Card Slot-1/1(s36-100gb-qsfp28-3.6t) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Product 7750 SR	
Card-1/1(s36-100gb-qsfp28-3.6t), Operational State: enabled, Administrative State: unlocked	:	NE Type 7750 SR-14s	
1/1/c2, Operational State: disabled, Administrative State: unlocked	:	NE Version TiMOS-C-23.7.R2	
1/1/c2/1, Operational State: enabled, Administrative State: unlocked	:	Network Type Ip	
1/1/c2/10, Operational State: disabled, Administrative State: locked	:	Operational State enabled	
[9] Logical Group ILast Refresh: 2024-6-25 02:19:59)		Communication State	
En Link Aggregation Groups		SNMP://135.121.158.32 Communication	on State:
Routing Instances		PING://135.121.158.32 Communicatio	n State:
ACL Sets	I	Managed State	
• Tai BFD		Administrative State	
	A Back to top	Resync State done	
Auto-refresh equipment group	Filtered Count: 2		

From the NE Inventory, we can plot utilization statistics for the port. This will show that traffic is flowing.

From the port level in the equipment tree, choose Plot utilization statistics from the More menu (

■ NOCIA Network Services Platform		User: admin	• ⑦
NE Inventory Boston			Ċ
Equipment type filters	^		ê —
Operational State: All + Administrative State: All + APPLY FILTERS		∧ Properties	
Boston (7750 SR-14s), Operational State: enabled, Administrative State: unlocked	1	Name 1/1/c2/1	
- 🖪 Equipment Group (Last Refresh: 2024-7-18 10:47:29)	~	Description —	
Power Shelf Slot-1(ps-a10-shelf-dc) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Operational State enabled	
Power Shelf Slot-2(unassigned) (installedNotExpected), Operational State: disabled, Administrative State: unlocked	:	Administrative State unlocked	
🔹 🚆 Shelf-1, Operational State: enabled, Administrative State: unlocked	:	Standby State providingService	
🝷 📗 Card Slot-1(xcm-14s-b) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Position shelf=1/cardSlot=1/card=1/m	daSlot=1/mda=1/port=
Card-1(xcm-14s-b), Operational State: enabled, Administrative State: unlocked	:	MAC Address	
Card Slot-1/x1(unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked	:	Pert Index 1610899585	
👻 📗 Card Slot-1/1(s36-100gb-qsfp28-3.6t) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:	Port Type ethernet	
Card-1/1(s36-100gb-qsfp28-3.6t), Operational State: enabled, Administrative State: unlocked	:	Port Mode trunk	
1/1/c1, Operational State: enabled, Administrative State: unlocked	:	Encapsulation Type dot1q	
1/1/c2, Operational State: enabled, Administrative State: unlocked	:	MTU (bytes) 9212	
1/1/c2/1, Operational State: enabled, Administrative State: unlocked	:	Rate	
1/1/c2/2, Operational State: enabled, Administrative State: unlocked	Open in Current Alarms Open object	Actual Rate (Mbps)	
1/1/c2/3, Operational State: disabled, Administrative State: locked	Plot utilization statistics	State Reasons	
	Expand all		
Auto-refresh equipment group	Displayed Count: 82		

The Data Collection and Analysis Visualizations view opens in a new tab, showing a plot of utilization statistics for the port.



We can close the chart and inventory tabs, and return to the Ports dashlet. Select Open in Object Troubleshooting to see a summary of configuration and health information for the port.

twork Map and Health	Overview	•										
Ports												:
Content updated on 2024/	/06/25 14:19:43 (Click to update)											
ame		Operational State	NE ID	NE Name	Description	Administrative State	Standb	y State	Position	Por	t Index	:
1/1/c2/1	× T	•	T		т	т	•			Ŧ	T	
1/c2/10		disabled	92.168.96.46	Boston		locked	providi	ngService	shelf=1/car.		1610899594	
1/c2/10		disabled	92.168.96.93	Core_2		locked	providi	ngService	shelf=1/car.		1610899594	
'1/c2/1		enabled	92.168.96.46	Boston		unlocked	providi	ngService	shelf=1/car.		1610899585	
1/c2/1		enabled	92.168.96.93	Core_2		unlocked	providi	ngService	shelf= 👩	View in Cu	rrent Alarms	
											E Inventory	
											oject Troublesh	
									0	Plot utiliza	ation statistics	
										Plot error	statistics	
									0	Floterior		
twork Elements		e <sup>n</sup> Links		я L	Tunnel Bindings		u <sup>N</sup>	Services	0	FIGUEITO		
	Operational State	e <sup>n</sup> Links Name	Operational State	× <sup>3</sup>	Tunnel Bindings Name	Operational State		Services Name	0			
me				××						Operati	3	
ame 5R-NRC	Operational State	Name		× <sup>3</sup>		Operational State					3	× (
etwork Elements ame SR-NRC ore_1 ore_2	Operational State	Name		e <sup>8</sup>						Operati	3	

ect Troubleshooting > 1/1/c2/1 (92.168.96.46)	Troublesh	ooting				CHANGE TARGET	9
Troubleshooting Summary Board View troubleshooting summary information							
rt Overview mmary information for the selected port				Equipment Overview Summary information for the selected port equipment	t		
Port Type:			ethernet	Position:		shelf=1/cardSlot=1/card=1/mdaSlot=1/m	da=1/por.
Port Mode:			trunk	Product:			7750 S
Management Address:			135.121.158.32	Chassis Type:		7	750 SR-14
System Address:			92.168.96.46	Version:		TIMOS	5-C-23.7.R
Location:			N/A	Manufacture Date:			N
irrent Health Summary alth status for the selected port		Alarm Summary Alarms and impacts for the sel	ected port	Analytics Reports Run Analytics Reports			
Operational State:	enabled			Port			
	nlocked			Port Throughput Summary (NSP)	•		
Availability State:	N/A		0 0				
NE Communication State:	up	Critical Major	TCAs Total Impacts				
Open in NE Inventory		View in C	urrent Alarms				

From here, we can plot error statistics to see if problems are occurring on the port.

bject Troubleshooting > 1/1/c2/1 (92.168.	96.46) Troublesh	ooting						CHANGE TARGET	9
Troubleshooting Summary Board View troubleshooting summary information									dashboard
View troubleshooting summary information									utilization statis
									settings_label
Port Overview Summary information for the selected port						Equipment Overview Summary information for the selected port equipment			secongs_laber
Port Type:					ethernet	Position:	shelf=1/cardSlot=1/ca	ard=1/mdaSlot=1/	mda=1/por
Port Mode:					trunk	Product:			7750 SR
Management Address:				1	35.121.158.32	Chassis Type:			7750 SR-14s
System Address:					92.168.96.46	Version:		TiM	OS-C-23.7.R2
Location:					N/A	Manufacture Date:			N/A
Current Health Summary Health status for the selected port		Alarm Summa Alarms and impa		cted port		Analytics Reports Run Analytics Reports			
Operational State:	enabled					Port			
Administrative State:	unlocked					Port Throughput Summary (NSP)	►.		
Availability State:	N/A	0	0	0	0				
NE Communication State:	up	Critical	Major	TCAs	Total Impacts				
Open in NE Inventory			View in Cu	rrent Alarms					

The plot shows no errors.



## 5.3.8 Perform OAM tests

1

Performing OAM tests will provide another way to confirm connectivity of the NE. Click OAM Tests from the NSP main menu.

■ NO <ia network="" p="" pi<="" services=""></ia>	latform						User: admin	-	• @
NETWORK FUNCTIONS Network Map and Health	*							E,	
Network Health View									
Network Map View									:
Network Inventory View									
Object Troubleshooting									
Current Alarms	Operational State	NE ID	NE Name	Description	Administrative State	Standby State	Position	Port Index	:
OAM Tests	- [		T						
Device Management	· ·		<u>т</u>	· · · · · · · · · · · · · · · · · · ·	•	·	. т. Т. т.	Т	
Model Driven Configurator	disabled	92.168.97.250	Core_1	QSFP28 Connec	unlocked	providingService	shelf=1/slot	1610899520	
Device Discovery	disabled	92.168.96.215	Toronto	10/100 Etherne	locked	providingService	shelf=1/slot	1612447768	
IP/Optical Coordination	disabled	92.168.96.215	Toronto	10/100 Etherne	locked	providingService	shelf=1/slot	1612447776	
Data Collection and Analysis Service Management	disabled	92.168.97.250	Core_1	QSFP28 Connec	unlocked	providingService	shelf=1/slot	1610899584	
Path Control	disabled	92.168.96.215	Toronto	10/100 Etherne	unlocked	providingService	shelf=1/slot	1612709896	
PROGRAMMING	disabled	92.168.96.215	Toronto	10/100 Etherne	locked	providingService	shelf=1/slot	1612709912	
Developer Portal	disabled	92.168.96.215	Toronto	10/100 Etherne	locked	providingService	shelf=1/slot	1612709920	
Network Intents Workflows	disabled	92.168.97.250	Core_1	QSFP28 Connec	unlocked	providingService	shelf=1/slot	1610899648	
	disabled	92.168.97.250	Core_1	QSFP28 Connec	unlocked	providingService	shelf=1/slot	1610899712	
NSP ADMINISTRATION System Health					_			•	4
Map Layouts and Groups									
ile Server	⊭ <sup>≭</sup> Links		<sub>⊭</sub> " Ti	innel Bindings		⊭ <sup>∦</sup> Services			к <sup>3</sup>
Jsers and Security									
Artifacts	Name	Operational	State Na	ime	Operational State	Name	(	Operational State	

#### 2 –

We'll create TWAMP Light tests for the interfaces we created:

- 1. In the Data Collection and Analysis Management, Test Suites view, click + SUITE.
- 2. In the form that opens, select Twamp-light from the Test type drop-down.
- 3. Select Network Interface Address in the Entity type drop-down.
- 4. In the form that opens, select the interfaces we configured earlier in this process, and click

#### SELECT.

Test type											
Twamp-light											
ntity type											
Network Interface Addrei	Se	lect Network Interface A	ddresses							×	
Network Interf	0	Select between 2 and 10 item	5.				🖨 Bin (2 Items)			EMPTY	+ SELECT
NE ID		NE ID	Name	Operational status	Port	IPv4 Addresses	NE ID	Name	Operational status	Por :	Loopback :
							92.168.96.93	to_Bos_Int1	UP	1/1 🔳	
		92.168.96.215	system	UP		92.168.96.215/32	92.168.96.46	to_Core2_Int2	UP	1/1 🔳	
		92.168.99.38	system	UP		92.168.99.38/32					
		92.168.96.190	system	UP		92.168.96.190/32					
		92.168.96.46	system	UP		92.168.96.46/32					
		92.168.96.46	to_Core2_Int2	UP	1/1/c2/2:22	10.10.17.5/30					
		92.168.96.46	to_core2_int1	UP	1/1/c2/1:23	10.10.17.2/30					
		92.168.96.93	system	UP		92.168.96.93/32					
nplate elay Streaming (proacti		92.168.96.93	to_Bos_int1	UP	1/1/c2/1:23	10.10.17.1/30					
eray Streaming (proace	4 >	< e		IC C Page:	1 /1 > >	Row Count: 11					
t suite name 🔘									CANCEL	SELECT	
t suite description @	-										
st suite description 🔘											

- 5. Click GENERATE & EXECUTE to run the tests immediately.
- 3

Double click on the test suite to see the results. All tests are passing, verifying connectivity over the link.

Vfxr9JEzSISI8T	wmg2_Cyw Vie	v Test Suite D	retails						
AGGREGATE	D RESULTS	LIFECYC	CLE RESULTS	INDIVIDUAL RESULTS	GENERATION LOG	TESTS			
est suite execution IC	•								
46		SET TEST SU	ITE EXECUTION ID						
ast 7 days	•	telemetry:/ba	se/oam-pm/twamp-light	-delay-streaming - 4	est suite execution ID 6				Refresh Results
Test execution ID	Session name		System ID	Result classification	n Record stats	Time captured	Direction	Metric ID	Dela:
18	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	Passed	delay	2024-06-25 15:54:02	Round-trip	fd-average	6351
17	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	Passed	delay	2024-06-25 15:54:02	Round-trip	fd-average	6160
8	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	📀 Passed	delay	2024-06-25 15:53:52	Round-trip	fd-average	6246
17	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	Passed	delay	2024-06-25 15:53:52	Round-trip	fd-average	6472
18	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	Passed	delay	2024-06-25 15:53:42	Round-trip	fd-average	6106
17	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	📀 Passed	delay	2024-06-25 15:53:42	Round-trip	fd-average	6176
8	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	📀 Passed	delay	2024-06-25 15:53:32	Round-trip	fd-average	5647
7	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	🕑 Passed	delay	2024-06-25 15:53:32	Round-trip	fd-average	6048
8	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	📀 Passed	delay	2024-06-25 15:53:22	Round-trip	fd-average	6602
7	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	🔗 Passed	delay	2024-06-25 15:53:22	Round-trip	fd-average	6612
8	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	🔗 Passed	delay	2024-06-25 15:53:12	Round-trip	fd-average	6395
7	Vfxr9JEzSISI8Twr	ng2_Cyw-1	92.168.96.46	Seased	delay	2024-06-25 15:53:12	Round-trip	fd-average	5990
8	Vfxr9JEzSISI8Twr	ng2_Cyw-2	92.168.96.93	Passed	delay	2024-06-25 15:53:02	Round-trip	fd-average	6752

## 5.3.9 Restore the NE configuration

1

Finally, we can perform an optional restore operation. Returning to the Device Management, Managed Network Elements view, choose **Review backups**, **View backup history** from the Table row actions menu ( **‡** )

evice Management Managed Network El	lements <del>-</del>							
IE Name	Reachability	Management State	NE Mode	Management IP	NE ID	Product	। 🗊 २	₽,
	т –	· · · · ·	T	*			∧ Summary	
eattle	Reachable	-	MDM	135.121.147.210	92.168.96.190	7750 SR	1	
oston	Reachable	-	MDM	135.121.158.32	92.168.96.46	7750 SR	Boston	
pre_2	Reachable	-	MDM	135.121.158.121	92.168.96.93	Open NE Inventory	Management IP 135,121,158,32	
lgary	Reachable	Managed	Classic	135.121.149.11	92.168.98.97	View applicable adapto	NEID	
R-NRC	Reachable	Managed	Classic	135.121.148.123	92.168.99.38	Operation View operation history	92.168.96.46 NE Type	
re_1	Reachable	Managed	Classic	135.121.147.182	92.168.97.250	Review backups	SR-7750	
ironto	Reachable	Managed	Classic	135.121.147.235	92.168.96.215	Create an operation	View backup history View all backup files	
						Manage	• TIMOS-C-23.7.R2	
							Vender Nokia	
							Product	

NSP

#### 2

Select the most recent backup and choose **Restore** from the Table row actions menu (

■ NO <ia network<="" p=""></ia>	Services Platform							User: admin	• ⑦
Device Management > Manag Bos	ton Backup History	•							C
Displaying files in Device Mana	agement storage, view older	backup files. To compare back	up files, choose two successful backup	s.					
Completion Date =	Category	Operation Type	Operation Name	Duration	Status	Trigger			
DD/MM/YYY - DD/MM/YYY 🖬		T	Т		T	T	T		
2024/07/15 13:01:30	backup	nsp-ne-backup	Boston_17210628671	19s 684ms	Success	admin			
									Restore
									View files
									Open in Workflov

3

When the restore is completed, select the NE and click Manage, Resync.

The NE is working and is ready for further configuration.

# 5.4 Onboarding a service into NSP

### 5.4.1 Purpose

This process shows you how to use the NSP to create a service and to monitor service health, service components' health, and service performance.

See the NSP Network and Service Assurance Guide for detailed procedures.

### 5.4.2 Create a service using service management

**i** Note: This process assumes that intent types for service creation have already been imported into Network Intents.

1 -

In NSP's service management views, create an Epipe service template, and use the template to create an Epipe service.

See the service creation procedure in the NSP Service Management Guide.

## 5.4.3 View service information in the Network Map and Health dashboard

1 -

The Network Health View at the top of the Network Map and Health dashboard shows the health and configuration status of the services in the network.

NOCIA Network Services Platform				User: admin	•
vork Map and Health Overview	*				
Network Health View Determine the overall health of your network using the metr	cs below				
uipment Health Last Hour +	Service Health The status of all network services	Last 12 Hours +	Service Configuration Health The configuration status of all network services	Alarm Summary Unacknowledged root cause alarms	Last 6 Hours 👻
0% 0. <b>5</b> 0.	17: 21.	1.	38 2	37. 176△ 98△	0
Network Healthy NEs Affected Unreachable Health NEs NEs	Healthy Affected Services Services	Degraded Services	Total Misaligned Services Services	Critical Major Minor	TCAs
	-		View in Service Management	View in Current Alarm	s

2 -

Click on the Healthy Services circle in the Service Health dashlet to navigate to a filtered list of services. You can change the filters in this list as needed.

Select a service to navigate to Service Management or to the Object Troubleshooting dashboard from the table row actions menu.

etwork Map and Health	Overview .								E.
ervices									:
Content updated on 2024	/05/2 13:42:04 (Click to update)								
ame	Operational State	# Affected Objects	Degraded Status	Life Cycle S	itate Alignment St	ate Service Type	Description	Customer ID	5
	T	- 0 × T	•					Т	r ([
st	unknown	0		Removed	Aligned	E-Line		10	
RN 5101	enabled	0		Unknown	Unknown	L3 VPN	Vprn-5101	20	
S 6006	enabled	0		Unknown	Unknown	IES	les-6006	30	
SNodeB100	enabled	0		Deployed	Aligned	IES	N/A	100	
atarina_Epipe_200	enabled	0		Unknown	Unknown	E-Line		Demo	
nis is Site A	enabled	0		Unknown	Unknown	E-Line	Site A desc	Demo	
PIPE 979	enabled	0		Unknown	Unknown	E-Line	N/A	100	
SNodeC100	enabled	0		Deployed	Aligned	IES	N/A	100	
emoEpipe	enabled	0		Unknown	Unknown	E-Line	N/A	30	-
		10						<ul> <li>View in Current Alarms</li> <li>View in Object Troubles</li> </ul>	
etwork Elements	x <sup>7</sup>	Links		к <sup>л</sup>	Ports			View in Service Manage	-
								Add to Watchlist	
me	Operational State	Name	Operational State		Name	Operational State			
dNodeE	enabled	mdNodeE:1/1/c1/8mdN	disabled		Port 1/4/10	disabled	1		
ssicNodeB	enabled	mdNodeE:1/1/c1/1mdN	enabled		Port 1/1/34	disabled			
dNodeD	enabled	classicNodeC:Port 1/1/c1/	enabled		Port 1/4/12	disabled			

Click on the Total Services circle in the Service Configuration Health dashlet to navigate to a list of all services.

Select a service to navigate to Service Management or to the Object Troubleshooting dashboard from the table row actions menu.

etwork Map and Health	Overview	÷									E.	
ervices												:
Content updated on 2024	/05/2 14:52:07 (Click to update) Operational State	# Affected Objects	Degraded Status	Life Cycl	e State	Alignment State	Service Type	Description		Customer ID	1	
	T	- T						•	1		T	
INE-Service-229	disabled	6		Deploye	d	Aligned	E-Line	Service for R	ogers Telecomm	6		
PLS 5005	disabled	6		Unknow	n i	Unknown	E-LAN	Vpls-5005		10	ŧ	
pipe-5002	disabled	6		Unknow	n	Unknown	E-Line	Epipe-5002		Customer20		
INE-Service-228	disabled	6		Deploye	d	Misaligned	E-Line	Service for R	ogers Telecomm	6		
PIPE 6004	disabled	5		Unknow	i i	Unknown	E-Line	N/A		30	ŧ	
INE_Demo	disabled	5		Unknow	i	Unknown	E-Line			1		
moEpipe	disabled	4		Unknow	1	Unknown	E-Line	N/A		30	ſ	1
arc_epipe_100	enabled	4		Deploye	d	Misaligned	E-Line	Marc_epipe_	8 6 6 7 7 7 9 8 9 8 9 8 9 8 9 8 9 8 9 8 9 8 9	View in Current Ala		
PIPE 10	disabled	4		Unknow	1	Unknown	E-Line	Marc_epipe_	10 Desc A	View in Object Trou View in Service Ma		100
etwork Elements	к <sup>л</sup>	Links		к <sup>я</sup>	Ports			к <sup>л</sup>		Add to Watchlist		
ime	Operational State	Name	Operational State		Name	Op	erational State					
dNodeE	enabled	mdNodeE:1/1/c1/8mdN	disabled	î	Port 1/4/10	dis	abled	î				
ssicNodeB	enabled	mdNodeE:1/1/c1/1mdN	enabled		Port 1/1/34	dis	abled					
	enabled	classicNodeC:Port 1/1/c1/	enabled		Port 1/4/12		abled					

# 5.4.4 View the service in Service Management

1 -

Open **Service Management**, **Services**. Green icons indicate that the service was created and deployed successfully and is aligned with the template used to create it.

Service Management Services	•							+ CREATE	C.	
ife Cycle State	Alignment State	Composite Service	Service Name	Description	Service Template	:	(i) Info			
	-	T		T	T	T	States			
Unknown	Unknown		EPIPE 2121	N/A		: .				
Unknown	Unknown		EPIPE 6004	NZA		:	Life Cycle State			,
Unknown	Unknown		ELINE_Demo			:	Deployed	Nov 25, 2023, 12	:39:42 PM E	EST
Unknown	Unknown		Epipe-5002	Epipe-5002		:	Alignment State			
Unknown	Unknown		Katarina_Epipe_200			- E -	Aligned			
Deployed	Aligned		Marc_epipe_100		epipe	1				
Unknown	Unknown		NewTestEpipe	abcd		:	General Info			
Unknown	Unknown		NewerEPipe			1				
Unknown	Unknown		Rmtest			1	Service ID DemoEpipe			
Deployed	Aligned		AnooptestEpipe	abcdef	epipe	1	NE Service ID			
Deployed	Aligned		Anooptest02		epipe		999			
Deployed	() Misaligned		Marc Epipe 1		epipe	1	Service Name			
Deployed	<ul> <li>Aligned</li> </ul>	<	DemoEpipe		epipe	;	DemoEpipe			
Unknown	Unknown Green	icons indicate successful creation	EPIPE 5	N/A		:	Description			
Unknown	Unknown		EPIPE 3	Default Eline Template		:	N/A			
Unknown	Unknown		VPLS 6001	N/A		:	Service Type			
Unknown	Unknown		VPLS 5005	Vpls-5005		:	Customer ID			
Unknown	Unknown		VPLS 5006	Vpls-5006		:	30			
Unknown	Unknown		Vpls-6002				Service Manager ID			

2 -

Select the service. In the More I menu, there are multiple options for more information.

Service Management Services	•								+ CREATE	C+	
ife Cycle State	Alignment State	Composite Service	Service Name	Description	Servic	e Template	:	(i) Info			
	•		T	T	T		T	States			
Unknown	Unknown		EPIPE 2121	N/A		1.000					
Unknown	Unknown		EPIPE 6004	N/A View or o	change provisioning	Edit		Life Cycle State			,
Unknown	Unknown		ELINE_Demo			Clone		Deployed	Nov 25, 2023, 12:39	:42 PM E	ST
Unknown	Unknown		Epipe-5002	Epipe-5002		View Service Definition		Alignment State			,
Unknown	Unknown		Katarina_Epipe_200	-	-	Audit config		Aligned			
Deployed	Aligned		Marc_epipe_100	Aligh service	epip	Align Unassociate	_ '	AUDIT CONFIG	ALIGN		
Unknown	Unknown		NewTestEpipe	abcd		Migrate	- 1				
Unknown	Unknown		NewerEPipe			Resync	- 1	General Info			
Unknown	Unknown		Rmtest			Execute workflow	- 1				
Deployed	Ø Aligned		AnooptestEpipe	abcdef	epip	Remove		Service ID			
Deployed	Aligned		Anooptest02	Details a		View Service details		DemoEpipe Map			
Deployed	O Aligned		Marc Epipe 1		epip	Open in Object Troublesh	option	Map Components			
Deployed	O Aligned		DemoEpipe	N/A	epipe			Workflow executions			
Unknown	Unknown		EPIPE 5	N/A	Focused look at d	etails and problems	1	life cycle history			
Unknown	Unknown		EPIPE 3	Default Eline Templa	ate		:	Description			
Unknown	Unknown		VPLS 6001	N/A				N/A			
Unknown	Unknown		VPLS 5005	Vpls-5005			:	Service Type			
Unknown	Unknown		VPLS 5006	Vpls-5006				ELINE			
Unknown	Unknown		Vpls-6002				: -	Customer ID			

Choose **Open in Object Troubleshooting** to view the service in the Object Troubleshooting dashboard.

3

The Object Troubleshooting dashboard displays summaries of alarm, site, endpoint, and tunnel binding health, and if event recording has been enabled, an event timeline summary. From the view drop-down, you can navigate to the event timeline or to the Current Alarms page.

From the More menu ( ) at the top of the page, you can add the service to the watchlist or open other detailed views. Adding the service to the watchlist allows you to easily navigate directly to it in the future.

oject Troubleshooting > DemoEpine	Troubleshooting	÷				CHANGE TARGET	œ.	Ċ.	0	
Troubleshooting Summary Board     View troubleshooting summary information	Troubleshooting Event Timeline Current Alarms						1	Edit dashboa /iew in IP/Op /iew OAM te:	ird otical Coord	dinatic
ervice Overview ummary information for the selected service Customer Name: Service Type: Number of Sites:	Customer30 E-Line 2	Current Health Summary Health status for the selected service Administrative State: Life Cycle State: Alignment State: Operational State: State Cause:	unlocked Deployed Aligned enabled N/A	Sites Health Summary Service sites operational statistics	0 TCAs	Endpoints End			o CAs	
View in Service Management		Alarm Summary Alarms and impacts for the selected service		Analytics Reports Run Analytics Reports						
	0 CAs	0 0 0 0 TCAs	0 Total Impacts	Service OAM-PM Service Site Summary OAM-PM Service Summary	Þ					
Vent Timeline Summary Hetwork event timing for the selected service	State Updates Alarms	Sat, Nov 25, 1 19 TC Alarms 8 OAN Tests	2:51:00 EST 📑							

Scroll down in the view to see the Service map and Service inventory summaries.



Click **Expand size** ( $_{\mathbf{x}}^{\mathbf{x}}$ ) on the Service Endpoint summary dashlet to see detailed information about the port associated with the endpoint.

Select an endpoint and choose Open in NE Inventory from the table row actions menu (

bject Troublesho	nooting > Service DemoEpipe	Troublesh	ioting		•													CHANGE	TARGET	e,	Ð	
ervice Endpoi	pints																					:
Content upda	dated on 2023/11/25 14:58:24 (Clic	ck to update)																				
ame	Operational State	Site ID	1	Service	Por	rt Name		LAG Name		NE Name		Descriptio	n		State Cause(	)						
T			۲		T		٣		T		T			T								
ort 1/1/	enabled	92.168.96	. 1	DemoEpipe	Por	rt 1/1/c1/8				classicNode(	C	N/A										
rt 1/1/	enabled	92.168.96.7	- 0	DemoEpipe	Por	rt 1/1/8				classicNode	В	N/A									Current Al	
																					NE Invent	
																			0			
ervice Sites			х <sup>л</sup> х							т	unnel B	indings					e <sup>A</sup>					
	Operations		× <sup>a</sup>								unnel B	indings			Operational	tate	¥.					
me			л ¥							N	lame	indings	90-999		Operational : enabled	tate	×					
ame emoEpipe	Operationa		×							N 9	lame 2.168.96					itate	ж. К.					
ervice Sites ame emoEpipe emoEpipe	<b>Operationa</b> enabled		х <sup>л</sup> .							N 9	lame 2.168.96	5.26-circuit-			enabled	tate	×					

In the NE Inventory view, click on the port to see port details in the Info panel.

NOCIA Network Services Platform		User: admin	• ?
NE Inventory classicNodeC			G
Equipment type filters	+ +	0	ê =
Operational State: All + Administrative State: All + APPLY FILTERS		∧ Properties	
classicNodeC (7750 SR-2a), Operational State: enabled, Administrative State: unlocked	:	Name Port 1/1/c1/8	
Equipment Group	:	Description 10-Gig Ethernet	
🔹 🚆 classicNodeC, Operational State: enabled, Administrative State: unlocked	:	Operational State enabled	
Card Slot - 1 (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:	Administrative State unlocked	
Card - 1, Operational State: enabled, Administrative State: unlocked	:	Standby State providingService	
Daughter Card Slot - 1/1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked		Position shelf=1/slot=1/card=1/slot=1/	/card=1/port=c1/port=
Daughter Card - 1/1, Operational State: enabled, Administrative State: unlocked	1	MAC Address C0-5C-01-01-00-08	
Port 1/1/c1, Operational State: enabled, Administrative State: unlocked	1	Port Index 1610899528	
Port 1/1/c1/8, Operational State: enabled, Administrative State: unlocked		Port Type ethernet	
- 🗓 Logical Group		Port Mode access	
Eurik Aggregation Groups		Encapsulation Type dot1q	
Routing Instances		MTU (bytes) 1518	
ACL Sets		Rate lineRate	
• a SFD		Actual Rate (kbps) 10000000	
		State Reasons	
Auto-refresh     Last Refresh: 2023/11/25 15:08:59	▲ Back to top	Port Name 1/1/c1/8	

### 5.4.5 Initiate OAM tests from the service in the Object Troubleshooting dashboard

Returning to the Object Troubleshooting dashboard, create OAM tests to verify that the new service was provisioned and activated properly. On-demand testing verifies that traffic is flowing. After we have confirmed traffic, we can run proactive tests.

1 -

From the Object Troubleshooting dashboard, choose Create OAM Test Suite (2).

2 -

In the form that opens, configure the test parameters:

- 1. Choose the test type and select both service endpoints.
- 2. Choose an on-demand template from the Template drop-down.
- 3. Enter a name for the group of tests. Choose a name that will make the tests easy to tell apart from others in a test results page.

Click GENERATE & EXECUTE.

Image: Configure test datais       Configure test datais         Image: Configur	NOKIA Network Se	ervices Platform						User: admin	- ?
CMOM   titype   ELNE fadjoot   a emotipse   ELNE fadjoot to the set of the set	Generate OAM Tests								×
Carryine   ELNE Endpoint   Co tendigue test details   Configure test details   ELNE Endpoints     ELNE Endpoints     Site same     Site same   Site D   Service D     Service D   Service D        Service D <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>Î</td>									Î
IN Endpoint       •         Service       •         Q. Demotippe       •         ELINE Endpoints       •         \$2168.56.26.171/c1/8999       Port 1/1/1/8999.       unlocked       enabled       Demotippe       92.168.96.25       Demotippe         92.168.95.7.171/8999       Port 1/1/1/8999.       unlocked       enabled       Demotippe       92.168.96.7       Demotippe         92.168.95.7.171/8999       Port 1/1/1/8999.       unlocked       enabled       Demotippe       92.168.96.7       Demotippe         Stream	L		-						
service Q. Demotippe ELINE Enclopoints								Configure test details	
Q. Demotoppe         ELINE Endpoints         21.68.96.26-1/16/18.999         Q. 168.96.26-1/16/18.999         Q. 168.96.27-1/18.999         Port 1/17.8999         Port 1/17.8990         Port 1/17.8990         Port 1/17.8990         Port 1/17.8990         Port 1/17.8990         Port 1/17.8990         Port 1/17.8900	· · · · ·		·						
ELINE Endpoints     Endpoint ID     Name     Admin state     Operational   state     Site ID   Service ID        Site ID   Service ID        Site ID        Site ID   Site ID   Service ID        Site ID   Service ID        Site ID   Site ID   Service ID   Site ID   Service ID   Site ID   Service ID   Site ID   Site ID   Site ID   Service ID   Site ID   Site ID   Site ID   Service ID   Site ID <									
Endpoint ID Name Admin state Operational state Site name Site ID Service ID   2.188.96.2-11/1c1/8999 Port 11/1c1/899.0 unlocked enabled DemoEppe 92.168.96.7 DemoEppe   32.188.96.7-11/18.599 Port 11/18.599.0 unlocked enabled DemoEppe 92.168.96.7 DemoEppe   Template Template Choosing an on-demand template generates on-demand tests Text states description © Ap ID © Ap ID ©									
Statistice     Statistice <td>ELINE Endpoints</td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td>+ SELECT</td>	ELINE Endpoints								+ SELECT
92.168.95.7-1/1/8:99     Port 1/1/8:99     Port 1/1/8:99 </td <td>Endpoint ID</td> <td>Name</td> <td>Admin state</td> <td>Operational state</td> <td>Site name</td> <td>Site ID</td> <td>Service ID</td> <td></td> <td>:</td>	Endpoint ID	Name	Admin state	Operational state	Site name	Site ID	Service ID		:
Yampiate   Delay Streaming (on-demand)	92.168.96.26-1/1/c1/8:999	Port 1/1/c1/8:99	unlocked	enabled	DemoEpipe	92.168.96.26	DemoEpipe		Î
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test results easy to find in a list  App ID	92.168.96.7-1/1/8:999	Port 1/1/8:999.0	unlocked	enabled	DemoEpipe	92.168.96.7	DemoEpipe		î
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test Test suite description  App ID									
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test Test suite description  App ID									
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test results easy to find in a list  App ID									
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test results easy to find in a list  App ID									
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test results easy to find in a list  App ID									
Delay Streaming (on-demand)  Test suite same  Provide a name that will make the test results easy to find in a list  App ID									
Delity streaming (on-demand)       Test wite same ①       DemoSuiteOnDemand       Test wite description ②				Choosing an on	-demand template gen	erates on-demand tes	s		
DemoSuitconDemand     Provide a name that will make the test       results easy to find in a list       App ID ①	Delay Streaming (on-demand)		•						
DemoSulteOnDemand results easy to find in a list Test wite description  App ID	Test suite name 👔								
Test suite description (t)	DemoSuiteOnDemand				t				
	Test suite description 🚯								
CANCEL GENERATE & EXECUTE	App ID 🚯								-
								CANCEL	GENERATE & EXECUTE

The tests are executed.

3

When test generation is completed, choose **View OAM test results** from the More menu ( **:** ) in the **Object Troubleshooting** dashboard.

The **Data Collection and Analysis Management**, **Tests** page opens, filtered to show the tests on the service. Select an on-demand test and choose **View Results** from the table row actions menu ( **•**).

Data Collection and Analysis Management	Tests							+ TEST C
ilter	Test name	Admin state	Execution status	NE ID	Test type	Execute type	Service ID	Test suite
ist type	DemoSuite-1	Disable	Stopped	92.168.96.26	CFM DMM	Proactive	DemoEpipe	DemoSui
CFM DMM +	DemoSuite-2	Enable	Running	92.168.96.7	CFM DMM	Proactive	DemoEpipe	DemoSui
me	DemoSuiteOnDemand-1	Disable	Stopped	92.168.96.26	CFM DMM	On-demand	DemoEpipe	DemoSul 🤃
	DemoSuiteOnDemand-2	Disable	Stopped	92.168.96.7	CFM DMM	On-demand	DemoEpipe	View Results
D								Edit
								Execute Delete
cute types								
•								
vice ID								
DemoEpipe								
it suite								

The on-demand test has passed, verifying that traffic is flowing.

st 1 day	- tel	emetry:/base/oam-pm/eth-cfm-delay-streaming (Default)	•					Refresh Results
est execution	Result	Session name	NE ID	Time captured	Owner	App ID	Object ID	:
3	Passed	DemoSuiteOnDemand-1	92.168.96.	26 2023-11-27 13:40:26		NSP	/state/oam-pr	n/session[session

### 5.4.6 View port details and utilization data in real time

From the NE inventory view, you can launch a utilization chart to view raw utilization data and verify that traffic is moving between service endpoints. This request creates a temporary telemetry subscription, which is deleted when the utilization chart is closed.

1 -

Identify the service endpoints:

- 1. Open the Object Troubleshooting dashboard for the service and navigate to **Service Endpoints**.
- Select an endpoint and choose Open in NE Inventory from the table row actions menu (
   ).

The NE Inventory view for the endpoint NE opens.

2 -

In the **NE Inventory** view, click on a port. The port properties display in the **Info** panel. From the More menu for the port ( **1**), choose **Plot utilization statistics**.

CLOSE

ventory classicNodeC			
pment type filters • $\overline{T}_{+}$ Any of:	*	0	έΞ
rational State: All    Administrative State: All   APPLY FILTERS		∧ Properties	
classicNodeC (7750 SR-2a), Operational State: enabled, Administrative State: unlocked	:	Name Port 1/1/c1/8	
Equipment Group	:	Description 10-Gig Ethernet	
ClassicNodeC, Operational State: enabled, Administrative State: unlocked	:	Operational State enabled	
Card Slot - 1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Administrative State unlocked	
Gard - 1, Operational State: enabled, Administrative State: unlocked	:	Standby State providingService	
🔹 📗 Daughter Card Slot - 1/1 linstalledAndExpected], Operational State: enabled, Administrative State: unlocked	:	Position shelf=1/slot=1/card=1/slot=1	1/card=1/port=c1/
Daughter Card - 1/1, Operational State: enabled, Administrative State: unlocked	:	MAC Address C0-5C-01-01-00-08	
Port 1/1/c1, Operational State: enabled, Administrative State: unlocked	:	Port Index 1610899528	
Port 1/1/c1/8, Operational State: enabled, Administrative State: unlocked	(;)	Port Type ethernet	
Logical Group	Open in Current Alarms	Port Mode access	
Link Aggregation Groups	Plot utilization statistics	Encapsulation Type dot1q	
Routing Instances		MTU (bytes) 1518	
ACL Sets		Rate	
BFD.		Actual Rate (kbps)	
		State Reasons	
	A Back to top		

3 -

**Data Collection and Analysis**, **Visualizations** opens, showing the chart of the pre-configured utilization counters.

NSP

#### Network troubleshooting using NSP functions Troubleshooting using NSP assurance functions Onboarding a service into NSP



4

The creation of the chart creates a temporary subscription for the utilization counters.

The subscription is automatically deleted when you close the chart.

Tip: The description of the temporary subscription is Created by telemetry data subscription.

5

While the chart is open, you can:

- a. Review the details of the pre-configured subscription by clicking Configure.
   Tip: From the New Chart, Configuration form, copy the Object Filter string. You can use this string to create a permanent subscription.
- b. Edit the chart configuration, for example, to show different counters.

NOCIA Network Services Platform		User: admin 🗸 🦪
New Chart Configuration		×
Collection Interval Seconda)* 10 Combine charts	Time Range Last 1 hour -	
Telemetry & Resource Filter Definitions		+ DEFINITION
Telemetry Type telemetry-/base/interfaces/utilization		×
Counters (input-utilization X) output-utilization X received-octets-periodic X	transmitted-actes-periodic ×)	
Object Filter	/hardware-component/port[component-id='shelf=1/slot=1/card=1/slot=1/card=1/port=c1/port=8']	

c. Save the chart to make the chart available from **Data Collection and Analysis**, **Visualizations** in the future.

NOCIA Network Services Platform		User, admin	• ⑦
New Chart Configuration			×
Collection Interval Secondal* 10 Combine charts	Time Range Last 1 hour	•	
Telemetry & Resource Filter Definitions			+ DEFINITION
Telemetry Type telemetry /base/interfaces/utilization Counters Object Filer  1 /nsp-equipment.network/network-element[ne-id=92.168.96.201/hardware-component]	Chart for utilization		
SAVE AS		CANCEL	PLOT

## 5.4.7 Create permanent telemetry subscriptions for the service endpoints

Creating a telemetry subscription is an optional step, used for monitoring performance over time. A telemetry subscription allows you to configure statistics collection, for example, utilization statistics for a service, and to run the collection at any time, for example, for use in SLA management. Statistics can also be used to generate Analytics reports. To learn how to create a subscription, and for information about aggregation and retention for use in reporting, see the *NSP Data Collection and Analysis Guide*.

Perform the subscription creation procedure to create subscriptions for the service SAPs. See the *NSP Data Collection and Analysis Guide* for more information.

Use the object filter string you copied from the temporary subscription in Stage 5.

<sup>1</sup> 

NO <ia network="" platform<="" services="" th=""><th></th><th></th><th></th><th></th><th>User: admir</th><th>1</th><th>• (?</th><th>Ð</th></ia>					User: admir	1	• (?	Ð
Create Subscription							3	×
General	General							Î
Filters & Counters	Name ServiceSubscription		Description					
These parameters control when and how often	Collection Interval (seconds)	Sync-Time (hh:mm)	State	DB Subscriptic				
These parameters control when and how often	900	00:00	KANNA DATA AND A	Enabled	- Cx			
	File Subscriptions Disabled	Filename Prefix for File Subscriptions						
	Filters & Counters	t[ne-id='92.168.96.26']/hardware-component/po	t[component-id="shelf=1/slot=1/card=1/	/slot=1/card=1/port=c1/	port=8']			ļ
	Telemetry Type							
	Type to find telemetry type	×						
	Enable notifications and notification counter	ers + COUNTERS						
	No Co	unters						
						CANCEL	CREAT	

## 5.4.8 View utilization statistics from the Network Map and Health dashboard

1 -

In the Network Map and Health dashboard, navigate to the network map. Choose **Enabled** from the **Utilization** drop-down.



Hover over a link in the network map to show utilization information.



A subscription is automatically created for the ports associated with the endpoints for NEs present on the Network Map and Health dashboard utilization map.

3

Open **Data Collection and Analysis**, **Management**. Edit the temporary subscription as needed.

To chart a subscription, select the subscription and choose **Open in Data Collection and Analysis Visualizations** from the table row actions menu ( **‡** )

Note: Two subscriptions are automatically generated, for two telemetry types: base/classic-utilization/utilization and base/interfaces/utilization. The interfaces telemetry type must be used for charting.

Tip: The name of each subscription starts with netsup-.

Data Collection and Ar	alysis Management Subscriptions -						+ SUBSCRIPTION	<i>}</i> :
Telemetry Subscripti	ons 👻							
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	
	·							
Enabled	TestSuiteExOAM-PM-DMM-bin-acc	telemetry:/base/oamp	300	00:00	$\checkmark$			
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM-DMM-accounting	telemetry:/base/oamp	300	00:00	$\checkmark$			
Enabled	TestSuiteExOAM-PM-CFM-delay-streaming	telemetry:/base/oam	10	00:00	~			
Enabled	ServiceSubscription	telemetry:/base/interf	900	00:00		$\checkmark$		
Enabled	netsup-link-utilization-admin-1701120188633	telemetry:/base/interf	30	00:00	$\checkmark$			
Enabled	netsup-link-utilization-admin-1701120188633_classic_telemetry	telemetry:/base/classi	30	00:00	~			
						🖍 Edit		
						🖸 Open in Data (	Collection and Analysis Visua	lization

Last Refresh: 2023-11-27 16:25:09 (Local Time)

▶ 4 ▶ Row Count: 6

# 5.5 LSP Throughput with Forecast reporting scenario

### 5.5.1 Purpose

The LSP Throughput with Forecast (NSP) report provides the throughput trend for an LSP. The report can generate a forecast for daily and monthly granularities.

This process shows how to set up a service for LSP Throughput with Forecast reporting in Analytics.

### 5.5.2 Confirm that prerequisites for service provisioning are completed

1

Two intent type bundles are required for provisioning our service, and for setting up QoS and telemetry: icm-intent-types, and mdt-intents.

Checking the list in the **Artifacts**, **Artifact Bundles** view shows that both bundles are in Installed status.

	*								IMPORT & INSTALL
Automatic reconcile of artifacts and artifact bu	ndles is do	one every 3 mins. Next reco	ncile will happen in 2 min 6 sec						
undle Name		Bundle Version	Status	N	lumber of Artifacts	Author	Import Time =	:	(i) Artifact Bundle Details
	T		T	T					Status
nsp-telemetry-cr-va-sros-1.0.0-rel.17.zip		1.0.0	Installed		2	NOKIA R&D	2023/11/27 20:52:03	:	Installed
nsp-icm-intent-types-23.11.0-rel.505-cam.zip		23.11.0-rel.505	Installed		47	NOKIA R&D	2023/11/22 09:06:27	:	Bundle(s) Name
nsp-mdt-intents-23.11.0-rel.756-svc-assuran bundle.zlp	:e-	23.11.0	Installed		8	NOKIA R&D	2023/11/22 09:06:27	1	nsp-lcm-intent-types-23.11.0-rel.505-cam.zip
nsp-mdt-intents-23.11.0-rel.756-svc-intent- bundle.zip		23.11.0	Installed		26	NOKIA R&D	2023/11/22 09:06:27	:	Author NOKIA R&D
nsp-ne-upgrade-1.4.0.zip		1.4.0	Partially Installed		20	NOKIA R&D	2023/11/21 22:27:02	1	Version
nsp-ne-backup-audit-1.0.1.zip		1.0.1	Installed		2	NOKIA R&D	2023/11/21 22:26:59	1	23.11.0-rel.505 Number of Artifacts
nsp-ne-upgrade-with-phases-1.4.0.zip		1.4.0	Installed		27	NOKIA R&D	2023/11/21 22:26:59	1	47 Import Time
nsp-ne-restore-1.2.0.zip		1.2.0	Installed		6	NOKIA R&D	2023/11/21 22:26:58	:	2023/11/22 09:06:27
nsp-ne-upgrade-eth-sat-1.3.0.zip		1.3.0	Installed		8	NOKIA R&D	2023/11/21 22:26:54	:	Additional Info N/A
nsp-ne-wavence-upgrade-1.0.0.zip		1.0.0	Installed		9	NOKIA R&D	2023/11/21 22:26:54	:	Signature
nsp-ne-backup-1.3.0.zip		1.3.0	Installed		6	NOKIA R&D	2023/11/21 22:26:53	:	
nsp-ne-sw-import-1.2.0.zip		1.2.0	Installed		4	NOKIA R&D	2023/11/21 22:26:53	:	
nsp-wavence-service-migration-1.0.0.zip		1.0.0	Installed		4	NOKIA R&D	2023/11/21 22:26:53	1	

#### 2 -

NSP installs the intent types to Network Intents, from which they can be imported to Service Management.

The **Service Management**, **Intent Type Catalogue** view shows that the intent types have been imported and are available for use in service management.

NSP

	Network Services Platform						User: admin	•	(
iervice Management	Intent Type Catalogue	•						IMPORT	(
tent Type	Intent Type Version		Labels	Build	Last Updated Time	:	(i) Info		
	Т	T	T	T		T	Select an intent type		
unnel		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
pipe		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
orn		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
ols		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
s		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			

Switching to the **Service Management**, **Service Templates** view shows that the intent types have been used to create templates for various service types.

rvice Management	Service Te	emplates 👻											Е (
rvice management	Service le	mpiates •										+ CREAT	- (
nplate Name		Description		Intent Type		Intent Version		State		Config Form	:	i Info	
	T		Ŧ		T		T		•			Select a service template	
pe		Default Epipe template		epipe			2	Released		default	:		
n		Default VPRN template		vprn			2	Released		default	:		
5		Default VPLS template		vpls			2	Released		default	:		
		Default IES template		ies			2	Released		default	1		

## 5.5.3 Verify the service parameters

1 –

From the Service Management, Services view, we can see the provisioned services.

ervice Management Services						+ CREATE C
e Cycle State	Alignment State Composite Servic	e Service Name	Description	Service Template	:	i Info
•		T	T	т	۲.	States
Unknown	Unknown	NewTestEpipe	abcd		: ^	
Unknown	Unknown	NewerEPipe			:	Life Cycle State
Unknown	Unknown	Rmtest			:	<ul> <li>Deployed Nov 27, 2023, 10:06:50 PM EST</li> </ul>
Deployed	Aligned	AnooptestEpipe	abcdef	epipe	:	Alignment State
Deployed	⊘ Aligned	Anooptest02		epipe	:	O walked
Deployed	⊘ Aligned	Marc Epipe 1		epipe	:	
Deployed	Aligned	DemoEpipe		epipe		General Info
Deployed	Ø Aligned	EPIPE 5	N/A	epipe	:	Service ID
Deployed	Ø Aligned	EPIPE 3	Default Eline Template	epipe	:	DemoEpipe
Deployed	Aligned	Marc_epipe_10	test	epipe	:	NE Service ID
Unknown	Unknown	VPLS 6001	N/A			999
Unknown	Unknown	VPLS 5005	Vpls-5005			Service Name DemoEpipe
Unknown	Unknown	VPLS 5006	Vpls-5006		:	Description
Unknown	Unknown	Vpls-6002			:	a can prove
Unknown	Unknown	IES 6006	les-6006			Service Type
Unknown	Unknown	IES 5201	les-5201		:	ELINE
Unknown	Unknown	les-5200	les-5200		:	Customer ID
Unknown	Unknown	les-6005			:	30
19-1	101	100.40	1777			Service Manager ID

2 -

Opening the Edit form for a service will let us verify that everything we'll need is in place. Select the service and select Edit from the Table row actions menu.

ervice Management Services	÷						+ CREATE	G
e Cycle State	Alignment State Composite Ser	vice Service Name	Description	Service Template	:	(i) Info		
•	•	τ.	T [	τ	۲	States		
Unknown	Unknown	NewTestEpipe	abcd		: 1			
Unknown	Unknown	NewerEPipe			:	Life Cycle State		
Unknown	Unknown	Rmtest			:	<ul> <li>Deployed</li> </ul>	Nov 27, 2023, 10:06:50	) PM EST
Deployed	⊘ Aligned	AnooptestEpipe	abcdef	epipe	:	Alignment State		
Deployed	⊘ Aligned	Anooptest02		epipe	:	( AilBried		
Deployed	Aligned	Marc Epipe 1		epipe	:			
Deployed	Aligned	DemoEpipe		epipe		General Info		
Deployed	Aligned	EPIPE 5	N/A	epip Edit		Service ID		
Deployed	Aligned	EPIPE 3	Default Eline Template	epip Clone		DemoEpipe		
Deployed	Aligned	Marc_epipe_10	test	epip View Service Definition	n	NE Service ID		
Unknown	Unknown	VPLS 6001	N/A	Audit config		999		
Unknown	Unknown	VPLS 5005	Vpls-5005	Align	,	Service Name DemoEpipe		
Unknown	Unknown	VPLS 5006	Vpls-5006	Migrate		Description		
Unknown	Unknown	Vpls-6002		Resync		Desciption		
Unknown	Unknown	IES 6006	les-6006	Execute workflow		Service Type		
Unknown	Unknown	IES 5201	les-5201	Remove		ELINE		
Unknown	Unknown	les-5200	les-5200	View Service details		Customer ID		
Unknown	Unknown	les-6005		Open in Object Trout	leshooting	30		
11.1	10	170.40				Service Manager ID		

3 -

The Edit service form shows the basic service parameters such as service name and customer ID, and the service endpoints.
	Network Services Platform						User: admin	• ②
Edit Service: DemoEpip	e							
Site A	Template Name 0		Current Life Cycle State		Alignment State			
Site B	epipe		Deployed		Aligned			
SDP Details	Service Name"		NE Service ID*		мти			
	DemoEpipe		999		1492			
	Customer ID*		Description		Admin State			
	30	0			unlocked	✓ □x		
	Job ID							
	Site A							
	Device ID		Site Name		Description			
	92.168.96.7	× 0						
	мти							
	Endpoint					+ ADD		
	Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		
	Port 1/1/8	dot1q	-1	999	unlocked	1		
						► 4 F		

Site A of the service is on node B. Select the endpoint and choose Edit to verify the endpoint parameters.

In the Edit Endpoint form, we can see the ingress and egress QoS policies applied, and any overrides that have been added.

Ingress Adm SAP Ingress Un Overnides Accor Policer Control Policy 202 Overnides Root CP Priority Mts Thresholds	rt 1/1/8 nin State allocked • C	0 	Encap Type dot1q Description Multi Service Site	Outer VLAN Tag 999 Collect Accounting Statistics		
Ingress Por QOS Adm SAPIngress U Overrides Acce Policer Control Rolky Z2C Overrides Root CP Priority Mts Thresholds	rt 1/1/8 nin State Nocked - C ounting Policy 0 ×	0 	dottq Description	999		
QSS Adm SAP Ingress un Overrides Acces Policer Control Rolicy 202 Overrides Root CP Priority Mts Thresholds	nin State Nicked - C ounting Policy 0 X	Ē	Description			
SAP Ingress un Overrides Acce Policer Control Policy 20 Overrides Root CF Priority Mts Thresholds	nlocked • Counting Policy	□ x		Collect Accounting Statistics		
Overrides Acces Policer Control Policy 20 Overrides Root CF Priority Mbs Thresholds	sunting Policy 0 X		Multi Service Site	Collect Accounting Statistics		
Policer Control Policy 20 Overrides Root CCF Priority Mbs Thresholds	0 ×		Multi Service Site			
Overrides Root Priority Mbs Thresholds		0				
Root CF Priority Mbs Thresholds	PU Protection					
Priority Mbs Thresholds	PU Protection					
. K. 197 K.						
Scheduler Policy Pe Overrides	olicy ID					
Aggregate Policer	Enable QoS		Enable IP/IPv6 Filter			
QoS Ing SAP Egress	gress					
Overrides						
Overrides Root	Qo5 Match QinQ DotTp Select Item -					
Priority Mbs Thresholds Scheduler Policy						
	SAP Ingress					
Vlan Qos Policy	Queuing Type		Policy Name			
Egress Remark Policy	Select Item	-	Ingress99			
					CANCEL	UPDATE

Returning to the Edit Service form, we can see the SDP details, the service destination points. An SDP has been added to the service for each direction.

A B Details	SDP Details							
	Admin State					+ ADD		
		Source Device ID	Destination Device ID	Steering Parameter	SDP ID	Description		
	unlocked	92.168.96.7	92.168.96.26		90	I		
	unlocked	92.168.96.26	92.168.96.7		90	I		
	4		< < Page: 1	/1 > >		Total: 2		

Each SDP uses an LSP, and it's this LSP that will provide the throughput telemetry data for our report.

## 5.5.4 Verify accounting policy configuration

1 -

To collect statistics on an NE, a file and accounting policy must be configured on the NE. This can be done by deploying a template in the **Device Management**, **Configuration Deployments** view.

In the Configuration Deployments list, we can see that a template called Custom File and Accounting has been deployed on the NE and the Deployment Status is Deployed Aligned.

NSP

Dev	rice Management Configurat	ion Deployments 🔹							+ DEPLOYMENT
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Catego :	(i) Deployment Details
_	*	•		<b>T</b>	T	т	•		NE Name
	Deployed Aligned	• Modified	mdNodeD	92.168.96.60	1/1/c1/1	ICM Ethernet	Physical	Port	<ul> <li>classicNodeC</li> <li>NE ID</li> </ul>
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Port 1/1/c1/9	ICM Ethernet	Physical	Port	92.168.96.26
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Port 1/1/9	ICM Ethernet	Physical	Port	Identifier Accounting Policy ID
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	20	File and Accounting	Logical	Log 🚦	66
	Deployed Aligned	Modified	mdNodeD	92.168.96.60	20	File and Accounting	Logical	Log :	
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	20	File and Accounting	Logical	Log	Deployment Status     Opployed Aligned
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	20	File and Accounting	Logical	Log :	AUDIT ALIGN
	Deployed Aligned	Modified	mdNodeE	92.168.96.16	Ingress99#99	SAP Ingress QoS	Logical	QoS :	
	Deployed Aligned	Modified	mdNodeD	92.168.96.60	Ingress99#99	SAP Ingress QoS	Logical	QoS :	Last Audit
	Deployed Aligned	Modified	classicNodeC	92.168.96.26	Ingress99#99	SAP Ingress QoS	Logical	QoS :	Last Alignment Nov 28, 2023 9:10:31 am by admin
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Ingress99#99	SAP Ingress QoS	Logical	QoS :	Template Name
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	Egress99#99	SAP Egress QoS	Logical	QoS :	Custom File and Accounting
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	Egress99#99	SAP Egress QoS	Logical	QoS :	Nov 28, 2023 8:44:19 am
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Egress99#99	SAP Egress QoS	Logical	QoS	Last Updated Nov 28, 2023 9:10:31 am
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Egress99#99	SAP Egress QoS	Logical	QoS .	Role
	Deployed Aligned	• Modified	mdNodeE	92.168.96.16	66	Custom File and Accou	Logical	Log	Category
	Deployed Aligned	• Modified	mdNodeD	92.168.96.60	66	Custom File and Accou	Logical	Log 🚦	log Configuration Status
~	Deployed Aligned	Modified	classicNodeC	92.168.96.26	66	Custom File and Accou	Logical	Log	Modified
	Deployed Aligned	• Modified	classicNodeB	92.168.96.7	66	Custom File and Accou	Logical	Log	

We can view the template details to see policy details:

- 1. Select the deployment and choose View/Edit from the Table row actions menu.
- 2. In the form that opens, click VIEW/EDIT TEMPLATE CONFIG.

The template information shows the rollover duration, or how long a statistics collection file remains open before a new file is started, the retention period for the file, and the compact flash location where the file is stored. Accounting policy details show that the policy applied is number 66, and it will be collecting Combined MPLS LSP Egress statistics.

Set of the defendence of th		OKIA Network Services Platform			User: ad	min	• ⑦
seet ive     Ing     Ing <th>Deploy Log</th> <th>ical Configuration</th> <th></th> <th></th> <th></th> <th></th> <th>×</th>	Deploy Log	ical Configuration					×
ric         Corpact Flank Location         Receiving Policy         Fie         Fie <th>Select Tem;</th> <th>Custom File and Accounting</th> <th></th> <th></th> <th></th> <th>×</th> <th></th>	Select Tem;	Custom File and Accounting				×	
Accounting Pailsy     File     Image:     File     Image:		File	Log				Î
66 Fe Polyo 66   Fe Polyo 66 Fe Polyo for collection LSP Egress statistics   15 4    Compact Flash Location   memory   etcourting Policy     Accounting Policy    Accounting Policy for collection LSP Egress statistics   terred   control   Accounting Policy for collection LSP Egress statistics   terred   control   control   control      Accounting Policy for collection LSP Egress statistics   terred   control   control    Accounting Policy Farses statistics   terred   control    Accounting Policy Farses statistics   terred   control    Accounting Policy Farses statistics   terred   control    Accounting Policy Farses statistics     Accounting Policy Farses statistics Terred   Control Control  Accounting Policy Farses statistics Terred  Control  Control			File				_
Image:						_	
15 4   Compact Flash Location   Ninnry   Constrained Policy   Accounting Policy data   Accounting Policy data   Named   Constrained MPLS LSP Egress   Combined MPLS LSP Egress			66	File Policy 66	File Policy for collection LSP Egress statistics	_	/
15 4     Compact Flash Location     Pinary     CB:     Accounting Policy     Accounting Policy Sone     Accounting Policy Sone     Combined MPLS LSP Egress     S     Combined MPLS LSP Egress     Combined MPLS LSP Egress     Combined MPLS LSP Egress     S     Combined MPLS LSP Egress     Combined MPLS LSP Egres				Retention (hours)			sust: 1
Pinnyy     d:::::::::::::::::::::::::::::::::::			15	4			Contra - 1
Pinnyy     d:::::::::::::::::::::::::::::::::::							
Accounting Policy         Accounting Policy Hame         Accounting Policy 65         Reserd         Combined MPLS LSP Egress			Compact Flash Location				
cts:       Image: Constraint of Constraints Policy for collection LSP Egress statistics         Accounting Policy for       enable       Description         Accounting Policy 66       enable       Image: Collection LSP Egress statistics         Becode       Collection Interval (Iminutes)       Image: Collection LSP Egress statistics         Combined MPLS LSP Egress       Image: Collection LSP Egress statistics       Image: Collection LSP Egress statistics			Primary				CONFIG
Accounting Policy         Accounting Policy Hame       Admin State       Description         Accounting Policy 65       enable       Control Co							
Accounting Policy 66       enable       Calculation Result       Calculation Interval (minutes)         Combined MPLS LSP Egress       C       5       S         1. Custem File and Accounting:       1. Custem File and Accounting:       C							
Accounting Policy 66       enable       Calculation Result       Calculation Interval (minutes)         Combined MPLS LSP Egress       C       5       S         1. Custem File and Accounting:       1. Custem File and Accounting:       C							
Accounting Policy 66       enable <ul> <li>Accounting Policy for collection LSP Egress statistics</li> <li>Second</li> <li>Combined MPLS LSP Egress</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> </ul> <ul> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> </ul> 1. Custem File and Accounting: <ul> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> </ul> <ul> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> <li>Control of the set Accounting Policy for collection LSP Egress statistics</li> </ul>			Accounting Policy				
Record     Collection Interval (minutes)     curret:1       Combined MPLS LSP Egress     CR     5							
Combined MPLS LSP Egress  CR S CANCEL UPDATE			Accounting Policy 66	enable - 🗸	Accounting Policy for collection LSP Egress statistics		
CANCEL UPDATE							punt:1
1. Custom File and Accounting :			Combined MPLS LSP Egress -	5			
1. Custom File and Accounting :							
1. Custom File and Accounting :							
						ANCEL OPDATE	
		1. Cust	om File and Accounting :				
						CANCEL	

## 5.5.5 Verify the LSP parameters

1 -

LSPs must be configured on the NE. Opening an NE session will show us the configuration of the LSP in use by the SDP. It's called lsp\_NodeC\_to\_nodeB.

We can see that an accounting policy is in place on the LSP, and collection of egress statistics is enabled. These are required for any LSPs we want to monitor for LSP Throughput reporting.

The account policy ID for this LSP is 66.

NE Session	NOCIA Network Services Platform	User; admin	
SSH     IPAdersa     DSCONNECT     Theme	NOCIA Network Services Platform	User: admin	- ?
SSH     IPAdersa     DSCONNECT     Theme	asion (		
SSH     198.51.00.0     DISCONNECT     Theme       classicktodedC     configure router mpls lap "lap_nodeC_to_nodeB"	Search1		
<pre>classicRodeCf configure router mpls lsp "lsp_nodeC_to_nodeB" classicRodeCf configUrenter&gt;mplslsp info</pre>			_
<pre>classicNodeC&gt;config&gt;route=*mpls&gt;lapf info to 92.168.96.7 from 92.168.96.7 from 92.168.96.6 agrees=vtatistics accounting=policy accoun</pre>	* 198.51.100.0 DISCONNECT		Theme 🛑
<pre>classicNodeC&gt;config&gt;route=*mpls&gt;lapf info to 92.168.96.7 from 92.168.96.7 from 92.168.96.6 agrees=vtatistics accounting=policy accoun</pre>			
to 92.163.96.7 from 92.163.96.7 from 92.163.96.7 exproduces that constructions accounting-policy 66 no shutdown exit path-computation-method local-capf for a site per-control facility exit per-control primary "path_toNodes" exit no shutdown	sicWedeXt configure router mpls lsp "lsp_nodeC_to_nodeB"		
<pre>from 92,168.96.26 egreas-statistics collect-stats collect-stats collect-stats counting-policy 66 no shutdown exit peth-computation-method local-capf fest-recoute facility exit pow-controls pow-report shable pow-montrols put y puth_toNode8* exit no shutdown </pre>			
egress-statistics collect-stats accounting-policy 66 min o shutdown path-computation-method local-cspf fast-reroute facility exit pce-control primary "path_toxodes" exit exit o shutdown	to 92.160.96.7 from 92.168.96.26		
accounting-policy 66 no shutdown whit past-computation-matched local-capf f actions per-control primary "path_toNodes" shit art no shutdown			
no shutdown exit path-computation-method local-capf fmat-reroute facility exit poe-capport enable poe-control putancy 'path_toXodeB" a no shutdown	collect-stats		
exit path-computation-method local-capf fast-reroute facility exit per-report enable per-control primary "path_tANodeB" exit no shutdown	accounting-policy 66		
fast-zeroute facility exit pee-report emable pee-control primary "path_tANodeB" exit no shutdown	exit		
exit pee-report enable pe-control primary "peth_toxOdeB" exit exit to shurtdown	path-computation-method local-capf		
pee-report enable pee-control primary "path_tANodeB" exit no shutdown	fast-reroute facility		
pe=control primary "path_toNodeB" exit no ahutdown			
exit no shutdown	pce-control		
no shutdown	primary "path_toNodeB"		

### 5.5.6 Verify statistics collection configuration

Now that we have verified that the service and LSP are configured, we can confirm that statistics collection has been set up.

### 1 -

In the **Data Collection and Analysis Management**, **Subscriptions** view, we can see that there is a subscription called LSP Egress Statistics.

The telemetry type is base/lsps/lsp-egress. The collection interval is 60 s, meaning that every minute the NSP will collect the statistics from the node.

Most importantly, database subscriptions are enabled. Data is stored in the NSP auxiliary database and is available to Analytics.

	Network Services Platform					User	admin	• ?
Data Collection and Ana	lysis Management Subscripti	ions •					+ SUBSCRIPTION (	C→ :
Telemetry Subscription	ns 👻							
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions	:
-								
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM	telemetry:/base/oampm-accounting/cfm-dmm-bin-acc-stats	300	00:00	$\checkmark$			:
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM	telemetry:/base/oampm-accounting/cfm-dmm-session-acc-stats	300	00:00	$\checkmark$			:
<ul> <li>Enabled</li> </ul>	TestSuiteEx_OAM-PM	telemetry:/base/oam-pm/eth-cfm-delay-streaming	10	00:00	$\checkmark$			:
<ul> <li>Enabled</li> </ul>	System CPU and Memory	telemetry:/base/system-info/system	10	00:00	$\checkmark$	$\checkmark$		:
Enabled	System Temperature	telemetry:/base/hardware/temperature	10	00:00	~	$\checkmark$		:
Enabled	SAP Throughput Ingress	$telemetry:/base/accounting/complete-service-ingress-packet-o\dots$	60	00:00	~	$\checkmark$		:
Enabled	SAP Throughput Egress	$telemetry:/base/accounting/complete-service-egress-packet-o\dots$	60	00:00	$\checkmark$	$\checkmark$		:
Enabled	TestSuiteEx_OAM-LO	telemetry:/base/oam-result/loopback-result	10	00:00	$\checkmark$			:
Enabled	TestSuiteEx_OAM-LIN	telemetry:/base/oam-result/link-trace-result	10	00:00	$\checkmark$			:
Enabled	LSP Egress Statistics	telemetry:/base/lsps/lsp-egress	60	00:00	$\checkmark$	$\checkmark$		:
<ul> <li>Enabled</li> </ul>	nsp-tds-netw-health	telemetry:/base/interfaces/utilization	10	00:00	$\checkmark$			:
Enabled	nsp-tds-netw-health	telemetry:/base/interfaces/interface-errors	10	00:00	$\checkmark$			:

Last Refresh: 2023-11-28 13:31:57 (Local Time)

Row Count: 12

2 -

The report we need creates forecasts based on aggregated data. Switching to the **Data Collection and Analysis Management**, **Aggregation** view, we'll take a look at the aggregation settings for the telemetry type. Select the telemetry type and click Edit.

Here we see that all aggregation types are enabled, and the retention period is set for each. The Last Success Time can also be used to verify that the subscriptions are working. For example, the last success time for daily aggregation should not be longer than a day ago.

Data Collection and Analys	is Management	Aggregation	•					G	1
Name	Туре			Hourly Enabled - Last Success	Daily Enabled - Last Success	Weekly Enabled - Last Success	Monthly Enabled - Last Success		
md-aggr:/md-aggr-ba	telemetry:/bas	e/lsps/lsp/egress/path		Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
nd-aggr:/md-aggr-ba	telemetry:/base	e/accounting/complete/service/in	gress/packet/octets	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
nd-aggr:/md-aggr-ba	telemetry:/bas	e/lsps/lsp/egress	Edit Aggregation Rule				× <sup>id, -</sup>		
nd-aggr:/md-aggr-ba	telemetry:/base	e/interfaces/interface	Name				:d, -		
md-aggr:/md-aggr-ba	telemetry:/base	e/system-info/system	md-aggr:/md-aggr-base/te	lemetry-base-lsps-lsp-egress/	'telemetry-base-lsps-lsp-egress		:d, -		
nd-aggr:/md-aggr-ba	telemetry:/bas	e/oam-pm/eth-cfm-slm-loss-ses	Туре				id, -		
md-aggr:/md-aggr-ba	telemetry:/bas	e/oampm-accounting/twl-session	telemetry:/base/lsps/lsp/e	gress			id, -		
md-aggr:/md-aggr-ba	telemetry:/base	e/oam-pm/eth-cfm-delay-session	Enable Aggregation	Retention Period		Last Success Time	łd, -		
md-aggr:/md-aggr-ba	telemetry:/base	e/oampm-accounting/cfm-dmm+	Hourly	30	days (1 - 403)	2023-11-28 12:00:00	id, -		
md-aggr:/md-aggr-ba	telemetry:/bas	a/accounting/complete/ethernet	Daily	90	days (1 - 403)	2023-11-28 00:00:00	d, -		
md-aggr:/md-aggr-ba	telemetry:/base	e/hardware/temperature	Veekly	26	weeks (1 - 52)	2023-11-26 19:00:00	:d, -		
nd-aggr:/md-aggr-ba	telemetry:/base	e/mpls-interfaces/mpls-interface	Monthly	24	months (1 - 36)		:d, -		
md-aggr:/md-aggr-ba	telemetry:/base	e/oampm-accounting/twl-bin-acc					ıd, -		
nd-aggr:/md-aggr-ba	telemetry:/base	e/interfaces/interface/errors	4 @			CANCEL	UPDATE Id, -		
nd-aggr:/md-aggr-ba	telemetry:/base	e/oampm-accounting/cfm-dmm-b	m-auc-stats	CHADIEU, 2020-11-20	CHADIEU, 2020-1 1-20	Enabled, 2020-11-20	chabled, -		
md-aggr:/md-aggr-ba	telemetry:/bas	e/accounting/complete/service/eg	gress/packet/octets	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		

3 -

We also need to confirm that the aggregation time zone has been set correctly. If the aggregation time zone doesn't match the reporting time zone, Analytics will show an error when we try to generate an aggregated report. Click on the More Actions menu at the top of the page and select **Time Zone Setting**.

The time zone has been set to local time.

	-	Hourly Enabled -	Daily Enabled - Last	Weekly Enabled -	Monthly Enabled -		
ame	Туре	Last Success	Success	Last Success	Last Success		
d-aggr:/md-aggr-ba	telemetry:/base/interf	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
l-aggr:/md-aggr-ba	telemetry:/base/lsps/l	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
l-aggr:/md-aggr-ba	telemetry:/base/syste	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
l-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
d-aggr:/md-aggr-ba	telemetry:/base/accou	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
d-aggr:/md-aggr-ba	telemetry:/base/lsps/l	Enabled, 2023-11-28	Enabled, 2023-11 Time	Zone Setting	×		
d-aggr:/md-aggr-ba	telemetry:/base/oam	Enabled, 2023-11-28		Changing the Aggregation Time Z			
d-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11	start/end time for all future daily, aggregations.	weekly and monthly		
d-aggr:/md-aggr-ba	telemetry:/base/hard	Enabled, 2023-11-28	Enabled, 2023-11 Aggre	gation Time Zone			
d-aggr:/md-aggr-ba	telemetry:/base/interf	Enabled, 2023-11-28	Enabled, 2023-11	erica/Toronto			
d-aggr:/md-aggr-ba	telemetry:/base/oam	Enabled, 2023-11-28	Enabled, 2023-11		CANCEL SAVE		
d-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11				
d-aggr:/md-aggr-ba	telemetry:/base/accou	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
nd-aggr:/md-aggr-ba	telemetry:/base/mpls	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
nd-aggr:/md-aggr-ba	telemetry:/base/accou	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
nd-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		

To generate a report using daily or monthly data, we need to ensure we have an appropriate retention policy for the telemetry type. Switching to the **Data Collection and Analysis Management**, **Age-Out Policy** view, we can see that the retention policy for the telemetry type has been set to the maximum.

NO <ia network="" platform<="" services="" td=""><td></td><td>User: admin</td><td>• ⑦</td><td></td></ia>		User: admin	• ⑦	
Data Collection and Analysis Management Age-Out Policy			с :	
Telemetry Policies 🔹				
Name	Retention (hours)			:
Isp				
telemetry:/base/accounting/combined-ldp-lsp-egress	4			/
telemetry:/base/accounting/combined-mpls-lsp-egress	4			
telemetry:/base/accounting/combined-mpls-lsp-ingress	4			
telemetry:/base/lsps/lsp-ingress	4			
telemetry:/base/lsps/lsp-egress-path	9672			
telemetry:/base/lsps/lsp-egress	9672			1

#### Last Refresh: 2023-11-28 13:34:57 (Local Time)

#### Row Count: 6

NSP

### 5.5.7 Generate the report in Analytics

Now that we've confirmed that all the prerequisites are in place, we can run the report.

1 -

In the Analytics repository, the report we need is under Reports and Dashboards, NSP, Utilization. Navigate through the folders and choose LSP Throughput with Forecast (NSP).

E NOCIA Ne	etwork Services Platform			User: admin	6	• ⑦
Data Collection and Analysis	s Visualizations Repository -				REPOSITORY TO	P :
epository						
Folders	Run Edit Open Copy Cut Paste Delete				Sort By: Name M	lodified Date
in root	Name	Description	Туре	Modified Date		
Data Domains	Interface Utilization Summary (NSP)	Summary of Utilization data of interfaces	Report	November 21		
DataSource     Images	Interface Utilization with Forecast(NSP)	Daily and monthly interface utilization with forecasting	Report	November 21		
Reports and Dashbo	LSP Throughput with Forecast (NSP)	Egress throughput details of Lsps and Daily and Monthly LSP Throughput with forecasting		November 21		
🕨 🚞 Administration	Port-LAG Details (NSP)	Total, egress and ingress throughput and utilization for a selected port or LAG or an MC-LAG	Report	November 21		
Application Ass	Port Throughput Summary (NSP)	Total, ingress and egress throughput and utilization summary for the selected ports, LAGs, MC-LAG'	Report	November 21		
Custom     Metwork and Se	Resource Group Utilization Detail with Forecast (NSP)	Throughput and utilization based on ports and lags contained in the selected resource group	Report	November 21		
NSP	Resource Group Utilization Summary (NSP)	Throughput and utilization based on ports and lags contained in the selected resource groups	Report	November 21		
Inventory	SAP Throughput (NSP)	Summary of ingress and egress throughput for selected services and SAP on a node	Report	November 21		
🕨 🚞 ОАМ	Temperature, CPU, Memory Utilization Details (NSP)	Temperature, CPU and Memory utilization details for selected NE	Report	November 21		
🕨 🚞 Utilization	Temperature, CPU, Memory Utilization Summary (NSP)	Temperature, CPU and Memory utilization summary for the selected NSP and NFMP Managed NEs	Report	November 21		
Results						

We'll start with a raw data report.

- 1. Select all the NE types.
- 2. In the NE list, choose NEs that host the service endpoints.
- 3. In the LSP field, choose the LSP between the two NEs.
- 4. Select the Show report output on one page check box.
- 5. Click Apply.

Data Collection and Analysis Visualizations Repository +					REPOSITORY TOP	:
LSP Throughput with Forecast (NSP)						
Options X 🖺 - 🖾 - 🔶 🕥		- + 100% -	search report	Q - 4 >		÷.
ame or name pattern for NE						
ε						
Available: 6 Selected: 2						
earch list Q	Ę					
suranceNFMP-1(11.11.11.17750-SR	Please apply input values to display the report.					
suranceNFMP-2(12.12.12.12:7750-SR						
sskNodeB(92.168.96.7:7750-SR12) sskNodeC(92.168.96.26:7750 SR-2s)						
sscNodeC(92.168.96.26:7750 SR-2s) NodeD(92.168.96.60:7750 SR-7s)						
INodeE(92.168.96.16:7750 SR-14s)						
Select X None 🖾 Invert						
ne or name pattern for LSP						
sp						
ssicNodeC-lsp_nodeC_to_nodeB						
sacroued-sp_noted_to_noteb						
ecast periods						
iods per Season						
o resource ID						
fault (Nokia)						
go position						
ft v						
Show report output on one page						

The report shows the raw LSP utilization data.

NOCIA Network Services Platform					User: admin	•	?
Data Collection and Analysis Visualizations Repository -						REPOSITORY TOP	
LSP Throughput with Forecast (NSP) Data refreshed 2023-11-28 at 13:40:53 Optimized 2023-11-28 at 13:40:53							
< Options X 🔛 - 🖶 - 🔶 - 🔿					- + 100% +	search report Q -	▲ →
* Name or name pattern for NE	NOCIA	LSP Throughp	ut with Forecast (NSP	)			
• NE Available: 6 Search list. AssuranceNFMP-111.1.1.1.1.17250-SR. AssuranceNFMP-2112.1.2.12.7750-SR. classer/society.108.96.2.7720-SR12 classer/society.108.96.2.7720.58.2.20 mRNodeD(92.168.96.6.7750.58.7.6) mRNodeD(92.168.96.6.7750.58.7.6) mRNodeD(92.168.96.16.7750.58.7.6) mRNodeD(92.168.96.16.7750.58.7.6)	Start date: Report date: NE (Jo (Pom): NE (Jo (Pol): LSP name: LSP type:	2023-11-28 09-61:00 EST 2023-11-28 13-40:53 EST 92.168:96:26 92.168:96:7 Isp_nodeC_to_node8 Dynemic	End date: Granularity: NE Name (Prom): NE Name (Pol: LSPID: Tannel ID:	2023-11-28 13:40:53 EST Raw Collection Interval classicNode0 ClassicNode8 3 3			
Name or name pattern for LSP	0 <sub>0 *</sub>	LSP Eg	ress Throughput				
% * LSP ClassiCNodeC-lsp_nodeC_to_node8 ▼	15 10 5d ct	A 0 - D	. 1	AN			
Forecast periods 5	5	MM	M M				
Periods per Season	0 10:30		12:00 12:30	13:00 13:30			
Logo resource ID default (Nokia)							
* Logo position Left •							
Show report output on one page Apply Reset Save							

Next, we'll re-run the report on daily aggregated data. When you run this report with daily or monthly aggregation, a forecast is provided.

We'll set the report range to 10 days, the forecast periods to 5 and the periods per season to 1.

Periods per season refers to the number of aggregations you want to track to see a repeating pattern. For example, to see a weekly pattern with daily aggregation, you would set Periods per season to 7. Setting this to one means we expect traffic to be similar from one day to the next.

To generate a forecast, you must provide at least two seasons of data, although more may be required if the input data is not linear. For example, if you choose a periods per season value of 7 and the granularity is daily, you must use a report range of at least 14 days.

4

View the report.



This report shows the 10 days of collected data and 5 days of forecasting based on that data. The blank space on the graph indicates that data hasn't been aggregated yet for the current date.

After the current date is the forecasted data. The shading shows the upper and lower range of the predicted throughput, and the line shows the expected throughput value for the next five days.

# 5.6 SAP Throughput reporting scenario

### 5.6.1 Purpose

The SAP Throughput (NSP) report shows throughput by a specified service and SAPs. The SAP Throughput (NSP) report includes throughput data for NEs managed by the NFM-P only, MDM (model-driven) only, or NFM-P+MDM-mediated NEs. The default display is a set of time series graphs, showing ingress, egress and total throughput.

This process shows how to set up a service for SAP Throughput reporting in Analytics.

### 5.6.2 Confirm that prerequisites for service provisioning are completed

1

Two intent type bundles are required for provisioning our service, and for setting up QoS and telemetry: icm-intent-types, and mdt-intents.

							IMPORT & INSTALL
Automatic reconcile of artifacts and artifact bundle	es is done every 3 mins. Next rec	concile will happen in 2 min 6 sec					
ndle Name	Bundle Version	Status	Number of Artifacts	Author	Import Time =	:	(i) Artifact Bundle Details
	T	T	т [] т				Status
nsp-telemetry-cr-va-sros-1.0.0-rel.17.zip	1.0.0	Installed	2	NOKIA R&D	2023/11/27 20:52:03	:	Installed
nsp-icm-intent-types-23.11.0-rel.505-cam.zip	23.11.0-rel.505	Installed	47	NOKIA R&D	2023/11/22 09:06:27	:	Bundle(s) Name
nsp-mdt-intents-23.11.0-rel.756-svc-assurance- bundle.zip	23.11.0	Installed	8	NOKIA R&D	2023/11/22 09:06:27		nsp-icm-intent-types-23.11.0-rel.505-cam.zip
nsp-mdt-intents-23.11.0-rel.756-svc-intent- bundle.zip	23.11.0	Installed	26	NOKIA R&D	2023/11/22 09:06:27		Author NOKIA R&D
nsp-ne-upgrade-1.4.0.zip	1.4.0	Partially Installed	20	NOKIA R&D	2023/11/21 22:27:02	1	Version 23.11.0-rel.505
nsp-ne-backup-audit-1.0.1.zip	1.0.1	Installed	2	NOKIA R&D	2023/11/21 22:26:59	1	Number of Artifacts
nsp-ne-upgrade-with-phases-1.4.0.zip	1.4.0	Installed	27	NOKIA R&D	2023/11/21 22:26:59	1	47 Import Time
nsp-ne-restore-1.2.0.zip	1.2.0	Installed	6	NOKIA R&D	2023/11/21 22:26:58	:	2023/11/22 09:06:27
nsp-ne-upgrade-eth-sat-1.3.0.zip	1.3.0	Installed	8	NOKIA R&D	2023/11/21 22:26:54	:	Additional Info N/A
nsp-ne-wavence-upgrade-1.0.0.zip	1.0.0	Installed	9	NOKIA R&D	2023/11/21 22:26:54	:	Signature
nsp-ne-backup-1.3.0.zip	1.3.0	Installed	6	NOKIA R&D	2023/11/21 22:26:53		
nsp-ne-sw-import-1.2.0.zip	1.2.0	Installed	4	NOKIA R&D	2023/11/21 22:26:53	:	
nsp-wavence-service-migration-1.0.0.zip	1.0.0	Installed	4	NOKIA R&D	2023/11/21 22:26:53	1	

### Checking the Artifacts, Artifact Bundles view shows that both bundles are in Installed status.

2

NSP installs the intent types to Network Intents, from which they can be imported to Service Management.

Checking the **Service Management**, **Intent Type Catalogue** view shows that the intent types have been imported and are available for use in Service Management.

T         T	ervice Management	Intent Type Catalogue	•						IMPORT	(
nel         2         ArtifactAdmin, ServiceFiulfill         23.11.0-rel_2.2.0         2023-11-22 13.42.36         ii           pe         2         ArtifactAdmin, ServiceFiulfill         23.11.0-rel_2.2.0         2023-11-22 13.42.36         ii           n         2         ArtifactAdmin, ServiceFiulfill         23.11.0-rel_2.2.0         2023-11-22 13.42.36         ii           a         2         ArtifactAdmin, ServiceFiulfill         23.11.0-rel_2.2.0         2023-11-22 13.42.36         ii           a         2         ArtifactAdmin, ServiceFiulfill         23.11.0-rel_2.2.0         2023-11-22 13.42.36         ii	tent Type	Intent Type Version		Labels	Build	Last Updated Time	:	(i) Info		
nel       2       ArtifactAdmin, ServiceFulfill       23.11.0-rel_2.2.0       2023-11-22 13.42.36       :         pe       2       ArtifactAdmin, ServiceFulfill       23.11.0-rel_2.2.0       2023-11-22 13.42.36       :         n       2       ArtifactAdmin, ServiceFulfill       23.11.0-rel_2.2.0       2023-11-22 13.42.36       :         s       2       ArtifactAdmin, ServiceFulfill       23.11.0-rel_2.2.0       2023-11-22 13.42.36       :		T	т	T		Т	T	Select an intent type		
n         2         ArtifactAdmin, ServiceFulfill         23.11.0-rel_2.2.0         2023-11-22 13:42:36         :           s         2         ArtifactAdmin, ServiceFulfill         23.11.0-rel_2.2.0         2023-11-22 13:42:36         :	nnel		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
s 2 ArtifactMdmin, ServiceFulfill 23.11.0-rel_2.2.0 2023-11-22.13/42:36	ipe		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
	rn		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
2 ArtifactAdmin, ServiceFuldHL 23.110-rel_2.2.0 2023-11-2213-42.36 *	ls		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			
	\$		2	ArtifactAdmin, ServiceFulfill	23.11.0-rel_2.2.0	2023-11-22 13:42:36	:			

Switching to the **Service Management**, **Service Templates** view shows that the intent types have been used to create templates for various service types.

NSP

ervice Management Ser	vice Tem	iplates -										+ CREATE	(
mplate Name		Description								nfig Form			
		Jescription		Intent Type		Intent Version		State		nng rorm	-	i Info	
	T		T		T		Ŧ					Select a service template	
be		Default Epipe template		epipe			2	Released		fault	-		
n		Default VPRN template		vprn			2	Released	de	fault	:		
5	E	Default VPLS template		vpls			2	Released	de	fault	1		
	(	Default IES template		ies			2	Released	de	Fault	- 1		

## 5.6.3 Verify policy configuration

1

To collect statistics on an NE, a file and accounting policy must be configured on the NE. This can be done by deploying a template in the **Device Management**, **Configuration Deployments** view.

In the Configuration Deployments list, we can see that a template called File and Accounting has been deployed on the NE and the Deployment Status is Deployed Aligned. The policy identifier is 20.

Dev	ice Management Configuration	on Deployments 🔹								+ DEPLOYMENT
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	:	(i) Deployment Details
		-	Т	T	T	T	Logical -			NE Name
ו	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	20	File and Accounting	Logical	Log	:	classicNodeC
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	20	File and Accounting	Logical	Log	:	92.168.96.26
1	Deployed Aligned	Modified	classicNodeC	92.168.96.26	20	File and Accounting	Logical	Log	:	Identifier
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	20	File and Accounting	Logical	Log	:	Accounting Policy ID 20
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	Ingress99#99	SAP Ingress QoS	Logical	QoS	:	
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	Ingress99#99	SAP Ingress QoS	Logical	QoS	:	Deployment Status Deployed Aligned
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Ingress99#99	SAP Ingress QoS	Logical	QoS	:	and the second s
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Ingress99#99	SAP Ingress QoS	Logical	QoS	:	AUDIT ALIGN
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	Egress99#99	SAP Egress QoS	Logical	QoS	:	Last Audit
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	Egress99#99	SAP Egress QoS	Logical	QoS	:	Nov 27, 2023 8:16:01 pm by admin
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Egress99#99	SAP Egress QoS	Logical	QoS	:	VIEW RESULT
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Egress99#99	SAP Egress QoS	Logical	QoS	:	Last Alignment Nov 27, 2023 8:21:54 pm by admin
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	66	Custom File and Accou	Logical	Log	:	Template Name File and Accounting
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	66	Custom File and Accou	Logical	Log	:	Created
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	66	Custom File and Accou	Logical	Log	:	Nov 27, 2023 7:49:44 pm
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	66	Custom File and Accou	Logical	Log	:	Nov 27, 2023 8:21:54 pm
									4.2	Role Logical Category log Configuration Status Modified

We can view the template details to see policy details:

- 1. Select the deployment and choose View/Edit from the Table row actions menu.
- 2. In the form that opens, click VIEW/EDIT TEMPLATE CONFIG.

The template information shows the rollover duration, or how long a statistics collection file remains open before a new file is started, the retention period for the file, and the compact flash location where the file is stored.

Accounting policy details show that the policy applied is number 20, and it will be collecting Complete Service Ingress Egress statistics. The collection interval is 5 min, meaning that every 5 min the NSP will collect the statistics from the node and save them to the database.

= N	OKIA Network Services Platform				User: admin	• ⑦
Deploy Log	ical Configuration					×
Select Tem;	File and Accounting				>	<
Select Targe Assign Ident	Log File	Log				Î
	Compact Flash Location Accounting Policy	File				
		File Id"	File Policy Name*	Description		
		20 Rollover (minutes)	File Policy 20 Retention (hours)	Migration File Policy 20		-
		15	4			punt : 1
		Compact Flash Location Primary cf3: • □2				CONFIG
		Accounting Policy				
		Accounting Policy Name Accounting Policy 20	Admin State	Description Migration Accounting Policy 20		
		Record	Collection Interval (minutes)	Ex Migration Accounting Policy 20		punt:1
		Complete Service Ingress Egress 👻 🗖	5			bunt: (
					CANCEL UPDAT	
	1. File	and Accounting :				
					CANCE	L DEPLOY

Additionally, there are egress and ingress QoS policies deployed, which allows traffic shaping and to prioritize certain types of traffic.

The ingress QoS policy identifier is Ingress99#99.

	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	i Deployment Details	
		-	T	T	τ	T	Logical -		NE Name	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	20	File and Accounting	Logical	Log	classicNodeC	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	20	File and Accounting	Logical	Log	92.168.96.26	
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	20	File and Accounting	Logical	Log	Identifier	
ו	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	20	File and Accounting	Logical	Log	SAP Ingress Policy Name Ingress99	
ו	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	Ingress99#99	SAP Ingress QoS	Logical	QoS	SAP Ingress Policy ID	
ו	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	Ingress99#99	SAP Ingress QoS	Logical	QoS	:	
1	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Ingress99#99	SAP Ingress QoS	Logical	QoS	E Deployment Status	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Ingress99#99	SAP Ingress QoS	Logical	QoS	Deployed Aligned	
ו	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	Egress99#99	SAP Egress QoS	Logical	QoS	AUDIT ALIGN	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	Egress99#99	SAP Egress QoS	Logical	QoS	:	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Egress99#99	SAP Egress QoS	Logical	QoS	Nov 27, 2023 9:37:00 pm by admin	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	Egress99#99	SAP Egress QoS	Logical	QoS	VIEW RESULT	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	66	Custom File and Accou	Logical	Log	Last Alignment	
כ	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	66	Custom File and Accou	Logical	Log	Nov 27, 2023 9:38:56 pm by admin Template Name	
3	Deployed Aligned	• Modified	classicNodeC	92.168.96.26	66	Custom File and Accou	Logical	Log	SAP Ingress QoS	
]	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeB	92.168.96.7	66	Custom File and Accou	Logical	Log	Nov 27, 2023 9:36:52 pm	
	4							Þ. 4	Last Updated Nov 27, 2023 9:38:56 pm Role Logical Category QoS	

We'll view the ingress template details as an example:

- 1. Select the deployment and choose View/Edit from the Table row actions menu.
- 2. In the form that opens, click VIEW/EDIT TEMPLATE CONFIG.

There are a total of nine queues configured. The three that display on this page have been configured as expedited queues with high priority. At the bottom of the form, we can see two of the forwarding classes.

= N	OCIA Network Services Platform						User: admin	• ⑦
Deploy Log	gical Configuration							×
Select Tem;	SAP Ingress QoS							×
Select Targe	SAP Ingress	SAP Ingress						Î
Assign ident		Description		Default FC		Default Priority		
		Ingress QoS 99		be	• 🗔	low	• Ex	
		Queue					+ ADD	1
		Queue ID	Queue Type	Queue Mode				
								punt : 1
		8	expedited	priority			:	
		7	expedited	priority			1	
		6	expedited	priority			:	CONFIG
				< < Page: 1 / 3 > >			Total: 9	
		FC					+ ADD	
		FC Name	Profile	Queue				
								punt : 1
		af	none	3			:	
		12	none	2			:	-
							CANCEL	UPDATE
	1. SAP	Ingress QoS :						_
								CANCEL DEPLOY

Policers have also been applied directly to the NEs.

### 5.6.4 Verify the service parameters

1

In the Service Management, Services view, we can see the provisioned services.

ervice Management Services	<del>.</del>					+ CREATE C
e Cycle State	Alignment State Composite Service	e Service Name	Description	Service Template	:	(i) Info
•		T	T	T	T	States
Unknown	Unknown	NewTestEpipe	abcd		: ^	
Unknown	Unknown	NewerEPipe			:	Life Cycle State
Unknown	Unknown	Rmtest			:	<ul> <li>Deployed Nov 27, 2023, 10:06:50 PM EST</li> </ul>
Deployed	⊘ Aligned	AnooptestEpipe	abcdef	epipe	:	Alignment State
Deployed	⊘ Aligned	Anooptest02		epipe	:	⊘ Aighed
Deployed	Aligned	Marc Epipe 1		epipe	:	
Deployed	Aligned	DemoEpipe		epipe		General Info
Deployed	Aligned	EPIPE 5	N/A	epipe		Service ID
Deployed	Aligned	EPIPE 3	Default Eline Template	epipe	1	DemoEpipe
Deployed	O Aligned	Marc_epipe_10	test	epipe	:	NE Service ID
Unknown	Unknown	VPLS 6001	N/A			999
Unknown	Unknown	VPLS 5005	Vpls-5005		:	Service Name DemoEpipe
Unknown	Unknown	VPLS 5006	Vpls-5006		1	Description
Unknown	Unknown	Vpls-6002			:	a care prove
Unknown	Unknown	IES 6006	les-6006			Service Type
Unknown	Unknown	IES 5201	les-5201		:	ELINE
Unknown	Unknown	les-5200	les-5200		:	Customer ID
Unknown	Unknown	les-6005			:	30
12.7		100.00	100			Service Manager ID

#### 2 -

DemoEpipe is Deployed and Aligned.

Opening the Edit form for the service will let us verify that everything we'll need is in place. Select the service and select Edit from the Table Row actions menu.

rvice Management Services							+ CREATE	G	
Cycle State	Alignment State Composite Servic	e Service Name	Description	Service Templa	ate :	() Info			
*	•	T	T	T	۲.	States			
Unknown	Unknown	NewTestEpipe	abcd		1 (	•			
Unknown	Unknown	NewerEPipe			:	Life Cycle State			
Unknown	Unknown	Rmtest			:	Deployed	Nov 27, 2023, 10:00	5:50 PM E	ST
Deployed	O Aligned	AnooptestEpipe	abcdef	epipe	:	Alignment State			
Deployed	⊘ Aligned	Anooptest02		epipe	:	Viighed			
Deployed	Aligned	Marc Epipe 1		epipe	:				
Deployed	⊘ Aligned	DemoEpipe		epipe	:	General Info			
Deployed	⊘ Aligned	EPIPE 5	N/A	eplp Action Edit		Service ID			
Deployed	Aligned	EPIPE 3	Default Eline Template	epip Clone		DemoEpipe			
Deployed	Aligned	Marc_epipe_10	test	epip View Se	rvice Definition	NE Service ID			
Unknown	Unknown	VPLS 6001	N/A	Audit co		999			
Unknown	Unknown	VPLS 5005	Vpls-5005	Align	riste ·	Service Name DemoEpipe			
Unknown	Unknown	VPLS 5006	Vpls-5006	Migrate		Description			
Unknown	Unknown	Vpls-6002		Resync		Description			
Unknown	Unknown	IES 6006	les-6006		workflow	Service Type			
Unknown	Unknown	IES 5201	les-5201	Remove	2	ELINE			
Unknown	Unknown	les-5200	les-5200	View Service	details >	Customer ID			
Unknown	Unknown	les-6005		Open in	Object Troubleshooting	30			
n 1		170.40	100			Service Manager ID			

3 -

The Edit service form shows the basic service parameters such as service name and customer ID, and the service endpoints.

≡ NO <ia netwo<="" th=""><th>ork Services Platform</th><th></th><th></th><th></th><th></th><th></th><th>User: admin</th><th>- ?</th></ia>	ork Services Platform						User: admin	- ?
Edit Service: DemoEpipe								
Site A	Template Name 0		Current Life Cycle State		Alignment State			i
Site B	epipe		Deployed		Aligned			
SDP Details	Service Name*		NE Service ID*		мти			
	DemoEpipe		999		1492			
	Customer ID*		Description		Admin State			
	30	0			unlocked	* Cx		
	Job ID							
	Site A							
	Device ID		Site Name		Description			
	92.168.96.7	× 0						
	мти							
	Endpoint					+ ADD		
	Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State	Description		
	Port 1/1/8	dot1q	-1	999	unlocked	:		
				_		• • •		
				-		1 3 1	Reserve Resources CLOSE	

Site A of the service is on port 1/1/8. Select the endpoint and choose Edit to verify the endpoint parameters.

In the Edit Endpoint form, we can see that accounting statistics collection and QoS have been enabled, and the policies and overrides that have been applied. The accounting policy is 20, and the SAP Ingress policy is Ingress99: the policies we verified in the device management views.

■ NO <ia network<="" p=""></ia>	Services Platform				User: admin 👻
ervice > Edit Endpoint 1					
PU Protection	Port ID		Encap Type	Outer VLAN Tag	
gress	Port 1/1/8	0	dot1q	999	
QoS	Admin State		Description		
SAP Ingress	unlocked -	□_x		Collect Accounting Statistics	
Overrides	Accounting Policy		Multi Service Site		
Policer Control Policy	20 ×	0			
Overrides					
Root Priority Mbs Thresholds	CPU Protection				
Scheduler Policy Overrides	Policy ID				
Aggregate Policer ress	✓ Enable QoS		Enable IP/IPv6 Filter		
QoS SAP Egress	Ingress				
Overrides					
Policer Control Policy	QoS				
Overrides	Match QinQ Dot1p				
Root	Select Item -	-			
Priority Mbs Thresholds					
Scheduler Policy					
Overrides Vlan Qos Policy	SAP Ingress				
vian Qos Policy Egress Remark Policy	Queuing Type		Policy Name		
Egrees wernand offer	Select Item	• 🖂	Ingress99		
					CANCEL UPD

Scroll down to see the egress settings: the egress policy is Egress99.

5 -

Set E de day of the financial de la	
liger	
QG       SAF Inges       QC       QC Indicator Data       Pace Control Roles       QC Indicator Data       Pace Roles       And Roles Control Roles       QC Indicator Data       Pace Roles	
g8 Ingrest     Q0       indexide     indexides (Dolly)       indexides     indexides (Dolly)	
Note: Costal Policy   Overrides   Roit   Policy Name   Safe Transmission   Safe Transmission <tr< td=""><td></td></tr<>	
SAP Egress       Rot     Policy Mans       scheduler Policy     Egress99       Outrides     Outrides       Sape Gas     Queue D       Sape Gas     Queue D       Outrides     Policy Mans       Sape Gas     Mass       Outrides     Policy Mass       Sape Gas     Queue D     CBS       Outrides     Pilcy Mass       Outrides     Pilcy Mass Threadout       Scheduler Policy     No data to display	
Nointy Miss Threeholds   solution Services   Solution Service	
Subscience       Overrides       segregate Rollicar       Segregate Rollicar       Segregate Rollicar       Segregate Rollicar       Segregate Rollicar       Subscience Rollicar       Overrides       Gegregate Rollicar       Segregate Rollicar	
Age spect holic     Current description       test     Test       point     Test       point des     Test       point des     Test       point des Threadoits     Test       stabedur Polity     Test	
Basi on the second sec	
open        4 DD        SAP Egress        (	
Overrides     Queue ID     CBS     MBS     PIR (kbps)     CIR (kbps)       Overrides     Image: Control Palicy     Image: Control Palicy     Image: Control Palicy       Root:     Image: Control Palicy     Image: Control Palicy       PIR (kbps)     CIR (kbps)     CIR (kbps)       Root:     Image: Control Palicy       PIR (kbps)     CIR (kbps)       State (kbps)     CIR (kbps)	
Queue ID     CS     MBS     PIR (lubps)     CIR (lubps)       Overrides     Image: Control Mail Control	
Overrides     Image: Comparison of the c	
Priority Mbs Thresholds Scheduler Policy	
Scheduler Policy	
Overrides         I         Page:         0         /0         >1         Total: 0	
Egress Remark Policy	
Policer + ADD	
Policer ID CBS MBS Stat Mode	
	CANCEL UI
	Contract 0
	entral 0

Returning to the Edit Service form, we can see the SDP details, the service destination points. An SDP has been added to the service for each direction.

NSP

SDP Details	Source Device ID 92.168.96.7 92.168.96.26	Destination Device           ID           92.168.96.26           92.168.96.7	Steering Parameter	SDP ID 90 90	+ ADD Description : : :		
Admin State	92.168.96.7	D 92.168.96.26 92.168.96.7		90	Description		
unlocked	92.168.96.7	D 92.168.96.26 92.168.96.7		90			
unlocked		92.168.96.7			I		
unlocked		92.168.96.7	<i>I</i> 1 → 51		I		
	52.100.50.20		ZT Σ SL	50			
		< < Page: 1	/1 > >		► 4 F		
		< < Page: 1	/ T - > - >				
					Total: 2		

## 5.6.5 Verify statistics collection configuration

Now that we have verified that the service is configured, we can confirm that statistics collection has been set up.

1

For the report we need to generate, we need to collect statistics for two telemetry types: base/ accounting/complete-service-ingress-packet-octets and base/accounting/complete-serviceegress-packet-octets.

In the **Data Collection and Analysis Management**, **Subscriptions** view, we see that subscriptions have been configured and enabled for each. The collection interval is 60 s, meaning the data will be collected by NSP every minute.

Database subscriptions are enabled: this will make the historical data available to Analytics.

	Network Services Platform					User: admin	- ?
Data Collection and An	nalysis Management Subscript	ions 👻				+ su	
Telemetry Subscription	ons 🔹						
State	Name	Telemetry Type	Collection Interval (seconds)	Sync-time (UTC)	Notification Subscriptions	DB Subscriptions	File Subscriptions
	•						
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-PM	telemetry:/base/oampm-accounting/cfm-dmm-bin-acc-stats	300	00:00	$\checkmark$		:
Enabled	TestSuiteEx_OAM-PM	telemetry:/base/oampm-accounting/cfm-dmm-session-acc-stats	300	00:00	$\checkmark$		:
Enabled	TestSuiteEx_OAM-PM	telemetry:/base/oam-pm/eth-cfm-delay-streaming	10	00:00	$\checkmark$		:
Enabled	System CPU and Memory	telemetry:/base/system-info/system	10	00:00	$\checkmark$	$\checkmark$	:
Enabled	System Temperature	telemetry:/base/hardware/temperature	10	00:00	$\checkmark$	$\checkmark$	:
Enabled	SAP Throughput Ingress	telemetry:/base/accounting/complete-service-ingress-packet-octets	60	00:00	$\checkmark$	$\checkmark$	:
Enabled	SAP Throughput Egress	telemetry:/base/accounting/complete-service-egress-packet-octets	60	00:00	$\checkmark$	$\checkmark$	:
Enabled	TestSuiteExOAM-LO	telemetry:/base/oam-result/loopback-result	10	00:00	~		:
<ul> <li>Enabled</li> </ul>	TestSuiteExOAM-LIN	telemetry:/base/oam-result/link-trace-result	10	00:00	~		:
<ul> <li>Enabled</li> </ul>	LSP Egress Statistics	telemetry:/base/lsps/lsp-egress	60	00:00	~	$\checkmark$	:

Last Refresh: 2023-11-28 10:50:42 (Local Time)

2

The report we need also reports based on aggregated data. Switching to the **Data Collection and Analysis Management**, **Aggregation** view, we'll take a look at the aggregation settings for the telemetry types.

Here we see that all aggregation types are enabled for the telemetry types of interest. The Last Success Time can also be used to verify that the subscriptions are working. For example, the last success time for daily aggregation should not be longer than a day ago.

NSP

Aggregation       Type       Hourly Enabled - Last       Weekly Enabled - Last       Weekly Enabled - Last       Monthy Enabled - Last       Success       Last	tion and Analysis Management Aggregation -						
iype     Last Success     Success     Last Success     Last Success       md-agg-base/complete-service-egress-packet-octets/complete-service-ingress-packet-octets/complete-service-service-ingress-packet-octets/comple							C+
md-aggr-base/complete-service-egress-packet-octets/complete-service-ingress-packet-octets telemetry/base/accou Enabled, 2023-11-29 Enabled, 2023-11-29 Enabled, 2023-11-29 Enabled, 2023-11-26 Enabled, 2023-11-26		Туре	Hourly Enabled - Last Success		Weekly Enabled - Last Success		
		×					
md-aggr-base/complete-service-egress-packet-octets/complete-s	nd-aggr-base/complete-service-egress-packet-octets/complete-service-ingress-packet-octets	telemetry:/base/accou	Enabled, 2023-11-29	Enabled, 2023-11-29	Enabled, 2023-11-26	Enabled, -	
	nd-aggr-base/complete-service-egress-packet-octets/complete-service-egress-packet-octets	telemetry:/base/accou	Enabled, 2023-11-29	Enabled, 2023-11-29	Enabled, 2023-11-26	Enabled, -	

Row Count: 2

3 –

Last Refresh: 2023-11-29 19:28:41 (Local Time) Aggregation Time Zone: America

We also need to confirm that the aggregation time zone has been set correctly. If the aggregation time zone doesn't match the reporting time zone, Analytics will show an error when we try to generate an aggregated report. Click on the More menu at the top of the page and select **Time Zone Setting**.

The time zone has been set to local time.

ata Collection and Analys	s Management Aggreg	gation 👻				G	
ame	Туре	Hourly Enabled - Last Success	Daily Enabled - Last Success	Weekly Enabled - Last Success	Monthly Enabled - Last Success		
d-aggr:/md-aggr-ba	telemetry:/base/interf	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
d-aggr:/md-aggr-ba	telemetry:/base/lsps/l		Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
l-aggr:/md-aggr-ba	telemetry:/base/syste	. Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
d-aggr:/md-aggr-ba	telemetry:/base/oamp.	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
d-aggr:/md-aggr-ba	telemetry:/base/accou.	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
l-aggr:/md-aggr-ba	telemetry:/base/lsps/l	Enabled, 2023-11-28	Enabled, 2023-11 Time	Zone Setting	×		
l-aggr:/md-aggr-ba	telemetry:/base/oam	. Enabled, 2023-11-28	Enabled, 2023-11	hanging the Aggregation Time Z	Cone, will change the		
-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28		tart/end time for all future daily, ggregations.	, weekly and monthly		
-aggr:/md-aggr-ba	telemetry:/base/hard	Enabled, 2023-11-28	Enabled, 2023-11 Aggreg	ation Time Zone			
-aggr:/md-aggr-ba	telemetry:/base/interf	Enabled, 2023-11-28	Enabled, 2023-11	rica/Toronto			
-aggr:/md-aggr-ba	telemetry:/base/oam	. Enabled, 2023-11-28	Enabled, 2023-11		CANCEL SAVE		
-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11		CANCEL SAVE		
-aggr:/md-aggr-ba	telemetry:/base/accou.	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
-aggr:/md-aggr-ba	telemetry:/base/mpls	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
-aggr:/md-aggr-ba	telemetry:/base/accou.	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		
-aggr:/md-aggr-ba	telemetry:/base/oamp	Enabled, 2023-11-28	Enabled, 2023-11-28	Enabled, 2023-11-26	Enabled, -		

To generate a report using daily or monthly data, we need to ensure we have an appropriate retention policy for the telemetry type. Switching to the Age-Out Policy list, we can see that the retention policy for the telemetry types have been set to the maximum.

NOCIA     Network Services Platform			User: admin	÷	?
Data Collection and Analysis Management Age-Out Policy	•			G	:
Telemetry Policies					
Name		Retention (hours)			:
complete-service	×				
		9672			
telemetry:/base/accounting/complete-service-ingress-packet-octets		2072			

Last Refresh: 2023-11-28 10:52:52 (Local Time)

### 5.6.6 Generate the report in Analytics

Now that we've confirmed that all the prerequisites are in place, we can run the report.

1 -

In the Analytics repository, the report we need is under Reports and Dashboards, NSP, Utilization. Navigate through the folders and choose SAP Throughput (NSP).

Row Count: 2

	etwork Services Platform			User: admin	•	?
Data Collection and Analysis	s Visualizations Repository -				REPOSITORY TOP	:
epository						
Folders	Run Edit Open Copy Cut Paste Delete				Sort By: Name Mo	odified Date
Toot	Name	Description	Туре	Modified Date		
Data Domains	Interface Utilization Summary (NSP)	Summary of Utilization data of interfaces	Report	November 21		
DataSource     Images	Interface Utilization with Forecast(NSP)	Daily and monthly interface utilization with forecasting	Report	November 21		
Reports and Dashbo	LSP Throughput with Forecast (NSP)	Egress throughput details of Lsps and Daily and Monthly LSP Throughput with forecasting	Report	November 21		
Administration	Port-LAG Details (NSP)	Total, egress and ingress throughput and utilization for a selected port or LAG or an MC-LAG	Report	November 21		
Application Ass	Port Throughput Summary (NSP)	Total, ingress and egress throughput and utilization summary for the selected ports, LAGs, MC-LAG'	Report	November 21		
Custom     Metwork and Se	Resource Group Utilization Detail with Forecast (NSP)	Throughput and utilization based on ports and lags contained in the selected resource group	Report	November 21		
<ul> <li>NSP</li> </ul>	Resource Group Utilization Summary (NSP)	Throughput and utilization based on ports and lags contained in the selected resource groups	Report	November 21		
Inventory	SAP Throughput (NSP)	Summary of ingress and egress throughput for selected services and SAP on a node		November 21		
🕨 🚞 ОАМ	Temperature, CPU, Memory Utilization Details (NSP)	Temperature, CPU and Memory utilization details for selected NE	Report	November 21		
Utilization	Temperature, CPU, Memory Utilization Summary (NSP)	Temperature, CPU and Memory utilization summary for the selected NSP and NFMP Managed NEs	Report	November 21		

#### 2 -

We'll start with a raw data report.

- 1. Select all the NE types.
- 2. In the NE list, choose NEs that host the service endpoints.
- 3. Choose a customer, a service, and one or more SAPs.
- 4. Select the Show report output on one page check box.
- 5. Click Apply.

The report shows the raw SAP utilization data.





Next, we'll re-run the report with a threshold. A threshold helps to visualize whether traffic is exceeding expected values.

For example, we'll set an egress threshold of 2 000 kbps.

The report shows the threshold level on the graphs. If the average throughput rate exceeds the threshold, the table shows the values in red.



# 5.7 End-to-end NE troubleshooting scenario

## 5.7.1 Purpose

This process shows you how to use NSP in troubleshooting issues on NEs.

In this scenario, an NE is experiencing problems.

### 5.7.2 View affected equipment related resources

1

The **Equipment Health** dashlet in the **Network Map and Health** dashboard uses KPIs to show NE states.

The **Affected NEs** KPI indicates that there are NEs to look at to start investigating. Click the **Affected NEs** circle to launch the **Network Elements** data page.

work Map and Health	Overview	÷							E	
Network Health Vie Determine the overall h	<b>W</b> lealth of your network usin	ng the metrics below								
<b>uipment Health</b> e status of all network eler	nents		ervice Health e status of all network	services	Last Hour 🔹	Service Configuration Health The configuration status of all net		Alarm Summary Unacknowledged root cause alarms	Last Hou	ur •
0%- Peor Network Health	Es Affected Unre	0- eachable NEs	13- Healthy Services	13. Affected Services	0. Degraded Services	26 Total Services	9 Misaligned Services	32: Critical Major Minor	0. TCAs	)
					View in Service	Management	View in Current Alarr	ns		
which network objects as By Service Sites	e affecting services By Service Endpoints	By Tunnel Bind	dings				Last Hour 👻	News Feed View unacknowledged root cause alarms as T Alarms • = By Impact •	they occur	:
which network objects a		• By Tunnel Bind	dings				Last Hour •	View unacknowledged root cause alarms as	they occur 21 seconds ago	:
which network objects an By Service Sites		By Tunnel Bind	lings				Last Hour • :	View unacknowledged root cause alarms as Alarms  F By Impact TunnelDown from-92.168.96.26-id-5		
which network objects and By Service Sites •		By Tunnel Binc	lings				Last Hour • :	View unacknowledged root cause alarms as Alarms • = By Impact • TunnelDown from-92.168.96.26-Id-5 Impact: 3 SdpBindingDown crout-3-6003	21 seconds ago	:
12 12 6		By Tunnel Binc	lings				Last Hour • :	View unacknowledged root cause alarms as View unacknowledged root cause alarms as TunnelDown from 92:168.96.26-id-5 Impact: 3 SdpBindingDown drout-3-3322	21 seconds ago 5 days ago	:

The **Network Elements** data page appears, filtered to show the list of NEs with at least one affected object. The default filter can be changed if needed, for example, to focus on NEs with more affected objects. We'll focus on the Affected Objects column for the NE we're troubleshooting.

Select the NE and click (Table row actions), View in Current Alarms.

NSP
NOKIA	Network Services Platfo	rm													Us	er: admin		•	- (
twork Map and	Health Overview	-																	
etwork Eleme	5/4 120																		:
Content upd	lated on 2023/11/6 11:07:59 (Click Operational State	k to update) # Affected Objects	1	System Address		Management Address		Product	Chassis Type		Version		Commun	cation State	Man	aged State		Administrat	tiv
τ.	-	> 0	× T.		۲.		Τ.	τ.		<b>T</b> _		τ.	up						
ndNodeE	enabled		44	92.168.96.16		135.121.152.20		7750 SR	7750 SR-14s		TIMOS-C-2		up		man	aged		unlocked	
assicNo	enabled		18	92.168.96.7		192.168.96.33		7750 SR	7750-SR12		TiMOS-B-2		up		mar	aged		unlocked	
dNodeD	enabled		8	92.168.96.60		135.121.157.2		7750 SR	7750 SR-7s		TiMOS-C-2		up		mar	aged		unlocked	
ssicNo	enabled		6	92.168.96.26		192.168.97.146		7750 SR	7750 SR-2s		TiMOS-C-2		up		ma	Ø View i	n Current	Alarms	
																	n Object ' in NE Ses tatistics	st	
rvice Sites		и <sup>2</sup>	Lin	ks			к <sup>7</sup>	Ports					ĸ'n	Services					,
ime	Operational	State	Nai	ne		Operational State		Name		Ope	erational State			Name		OF	perational S	State	
ipe-6004	disabled		md	NodeE:1/1/c1/1mdN.		disabled		Port 1/4/5		disa	abled		î	Epipe-5002		dis	sabled		
ipe-5001	disabled		md	NodeE:1/1/c1/10md.		disabled		1/2/c12		disa	abled			ELINE_Demo	>	dis	sabled		
-5201	disabled		cla	ssicNodeB:1/1/1class.		enabled		1/1/c27		disa	abled			EPIPE 6004		dis	sabled	(	1

**Current Alarms** opens, showing a filtered list of alarms. Click on an alarm to see information in the **Details** panel, or use (Table row actions) menu to show impacts, root cause, or open NE CLI session.

letwork Map and H	lealth > Netw 92.1	work Element 168.96.60 (mdNodeD) Current Alarms	÷						Ģ
<b>1</b> .							G	Details	
everity	Impact	Last Time Detected	Alarmed Object Type	Alarmed Object Name		Alarm Name	~	General	
- T,	Τ.	ҮҮҮҮ-ММ-D - ҮҮҮҮ-ММ-D 🛅	Τ.		Τ.				
	0	2023/11/7 06:01:05 PM GMT+05:00	equipment.NetworkElement	92.168.96.60		TelemetryCollect	~	Severity	
)	0	2023/11/7 06:00:58 PM GMT+05:00	equipment.NetworkElement	mdNodeD		TelemetryCollect	~	Acknowledgement	
	0	2023/11/7 06:00:58 PM GMT+05:00	equipment.NetworkElement	mdNodeD		TelemetryCollect		J.	
	0	2023/11/7 03:33:59 PM GMT+05:00	necontrol.DiscoveredNe	mdNodeD		NodeConfiguratio	~	Acknowledgement Notes	
	0	2023/11/6 07:35:30 PM GMT+05:00	equipment.Equipment	port=1/1/c1/10		LinkDown		Challen Line	
	0	2023/11/6 03:55:11 PM GMT+05:00	equipment.Equipment	port=1/1/c1/1		LinkDown	~	Statistics	
	0	2023/09/20 04:13:12 PM GMT+04:00	equipment.Equipment	port=1/1/c1/7		LinkDown	~	Description	
	0	2023/09/20 04:11:42 PM GMT+04:00	equipment.Equipment	power-shelf=1		TmnxPowerShelf			
<b>-</b>						initial official contents of			
·							^	Remedial Action	
							^	Remedial Action	
							~	Remedial Action	
<b>D</b>							~	Raising Condition	

#### 5.7.3 View the News Feed

The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to Current Alarms.

#### 1 -

From the **News Feed**, select an alarm affecting the node. Click **View in Current Alarms** from the More menu.

rork Map and Health Ov	verview -					₽
Network Health View Determine the overall healt	th of your network using the metrics b	elow				
<b>ipment Health</b> status of all network elemen	Last 24 Hours 👻	Service Health The status of all network services	Last Hour +	Service Configuration Health The configuration status of all network services	Alarm Summary Unacknowledged root cause alar	ms Last Hour
0%- Poor Network Health	5. O. Affected Unreachable NEs NEs	13. Healthy Services Services	0- Degraded Services	26 9 Total Misaligned Services Services	Z6A Critical Major	514 Q. Minor TCAs
				View in Service Management	View in Cur	rent Alarms
					view in cur	
which network objects are af By Service Sites • By	fecting services Service Endpoints • By Tunn	el Bindings		Last Hour •	: News Feed View unacknowledged root Cau Y Alarms - F By classichodeB Impact. 0	View In Current Alarms View Impacts View Root Causes View Object Impacts
which network objects are af By Service Sites • By		el Bindings			: News Feed View unacknowledged root cau	View In Current Alarms View Impacts View Root Causes
which network objects are af By Service Sites • By		el Bindings			News Feed           View unacknowledged root cau           Y Alarma - F By           classicNodeB           Impact: 0           LinkDown           interfaceL3int           impact: 0	View In Current Alarms View Impacts View Root Causes View Object Impacts Open in Network Inventory View in Object Troubleshooting Plot utilization statistics
14 12 10 8		el Bindings			News Feed View unacknowledged root cau     Y Alarms      F By     classichodeB     Impact: 0     LinkDown     interface+L3int     Impact: 0     LinkDown     portr1/1/c1/10	View in Current Alarms View Impacts View Root Causes View Object Impacts Open in Network Inventory View in Object Troubleshooting Plot utilization statistics Plot error statistics

Current Alarms provides details of the alarm, such as the alarm description, raising and clearing conditions, and remedial action.

	Network Service	es Platform						User: admin 👻
etwork Map and	Health > 92.	work Element 168.96.60 (mdNodeD) Current Alarms	-					C.
, +							() <b>E</b>	Details
everity	Impact	Last Time Detected	Alarmed Object Type	Alarmed Object Name		Alarm Name	~ G	eneral
т Т,	Τ,	YYYY-MM-D - YYYY-MM-D 🖬	Τ,		Τ.			
	0	2023/11/7 06:07:55 PM GMT+05:00	equipment.NetworkElement	92.168.96.60		TelemetryCollect	∨ S	everity
	0	2023/11/7 06:05:59 PM GMT+05:00	equipment.NetworkElement	mdNodeD		TelemetryCollect	~ A	cknowledgement
	0	2023/11/7 06:05:59 PM GMT+05:00	equipment.NetworkElement	mdNodeD		TelemetryCollect		
)	0	2023/11/7 03:33:59 PM GMT+05:00	necontrol.DiscoveredNe	mdNodeD		NodeConfiguratik	~ A	cknowledgement Notes
	0	2023/11/6 07:35:30 PM GMT+05:00	equipment.Equipment	port=1/1/c1/10		LinkDown	~ s	tatistics
	0	2023/11/6 03:55:11 PM GMT+05:00	equipment.Equipment	port=1/1/c1/1		LinkDown	× 3	
	0	2023/09/20 04:13:12 PM GMT+04:00 2023/09/20 04:11:42 PM GMT+04:00	equipment.Equipment	port=1/1/c1/7 power-shelf=1		LinkDown TmnxPowerShelf	~ D	escription
							to ent prese oper-	larm is generated when the SNMP entity, acting in an agent role, etected that port used for one of its communication links is abou- ter the down state from some other state (but not from the not- nt state). This other state is indicated by the included value of if- status leaf
							^ R	emedial Action
							is no i	admin state is 'down' then the interface state is deliberate and t recovery. If the admin state is 'up' then try to determine the cau terface going down: cable cut, distal end went down, etc.
							~ R	aising Condition
							~ c	learing Condition
							~ A	dditional Text
Þ						► < ►	~ c	ustom Text
Auto-refres						Row Count: 8		

3 -

Another option is to note the NE name and switch to the **Unhealthy NEs** or **Top Problems** view, to see what other alarms are present on the NE and what other issues the NE is experiencing.

## 5.7.4 View the Network Map and Health dashboard map view

Another option on the **Network Map and Health** dashboard is the **Network Map View**. Viewing the NE in the map will show us the status of links, in case there are any port issues affecting connectivity.

1 -

Navigate back to the **Network Elements** data page. Click on the NE and choose **Plot statistics**.

etwork Map and Hea	ilth	Overview	·																	
etwork Element	5																			:
Content updated	l on 2023/	11/7 13:53:11 (Click to update)																		
ame 🗠		Operational State	# Affected O	bjects		System Address		Management Address		Product		Chassis Type		Version	(	Communication State		Managed State		
	Τ.	•	> 0	×	₹.		Τ.		Τ.		Τ.		<b>T</b> _+		<b>T</b> .	up			•	
ssicNodeB		enabled			18	92.168.96.7		192.168.96.33		7750 SR		7750-SR12		TiMOS-B-2		qu		managed		
issicNodeC		enabled			6	92.168,96.26		192.168.97.146		7750 SR		7750 SR-2s		TiMOS-C-2		qu		managed		
dNodeD		enabled			7	92.168.96.60		135.121.157.2		7750 SR		7750 SR-7s		TIMOS-C-2		qu		managed		
dNodeE		enabled			44	92.168.96.16		135.121.152.20		7750 SR		7750 SR-14s		TIMOS-C-2		μp		View in Current		
r-nrc		enabled			1	92.168.99.227		192.168.96.155		7750 SR		VSR-I		TIMOS-B-2		μp		Show in networ Open in Netwo		
																		View in Object '		
																		Open in NE Ses		
																	0	Plot statistics		
																		Add to Watchlis	t	
			к <sup>л</sup>	Links				× ×	Port	s				κ <sup>π</sup>		Services				ĸ
rvice Sites									Nam			Operationa	Stat	e		Name		Operational S	tate	
		Operational State		Name		c	peration	al State	Nam									•		
me		Operational State	Î		:1/1/c1		<b>peration</b> lisabled	al State		1/4/5		disabled			î	Epipe-5002		disabled		
ime Ipe-6004			Î	mdNodeE		/1mdN c		al State		1/4/5		disabled disabled				Epipe-5002 EPIPE 6004		disabled disabled		
lame ipipe-6004 ipipe-5001 es-5201		disabled	Î	mdNodeE mdNodeE	1/1/c1	/1mdN c	lisabled	al State	Port	1/4/5 :12										4

**Data Collection and Analysis Visualizations** launches, showing on-demand charts for memory and CPU usage for the NE.



Back in the **Network Elements** data page, click on the NE and select **Show in network map** to open the **Network Map View** with the NE highlighted.

NSP



View the Multi-layer map to see the state of the links at the IGP layer.



Return to the Operational map and enable **Utilization** to show utilization statistics displayed on the map.



Right click on the node and select View in Object Troubleshooting.



## 5.7.5 Check the Object Troubleshooting dashboard

1

Viewing a target in the Object Troubleshooting dashboard can help you see where to look to investigate a problem. The dashboard shows summary information for the NE, and provides a health and an alarm summary.

From the **Object Troubleshooting**, we can click **View in Current Alarms** to view alarms and impacts, or run **Analytics Reports**.

Product:     If Journal     Administrative state:     Glicked     Critical     Major     TCAs     Total Impacts       Location:     N/A     Availability State:     N/A     Critical     Major     TCAs     Total Impacts     Port Inventory     Port Inventory       Open in NE Inventory     View in Current Alarms     Temperature CPU Memory Utilization Summary     Port Inventory										
We traubleatooding summary unformation for the selected NE   System Address: 22,188,96,60   Management Address: 155,121,157,2   Analysic Test: Communication State:   Operational State: Unicode dotted   Analysic Test: Communication State:   Operational State: Unicode dotted   Communication State: Unicode dotted   Analysic Test: Communication State:   Operational State: Unicode dotted   Analysic Test: Unicode dotted   Communication State: Unicode dotted   Marketed Alle: #Affected LAGS:   #Affected Components: 6 (13%)   #Affected LaGS: 1 (10%)   #Affected Components: 5 (71%)   #Affected Components: 0 (0%)   #Affected Components: 5 (71%)   #Affected Components: 0 (0%)   #Affected Components: 0 (0%)   Toproversite	oject Troubleshooting > Network Ele mdNodeD	Troubleshootin	g 👻					CHANGE TARGET	Ð	
ummary information for the selected NE Prediati status for the selected NE   System Address: 92.168.96.60   Management Address: 135.121.157.2   Product: 7750 SR   Administrative State: unulocedo   Verified Communication State: 2 (100%)   Verified Communication State: 1 (20%)   Verified Communication State: 2 (100%)   Verified Communication State: 1 (20%)   Verified Communication State: 2 (100%)   Verified Communication State: 2 (100%)   Verified Communication State: 2 (100%)   Verified Communication State: 2 (100%) <th>Troubleshooting Summary Board View troubleshooting summary inform</th> <th>ation</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th>	Troubleshooting Summary Board View troubleshooting summary inform	ation								
Product: 133.121.137.2     Product: 7750 SR     Location: N/A     Mangament Address: 133.121.73.2     Communication State: up     Administrative State: 000     Open in NE Inventory     Open in NE Inventory     Open in NE Inventory     Open in NE Inventory     Teal     Address: 6 (35%) # Affected LAGs: 2 (100%)     # Affected Components: 6 (35%) # Affected LAGs: 2 (100%)     # Affected Components: 0     # Affected Components: 0     # Affected LAGs: 1 (20%)     # Affected LAGs: 1 (20%)     # Affected LAGs: 1 (20%)     # Affected Cards: 5 (71%)     # Affected Cards: 5 (71%)     # Affected Cards: 5 (71%)     # Affected Lags     Tou, Nov 23, 1607-00EST     #										
Maniageinen Address: 100x F1702xE   Product: 77503R   Administrative State: unlocked   Administrative State: unlocked   Control Open in NE Inventory     View in Current Alarms     EKPIs   protrati KPis for the selected NE:   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected LAGs:   2 (100%)   # Affected Components:   6 (35%)   # Affected Components:   6 (35%)   # Affected Components:   6 (35%)   # Affected Ports:   0 (0%)      Thu, Nev 23, 1607-00 EST Components:	System Address:	92.168.96.60	Operational State:	enabled				Inventory Reports		
Product:: 7750 5R Administrative State:: unlocked   Location:: N/A Availability State:: N/A   Resync State:: done   Open in NE Inventory View in Current Alarms <b>E KPIs</b> moortant KPIs for the selected NE: # Affected Components:: 6 (35%) # Affected Links: 1 (20%) # Affected Cards:: 5 (71%) # Affected NE: * Affected Ports:: 0 (0%) Thu, Nov 23, 1607:00 EST C Nu 122 State Updates 71 Thu Zamma Thu 200 C Thu 20	Management Address:	135.121.157.2	Communication State:	up				Card Inventory	•	4
Location: NA   Resync State: done   Open in NE Inventory View in Current Alarms     IE KPIs   morant KPis for the selected NE:   # Affected Components:   6 (35%)   # Affected LaGs:   2 (100%)   # Affected Cards:   5   # Affected Links:   1 (20%)   Thus, Nov 23, 16:07:00 EST Carmet    All   1422   State Updates   71   Thus Roy 2 Thus Ro	Product:	7750 SR	Administrative State:	unlocked	0	2 0	•	Port Details	•	•
Resync State: done   Open in NE Inventory View in Current Alarms     View in Current Alarms     Important Respects   # Affected Components: 6 (35%)   # Affected LAGs: 2 (100%)   # Affected Components: 6 (35%)   # Affected Links: 1 (20%)   # Affected Cards: 5 (71%)   # Affected Cards: 5 (71%)   # Affected Cards: 5 (71%)   Thu. Nov 23, 16.07.00.EST    All 142   State Updates 71   Charms 0	Location:	N/A	Availability State:	N/A	Critical	Major TCAs		Port Inventory	•	
Open in NE Inventory     View in Current Alarms     Temperature CPU Memory Utilization Summary       IE KPIs inportant KPis for the selected NE.     # Affected LAGs:     2 (100%)       # Affected Components:     6 (35%)     # Affected LAGs:     2 (100%)       # Affected Cards:     5     # Affected Links:     1 (20%)       # Unacknowledged Critical Alarms:     0       # Affected Cards:     5 (71%)       # Affected Ports:     0 (0%)			Resync State:	done			impacts	Utilization Reports		
EKPS   mportant KPis for the selected NE:   # Affected Components:   6 (35%)   # Affected LoGs:   2 (100%)   # Alarms:   5   # Affected Links:   1 (20%)   # Unacknowledged Critical Alarms:   0   # Affected Cards:   5 (71%)   # Affected Ports:   0 (0%)   Thu, Nov 23, 16:07:00 EST    1   1   14   1422   State Updates   711   TC Alarms			Open in NE Invento	ry		View in Current Alarm	s		•	►
portant KPis for the selected NE # Affected Components: 6 (35%) # Affected LAGs: 2 (100%) # Alarms: 5 # Affected Links: 1 (20%) # Unacknowledged Critical Alarms: 0 # Affected Cards: 5 (71%) # Affected Ports: 0 (0%) Went Timeline Summary tetrork event timing for the selected NE.								Temperature CPU Memory Utilization Details	•	•
Marketed Components: 6 (35%)   # Affected Longs: 2 (100%)   # Affected Components: 5   # Affected Links: 1 (20%)   # Unacknowledged Critical Alarms: 0   # Affected Cards: 5 (71%)   # Affected Ports: 0 (0%)								OAM Reports		
# Alarms: 5 # Affected Links: 1 (20%)   # Unacknowledged Critical Alarms: 0   # Affected Cards: 5 (71%)   # Affected Ports: 0 (0%)	mportant KPIs for the selected NE									Þ
# Unacknowledged Critical Alarms:     0       # Affected Cards:     5 (71%)       # Affected Ports:     0 (0%)	# Affected Components:	6 (35%)	# Affected LAGs:	2 (100%)				OAM-PM Loss	•	•
# Unacknowledged Critical Alarms: 0   # Affected Cards: 5 (71%)   # Affected Ports: 0 (0%)     Chu, Nov 23, 16:07:00 EST      NI 1422   State Updates 711   TC Alarms 0	# Alarms:	5	# Affected Links:	1 (20%)				OAM DM Notwork Site Summony		
# Affected Ports: 0 (0%)  went Timeline Summary etwork event timing for the selected NE UI 1422 State Updates 711 TC Alarms 0	# Unacknowledged Critical Alarms:	0								
Vent Timeline Summary etwork event timing for the selected NE Thu, Nov 23, 16-07-00 EST	# Affected Cards:							OAM-PM Network Summary		Þ
etwork event timing for the selected NE TILU, NOV 23, TeX/JSU EST	# Affected Ports:	0 (0%)								
			Thu, Nov	23, 16:07:00 EST 📑						
Configurations 711 Alarms 0 OAM Tests 0	ul 1422	State Updates	711 TC Alarms	0						
	Configurations 711	Alarms	0 OAM Tests	0						



In the **Object Troubleshooting** map, we can change the **Hop Count** to see nodes that are further from the target and enable **Utilization**.

NSP

Network troubleshooting using NSP functions Troubleshooting using NSP assurance functions End-to-end NE troubleshooting scenario



NOKIA Network Services Platform	User: admin	•
t Troubleshooting > Network Element mdNodeD Troubleshooting -	CHANGE TARGET 臣員	Ð
todeD	View Operational	-
ation Hop Count abbled • 3 •		
sabled		(
abled		1
<b>D</b> .		
mgkoop		
The second se		
classificate		
3		
CassiChode®		
1		

3 -

In the **Object Troubleshooting** dashboard, the **Event Timeline** dashlet show today's events summary. Click **View in Event Timeline** to launch the full view.

Location: N/A Availability State: N/A Reynd State: done Open in HE Inventory EKPIs sportant KPIs for the selected NE # Affected Components: 6 (35%) # Affected Links: 2 (100%) # Alarms: 5 # Affected Links: 1 (20%) # Alarms: 5 # Affected Links: 1 (20%) # Affected Critical Alarms: 0 # Affected Critical Alar						
coldulor: invasion in years   Regind: invasion in years   Begind: invasion in years   Construction: invasion in years   # Affected Components: 0 (35%)   # Affected Condoc invasion:   # Invasion: invasion:	bject Troubleshooting > Network Ele mdNodeD	Troubleshooting	s •			CHANGE TARGET
# Alarms: 5 # Affected Links: 1 (20%)   # Unacknowledged Critical Alarms: 0   # Affected Cards: 5 (71%)   # Affected Ports: 0 (0%)     * et Timeline Summary   etwork event timing for the selected NE     al   1425   State Updates   712   Alarms   1500     * etwork event timing for the selected NE     al   1425   State Updates   712   Alarms   1500     * etwork event timing for the selected NE     al   1425   State Updates   712   Alarms   1500     * etwork event timing for the selected NE     * etwork event timing for the selected NE     al   1425   State Updates   712   Alarms   1500   1500     * etwork event timing for the selected NE     * etwork event timeline <td< th=""><th>E KPIs E KPIs for the selected NE # Affected Components:</th><th></th><th>Resync State: Open in NE Inv</th><th>done</th><th>Impacts</th><th>Utilization Reports Temperature CPU Memory Utilization Summan Temperature CPU Memory Utilization Details OAM Reports OAM-PM Latency</th></td<>	E KPIs E KPIs for the selected NE # Affected Components:		Resync State: Open in NE Inv	done	Impacts	Utilization Reports Temperature CPU Memory Utilization Summan Temperature CPU Memory Utilization Details OAM Reports OAM-PM Latency
twork event timing for the selected NE TIM, two ZS, fiel results T II 1425 State Updates 712 TC Alarms 0 onfigurations 712 Alarms 1 OAM Tests 0 v 2023 23 Nov 2023 24 Nov 2023 occoord View in Event Timeline two the transmission of the transm	# Alarms: # Unacknowledged Critical Alarms: # Affected Cards:	0 5 (71%)				OAM-PM Network Site Summary
ANDED View in Event Timeline						
Operational	Network event timing for the selected NE	State Updates		_		
	Configurations 712	Alarms 23 Nov 2 16:00	712 TC Alan 1 OAM Te 00	ms 0 ests 0 24 Nov 2023 04.000.000		
	All 1425 Configurations 712 New 2028	Alarms 23 Nov 2 16:00	712 TC Alan 1 OAM Te 00	ms 0 ests 0 24 Nov 2023 04.000.000		

In the **Object Troubleshooting** dashboard, click **CHANGE TARGET** to troubleshoot other NEs or other types of objects.

4

Object Troubleshooting > Network Element	Troubleshootin								CHANGE TARGET	E.
oject iroubleshooting > mdNodeD		8 *							CHANGE TARGET	C a
Location:	N/A	Availability State:		N/A	Critical	Major T	CAs Total Impacts	Port Inventory	(	
		Resync State:		done				Utilization Reports		
		Ope	n in NE Inventory			View in Current A	larms	Temperature 0	CPU Memory Utilization	Jummary
								Temperature 0	CPU Memory Utilization	Details
NE KPIs mportant KPIs for the selected NE								OAM Reports		
								OAM-PM Later	ncy	
# Affected Components:	6 (35%)	# Affected LAGs:		2 (100%)				OAM-PM Loss		
# Alarms:	5	# Affected Links:		1 (20%)				OAM-PM Netw	vork Site Summary	
# Unacknowledged Critical Alarms:	0							OAM-PM Netw	ork Summary	
# Affected Cards: # Affected Ports:	5 (71%) 0 (0%)								100 BEEFE 101 BEEFE 1	
Event Timeline Summary Network event timing for the selected NE			Thu, Nov 23,	16:23:00 EST 🛅						
All 1425	State Updates	712	TC Alarms	0						
Configurations 712	Alarms	1	OAM Tests	0						
Nov 2023 4:00:00	23 Nov 2 16:00	00	1.7.15.1.15.15.15	24 Nov 2023 04:00:00						
	View in Ever	nt Timeline								
mdNodeD									View	
Utilization Hop Count										
Disabled - 1 -										

In the **Object Troubleshooting** dashboard, click **Add to Watchlist** in the More menu.

Adding the NE to a watchlist will allow you to navigate quickly to the NE in the future. To open the watchlist, click Watchlist (IP).

NSP

oject Troubleshooting > Network E mdNodel	Troubleshootin	g -			CHANGE TARGET	9
Troubleshooting Summary Board View troubleshooting summary inform	<b>1</b> nation	Current Health Summary		Alarm Summary	Analytics Reports	Edit dashboard Open in NE Sess Plot statistics Add to Watchlis
Winnay information for the selected NE System Address: Management Address: Product: Location:	92.168.96.60 135.121.157.2 7750.SR N/A	Operational State: Operational State: Communication State: Administrative State: Availability State: Resync State: Open in NE Inventory	enabled up unlocked N/A done	Alarms and impacts for the selected NE	0 Total	Þ Þ ary
IE KPIs mortant KPIs for the selected NE # Affected Components: # Jaarms: # Unacknowledged Critical Alarms: # Affected Cards: # Affected Ports:	6 (35%) 5 0 5 (71%) 0 (0%)	# Affected LAGs: # Affected Links:	2 (100%) 1 (20%)		Temperature CPU Memory Utilization Details OAM Reports OAM-PM Latency OAM-PM Loss OAM-PM Network Site Summary OAM-PM Network Summary	
vent Timeline Summary etwork event timing for the selected NE All 1425 Configurations 712	State Updates Alarms	Thu, Nov 23           712         TC Alarms           1         OAM Tests	8, 16:23:00 EST 📑			

## 5.7.6 Check configuration alignment and operation history in the NE Inventory

1

From the **Current Health Summary** dashlet, click **Open in Network Inventory** to launch equipment inventory.

■ NOKIA Network Services Platform		User: admin	-	0
NE Inventory mdNodeD				G
Equipment type filters • T <sub>e</sub> Any of:	*	0	ê =	
Operational State: All + Administrative State: All + APPLY FILTERS		Select an item to see the det	ails	
mdNodeD (7750 SR-7s), Operational State: enabled, Administrative State: unlocked	÷ į			
Bi Equipment Group				
Shelf-1, Operational State: enabled, Administrative State: unlocked				
Card Slot-2[unassigned] (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked				
Card-2(unassigned), Operational State: disabled, Administrative State: unlocked				
Card Slot-3 (unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked				
Card-3(unassigned), Operational State: disabled, Administrative State: unlocked				
Card Slot-4/unassigned) (notExpectedNotInstalled), Operational State: disabled, Administrative State: unlocked				
Card-4lunassigned), Operational State: disabled, Administrative State: unlocked				
Card Slot-5(unassigned) (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked				
Card-5(unassigned), Operational State: disabled, Administrative State: unlocked				
Card Slot-6funassigned] (notExpectedNotinstalled), Operational State: disabled, Administrative State: unlocked				
Card-6funassigned), Operational State: disabled, Administrative State: unlocked	:			
- 🖲 Logical Group				
	*			
Auto-refresh     Last Refresh: 2023/11/23 16:27:59	A Back to top			
WUVTETERSII LESK RETEXIL 2023/11/23 10.21.33				

2 -

In the **Device Management**, **Managed Network Elements** view, select the NE and click (Table row actions), **View operation history**.

evice Management M	lanaged Network Elements 👻											
achability	NE Name	Ņ	Management IP		NE ID		Product		Chassis		Software Version	: 0 8
	•	Ŧ		T		T		Ŧ		T		∧ Summary
Reachable	classicNodeB	4	135.121.153.11		92.168.96.7		7750 SR		7750 SR-12		TIMOS-B-21,5.R2	1
Reachable	mdNodeD	1	135.121.157.2		92.168.96.60		7750 SR		7750 SR-7s		TIMOS-C-22.10.R6	ME Name mdNodeD
Reachable	mdNodeE	1	135.121.152.20		92.168.96.16		7750 SR		7750 SR-14s		1 Open NE Inventory	Management IP 135.121.157.2
Reachable	classicNodeC	1	135.121.151.102		92.168.96.26		7750 SR		7750 SR-2s		View applicable adaptors	5 NEID
											View operation history	92.168.96.60 NE Type
												SR-7750
											Create an operation	NE Version     22.10.R6
											Resync	Vender Nokia
											Unmanage	Product
												7750 SR Chassis
												7750 SR-7s
												Software Version TIMOS-C-22.10.R6
												Resync Status done
												Last Manual Resync
												2023/11/22 10:07:59 451 (Local time) Resync Duration (ms)
												7357
												Discovered 2023/11/22 10:00:34 202 (Local time)
												Discovery Rule ID 24253
												Discovery Rule Name
												sros_discovery_rule

From the history list, we can see when the most recent successful backup was performed, and see if any recent operations have failed.

3

To restore from a backup, select a successful backup and choose (Table row actions), **Restore**. The restore operation is launched.

rice Management > Man	lodeD Operation History	· •					
Displaying files in Device Manag	ement storage, view older bad	kup files. To compare backup	files, choose two successful backu	IDS.			
pletion Date =	Category	Operation Type	Operation Name	Duration	Status	Trigger	
/////////////////////////////							
3/11/23 16:32:28	backup	nsp-ne-backup	mdNodeD_17007751	20s 169ms	Success	admin	
							Restore
							View files
							Open in Work
📄 Auto-refresh 🥶 Last Re	fresh: 2023/11/23 16:32:47						Row

Go to **Configuration Deployments** view in **Device Management** and check for misaligned objects on the affected NE by running an **AUDIT** on deployments related to that NE.

	NO <ia netwo<="" th=""><th>JIK SE</th><th>rvices Platform</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>User: admin 👻</th><th></th></ia>	JIK SE	rvices Platform										User: admin 👻	
Dev	rice Management Conf	gurati	on Deployments 🔹 👻										+ DEPLOYMENT (	Э
	Deployment Status		Configuration Status	NE Name		NE ID		Identifier	Template	Role	Category	:	(i) Deployment Details	
		•			Ŧ		т	т	Т	•			NE Name	
]	Deployed Aligned		<ul> <li>Modified</li> </ul>	mdNodeE		92.168.96.16		1/1/c1/9	ICM Ethernet	Physical	Port	:	mdNodeD	
I	Deployed Aligned		<ul> <li>Modified</li> </ul>	mdNodeD		92.168.96.60		1/1/c1/9	ICM Ethernet	Physical	Port	:	92.168.96.60	
]	Deployed Aligned		<ul> <li>Modified</li> </ul>	mdNodeE		92.168.96.16		1/1/c1/1	ICM Ethernet	Physical	Port	:	Identifier	
1	<ul> <li>Deployed Aligned</li> </ul>		Modified	mdNodeD		92.168.96.60		1/1/c1/1	ICM Ethernet	Physical	Port	:	Port-ID 1/1/c1/1	
												<u>&gt;</u>	- Liss Alignment Nov 23, 2023 4:51:04 pm by admin Templete Name LOK Ethernet Created Nov 23, 2023 4:43:22 pm Last Ugdsted Nov 23, 2023 4:43:22 pm Last Ugdsted Nov 23, 2023 4:51:04 pm Rele Physical Cetegory port Configuration Status © Modified	
												< ▶		

The audit results show the misaligned attributes.

Deployment Status       NEI Name       NEI D       identifier       Template       Rele       Cutegy:       Image: Cutegy: Cutegy:       Image: Cutegy: Cutegy: <t< th=""><th>Dev</th><th>ice Management Configurati</th><th>ion Deployments 👻</th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th></th><th>+ DEPLOYMENT C</th></t<>	Dev	ice Management Configurati	ion Deployments 👻									+ DEPLOYMENT C
Deployed Algred       motiode       52.169.95.16       1/1/c1/9       Liot Ethernet       Physical       Port       E       S2.169.95.0       1/1/c1/9         Deployed Algred       Modified       motiodeD       52.169.95.0       1/1/c1/9       Liot Ethernet       Physical       Port       E       S2.169.95.0       1/1/c1/9         Deployed Algred       Modified       motiodeD       52.169.95.0       1/1/c1/1       Liot Ethernet       Physical       Port       E       S2.169.95.0       1/1/c1/1         Deployed Missigned       Modified       motiodeD       92.168.95.00       1/1/c1/1       ICM Ethernet       Physical       Port       E       Firstignet       Firstigne		Deployment Status	Configuration Status	NE Name		NE ID	Identifier	Template	Role	Category	y :	(i) Deployment Details
Capacity et aligned     Control of Modified     Modi					T	Т	T	T	•			
• Decloyed Algued       • Modified       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       2         • Deployed Mitaligned       • Modified       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       2         • Deployed Mitaligned       • Modified       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       1         • Deployed Mitaligned       • Modified       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       • I         • Deployed Mitaligned       • Modified       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       • I         • Physical       mdNodeD       92.168.96.60       1/1/c1/1       ICM Ethernet       Physical       • Port       • I		<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	mdNodeE		92.168.96.16	1/1/c1/9	ICM Ethernet	Physical	Port	:	
• Modified       • Modified <td></td> <td>Deployed Aligned</td> <td><ul> <li>Modified</li> </ul></td> <td>mdNodeD</td> <td></td> <td>92.168.96.60</td> <td>1/1/c1/9</td> <td>ICM Ethernet</td> <td>Physical</td> <td>Port</td> <td>:</td> <td>92.168.96.60</td>		Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD		92.168.96.60	1/1/c1/9	ICM Ethernet	Physical	Port	:	92.168.96.60
● Deployed Misaligned       ● Modified       92.168.95.60       1/1/1/11       ICM Ethernet       Physical       Port       1/1/1         ● Deployed Misaligned       ■ Modified       92.168.95.60       1/1/1/11       ICM Ethernet       ● Deployed Misaligned       ■ I/1/2/11         ● Deployed Misaligned       ■ Modified       ■ Modified       ■ Modified       ■ I/1/2/11       ■ I/1/2/11         ■ Deployed Misaligned       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ Modified       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11         ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11       ■ I/1/2/11		<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	mdNodeE		92.168.96.16	1/1/c1/1	ICM Ethernet	Physical	Port	:	
E Deployed Misaligned LOD LOD LOD Lot Auti Lot Auti Lot Auti Lot Auti Lot 23, 2023 4:56:54 pm by admin Lot 23, 2023 4:51:04 pm by admin Template Name Lot 20, 2023 4:51:04 pm by admin Template Name Lot 20, 2023 4:51:04 pm Nov 23, 2023 4:51:04 pm Lot 20, 2023 4:51:04 pm Nov 23, 2023 4:51:04 pm Lot 20, 2024		<ul> <li>Deployed Misaligned</li> </ul>	<ul> <li>Modified</li> </ul>	mdNodeD		92.168.96.60	1/1/c1/1	ICM Ethernet	Physical	Port	:	
		(						•		,	٠.	VIEW RESULT Last Alignment Nov 23, 2023 4:51:04 pm by admin Template Name LOM Ethernet Created Nov 23, 2023 4:43:02 pm Last Updated Nov 23, 2023 4:51:04 pm Role Physical Chappy port Configuration Status

Click VIEW RESULT in the Deployment Details panel.

evice Management Configuration	on Deployments 🔹							+ DEPLOYMENT
Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category :	(i) Deployment Details
•			T	T	T	T -		NE Name
Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	1/1/c1/9	ICM Ethernet	Physical	Port	mdNodeD
Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	1/1/c1/9	ICM Ethernet	Physical	Port	92.168.96.60
Deployed Aligned	Modified	mdNodeE	92.168.96.16	1/1/c1/1	ICM Ethernet	Physical	Port	Identifier
Deployed Misaligned	<ul> <li>Modified</li> </ul>	mdNodeD	92.168.96.60	1/1/c1/1	ICM Ethernet	Physical	Port :	Port-ID 1/1/c1/1
							¢	<ul> <li>Nov 23, 2023 4:56:54 pm by admin</li> <li>VIEW RESULT</li> <li>Last Alignment</li> <li>Nov 23, 2023 4:51:04 pm by admin</li> <li>Template Name</li> <li>ICM Ethernet</li> <li>Created</li> <li>Nov 23, 2023 4:51:04 pm</li> <li>Last Uplated</li> <li>Nov 23, 2023 4:51:04 pm</li> <li>Rele</li> <li>Physical</li> <li>Creasery</li> <li>port</li> </ul>

The results open. Click ALIGN ALL CONFIG to fix the misalignment.

KOKIA Network Services Platform			User: admin	• ③
Audit Result from Nov 23, 2023 4:56:54 pm				С×
MISALIGNED ATTRIBUTES MISALIGNED OBJECTS				
Attribute	Expected Value (Template)	Actual Value (NE)		
/configure/port=1/1/c1/1/admin-state	enable	disable		

# 5.8 End-to-end service troubleshooting scenario

#### 5.8.1 Purpose

This process shows you how to troubleshoot issues on services. In this scenario, a service is experiencing problems.

#### 5.8.2 View service health summary

1

The Service Health dashlet in the Network Health dashboard uses KPIs to show service states. The Affected Services KPI indicates that there are several unhealthy services in the network.

The Service Configuration Health dashlet indicates that three of the services are misaligned from the templates used to create them.

CANCEL ALIGN ALL C

The status of all network services The configuration services The configuration status of all network services The configuration status of all network services The configuration services The configuration services The configuration services The configuration services The configurat	work Map and Health Over	view -				E=																	
e status of all network elements Litt Not   The status of all network services <ul> <li>Described Services</li> <li>By Service Sites</li> <li>B</li></ul>	Network Health View Determine the overall health	of your network using the metrics I	below																				
Corr       Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr       Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr       Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr       Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr       Corr       Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th></th>	Corr< <th>Corr       Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th></th>	Corr       Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th></th>	Corr< <th>Corr&lt;<th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th></th>	Corr< <th>Corr&lt;<th>Co</th><th></th><th>Last Hour 💌</th><th></th><th>Last Hour 👻</th><th></th><th></th></th>	Corr< <th>Co</th> <th></th> <th>Last Hour 💌</th> <th></th> <th>Last Hour 👻</th> <th></th> <th></th>	Co		Last Hour 💌		Last Hour 👻		
Acted Services       Last Hour       I       News Feed         We unacknowledged root cause alarms as they occur       Image box region regi	Poor Network Healthy NEs	Affected Unreachable	Healthy Affected	Degraded	Total Misaligned																		
Wein network objects are affecting services     List Hour     :     Wein unacknowledged root cause alarms as they occur       By Service Sites     By Service Endpoints     By Tunnel Bindings     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     SendNotification     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     SendNotification     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       10     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       11     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       12     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       13     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites       14     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites     Image: Discrete Sites </td <td></td> <td></td> <td></td> <td></td> <td>View in Service Management</td> <td>View in Current Alarms</td>					View in Service Management	View in Current Alarms																	
12     Image biological station       12     Image biological station       10     Image biological station       10     Image biological station       11     Image biological station       12     Image biological station       13     Image biological station       14     Image biological station       15     Image biological station       16     Image biological station       17     Image biological station       18     Image biological station       19     Image biological station       10     Image biological station       10     Image biological station       10     Image biological station       11     Image biological station       12     Image biological station       13     Image biological station       14     Image biological station       15     Image biological station       16     Image biological station       17     Image biological station       18     Image biological station       17     Image biological station       17     Image biological station       18     Image biological station       17     Image biological station       18     Image biological station       17     Image biolog					Last Mour.	News Feed																	
a     Impact: 0     1 second a       a     a     a       a     a     a       a     a     a       b     a     b       c     a     a       a     b     a       b     a     b       c     a     b       c     b     a       c     a     b       c     b     a       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     b     b       c     c     c	-		nel Bindings		Lastinui	View unacknowledged root cause alarms as they occur																	
6 SendNotification 1 minute a Impact: 0 SendNotification 2 SendNotification 1 minute a	By Service Sites • By Service Sites		nel Bindings			View unacknowledged root cause alarms as they occur View unacknowledged root cause alarms as they occur Alarms  Fig By Time Reported  SendNotification Regiborr92.168.96.7 0 seconds ago																	
SendNotification	By Service Sites • By Service Si		nel Bindings			View unacknowledged root cause alarms as they occur Alarms  F By Time Reported  SendNotification meighborr92.168.96.7 0 seconds ago SendNotification neighborr92.168.96.26 1 second ago																	
2 Impact 0	By Service Sites • By Service Si		nel Bindings			View unacknowledged root cause alarms as they occur View unacknowledged root cause alarms as they occur Values and the second																	

Click on the Misaligned Services circle.

The Service Management, Services view opens, filtered to show the misaligned services.

iervice Management Services	÷							C+	
fe Cycle State	Alignment State	Composite Service	Service Name	Description	Service Template	:	(i) Info		
	Misaligned 🗸		T	T	T	т	Select a service		
Deployed	() Misaligned		Marc Epipe 1		epipe	1	Select a sel vice		
Deployed-Modified	() Misaligned		VPRN 5101	Vprn-5101	vprn	:			
Deployed	() Misaligned		Anooptestvprn		vprn	:			

Returning to the Network Map and Health dashboard, click on the Affected Services circle.

The Services data page appears, filtered to show the list of services with at least one affected object. The default filter can be changed if needed, for example, to focus on services with more affected objects. From the Services data page, we can see that the Operational State of our service of interest is disabled.

Let's open the object troubleshooting dashboard to get more details. Select the affected service and choose (Table row actions), **View in Object Troubleshooting**.

etwork Map and Health	Overview		•												e	
Services																:
Content updated on 202	23/11/25 11:08:15 (Click	to update)														
Name	Operational S	ate	# Affected O	bjects	Degrade	d Status	Life Cycle State	Alignment State	Service Type		Description	) (	Customer ID		State Cause(s)	:
	T		> 0	×	T					•		۲		т		
PIPE 6003	disabled				ŧ		Unknown	Unknown	E-Line		N/A		30		sdpBindingDown, s	
EPIPE 2121	disabled			1	3		Unknown	Unknown	E-Line		N/A		100			
/PLS 5005	enabled			1	3		Unknown	Unknown	E-LAN		Vpls-5005		10		sdpBindingDown	
ES 5201	disabled			-	2		Unknown	Unknown	IES		les-5201		20		siteDown	
es-6005	disabled			1	2		Unknown	Unknown	IES				Customer30			
EPIPE 3322	disabled			1	2		Unknown	Unknown	E-Line		N/A		100		sdpBindingDown, s	
Marc_epipe_100	disabled			1	2		Deployed	Misaligned	E-Line				Demo			:
PIPE 12345	disabled			1	2		Unknown	Unknown	E-Line		N/A		99 0	View in	Current Alarms	
PIPE 5001	enabled			3	2 degrade	d	Unknown	Unknown	E-Line		Epipe-5001		10		Object Troublesho	
DIDE 4402	31.201.3				,		Halizania	Octores	P.11-2		e				Service Managem Watchlist	ent
Network Elements			e" Lin	ks			* <sup>2</sup>	Ports			х <sup>л</sup>					
lame	Operational	State	Nar	ne		Operational St	tate	Name	Operational State							
ndNodeE	enabled		md	NodeE:1/1/o	:1/8mdN	disabled	î	Port B/1	disabled		î					
lassicNodeB	enabled		md	NodeE:1/1/c	1/1mdN	enabled		1/1/c12	disabled							
ndNodeD	enabled		md	NodeE:1/1/c	:1/9mdN	enabled		Port 1/1/c10	disabled							
classicNodeC	enabled		md	NodeD:1/1/	:1/2class	enabled		Port 1/1/7	disabled							( î

The Object Troubleshooting dashboard opens, filtered to show the service we're investigating.

## 5.8.3 Explore the Object Troubleshooting dashboard

1 -

Let's take a look at the Troubleshooting Summary Board. The Service Overview and Current Health Summary dashlets show similar information to what we saw in the Network Health dashboard: The dashboard also includes health summaries for the sites, endpoints, and tunnel bindings. Here we can see that there is a problem with one site and one endpoint. The tunnel bindings look healthy.

ect Troubleshooting > Service Marc_epipe_100 Troubleshooting	eshooting •			CHANGE TARGET	<b>1</b> 19	
Troubleshooting Summary Board View troubleshooting summary information						
rvice Overview mmary information for the selected service	Current Health Summary Health status for the selected service	Sites Health Summary Service sites operational statistics		Endpoints Health Summary Service endpoints operational statistic	īš	
Customer Name: Dei						
Service Type: E-L		2 50%	0	2 50%	0	
Number of Sites:	2 Alignment State: Misaligned Operational State: disabled	Sites Sites Down	TCAs	Endpoints Endpoints	TCAs	
	State Cause: N/A			Down		
View in Service Management						
nnel Bindings Health Summary rvice tunnel bindings operational statistics	Alarm Summary Alarms and impacts for the selected service	Analytics Reports Run Analytics Reports Service				
2 0% 0 Tunnel Tunnel Eindings	0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	OAM-PM Service Site Summary OAM-PM Service Summary	*			
Down	View in Current Alarms					
ent Timeline Summary twork event timing for the selected service	Sat, Nov 25, 11:09:00 EST					
II 12 State Upo	tes 7 TC Alarms 0					
	0 OAM Tests 0					

Scroll down to the service map, select the link and click **Details** (()) to see more information in the service summary panel.

NSP



Select **Show in multi-layer map** from the More ( ) menu in the service summary panel. The multi-layer map shows the health of the service, the tunnel, and the IGP and physical layers.

NOCIA Network Services Platform		User: admin	•
ect Troubleshooting > Service Marc_epipe_100 Troubleshooting +		CHANGE TARGET 🔄 4	0
rc_epipe_100 ×		View Molti-layer	- C
	Service Prince		
	nonor		
- 1.	100		
2. 9.	and the second sec		
•	Protect Second		
-			

From the **Object Troubleshooting** dashboard, we can also create an OAM test suite ( ), or select **View OAM test results** from the More () menu. OAM testing can provide valuable information about traffic flow.

ect Troubleshooting > Service Marc_epipe_100 Troubleshooting -	CHANGE TARGET	9	
	View	Edit dashbo	
arc_epipe_100 ×	Mult-Isyer	View OAM te	
		Add to Watc Settings	.hlist
			1
	Service		
	insteador.		
	Tunner A		
	manue		
E3			
A			
e.			
·,	ICP 200		
	And the second sec		
♡, ₽,			
₽,			
₽,	Martin Pa		
₽,	Brain Pas		

5 -

Also from the More menu, we can add the service to the Watchlist. Adding an object to the watchlist allows us to navigate quickly and directly to the object in the future. Choose **Add to Watchlist**.

bject Troubleshooting > Service Marc_epipe_100 Troubleshooting	ng 🔹	CHANGE TARGET 🔄 4	0
		Edit da	ishboard
farc_epipe_100 ×		View Multi-layer View O	AM test res
		Add to	Watchlist
		Setting	gs
			î
a	Service Service		

Click Watchlist (E) to view the Watchlist.

NSP

=		Network Services Pla	atform	User: admin 👻 🕐	
Watch	lst			\$	
			Services & Network elements Monitor and navigate to most important Services & Network elements   Service & NE		*
			mdNodeD (92.168.96.60)           T750 58-76           Affected: Cards 517 Hel, Ports 0 10Hel, Links 1 (20Hel, Unack Ontical Alarme 0		
			Marc_epipe_100 E-Une Store cause: n/e, OAM Validation test: n/s		
					Ŧ

You can click **CHANGE TARGET** in the Object Troubleshooting dashboard to troubleshoot other services or objects.

NOCIA Network Services Platform									• (
ect Troubleshooting > Service Marc_epipe_100 T	Troubleshooting +					CHANGE TARGET		•	
arc_epipe_100 ×						Vie	ew fulti-layer		C
			inener a						6
	Select a Troubleshooting	; Target			×				
	Target Type Service								
	Troubleshooting Target								
	Service Name 🔹			(Max 3)					
	Service Name	Service ID	Customer Name	Customer ID	_				
	Epipe-5002	Epipe-5002	Customer20	Customer20	i				
	IES 5201	IES 5201:15:sam	Customer20	20					
[]	EPIPE 12345	EPIPE 12345:12:sam	Demo Customer	99	_				
	VPLS 5005	VPLS 5005:6:sam	Customer10	10					
<b>•</b>	FPIPE 4	FPIPE 4:18:sam	Default customer	1	*				
~. 2,	Results limited to 100 objects								
٩ ٩				c	CANCEL CHOOSE				
1									
•			ana	. 7					
		Physical	mativos	ne /					

Expand the Sites, Tunnel Bindings, and Endpoints dashlets in the Service Inventory area to see details about service components.

bject Troubleshoo	Familes																			
	ooting > Service Marc_epipe_1	100 Trouble	hooting		•											CHANGE TARGET	E	Ŵ	Ð	
ervice Endpoir	ints ited on 2023/11/25 11:32:25 (Clic	( to undata)																		:
	Operational State	Site ID	Service		Port Name		LAG Name		NE Name		Description		State Cau	se(s)						
T	-			Ŧ		T		т		T		т								
1/c1/9:	disabled	92.168.96	Marc_ep	ipe	1/1/c1/9				mdNodeD		SAP A									
1/c1/9:	enabled	92.168.96	Marc_ep	pipe	1/1/c1/9				mdNodeE		SAP B									
ervice Sites									,	unnel Bi	indings				× <sup>7</sup>					
rvice Sites	Operation									unnel Bi	indings		Operation	al State	ĸ <sup>n</sup>					
me									ħ	lame	indings	100	Operation	al State	× <sup>3</sup>					
	disabled								M	l <b>ame</b> 12.168.96				al State	<i>κ</i> <sup>3</sup>					
ervice Sites									,	unnel Bi	indings				κ <sup>π</sup>					

Select a faulty endpoint and choose **View in Event Timeline** from the Table row actions menu ( • ) to view a history of events for the service.



Click on an event to see a list of actions and alarms associated with the event.

Release 24.8

July 2025

Issue 2


### 5.8.4 Investigate service alarms from the News Feed

Another option for investigating alarm details is to start from the News Feed. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to the Current Alarm List.

1

From the **News Feed**, select the alarm and choose **View in Current Alarms** from the More menu.

NSP



The Current Alarms list opens, with the alarm selected.

2

From the Current Alarms list, you can click **View Impacts** from the table row actions menu for the alarm. This alarm has no impacts.

Release 24.8

July 2025

Issue 2

	Current Alarms		·											C	)
Unsaved Advance	d Filter X					Total Unfiltered Alarms:	C 36	126 5	0 95	0	<b>0 0 0</b>		6	Τ,	
everity	Impact =	Ĺ	ast Time Detected	Site ID		Site Name		larmed Objec			Alarmed Object	~	General		
•	Т	T	זיזיז - זיזיז 🖬		T		T			T					
Э	0	2	2023/11/25 1:22:52 P	92.168.96.26		classicNodeC	v	II.L2Accessint	terface		Port 1/1/c1/9:10.0	~	Severity		
												~	Acknowledgement		
												~	Acknowledgement Notes		
												~	Statistics		
												^	Description		
												^	Remedial Action		
												~	Raising Condition		
													Raising Condition		
													Clearing Condition		

Network Map and Health	Current Alarms		•										C-
T_ Unsaved Advanced Fi	lter X :					Total Unfiltered Alarms:		C M	50 9				Ū <b>T</b> ,
Severity	Impact =		Last Time Detected	Site ID		Site Name			Object Type		Alarmed Object	~	General
- T		T	YYYY - YYYY 🖬		T		т			Т			
G	0		2023/11/25 1:22:52 P	92.168.96.26		classicNodeC		vll.L2Acc	essinterface		Port 1/1/c1/9:10.0 🤃	Ň	Severity
											View impacts	~	Acknowledgement
											View root causes View object impacts	~	Acknowledgement Notes
											Edit alarm(s)		autor -
											Delete alarm(s) Clear alarm(s)	~	Statistics
											Open affected object	^	Description
											Open in NE Session		The alarm is raised when an L2 or L3 interface operational state is Down. The alarm is not raised against an L2 access interface that is associated with an MC ring or MC LAG in the standby state.
												^	Remedial Action
													The condition exists because the physical interface is down either because it is administratively disabled, faulty or a cabling fault has occurred. Ensure that the interface is administratively up. Check for a poor cable connection to the port or for a faulty cable/fiber. If nether appears to be the problem run diagnostics on the port to determine if it
												~	Raising Condition
												~	Clearing Condition
												~	Additional Text



3

Use the drop-down menu at the top of the view to switch to the Top Unhealthy NEs or Top Problems views to see more information about problems in the network.

letwork Map and Health	Current Alarms	•											C+	
Unsaved Advanced F	Overview ilt Current Alarms				Total Unfiltered Alarms:	<b>G</b> 36	() 126 50 9		<b>0</b> 6 0	•		6	T,	
everity	Alarm Distribution	ne Detected	Site ID		Site Name		med Object Type	1	Alarmed Object Name		~	General		
- T	Alarm Statistics	- YYYY 🖬		Ŧ		т		т						
	Merged Alarms	1/25 1:22:52 P	92.168.96.26		classicNodeC	vII.L	2AccessInterface		Port 1/1/c1/9:1	0.0	~	Severity		
	Historical Alarms											Acknowledgement		
	Unhealthy NEs										~	Acknowledgement		
	Top Problems										~	Acknowledgement Notes		
											~	Statistics		
												Statistics Description		
											^			
											^	Description		
											^	Description		
											^	Description		
											^	Description		
											^	Description		
											<ul> <li>.</li> <li>.</li> <li>.</li> </ul>	Description Remedial Action		
											* *	Description Remedial Action Raising Condition Clearing Condition		
											* *	Description Remedial Action Raising Condition		





# 5.8.5 View service provisioning details

Returning to the Troubleshooting dashboard, we can also launch Service Management to look at the provisioning of the service.

1

From the Service Overview dashlet, click View in Service Management.

NSP

ject Troubleshooting > Service Marc_epipe_100	Troubleshooti	ing 👻				CHANGE TARGE			Ð
Troubleshooting Summary Board View troubleshooting summary information									
ervice Overview ummary information for the selected service		Current Health Summary Health status for the selected service		Sites Health Summary Service sites operational statistics		Endpoints Health Summ Service endpoints operation			
Customer Name:	Demo	Administrative State:	unlocked						
Service Type:	E-Line	Life Cycle State:	Deployed	2 50%		2	50%	0	Y
Number of Sites:	2	Alignment State:	Misaligned						
		Operational State:	disabled	Sites Sites Down	TCAs	Endpoints	Endpoints Down	TCAS	
		State Cause:	N/A						
View in Service Management									
unnel Bindings Health Summary ervice tunnel bindings operational statistics		Alarm Summary Alarms and impacts for the selected service		Analytics Reports Run Analytics Reports					
				Service OAM-PM Service Site Summary	•				
2 0% 0			0	OAM-PM Service Summary	•				
Tunnel Tunnel TCA		Critical Major TCAs	Total	CAM-PM Service Summary	·				
Bindings Bindings Down			Impacts						
		View in Current Alarms							
vent Timeline Summary									
etwork event timing for the selected service		Sat, Nov 25,	11:09:00 EST 🛅						
dl 12 5	State Updates	7 TC Alarms	0						
onfigurations 5	Marms	0 OAM Tests	0						

Service Management opens, filtered to show the service in question.

	> Service Marc_epipe_100	Sites	•						G	
te ID	Network Element	Customer ID	Site Name	Service Name	Description	Admin State	Operational State	i Info		
т	T	Т	T		т			Select a service site		
.168.96.60	mdNodeD	100	Marc_epipe_100	Marc_epipe_100	Marc_epipe_100 Desc A	Unlocked	Disabled			
.168.96.16	mdNodeE	100	Marc_epipe_100	Marc_epipe_100	Marc_epipe_100 Desc B	Unlocked	Enabled			

2

From here, we can open the service for editing to verify that the service provisioning is correct. Click **(**Table row actions), **Edit Service**.

T     T     T     T     T     T     Open in Object Troubleshoo       168.96.60     mdNodeD     100     Marc_epipe_100     Marc_epipe_100 Desc A     Unlocked     Disabled     Disabled     Remove	ervice Management	> Service Marc_epipe_100	Sites	Ŧ							0-
T         T         T         T         T         T         T         T         Select a servic         Select a servic         Receive workflow           168.96.60         mdNodeD         100         Marc_epipe_100         Marc_epipe_100 Desc A         Unlocked         Disabled         Remove	e ID	Network Element	Customer ID	Site Name	Service Name		Description	Admin State	Operational State	(i) Info	
Remove	т	T	1	T		T	T	•	-	Select a servic	
188.96.16 mdNodeE 100 Marc_epipe_100 Marc_epipe_100 Desc.B Unlocked Enabled	.168.96.60	mdNodeD	100	Marc_epipe_100	Marc_epipe_100		Marc_epipe_100 Desc A	Unlocked	Disabled		
	.168.96.16	mdNodeE	100	Marc_epipe_100	Marc_epipe_100		Marc_epipe_100 Desc B	Unlocked	Enabled		

3 -

In the Edit form, we can see that all the mandatory fields for the service are populated and the administrative state is unlocked as expected.

We'll scroll further down to look at the sites.

Edstartic:     Aligned     Aligned       Site A     Spile     Deployed     Mailgned       Site A     Spile     Million     Million       Marc_spile_100     100     Million     Million       Marc_spile_100     Deployed     Million     Million       Sor Details     Spile     Million     Million       Sor Detail     Spile <th></th> <th>twork Services Platform</th> <th></th> <th></th> <th></th> <th></th> <th></th> <th></th> <th>User: a</th> <th>ıdmin</th> <th>• ?</th>		twork Services Platform							User: a	ıdmin	• ?
Ste B epipe Depiped Malagned   SDP Details Sarvice Name* Nt Sarvice ID* HTU   Marc_epipe_100 100 Indocked   Customer ID* Description Annie State   100 Indocked Indocked   Ste A   Device ID Site Name* Description   92:159:96:60 Imarc_epipe_100 Marc_epipe_100 Desc A   HTU   Endpoint + ADD	dit Service: Marc_epipe_1	00									
SDP Details       Service kinne*       NE service LD*       Mar_cepipe_100       L0         Custemer 10*       Description       Admin State       Description         Job ID       Site A       Site Name       Description         Sorte Kinne       Description       Marc_epipe_100 Desc A       Marc_epipe_100 Desc A         Portei D       Site Name       Description         Portei D       Site Site Name       Description         Portei D       Site Site Name       Description         Portei D       Inner VLAN Tag       Outer VLAN Tag       Admin State       Description	Site A	Template Name 🛛		Current Life Cycle State		Alignment State					
Sub V defails   Marepipe_100 100   Custemer ID* Description   100 unlocked     100     Site A     Derke ID   92.168.96.60   X •     Marepipe_100     Marepipe_100     Description     Marepipe_100     Description     Port ID     Encep Type     Inner VLAN Tag     Outer VLAN Tag     Admin State	Site B	epipe		Deployed		Misaligned					
Custemer ID* Description     100     Job ID     Site A     Device ID     Site Site.Side.GO     Site Side.side.CO     Marc_epipe_100     Marc_epipe_100 Desc A     Fordpoint     Port ID     Inner VLAN Tag     Outer VLAN Tag     Admin State     Description	SDP Details	Service Name*		NE Service ID*		мти					
100 unlocked C JabiD Site A Device 10 Site Name. Description 92.168.96.60 ×  Marc_epipe_100 Marc_epipe_100 Desc A Marc_epipe_100 Desc A Fru Port ID Encep Type Inner VLAN Tag Outer VLAN Tag Admin State Description		Marc_epipe_100		100							
JabiD  Site A  Pervice ID  Endpoint  Fund  Endpoint  Fund  Site Name  Land  Site Name  Land  Site Name  Land  Site Name  Land  Land Land				Description							
Site A          Device ID       Bite Name       Description         02.168.96.60       X       Marc_epipe_100       Marc_epipe_100 Desc A         MTU		100	0			unlocked	•	⊑x ⊂			
Device 10     Sile Name.     Description       92.168.96.60     X     Marc_epipe_100     Marc_epipe_100 Desc A       MTU		Job ID									
Device ID     Site Name     Description       92.168.96.60     X     Marc_epipe_100     Marc_epipe_100 Desc A       MTU											
92.168.96.60     X     Marc_epipe_100     Marc_epipe_100 Desc A       MTU     Findpoint     + ADD       Port ID     Encep Type     Inner VLAN Tag     Admin State     Description		Site A									
92.168.96.60     X     Marc_epipe_100     Marc_epipe_100 Desc A       MTU     Findpoint     + ADD       Port ID     Encep Type     Inner VLAN Tag     Admin State     Description				-							
MTU Endpoint + ADD Port ID Encep Type Inner VLAN Tag Outer VLAN Tag Admin State Description			×								
Endpoint + ADD Port ID Encep Type Inner VLAN Tag Outer VLAN Tag Admin State Description											
Port ID Encap Type Inner VLAN Tag Outer VLAN Tag Admin State Description		мто									
Port ID Encap Type Inner VLAN Tag Outer VLAN Tag Admin State Description		Endpoint						+ ADD			
		Port ID	Encap Type	Inner VLAN Tag	Outer VLAN Tag	Admin State					
1/1/c1/9 -1 100 unlocked SAPA											
		1/1/c1/9		-1	100	unlocked	SAP A	:			

For both sites, everything looks good. The administration state is unlocked, inner and outer VLAN tags are present and correct.

If we scroll further down to look at the service tunnels, they're both unlocked and provisioned with a source and destination.

The provisioning looks good on the NSP side, so we'll close the Edit form.

4

The next thing we can do is confirm that the provisioning is also correct on the NEs by doing an audit config. This will compare the configuration on the NSP with what is present on the NE.

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

vice Management Services						+ CREATE C
Cycle State	Alignment State Composite Service	Service Name	Description	Service Template	Customer ID	Admin Stat
•	· · · · ·	T	T	T	Т	T
Unknown	Unknown	EPIPE 6003	N/A		30	Unlocked
Unknown	Unknown	EPIPE 12345	N/A		99	Unlocked
Unknown	Unknown	EPIPE 2121	N/A		100	Unlocked
Unknown	Unknown	EPIPE 6004	N/A		30	Unlocked
Unknown	Unknown	ELINE_Demo			1	Unlocked
Unknown	Unknown	Epipe-5002	Epipe-5002		Customer20	Unlocked
Unknown	Unknown	Katarina_Epipe_200			Demo	Unlocked
Deployed	() Misaligned	Marc_epipe_100		epipe	Demo	Unlocked
Unknown	Unknown	NewTestEpipe	abcd		120	Action Edit
Unknown	Unknown	NewerEPipe			Demo	Clone
Unknown	Unknown	Rmtest			Customer30	View Service Definition
Deployed	Aligned	AnooptestEpipe	abcdef	epipe	30	Audit config
Deployed	⊘ Aligned	Anooptest02		epipe	44	Align +
Deployed	() Misaligned	Marc Epipe 1		epipe	100	Migrate
Unknown	Unknown	EPIPE 5	N/A		1	Resync
Unknown	Unknown	EPIPE 3	Default Eline Template		1	Execute workflow
Unknown	Unknown	VPLS 6001	N/A		30	Remove
Unknown	Unknown	VPLS 5005	Vpls-5005		10	View Service details
Unknown	Unknown	VPLS 5006	Vpls-5006		20	Open in Object Troubleshooting

The audit operation has found a misaligned attribute. The NSP configuration shows that the state of this SAP should be enable, but the actual value is disable.

Release 24.8

July 2025

Issue 2

	neenoneoerne	es Platform						User: admin	*	
vice Management	Services	•						+ (		
Cycle State	Audit Result -	Marc_epipe_100						×		
	MISALIG	NED ATTRIBUTES	MISSING OBJECTS	UNDESIRED OBJECTS	APPROVED MIS	SALIGNMENTS				
Unknown				y to save all changes and close the Audit Re						
Jnknown	U Select n	nisaligned attributes(s) to	approve the misalignment(s). Click Apply	/ to save all changes and close the Audit Re	esuit form.					
Jnknown	Name Name		Attribute			Desired Value	Observed Value		10:44:48 AM ES	EST
Jnknown										
Inknown		92.168.96.60(1)								
Inknown		92.168.96.60	/nokia-conf:/configure/service/	e/epipe=Marc_epipe_100/sap=1/1/c1/9:10	00/admin-state	enable	disable			
nknown										
eployed										
nknown										
nknown										
inknown										
nknown eployed										
nknown eployed eployed										
nknown eployed eployed eployed										
nknown eployed eployed eployed inknown										
Jinknown Deployed Deployed Deployed Jinknown										
Jinknown Deployed Deployed Deployed Joknown Jinknown Jinknown										
Inknown Heployed Heployed Inknown Inknown							CANCEL APPROVE S	elected apply		

5

Now that we have verified that there is a mismatch between NSP provisioning and the NE, we can use the align function to push the configuration to the network.

From the services tab, click **t** (Table row actions), **Align**, **Push to network** and confirm.

ervice Management Services							+ CREATE	G	
fe Cycle State	Alignment State Composite Service	Service Name	Description	Serv	ice Template	() Info			
•	×	T	τ []	T	۲	States			
Unknown	Unknown	EPIPE 6003	N/A		1	•			
Unknown	Unknown	EPIPE 12345	N/A		:	Life Cycle State			3
Unknown	Unknown	EPIPE 2121	N/A		:	<ul> <li>Deployed</li> </ul>	Nov 25, 2023, 10:44:4	8 AM E	ST
Unknown	Unknown	EPIPE 6004	N/A		:	Alignment State			
Unknown	Unknown	ELINE_Demo			:	() Misaligned			
Unknown	Unknown	Epipe-5002	Epipe-5002		:				
Unknown	Unknown	Katarina_Epipe_200			1	General Info			
Deployed	() Misaligned	Marc_epipe_100		epip	e i				
Unknown	Unknown	NewTestEpipe	əbcd		Action Edit	Service ID Marc_epipe_100			
Unknown	Unknown	NewerEPipe			Clone	NE Service ID			
Unknown	Unknown	Rmtest			View Service Definition	100			
Deployed	Aligned	AnooptestEpipe	abcdef	epip	Audit config	Service Name			
Deployed	Aligned	Anooptest02		epip	Align +	Push to network			
Deployed	() Misaligned	Marc Epipe 1		epip	Unassociate Migrate	Pull from network			
Unknown	Unknown	EPIPE 5	N/A		Resync				
Unknown	Unknown	EPIPE 3	Default Eline Template		Execute workflow	Service Type			
Unknown	Unknown	VPLS 6001	N/A		Remove				
Unknown	Unknown	VPLS 5005	Vpls-5005		View Service details	Customer ID Demo			
Unknown	Unknown	VPLS 5006	Vpls-5006		Service details   Open in Object Troubleshooting	▼ Service Manager ID			

When the alignment operation is complete, the Alignment State shows as Aligned. Within a minute or two, the operational state should be changed to enabled and the service should be working.

ervice Management Services	•					+ CREATE C
fe Cycle State	Alignment State Composite Service	Service Name	Description	Service Template	:	(i) Info
	•	T	T	T	٣	States
Unknown	Unknown	EPIPE 6003	N/A		: -	
Unknown	Unknown	EPIPE 12345	N/A		:	Life Cycle State
Unknown	Unknown	EPIPE 2121	N/A		:	Deployed Nov 25, 2023, 10:44:48 AM EST
Unknown	Unknown	EPIPE 6004	N/A		- E	Alignment State
Unknown	Unknown	ELINE_Demo			:	Aligned
Unknown	Unknown	Epipe-5002	Epipe-5002			
Unknown	Unknown	Katarina_Epipe_200			:	General Info
Deployed	O Aligned	Marc_epipe_100		epipe	:	Service ID
Unknown	Unknown	NewTestEpipe	abcd		:	Marc_epipe_100
Unknown	Unknown	NewerEPipe			:	NE Service ID
Unknown	Unknown	Rmtest			:	100
Deployed	⊘ Aligned	AnooptestEpipe	abcdef	epipe		Service Name
Deployed	Aligned	Anooptest02		epipe	:	Marc_epipe_100
Deployed	() Misaligned	Marc Epipe 1		epipe	:	Description
Unknown	Unknown	EPIPE 5	N/A		:	72 W 24
Unknown	Unknown	EPIPE 3	Default Eline Template		:	Service Type ELINE
Unknown	Unknown	VPLS 6001	N/A		:	Customer ID
Unknown	Unknown	VPLS 5005	Vpls-5005		:	100
Unknown	Unknown	VPLS 5006	Vpls-5006			Service Manager ID

# 5.9 End-to-end link troubleshooting scenario

### 5.9.1 Purpose

This process shows you how to use NSP in troubleshooting issues on links.

In this scenario, a link is experiencing problems.

### 5.9.2 View the Network Map

1

The Network Map provides a graphical view of links in the network. Problem links are displayed in red on the map.

#### Open Network Map and Health, Network Map View.

Hover over a problem link to display link details.

■ NOCIA Network Services Platform				User: admin 🗸 🤅
NETWORK FUNCTIONS Network Map and Health Network Health View	*			E
Network Map View Network Inventory View	he metrics below			
Object Troubleshooting Current Alarms OAM Tests	Hour + Service Health The status of all netwo	ork services	Service Configuration Health The configuration status of all network services	Alarm Summary Unacknowledged root cause alarms
Device Management Model Driven Configurator Network Mediation WaveSuite - Network Operations Center IP/Optical Coordination	able 15. Healthy Services	10. Affected Services	25 Total Services View in Service Management	29; Critical Major 49. 0. TCAs
Data Collection and Analysis Service Management Path Control			Last Hour 🔹 🗄	News Feed View unacknowledged root cause alarms as they occur
PROGRAMMING Network Intents	By Tunnel Bindings			T Alarms • 🖅 By Time Reported •
Workflows NSP ADMINISTRATION				SendNotification neighbor=92.168.96.26 10 seconds ago Impact: 0
System Health Map Layouts and Groups File Server				SendNotification neighbor=92.168.96.7 12 seconds ago Impact: 0
Users and Security Artifacts				SendNotification neighbor=92.168.96.7 1 minute ago Impact: 0
				NspBaseServiceDown marci-nsp-23-11-node4.nspos- system-admin-app-svc Impact. 0 1 minute ago
				NspBaseServiceDown

2 -

Choose **Multi-layer** from the **View** drop-down above the map to show the IGP links in a plane above the physical links.

If there are problems in both layers, the link is displayed in red on both planes.

NSP

E NOCIA Network Services Platform	User: admin 🗸	?
Network Map and Health Overview	晤	:
Network Map View View your network in the context of a map		
	Operational Multi-layer	: : ::

Choose Operational from the View drop-down to return to the previous view.

4

3

We can view utilization data from the Network Map.

Choose **Enabled** from the **Utilization** drop-down. With utilization enabled, hover over the problem link to see utilization information. Utilization on our link of interest is currently zero.



5

We can also open a utilization tracking chart from the link list in the **Network Map and Health** dashboard.

Choose **Disabled** from the **Utilization** drop-down, then right-click on the link and choose **Show in Links list** from the context menu.



The Links dashlet in the Network Map and Health dashboard opens, filtered to the target link.

6

Click on the link and choose (Table row actions), **Plot utilization statistics**.

									Use	er: admin	•
twork Map and	d Health Overview	÷								e,	
Network View deta	Inventory View led information relating to you	ur network objects									
nks											:
Content up	dated on 2023/11/1 16:45:55 (Cl	lick to update)									
ame	Operational State	Manually Created	Link Type	Туре	Latency (ms)	Description	EndPoint A Source	EndPoint A	EndPoint A Capacity Mb/s	EndPoint A Type	
= n × T,	•	•	•	•			<b>t</b>				
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo	-	1 N/A	mdNodeE	1/1/c1/2	10000	physicalPort	
										View in Current Alarms	
										C Show in network map	
										<ul><li>Show in network map</li><li>View in Object Troublesho</li></ul>	
										<ul> <li>Show in network map</li> <li>View in Object Troublesho</li> <li>Plot utilization statistics</li> </ul>	
										<ul><li>Show in network map</li><li>View in Object Troublesho</li></ul>	

7 –

A new tab opens in Data Collection and Analysis Visualizations, showing utilization charts.



NSP

We'll leave the tab open to check again later.

#### 5.9.3 Investigate from the Object Troubleshooting dashboard

1 Returning to the Links dashlet, choose (Table row actions), View in Object Troubleshooting.

	Network Services Platf	orm								U	ser: admin	• (
letwork Map and I	Health Overview	•									E)	
Network I View detaile	Inventory View ed information relating to you	ur network objects										
Links												:
Content upda	ated on 2023/11/1 16:45:55 (Cil	ick to update)										
Name	Operational State	Manually Created	Link Type	Туре	Latency (ms)	D	Description	EndPoint A Source	EndPoint A	EndPoint A Capacity Mb/	/s EndPoint A Type	
= n × T.	•						Τ.					
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000	physicalPort	
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000	physicalPort <ul> <li>View in Current Alarms</li> </ul>	
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000		
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000	View in Current Alarms	hootin
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000	<ul> <li>View in Current Alarms</li> <li>Show in network map</li> </ul>	
ndNodeE	disabled	No	IP/IGP/CUPS	pointTo		-1 N	N/A	mdNodeE	1/1/c1/2	10000	<ul> <li>View in Current Alarms</li> <li>Show in network map</li> <li>View in Object Troublest</li> </ul>	

The **Object Troubleshooting** dashboard shows summary dashlets with information about our object of interest. You can click **CHANGE TARGET** to view another object if needed.

ect Troubleshooting > Lind md	k NodeE:1/1/c1/2classicNodeC:P	ort 1/1/c1/2 Troubleshooting					CHANGE D
Troubleshooting Summary Select a link to view troubleshoo	Board oting summary information						
nk Endpoints Overview e the summary endpoint information	on of the selected Link.			Current Health Summary See what object you are troubleshooting a	nd how healthy it is.		
mdNodeE	1/1/c1/2	classicNodeC	Port 1/1/c1/2	mdNodeE	1/1/c1/2	classicNodeC	Port 1/1/c1
Port Type:	ethernet	Port Type:	ethernet	Operational State:	disabled	Operational State:	enable
Port Mode:	trunk	Port Mode:	trunk	Administrative State:	locked	Administrative State:	unlocke
Management Address:	135.121.152.20	Management Address:	192.168.97.146	Availability State:	N/A	Availability State:	N
System Address:	92.168.96.16	System Address:	92.168.96.26	NE Communication State:	up	NE Communication State:	L
arm Summary - Link e alarms and impacts for the select	ted link	Alarm Summary - mdNodeE See alarms and Impacts for endpoint	A	Alarm Summary - classicNodeC See alarms and impacts for endpoint B			
• • •	0 0	0 1	0	000	•		
Critical Major	TCAs Total Impacts	Critical Major	TCAs Total Impacts	Critical Major TCA:	s Total Impacts		
View in Current	t Alarms	View in Curren	t Alarms	View in Current Alar	ms		
						View	v

In the **Object Troubleshooting** dashboard map, we can change the **Hop Count** to see nodes that are further from the target.

t Troubleshooting > mdNodeE:1/1/c	1/2classicNodeC:Port 1/1/c1/2 Troubleshooting		CHANGE TARGET
m Summary - Link alarms and impacts for the selected link	Alarm Summary – mdNodeE See alarms and impacts for endpoint A	Alarm Summary - classicNodeC See alarms and impacts for endpoint B	
0 0 0 0 Critical Major TCAs	O         O         O         O         O         O         O         O         O         O         O         O         O         O         O         Total         Major         TCAs         Total         Total	al Critical Major TCAs Total	
View in Current Alarms	View in Current Alarms	View in Current Alarms	
lodeE:1/1/c1/2classicNodeC:Port 1/1	/c1/2		View Operational
ation Hop Count sabled + 1 +			
0			
3 2		C C C C C C C C C C C C C C C C C C C	
B. 3 4. 5. 2.	Chastichore	foreste s	

You can select **Utilization** to display link utilization statistics on the Troubleshooting map, just as we can on the Network map.

NSP

ct Troubleshooting > m	nk dNodeE:1/1/c1/2classicNodeC:Port 1/1/c1/2	Troubleshooting			CHANGE TARGET
NodeE:1/1/c1/2classicNod	deC:Port 1/1/c1/2				View Operational
	Physical Link	Endpoint A	Endpoint B		
	NE Name:	mdNodeE	classicNodeC		
	Endpoint Name:	1/1/c1/2	Port 1/1/c1/2		
	Utilization	0%	0%		
	Capacity	10 Gb/s	10 Gb/s		
1	Operational State:	Enabled	Enabled	mdNadeE	
£	Administrative State:	Unlocked	Unlocked	10.05/8-000	
6					
- -					

Back in the **Object Troubleshooting** dashboard, navigate to the **Alarm Summary** dashlet and click the **Major** alarm circle to view **Current Alarms** with a filter for the pertinent alarm.

■ NOKIA Network Service	s Platform					User: admi	n	Ŧ	0
Dbject Troubleshooting > Link mdN	NodeE:1/1/c1/2classicNodeC:P(	ort 1/1/c1/2 Troubleshooting					CHANGE TARGET	Ð	
Troubleshooting Summary B Select a link to view troubleshoot	Board ting summary information								
Link Endpoints Overview See the summary endpoint information	n of the selected Link.			Current Health Summary See what object you are troubleshooting.	and how healthy it is.				
mdNodeE	1/1/c1/2	classicNodeC	Port 1/1/c1/2	mdNodeE	1/1/c1/2	classicNodeC		Port 1/1/c1	1/2
Port Type:	ethernet	Port Type:	ethernet	Operational State:	disabled	Operational State:		enab	led
Port Mode:	trunk	Port Mode:	trunk	Administrative State:	locked	Administrative State:		unlock	
Management Address:	135.121.152.20	Management Address:	192.168.97.146	Availability State:	N/A	Availability State:		٦	N/A
System Address:	92.168.96.16	System Address:	92.168.96.26	NE Communication State:	up	NE Communication State:			up
Alarm Summary - Link See alarms and impacts for the selecte	ed link	Alarm Summary - mdNodeE See alarms and impacts for endpoint A		Alarm Summary - classicNodeC See alarms and impacts for endpoint B					
	0 0		0 0						
Critical Major	TCAs Total Impacts	Critical Major	TCAs Total Impacts	Critical Major TC	As Total Impacts				
View in Current	Alarms	View in Current	Alarms	View in Current Ala	arms				

We can see that there are no impacts, but there may be a root cause. Click on the alarm, choose (Table row actions), select **View Root Causes**.

etwork Map and H	ealth Curre	nt Alarms 👻																Ģ	
Unsaved Ad	vanced Filter X	1			Total Unfil	tered Alarms:	G 37		00 49	<b>9</b>	0	1	0	0	(	D		Ţ	
verity	Impact	Last Time Detected 🔘	Alarmed Object Type		Alarmed Object Name		Alarm Nan	ne	P	robable	Cause			:	∽ General				
- T,	τ	, YYYY-м - YYYY-м 🖬		Τ.		Τ.			τ.			T							
	0	2023/11/1 06:44:42 PM G	equipment.Equipment		port=1/1/c1/2	J	LinkDown		e	quipmer	ntMalfu	incti		:	✓ Severity				
												/iew Imj /iew Ro		ses	✓ Acknowle	dgement			
											V	/iew Ob	ject Im		✓ Acknowle	dgement Notes			
											C	)elete A	larm(s	)	<ul> <li>Statistics</li> </ul>				
												Clear Ala Open af		object	^ Description	in			
											0	Open in	NE Ses	sion	This alarm is ge has detected ti to enter the do present state). oper-status lea	nerated when the SNI at port used for one o wn state from some o This other state is ind f	MP entity, acting of its communica ther state (but n icated by the inc	in an agent ro tion links is a ot from the n luded value o	ole, bout ot- f if-
															^ Remedial	Action			
															If the admin sta is no recovery. the interface g	te is 'down' then the f the admin state is 'u ing down: cable cut, e	interface state is up' then try to de distal end went d	deliberate ar termine the c own, etc.	nd the
															✓ Raising Control	ndition			
															<ul> <li>✓ Clearing 0</li> </ul>	ondition			
															<ul> <li>Additional</li> </ul>	Text			
															✓ Custom T	ext			

In this case, the root cause diagram does not show a specific root cause: the alarm in question is the only one present.

NSP

NOKIA Network Services Platform	User: admin	• ⑦
Network Map and Health > Alarm Id fdn.model:fm.Alarm.221883 Root Cause Diagram		:
Root Cause Diagram Overview	0	ŧΞ
Impacted Alarm LinkDown	Choose Alarm t	to Display

# 5.9.4 Investigate link alarms from the News Feed

Another option for investigating alarm details is to start from the News Feed. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm. All alarms can cross launch to Current Alarms.

1

From the **News Feed** in the **Network Map and Health** dashboard, select the alarm and choose **View in Current Alarms** from the More menu.

work Map and	d Health Overv	view -					
Network Determine	: Health View e the overall health o	of your network using the metrics	below				
<b>uipment He</b> e status of all	ealth I network elements	Last Hour 🔹	Service Health The status of all network servic	Last Hour •	Service Configuration Health The configuration status of all network services	Alarm Summary Unacknowledged root cause ala	Last Hour
0%- Poor Network Health	0. Healthy NEs	5- 0- Affected Unreachable NEs NEs	Healthy Aff	10- Hected Degraded services	25 9 Total Missigned Services	29. 111. Critical Major	49. O. Minor TCAs
					View in Service Management	View in Cu	irrent Alarms
ected Servi	ices ork objects are affec	ting services			Last Hour 👻	News Feed	View In Current Alarms
which netwo	ork objects are affec		nel Bindings		Last Hour -		View Impacts
which netwo	ork objects are affec	tting services ervice Endpoints • By Tur	nel Bindings		Last Hour - :	View unacknowledged root cause	View Impacts View Root Causes View Object Impacts
which netwo By Service	ork objects are affec		nel Bindings		Last Hour • :	View unacknowledged root caus	View Impacts View Root Causes View Object Impacts Open In Network Inventory
which netwo	ork objects are affec		nel Bindings		Last Hour • :	View unacknowledged root cau Alarma	View Impacts View Root Causes View Object Impacts Open In Network Inventory View in Object Troubleshootin
Which netwo	ork objects are affec		nel Bindings		Last Hour • :	View unacknowledged root cau T Alarms -	View Impacts View Root Causes View Object Impacts Open in Network Inventory View in Object Troubleshootin Plot utilization statistics
which netwo By Service	ork objects are affec		nel Bindings		LastHour - :	View unacknowledged root cau Alarma = = By path_toNodeE Impact: 0 LinkDown Interface=toNodeC Impact: 0 LinkDown port=1/1/c/12	View impacts View Root Causes View Object Impacts Open in Network Inventory View in Object Troubleshootin Plot utilization statistics Plot error statistics 20 hours ago

Current Alarms cross launches, with the alarm selected.

2 -

From **Current Alarms**, you can view the NE in the **Unhealthy NEs** tab to see what correlated alarms may be present on the endpoint NEs, or check **Top Problems** to see what other issues the network is experiencing. Here we see that Link Down is currently the third most common problem.



# 5.9.5 View port details

1

Returning to the **Object Troubleshooting** dashboard, click on one of the ports to cross launch **Network Inventory** to look at the status of the endpoint ports.

NOCIA Network Services Platform		User: admin	•
nventory mdNodeE			
ipment type filters  • T <sub>+</sub> Any of: Port: 1/1/c1/2 ×	^	0	ŧΞ
erational State: All + Administrative State: All + APPLY FILTERS		∧ Properties	
mdNodeE (7750 SR-14a), Operational State: enabled, Administrative State: unlocked	:	Name 1/1/c1/2	
Equipment Group	v	Description Network Port	
Shelf-1, Operational State: enabled, Administrative State: unlocked	:	Operational State disabled	
👻 📗 Card Slot-1(scm-14a) (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:	Administrative State locked	
Card-1fxcm-14al, Operational State: enabled, Administrative State: unlocked	:	Standby State providingService	
🔹 📗 Card Slot-1/1(s36-100gb-qs/p28) (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:	Position shelf=1/cardSlot=1/card=1/md MAC Address	daSlot=1/mda=1/p
Card-1/1fs36-100gb-qsfp281, Operational State: enabled, Administrative State: unlocked	:	MAC Address — Port Index	
Init 1/1/c1, Operational State: enabled, Administrative State: unlocked	:	1610899522 Port Type	
1/1/c1/2, Operational State: disabled, Administrative State: locked	;	ethernet Port Mode	
E Legical Group		trunk Encapsulation Type	
En Link Aggregation Groups		dot1q MTU (bytes)	
Routing Instances		Rate	
ACLSets		Actual Rate (Mbps)	
• a BFD		State Reasons	
	A Back to top		

# 5.9.6 Evaluate the NE configuration

1 -

In **Device Management**, select **Configuration Deployments** to check the state of the link endpoint port deployments.

	twork Services Platform												User: ai		•
Device Management	Managed Network Elements 🗸 🗸														
eachability	Devices		Management IP		NE ID		Product		Chassis		Software Version	:	0	*	
achaomry	Managed Network Elements ZTP Process	Τ.	Hanagement ir	Τ.	NE ID	Τ.	Froduct	T,	Cilussis	τ.		•			LO
Reachable	Configuration	1+		1+		1+	7750.00	1+	7750.00.40	1+			Select an NE to	see the details	
	Configuration Deployments		135.121.153.11		92.168.96.7		7750 SR		7750 SR-12		TiMOS-B-21.5.R2				
Reachable	Configuration Templates		135.121.152.20		92.168.96.16		7750 SR		7750 SR-14s		TiMOS-C-21.10.R12	:			
Reachable	Configuration Intent Types		135.121.157.2		92.168.96.60		7750 SR		7750 SR-7s		TiMOS-C-22.10.R6	:			
Reachable	Operation		135.121.151.102		92.168.96.26		7750 SR		7750 SR-2s		TiMOS-C-22.7.R2	:			
	All Operations														
	Operation Schedules														
	Operation Types														
	Node Images														

If required, filter the Identifier column with the port number to display the deployments that configured the ports in the link. The deployment status column shows the status from the last audit operation performed.

2

For each port, click **AUDIT** in the **Deployment Details** panel to compare the NSP configuration against the NE configuration.

Devi	ice Management Configuratio	on Deployments 🔹												+ DEPLOYMENT C+
	Deployment Status	Configuration Status	NE Name		NE ID		Identifier	Template		Re	ole	Categor	ry :	(i) Deployment Details
	•			<b>T</b> .,		Τ.	T,		Τ,		•			NE Name
	<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	classicNodeC		92.168.96.26		Port 1/1/c1/2	Default Ethernet	Port	Pł	hysical	Port	:	mdNodeE NE ID
	Deployed Aligned	Modified	mdNodeE		92.168.96.16		1/1/c1/2	Default Ethernet	Port	Ph	hysical	Port	1	92.168.96.16
														Identifier
														Port-ID 1/1/c1/2
														Deployment Status
														Deployed Aligned
														AUDIT ALIGN
														Last Audit
														-
														Last Alignment Nov 2, 2023 1:54:48 pm by admin
														Template Name Default Ethernet Port
														Created Nov 2, 2023 1:52:20 pm
														Last Updated
														Nov 2, 2023 1:54:48 pm
														Role Physical
														Category port
														Configuration Status
														<ul> <li>Modified</li> </ul>
						_						,		
	Auto-refresh Last Refresh:	2023/11/2 16:14:11					< Page: 1 /1 > >						unt:2	

3

After auditing the port deployment, we can see that it is misaligned. Select the deployment and click **VIEW RESULT** to see the results of the audit.

Dev	ice Management Configurat	ion Deployments 🔹												+ DEPLOYMENT C+
	Deployment Status	Configuration Status	NE Name		NE ID		Identifier		Template		Role	Category	y i	(i) Deployment Details
				Τ.		T,		T		$\overline{T}_{\mu}$	•			NE Name
	Deployed Aligned	<ul> <li>Modified</li> </ul>	classicNodeC		92.168.96.26		Port 1/1/c1/2		Default Ethernet Port		Physical	Port	:	mdNodeE
	Deployed Misaligned	<ul> <li>Modified</li> </ul>	mdNodeE		92.168.96.16		1/1/c1/2		Default Ethernet Port		Physical	Port	:	NE ID 92.168.96.16
														Identifier
														Port-ID 1/1/c1/2
														Deployment Status
														Deployed Misaligned
														AUDIT ALIGN
														Last Audit
														> Nov 2, 2023 4:51:59 pm by admin
														VIEW RESULT
														Last Alignment
														Nov 2, 2023 1:54:48 pm by admin
														Default Ethernet Port
														Created Nov 2, 2023 1:52:20 pm
														Last Updated
														Nov 2, 2023 1:54:48 pm
														Physical
														Category
														port

The results show a misaligned attribute. The administrative state for one of the ports is incorrect.

KOCIA Network Services Platform			User: admin	*	0
Audit Result from Nov 2, 2023 4:51:59 pm				Ģ	×
MISALIGNED ATTRIBUTES MISALIGNED OBJECTS					
Attribute	Expected Value (Template)	Actual Value (NE)			
/configure/port=1/1/c1/2/admin-state	enable	disable			

CANCEL ALIGN ALL CONFIG

4

Select ALIGN ALL CONFIG to perform an alignment to fix the discrepancy.

			0
NOCIA Network Services Platform		User: admin	• ?
Audit Result from Nov 2, 2023 4:51:59 pm			G ×
MISALIGNED ATTRIBUTES			
Attribute	Expected Value (Template) Actual Value (NE)		
/configure/port=1/1/c1/2/admin-state	enable disable		

CANCEL ALIGN ALL CONFIG

Perform another **AUDIT** to confirm the alignment.

5 -

Returning to **Network Inventory**, we can see that the port now displays green and its administrative state is unlocked.

NOCIA Network Services Platform		User: admin	•	?
NE Inventory classicNodeC				G
Equipment type filters - T <sub>4</sub> . Any of:	+++++++++++++++++++++++++++++++++++++++	0	ê =	
Operational State: All   Administrative State: All   Apply FILTERS		Select an item to see the de	tails	
classicNodeC (7750 SR-2s), Operational State: enabled, Administrative State: unlocked	:			
B Equipment Group	:			
ClassicNodeC, Operational State: enabled, Administrative State: unlocked	:			
Card Slot - 1 (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Card - 1, Operational State: enabled, Administrative State: unlocked	:			
Daughter Card Slot - 1/1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	:			
Daughter Card - 1/1, Operational State: enabled, Administrative State: unlocked	:			
Port 1/1/c1, Operational State: enabled, Administrative State: unlocked	:			
Port 1/1/c1/2, Operational State: enabled, Administrative State: unlocked	:			
B Logital Group				
Link Aggregation Groups				
Routing Instances				
ACL Sets				
• a BFD				
	▲ Back to top			
Auto-refresh Last Refresh: 2023/11/29 12:53:18				

6 -

#### In the Multi-layer view, the links now also display green.

NOCIA Network Services Platform		User: admin	•	?
Network Map and Health Overview			F	:
		View Multi-løyer 👻	G	:
				0
•       •       •       •       •       •       •       •       •       •       •	ICD Protection			
7 -



Returning to **Data Collection and Analysis Visualizations**, we can also see that traffic utilization has resumed.

# 5.10 End-to-end port troubleshooting scenario

#### 5.10.1 Purpose

This process shows you how to use NSP in troubleshooting issues on ports.

In this scenario, a service has been affected or an alarm has come up. Investigation will show that the problem is due to a port issue.

## 5.10.2 View the Object Troubleshooting dashboard

Viewing a target in the Object Troubleshooting dashboard can help you see where else you can look to investigate a problem.

#### 1 -

Start from the **Object Troubleshooting** dashboard, select **Port** for Target Type, and then select the target port of interest.

			User: admin
ubleshooting > Select target type Select troubleshooting target Troubleshooting			
	Select a Troubleshooting Target	×	
	Target Type		
	Port		
	Troubleshooting Target		
	Port Name 👻 🏹 (Max 3)		
	1+ (Pink 3)		
	Port Name Description	NE Nai	
	1/2/14	Assi	
		Assi	
	1/2/40	Assi	
		Assi	
		Assi	
	2/1/1	mtli™ ▶	
	CANCEL CH	IOOSE	

The **Object Troubleshooting** dashboard displays summaries of information about the port. The Alarm Summary shows that an alarm is present, and the Current Health Summary shows the operational and administrative states.

Object Troubleshooting > Pert Port 1/1/c1/2, classicNodeC Troubleshooting Troubleshooting Summary Board Select a port to view troubleshooting summary information Port Overview				TARGET	
Port Overview					
ee the summary information for the selected port		Equipment Overview See the summary information of the s	elected port equipment		
Port Type: ethernet		Position:	shelf=1/slot=1/card		
Port Mode: trunk		Product:	7750 SR		
Management Address: 192.168.97.146		Chassis Type:	7750 SR-2s		
System Address: 92.168.96.26		Version:	TIMOS-C-22.7.R2		
Location: N/A		Manufacture Date:	N/A		
Current Health Summary Alarm Sum ee what object you are troubleshooting and how healthy it is See alarms as	mary nd impacts for the selected port	Analytics Reports Run Analytics Reports			
Operational State: disabled		Port			
Administrative State: locked		Port Throughput Summary	>		
Availability State: N/A					
NE Communication State: up Critical	Major TCAs Total Impacts				
Open in Network Inventory	View in Current Alarms				

Use **CHANGE TARGET** if the wrong port is selected or if you wish to troubleshoot a different port.

oject Troubleshooting > Port Port 1/1/c1/2 Trou	ubleshooting		CHANGE TARGET
Troubleshooting Summary Board Select a port to view troubleshooting summary info	rmation		
ort Overview ee the summary information for the selected port		Equipment Overview See the summary information of the selected port equipment	
Port Type:	ethernet	Position: shelf=1/slot=1/card	
Port Mode:	trunk	Product: 7750 SR	
Management Address: 192.16	68.97.146	Chassis Type: 7750 SR-2s	
System Address: 92.1	68.96.26	Version: TiMOS-C-22.7.R2	
Location:	N/A	Manufacture Date: N/A	
urrent Health Summary ee what object you are troubleshooting and how healthy	Alarm Summary It is See alarms and impacts for the selected port	Analytics Reports Run Analytics Reports	
Operational State: d	isabled	Port	
	locked	Port Throughput Summary	
Availability State:	N/A 0 0 2		
NE Communication State:	up Critical Major TCAs Tot Impa		
Open in Network Inventory	View in Current Alarms		

Click the **Major** alarm circle in the **Object Troubleshooting** dashboard to launch **Current Alarms**, with that pertinent alarm filtered.

oject Troubleshooting > Port 1/1,	/c1/2, classicNodeC Tro	ubleshooting				CHANGE TARGET	Ð
Troubleshooting Summary Boar Select a port to view troubleshooting	<b>d</b> summary information						
ort Overview ee the summary information for the selec	ted port			Equipment Overview See the summary information of	he selected port equipment		
Port Type:	ethernet			Position:	shelf=1/slot=1/card		
Port Mode:	trunk			Product:	7750 SR		
Management Address:	192.168.97.146			Chassis Type:	7750 SR-2s		
System Address:	92.168.96.26			Version:	TIMOS-C-22.7.R2		
Location:	N/A			Manufacture Date:	N/A		
urrent Health Summary ee what object you are troubleshooting ar	nd how healthy it is	Alarm Summary See alarms and impacts for the selec	cted port	Analytics Reports Run Analytics Reports			
Operational State:	disabled			Port			
Administrative State:	locked			Port Throughput Summary	►		
Availability State:	N/A		0 2				
NE Communication State:	up	Critical Major	TCAs Total Impacts				
Open in Network Inver	ntory	View in Curren	t Alarms				

In Current Alarms, view the Root Causes for the alarm.

																	•
letwork Map and I	Health Curren	nt Alarms 👻														C	)
Unsaved A	dvanced Filter 🗙	1			Total Unfiltered Alarms:	G (38 124	5	0 ( 49 7	9	0	0		0	G	)	T	
everity	Impact	Last Time Detected	Alarmed Object Type		Alarmed Object Name						Alarm Nai	ne	:	✓ General			
• T,	Τ.	уууу-мм-р - уууу-мм-р 🖬		Τ.,						¢.							
	2	2023/11/3 06:05:23 PM GMT+04:00	equipment.PhysicalPort		Port 1/1/c1/2					)	Equipmer	tAdmin		✓ Severity			
											ew Impac			~ Acknowled	gement		
											ew Root (						
											ew Objec it Alarm(:		cts	✓ Acknowled	gement Notes		
											elete Alar			<ul> <li>Statistics</li> </ul>			
										Cle	ear Alarm	(s)					
											en affec			<ul> <li>Description</li> </ul>	n		
										Op	oen in NE	Sessio	on	The alarm is raise	ed when the compositeEquipme	ntState attribute	has
														value of equipme	entAdministrativelyDown.		
														^ Remedial A	action		
														leformational o	o corrective action required.		
														informational - n	to corrective action required.		
														✓ Raising Cor	ndition		
														✓ Clearing Co	ondition		
														<ul> <li>Additional</li> </ul>	Text		
														✓ Custom Tex	xt		

Current Alarms shows that there is no root cause for this particular alarm as it is a root cause alarm.

NSP



Another option is to switch to the **Unhealthy NEs** or **Top Problems** view in the **Network Map and Health** dashboard to see what other alarms are present on the NE, and to see what other issues the network is experiencing.

#### 5.10.3 View the News Feed

Another starting point could be the News Feed in the Network Map and Health dashboard. The News Feed provides a live feed of unacknowledged root cause alarms as they occur in real time. Alarm severity and number of impacts are displayed, and cross launch is available depending on the alarm.

1 -

The News Feed shows a Equipment Down alarm on a port. Select the alarm and choose **View in Current Alarms** from the More menu.

NSP

twork Map and Health Overview								E
Network Health View Determine the overall health of you	r network using the metrics l	below						
uipment Health e status of all network elements	Last Hour 🔹	Service Health The status of all network	k services	Last Hour 🔹	Service Configuration Health The configuration status of all net		Alarm Summary Unacknowledged root cause ala	Last Hour
0%- Poor 0. 5	0. Lted Unreachable	11, Healthy	14: Affected	0- Degraded	25 Total	9 Misaligned	32A 114t Critical Major	49A O. Minor TCAs
Health NE	s NES	Services	Services	Services	Services	Services		
					View in Service	Management	View in Cu	rrent Alarms
					View in Service	Management	View in Cu	View In Current Alarms
fected Services					View in Service	Management	News Feed	View In Current Alarms View Impacts
fected Services e which network objects are affecting s	ervices				View in Service		News Feed View unacknowledged root caus	View In Current Alarms View Impacts View Root Causes
e which network objects are affecting s By Service Sites • By Service		nel Bindings			View in Service		News Feed	View In Current Alarms View Impacts View Root Causes View Object Impacts
		nel Bindings			View in Service		News Feed View unacknowledged root caus	View In Current Alarms View Impacts View Root Causes
e which network objects are affecting s By Service Sites • By Service		nel Bindings			View in Service		News Feed View unacknowledged root cau Tairms  By TunnelDown from-92168.96.26-1d-5	View In Current Alarms View Impacts View Root Causes View Object Impacts Open in Network Inventory
ewhich network objects are affecting s By Service Sites  By Service		nel Bindings			View in Service		News Feed View unacknowledged root cau Y Alarms - = By TunnelDown	View In Current Alarms View Impacts View Root Causes View Object Impacts Open In Network Inventory View In Object Troubleshootin
ewhich network objects are affecting s By Service Sites  By Service		nel Bindings			View in Service		News Feed View unacknowledged root cau Tairms  By TunnelDown from-92168.96.26-1d-5	View In Current Alarms View Impacts View Root Causes View Object Impacts Open in Network Inventory View In Object Troubleshootin Plot utilization statistics Plot error statistics
e which network objects are affecting s By Service Sites  By Service By Servi		nel Bindings			View in Service		News Feed View unacknowledged root cau TunnelDown from 92,168,96,26-id-5 Impact: 3 EquipmentAdministrativ Port 1/1/c1/2	View in Current Alarms View Impacts View Root Causes View Object Impacts Open in Network Inventory View in Object Troubleshootin Plot utilization statistics Plot error statistics Plot error statistics

Current Alarms opens, showing the current alarm.

		es Platform												nin	•	?
Network Map and I	Health Current	t Alarms 👻													Ģ	
Unsaved Ac	dvanced Filter 🛛 🗙				Total Unfiltered Alarms:	G ()	<b>0</b> 6 49	♥ 0 78 0	0	0 0 1 0	0		0		T,	
everity	Impact	Last Time Detected	Alarmed Object Type		Alarmed Object Name					larm Name	:	~	General			
т T,	Τ.	YYYY-MM-D - YYYY-MM-D 🖬		۳.				τ,	<b>Ç</b>			~	Severity			
3	2	2023/11/3 06:05:23 PM GMT+04:00	equipment.PhysicalPort		Port 1/1/c1/2				8	quipmentAdn	nin 🚦	~	Sevency			
												~	Acknowledgement			
												~	Acknowledgement Notes			
												~	Statistics			
												^	Description			
												^	Remedial Action			
												^	Remedial Action			
												^	Remedial Action			
												~	Remedial Action			
												~	Raising Condition			
												~	Raising Condition			

#### 5.10.4 Investigate from the Ports data page

Viewing the port in the Ports list on the Network Map and Health dashboard will show us some configuration and state details.

1

From **Overview** in the **Network Map and Health** dashboard, scroll down and expand the **Ports** dashlet and filter on the port being investigated.

twork Map and Health	Overview	÷									E.
Network Inventory	View										
View detailed informat	View tion relating to your network of	bjects									
etwork Elements		к <sup>л</sup>	Links		е <sup>ж</sup>	Ports		٢	Services		
ime	Operational State		Name	Operational State		Name	Operational State		Name	Operational State	
dNodeE	enabled	î	mdNodeE:1/1/c1/10md	disabled	î	Port 1/4/5	disabled	î	Epipe-5002	disabled	
ssicNodeB	enabled		classicNodeB:1/1/1class	enabled		1/2/c12	disabled		VPLS 5005	enabled	
dNodeD	enabled		classicNodeB:1/1/2Unm	enabled		1/1/c27	disabled		ELINE_Demo	disabled	
assicNodeC	enabled	-	classicNodeB:1/1/11vsr	enabled		Port 1/4/10	disabled	-	EPIPE 6004	disabled	
ervice Sites		к <sup>77</sup>	Service Endpoints		и <sup>ж</sup>	Tunnel Bindings		κ <sup>3</sup>			
ime	Operational State		Name	Operational State		Name	Operational State				
ls-5006	disabled	î	toCE2-ies-5201	disabled	î	92.168.96.26-circuit-5-50	disabled	î			
ipe-6004	disabled		Port 1/1/c1/8:501.0	disabled		92.168.96.26-circuit-4-60	disabled				
ipe-5001	disabled		lag-1:502	disabled		92.168.96.26-circuit-5-50	disabled				
-5201	disabled		1/1/c1/8:67	disabled		92.168.96.7-circuit-3-6003	disabled				
Ps		1									

2 -

From the Ports list, filter on the port name in the Name column, and the NE in the NE Name column. The dashboard shows that the Operational State of the port is disabled and the Administrative State is locked.

NOKIA Ne	etwork Services Platform								Use	er: admin	•	(
twork Map and Healt	th Overview	÷									e,	
orts												:
Content updated o	on 2023/11/3 16:52:42 (Click to upda Operational State	NE ID	NE Name	Description	Administrative State	Standby State	Position	Port Index	Port Type	Port Mode	MTL	:
	T	Τ.		Τ.	Υ.	•	Τ.	. Т.				
ort 1/1/c2	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899584	connector	undefined		
ort 1/1/c3	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899648	connector	undefined		
ort 1/1/c4	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899712	connector	undefined		
ort 1/1/c5	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899776	connector	undefined		
ort 1/1/c6	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899840	connector	undefined		
ort 1/1/c7	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899904	connector	undefined		
ort 1/1/c8	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610899968	connector	undefined		
ort 1/1/c9	disabled	92.168.9	classicNodeC	QSFP-DD Conn	locked	providingService	shelf=1/slot	1610900032	connector	undefined		

Issue 2

We can continue to investigate the issue by plotting statistics. Select the port and choose (Table row actions), **Plot utilization statistics**.

twork Map and Health	n Overview		•															P.	
orts																		:	
Content updated or	n 2023/11/3 18:20:30 (Clie	k to update																	
lame	Operational Stat	e	NE ID	NE Name	Des	scription	Admi	inistrative State	e Stand	by State	Position	Po	rt Index	Port Type	2	Port Mode		MTU (I	
Port 1/1/c1/2 ×	۲.			τ.	۳.		<b>T</b> .		•	*		۲.		Τ.					
ort 1/1/c1/2	disabled		92.168.9	classicNode	C Net	twork Port	locke	ed	provid	ingService	shelf=1/slo	t	161089952	2 ethernet		trunk			
															0	View in Obj Plot utilizat Plot error s	tion stati	stics	in
															0	Plot utilizat	tion stati	stics	
etwork Elements			e <sup>n</sup>	Links				x."	Tunnel Bindings				κ <sup>n</sup> 5ι	rvices	0	Plot utilizat	tion stati	stics	4
	Operations	State	e <sup>3</sup>	Links		Operatio	unal State	× <sup>n</sup>	Tunnel Bindings Name		Operational Sta			rvices	0	Plot utilizai Plot error s	tion stati	stics ≯	4
etwork Elements me	Operations enabled	l State	x <sup>3</sup>		/10md	Operatio		x <sup>n</sup>			Operational Sta disabled		Na		0	Plot utilizai Plot error s	tion statistics statistics onal State	stics ≯	4
<b>atwork Elements</b> i <b>me</b> dNodeE		State	e <sup>3</sup>	Name				×*	Name	ult-5-50			Na Ep	ime	0	Plot utilizat Plot error s Operatio	tion stati statistics onal State	stics ≯	4
etwork Elements	enabled	l State	x <sup>n</sup>	Name mdNodeE:1/1/c1	/1class	disabled		x*	Name 92.168.96.26-circ	ult-5-50	disabled		Na Ep VF	ime ilpe-5002	0	Plot utilizat Plot error s Operatio disabled	tion stati statistics onal State	stics ≯	

4

**Data Collection and Analysis Visualizations** opens, showing several charts of utilization statistics.



Here we can see that there is no traffic. This provides additional information about what has happened.

5

We can also plot error statistics for the port. Return to the port in the **Ports** list and choose (Table row actions), **Plot error statistics**.

NOKIA Netwo	ork Services Platform												
twork Map and Health	Overview	÷											
orts													:
Content updated on 20	023/11/3 18:20:30 (Click to update Operational State	NEID	NE Name	Descriptio		Administrative Sta	ite Standby State	Position	Port Index	Port Type	e Port Mode	мти	0
Port 1/1/c1/2 × T_			r.	τ.	T.				r.	τ.	•	-	
ort 1/1/c1/2	disabled	92.168.9	classicNodeC	Network P	ort	locked	providingService	shelf=1/slot	1610899	522 ethernet	trunk		
												ject Troubleshoo	y otir
											<ul> <li>View in Ot</li> <li>Plot utiliza</li> <li>Plot error</li> </ul>	ition statistics	
		××	Links			e <sup>n</sup>	Tunnel Bindings		e <sup>2</sup>	Services	Plot utiliza	tion statistics statistics	oti
twork Elements	Operational State		Links	OF	erational Sta		Tunnel Bindings Name	Operational State	e <sup>n</sup>	Services	<ul> <li>Plot utiliz</li> <li>Plot error</li> </ul>	tion statistics statistics	otii
twork Elements me	Operational State enabled				erational Sta		-	Operational State disabled	x <sup>3</sup>		<ul> <li>Plot utiliz</li> <li>Plot error</li> </ul>	tion statistics statistics • • •	otii
e <b>twork Elements</b> me dNodeE			Name	0md dis			Name		2	Name	<ul> <li>Plot utilizz</li> <li>Plot error</li> </ul>	tion statistics statistics onal State d	otir
etwork Elements ame dNodeE assicNodeB dNodeD	enabled		Name mdNodeE:1/1/c1/1	0md dis class en	abled		Name 92.168.96.26-circuit-5-50	disabled	2	Name Epipe-5002	<ul> <li>Plot utilizz</li> <li>Plot error</li> </ul>	tion statistics statistics	

Another **Data Collection and Analysis Visualizations** tab opens, charting multiple error statistics counters, for example, received bad or discarded packets. For this port, there are no errors being recorded.



## 5.10.5 Investigate using the Object Troubleshooting dashboard

1

You can cross-launch the **Object Troubleshooting** dashboard in context from the **Ports** data page in the **Network Map and Health** dashboard.

NSP

= NOKIA Net	work Services Platforr	n															User:	admin		•	0
Network Map and Health	Overview		·																1	E,	:
Ports																				:	
Content updated on	2023/11/3 16:54:27 (Click	to update)																			
Name	Operational State		NE ID		NE Name		Description		Administrative State		Standby State	Position		Port Index		Port Type		Port Mode		MTU (I	:
Port 1/1/c1/2 ×	τ.			Τ.,		₹.		Τ.		•	•		Ϋ.		۳.,		•		•		
Port 1/1/c1/2	disabled		92.168.9		classicNodeC		Network Port		locked		providingService	shelf=1/slo	it	16108995	522	ethernet		trunk			:
																	•	<ul> <li>View in Currer</li> <li>Open in Netw</li> <li>View in Object</li> <li>Plot utilization</li> <li>Plot error stat</li> </ul>	ork Inve t Trouble n statist	entory eshoot	

2 -

From the Current Health Summary dashlet in the Object Troubleshooting dashboard, click **Open in NE Inventory**.

NOKIA Network Services Platform			User: admin 👻 🕜
Object Troubleshooting > Port Port 1/1/c1/2 Troubleshooting			CHANGE TARGET 49
Troubleshooting Summary Board View troubleshooting summary information			
Port Overview Summary information for the selected port		Equipment Overview Summary information for the selected port equipment	
Port Type: ethernet		Position: shelf=1/slot=1/card=	
Port Mode: trunk		Product: 7750 SR	
Management Address: 135.121.151.102		Chassis Type: 7750 SR-2s	
System Address: 92.168.96.26		Version: TiMOS-C-22.7.R2	
Location: N/A		Manufacture Date: N/A	
Current Health Summary Health status for the selected port	Alarm Summary Alarms and impacts for the selected port	Analytics Reports Run Analytics Reports	
Operational State: enabled		Port	
Administrative State: unlocked		Port Throughput Summary	
Availability State: N/A			
NE Communication State: up	Critical Major TCAs Total Impacts		
	impacts		
Open in NE Inventory	View in Current Alarms		

The port is selected, and additional information is shown in the **Info** panel regarding the operational state and administrative state of the port.

NOCIA Network Services Platform		User: admin 🗸
rentory > Network Element classicNodeC		
uipment type filters	*	() ÉE
perational State: All + Administrative State: All + APPLY FILTERS	^ Prop	perties
<ul> <li>ClassicNodeC, Operational State: enabled, Administrative State: unlocked</li> </ul>	NE Nam Port 1	™ /1/c1/2
Card Slot - 1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	NE Dese Netwo	cription Irk Port
Card - 1, Operational State: enabled, Administrative State: unlocked	Operati	ional State ed
Xiom Card Slot - 1/x1 (notExpectedNotinstalled), Operational State: disabled (notinstalled), Administrative State: unlocked	invento	ry_property_displayedOperState ed
👻 📕 Daughter Card Slot - 1/1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	Adminis locked	strative State
Daughter Card - 1/1, Operational State: enabled, Administrative State: unlocked	Standby provid	y State ingService
👻 🛄 Port 1/1/c1, Operational State: enabled, Administrative State: unlocked	Position	n 1/slot=1/card=1/slot=1/card=1/port=c1/p
Ref 1/1/c1/1, Operational State: enabled, Administrative State: unlocked	MAC Ad CO-5C	Idress -01-01-00-02
Ref 1/1/c1/2, Operational State: disabled, Administrative State: locked	Port Ind 16108	dex 199522
Port 1/1/c1/3, Operational State: enabled, Administrative State: unlocked	Port Typ ethern	
Port 1/1/c1/4, Operational State: disabled, Administrative State: unlocked	Port Mo trunk	de
Port 1/1/c1/5, Operational State: disabled, Administrative State: unlocked	Encaps: dot1q	ulation Type
Port 1/1/c1/5, Operational State: disabled, Administrative State: unlocked	нти (b) 8704	rtes)
Port 1/1/c1/7, Operational State: disabled, Administrative State: unlocked	Rate UneRat	te
	Actual F A Back to top	Rate (kbps) 0000
Auto-refresh Last Refresh: 2023/11/3 19:11:34	State Re	asons

## 5.10.6 Check infrastructure configuration management details

1

If the NE was configured using Infrastructure Configuration Management, we can check for a misalignment in the **Device Management**, **Configuration Deployments** view. Navigate to **Device Management**.

NETWORK FUNCTIONS				
Network Map and Health				
Object Troubleshooting		÷.	0	i=
Current Alarms		Ŧ		-
OAM Tests			∧ Properties	
Device Management	tate: All - APPLY FILTERS			
1odel Driven Configurator	Administrative State: unlocked	: 1	NE Name Port 1/1/c1/2	
letwork Mediation	perational State: enabled, Administrative State: unlocked		NE Description	
VaveSuite - Network Operations Center	perational brace, enabled, Administrative brace, unocked		Network Port	
P/Optical Coordination	d, Administrative State: unlocked	:	Operational State	
ata Collection and Analysis			disabled	
	ctedNotinstalled), Operational State: disabled (notinstalled), Administrative State: unlocked	:	inventory_property_displayedOperState disabled	
ervice Management	ledAndExpected), Operational State: enabled, Administrative State: unlocked	:	Administrative State	
ath Control			locked	
ROGRAMMING	tional State: enabled, Administrative State: unlocked	:	Standby State providingService	
letwork Intents	al State: enabled, Administrative State: unlocked		Position	
Vorkflows			shelf=1/slot=1/card=1/slot=1/card	d=1/port=c1/po
ISP ADMINISTRATION	rational State: enabled, Administrative State: unlocked	:	MAC Address C0-5C-01-01-00-02	
ise administration system Health	rational State: disabled, Administrative State: locked		Port Index	
ap Layouts and Groups	rational State: disabled, Administrative State: locked	:	1610899522	
ile Server	rational State: enabled, Administrative State: unlocked	:	Port Type	
sers and Security			ethernet	
rtifacts	rational State: disabled, Administrative State: unlocked	:	Port Mode trunk	
rtiracts	rational State: disabled. Administrative State: unlocked		Encapsulation Type	
			dot1q	
	rational State: disabled, Administrative State: unlocked	:	MTU (bytes) 8704	
	rational State: disabled, Administrative State: unlocked	1	Rate	
	reconstructor unseureu, AUMINISTRUTE State: UNIOCKEO	:	, lineRate	
			Actual Rate (kbps)	
		A Back to top	1000000	
			State Reasons	

2 -

In **Device Management**, select **Configuration Deployments** to view the deployed configurations.

													User: ad		-
Device Management	Managed Network Elements -														
achability	Devices Managed Network Elements		Management IP		NE ID		Product		Chassis		Software Version	:	0	*	<u>n</u>
	ZTP Process	Τ.		Τ.		۲.		Τ.		Τ.		1	Select an NE to	ono the dataile	
Reachable	Configuration		135.121.153.11		92.168.96.7		7750 SR		7750 SR-12		TIMOS-B-21.5.R2	:	Select all NE to	see the details	
Reachable	Configuration Deployments		135.121.152.20		92.168.96.16		7750 SR		7750 SR-14s		TiMOS-C-21.10.R12	:			
Reachable	Configuration Templates		135.121.157.2		92.168.96.60		7750 SR		7750 SR-7s		TiMOS-C-22.10.R6	:			
Reachable	Operation		135.121.151.102		92.168.96.26		7750 SR		7750 SR-2s		TiMOS-C-22.7.R2	:			
	All Operations														
	Operation Schedules														
	Operation Types														
	Node Images														
												4 )			

**Configuration Deployments** opens. Click on the port to see information about the port deployment. The Deployment Status column shows the status after the last alignment performed.

306

ce Management Configuratio	on Deployments 🛛 👻							+ DEPLOYMENT
Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	(i) Deployment Details
•	•	Τ.	Τ.	Τ.	Τ.	•		NE Name
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Port 1/1/c1/2	Default Ethernet Port	Physical	Port	classicNodeC
<ul> <li>Deployed Aligned</li> </ul>	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	1/1/c1/2	Default Ethernet Port	Physical	Port	92.168.96.26
								Identifier
								Port-ID Port 1/1/c1/2
								Deployment Status • Deployed Aligned
								AUDIT ALIGN
								Last Audit
								Nov 2, 2023 4:43:17 pm by admin
								VIEW RESULT
								Last Alignment Nov 2, 2023 1:54:27 pm by admin
								Template Name Default Ethernet Port
								Created Nov 2, 2023 1:52:20 pm
								Last Updated Nov 2, 2023 1:54:27 pm
								Role Physical
								Category
								port Configuration Status
							▶ 4	

Let's audit the configuration to compare the configuration of the port in the NSP to the configuration that is present in the network. Click **AUDIT** in the Deployment Details panel.

)evi	ce Management Configurati	on Deployments 👻								+ DEPLOYMENT C+
	Deployment Status	Configuration Status	NE Name	NEID	Identifier	Template	Role	Category	:	(i) Deployment Details
	· ·	•	Τ.	Τ.	Τ.	Τ.	•			NE Name
	<ul> <li>Deployed Aligned</li> </ul>	Modified	classicNodeC	92.168.96.26	Port 1/1/c1/2	Default Ethernet Port	Physical	Port	:	classicNodeC
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	1/1/c1/2	Default Ethernet Port	Physical	Port	:	92.168.96.26
										Identifier
										Port-ID Port 1/1/c1/2
										Deployment Status Deployed Aligned
										AUDIT ALIGN
										Last Audit Nov 2, 2023 4:43:17 pm by admin
										VIEW RESULT
										Last Alignment Nov 2, 2023 1:54:27 pm by admin
										Template Name Default Ethernet Port
										Created Nov 2, 2023 1:52:20 pm
										Last Updated Nov 2, 2023 1:54:27 pm
										Role Physical
										Category port
i i									• •	Configuration Status <ul> <li>Modified</li> </ul>
		: 2023/11/3 19:20:16		102	< Page: 1 /1 >	20		Courr		Houned

When the audit completes, we see that the deployment is misaligned. The configuration on the port is different from the configuration in **Device Management**.

Click VIEW RESULT for more details.

levi	ce Management Configuration	on Deployments 🔹 👻								+ DEPLOYMENT C+
	Deployment Status	Configuration Status	NE Name	NE ID	Identifier	Template	Role	Category	:	(i) Deployment Details
			τ.	Τ.	Τ.	Τ.	•			NE Name
	<ul> <li>Deployed Misaligned</li> </ul>	<ul> <li>Modified</li> </ul>	classicNodeC	92.168.96.26	Port 1/1/c1/2	Default Ethernet Port	Physical	Port	:	classicNodeC
	Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.16	1/1/c1/2	Default Ethernet Port	Physical	Port	:	92.168.96.26
										Identifier
										Port-ID Port 1/1/c1/2
										Deployment Status • Deployed Misaligned
										AUDIT ALIGN
										Last Audit Nov 3, 2023 7:21:44 pm by admin
									Ý	VIEW RESULT
										Last Alignment Nov 2, 2023 1:54:27 pm by admin
										Template Name Default Ethernet Port
										Created
										Nov 2, 2023 1:52:20 pm
										Nov 2, 2023 1:54:27 pm
										Role Physical
										Category
										port Configuration Status
4	6								• •	<ul> <li>Modified</li> </ul>
	Auto-refresh Last Refresh:	2023/11/3 19:27:13			< Page: 1 /1 > )			Count	: 2	

The audit results show a state mismatch for the port.

NOKIA Network Services Platform			User: admin	• ⑦
Audit Result from Nov 3, 2023 7:21:44 pm				С×
MISALIGNED ATTRIBUTES MISALIGNED OBJECTS				
Attribute	Expected Value (Template)	Actual Value (NE)		
equipment.PhysicalPort[network:92.168.96.26:shelf-1:cardSlot-1:card:daughterCardSlot-1:daughterCard:conn-1:port-2]administrativeState	portInService	portOutOfService		

CANCEL ALIGN ALL CONFIG

7

The port configuration can be aligned by clicking on ALIGN ALL CONFIG in the audit result.

NOCIA Network Services Platform			User: admin	•	0
Audit Result from Nov 3, 2023 7:21:44 pm				G	×
MISALIGNED ATTRIBUTES					
Attribute	Expected Value (Template)	Actual Value (NE)			
equipment. PhysicalPort]network:52.168.96.26.shelf-1.cardSlot-1.card.daughterCardSlot-1.daughterCardslot-1.port-2 administrativeState	portinService	portOutOfService			

#### 5.10.7 Verify the results

1 -

After the audit is completed, we can check that the problem has cleared. **Device Management** shows that the configuration is now aligned:

ce Management Configurat	ion Deployments 🔹										+ DEPLOYMENT
Deployment Status	Configuration Status	NE Name	NE ID		Identifier		Template	Role	Category	v :	(i) Deployment Details
			τ.	Τ.		Τ.	T.	-			NE Name
Deployed Aligned	Modified	classicNodeC	92.168.96.2	6	Port 1/1/c1/2		Default Ethernet Port	Physical	Port	:	classicNodeC
Deployed Aligned	<ul> <li>Modified</li> </ul>	mdNodeE	92.168.96.1	6	1/1/c1/2		Default Ethernet Port	Physical	Port	:	NEID 92.168.96.26
											Identifier
											Port-ID Port 1/1/c1/2
											Deployment Status Deployed Aligned
											AUDIT ALIGN
											Last Audit Nov 3, 2023 7:21:44 pm by admin VIEW RESULT
											Last Alignment Nov 3, 2023 7:32:50 pm by admin
											Template Name Default Ethernet Port
											10000-0000
											Created Nov 2, 2023 1:52:20 pm
											Nov 2, 2023 1:52:20 pm Last Updated
											Nov 2, 2023 1:52:20 pm Last Updated Nov 3, 2023 7:32:50 pm Role

**Inventory** shows the port in green, with Operational State enabled and Administrative State unlocked:

NOCIA Network Services Platform	User: adm	in 👻
antory > Network Element classicNodeC		
ipment type filters	÷ ()	≜= =
erational State: All - Administrative State: All - APPLY FILTERS	^ Properties	
classicNodeC (7750 SR-2s), Operational State: enabled, Administrative State: unlocked	NE Name Port 1/1/c1/2	
B Equipment Group	NE Description Network Port	
ClassicNodeC, Operational State: enabled, Administrative State: unlocked	Operational State enabled	
Card Slot - 1 (installedAndExpected), Operational State: enabled, Administrative State: unlocked	inventory_property_d enabled	displayedOperState
Card - 1, Operational State: enabled, Administrative State: unlocked	Administrative State unlocked	
Xiom Card Slot - 1/x1 (notExpectedNotInstalled), Operational State: disabled (notInstalled), Administrative State: unlocked	Standby State providingService	
👻 📗 Daughter Card Slot - 1/1 (InstalledAndExpected), Operational State: enabled, Administrative State: unlocked	Position shelf=1/slot=1/car	rd=1/slot=1/card=1/port=c1/p
Daughter Card - 1/1, Operational State: enabled, Administrative State: unlocked	MAC Address C0-5C-01-01-00-0	02
Finit Port 1/1/c1, Operational State: enabled, Administrative State: unlocked	Port Index 1610899522	
Port 1/1/c1/1, Operational State: enabled, Administrative State: unlocked	Port Type ethernet	
Port 1/1/c1/2, Operational State: enabled, Administrative State: unlocked	Port Mode trunk	
Port 1/1/c1/3, Operational State: enabled, Administrative State: unlocked	Encapsulation Type dot1q	
Port 1/1/c1/4, Operational State: disabled, Administrative State: unlocked	MTU (bytes) 8704	
Port 1/1/c1/5, Operational State: disabled, Administrative State: unlocked	Rate 	
	Actual Rate (kbps) 10000000	
Auto-refresh Last Refresh: 2023/11/3 19:34:38	State Reasons	

The **Object Troubleshooting** dashboard shows the Major alarm cleared and Operational and Administrative states as expected:

NSP

Troubleshooting Summary Board Select a port to view troubleshooting summary information		
Port Overview		
ee the summary information for the selected port	Equipment Overview See the summary information of the selected port equipment	
Port Type: ethernet	Position: shelf=1/slot=1/card=	
Port Mode: trunk	Product: 7750 SR	
Management Address: 192.168.97.146	Chassis Type: 7750 SR-2s	
System Address: 92.168.96.26	Version: TiMOS-C-22.7.R2	
Location: N/A	Manufacture Date: N/A	
Current Health Summary Alarm Summary See what object you are troubleshooting and how healthy it is See alarms and impacts for the selected port	Analytics Reports Run Analytics Reports	
Operational State: enabled	Port	
Administrative State unlocked	Port Throughput Summary	
Availability State: N/A 0 0 0		
NE Communication State: up Critical Major TCAs Total Impacts		

Clicking **View in Current Alarms** from the **Object Troubleshooting** dashboard takes you to the alarm list, where the Equipment Down alarm no longer appears.

work Map and	Health Cu	irrent Alarms	-														Q
Unsaved A	dvanced Filter	× :					Total Unfiltered Alarms:	<b>G</b> 31	123	(1) (1) (1) (1) (1) (1) (1) (1) (1) (1)	0	(	0 1 0	0	0	τ,	
erity	Impact	Last 1	ime Detected	Alarmed Objec	t Type		Alarmed Object Name					Ala	arm Name	:	∽ General		
- T.		<b>T</b> . YYY	Y-MM-E - ҮҮҮҮ-ММ-			<b>T</b> .,					Τ.				<ul> <li>Severity</li> </ul>		
															<ul> <li>Acknowledgement</li> </ul>		
															<ul> <li>Acknowledgement Notes</li> </ul>		
															<ul> <li>Statistics</li> </ul>		
															<ul> <li>Description</li> </ul>		
															^ Remedial Action		
															✓ Raising Condition		
															<ul> <li>Clearing Condition</li> </ul>		
															<ul> <li>Additional Text</li> </ul>		
															✓ Custom Text		

#### The Ports list in the Network Map and Health dashboard shows the updated port states:

twork Map and	Health Overview		•									E,	
orts													:
Content upda	ited on 2023/11/3 18:14:42 (Clic	k to update)											
ime	Operational State	NE ID	NE Name	Description	Adminis	istrative State	Standby State	Position	Port Index	Port Type	Port Mode	MTU (byte	e
T	· ·	T	×	r	×T			T	T		*		
t 1/1/	enabled	92.168.9	classicNodeC	Network Port	unlocke	ed	providingService	shelf=1/slot	1610899522	ethernet	trunk		
									_			•	
twork Eleme	ents	×*	Links			× <sup>3</sup>	Tunnel Bindings		u <sup>n</sup> S	ervices			
	ents		Links		Operational State		Tunnel Bindings Name	Operational State		ervices	Operation		
ne			Name	/1/c1/8mdN	Operational State disabled		2000-000-000-000-000-000-000-000-000-00	Operational State	N		Operation		
ne NodeE	Operation		Name mdNodeE:1	/1/c1/8mdN		i	Name		N Ei	ame			
rtwork Elemen me iNodeE ssicNodeB iNodeD	Operationa		Name mdNodeE:1 mdNodeE:1		disabled	Î	Name 92.168.96.7-circuit-3-3322	disabled	N EI EI	ame plpe-5002	disabled		4 ×

The News Feed also shows that the Equipment Down alarm has cleared:

NOCIA Network Services Platform					User: admin	•
Network Map and Health Overview -						
Network Health View Determine the overall health of your network using the metrics	below					
Equipment Health The status of all network elements	Service Health The status of all network services		Service Configuration Healt The configuration status of all ne		Alarm Summary Unacknowledged root cause alarms	Last Hour
0% 0. 5. 0. Network Healthy NEs Affected Unreschable NEs NEs NEs	11- Healthy Affected Services Services	0. Degraded Services	25 Total Services	9 Misaligned Services	27. Critical Major Minor	O. TCAs
			View in Servic	ce Management	View in Current Alarm:	5
Affected Services See which network objects are affecting services				Last Hour 🔹	News Feed View unacknowledged root cause alarms as th	ey occur
By Service Sites  By Service Endpoints By Tun	nel Bindings				Y Alarms • Ev Impact •	
12					EquipmentDown Port 1/1/4 Impact: 1	2 days ago 🚦
10 88 8 8 8					EquipmentDown Port 1/1/c1/6 Impact: 1	2 days ago
					EquipmentDown Port 1/1/c1/7 Impact: 1	2 days ago 🚦

Returning to **Data Collection and Analysis Visualizations**, we can also see that the traffic on the port has resumed.



# **Troubleshooting using Analytics**

## 5.11 Analytics troubleshooting overview

#### 5.11.1 Troubleshooting

An effective troubleshooting model for solving Analytics report problems includes the following tasks:

- Eliminate the possibility of a hardware or network problem. For example, if you are having trouble with a Port Throughput report, verify that the port is up.
- Check the report description in this guide for the report-specific requirements, such as statistics, aggregation, or policies that must be in place.
- Verify that the NE is generating the required files. For example, if the report requires a statistic, verify that counters for that statistic are being generated.
- Categorize the problem.

The following are the most common categories of problems affecting reports:

- Data collection issues
- Data storage issues
- Report generation issues
- Plan corrective action and resolve the problem.
- Verify that the problem is resolved.

## 5.12 Troubleshooting data collection

#### 5.12.1 Statistics collection for Application Assurance reports

A blank report may be due to a statistics collection issue, or a prompt selection that excludes all available data.

The description of the report shows the statistics type required for the report, and whether NSP flow collection is required. Table 5-1, "Troubleshooting statistics collection for Application Assurance reports" (p. 320) describes options for checking statistics collection.

Statistics type	Items to verify	See
AA accounting	<ul> <li>Are required policies in place?</li> <li>Are statistics being collected?</li> <li>What is the accounting retrieval status of the NE?</li> <li>Is additional information available from server performance statistics?</li> </ul>	"Workflow for accounting statistics collection" in the NSP NFM-P Statistics Management Guide "Workflow for server performance statistics collection" in the NSP NFM-P Statistics Management Guide "To view the accounting statistics collection status of an NE" in the NSP NFM-P Classic Management User Guide
AA Cflowd	<ul> <li>Has AA Cflowd sampling been configured?</li> <li>Are required policies in place?</li> </ul>	"To enable and configure global Cflowd sampling on an NE" in the NSP NFM-P Classic Management User Guide "To configure Cflowd collectors on an ISA-AA group or partition" in the NSP NFM-P Classic Management User Guide "To configure an AA Cflowd group policy" in the NSP NFM-P Classic Management User Guide "Workflow to configure flow statistics collection" in the NSP NFM-P Statistics Management Guide If the report requires special study statistics collection, see "Workflow to configure AA Cflowd special study statistics collection" in the NSP NFM-P Statistics Management Guide
Subscriber	<ul><li>Are required policies in place?</li><li>Are statistics being collected?</li></ul>	"To configure AA subscriber statistics collection on an ISA-AA group or partition" in the NSP NFM-P Classic Management User Guide

Table 5-1 Troubleshooting statistics collection for Application Assurance reports

# 5.12.2 Statistics and data collection for Network and Service reports and NSP reports

A blank report may be due to a statistics collection issue, or a prompt selection that excludes all available data.

The description of the report shows the statistics or data type required for the report, and any other prerequisites that may apply. Table 5-2, "Troubleshooting statistics and data collection for Network and Service reports and NSP reports" (p. 321) describes options for checking collection.

Statistics type	Items to verify	See
Accounting (also known as XML statistics)	<ul> <li>Are required policies in place?</li> <li>Are statistics being collected?</li> <li>Are required aggregators configured?</li> </ul>	"Workflow for accounting statistics collection" in the <i>NSP NFM-P</i> <i>Statistics Management Guide</i> "How do I configure analytics aggregation?" in the <i>NSP Analytics</i> <i>Report Catalog</i>
Performance (SNMP) data	<ul> <li>Are required policies in place?</li> <li>Is SNMP connectivity established between the NE and the NFM-P?</li> <li>Are required statistics being collected?</li> <li>Are required aggregation rules enabled?</li> <li>Alarms: if the system cannot collect and process all performance statistics in the specified polling period, the PollerDeadlineMissed alarm will be raised.</li> </ul>	"How do I configure analytics aggregation?" in the <i>NSP Analytics</i> <i>Report Catalog</i>
IPFIX (also called System Cflowd or Netflow v10)	<ul><li> Has IPFIX sampling been configured?</li><li> Are required policies in place?</li></ul>	"Workflow to configure flow statistics collection" in the NSP NFM-P Statistics Management Guide
OAM data	<ul> <li>Is OAM testing configured in the NFM-P?</li> <li>Are required policies in place?</li> <li>Are OAM aggregation rules enabled?</li> </ul>	"How do I configure analytics aggregation?" in the <i>NSP Analytics</i> <i>Report Catalog</i>
Event data for Uptime reports	<ul> <li>Is an event log policy in place with an appropriate retention time for assurance events?</li> <li>Are maintenance windows configured appropriately?</li> </ul>	"To configure an event log policy" in the NSP NFM-P Classic Management User Guide "To create and manage custom auxiliary database table attributes" in the NSP System Administrator Guide

Table 5-2	Troubleshooting statistics and data collection for Network and Service reports and NSP
	reports

## 5.12.3 NSP auxiliary database

If you suspect an auxiliary database problem, you can run the following script on an auxiliary database station to collect log files for technical support:

/opt/nsp/nfmp/auxdb/install/bin/auxdbAdmin.sh getDebugFiles

#### 5.12.4 NFM-P main database

For Inventory reports, the NFM-P main database must be operational and able to receive files from NEs.

To confirm that files are being received and stored, monitor the following folder on the standalone or primary main server to ensure that new statistics files are being generated:

/opt/nsp/nfmp/server/xml\_output

## 5.13 Troubleshooting data storage

#### 5.13.1 OAM test result storage

For OAM test reporting, the OAM test results must be stored in the auxiliary database, which requires that the oam-test-results parameter is enabled in the samauxdb section of each NFM-P main server configuration. See the *NSP Installation and Upgrade Guide* for information about using the samconfig utility to modify the NFM-P configuration.

## 5.13.2 Statistics retention policy

Verify that the statistics retention policy is appropriate; data is unavailable for reporting if statistics are removed prematurely.

## 5.13.3 Auxiliary database log locations

Logs for each NE can be found in the following directory on an NSP auxiliary database station:

/opt/nsp/nfmp/auxdb/catalog/samdb/member\_ID\_catalog/vertica.log

where member\_ID is the ID of the auxiliary database station, for example, v\_samdb\_node0002

The following log file contains basic auxiliary database status information:

/opt/nsp/nfmp/auxdb/install/proxy/log/EmsAuxDbProxy.log

## 5.13.4 Assurance event logging

If an NSP auxiliary database is present, assurance events are recorded in the following auxiliary database table:

samdb.assurance\_assuranceevent

If no auxiliary database is present, assurance events are recorded in the following main database table:

PsoAssuranceEvent obj\_199a4deb

# 5.14 Troubleshooting Analytics reporting

## 5.14.1 Configuring NSP Analytics logging

By default, NSP Analytics logs only errors, but additional logging options are available. For example, the SQL log shows the data table names so that you can verify that the table for your report is requesting and receiving timed frame data to generate reports.

See "How do I manage NSP Analytics logging?" in the *NSP System Administrator Guide* for information about enabling various NSP Analytics log levels.

#### 5.14.2 Additional troubleshooting options

The following may assist with troubleshooting Analytics reporting:

- See "Using Analytics" in the *NSP Analytics Report Catalog* to ensure that the reporting criteria are correctly specified. For example, all data for a report must be collected using the same collection interval.
- Verify the connectivity between the NSP cluster, NSP auxiliary database, and other system elements.
- If a report takes a long time to create, or generates errors, try reducing the number of objects in the data set.

# Troubleshooting using NSP workflows

## 5.15 Evaluating failed or slow workflow executions

#### 5.15.1 Purpose

This article shows you how to evaluate failed or slow workflow executions and troubleshoot the source of workflow errors.

#### 5.15.2 Parent workflows and sub-workflows

Workflows may call other workflows as part of their execution. Both the parent workflow and the sub-workflow appear in the Workflow Execution list.

If a workflow execution's **Executed by** parameter is blank, the workflow was executed by another workflow, as shown in the following figure.

= N	OCIA Network Services Pla	tform					User: admin	•	0
Workflows	Workflow Executions	•							G
T All	•								
Status	Workflow Name	Created	Run Time	Description	Executed By	Worker			
		T			T				
8	LSO_7x50_Backup	2 days ago	20s	execution_identifier =/nsp-lso-operati	. nsp_internal_system_user	lsom	Parent workflow		:
8	LSO_7x50_Backup_MD_Mixed	2 days ago	19s	execution_identifier =/nsp-lso-operati		lsom	Sub-workflow		:
0	LSO_Transfer_Files_NE	2 days ago	1s	execution_identifier =/nsp-lso-operati		Isom			:
0	LSO_Transfer_Files_NE	2 days ago	2s	execution_identifier =/nsp-lso-operati		lsom			:

Note the Created field for these example executions. The  $LSO_7x50_Backup_MD_Mixed$  sub-workflow execution was created at the same time as the  $LSO_7x50_Backup$  workflow execution. The  $LSO_7x50_Backup$  may be the parent workflow that created this failed execution.

Start your troubleshooting with a parent workflow to ensure that you see all the relevant information.

## 5.15.3 Check the information page of a successful execution

If you have an example of a successful execution of the workflow, it can help you narrow your search for the source of issues with slow or failing workflows.

1 -

Double click on a successful workflow execution. The Execution info page displays.

2 —

Choose **Flow** from the **Info** drop-down. The Flow diagram shows the sequence of tasks performed when the workflow was executed.

NSP


Hover over the icons on each task for more information on the task type. In this example, decideMode is a message action, and runBackupOnMdNode is a sub-workflow.

3

Expand the panel at the right of the screen for further details:

Click ORun Time to see the run time for each task.

Δ

<ul> <li>Selec</li> </ul>	t a task and click	Action	Executions	to see t	the list of	actions	executed b	by the tasl	k.
---------------------------	--------------------	--------	------------	----------	-------------	---------	------------	-------------	----

For this example, runBackupOnMdNode represents most of the runtime of the workflow, and it took 16 seconds to run. This provides expected behavior to compare to a workflow that may be running slowly.

The list of actions performed also shows whether the workflow is transferring files, calling APIs, or communicating with other applications. Problems with any of these could be the cause of a slowdown or failure.

Double-click on a sub-workflow task to see the execution status.

≡ NO <ia netv<="" th=""><th>vork Services Platform</th><th></th></ia>	vork Services Platform	
Execution -		8111 Flow -
Execution	Status	
c270b738-7cc7-4f13	SUCCESS	
∢ runBackupOnMdN…	1	>
SUCCESS 몸		
SUCCESS		
backupSuccessful		
SUCCESS		

Double click on the execution status to open the info page for the sub-workflow execution in a new tab, and investigate actions and tasks executed by the sub-workflow.

END OF STEPS -

# 5.15.4 Check the process of a slow workflow

1 -

Double-click on a workflow execution, and select **Tasks** from the Info drop-down. The Tasks list shows the time stamps when each task was created, and each task's run time.

The Created column shows the time since the task was created. Hover over a time in the Created column to see the precise time of creation.

2 —

Check for delays in the sequence of tasks. For example, if one task was created at midnight and had a run time of 2 seconds, the following task should be created at 2 seconds after midnight.

3 —

If there are delays, NSP is experiencing slowness due to memory usage. When database usage is high, it takes longer than expected to query the database for the next action.

If you are experiencing these delays, your cleanup policy may need to be adjusted. For more information, see the *NSP Network Automation Guide*.

END OF STEPS -

## 5.15.5 Check concurrency

If a workflow is experiencing slowdowns or API errors, check for tasks with loops and ensure the concurrency is set correctly. If NSP is creating too many actions at one time, the workflow database could be impacted, causing slowdowns, or APIs could be overwhelmed with too many simultaneous calls.

From the Workflows page, double click on a workflow to open the Info page. Choose **Definition** from the Info drop-down.

2 \_\_\_\_\_

In the YAML panel, search for a task with a with-item statement. The with-item statement provides the number of times the task will initiate the action.

3

Verify that any task with a with-item statement also has a concurrency property set.

<sup>1 –</sup> 

The concurrency property sets a limit on the number of times the task will create the action concurrently. For example, if the concurrency is set to 1, the task will create the action once and wait for it to complete before executing it again.

# 4 \_\_\_\_\_

Ensure that the concurrency value and the size of the with-items loop are appropriate for the task. For example, if the task is an API call, ensure that the concurrency is low enough to prevent the resource from being overwhelmed with simultaneous API calls. Remember that this workflow may not be the only entity calling the API at the time you execute it.

END OF STEPS

## 5.15.6 Check task output

If a workflow is experiencing slowdowns or getting stuck in a Running state, resource usage may be impacted by large amounts of output.

1 -

From the Workflows page, double click on a workflow to open the Info page. Choose **Definition** from the Info drop-down.

2 -

In the YAML panel, search for the output statements for the tasks and the workflow itself, as applicable.

3

Ensure that output for all tasks is as minimal as possible. This minimizes the database usage of each task execution and helps to prevent resource overload. For more information; see the Mistral documentation and the Best Practices section in the Network Automation tutorial on the Network Developer Portal.

END OF STEPS

## 5.15.7 Heartbeat errors

A Heartbeat not received error occurs when a workflow attempts to contact an API or NSP and no response is received within ten minutes. Check logs to verify the source of the error.

#### 1

Check the logs for the Mistral executor to see whether responses were received from the other entity.

#### 2 –

Check logs for the RabbitMQ messaging bus to see whether there was an interruption to monitoring, which may have caused Mistral to miss a response.

END OF STEPS -

# 6 Network troubleshooting using NFM-P

# 6.1 Overview

## 6.1.1 Purpose

This chapter provides information about troubleshooting a managed network using the NFM-P.

# 6.1.2 Contents

6.1 Overview	331
Troubleshooting services and connectivity	333
6.2 Service and connectivity diagnostics	333
6.3 Workflow to troubleshoot a service or connectivity problem	333
6.4 To identify whether a VPLS is part of an H-VPLS	335
6.5 To verify the operational and administrative states of service components	336
6.6 To verify the FIB configuration	337
6.7 To verify connectivity for all egress points in a service using MAC Ping and MAC Trace	338
6.8 To verify connectivity for all egress points in a service using MEF MAC Ping	340
6.9 To measure frame transmission size on a service using MTU Ping	342
6.10 To verify the end-to-end connectivity of a service using Service Site Ping	343
6.11 To verify the end-to-end connectivity of a service tunnel using Tunnel Ping	345
6.12 To verify end-to-end connectivity of an MPLS LSP using LSP Ping	347
6.13 To review the route for an MPLS LSP using LSP Trace	349
6.14 To review ACL filter properties	350
6.15 To view anti-spoof filters	351
6.16 To retrieve MIB information from a GNE using the snmpDump utility	352
Troubleshooting using the NE resync audit function	354
6.17 NE resync auditing overview	354
6.18 Workflow for NE resync auditing	355
6.19 To clear a Frame Size Problem (MTU Mismatch) alarm	355

6.20 To perform an NE resync audit	356	
6.21 To view NE resync audit results using the NE audit manager	357	
Troubleshooting network management LAN issues	359	
6.22 Problem: All network management domain stations experience performance degradation	359	
6.23 Problem: Lost connectivity to one or more network management domain stations	359	
6.24 Problem: Another station can be pinged, but some functions are unavailable	360	
6.25 Problem: Packet size and fragmentation issues	361	
Troubleshooting using NFM-P client GUI warning messages	363	
6.26 Client GUI warning message overview	363	
6.27 To respond to a GUI warning message	364	
Troubleshooting with Problems Encountered forms		
6.28 Overview	366	
6.29 To view additional problem information	366	
6.30 To collect problem information for technical support	367	
Troubleshooting using the NFM-P user activity log	368	
6.31 User activity log overview	368	
6.32 To identify the user activity for a network object	368	
6.33 To identify the user activity for an NFM-P object	369	
6.34 To navigate to the object of a user action	370	
6.35 To view the user activity records of an object	371	
6.36 To view the user activity performed during a user session	371	

# Troubleshooting services and connectivity

# 6.2 Service and connectivity diagnostics

## 6.2.1 STM OAM diagnostics for troubleshooting

This chapter documents how to troubleshoot service and general connectivity problems when there is no associated alarm condition.

You can use the NFM-P Service Test Manager, or STM, OAM diagnostic tools for network troubleshooting and for verifying compliance with SLAs. The STM provides the ability to group OAM diagnostic tests into test suites for more comprehensive fault monitoring and troubleshooting. A test suite can perform end-to-end testing of a customer service and the underlying network transport elements. The use of test suites is especially valuable when multiple objects of the same type require testing. Test suites can be scheduled to run on a regular basis to provide continual network performance feedback. See the *NSP NFM-P Classic Management User Guide* for information about using the STM and creating scheduled tasks.

# 6.2.2 OAM diagnostics sample network

The configuration below shows a network that is used as an example for the OAM diagnostics procedures in this chapter.

#### *Figure 6-1* Sample network



BGP, OSPF, and MPLS are on each network interface.

17557

# 6.3 Workflow to troubleshoot a service or connectivity problem

## 6.3.1 Purpose

Perform the following tasks in sequence until you identify the root cause of the problem.

## 6.3.2 Stages

1

Verify that there are no alarms associated with the service by clicking on the Faults tab in the Service form.

a. If there are no alarms that affect the service, see Stage 2.

2

If you are troubleshooting a VPLS service, determine whether it is part of an H-VPLS configuration. See 6.4 "To identify whether a VPLS is part of an H-VPLS" (p. 335).

3

Verify whether the administrative and operational states of each component of the service are Up; see 6.5 "To verify the operational and administrative states of service components" (p. 336).

4

Verify the connectivity of the customer equipment using the entries in the FIB; see 6.6 "To verify the FIB configuration" (p. 337).

5

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

6

Verify the connectivity of all egress points in the service:

- a. using MAC Ping and MAC Trace; see 6.7 "To verify connectivity for all egress points in a service using MAC Ping and MAC Trace" (p. 338).
- b. using MEF MAC Ping; see 6.8 "To verify connectivity for all egress points in a service using MEF MAC Ping" (p. 340).

7 -

Use the results from the MAC Ping and MAC Trace diagnostics to choose one of the following options:

a.

If the MAC Ping, MEF MAC Ping, or MAC Trace diagnostics returned the expected results for the configuration of your network:

- 1. Measure the frame transmission size on all objects associated with the service such as the service sites, access and network ports, service tunnels, and circuits; see 6.9 "To measure frame transmission size on a service using MTU Ping" (p. 342).
- 2. Review the ACL filter policies to ensure that the ACL filter for the port is not excluding packets that you want to test; see 6.14 "To review ACL filter properties" (p. 350).

3. Verify the QoS configuration.

b.

If the MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network:

- Verify the end-to-end connectivity on the service using the Service Site Ping diagnostic; see 6.10 "To verify the end-to-end connectivity of a service using Service Site Ping" (p. 343).
- Verify the end-to-end connectivity on the service tunnel using the Tunnel Ping diagnostic; see 6.11 "To verify the end-to-end connectivity of a service tunnel using Tunnel Ping" (p. 345).
- 3. Verify the end-to-end connectivity of an MPLS LSP using the LSP Ping diagnostic; see 6.12 "To verify end-to-end connectivity of an MPLS LSP using LSP Ping" (p. 347).

c.

If the MAC Ping diagnostic returned the expected results for the configuration of your network, and the MAC Trace diagnostic did not return the expected results for the configuration of your network:

- 1. Verify that the correct service tunnels are used for the service.
- 2. Correct the service tunnel configuration, if required.
- 3. Review the route for the MPLS LSP using the LSP Trace OAM diagnostic. (For MPLS encapsulation, only.) If the LSP Trace results do not meet the requirements of your network, review the resource availability and configurations along the LSP expected routes; see 6.13 "To review the route for an MPLS LSP using LSP Trace" (p. 349).
- 8

As required, perform one or more of the following.

- a. Review ACL filter properties; see 6.14 "To review ACL filter properties" (p. 350).
- b. View anti-spoof filters; see 6.15 "To view anti-spoof filters" (p. 351).
- c. Retrieve MIB information from a GNE using the snmpDump utility; see 6.16 "To retrieve MIB information from a GNE using the snmpDump utility" (p. 352).
- 9

Contact your technical support representative if the problem persists; see Chapter 1, "NSP troubleshooting overview".

# 6.4 To identify whether a VPLS is part of an H-VPLS

## 6.4.1 Steps

1

Choose Manage  $\rightarrow$  Service  $\rightarrow$  Services from the NFM-P main menu.

2	
	Choose the service associated with the service problem.
3	
•	Click Properties. The Service form opens.
л	
-	Click on the Mesh SDP Bindings or Spoke SDP Bindings tab.
5	
Ū	Drag and drop the Service ID, VC ID, and Service Type columns to first three positions on the left side of the form.
6	
U	Sort the list by VC ID.
	If a VC ID has more than one unique Service ID, these services are involved in an H-VPLS relationship.
	a. If there are no alarms on the H-VPLS service, go to Stage 3 in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
	a. If there are no alarms on the H-VPLS service, go to Stage 3 in 6.3 "Workflow to troublesh

# 6.5 To verify the operational and administrative states of service components

## 6.5.1 Steps

1 -

Open the service properties form.

2 —

On the navigation tree, click on the site on which you want to verify the operational and administrative states of service components; expand the entries for that site.

3

Click on the site. The *service* (Edit) form opens. Review the states for the site using the Operational State and Administrative State parameters.

4

On the navigation tree, click on the L2 Access Interfaces, L3 Access Interfaces, and Mesh SDP Bindings or Spoke SDP bindings objects to review the operational and administrative states for the remaining components of the service.

#### 5 –

Use the operation and administrative states of the service components to choose one of the following options:

- a. If the operational and administrative states for all service components are Up, go to Stage 4 in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- b. If the operational state is Down and the administrative state is Up for one or more service components, the NFM-P generates an alarm. You must investigate the root problem on the underlying object.
- c. If the administrative state is Down for one or more service components, change the administrative state to Up. Go to Step 7 .
- 6

If the service problem persists, another type of service problem may be present. Perform the steps of the 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333) troubleshooting workflow.

#### 7 -

If the workflow does not identify the problem with your service, contact your technical support representative. See Chapter 1, "NSP troubleshooting overview" for more information.

END OF STEPS

# 6.6 To verify the FIB configuration

#### 6.6.1 Purpose

This procedure describes how to verify the connectivity of customer equipment on the service tunnel.

### 6.6.2 Steps

1 –

Click on the L2 Access Interfaces tab on the Services (Edit) form. A list of L2 access interfaces appears.

2 –

Double-click on a row in the list. The L2 Access Interface form appears.

3

Click on the Forwarding Control tab.

4

Click on the FIB Entries tab.

#### 5 —

Click Resync.

- a. If there is a list of FIB entries, confirm the number of entries with the customer configuration requirement. If the configuration meets the customer requirement, go to Stage 5 in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- b. If there are no FIB entries, there is a configuration problem with the customer equipment or the connection from the equipment to the service tunnel.
  - 1. Confirm that the NFM-P service configuration aligns with the customer requirements.
  - 2. Confirm that there are no problems with the customer equipment and associated configuration.

#### 6 —

If the service problem persists, another type of service problem may be present. Perform the steps of the 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333) troubleshooting workflow.

#### 7 -

If the workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS -

# 6.7 To verify connectivity for all egress points in a service using MAC Ping and MAC Trace

### 6.7.1 Steps

1 -

Choose Tools $\rightarrow$ Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2 –

Click Create.

3 -

Choose L2 Service  $\rightarrow$  Create MAC Ping from the Create contextual menu. The MAC Ping (Create) form appears.

4

i

Clear the results from the previous diagnostic session from the Results tab, if necessary.

**Note:** You must use the MAC Ping and MAC Trace diagnostic to test the service in both directions for the connection.

NSP

NSP

#### 5

Configure the required parameters for the diagnostic session and run the diagnostic.

a. You can target the MAC broadcast address of FF-FF-FF-FF-FF in the data plane to flood the service domain and receive a response from all operational service access ports. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to ping, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

b. You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping, in this case, from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6

Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. The table below lists the displayed messages.

Displayed message	Description
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.
fecNoMap (2)	The replying router has no mapping for the FEC.
notDownstream (3)	The replying router is not a downstream router.
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.
malformedEchoRequest (8)	The received echo request is malformed.
tlvNotUnderstood (9)	One or more TLVs were not understood.

Table 6-1 MAC Ping OAM diagnostic results

NSP

# 7 \_\_\_\_\_

Click Create.

8

Choose L2 Service  $\rightarrow$  Create MAC Trace from the Create contextual menu. The MAC Trace (Create) form appears.

9

Configure the required parameters for the diagnostic session and run the diagnostic. A MAC Trace shows the path, protocol, label, destination SAP, and hop count to the location of the destination MAC. Enter the service ID for the VPLS or VLL service between the sites, and the sites you want to trace, in this case, from site ID 10.1.200.51/32 to site IDs 10.1.200.52/32 and 10.1.200.53/32 using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

#### 10 –

Review the diagnostic results and assess whether the configuration meets the network requirements.

- a. If MAC Ping and MAC Trace diagnostics returned the expected results for the configuration of your network, go to Stage 7 a in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- b. If MAC Ping and MAC Trace diagnostics did not return the expected results for the configuration of your network, go to Stage 7 b in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- c. Go to Stage 7 c in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333) if:
  - MAC Ping diagnostic returned the expected result for the configuration of your network
  - MAC Trace diagnostic did not return the expected result for the configuration of your network

END OF STEPS

# 6.8 To verify connectivity for all egress points in a service using MEF MAC Ping

## 6.8.1 Steps

1 -

Choose Tools $\rightarrow$ Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

	Click Create.
3	
	Choose L2 Service $\rightarrow$ Create MEF MAC Ping from the Create contextual menu. The MEF MAC Ping (Create) form appears.
4	
	Clear the results from the previous diagnostic session from the Results tab, if necessary.
	<b>Note:</b> MEF MAC Ping must run simultaneously in both directions between the source and destination VPLS sites.
5	
	Configure the required parameters for the diagnostic session and run the diagnostic.
	You can target the specific MAC address of a service site. Enter the target MAC address of the specific site in the service that you want to ping.
	Click on the Results tab to view the list of ping responses. Double-click on a row in the list to view its details.

6

2 -

Review the results and assess whether the configuration meets the network requirements.

In particular, review the results in the Return Code column. The table below lists the displayed messages.

Table 6-2 MEF MAC Ping OAM diagnostic results

Displayed message (return code)	Description
responseReceived (1)	A response was received on the device to the OAM diagnostic performed.
requestTimedOut (5)	The OAM diagnostic could not be completed because no reply was received within the allocated timeout period.

7 -

Review the diagnostic results and assess whether the configuration meets the network requirements.

a. If MEF MAC Ping diagnostics returned the expected results for the configuration of your network, go to Stage 7 a in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

END OF STEPS -

# 6.9 To measure frame transmission size on a service using MTU Ping

## 6.9.1 Steps

1

2

Record the maximum frame transmission size for the service.

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form appears.

3

Filter to list only the source and destination routers of the service tunnel and click Search. The list of service tunnels appears.

4

Double-click on a service tunnel from the list. The Tunnel (Edit) form appears.

5

Click on the Tests tab.

6

Click on the MTU Ping tab and click Create. The MTU Ping (Create) form appears with the General tab selected. The form displays information about the service tunnel being tested and the originating tunnel ID.

**Note:** You must use the MTU Ping diagnostic to test the service in both directions for the connection.

7

Configure the required parameters for the diagnostic session. Click on the Test Parameters tab and enter the MTU value recorded in Step 1 for the MTU End Size (octets) parameter.

8

Run the diagnostic. The MTU Ping increments the datagram size until it fails to pass through the SDP (service tunnel) data path, in this case, an MTU Ping from site ID 10.1.200.52/32 to site ID 10.1.200.53/32 using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. The number of responses is determined by the incremental increase in datagram size.

9

Review the diagnostic results and assess whether the configuration meets the network requirements. Click on the Packets tab.

- a. If the Status column displays Response Received for all circuits, the service tunnel supports the configured frame transmission size for the circuit. Go to Stage 7 a 2 in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- b. If the Status column displays Request Timed Out for any of the circuits, the transmission failed at that frame size. If the frame size for the failure point is below the MTU value configured for the service, the packets are truncating along the service route. Investigate the cause of the truncated packets.

#### 10 -

If the service problem persists, another type of service problem may be present. Perform the steps of the troubleshooting workflow in this chapter.

11 -

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS

# 6.10 To verify the end-to-end connectivity of a service using Service Site Ping

### 6.10.1 Steps

1

Choose Tools $\rightarrow$ Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2 -

Click Create.

3

Choose Service  $\rightarrow$  Create Service Site Ping from the Create contextual menu. The Service site ping (Create) form appears.

**Note:** You must use the Service Site Ping diagnostic to test the service in both directions for the connection.

4

Configure the required parameters for the diagnostic session and run the diagnostic.

The originating service tunnel for the Service Site Ping is from site ID 10.1.200.51/32 to site ID 10.1.200.53/32, the other end of the service using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details.

#### 5

Review the diagnostic results and assess whether the configuration meets the network requirements. The table below lists the displayed messages.

Table 6-3	Service	Site	Pina	OAM	diagnostic results
		•		•	

Displayed message	Description	
Sent - Request Timeout	The request timed out with a reply.	
Sent - Request Terminated	The request was not sent because the diagnostic was terminated by the operator.	
Sent - Reply Received	The request was sent and a successful reply message was received.	
Not Sent - Non-Existent Service-ID	The configured service ID does not exist.	
Not Sent - Non-Existent SDP for Service	There is no SDP for the service tested.	
Not Sent - SDP For Service Down	The SDP for the service is down.	
Not Sent - Non-Existent Service Egress Label	There is a service label mismatch between the originator and the responder.	

a. If the Service Site ping passes, the routes between the two sites are complete and in an operational state. If the MAC Ping performed in 6.7 "To verify connectivity for all egress points in a service using MAC Ping and MAC Trace" (p. 338) failed:

- 1. Investigate the status of the two SAPs used for the circuit.
- 2. Correct the configuration issue related to the SAPs, if required.

If there is no configuration problem with the SAPs, the service problem is related to the MAC addresses.

The MAC address problem could be caused by the:

- · ACL MAC filter excluding the required MAC address
- · external customer equipment
- b. If the Service Site Ping fails, there is a loss of connectivity between the two sites.
  - 1. Log in to one of the sites using the CLI.
  - 2. Enter the following command:

ping <destination\_site\_ip\_address> +

where <destination\_site\_ip\_address> is the address of the other site in the route

If the CLI IP ping passes, go to Stage 7 b 2 of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

6

Use the CLI to verify that the IP address of the destination site is in the routing table for the originating site by entering:

#### show router route-table $\prec$

If the IP address for the destination site is not in the routing table for the originating site, there is an L3 or L2 problem.

- 1. Verify that the appropriate protocols are enabled and operational on the two sites.
- 2. Verify the administrative and operational states of the underlying L2 equipment, for example, ports and cards.
- 7 —

If the service problem persists, another type of service problem may be present. Perform the steps 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

8

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS -

# 6.11 To verify the end-to-end connectivity of a service tunnel using Tunnel Ping

### 6.11.1 Steps

1

Choose Manage  $\rightarrow$  Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form appears.

2 -

Filter to list only the source and destination routers of the service tunnel and click Search. The list of service tunnels appears.

3 –

Double-click on a service tunnel from the list. The Tunnel (Edit) form appears.

4 —

Click on the Tests tab.

5

Click on the Tunnel Ping tab and click Create. The Tunnel Ping (Create) form appears with the General tab displayed. The form displays information about the circuit being tested, including the originating tunnel ID.



**Note:** You must use the Tunnel Ping diagnostic to test the service in both directions for the connection.

6 —

Configure the required parameters for the diagnostic session as follows.

- The Return Tunnel parameter must specify the return tunnel ID number, because the tunnels are unidirectional.
- From the Test Parameters tab, the Forwarding Class parameter must specify the forwarding class for the service tunnel. Make sure that the forwarding classes for the service tunnels map to the QoS parameters configured for customer services, such as VLL.
- The Number of Test Probes and Probe Interval parameters must be configured to send multiple probes.

7 -

Run the diagnostic. Set the diagnostic configuration for a Tunnel Ping from site ID 10.1.200.51/32 to site ID 10.1.200.53/32 using the network in Figure 6-1, "Sample network" (p. 333), by specifying the return ID of the tunnel you want to test.

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the Tunnel Ping results form to view the diagnostic details.

8

Review the diagnostic results and assess whether the configuration meets the network requirements.

The table below lists the displayed messages.

Displayed message	Description
Request Timeout	The request timed out with a reply.
Orig-SDP Non-Existent	The request was not sent because the originating SDP does not exist.
Orig-SDP Admin-Down	The request was not sent because the originating SDP administrative state is Down.
Orig-SDP Oper-Down	The request was not sent because the originating SDP operational state is Down.
Request Terminated	The operator terminated the request before a reply was received, or before the timeout of the request occurred.
Far End: Originator-ID Invalid	The request was received by the far-end, but the far-end indicates that the originating SDP ID is invalid.
Far End: Responder-ID Invalid	The request was received by the far-end, but the responder ID is not the same destination SDP ID that was specified.
Far End:Resp-SDP Non-Existent	The reply was received, but the return SDP ID used to respond to the request does not exist.
Far End:Resp-SDP Invalid	The reply was received, but the return SDP ID used to respond to the request is invalid.

Table 6-4 Tunnel OAM diagnostic results

Table 6-4 Tunnel OAM diagnostic results (continued)

Displayed message	Description		
Far End:Resp-SDP Down	The reply was received, but the return SDP ID indicates that the administrative or operational state of the SDP is Down.		
Success	The tunnel is in service and working as expected. A reply was received without any errors.		

a. If the Tunnel Ping passes, the network objects below the tunnel are operating with no performance issues.

- b. If the Tunnel Ping fails, go to Stage 7 b 3 of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333) to verify the end-to-end connectivity of services using MPLS LSP paths, if required.
- 9 –

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

#### 10 -

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS -

# 6.12 To verify end-to-end connectivity of an MPLS LSP using LSP Ping

### 6.12.1 Steps

1 —

Choose Tools $\rightarrow$ Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears.

2 —

Click Create.

3

Choose MPLS $\rightarrow$ Create LSP Ping from the Create contextual menu. The LSP Ping (Create) form appears.

**i** Note: You must use the LSP Ping diagnostic to test the service in both directions for the connection.

4

Configure the required parameters for the diagnostic session and run the diagnostic. Target an LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP you want to

ping that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, "Sample network" (p. 333).

Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Ping results form to view the diagnostic details.

5

Review the diagnostic results and assess whether the configuration meets the network requirements.

The table below lists the displayed messages.

Displayed message	Description	
notApplicable (0)	The OAM diagnostic message does not apply to the OAM diagnostic performed.	
fecEgress (1)	The replying router is an egress for the FEC. The far-end egress point exists and is operating correctly. No action required.	
fecNoMap (2)	The replying router has no mapping for the FEC.	
notDownstream (3)	The replying router is not a downstream router.	
downstream (4)	The replying router is a downstream router, and the mapping for this FEC on the router interface is the specified label.	
downstreamNotLabel (5)	The replying router is a downstream router, and the mapping for this FEC on the router interface is not the specified label.	
downstreamNotMac (6)	The replying router is a downstream router, but it does not have the specified MAC address.	
downstreamNotMacFlood (7)	The replying router is a downstream router, but it does not have the specified MAC address and cannot flood the request to other routers.	
malformedEchoRequest (8)	The received echo request is malformed.	
tlvNotUnderstood (9)	One or more TLVs were not understood.	

Table 6-5 LSP Ping OAM diagnostic results

a. If the LSP Ping passes, you have completed the workflow for troubleshooting services. Contact your technical support representative if the problem persists; see Chapter 1, "NSP troubleshooting overview".

b. If the LSP Ping fails, verify the administrative and operational status of the underlying L2 equipment.

6

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

7 –

6.13

technical support representative; see Chapter 1, "NSP troubleshooting overview". END OF STEPS -To review the route for an MPLS LSP using LSP Trace 6.13.1 Steps 1 -Choose Tools→Service Test Manager (STM) from the NFM-P main menu. The Manage Tests form appears. 2 -Click Create. 3 -Choose MPLS→Create LSP Trace from the Create contextual menu. The LSP trace create form appears. Note: You must use the LSP Trace diagnostic to test the service in both directions for the connection. Δ Configure the required parameters for the diagnostic session and run the diagnostic. Target an LSP, any LSP or an LSP path. Choose the MPLS site for the test, then configure the LSP or LDP you want to trace that is associated with the MPLS site, in this case, an LSP Ping from site ID 10.1.200.51/32 to site ID 10.1.200.52/32 using the network in Figure 6-1, "Sample network" (p. 333). Click on the Results tab to view the list of trace responses. Double-click on a row in the list to view its details. Double-click on the entry in the LSP Trace results form to view the diagnostic details. 5 Review the diagnostic results and assess whether the configuration meets the network requirements. a. If the LSP Trace returned the expected results for the configuration of your network, the troubleshooting is complete. b. If the LSP Trace did not return the expected results for the configuration of your network, verify that the correct MPLS LSP is used for the service. 6 If the service problem persists, another type of service problem may be present. Perform the

If the troubleshooting workflow does not identify the problem with your service, contact your

steps of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

7 –

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS —

# 6.14 To review ACL filter properties

#### 6.14.1 Steps

1

Click on the L2 Access Interfaces or L3 Access Interfaces tabs on the Services (Edit) form. A list of interfaces appears.

2 -

Double-click on a row in the list. The L2 or L3 Interface configuration form appears.

3

Click on the ACL tab.

4

Review the ingress and egress filter configurations to ensure that ACL filtering configurations do not interfere with the service traffic.

- a. If there are no ACL filtering configurations that interfere with the service traffic, go to Stage 7 a 2 in 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).
- b. If there are ACL filtering configurations that interfere with the service traffic, implement and verify the solution for the service problem.
- 5 —

If the service problem persists, another type of service problem may be present. Perform the steps of 6.3 "Workflow to troubleshoot a service or connectivity problem" (p. 333).

6

If the troubleshooting workflow does not identify the problem with your service, contact your technical support representative; see Chapter 1, "NSP troubleshooting overview".

END OF STEPS -

# 6.15 To view anti-spoof filters

### 6.15.1 Purpose

If a host is having a problem connecting to the network, one possibility for the problem is dropped packets as a result of anti-spoofing filters on the SAP. The NFM-P allows you to view the anti-spoof filters currently in effect on a SAP.

Anti-spoof filters are frequently created and deleted in the network. As a result, the NFM-P does not keep synchronized with the anti-spoof filters on the managed devices. However, the NFM-P allows you to retrieve, on demand, the current anti-spoof filters for a SAP.

## 6.15.2 Steps

1 -

Select Manage  $\rightarrow$  Service  $\rightarrow$  Services from the NFM-P main menu. The Manage Services form opens.

2 \_\_\_\_\_

Select the service for which you want to view the anti-spoof filters.

\_\_\_\_\_

Click Properties. The Service (Edit) form opens.

4

3

Click on the L2 Access Interfaces or L3 Access Interfaces tab, depending on the service that you selected.

5

Select an interface from the list and click Properties. The Access Interface (Edit) form opens.

6

Click on the Anti-Spoofing tab.

7 \_\_\_\_\_

Click on the Filters tab.

8 –

Click Search to retrieve the current anti-spoof filters for the SAP. The Filters tab refreshes with a list of the current anti-spoof filters.

END OF STEPS -

# 6.16 To retrieve MIB information from a GNE using the snmpDump utility

## 6.16.1 Purpose

Perform this procedure to export all object values from the NFM-P-supported SNMP MIBs on a GNE. The exported information may help with troubleshooting the GNE configuration on the device or in the NFM-P.

## 6.16.2 Steps

1 Log in to an NFM-P main server station as the nsp user.

2 -

Open a console window.

3

Navigate to the /opt/nsp/nfmp/server/nms/bin directory.

4 -

Enter the following:

```
./snmpDump.bash option_list +
```

where *option\_list* is one or more of the options listed in Table 6-6, "snmpDump .bash options" (p. 351)



**Note:** Each option must be separated by a space, as shown in the following example: snmpDump.bash -v 3 -h 192.168.18.77 -u jsmith -apw mypass -ppw yoda If an option has a default value, the default value is included in the option description.

#### Table 6-6 snmpDump .bash options

Option	Description	
-v version	The SNMP version in use on the GNE Default: 2	
-f file_name	The output filename Default: <i>host</i> -snmpDump.out in the current directory	
-h <i>host</i>	The IP address or hostname of the GNE Default: localhost	
-c community	The SNMP community	
-u v3_user	The SNMPv3 user name	
-e snmp_engine_ID	The SNMP engine ID	

NSP

Table C C		le a a la caratta		(	
<i>Table</i> 6-6	snmpDump	.bash optic	ons (	(continuea)	

Option	Description	
-ap v3_auth_protocol	The SNMPv3 authorization protocol, which can be MD5 or SHA Default: MD5	
-apw v3_auth_password	The SNMPv3 authorization password	
-ppw v3_privacy_password	The SNMPv3 privacy password	
-cn v3_context_name	The SNMPv3 context name	
-ci v3_context_ID	The SNMPv3 context ID	
-p port	The TCP port on the main server that snmpDump must use to reach the GNE Default: 161	
-t timeout	A communication timeout value	
-r retries	The number of times to retry connecting to the GNE	

The utility displays status messages similar to the following as it initializes:

```
Init Products ...
Init ProductFamilyDefs ...
Init PollingDirectiveDefs ...
Start reading from Node ...
```

The utility then begins to retrieve the MIB tables. As It processes a MIB table, it lists the table name and the number of entries the table contains, as shown below:

```
IF-MIB.ifEntry : 21

IP-MIB.ipAddrEntry : 5

MPLS-LSR-STD-MIB.mplsInterfaceEntry : 8

MPLS-TE-STD-MIB.mplsTunnelEntry : 0

MPLS-TE-STD-MIB.mplsTunnelARHopEntry : 0

MPLS-TE-STD-MIB.mplsIdpEntityEntry : 3

MPLS-LDP-STD-MIB.mplsLdpEntityStatsEntry : 3

MPLS-LDP-STD-MIB.mplsLdpPeerEntry : 3
```

The utility is finished when the command prompt is displayed.

5

To view the utility output, open the file using a MIB browser or a text editor.

END OF STEPS -

# Troubleshooting using the NE resync audit function

# 6.17 NE resync auditing overview

# 6.17.1 Functional description

The NE resync audit function detects and reports differences between the NFM-P database version of the NE configuration and the version stored on the NE. The NE resync audit manager displays a list of misaligned parameters and values as represented in the NE and NFM-P databases, and provides quick navigation to the affected object. A resync audit polls the NE in the same manner as a standard full resynchronization, but instead of updating the objects in the NFM-P database, the NFM-P compares the NE configuration retrieved by the resync with the NE configuration in the NFM-P. See 6.20 "To perform an NE resync audit" (p. 356) for information about performing an NE resync audit.

Differences identified during the audit are displayed in the Show Difference manager. In this manager, you can navigate to the associated NE object that contains the difference and perform a resync on that object to resolve the difference. You can access the results of one audit per NE in the NE audit result list.

You can specify whether to include or ignore read-only parameters in a resync audit. Some readonly parameters are set by the NE after a configuration change. Other read-only parameters, such as temperature measurements and time stamps, change frequently on the NE and will often differ from the values in the NFM-P database. Disabling the inclusion of read-only parameters can help prevent cluttered audit results.

The difference entries that an NE resync audit returns are categorized as follows:

- Property Change-the value of a specific parameter is different in the NFM-P and NE databases
- Missing-the object and contained parameters exist in the NFM-P, but not on the NE
- · Added-the object and contained parameters exist on the NE, but not in the NFM-P

# 6.17.2 Additional information

Consider the following information about NE resync audits:

- The NFM-P limits the audit result to 1 000 differences.
- NE resync audits only compare parameters that are synchronized with the NFM-P database. Parameters that are stored in the NE database only and are not managed by the NFM-P are not included in the audit report.
- NE resync audit results do not include statistics.
- NE resync audits cannot be used to deploy changes to an NE.
- You cannot perform a full resync from the NE audit manager or Show Differences form.
- Dynamic read-only objects and dynamic parameters are excluded from NE resync audits. For example, the following objects are excluded: LDP session, RSVP session, MPLS In Segment, Out Segment, Cross Connect, MPLS Actual Hop and Actual Path, ISIS SPF Log.

# 6.18 Workflow for NE resync auditing

# 6.18.1 Stages

## 1 -

Perform NE resync auditing to identify specific object and parameter misalignment between an NE and the NFM-P; see 6.20 "To perform an NE resync audit" (p. 356).

2 \_\_\_\_\_

View the results of NE resync audits and manage audit results; see 6.21 "To view NE resync audit results using the NE audit manager" (p. 357).

3 —

Clear the SDP binding Frame Size Problem alarm; see 6.19 "To clear a Frame Size Problem (MTU Mismatch) alarm" (p. 354) .

# 6.19 To clear a Frame Size Problem (MTU Mismatch) alarm

## 6.19.1 Purpose

This procedure describes how to clear the SDP binding Frame Size Problem alarm.

# 6.19.2 Steps

1 –

Choose Manage $\rightarrow$ Service $\rightarrow$ Services from the NFM-P main menu.

2 —

Choose the service identified by the Alarmed Object Id in the Alarm Info form for the alarm that you are trying to clear.

3 —

Click Properties. The Service form opens.

- 4 Click on the Sites tab. The list of available sites for the service appears.
- 5 \_\_\_\_\_

Choose the site identified by the Site Id in the Alarm Info form for the alarm that you are trying to clear.

6 -

Click Properties. The Site form opens.

#### 7 —

Change the MTU to a value less than 1492, for example, 1000.

8

Save your changes. The MTU configuration change is applied to customer, service, and site objects. The SDP binding and related service alarms clear automatically.

END OF STEPS -

# 6.20 To perform an NE resync audit

## 6.20.1 Steps

1 -

Choose Equipment from the navigation tree view selector. The managed NEs are displayed.

- 2 Right-click on an NE and choose NE Resync Audit.
- 3

Enable the check box if you want to include read-only attributes in the audit and click Yes. The NE Audit Result form appears and displays the NE Audit State as "in progress".

**i** Note: The NFM-P displays an error message and does not begin the resync audit if the NE in unreachable.

4

When the audit completes, choose one of the following based on the NE Audit State:

- a. If the NE Audit State displays "succeeded" and the NE Audit Result displays "misaligned", go to Step 5.
- b. If the NE Audit State displays "succeeded" and the NE Audit Result displays "aligned", then no further action is required.
- c. If the NE Audit State displays "failed", information about the failure is displayed in the Error Messages panel. Click to expand the panel.

5 –

Click Show Difference. The Show Difference form opens with a list of difference entries displayed.

6

To resync a missing or added object, perform a full resync.

#### 7 —

To resync a property change for a single object with the NFM-P:

- 1. Select a difference entry from the list. The panes at the bottom of the form display the misaligned data for the entry.
- 2. Click Properties for the SAM Object. The Properties form of the object is displayed.
- 3. Click Resync.
- 4. Click Yes and wait for the object to resync with the NFM-P. The value of the misaligned parameter changes if the resync operation is successful.
- 8 —

To save the results of the resync audit to an HTML or CSV file:

- 1. Right-click on a column header in the differences list and choose Save to File. The Save As form is displayed.
- 2. Navigate to the required location on the client workstation and specify a file name.
- 3. Choose a file type and click Save.
- 9 -

Close the forms.

END OF STEPS -

# 6.21 To view NE resync audit results using the NE audit manager

#### 6.21.1 Purpose

You can use the NE audit manager to view the results of previous NE audits and delete audit results.

### 6.21.2 Steps

1 -

Choose Administration $\rightarrow$ NE Maintenance $\rightarrow$ NE Audit Results from the NFM-P main menu. The NE Audit Manager list form opens.

2 —

To view an entry, select an entry from the list and click Show Difference. If there are results to display, the Show Difference form opens.

3

To delete an entry:

1. Select an entry from the list and click Delete.

2. Click Yes. The entry is deleted.

4

Close the NE Audit Manager list form.

END OF STEPS

# Troubleshooting network management LAN issues

# 6.22 Problem: All network management domain stations experience performance degradation

# 6.22.1 Steps

#### 1 -

Verify that there is sufficient bandwidth between the elements of the network management domain.

Bandwidth requirements vary depending on the type of management links set up, and the number of devices in the managed networks. For information about network planning expertise, contact your technical support representative.

See the NSP Planning Guide for more information about the bandwidth requirements.

#### 2 —

When you are using in-band management, ensure that the network devices used to transport the management traffic are up. Ping each of the devices to ensure the management traffic can flow along the in-band path.

In-band management uses a connection provided by a customer service, such as a VLL. The management traffic is sent in-band along with the customer payload traffic. The packets with the management data arrive at the device using one of the virtual interfaces.

END OF STEPS -

# 6.23 Problem: Lost connectivity to one or more network management domain stations

## 6.23.1 Purpose

Perform this procedure on a RHEL or Windows station to check the reachability of another station.

# 6.23.2 Steps

1 —

Log in to the station.

2 —

Open a console window.

3 —

Enter the following:

ping station  $\downarrow$ 

where station is the station hostname or IP address

To interrupt the ping operation, press Ctrl+C.

5 -

Review the output, which resembles the following when connectivity is good:

```
PING station: 56 data bytes
64 bytes from station (192.168.106.169): icmp_seq=1, time=1.0 ms
64 bytes from station (192.168.106.169): icmp_seq=2, time=0.3 ms
64 bytes from station (192.168.106.169): icmp_seq=3, time=0.2 ms
----station PING Statistics----
3 packets transmitted, 3 packets received, 0% packet loss
rtt (ms) min/avg/max = 0.2/0.7/1.0
```

6

If the packets arrive out of order, if some packets are dropped, or if some packets take too long to complete the round trip, LAN congestion may be a problem. Contact your IT department or check the physical LAN connectivity.

7 –

If you can ping the station, but are unable to connect to the station to perform a function, there may be a problem with access to a function on the station.

If the NFM-P deployment includes a firewall, the firewall log entries are in the /var/log/ messages file on a RHEL station.

See 6.24.1 "Purpose" (p. 360) for information about how to verify the following:

- · ports that need to be open across firewalls
- routing configuration

END OF STEPS

# 6.24 Problem: Another station can be pinged, but some functions are unavailable

### 6.24.1 Purpose

Perform this procedure to determine whether port availability or routing is the cause of a management domain LAN issue.

The NFM-P uses TCP and UDP ports for communication between components. Some of the ports, such as the SNMP trap port, are configured during installation. Other ports are configured automatically by the NFM-P software.
### 6.24.2 Steps

1

3

```
Log in as the root user on a station in the network management domain.
2 -
  Verify that the required ports are open or protected by a firewall. See the NSP Planning Guide
  for a complete list of the ports that the NFM-P requires and the purpose of each port.
   i
       Note: If you modify the port configuration, ensure that you record the changes for future
        reference.
  Perform the following steps to check the local routing configuration .:
  1. Open a console window on a station in the management domain.
  2. Use one of the following commands to determine the path to a destination:

    on a Windows station—tracert

      • on a RHEL station-traceroute
      The command uses ICMP echo request messages to list the near-side interfaces that
      packets traverse between the source and destination stations. A near-side interface is the
      interface closest to the source host.
  3. Use OS commands such as netstat -r and arp -a to display a list of active TCP connections,
      Ethernet statistics, the IP routing table, and the ports on which the station is listening.
```

END OF STEPS

#### 6.25 Problem: Packet size and fragmentation issues

### 6.25.1 General information

Large packet sizes from the managed devices are being dropped by intermediate routers because the packets exceed the device MTU or the devices are not configured to forward fragmented packets, causing resynchronizations to fail. The managed devices are configured to send SNMP packets of up to 9216 bytes. The NFM-P can accept such large SNMP packets.

However, the typical L2 or L3 interface MTU on an NFM-P-managed device is likely configured to transmit smaller SNMP packets, usually in the 1500-byte range. This causes packet fragmentation. In order to handle these fragmented packets, intermediate devices between the NFM-P-managed device and NFM-P must be configured to handle or forward fragmented packets. When an intermediate network device, such as a router, cannot handle or forward fragmented packets, then packets may be dropped and resynchronization may fail.

Consider the following:

The network infrastructure that carries traffic between the NFM-P main and auxiliary servers and the managed NEs must support fragmentation and reassembly of the UDP packets for NEs that

have an SNMP PDU size greater than the MTU configured for the network path between the NE and NFM-P. The 7210 SAS, 7450 ESS, 7705 SAR, 7710 SR, 7750 SR, and 7950 XRS require an SNMP PDU size of 9216 bytes and fragmentation support in the network path between the NFM-P and the NE.

- Ensure that the CPM filters on managed devices are configured to accept fragmented packets, and that this filter policy is configured on each server in a redundant NFM-P deployment.
- Ensure that devices located between the managed devices, such as the 7750 SR, and the NFM-P can handle an MTU size of 9216 bytes, can fragment large SNMP packets, or can forward fragmented L2 or L3 packets.
- Verify the MTU packet sizes for all LAN devices.
- Verify that large packets can travel from the managed devices to the NFM-P by using CLI to ping the IP address of the NFM-P server, with a large packet.
- Ensure that the firewalls between the managed devices and the NFM-P server are configured to allow traceroute and ping packets.

## 6.25.2 Steps

1 -

Log in to the 7750 SR or another NFM-P-managed device.

2 —

Run the traceroute command:

```
> traceroute SAM_server_IP_address +
```

A list of hops and IP addresses appears.

3 -

Ping the first hop in the route from the managed device to the NFM-P server:

```
> ping intermediate_device_IP_address size 9216 4
```

A successful response indicates that the intermediate device supports large SNMP packets or packet fragmentation.

4

Repeat for all other hops until a ping fails or until a message indicates that there is an MTU mismatch. A failed ping indicates that the intermediate device does not support large SNMP packets or packet fragmentation.

5

Check the configuration of the intermediate device, and configure fragmentation or enable a larger MTU size.

END OF STEPS -

NSP

# Troubleshooting using NFM-P client GUI warning messages

## 6.26 Client GUI warning message overview

#### 6.26.1 Warning message scenarios

Warning messages in the NFM-P client GUI provide an error recovery mechanism to inform you when:

- information has been entered incorrectly
- additional information is required
- the operation you are attempting cannot be completed
- a change to a configuration sub-form is not committed until the parent form is committed
- · an operation that may result in service disruption is requested
- a configuration form for an object is open that can potentially conflict with a previously opened form

When an error condition is encountered that the NFM-P client has not anticipated, a Problems Encountered form is displayed. See 6.28 "Overview" (p. 366) for more information.

You can use the client GUI to suppress warning messages within containing windows. See the *NSP NFM-P Classic Management User Guide* for more information.

### 6.26.2 Incorrect data entry

When incorrect information is entered for a parameter, a warning message that describes the error is displayed. For example, when you configure a password for a site user, the value entered for the Password parameter and the Confirm Password parameter must match. If they do not match, a warning message is displayed.

### 6.26.3 Additional information required

When the value selected for a parameter has a condition that requires another parameter to be configured, a warning message indicates the missing information that is required. For example, when you configure a new or existing user with MD5 or SHA as the value for the Authentication Protocol parameter, a password must be configured. If you do not configure a password, a warning message is displayed.

The warning message indicates the information that is required. In this case, click OK to close the dialog box, and configure the New Authentication Password and Confirm New Auth Password parameters.

### 6.26.4 Unable to complete requested action

Warning messages are used to indicate that a specific action cannot be completed. These warnings may occur when you try to create a new object or modify an existing object that results in an unsupported configuration. For example, the message "Can't bind LSP to a non-mpls service tunnel" indicates that you cannot bind an LSP to a service tunnel that is not configured with the MPLS protocol.

These errors can be difficult to resolve and may require that you retrace your steps to determine the cause of the warning. Check the documentation to ensure that you are following procedures

## 6.26.5 Commitment of changes from a form and its sub-forms

From a configuration form, you can open sub-forms that require completion before you continue with the parent form. For example, when you create a VLL service, the Create Service Site form opens during one of the configuration steps. After you configure parameters in this sub-form and click on the Finish button, a warning message is displayed.

Changes entered in the sub-form are not committed until you click OK or Apply on the parent form. When you click OK or Apply on the parent form, a final confirmation is displayed.

When you click Yes for the last confirmation, the changes to the parent or sub-forms are committed.

#### 6.26.6 Service disruption warning

correctly.

A service disruption dialog box is displayed when you perform an action that may be serviceaffecting. For example, if you attempt to shut down a daughter card, a warning message is displayed.

As indicated by the warning message, the action you are about to perform may cause a disruption to customer service because of a potential dependency that another object or service has on the current object. Click View Dependencies to indicate the number of services that may be affected by the action.

Verify that the requested action is appropriate. Click on the checkbox beside the statement "I understand the implications of this action" to continue with the action.

### 6.26.7 Duplicate configuration form conflicts

There are multiple ways to access a configuration form for the same object. For example, you can view the configuration form for a port by choosing Manage→Equipment, or you can access the port by clicking on the port object in the expanded navigation tree. When you try to perform both accesses, a warning message is displayed.

When this warning message is displayed, another form is open for the same object. When two forms are open concurrently for the same object, there may be unexpected results because changes committed from one form are not reflected in the other form.

# 6.27 To respond to a GUI warning message

### 6.27.1 Steps

1

Perform an action.

A warning message dialog box opens. For example, when you configure a site password policy, at least one authentication order must be specified as the default in order to configure the authentication order parameters. If at least one authentication order is not configured, a warning message is displayed.

#### 2 —

After you read the warning message, click OK. The warning message dialog box closes.

Correct the problem based on the information provided.

#### 4 -

3

If you cannot correct the problem and continue to get the same warning message:

- a. Check the documentation to ensure that you are following the steps correctly.
- b. Verify that you are trying to perform an action that is supported.
- c. Review the general troubleshooting information in 1.2.4 "Checklist for identifying problems" (p. 16) .
- d. If you cannot resolve the problem, collect the logs identified in 4.2 "To collect NFM-P log files" (p. 44) before you contact your technical support representative.

END OF STEPS -

# **Troubleshooting with Problems Encountered forms**

### 6.28 Overview

#### 6.28.1 The Problems Encountered form

The Problems Encountered form reports error conditions on the client software for which there are no associated warning messages or when the client software cannot identify the problem.

Table 6-7 Problems Encountered form field descriptions	Table 6-7	Problems	Encountered	form 1	field	descriptions
--	-----------	----------	-------------	--------	-------	--------------

Field name	Description		
Class	Specifies the object type that is the source of the problem		
Operation	Specifies the type of operation that was attempted when the problem occurred.		
Affected Object	Specifies the name of the affected object. Typically, if a Problems Encountered form appears when you are trying to create a object, this field contains N/A because the object has not been created.		
Description	Specifies a short description of the problem, which may help you determine the cause of the problem and how to correct the problem. For additional information, click on the Properties button. The information may not be enough for you to correct the problem. The information can be used by your technical support representative to help resolve the problem.		

# 6.29 To view additional problem information

#### 6.29.1 Steps

Choose an entry in the Problems Encountered form and click Properties.

2 —

1 -

Try to correct the problem based on the information provided. If you cannot correct the problem, complete the procedure and perform 6.30 "To collect problem information for technical support" (p. 367).

3 \_\_\_\_\_

Close the details form.

4 \_\_\_\_\_

If there is more than one problem, repeat Step 1 to Step 3 .

5 -----

Close the form.

END OF STEPS —

# 6.30 To collect problem information for technical support

#### 6.30.1 Purpose

The following procedure describes what to do before you contact your technical support representative when you cannot resolve a problem on the Problems Encountered form.

### 6.30.2 Steps

Review the problem information in the Problems Encountered form, as described in 6.29 "To view additional problem information" (p. 366).

2

1

Record the actions performed up to the point when the Problems Encountered form appeared. For example, if you were trying to create a VLL service, record the details about the service that you were trying to create.

3

Record the appropriate problem information, as described in Chapter 1, "NSP troubleshooting overview" .

4

Collect logs for your support representative, as described in 4.2 "To collect NFM-P log files" (p. 44).

END OF STEPS -

# Troubleshooting using the NFM-P user activity log

#### 6.31 User activity log overview

### 6.31.1 Logging user activity

The NFM-P user activity log allows an operator to view information about the actions performed by each NFM-P GUI and OSS user.



i Note: An NFM-P operator with an Administrator scope of command role can view all user activity log records except records associated with LI management. Viewing LI management records requires the Lawful Intercept Management role.

You can use the User Activity form to do the following:

- List and view information about recent user activities.
- · List and view information about recent user sessions and the actions performed during each session.
- · Navigate directly to the object of a user action.
- · View NFM-P client session information that includes connection, disconnection, and authentication failure events.
- · View NFM-P server session information, that includes startup, shutdown, and access violation events.

| i | Note: The NFM-P also raises an alarm for a security-related event such as an authentication failure or access violation.

You can navigate directly from an object properties form to a filtered list of the activities associated with the object. See the NSP NFM-P Classic Management User Guide for more information about the user activity log and using the User Activity form.



Note: The User Activity form and related list forms do not refresh dynamically. To view the latest log entries in a list form, you must click Search.

Each log entry has a request ID. There can be multiple log entries associated with a single request ID. For example, the creation of a discovery rule that has multiple rule elements creates one log entry for each rule element. You can use the request ID to sort and correlate the multiple log entries associated with a single client operation.

#### 6.32 To identify the user activity for a network object

## 6.32.1 Steps

1

Open the User Activity form.

#### 2 —

3 —

Click on the Activity tab.

Specify the filter criteria for the object and click Search. A list of user activity entries is displayed.

w the State column values for the activities ass

View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success represents the successful deployment of the configuration action.

5 —

4

To view a suspect entry, such as a failed or incorrect configuration attempt, select the required entry and click Properties. The Activity form opens.

6 —

Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.

7 \_\_\_\_\_

Close the forms.

END OF STEPS -

# 6.33 To identify the user activity for an NFM-P object

### 6.33.1 Steps

Open the User Activity form.

2 \_\_\_\_\_

1 \_\_\_\_\_

Click on the Activity tab.

3 \_\_\_\_\_

Specify a Site Name of NONE as the filter criterion and click Search. A list of user activity entries is displayed.

4 \_\_\_\_\_

Sort the entries to locate the affected NFM-P object.

	5	
		View the State column values for the activities associated with the object. A value of Failure or Timeout means that the action did not modify the object. A value of Success means that the object modification succeeded.
	6	To view an entry, select the required entry and click Properties. The Activity form opens.
	7	
		Use the activity information from one or more entries to determine whether a sequence of user actions is the source of the problem.
	8	
		Close the forms.
	END	OF STEPS
0.04	т.	
6.34	10	navigate to the object of a user action
6.34.1	Ste	eps
	1	Open the User Activity form.
	2	
		Click on the Activity tab.
	2	
	3	Specify the filter criteria, if required, and click Search. A list of user activity entries is displayed.
	4	
		Select an entry and click Properties. The Activity form opens.
	5	
		Click View Object. The object properties form opens.
	6	
		Close the forms.
	END	OF STEPS

# 6.35 To view the user activity records of an object

## 6.35.1 Steps

6.36

6.36.1

1	
-	Open the required object properties form.
2	Click User Activity, or, if the button is not displayed, click More Actions and choose User Activity. The User Activity form opens and displays a filtered list of user activity records associated with the object.
3	To view an entry, select the entry and click Properties. The Activity form opens.
4	Close the forms.
ENC	OF STEPS
То	view the user activity performed during a user session
Ste	eps
1	
•	Open the User Activity form.
	Specify the filter criteria, if required, and click Search. A list of user session entries is displayed.
C	Select an entry and click Properties. The Session form opens.
	Click on the Activity tab.
5	Specify the filter criteria, if required, and click Search. A list of the actions performed by the user during the session is displayed.
6	

#### 7 —

Close the forms.

END OF STEPS -