NOKIA

NSP
Network Services Platform
Release 26.4

Wavence Device Support Guide

3HE-29845-AAAA-TQZZA
Issue 1
April 2026

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

About this document **9**

1 Wavence device support **11**

1.1 Wavence device support **11**

1.2 Wavence management support **48**

1.3 NSP **48**

1.4 NEtO **53**

1.5 WebCT **55**

1.6 To open WebCT from NSP **55**

1.7 To open WebCT from NFM-P **56**

1.8 To reset the WebCT password on a Wavence UBT-SA node **56**

1.9 To change the WebCT password on one or more Wavence nodes using the NFM-P **57**

1.10 To change the WebCT password on one or more Wavence nodes using an NSP operation **58**

2 Wavence device commissioning and management **61**

2.1 Overview **61**

2.2 Wavence management **61**

2.3 Pathway to commission and manage Wavence devices **70**

2.4 To prepare a Wavence NE for NFM-P management **71**

2.5 To configure polling for a Wavence **73**

2.6 To collect Wavence statistics from an NFM-P auxiliary server **74**

2.7 To retrieve RSL files, I&C files, or log files stored by the Wavence using the NSP **74**

2.8 To create or modify a file retrieval policy in the NFM-P **75**

2.9 To assign a file retrieval policy to a Wavence device in the NFM-P **76**

2.10 To retrieve log files stored by Wavence devices using the NFM-P **77**

2.11 To retrieve RSL files stored by Wavence devices using the NFM-P **78**

2.12 To retrieve I&C files stored by Wavence Release 23A or later devices using the NFM-P **79**

2.13 To retrieve I&C files stored by Wavence Release 22 or earlier devices using the NFM-P **80**

2.14 To configure Wavence NE mediation for microwave backhaul L3 services **81**

2.15 Pathway to configure MPR system settings on Wavence MSS nodes using the NSP **82**

2.16 To display Wavence backhaul service status information on the NSP Network Map and Health dashboard **82**

3 Wavence statistics support **85**

3.1 Wavence statistics support **85**

3.2 To configure radio interface performance management statistics at the port level **89**

3.3 To configure link budget calculation statistics 90
3.4 To configure bulk changes for performance management statistics 91
3.5 RSL Deviation Alerts 93
3.6 Wavence example object filters for the NSP 95
3.7 Pathway to configure NSP test templates for Wavence CFM Loopback and CFM Stats 96

4 Wavence software upgrade 101
4.1 General description 101
4.2 Software upgrade pathway 104
4.3 To perform an on-demand Wavence software upgrade 104
4.4 To manage the Wavence running software 106

5 Wavence migration to revised service model 109
5.1 Migration pathway 109
5.2 To perform pre-upgrade tasks 109
5.3 To perform post-upgrade tasks 110

6 Wavence SCM device management 113
6.1 Secure certification mode (SCM) 113
6.2 Pathway to manage Wavence SCM devices 116
6.3 To configure an SNMPv3 user account on a Wavence SCM device 116
6.4 To configure Wavence SCM NE mediation 117
6.5 To configure a discovery rule 118

7 Wavence object configuration 121
7.1 Overview 121
7.2 Pathway to configure and manage Wavence device objects 121
7.3 To configure the system settings on a Wavence 122
7.4 To resolve Wavence MIB inconsistencies 122
7.5 To update the software activation status for Wavence SA nodes 123
7.6 To configure a scope of command role for NEtO access 124
7.7 To cross-launch NEtO from NFM-P 125

8 Wavence shelf and card object configuration 127
8.1 Overview 127
8.2 Supported Wavence device objects and auxiliary equipment 128
8.3 Equipment configuration 133
8.4 Pathway to manage Wavence devices 133
8.5 Pathway to manage shelf objects on Wavence devices 136
8.6 To perform protection switching in Core-E and CorEvo cards 137

8.7 To migrate the Wavence SA connected to a 7705 SAR from standalone mode to single NE mode 137

9 Wavence port object configuration 139

9.1 Overview 139
9.2 Pathway to manage port objects on Wavence devices 140
9.3 To configure Wavence Ethernet ports 141
9.4 To configure LLDP 142
9.5 To collect and view analog radio statistics on Wavence 1x Radio modem ports 143
9.6 To collect performance management statistics on Wavence 1x Radio modem ports 144
9.7 To configure Wavence port segregation on an EAS module 145
9.8 To configure a loopback test on Wavence ports 146
9.9 To configure 802.3ah EFM OAM remote loopbacks on Wavence ports 147
9.10 To configure Tx mute on radio ports 148
9.11 To configure WRED QoS on a Wavence MSS 149
9.12 To configure 2.5 Gb/s speed on the SFP port of CorEvo card 149
9.13 To configure bandwidth notification on Wavence nodes 150

10 Wavence LAG object configuration 153

10.1 Overview 153
10.2 Pathway to configure and manage Wavence LAG objects 155
10.3 To create an Ethernet LAG on a Wavence 155
10.4 To delete a Wavence Ethernet LAG 157

11 Wavence synchronization management 159

11.1 Introduction 159
11.2 IEEE 1588v2 PTP clocks 159
11.3 To configure synchronization on Wavence Ethernet ports 163
11.4 To configure synchronization on a CorEvo card or MSS-1 shelf using SYNC-IO SFPs 164
11.5 To configure an IEEEv2 1588 TC on a Wavence shelf 164
11.6 To configure IEEEv2 1588 BC and OC PTP clocks 165
11.7 To configure the PTP clock as a synchronization source 167
11.8 To configure the ToD 168

12 Wavence inventory management 169

12.1 Radio port inventory — Wavence SA and Wavence MSS-1c 169
12.2 To list and sort inventory information 169
12.3 To save an inventory list 170
12.4 To configure radio port inventory for Wavence SA and Wavence MSS-1c devices 171

12.5 Radio port inventory – Wavence devices 171
12.6 To configure radio port inventory for Wavence devices 172
12.7 Radio LAG member inventory – Wavence devices 172
12.8 To configure radio LAG member inventory for Wavence devices 173
12.9 Inventory list of Wavence system settings 173

13 QoS policies 175
13.1 Overview 175
13.2 Pathway to configure Wavence QoS policies 175
13.3 To configure a 9500 Radio Interface Queue Map policy 176
13.4 To configure a 9500 NE QoS policy 177

14 Wavence service tunnels 179
14.1 Overview 179
14.2 Configuring service tunnels on a Wavence 184
14.3 To create an Ethernet radio ring on a Wavence 184

15 Wavence microwave backhaul service management 189
15.1 Microwave backhaul service configuration 189
15.2 To configure microwave backhaul services 195
15.3 To complete a ring by automatically adding the ring adjacencies 198
15.4 To copy a microwave backhaul service 201
15.5 To view the microwave backhaul service objects 203
15.6 Microwave backhaul service discovery 205
15.7 To discover a microwave backhaul service 205
15.8 To move Wavence backhaul sites 207
15.9 To separate microwave backhaul service topologies 208
15.10 To propagate microwave backhaul service name to sites 209
15.11 To list microwave backhaul services 210
15.12 Microwave backhaul service associations 211
15.13 Microwave backhaul service management— considerations/limitations 217
15.14 Microwave backhaul service creation using NSP Intent-Based Service Management 218

16 Wavence composite service 221
16.1 Composite service 221
16.2 To configure a composite service 222

17 Wavence microwave backhaul L3 SNMP management 225
17.1 L3 network interface management 225
17.2 Pathway to configure L3 VPN transport setup 227

17.3 Pathway to configure a VPRN service using the Service Management view 229
17.4 To initialize an L3 VLAN ID 229
17.5 To configure a System and Network interface 230
17.6 To initialize the MPLS protocol 231
17.7 To configure an MPLS interface 231
17.8 To configure a static route 232
17.9 To configure a static LSP 233
17.10 To create static hops from an MPLS interface properties window 234
17.11 To configure static routes on a VPRN site 234
17.12 To create and configure a Two-Way Active Measurement Protocol Light reflector 235
17.13 To view all the configured TWAMP Light reflectors 237
17.14 To create an SDP Tunnel 237
17.15 To create a black-hole route 238
17.16 To configure a SAP access ingress policy 238
17.17 To configure a SAP access egress policy 240
17.18 To configure a QoS network policy 241
17.19 To configure an Auto-ID range for policies 242
17.20 To configure a VPRN service 243
17.21 To configure a VLAN group 245
17.22 To configure OSPFv2 Router ID 246
17.23 Pathway to configure OSPFv2 246
17.24 To configure OSPFv2 instance on a Routing instance 247
17.25 Pathway to configure OSPFv3 248
17.26 To enable LFA and remote LFA on an OSPF instance 248
17.27 To create an OSPF area 249
17.28 To add a Layer 3 interface to an OSPF router 249
17.29 To configure OSPF segment routing and discover dynamic LSPs 250
17.30 To configure IP/MPLS Service Tunnel 251
17.31 To create and run a VPRN Ping test from a service manager form 252
17.32 To create and run a VPRN Ping test on a SAP 253
17.33 Wavence VPRN service — considerations/limitations 254

A NEtO, WebCT, and NFM-P management comparison 257
A.1 Overview 257
A.2 Support for Wavence management features across element managers 257

About this document

Purpose

NSP NFM-P Wavence Device Support Guide describes how to discover, configure, and manage Wavence devices using the NFM-P and NSP. The guide is intended for network planners, administrators, and operators and is to be used in conjunction with other guides in the NFM-P and NSP documentation suite where management of Wavence devices does not differ from other network elements. Nokia recommends that you review the entire *NSP NFM-P Wavence Device Support Guide* before you attempt to manage Wavence devices.

Scope

The scope of this document is limited to the NFM-P application. Many configuration, monitoring, and assurance functions that can be accomplished from the NFM-P Java GUI are also delivered in NSP web-based applications accessible from the NSP Launchpad. Readers of this NFM-P guide should familiarize themselves with the capabilities of the NSP applications, which often offer more efficient and sophisticated features for network and service management. Help for all installed NSP applications is available in the NSP Help Center.

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@nokia.com.

1 Wavence device support

1.1 Wavence device support

1.1.1 Wavence radio family

The Nokia Wavence is a microwave digital radio family that supports PDH and Ethernet to migrate from TDM to IP. The Wavence provides a generic, modular IP platform for multiple network applications such as 2G, 3G, HSDPA, and WiMAX to accommodate broadband services to Metro Ethernet areas. This solution improves packet aggregation, increases bandwidth, and optimizes Ethernet connectivity.

The Wavence supports low, medium, and high capacity applications using ANSI and ETSI data rates, frequencies, channel plans, and tributary interfaces and has both indoor and outdoor applications.

The NE icon in the NFM-P GUI shows the chassis name Wavence, for example, Wavence MSS-4. NEs from earlier releases show the former name of the Wavence NE, 9500 MPR.

Note: To determine which versions of the Wavence NEs and variants are supported by NFM-P, see the *NSP NFM-P and 5620 SAM Network Element Compatibility Guide* for information.

Note: Only discovery of port segregation rules is supported.

Wavence SM

The Wavence SM is the split-mount application of a shelf unit and an indoor or outdoor radio. The Wavence SM provides fixed or mobile Ethernet site backhauling and supports converged MPLS metro networks. As a native NE, the Wavence SM appears on NFM-P maps and equipment managers. Some features require a cross-launch of the NEtO external element manager or the WebCT browser-based element manager. See 1.2 “Wavence management support” (p. 48) for more information.

Wavence SA

The Wavence SA is the standalone, outdoor application of the outdoor radio unit without a shelf unit. As a native NE, the Wavence SA appears on NFM-P maps and equipment managers. All standard SNMP-based features, including discovery and alarms, are supported with the same naming as the rest of the Wavence family. Some features require a cross-launch of the NEtO external element manager. See 1.2 “Wavence management support” (p. 48) for more information.

Note: From an NFM-P perspective, the Wavence SA (standalone), and Wavence MSS-1c variants belong to same product family; both variants display on the NFM-P GUI as the Wavence SA. However, for Wavence software upgrades, the Label column allows you to distinguish between the Wavence SA and Wavence MSS-1c variant types.

Wavence MSS-1c

The Wavence Microwave Service Switch-1c (MSS-1c) is an ultra-compact indoor unit (1/2 rack size) offering 10 E1 and 4 user interfaces. The Wavence MSS-1c provides user port interface, cross-connection, and switching management. The cross-connection matrix implements all the cross-connections between the User ports (four Ethernet ports and E1/T1 streams) and the radio port. The matrix is a standard Ethernet switch, based on VLAN, assigned by the MCT.

The NE backup and restore functionality for this node type is only supported for Releases W19A, W20A, W21A, W21A SP1, W22, W22A, W23, W23A, W24, and W25. A new backup and restore policy has been added to support this device type. You can access the policy from the Administration→NE Maintenance→Backup/Restore menu. Click on the Backup/Restore Policy tab, select the MPR-SA Default Policy and click Properties.

Note: This policy type requires the FTP/SFTP parameters to be configured.

The following functionality is supported for the Wavence MSS-1c using NFM-P:

- automatic server registration with NE discovery
- ports listed in the Navigation equipment tree
- port alarm management
- automatic radio link discovery
- automatic node software download managed via a policy (same as the Wavence SM/Wavence SA)
- automatic node MIB backup and restore managed via a policy (same as the Wavence SM/ Wavence SA)
- microwave backhaul service termination on the radio port

Wavence MSS-O

The Wavence Microwave Services Switch-Outdoor (MSS-O) is a compact, full outdoor microwave networking device, for boosting link capacity and reliability for small cell backhaul networks. The device provides both optical and electrical Ethernet interfaces and can be installed indoors or outdoors.

You can configure the following on a Wavence MSS-O using NFM-P:

- three 10/100/1000Base-TX Ethernet interfaces, two with PFoE, and one optical Gigabit Ethernet SFP interface. See 9.3 “To configure Wavence Ethernet ports” (p. 141) for more information about configuring Ethernet ports.
- Ethernet L2 LAGs. See 10.3 “To create an Ethernet LAG on a Wavence” (p. 155) for more information about configuring Ethernet LAGs.
- synchronization on Ethernet ports. See 11.3 “To configure synchronization on Wavence Ethernet ports” (p. 163) for more information about synchronization on Ethernet ports.
- port segregation. See 9.7 “To configure Wavence port segregation on an EAS module” (p. 145) for more information about port segregation.
- microwave backhaul services. See Chapter 15, “Wavence microwave backhaul service management”, for more information about how to configure microwave backhaul services.

Note: Only the P2M VLAN path type is supported.

- Ethernet ring. See 14.1.3 “Ethernet (G.8032) ring support” (p. 179) for more information about configuring Ethernet rings.

The LAG size for a Wavence MSS-O is restricted to the following:

- up to two LAG ports per NE, either Ethernet L2 LAG or radio L1 LAG
- up to two electrical Ethernet ports per Ethernet L2 LAG. Ports can have PFoE enabled
- ports 1, 2, and 3 on the Wavence MSS-O are available for Ethernet L2 LAG membership

UBT-SA

The Wavence Ultra Broadband Transceiver-SA (UBT-SA) is a standalone outdoor radio unit. Adaptive modulation is supported. The UBT microprocessor manages transmit and receive frequencies, transmit power, alarms, and performance monitoring. See the Wavence documentation for information about channel spacing, shifter and frequency management, and modem profiles.

As a native NE, the UBT-SA appears on NFM-P maps and equipment managers. Some features require a cross-launch of the WebCT browser-based element manager. See 1.2 “Wavence management support” (p. 48) for more information.

The UBT-SA is commissioned in the Wavence element manager. The NFM-P discovers the UBT-SA and displays the variant in the equipment tree. UBT-SA discovery is performed as a part of the Connect Service operation; see 15.1.7 “Connect service” (p. 191). When a UBT-SA is configured as a pass-thru in a Y-cable or ring topology, the NFM-P discovers all the UBT-SA nodes involved, regardless of the configured service on the Wavence element manager.

The following variants are supported:

- UBT-m: provides a single radio carrier in the E-band (80 Ghz) frequency
- UBT-I: provides a single radio carrier in the 5.8 Ghz - 42 Ghz frequency bands in addition to a combiner module
- UBT-S: provides a single radio carrier in the 5.8 Ghz - 42 Ghz frequency bands
- UBT-S2: provides a double carrier in a single box for the following RF frequencies: 6, 8, 13, 15, 18, 23 GHz
- UBT-T: provides a double carrier in one box in the 5.8 Ghz – 42 Ghz frequency bands
- UBT-T XP: provides a 6Ghz and 11Ghz channel in one box
- OCM: combines two or four UBT-T under a single antenna

The following functionality is supported for the UBT-SA using NFM-P:

- NE discovery
- ports listed in the navigation equipment tree
  only SFP ports of type Ethernet and Radio are supported
- backup and restore functionality
  - backup and restore for the MSS-4/8 is only available over SFTP
- NE software download or upgrade
- port alarm management

- automatic radio link discovery
- support of the following PM statistics (both current and historic):
  - Frame Hop
  - RSL
  - TSL
  - Adaptive Modulation
- support of the following Radio Analog statistics:
  - RSL
  - TSL
- QoS policies
- SMR, which displays UBT-SA nodes as sub-units of IXR or SAR nodes. Link utilization monitoring is not available for nodes in an SMR configuration

The following functionality is supported for the UBT-SA using NFM-P with the Wavence, Release 20A or later:

- Coupling port management
- The electrical port can be used as a data port

The following functionality is supported for the UBT-SA using NFM-P with Wavence, Release 22 or later:

- microwave backhaul service support
- carrier aggregation and CA mode 1B (UBT-S/S2 and UBT-I)

1+1 HSB FP/SD protection is supported for UBT-S/S2 and UBT-I standalone variants using Wavence 23A or later. Configuring protection is performed using WebCT, see the Wavence documentation for more information. Protection information is displayed in the NFM-P on the Protection tab of the Equipment view for the UBT-SA. One node is configured as Main and the other as Spare; these configurations do not change, instead the Protection switching status (EPS/TPS and RPS) will change between Active and Standby to indicate which node is currently active, mirroring the values displayed in the Wavence Element Manager. Statistics collection can be configured individually on each member of a protection link, as supported by the node; the following considerations apply for statistics collection in a protection configuration:

- For Ethernet statistics, all values are 0 for the UBT in an EPS standby state.
- PM statistics should be enabled on both the Main and Spare nodes.
- The following statistics are only displayed on the Main node; the statistics from the active node are relayed and displayed on the Main node:
  - Peak and Average Throughput and Link Utilization History Data Stats
  - Link History Data Stats

Note: Some node parameters are only updated by performing a manual node resync and not automatically when the values change. For the UBT-SA these parameters include:

- **UBT-m**: Adaptive Current TX modulation; Adaptive Current TX capacity

Wavence MSS-E/HE

The Wavence Microwave Service Switch-E/HE (MSS-E/HE) is a compact indoor unit. This is an extension of MSS1v2. All standard SNMP-based features, including discovery and alarms, are supported with the same naming as the rest of the Wavence family. As a native NE, the MSS-E/HE appears on NFM-P maps and equipment managers. Some features require a cross-launch of the WebCT browser-based element manager. See 1.2 “Wavence management support” (p. 48) for more information.

The NE backup and restore functionality for this node type is only supported using the NFM-P, Release 20.11 or later. A mediation policy with valid credentials must be configured for the node in order to support Backup/Restore operations. Refer to the node documentation for the credentials that are required.

The following functionality is supported for the Wavence MSS-E/HE using NFM-P:

- SNMPv2 and SNMPv3 based Discovery and Equipment Management
- port alarm management
- housekeeping alarm management
- backup and restore functionality
- NE software download or upgrade
- QoS management
- Ethernet statistics and maintenance
- Remote Inventory management at port and shelf level
- TDM2TDM service configuration
- OSPFv3
- Ethernet CFM
- configuration of combo ports 5 and 6 on MSS-HE

Wavence MSS-XE

The Wavence Microwave Service Switch-XE (MSS-XE) is an indoor split-mount solution. All standard SNMP-based features, including discovery and alarms, are supported with the same naming as the rest of the Wavence family. As a native NE, the MSS-XE appears on NFM-P maps and equipment managers. Some features require a cross-launch of the WebCT browser-based element manager. See 1.2 “Wavence management support” (p. 48) for more information.

The NE backup and restore functionality for this node type is only supported using the NFM-P, Release 22.9 or later. A mediation policy with valid credentials must be configured for the node in order to support Backup/Restore operations. Refer to the node documentation for the credentials that are required.

The following functionality is supported for the MSS-XE using NFM-P:

- SNMPv2 and SNMPv3 based Discovery and Equipment Management
- synchronization
- port alarm management
- housekeeping alarm management

- backup and restore functionality
- NE software download or upgrade
- QoS management
- Ethernet statistics and maintenance
- Remote Inventory management at port and shelf level
- VLAN services
- TMN in-band management
- MSS-XE Ethernet/Radio port management
- TDM2TDM service configuration
- Radio links
- OSPFv3
- Ethernet CFM
- configuration of combo ports 1, 2, and 8

Note: SFP Signal Level measurement statistics are only available on nodes Wavence Release 24 or later.

UBT-NIM

The Wavence Ultra Broadband Transceiver-Network Integrated Module (UBT-NIM) is a hardware plugin to be attached to UBT-m/-T/-S in order to provide multiple ethernet interfaces to UBT. The ethernet ports on NIM unit are managed as ethernet user ports or as connection ports to an UBT.

All standard SNMP-based features, including discovery and alarms, are supported with the same naming as the rest of the Wavence family. As a native NE, the UBT-NIM appears on NFM-P maps and equipment managers. Some features require a cross-launch of the WebCT browser-based element manager. See 1.2 “Wavence management support” (p. 48) for more information.

The NE backup and restore functionality for this node type is only supported from NFM-P from release, 21.6 onwards. Refer to node document for the credentials to be supplied. The UBT-NIM is commissioned in the Wavence element manager. After configuration in Wavence is complete, the NFM-P discovers the UBT-NIM and displays it in the equipment tree.

The following functionality is supported for the UBT-NIM using NFM-P:

- SNMPv2 and SNMPv3 based Discovery and NE Management
- ports listed in the Navigation equipment tree
- Radio link discovery
- port alarm management
- backup and restore functionality
- NE software download or upgrade
- QoS management
- Ethernet statistics and maintenance
- Performance monitoring management

- Synchronization support at Shelf level
- microwave backhaul service support
- Local Access Control management
- OSPFv3

The following functionality is supported for the UBT-NIM with Wavence, Release 24 or later:

- carrier aggregation and CA mode 1B
- Ethernet CFM

1.1.2 MPT device support using GNE drivers

GNE drivers are optional software modules corresponding to specific Wavence devices. They extend the management of selected Wavence devices beyond the basic GNE management that would otherwise be available to them.

The GNE drivers are installed with the NFM-P software. It is no longer necessary to obtain these drivers separately from the NSP software delivery site. See “Device management using drivers” in the *NSP NFM-P Classic Management User Guide* for more information. Driver compatibility information is located in the *NSP NFM-P and 5620 SAM Network Element Compatibility Guide*.

Drivers are provided for extended management of the following devices in the Wavence product family:

- “9500 MPT-GM” (p. 17)
- “9500 MPT-GS” (p. 23)
- “9500 MPT-SUB6” (p. 30)
- “9500 MPT-BWA” (p. 38)

Note: The 9500 MPT-BWA device is a hardware variant of the MPT-SUB6. The NFM-P uses the MPT-SUB6 driver to manage the MPT-BWA.

9500 MPT-GM

The MPTGM driver extends the management capabilities of the NFM-P for MPT-GM devices in the following applicable areas.

Table 1-1 MPTGM driver capabilities

Configuration management

Table 1-1 MPTGM driver capabilities (continued)

Radio link inventory – Operators can view all radio links terminating on this device by drilling down from the network topology map or network equipment tree representations of the MPT-GM. **Note:** To create a physical link, select the endpoints as type “Port”. Additionally, radio links associated with the MPT-GM are included in the inventory list accessed through the Equipment Manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Radio link (Network) from the object type drop-down). Radio link inventory information is also available to the XML API through the installation of the driver, under the following package and class *netw.RadioPhysicalLink*.
Radio link discovery – The NFM-P extends the link auto-discovery to radio links interconnecting MPT-GM devices.
Radio port parameters – The driver extends the NFM-P management of the MPT-GM to include its radio port interfaces. With the installation of the driver, a "Radio" tab is added to the Generic NE interface form, allowing NFM-P operators to view the following generic radio port parameters of the device: • ATPC Enabling • ATPC Max Tx Power • ATPC Low Power Threshold – The value displayed for this parameter is the minimum value, not a configurable threshold. • ATPC High Power Threshold • Mode • Current Modulation • Actual Speed (kbps) • MTU • Manual Local Tx Mute • Tx Frequency • MPT Shifter Value • Channel Spacing • Received Power Level • Transmitted Power Level • Radio PM • Normalized MSE (dB) • Available Bandwidth (Mbps) These parameters are also available to the XML API under the following package and class *radioequipment.RadioPortSpecifics*.

Table 1-1 MPTGM driver capabilities (continued)

Radio port inventory parameters – The following radio port inventory parameters are displayed on the Inventory tab for the radio ports: • Company ID • Mnemonic • Part No • Serial No • Port ID • Software Part No These parameters are also available to the XML API under the following package and class *radioequipment.RadioEquipmentInventory*.
Longitude and latitude – The NFM-P displays the location of the MPT-GM with latitude and longitude. The coordinates are displayed as additional parameters on the General tab of the Properties form. The longitude and latitude parameters are configurable.
Generic NE Profile automation – The Generic NE Profile for the MPT-GM is automatically created when the MPTGM driver is installed.
Alarm catalog integration – The MPT-GM alarm catalog is automatically populated during driver installation. Operators can edit the alarm catalog to customize alarm characteristics. **Note –** Since "info" traps are not present in the automatically generated alarm catalog, the NFM-P may throw an error in the log viewer. There is no impact on the functionality of alarms reporting.
NE software version display – The NE software version is displayed on the General tab of the NE Properties form.
Port labeling – The Name parameter in the MPT-GM port list is customized to facilitate the mapping of the interface index with the interface type.
TMN Inband management – The NFM-P displays the VLAN ID parameter identifying the TMN Inband management traffic/signal. On the Polling tab, click on the TMN Details sub-tab, and double-click on the row. The TMN Inband setting is read-only.
MAC address – The NFM-P displays the MAC Address of the node on the General tab of the NE form. The MAC Address is also accessed through the Equipment manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Network Element (Network) from the object type drop-down).
Bulk PM operations – Bulk PM operations are supported. Choose Tools→Bulk Operations from the NFM-P main menu to create a bulk change. You can specify filter options while creating a bulk change. During a bulk execution, if there are exceptions encountered, all following bulk executions are cancelled. See the "Bulk Operations" chapter in the *NSP NFM-P Classic Management User Guide* for more information.
PM enable/disable – You can enable/disable PM at the radio port level.

Table 1-1 MPTGM driver capabilities (continued)

<table>
<tr><td colspan="2">Port parameters – The NFM-P displays the following read-only parameters on the General tab of each port:
• Mode
• Encapsulation Type
• Speed</td></tr>
<tr><td colspan="2">Interface name description – The MPTGM port descriptions are aligned to the WebLCT as follows:</td></tr>
<tr><td>Port Name</td><td>Description</td></tr>
<tr><td>1/1/1</td><td>Mngt</td></tr>
<tr><td>1/1/2</td><td>Aux</td></tr>
<tr><td>1/1/6</td><td>LAN-2</td></tr>
<tr><td>1/1/9</td><td>Radio</td></tr>
<tr><td>1/1/10</td><td>LAN-1</td></tr>
<tr><td colspan="2">Service management</td></tr>
<tr><td colspan="2">When driver-managed GNE devices are collocated with the 9500 MPR, the NFM-P supports creation of the microwave backhaul service spanning across MPRs and OEMs. The NFM-P recognizes OEM as a site to add to the microwave backhaul service. The NFM-P also recognizes the Ethernet and radio ports on OEM as adjacencies to add to OEM sites. However, the NFM-P does not support deployment of these services to OEM devices. Deployment to OEM devices must be done from the respective EMS. Consequently, discovery of this service does not discover OEM sites. Therefore, OEM sites can be either manually added for the MPTGM/MPTGS/MPTSUB6, or populated using the Complete Ring feature for the MPTGM.</td></tr>
<tr><td colspan="2">Service assurance</td></tr>
<tr><td colspan="2">Performance management – The driver extends NFM-P performance management to the MPT-GM device so that statistics related to the GNE can be viewed through the NFM-P GUI. Statistics are also available to the XML API; see the NSP NFM-P Statistics Management Guide.</td></tr>
<tr><td colspan="2">Alarm resynchronization – The NFM-P performs periodic polling of trap sequence numbers and detects gaps, if present. Upon NE alarm loss detection, the NFM-P performs full NE alarm resynchronization.</td></tr>
<tr><td colspan="2">Alarm reporting – The NFM-P supports the reporting of all alarms present in the automatically generated alarm catalog.</td></tr>
</table>

Table 1-1 MPTGM driver capabilities (continued)

Radio link fault management – The NFM-P tracks the radio link down scenario. When a radio link interconnects two MPT-GM devices, the NFM-P manages the operational state at the node and processes any alarms affecting the radio link extremities. The NFM-P changes the operational state on the General tab of the radio interface based on the link down alarm. **Note –** The operational state on the Radio tab does not change based on link status. When the link is operationally down, the link shows red. When the link is operationally up, the link shows green.
Physical link fault management – The NFM-P tracks the physical link down scenario when a physical link is interconnecting an MPT-GM and an MSS-8/4/1/O. A link down alarm is raised when the LOS (Loss Of Signal) alarm at the MPT-GM port is notified by the node from the NFM-P. The link (physical or radio) is displayed as alarmed in the topology view (red line) and the link down alarm is reported in the alarm list.
Alarm correlation – The NFM-P supports alarm correlation for the following fault scenario: • radio link down • physical link down Both “LinkDown” alarms are correlated to the “adjacencyDown” alarm at the service level.
Device life cycle management
Backup – The driver extends the NFM-P management of the MPT-GM device to include the backup functionality. The driver receives the necessary information regarding the FTP/SFTP server from the NFM-P backup/restore policy and initiates a backup execution on the target device. The driver monitors the backup execution and provides the necessary information to the policy, such as success/failure, date of backup, etc. See the "NE backup and restore" chapter in the *NSP NFM-P Classic Management User Guide* for more information.
Software upgrade – The NFM-P supports software upgrade operations for the MPT-GM. An MPT-GM software package is provided by the vendor with a single zip file. The zip file name must not be changed. A folder containing this zip file must be selected on an import. The software upgrade consists of 2 steps: • download – Transfers the new software to the offline software bank. • activate – Reboots the system and switches the active status between the banks so the downloaded software becomes active. The Software tab on the NE form displays the software version and status of each bank. **Note –** When upgrading an operational link of an inband managed node, upgrade the remote system first and then the local system. Activate the software at both ends after verifying that the link performs as expected. Always upgrade both ends of the link. See the “NE software upgrades” chapter in the *NSP NFM-P Classic Management User Guide* for more information.

Pathway to discover and manage the MPT-GM

This pathway describes how to discover and manage the MPT-GM in the NFM-P after driver installation.

Consult the *NSP NFM-P Classic Management User Guide* chapter "Device commissioning and management" for full procedural details.

Create mediation policies and configure a discovery rule

1. Use the NFM-P to create an SNMPv1 mediation policy that specifies “admin” as the Read Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
2. Use the NFM-P to create an SNMPv1 mediation policy that specifies “NMS5UX” as the Write/Trap Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
3. Use the NFM-P to configure a discovery rule for the MPT-GM that specifies the following mediation policies; see the *NSP NFM-P Classic Management User Guide* for information about creating discovery rules:
   - Read Access Mediation Policy – mediation policy created in step 1.
   - Write Access Mediation Policy and Trap Access Mediation Policy - mediation policy created in step 2.

Perform configuration management tasks using the device EMS

1. Right-click on the MPT-GM icon on the NFM-P topology map and choose Open URL.
2. Enter your user name and password. The device EMS opens to allow configuration.
3. Choose Main→Alarm Severity Config→SETS and double-click on the following alarms to change the Severity setting from Warning to Status:
   - timingGeneratorFreeRunningStatus
   - timingGeneratorHoldoverStatus

View statistics

1. Click on the Statistics tab of the MPT-GM interface properties form. The MPT-GM Statistics form opens.
2. View statistics as required.

   The availability of historical data requires the activation of Performance Monitoring.

Note: It is recommended that you schedule historical data statistics only, and collect current data statistics on demand. For example, History Data Stats - 15 min returns the same information as Current Data Stats collected for the same 15 minute interval, therefore, it is redundant to schedule Current Data Stats. Scheduling Current Data Stats may result in an error message. Scheduling Interface Additional Stats (Generic NE) is not supported and may result in stopping the collection of other statistics.

Note: For the NFM-P to successfully display the supported History Data Stats, it is expected that the node has collected at least 19 entries of 15 minute statistics. For a newly deployed node, after statistics collection is initiated, you must wait for 5 h before you can view the History Data Stats on the NFM-P.

Note: The plotting of statistics is supported for Interface Stats (Generic NE).

The following counters are supported on Radio interface 9.

Interface Type	Statistic Type
Radio (index 9)	Adaptive Modulation Current Data Stats - 15 min
	Adaptive Modulation Current Data Stats – 24 Hr
	Adaptive Modulation History Data Stats - 15 min
	Adaptive Modulation History Data Stats – 24 H
	Hop Current Data Stats – 15 min
	Hop Current Data Stats – 24 Hr
	Hop History Data Stats - 15 min
	Hop History Data Stats - 24 Hr
	RSL Hop Current Data stats – 15 min
	RSL Hop Current Data stats – 24 Hr
	RSL Hop History Data Stats - 15 min
	RSL Hop History Data Stats - 24 Hr
	TSL Hop Current Data Stats – 15 min
	TSL Hop Current Data Stats – 24 Hr
	TSL Hop History Data Stats - 15 min
	TSL Hop History Data Stats - 24 Hr
Note – On the Ethernet interfaces with index 9 (Radio), 10 (LAN 1), and 6 (LAN 2), the Interface Stats (Generic NE) are also applicable. **Note –** On the Radio interfaces, real-time and historical plots are not supported. **Note –** On the Ethernet interfaces, real-time and historical plots are supported only for interface statistics.	

9500 MPT-GS

The MPTGS driver extends the management capabilities of the NFM-P for MPT-GS devices in the following applicable areas.

Table 1-2 MPTGS driver capabilities

Configuration management

Table 1-2 MPTGS driver capabilities (continued)

Radio link inventory – Operators can view all radio links terminating on this device by drilling down from the network topology map or network Equipment Tree representations of the MPT-GS device. **Note –**To create a physical link, select the endpoints as type “Port”. Additionally, radio links associated with the MPT-GS device are now included in the inventory list accessed through the Equipment Manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Radio link (Network) from the object type drop-down). Radio link inventory information is also available to the XML API through the installation of the driver, under the following package and class *netw.RadioPhysicalLink*.
Radio link discovery – The NFM-P extends the link auto-discovery to radio links interconnecting MPT-GS nodes.
Radio port parameters – The driver extends the NFM-P management of the MPT-GS device to include its radio port interfaces. With the installation of the driver, a "Radio" tab is added to the Generic NE Interface form, allowing NFM-P operators to view the following generic radio port parameters of the device: • Channel Width (MHz) • TX Frequency (MHz) • Role • Mode • Modulation • Actual Speed (kbps) • MTU • Sub Channels • Repetitions • FEC Rate • Rx Link ID • Tx Link ID • Rx State • Tx State • RSSI (dBm) • CINR (dB) • Oper. Status • RF Temperature • Tx Mute • Tx Mute Timeout (sec) • Tx Power (dBm) • Encryption Status These parameters are also available to the XML API under the following package and class *radioequipment.RadioPortSpecifics*.

Table 1-2 MPTGS driver capabilities (continued)

Radio port inventory parameters – The following radio port inventory parameters are displayed on the Inventory tab for the radio ports: • Company ID • Mnemonic • Port ID • Software Part No • Serial No These parameters are also available to the XML API under the following package and class *radioequipment.RadioEquipmentInventory*.
Ethernet (user) port parameters – The Actual Speed (kbps) parameter is displayed on the General tab for the Ethernet ports.
Generic NE Profile automation – The Generic NE Profile for the MPT-GS is automatically created when the MPTGS driver is installed.
Alarm catalog integration – The MPT-GS alarm catalog is automatically populated during driver installation. Operators can edit the alarm catalog to customize alarm characteristics.
NE software version display – The NE software version is displayed on the General tab of the NE Properties form.
TMN Inband management – The NFM-P displays the VLAN ID parameter identifying the TMN Inband management traffic/signal. On the Polling tab, click on the TMN Details sub-tab, and double-click on the row. The TMN Inband setting is read-only.
MAC address – The NFM-P displays the MAC Address of the node on the General tab of the Network Element form. The MAC Address is also accessed through the Equipment manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Network Element (Network) from the object type drop-down).
NTP management – The NFM-P reports NTP-related parameters. NTP enabling and disabling and server configuration is supported through the Alternate Element Manager. Server configuration is also supported using the NFM-P Create option. When the Main and Spare NTP servers are configured with the same IP address, the NFM-P displays only one server. You can modify an NTP server address using the NFM-P, but deleting an NTP server is not supported.
Radio encryption status – The NFM-P reports the Encryption Status (enable/disable) at the radio interface. This parameter is read-only.
Sensor measurements – The NFM-P reports the Equipment Input Voltage and Temperature (Celsius) parameters on the Statistics form.
SNMPv3 support – The NFM-P supports SNMPv3 management of the node.

Table 1-2 MPTGS driver capabilities (continued)

Port parameters– The NFM-P displays the following read-only parameters on the General tab of each port: • Mode • Encapsulation Type – for HBS **Note –** This parameter is not supported for HSU. • Speed
Service management
When driver-managed GNE devices are collocated with the 9500 MPR, the NFM-P supports creation of the microwave backhaul service spanning across MPRs and OEMs. The NFM-P recognizes OEM as a site to add to the microwave backhaul service. The NFM-P also recognizes the Ethernet and radio ports on OEM as adjacencies to add to OEM sites. However, the NFM-P does not support deployment of these services to OEM devices. Deployment to OEM devices must be done from the respective EMS. Consequently, discovery of this service does not discover OEM sites. Therefore, OEM sites can be either manually added for the MPTGM/MPTGS/MPTSUB6, or populated using the Complete Ring feature for the MPTGM.
Service assurance
Performance management – The driver extends NFM-P performance management to the MPT-GS device so that statistics related to the GNE can be viewed through the NFM-P GUI. Statistics are also available to the XML API; see the *NSP NFM-P Statistics Management Guide*.
Alarm resynchronization – The NFM-P performs periodic polling of trap sequence numbers and detects gaps, if present. Upon NE alarm loss detection, the NFM-P performs full NE alarm resynchronization.
Alarm reporting – The NFM-P supports the reporting of all alarms present in the automatically generated alarm catalog.
Radio link fault management – The NFM-P tracks the radio link down scenario. When a radio link interconnects two MPT-GS devices, the NFM-P manages the operational state at the node and processes any alarms affecting the radio link extremities. The radio link color is updated depending on the radio link status. The color is red when the link is down and green when the link is up, according to the radio interface operational status.
Alarm correlation – The NFM-P supports alarm correlation for the following fault scenario: • radio link down • physical link down Both “LinkDown” alarms are correlated to the “adjacencyDown” alarm at the service level.
Device life cycle management

Table 1-2 MPTGS driver capabilities (continued)

Backup – The driver extends the NFM-P management of the MPT-GS device to include the backup functionality. The driver receives the necessary information regarding the FTP/SFTP server from the NFM-P backup/restore policy and initiates a backup execution on the target device. The driver monitors the backup execution and provides the necessary information to the policy, such as success/failure, date of backup, etc. See the "NE backup and restore" chapter in the *NSP NFM-P Classic Management User Guide* for more information.
Software upgrade – The NFM-P supports software upgrade operations for the MPT-GS. An MPT-GS software package is provided by the vendor with a single file, e.g. siklu-uiimage-6.7.2-15594. The file name must strictly follow the format: siklu-uimage-<major>.<minor>.<sub>-<build #> The software upgrade consists of 3 steps: • download – Transfers the new software to the offline or “not running” software bank. • activate – Reboots the system and switches the active status between the banks. The downloaded software status is set to "Running Wait Accept", whereas the previously active software is set to "Not Running" or offline status. • accept – The new software is accepted, changing its state from "Running Wait Accept" to "Running”. The NFM-P performs reachability checks on GNEs every 10 min by default. Therefore the Accept Timeout parameter default is set to 20 min to allow the NFM-P to detect a node reboot triggered by an activate operation. If the timer for reachability checks for GNEs is changed, the Accept Timeout parameter must be adjusted accordingly or the node auto-reverts before the NFM-P sends the accept command, causing the accept to fail. If the accept time-out expires and an auto-revert occurs, it is recommended to resync the node to see the currently active software version on the NE. The Software tab on the NE form displays the software version and status of each bank. **Note –** When upgrading an operational link of an in-band managed node, upgrade the remote system first and then the local system. Accept the software at both ends after verifying that the link performs as expected. Always upgrade both ends of the link. See the “NE software upgrades” chapter in the *NSP NFM-P Classic Management User Guide* for more information. **Note –** Between activate and accept actions, it is recommended that you perform the following acceptance tests to ensure the radio link is restored correctly and the new software functions properly. RF Link verification - verifies the RF link status as before the upgrade. • Link is up • RSSI values are as prior to the upgrade • CINR values are as prior to the upgrade • ODU reaches the modulation prior to the upgrade RF Link test - verifies error-free operation of the radio link by checking the RF statistics counters for lost/errored packets. • No errors/loss on the RF statistics counters

Pathway to discover and manage the MPT-GS

This pathway describes how to discover and manage the MPT-GS in the NFM-P after driver installation.

Consult the *NSP NFM-P Classic Management User Guide* chapter "Device commissioning and management" for full procedural details.

Create mediation policies and configure a discovery rule

1. Use the NFM-P to create an SNMPv2 mediation policy that specifies “public” as the Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
2. Use the NFM-P to create an SNMPv3 mediation policy with V3 user and credentials as configured on the node. Authentication and privacy algorithms that are supported are MD5 and DES respectively.
3. Use the NFM-P to configure a discovery rule for the MPT-GS that specifies the following mediation policies; see the *NSP NFM-P Classic Management User Guide* for information about creating discovery rules:
   - Read Access Mediation Policy and Write Access Mediation Policy– default mediation policy

     Note – For NE backups and software downloads, the CLI user and password must be set to valid node credentials for the default (or “private” policy).
   - Trap Access Mediation Policy - mediation policy created in step 1

Perform configuration management tasks using the device EMS

1. Right-click on the MPT-GS icon on the NFM-P topology map and choose Open URL.
2. Enter your user name and password. The device EMS opens to allow configuration.

View statistics

1. Click on the Statistics tab of the MPT-GS interface properties form. The MPT-GS Statistics form opens.
2. View statistics as required.

   The availability of historical data requires the activation of Performance Monitoring.

Note: It is recommended that you schedule historical data statistics only, and collect current data statistics on demand. For example, History Data Stats - 15 min returns the same information as Current Data Stats collected for the same 15 minute interval, therefore, it is redundant to schedule Current Data Stats. Scheduling Current Data Stats may result in an error message. Scheduling Interface Additional Stats (Generic NE) is not supported and may result in stopping the collection of other statistics.

Note: The plotting of statistics is supported for Interface Stats (Generic NE).

The following counters are supported.

Interface Type	Statistic Type	Supported Counters
Radio (index 2: ETH0)	Ethernet Aggregate Rx Stats	Total Received Correct Frames Total Received Correct Octets Total Received Severely Errored Frames Rx Throughput (Mbps) Rx Utilization Percentage (%)
	Ethernet Aggregate Tx Stats	Total Transmitted Frames Total Transmitted Octets Aggregate Tx Throughput (Mbps) Aggregate Tx Utilization Percentage (%)
	RSL Hop Current Data Stats - 15 min	Average Level (dBm)
	MPT Equipment Measurement	Temperature (Celsius) Equipment Input Voltage

Interface Type	Statistic Type	Supported Counters
Ethernet (index 3–6: ETH1 to ETH4)	Ethernet Aggregate Rx Stats	Total Discarded Frames Total Received Correct Frames Broadcast Total Received Correct Frames Multicast Total Received Correct Frames Unicast Total Received Correct Octets Total Received Severely Errored Frames Rx Throughput (Mbps) Rx Utilization Percentage (%)
	Ethernet Aggregate Tx Stats	Total Discarded Frames Total Transmitted Frames Broadcast Total Transmitted Frames Multicast Total Transmitted Frames Unicast Total Transmitted Octets Aggregate Tx Throughput (Mbps) Aggregate Tx Utilization Percentage (%)
Note – On the Ethernet interfaces with index 2 (ETH0) and 3-6 (ETH 1-ETH 4), the Interface Stats (Generic NE) are also applicable. **Note –** On the Radio interfaces, real-time plots are not supported and historical plots are supported for all supported counters. **Note –** On the Ethernet interfaces, real-time plots are supported only for interface statistics and historical plots are supported for all supported statistics.		

9500 MPT-SUB6

The MPTSUB6 driver extends the management capabilities of the NFM-P for MPT-SUB6 devices in the following applicable areas.

Table 1-3 MPTSUB6 driver capabilities

Configuration management

Table 1-3 MPTSUB6 driver capabilities (continued)

Radio link inventory – Operators can view all radio links terminating on the device by drilling down from the network topology map or network equipment tree representations of the MPT-SUB6. **Note –**To create a physical link, select the endpoints as type “Port”. Additionally, radio links associated with the MPT-SUB6 device are now included in the inventory list accessed through the Equipment Manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Radio link (Network) from the object type drop-down). Radio link inventory information is also available to the XML API through the installation of the driver, under the following package and class *netw.RadioPhysicalLink*.
Radio port parameters – The driver extends the NFM-P management of the MPT-SUB6 to include its radio port interfaces. With the installation of the driver, a "Radio" tab is added to the Generic NE Interface properties form, allowing NFM-P operators to view the following generic radio port parameters of the device: • Channel Bandwidth (KHz) • Operational Frequency (MHz) • Band • Sector ID • HSU Far-end ID • Current Tx Power (dBm) • Current Rx Power (dBm) — This is not applicable for HBS in Point-to-Multipoint configurations, i.e. HBS connected to multiple HSUs. • MTU - This is not supported for version 2.8.X. • Antenna Type • Available Bandwidth (Mbps) • Encryption Status The following five parameters pertain to the radio link and differ according to the link that is present. The operator can create up to four separate radio links interconnecting the HBS and HSUs. Interfaces 101 – 104 are enabled as radio ports. The Radio panel is associated with each radio port so that operators can access the radio parameters by selecting any of the logical radio interfaces. These parameters are supported only on the Radio tab of HBS, not HSU. • RSL (dBm) • Down-link Throughput (Mbps) • Down-link Peak Throughput (Mbps) • Up-link Throughput (Mbps) • Up-link Peak Throughput (Mbps) These parameters are also available to the XML API under the following package and class *radioequipment.RadioPortSpecifics*.

Table 1-3 MPTSUB6 driver capabilities (continued)

Radio port inventory parameters – The following radio port inventory parameters are displayed on the Inventory tab for the radio ports: • Company ID • Factory ID • Mnemonic • Part No • Serial No • Port ID • Software Part No These parameters are also available to the XML API under the following package and class *radioequipment.RadioEquipmentInventory*.
Radio link discovery - The NFM-P extends link auto-discovery to radio links interconnecting HBS and HSUs. The HSU radio port with index 101 is connected to the HBS logical radio port matching the following criteria: • The remote HBS has the same sectorID as the selected HSU. • The HBS radio port index is equal to 101 + value (.1.3.6.1.4.1.4458.1000.4.1.3.0).
Longitude and latitude – The NFM-P displays the location of the MPT-SUB6 with latitude and longitude. The coordinates are displayed as additional parameters on the General tab of the Properties form. The longitude and latitude parameters are ready-only and are only displayed when the GPS state is synchronized. For all other states, the NFM-P displays an invalid value of 999.
Generic NE Profile automation – The Generic NE Profile for the MPT-SUB6 is automatically created when the MPTSUB6 driver is installed.
Alarm catalog integration – The MPT-SUB6 alarm catalog is automatically populated during driver installation. Operators can edit the alarm catalog to customize alarm characteristics.
NE software version display – The NE software version is displayed on the General tab of the NE Property form.
TMN Inband management – The NFM-P displays the VLAN ID parameter identifying the TMN Inband management traffic/signal. On the Polling tab, click on the TMN Details sub-tab, and double-click on the row. The TMN Inband setting is read-only.
MAC address – The NFM-P displays the MAC Address of the node on the General tab of the NE form. The MAC Address is also accessed through the Equipment manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Network Element (Network) from the object type drop-down).
NTP management – The NFM-P reports NTP-related parameters. NTP enabling and disabling and server configuration is supported through the Alternate Element Manager. Server configuration is also supported using the NFM-P Create option. When the Main and Spare NTP servers are configured with the same IP address, the NFM-P displays only one server. You can modify an NTP server address using the NFM-P, but deleting an NTP server is not supported.

Table 1-3 MPTSUB6 driver capabilities (continued)

Radio encryption status – The NFM-P reports the Encryption Status (enable/disable) at the radio interface. This parameter is read-only.
Sensor measurements – The NFM-P reports the Power Consumption (Watts) and Temperature (Celsius) parameters on the Statistics form.
SNMPv3 support – The NFM-P supports SNMPv3 management of the node.
Port parameters – The NFM-P displays the following read-only parameters on the General tab of each port: • Mode • Encapsulation Type **Note –** The Encapsulation Type parameter is not supported by the NFM-P for HSU. Any displayed value should be ignored. • Speed
Service management
When driver-managed GNE devices are collocated with the 9500 MPR, the NFM-P supports creation of the microwave backhaul service spanning across MPRs and OEMs. The NFM-P recognizes OEM as a site to add to the microwave backhaul service. The NFM-P also recognizes the Ethernet and radio ports on OEM as adjacencies to add to OEM sites. However, the NFM-P does not support deployment of these services to OEM devices. Deployment to OEM devices must be done from the respective EMS. Consequently, discovery of this service does not discover OEM sites. Therefore, OEM sites can be either manually added for the MPTGS/MPTSUB6/MPTGM, or populated using the Complete Ring feature for the MPTGM.
Service assurance
Performance management – The driver extends NFM-P performance management to the MPT-SUB6 so that statistics related to the GNE can be viewed through the NFM-P GUI. Statistics are also available to the XML API; see the *NSP NFM-P Statistics Management Guide*.

Table 1-3 MPTSUB6 driver capabilities (continued)

Alarm resynchronization – Since traps do not have a sequence ID to detect trap gaps, the "auto resynch of alarm table" based on the trap gap is not supported. The NFM-P performs the following for auto alarm table resync: 1. Before a resync of the alarm table, the NFM-P fetches the parameter that contains the "table last change time (or counter)" from the NE. This action is performed every polling interval. 2. The NFM-P compares the value of the last NE change with the value stored in the NFM-P for that alarm table. 3. Only if the NE value is different from the value stored in the NFM-P will the entire alarm table be resynchronized. OR After connectivity is restored, you can perform a manual full node resync from the NFM-P to fetch the current alarms present on the NE at that moment. To ensure that alarm table resync occurs after NE connection is lost with the NFM-P and a trap sequence number mismatch exists between the NFM-P and NE, you can modify the Polling Interval parameter. Choose Administration→Mediation→MIB Entry Policies→fm. CurrentAlarmEntry. For better performance, it is recommended to select 5 min for the Polling Interval. **Note –** For two consecutive polling intervals - If the NE connection is lost and then re-established, and if there are any trap losses in the NFM-P, but the alarm is in the NE alarm table (step 2 above is satisfied), then alarm table resync occurs (step 3 above). If an alarm is raised and cleared in between the interval of a connection lost and re-established from the NFM-P, the NFM-P does not detect the alarm.
Alarm reporting – The NFM-P supports the reporting of all alarms present in the automatically generated alarm catalog.
Radio link fault management – The NFM-P tracks the radio link down scenario. When a radio link interconnects two MPT-SUB6 devices (HBS and HSU), the NFM-P manages the operational state at the node and processes any alarms affecting the radio link extremities. The NFM-P changes the operational state on the General tab of the radio interface based on the link down alarm. **Note –** The operational state on the Radio tab does not change based on link status. When the link is operationally down, the link shows red. When the link is operationally up, the link shows green.
Physical link fault management – The NFM-P tracks the physical link down scenario when a physical link is interconnecting an MPT-SUB6 and an MSS-8/4/1/0. A link down alarm is raised when the LOS (Loss Of Signal) alarm at the MPT-SUB6 port is notified by the node from the NFM-P. The link (physical or radio) is displayed as alarmed in the topology view (red line) and the link down alarm is reported in the alarm list.
Alarm correlation – The NFM-P supports alarm correlation for the following fault scenario: • radio link down • physical link down Both “LinkDown” alarms are correlated to the “adjacencyDown” alarm at the service level.

Pathway to discover and manage the MPT-SUB6

This pathway describes how to discover and manage the MPT-SUB6 in the NFM-P after driver installation.

Consult the *NSP NFM-P Classic Management User Guide* chapter "Device commissioning and management" for full procedural details.

Create mediation policies and configure a discovery rule

1. Use the NFM-P to create an SNMPv1 mediation policy that specifies “public” as the Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
2. Use the NFM-P to create an SNMPv1 mediation policy that specifies “netman” as the Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
3. Use the NFM-P to create an SNMPv3 mediation policy with V3 user and credentials as configured on the node. Security level support is as follows:
   a. No Authentication.
   b. Authentication Only with MD5.
   c. Authentication and Privacy with MD5 and DES respectively.
   d. Authentication and Privacy with SHA and AES respectively.
4. Use the NFM-P to configure a discovery rule for the MPT-SUB6 that specifies the following mediation policies; see the *NSP NFM-P Classic Management User Guide* for information about creating discovery rules:
   - Read Access Mediation Policy and Trap Access Mediation Policy – mediation policy created in step 1
   - Write Access Mediation Policy – mediation policy created in step 2

Perform configuration management tasks using the device EMS

1. Right-click on the MPT-SUB6 icon on the NFM-P topology map and choose Alternate Element Manager. The device EMS opens to allow configuration.
2. Configure the parameters as required.

Note: The EMS is only available if the NFM-P client is on a Windows station. In addition, the EMS manager must be installed in the location pointed to by the default Alternate Element Manager in the Generic NE Profile.

View statistics

1. Click on the Statistics tab of the MPT-SUB6 interface properties form. The MPT-SUB6 Statistics form opens.
2. View statistics as required.

   The availability of historical data requires the activation of Performance Monitoring.

Note: It is recommended that you schedule historical data statistics only, and collect current data statistics on demand. For example, History Data Stats - 15 min returns the same information as Current Data Stats collected for the same 15 minute interval, therefore, it is redundant to schedule Current Data Stats. Scheduling Current Data Stats may result in an error message. Scheduling Interface Additional Stats (Generic NE) is not supported and may result in stopping the collection of other statistics.

Note: On the Radio interfaces:

- real-time plots are supported on all statistics except for Current Data Statistics.
- historical plots are supported on all statistics except for Power Consumption and Temperature Statistics.

Note: On the Ethernet interfaces:

- real-time plots are supported only on interface statistics.
- historical plots are supported on all supported statistics.

The plotting of statistics is supported for Interface Stats (Generic NE).

The following counters are supported on Radio interfaces 101 – 104 on HBS.

Interface Type	Statistic Type
Radio (index 101 – 104)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data Stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
	RSL Hop Current Data stats – 15 min
	RSL Hop History Data Stats – 15 min
	RSL Hop History Data Stats – 24 hr
	TSL Hop Current Data Stats – 15 min
	TSL Hop History Data Stats – 15 min
	TSL Hop History Data Stats – 24 hr
	MPT Equipment Measurement
Note - The aggregate historical data statistics and MPT equipment measurement statistics are not supported for version 2.8.X.	

Interface Type	Statistic Type
Ethernet (index 1 and index 2)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
Note – On Ethernet interfaces with indices 1(ETH) and 2(ETH), the Interface Stats (Generic NE) are also applicable	

On HSU, the following counters are supported only on interface 101.

Interface Type	Statistic Type
Radio (index 101)	Hop Current Data Stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
	RSL Hop Current Data stats – 15 min
	RSL Hop History Data Stats – 15 min
	RSL Hop History Data Stats – 24 hr
	TSL Hop Current Data Stats – 15 min
	TSL Hop History Data Stats – 15 min
	TSL Hop History Data Stats – 24 hr
	Power Consumption (Watts)
	Temperature (Celsius)
Ethernet (index 1)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr

Interface Type	Statistic Type
Ethernet (index 1 and index 2)	Hop Current Data stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
Note – On Ethernet interfaces with indices 1(ETH) and 2(ETH), the Interface Stats (Generic NE) are also applicable.	

9500 MPT-BWA

The MPT-SUB6 driver extends the management capabilities of the NFM-P for the MPT-BWA in the following applicable areas.

Table 1-4 MPTBWA driver capabilities

Configuration management
Radio link inventory – Operators can view all radio links terminating on this device by drilling down from the network topology map or network equipment tree representations of the MPT-BWA. **Note –**To create a physical link, select the endpoints as type “Port”. Additionally, radio links associated with the MPT-BWA device are now included in the inventory list accessed through the Equipment Manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Radio link (Network) from the object type drop-down). Radio link inventory information is also available to the XML API through the installation of the MPT-SUB6 driver, under the following package and class *netw.RadioPhysicalLink*.

Table 1-4 MPTBWA driver capabilities (continued)

Radio port parameters – The MPT-SUB6 driver extends the NFM-P management of the MPT-BWA device to include its radio port interfaces. With the installation of the driver, a "Radio" tab is added to the Generic NE Interface properties form, allowing NFM-P operators to view the following generic radio port parameters of the device:

- Channel Bandwidth (KHz)
- Operational Frequency (MHz)
- Band
- Sector ID
- HSU Far-end ID
- Current Tx Power (dBm)
- Current Rx Power (dBm) — This is not applicable for HBS in Point-to-Multipoint configurations, i.e. HBS connected to multiple HSUs.
- MTU
- Antenna Type
- Available Bandwidth (Mbps)
- Encryption Status

The following five parameters pertain to the radio link and differ according to the link that is present. Operators can create up to 64 separate radio links interconnecting the HBS and HSUs. Interfaces 101 – 164 are enabled as radio ports. The Radio panel is associated with each radio port so that operators can access the radio parameters by selecting any of the logical radio interfaces. These parameters are supported only on the Radio tab of HBS, not HSU.

- RSL (dBm)
- Down-link Throughput (Mbps)
- Down-link Peak Throughput (Mbps)
- Up-link Throughput (Mbps)
- Up-link Peak Throughput (Mbps)

These parameters are also available to the XML API under the following package and class *radioequipment.RadioPortSpecifics*.

Table 1-4 MPTBWA driver capabilities (continued)

NE parameters – The following read-only parameters are displayed on the NE Properties form, General tab: • Name • IP address • Location • SW version • Status • Geographic Location (longitude/latitude) • Up time • MAC Address • Serial Number • Temperature • Power Consumption The Temperature and Power Consumption parameters are refreshed when the NE Properties form is opened. Dedicated statistics based on periodic polling of the power consumption and temperature measures are provided by the NE. These parameters are also available to the XML API under the class *equipment.PhysicalPort*; see the *NSP NFM-P Statistics Management Guide*.
The configuration of the following Radius server parameters is supported at the HBS NE level: • Authorization mode – enable/disable HBS working with a radius server • User name and password – used for HSU authentication • Install confirmation required – if enabled, the HSU registration at HBS is completed when acknowledged by HSU The NFM-P supports the configuration of multiple Radius servers (two servers in nominal network scenario) on a single HBS. Configuration of the following server parameters is supported: • IP address – IP address of Radius server • Port – communication port to which HBS connects • Number of retries – max number of retries in case of connection failure to server • Timeout • Secret string – key used to encrypt passwords and exchange responses for communication between HSB and Radius server The following actions are supported for each server instantiated at HBS: • Clear config – clears selected server configuration Radius server configuration and deletion are supported network-wide through the Bulk Operations tool.

Table 1-4 MPTBWA driver capabilities (continued)

Queue configuration is supported at the radio port level for uplink and downlink traffic. Up to four queues can be enabled and configured on each port. For each queue the following parameters can be configured: • Strict – parameter enabling the strict priority working mode. Enabling strict priority on a queue is allowed only if the higher priority queues are also in strict priority. • Weight [%] – Percentage of the throughput dedicated to the selected queue. If Strict is enabled, the Weight parameter is dimmed. Validation prevents the weight percentage from exceeding 100%. • MIR [Mbs] Network-wide configuration is supported through the Bulk Operations tool.
Mapping between queues and the prio/exp bits range is supported at the NE level. Operators can associate each queue to a range of prio/exp bits. The configuration depends on the QoS mode that is selected: • Disable – queue mapping is disabled • VLAN – each queue can be mapped over a range of prio bits • DiffServ – each queue can be mapped over a range of exp bits Up to four queues are supported. Each queue can be configured as enabled or disabled. Choose Policies→QoS→9500 MPR QoS→9500 NE QoS from the NFM-P main menu.
Radio port inventory parameters – The following radio port inventory parameters are displayed on the Inventory tab for the radio ports: • Company ID • Factory ID • Mnemonic • Part No • Serial No • Port ID • Software Part No These parameters are also available to the XML API under the following package and class *radioequipment.RadioEquipmentInventory*.
Radio link discovery - The NFM-P extends link auto-discovery to radio links interconnecting HBS and HSUs. The HSU radio port with index 101 is connected to the HBS logical radio port matching the following criteria: • The remote HBS has the same sectorID as the selected HSU. • For each HSU the linked HBS radio port index is equal to 100 + value(winlink1000HsuAirHsuId).

Table 1-4 MPTBWA driver capabilities (continued)

Longitude and latitude – The NFM-P displays the location of the MPT-BWA with latitude and longitude. The coordinates are displayed as additional parameters on the General tab of the Properties form. The longitude and latitude parameters are ready-only and are only displayed when the GPS state is synchronized. For all other states, the NFM-P displays an invalid value of 999.
Generic NE Profile automation – The Generic NE Profile is automatically created when MPT-SUB6 driver is installed.
Alarm catalog integration – The MPT-BWA alarm catalog is automatically populated during driver installation. Operators can edit the alarm catalog to customize alarm characteristics.
NE software version display – The NE software version is displayed on the General tab of the NE Property form.
TMN Inband management – The NFM-P displays the VLAN ID parameter and Prio parameter identifying the TMN Inband management traffic/signal. On the Polling tab, click the TMN Details sub-tab, and double-click on the row. The TMN Inband setting is read-only.
MAC address – The NFM-P displays the MAC Address of the node on the General tab of the Network Element form. The MAC Address is also accessed through the Equipment manager (Manage→Equipment→Equipment from the NFM-P main menu, then choose Network Element (Network) from the object type drop-down).
NTP management – The NFM-P reports NTP-related parameters. NTP enabling and disabling and server configuration is supported through the Alternate Element Manager. Server configuration is also supported using the NFM-P Create option. When the Main and Spare NTP servers are configured with the same IP address, the NFM-P displays only one server. You can modify an NTP server address using the NFM-P, but deleting an NTP server is not supported.
Radio encryption status – The NFM-P reports the Encryption Status (enable/disable) at the radio interface. This parameter is read-only.
Sensor measurements – The NFM-P reports the Power Consumption (Watts) and Temperature (Celsius) parameters on the Statistics form.
SNMPv2/v3 support – The NFM-P supports SNMPv2 or SNMPv3 management of the node.
Port parameters – The NFM-P displays the following read-only parameters on the General tab of each port: • Mode • Encapsulation Type **Note –** The Encapsulation Type parameter is not supported by the NFM-P for HSU. Any displayed value should be ignored. • Speed
Service management

Table 1-4 MPTBWA driver capabilities (continued)

When driver-managed GNE devices are collocated with the 9500 MPR, the NFM-P supports creation of the microwave backhaul service spanning across MPRs and OEMs. The NFM-P recognizes OEM as a site to add to the microwave backhaul service. The NFM-P also recognizes the Ethernet and radio ports on OEM as adjacencies to add to OEM sites. However, the NFM-P does not support deployment of these services to OEM devices. Deployment to OEM devices must be done from the respective EMS. Consequently, discovery of this service does not discover OEM sites. Therefore, OEM sites can be either manually added or populated using the Complete Ring feature for the MPTGM.
Service category configuration is supported at the HBS (NE level). There are eight QoS profiles referenced by Radius for service provisioning. The following parameters are associated with the service category class: • Category name - text string representing the service category label • Uplink resources • Downlink resources • Resource type CIR - grants the service a certain guaranteed percentage of HBS resources Best Effort - grants resources as they become available in the sector • MIR Up • MIR Down To configure QoS queues profiles for uplink and downlink traffic, click on the relevant tab to open the QoS configuration form associated with the selected service category. You can configure up to four queues with the selected service category: 1. real time 2. near real time 3. controlled load 4. best effort For each queue, the following parameters can be configured: • Strict - Flag parameter enabling strict priority working mode. Enabling strict priority on a queue is allowed only if the higher priority queues are also in strict priority. • Weight [%] - Percentage of the throughput dedicated to the selected queue. If Strict is enabled, the Weight parameter is dimmed. Validation prevents the weight percentage to exceed 100%. • MIR [Mbs] • TTL [ms] Note: The node accepts TTL values in increments of 5 only. The range of values is 0 to 500 ms. Network-wide configuration is supported through the Bulk Operations tool.
Network assurance
Not applicable
Service assurance

Table 1-4 MPTBWA driver capabilities (continued)

Performance management – The MPT-SUB6 driver extends NFM-P performance management to the MPT-BWA device so that statistics related to the GNE can be viewed through the NFM-P GUI. Statistics are also available to the XML API; see the *NSP NFM-P Statistics Management Guide*.
Alarm resynchronization – Since traps do not have a sequence ID to detect trap gaps, the "auto resynch of alarm table" based on the trap gap is not supported. The NFM-P performs the following for auto alarm table resync: 1. Before a resync of the alarm table, the NFM-P fetches the parameter that contains the "table last change time (or counter)" from the NE. This action is performed every polling interval. 2. The NFM-P compares the value of the last NE change with the value stored in the NFM-P for that alarm table. 3. Only if the NE value is different from the value stored in the NFM-P will the entire alarm table be resynchronized. OR After connectivity is restored, you can perform a manual full node resync from the NFM-P to fetch the current alarms present on the NE at that moment. To ensure that alarm table resync occurs after NE connection is lost with the NFM-P and a trap sequence number mismatch exists between the NFM-P and NE, you can modify the Polling Interval parameter. Choose Administration→Mediation→MIB Entry Policies→fm. CurrentAlarmEntry. For better performance, it is recommended to select 5 min for the Polling Interval. **Note –** For two consecutive polling intervals - If the NE connection is lost and then re-established, and if there are any trap losses in the NFM-P, but the alarm is in the NE alarm table (step 2 above is satisfied), then alarm table resync occurs (step 3 above). If an alarm is raised and cleared in between the interval of a connection lost and re-established from the NFM-P, the NFM-P does not detect the alarm.
Alarm reporting – The NFM-P supports the reporting of all alarms present in the automatically generated alarm catalog.
Radio link fault management – The NFM-P tracks the radio link down scenario. When a radio link interconnects two MPT-BWA devices (HBS and HSU), the NFM-P manages the operational state at the node and processes any alarms affecting the radio link extremities. The NFM-P changes the operational state on the General tab of the radio interface based on the link down alarm. **Note –** The operational state on the Radio tab does not change based on link status. When the link is operationally down, the link shows red. When the link is operationally up, the link shows green.
Physical link fault management – The NFM-P tracks the physical link down scenario when a physical link is interconnecting an MPT-BWA and an MSS-8/4/1/0. A link down alarm is raised when the LOS (Loss Of Signal) alarm at the MPT-BWA port is notified by the node from the NFM-P. The link (physical or radio) is displayed as alarmed in the topology view (red line) and the link down alarm is reported in the alarm list.

Table 1-4 MPTBWA driver capabilities (continued)

Alarm correlation – The NFM-P supports alarm correlation for the following fault scenario: • radio link down • physical link down Both “LinkDown” alarms are correlated to the “adjacencyDown” alarm at the service level.

Pathway to discover and manage the MPT-BWA

This pathway describes how to discover and manage the MPT-BWA in the NFM-P after driver installation.

Consult the *NSP NFM-P Classic Management User Guide* chapter "Device commissioning and management" for full procedural details.

Create mediation policies and configure a discovery rule

1. Use the NFM-P to create an SNMPv1 mediation policy that specifies “public” as the Read/Trap Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
2. Use the NFM-P to create an SNMPv1 mediation policy that specifies “netman” as the Write Community String value. See the *NSP NFM-P Classic Management User Guide* for information about creating mediation policies.
3. Use the NFM-P to create an SNMPv3 mediation policy with V3 user and credentials as configured on the node. Security level support is as follows:
   a. No Authentication.
   b. Authentication Only with MD5.
   c. Authentication and Privacy with MD5 and DES respectively.
   d. Authentication and Privacy with SHA and AES respectively.
4. Use the NFM-P to configure a discovery rule for the MPT-BWA that specifies the following mediation policies; see the *NSP NFM-P Classic Management User Guide* for information about creating discovery rules:
   - Read Access Mediation Policy and Trap Access Mediation Policy – mediation policy created in step 1
   - Write Access Mediation Policy – mediation policy created in step 2

Perform configuration management tasks using the device EMS

1. Right-click on the MPT-BWA icon on the NFM-P topology map and choose Alternate Element Manager. The device EMS opens to allow configuration.
2. Configure the parameters as required.

Note: The EMS is only available if the NFM-P client is on a Windows station. In addition, the EMS manager must be installed in the location pointed to by the default Alternate Element Manager in the Generic NE Profile.

View statistics

1. Click on the Statistics tab of the MPT-BWA interface properties form. The MPT-BWA Statistics form opens.
2. View statistics as required.

The availability of historical data requires the activation of Performance Monitoring.

Note: It is recommended that you schedule historical data statistics only, and collect current data statistics on demand. For example, History Data Stats - 15 min returns the same information as Current Data Stats collected for the same 15 minute interval, therefore, it is redundant to schedule Current Data Stats. Scheduling Current Data Stats may result in an error message. Scheduling Interface Additional Stats (Generic NE) is not supported and may result in stopping the collection of other statistics.

Note: The plotting of statistics is supported for Interface Stats (Generic NE).

Note: On the Radio interfaces:

- real-time plots are supported on all statistics except for Current Data Statistics.
- historical plots are supported on all statistics except for Power Consumption and Temperature Statistics.

Note: On the Ethernet interfaces:

- real-time plots are supported only on interface statistics.
- historical plots are supported on all supported statistics.

The following counters are supported on Radio interfaces 101 – 164 on HBS.

Interface Type	Statistic Type
Radio (index 101 – 164)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data Stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
	RSL Hop Current Data stats – 15 min
	RSL Hop History Data Stats – 15 min
	RSL Hop History Data Stats – 24 hr
	TSL Hop Current Data Stats – 15 min
	TSL Hop History Data Stats – 15 min
	TSL Hop History Data Stats – 24 hr
	MPT Equipment Measurement

Interface Type	Statistic Type
Ethernet (index 1)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
Note – On Ethernet interfaces with index 1(ETH), the Interface Stats (Generic NE) are also applicable	

On HSU, the following counters are supported only on interface 101.

Interface Type	Statistic Type
Radio (index 101)	Hop Current Data Stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr
	RSL Hop Current Data stats – 15 min
	RSL Hop History Data Stats – 15 min
	RSL Hop History Data Stats – 24 hr
	TSL Hop Current Data Stats – 15 min
	TSL Hop History Data Stats – 15 min
	TSL Hop History Data Stats – 24 hr
	Power Consumption (Watts)
	Temperature (Celsius)
Ethernet (index 1)	Aggregate Rx History Data Stats – 15 min
	Aggregate Rx History Data Stats – 24 hr
	Aggregate Tx History Data Stats – 15 min
	Aggregate Tx History Data Stats – 24 hr
	Hop Current Data stats – 15 min
	Hop History Data Stats – 15 min
	Hop History Data Stats – 24 hr

Interface Type	Statistic Type
Note – On Ethernet interfaces with index 1(ETH), the Interface Stats (Generic NE) are also applicable.	

1.2 Wavence management support

1.2.1 Element manager support

Wavence devices support the following external element managers:

- NEtO: opens the GUIs to manage Wavence SA devices (MCT) and Wavence SM devices with Core-Enhanced cards (WebEML)
- WebCT: web interface for Wavence SM devices using the CorEvo card

1.3 NSP

1.3.1 Wavence management using the NSP

You can use the NSP to view, configure, and monitor Wavence objects. Wavence nodes that have been discovered using the NFM-P appear in the NSP, and are available for basic NSP functions including supervision and fault management. You can perform tasks on multiple devices using large-scale Operations, and configure devices and services using Intents. Management tasks you can accomplish using the NSP include the following.

Equipment monitoring:

- **Monitor device utilization and function** using the Network Map and Health dashboard. See the *NSP Network Automation Guide* for more information.
- **Fault management and root cause analysis** using the Network Map and Health dashboard. See the *NSP Network and Service Assurance Guide.*
- **Network inventory** using the Network Inventory view. See the *NSP Network and Service Assurance Guide*. This view supports SMR, displaying UBT-SA nodes as sub-units of IXR or SAR nodes.
- **Track indicators** using NSP data analysis. For information about Wavence-specific object filters, see 3.6 “Wavence example object filters for the NSP” (p. 95). For information about using NSP data collection see the *NSP Data Collection and Analysis Guide*. Statistics collection for Wavence nodes must be configured in the NFM-P.
- **Monitor backhaul service health** using the Network Map and Health dashboard. See 2.16 “To display Wavence backhaul service status information on the NSP Network Map and Health dashboard” (p. 82).

Configuration:

- **Perform software upgrades** using NSP operations. See the *NSP Device Management Guide*.
- **Perform backup and restore actions** using NSP operations. See 2.2.6 “Wavence backup and restore using NSP Operations” (p. 67).

- **Create microwave backhaul services** using intent-based service management. See 15.14 “Microwave backhaul service creation using NSP Intent-Based Service Management” (p. 218)
- **Large-scale device configuration** for MPR system settings on Wavence MSS nodes. See 2.15 “Pathway to configure MPR system settings on Wavence MSS nodes using the NSP” (p. 82) for an overview of how to import a template to configure MSS nodes, and the *NSP Network Automation Guide* and *NSP Device Management Guide* for more information about using the NSP.
- **Change the WebCT password** on Wavence nodes using an NSP operation. See 1.10 “To change the WebCT password on one or more Wavence nodes using an NSP operation” (p. 58).

Troubleshooting:

- **Perform OAM tests** using NSP troubleshooting. See the *NSP Network Automation Guide*.
- **Perform CFM Loopback and CFM DMM tests** using NSP Data Collection and Analysis Management. See 3.7 “Pathway to configure NSP test templates for Wavence CFM Loopback and CFM Stats” (p. 96)
- **Retrieve I&C, RSL, and log files** using NSP operations. See 2.7 “To retrieve RSL files, I&C files, or log files stored by the Wavence using the NSP” (p. 74).

Note: When using the wavence-service-migration operation in NSP, if two VLAN services have been created with the same sites and adjacencies, migrating one of the services will migrate both services – even if they have different VLAN service IDs.

Configuring Wavence operation default wait times

Optionally, you can create an environment file to change the wait time defaults for some operations that apply to Wavence devices. For more information about working with environments, see the Workflows tutorial on the Network Developer Portal. The environment file must be named WaitTimeEnv. The following table describes the variables you can define in the file, and the operations they affect.

Workflow	Variable	Definition	Default
Software Upgrade	SU_ waitTimeToRe-trieveResult	The amount of time, in seconds, to wait for a response before retrying.	120
	SU_ numOfRetries	The number of times to retry getting a response from the NE.	15

Workflow	Variable	Definition	Default
Backup and Restore	backup_ waitTimeToRe-trieveResult restore_ waitTimeToRe-trieveResult	The amount of time, in seconds, to wait for a response before retrying.	60 (backup) 120 (restore)
	backup_ numOfRetries restore_ waitTimeToRe-trieveResult	The number of times to retry getting a response from the NE.	10 (backup) 15 (restore)
Bulk password update	npm_ waitTimeToRe-trieveResult	The amount of time, in seconds, to wait for a response before retrying.	20
	npm_ numOfRetries	The number of times to retry getting a response from the NE.	5
File Retrieval	fileRetrieval_ waitTimeToRe-trieveResult	The amount of time, in seconds, to wait for a response before retrying.	20
	fileRetrieval_ numOfRetries	The number of times to retry getting a response from the NE.	5

Service management considerations

You can provision and activate services across Wavence devices discovered in the NSP. For more information about service management, see the *NSP Service Management Guide.* When using the NSP to manage Wavence services, be aware of the following considerations.

CAHD ports on MSS-4/8 nodes appear available for service deployment, but are only functional when used in a Radio LAG.

1.3.2 Intent-based Wavence configuration

The NSP provides intent types for configuring Wavence devices, contained in the nsp-mpr-icm-intent-types artifact package. If this package is not installed, you can obtain it from the Nokia Support Portal or your Nokia support representative.

Note: Misalignments only appear for attributes and objects configured in the intent. When you make a configuration change that creates new objects or attributes, misalignments are only shown for the changes to objects originally configured by the intent. For example, if you use WebCT to change the Radio QoS classification of a node from Disabled to Diffserv, new attributes and objects become available for configuration, but only the QoS classification attribute displays as misaligned in the NSP. Similarly, when WRED is enabled and Dot1p is configured from NSP, and you disable WRED using WebCT, only the WRED state shows as misaligned in the NSP, not the Dot1p configurations.

Device configuration intents

The following table lists supported device configuration tasks and the related intents to use in the NSP. For example, if you need to perform ethernet port configuration, you would import the icm-wavence-ethernet-port-configuration intent. For information on how to use intent-based device configuration, see the *NSP Network Automation Guide.* For detailed information about each intent, see the *NSP Device Configuration Intent Type Catalog.*

Task	Intent	Notes
Network element configuration	icm-wavence-network-element-config	Use the Bulk Configurations template to configure common parameters on multiple NEs, and the Default template to configure specific parameters for a single NE. For WRED configuration, use the QoS section of the Default template to configure WRED status, color classification, and Dot1p updates. Only use the Bulk template to configure WRED Status.
System preferences configuration	icm-wavence-system-preference	—
Feature and capacity configuration	icm-wavence-feature-capacity	—
Ethernet port configuration	icm-wavence-ethernet-port-configuration	Use the MSS-Based template to configure MSS nodes, the Pizzabox to configure single-shelf (MSS-E/HE/XE or UBT-NIM) nodes, and UBT-SA-Based template to configure UBT-SA nodes.
L3 system interface configuration	icm-wavence-l3-config-system-interface	—
L3 network interface configuration	icm-wavence-l3-config-network-interface	—
TDM port configuration	icm-wavence-tdm-port-specifics	—
Port timing synchronization configuration	icm-wavence-port-timing-config	—
1588 PTP configuration	icm-wavence-1588-ptp	—

Task	Intent	Notes
EPC power saving configuration	icm-wavence-epc-power-saving	Use to configure Light Sleep or Deep Sleep power saving modes, including Timeout values, on radio ports and channels on Wavence nodes.
Shelf timing synchronization configuration	icm-wavence-time-synchronization	—
Loopback radio configuration	icm-wavence-radio-port-specifics	—
Radio queue mapping configuration	icm-wavence-radio-queue-map	—
Radio QoS configuration	icm-wavence-radio-qos	Misalignments only appear for objects and attributes configured in the intent.
Radio port configuration	icm-wavence-radio-port-specifics	—
Radio LAG configuration	icm-wavence-radio-lag-specifics	—
Ethernet ring element configuration	icm-wavence-ring-element	—
Ethernet radio ring configuration	icm-wavence-radio-ring	—

Service configuration intents

The following table lists intents used in service configuration, such as backhaul services and tunnel configuration. For information on how to use intent-based device configuration, see the *NSP Network Automation Guide.*

Task	Intent	Notes
Service tunnel deployment	tunnel	When you create a tunnel template using the intent, select Wavence in the Config Form parameter.
Microwave service backhaul configuration	wavencebackhaul	See 15.14 “Microwave backhaul service creation using NSP Intent-Based Service Management” (p. 218)

Policy distribution intents

The following table lists intents used in policy configuration and distribution, for use with NSP operations such as bulk password changes. The role of each intent is described in the associated procedure.

Task	Intents	Notes
Bulk WebCT password change	icm-wavence-node-password-policy-management icm-wavence-node-password-policy-assignment	See 1.10 “To change the WebCT password on one or more Wavence nodes using an NSP operation” (p. 58)
Backup and restore	icm-wavence-backup-restore-policy icm-wavence-backup-restore-policy-assignment	See 2.2.6 “Wavence backup and restore using NSP Operations” (p. 67)
File retrieval (RSL, I&C, or log files)	icm-wavence-file-retrieval-policy icm-wavence-fileretrieval-policy-assignment	See 2.7 “To retrieve RSL files, I&C files, or log files stored by the Wavence using the NSP” (p. 74)
Software upgrade	icm-wavence-software-upgrade-policy icm-wavence-software-upgrade-policyassignment	See the *NSP Device Management Guide* and the *NSP Device Configuration Intent Type Catalog*.

1.4 NEtO

1.4.1 Overview

NEtO installation files are not bundled with the NSP and must be separately obtained as a part of the node software SWP, or as part of the TCO suite downloaded from the customer support portal for the node. When using the TCO suite, perform the following:

1. Locate the NEtO files in the WebEML directory of the TCO suite
2. Copy the files to the following directory of the client system:

   local_path\nsp\nms\thirdparty\neto

   where *local_path* is the location where the NSP client is installed

You can launch the NEtO from the NFM-P GUI; see 7.7 “To cross-launch NEtO from NFM-P” (p. 125) .

For the Wavence SA, NEtO cross-launch is possible only if the registration table entry has not reached the limit of 15 entries. Additionally, cross-launch to a node using IPv6 is successful only if the node can be reached from the NFM-P client initiating the cross-launch, and an IPv6 route exists.

NEtO cross-launch tasks are recorded in the NFM-P user activity log. To view the task status, choose Administration→Security→User Activity from the NFM-P main menu. The log indicates whether the cross-launch was successful.

1.4.2 NEtO distribution through NFM-P

NFM-P manages the distribution of the NEtO application and all related profiles. Any discovered Wavence NE has all cross-launch paths automatically configured in database so that no user configuration is required to use the NEtO. The cross-launch function also supports the option to run TACACS+ in the network, in which case NEtO has a NULL authentication when cross-launched, and the user is prompted for a username and password.

The NFM-P supports the selection of user profiles to access the NEtO. The Admin NEtO launch, Viewer NEtO launch, and Default NEtO launch are the NFM-P scope of command roles that allow access to the NEtO for a specific user profile. See the *NSP System Administrator Guide* for the list of scope of command roles. See 7.6 “To configure a scope of command role for NEtO access” (p. 124) for information about configuring a scope of command role for access to the NEtO for the required user profile.

1.4.3 Service management with Wavence element manager

You can use the Wavence element manager to manage services on the Wavence. The use of an external element manager to change key network management information usually managed by NFM-P (such as service IDs, SAP or site information, or VLAN information) could result in data loss or corruption. To avoid this problem, site information persists so that management actions (such as moving service access from one DS1 port to another) do not result in data loss.

Configuration of the following can only be performed using a Wavence element manager:

- cards
- port usage
- Radio LAGs
- port and card protection

NFM-P takes the following additional actions to accommodate service changes made using the Wavence element manager:

- A move between ports generates an alarm. The new port attachment is discovered and the deleted port is retained. The user can copy provisioning information to the new port in the NFM-P or manually reverse the change, if required.
- A move between radio backhaul paths generates an alarm and is accepted. The alarm message retains the old and new path information, allowing the user to change the service back to its original form, if required.
- A move between radio and Ethernet backhaul paths generates an alarm and is accepted. The alarm message retains the old and new path information, allowing the user to change the service back to its original form, if required.
- When using a Wavence element manager to change VLAN IDs for a service, the new service is discovered and alarms are generated for both services. An informational alarm is generated for the new service, and a major alarm is generated for the old service.

- A cleanup on the service deletes all new discovery alarms and old SAPs, and accepts the new SAPs.
- Service changes from the Wavence element manager are not supported for ERPS (radio or fiber).

1.5 WebCT

1.5.1 Overview

WebCT is the web interface for Wavence devices using the CorEvo card. WebCT provides configuration information, alarms, monitoring, and administration functions. See the *Wavence WebCT User Manual* for more information about WebCT.

NFM-P supports the cross-launch of WebCT from the equipment navigation tree and the topology map. You can also reset the password for the WebCT initial user using the NFM-P.

NSP supports the cross-launch of WebCT from the Network Map and Health view using the Open in NE Session action.

WebCT password complexity rules

By default, the minimum password length for WebCT is 8 characters. However, you can configure minimum password length and complexity on WebCT, and the settings can be viewed, but not modified, in NFM-P and NSP. When you change the WebCT password using NFM-P or NSP, the new password is validated against the WebCT password rules, and passwords that violate the rules are rejected.

After you change the password settings for WebCT, you can use the NSP to update WebCT passwords on one or more nodes; see 1.10 “To change the WebCT password on one or more Wavence nodes using an NSP operation” (p. 58).

TACACS+

TACACS+ server settings can be configured for UBT-SA and MSS-XE nodes using WebCT. After the server settings are configured, a resync must be triggered for the settings to appear in the NFM-P. See the *NSP NFM-P Classic Management User Guide* for information about performing a resync on a node.

1.6 To open WebCT from NSP

1.6.1 Steps

1

In the **Network Map and Health, Network Inventory View** dashboard, expand the Network Elements panel and select the Wavence device you need to manage.

2

Click **(Table row actions), Open in NE Session** to launch the WebCT interface for the selected Wavence device.

END OF STEPS

1.7 To open WebCT from NFM-P

1.7.1 Steps

Note: The external EMS browser is supported on the latest release of Firefox, IE, Chrome, and Safari.

1

Choose Equipment from the navigation tree view selector. The navigation tree displays the Equipment view.

2

Right-click on a Wavence device that has a CoreEvo and choose Launch External EMS Browser. The WebCT main view screen appears in the secure mode (https) or normal mode (http) depending on the Wavence device configuration.

Note: If a browser is not configured in the NFM-P user preferences, the default browser of the operating system is used to open the application.

END OF STEPS

1.8 To reset the WebCT password on a Wavence UBT-SA node

1.8.1 Purpose

An administrator can use the NFM-P to reset the password of the initial user for the WebCT interface of a Wavence UBT-SA node. The password is reset to the default value; see the node documentation for information about the default password. Only the password of the initial user is reset, any other users configured on the node are unaffected.

Note: After the password is reset, a warm reboot is triggered to apply the change.

1.8.2 Steps

1

In the navigation tree Equipment or Routing view, right-click on a Wavence UBT-SA and choose Properties. The Wavence network element form opens

2

Click on the System Settings tab.

3

Configure the WebCT Initial User Password Reset parameter to True, and save your changes. A confirmation dialog appears.

4

Click Yes. The node will perform a warm reboot and reset the WebCT initial user password to the default value.

END OF STEPS

1.9 To change the WebCT password on one or more Wavence nodes using the NFM-P

Note: Do not change the WebCT password on a Wavence node while a file retrieval is in progress.

1.9.1 Steps

1

Choose Administration→NE Maintenance→Node Password Management from the NFM-P main menu. The Node Password Management form opens.

2

In the Password Policy tab, click Create. The Node Password Management Policy form opens.

3

Configure the parameters as required, ensuring the old password and a new password are provided, then click Apply.

4

In the Node Password Management Policy Assignment tab, distribute the policy to the Wavence nodes you need to configure, then click OK.

5

In the Node Password Manager tab of the Node Password Management form, select one or more Wavence nodes and click the Update Password button. The NFM-P attempts to change the WebCT password for each node to the new password from the assigned policy.

6

You can confirm the status and completion of each password change in the Node Password Update Status tab of the Node Password Policy Management form for the policy.

END OF STEPS

1.10 To change the WebCT password on one or more Wavence nodes using an NSP operation

1.10.1 Prerequisites

You can use an NSP Operation to change the WebCT password on one or more Wavence nodes. The operation artifacts required to perform this task on Wavence devices are included in the Wavence artifact package; this package can be acquired from the Nokia Support Portal or your Nokia support representative.

1.10.2 Steps

Deploying password policies

1

Log in to the NSP and ensure that the nsp-ne-wavence-password-update and nsp-mpr-icm-intent-types artifact packages are installed. See the *NSP Network Automation Guide* for information about managing artifacts. If you have already configured and distributed password policies in the NFM-P, skip to Step 6.

2

Click on the NSP Menu and select Device Management. In the Configuration Intent Types view, import the following intent type: icm-wavence-node-password-policy-management

3

In the Configuration Templates view, create a configuration template for the intent you imported and click Release.

4

In the Configuration Deployments view, create a deployment using the configuration template you created. Configure the parameters as required.

5

Click Deploy to deploy the configuration template.

Assigning password policies to Wavence nodes

6

In the Configuration Intent Types view, import the following intent type: icm-wavence-node-password-policy-assignment

7

In the Configuration Templates view, create a configuration template for the intent you imported and click Release.

8

In the Configuration Deployments view, create a deployment using the template you created. Select the Wavence NEs you need to modify as targets in the template, and select the password configuration template you deployed in Step 5 from the list of policies available in the template. If you are using a password policy that was configured and distributed using the NFM-P, enter the unique Policy ID for the NFM-P password policy.

9

Click Deploy to deploy the configuration template. The password policy is assigned to the selected target NEs.

Performing an operation

10

In the All Operations view, create an operation using the nsp-ne-wavence-password-update operation type.

11

Configure the parameters as required, and select the same Wavence NEs you selected in Step 7 as targets of the operation.

12

Start or schedule the operation. For information about configuring and scheduling operations, see the *NSP Device Management Guide*.

END OF STEPS

2 Wavence device commissioning and management

2.1 Overview

2.1.1 General description

The Wavence requires commissioning and device-specific preconfiguration before NFM-P can discover and manage the device. See 2.3 “Pathway to commission and manage Wavence devices” (p. 70) for the sequence of high-level tasks required to commission a Wavence before discovery by NFM-P.

The Wavence requires two mediation policies be created manually as part of the discovery rule creation process: a read-write mediation and a trap mediation policy.

Note: While creating the read-write mediation policy, you must select FTP for the file transfer type, and specify the FTP username “ftp” and FTP user password “ftp”. While creating the trap mediation policy, you must specify “SNMP-trap” as the SNMP v1/v2c community string.

2.2 Wavence management

2.2.1 Supported management traffic types

A Wavence device requires preconfiguration before NFM-P management of the device is possible. NFM-P supports in-band and out-of-band management of devices.

When you configure in-band management only, management traffic between NFM-P and a Wavence is transmitted through any port that is configured for network access, but not the management port. Using in-band management, NFM-P sends management traffic to the system IP address of the device, or to an optional L3 management interface.

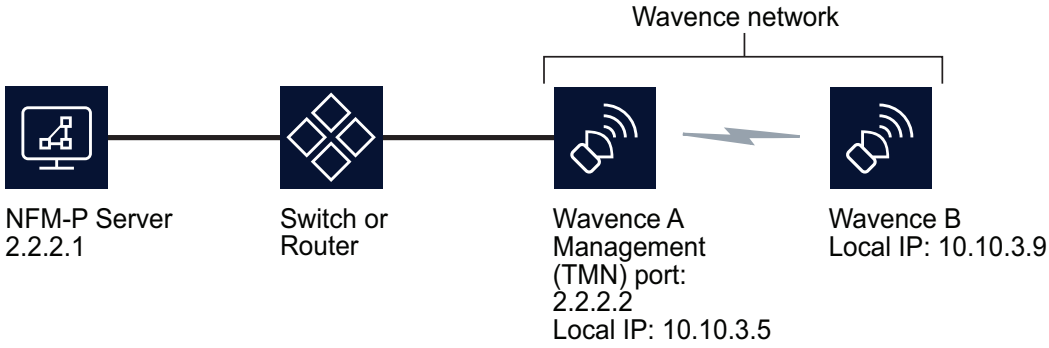
When you configure out-of-band management only, management traffic between NFM-P and a Wavence is transmitted through the management port of the device. Using out-of-band management, NFM-P sends management traffic to the management IP address of the device. See the *NSP NFM-P Classic Management User Guide* for more information about device bandwidth management.

Note: A Wavence device can be managed by up to five instances of NFM-P.

In-band management of Wavence devices

To enable Wavence in-band management, NFM-P requires connectivity to the Wavence NE, as shown in Figure 2-1, “Example of Wavence in-band management” (p. 62) and described in the associated example configuration steps. Ensure that the trap receiving interface on the NFM-P server is configured with the IP address of the in-band NIC that connects to the Wavence network.

Figure 2-1 Example of Wavence in-band management



Perform the following initial configuration on the Wavence:

1. Connect Wavence Node 1 to the switch using the TMN port or port 4 of the Wavence A.

   When NFM-P is connected to the Wavence network via non-Wavence devices like the 7705 SAR or 7750 SR, expect that the TMN in-band feature is enabled on Node 1 of the Wavence that is connected to non-Wavence devices. For example:

   NFM-P → 7705 SAR_1/1/1 → port1/4_Wavence1 → (Radio) → Wavence2

   In the preceding example, Wavence Node 1 and port 1/4 are enabled with VLAN ID and IP addresses, and the 7705 SAR is configured with the same VLAN and IP address from the same subnet.
2. Ensure that the Radio links between the Wavences are working by pinging the local IP addresses. A connection between two Wavence NEs could be over an Ethernet or optical link. If the core Ethernet or core optical port is used between two Wavences, the ports should be enabled with TMN in-band on the Wavence.

Note: The management port IP, TMN in-band IP, and local IP can be in different subnets.

Perform the following network configuration:

1. Verify that you can ping the local IP address of all the NEs from the NFM-P server.
2. Verify that you can ping the NFM-P server IP address from each of the Wavence NEs.

   Note: You can manage the Wavence through the local IP address even though the management interface of the NFM-P server is not reachable.
3. NFM-P should be able to discover and manage the local IP addresses of the Wavences after connectivity is established between the NFM-P and the Wavence NEs.

2.2.2 LAC management of Wavence devices

Introduction

NFM-P provides a Local Access Control (LAC) management synchronization mechanism to allow or deny (inhibit) user access to configure Wavence devices using a Local Craft Terminal (LCT). This prevents multi-write access sessions on Wavence devices. You can also enable or disable whether NFM-P receives LAC alarms from the nodes.

Enable LAC management

You can enable LAC management by configuring the Enable LAC Management parameter on the MPR tab of the Administration→System Preference→System Preference form. Enabling LAC management automatically denies LCT access to nodes that are newly managed only. There is no impact to existing managed Wavence nodes.

After the Enable LAC Management parameter is configured, you can enable or disable LAC alarms by configuring the Enable LAC Alarms parameter on the MPR tab of the Administration→System Preference→System Preference form. NFM-P generates a “LAC requested” alarm indicating LCT use is requesting access to the node. When disabled, no new alarms will be generated. The Enable LAC Alarms parameter cannot be configured if the Enable LAC Management parameter is disabled.

Note: The Enable LAC Management parameter is disabled by default. Therefore, the LAC state of any node that is newly managed by NFM-P will not be altered. This is done to allow LCT access for those users who normally provision the Wavence using a Wavence element manager or the 1350 OMS.

LAC management status of a Wavence device

You can configure the LAC management status of a Wavence device at the node level by selecting the node in the navigation tree Equipment view, and choosing Properties. The Network Element form opens. Click on the System Setting tab and verify the LAC state parameter in the LAC Configuration panel. You can reconfigure the LAC State parameter if required; any changes made at the NE level will only affect that NE.

Note:

- The LAC configuration parameters are available for configuration only if the LAC management is enabled. See “Enable LAC management ” (p. 63) for more information about enabling LAC management.
- The NFM-P allows you to unmanage a Wavence device regardless of the LAC status.

If the LAC management state of the node is set to Access Denied, LCT users can request access to the node from an LCT session to NFM-P. When this request is made, a LocalAccessRequest alarm is generated after the specified wait time and appears in the Alarm window.

You can:

- grant access to the LCT by changing the LAC state to Access Granted.
- deny access to the LCT by changing the LAC state to Access Denied.

2.2.3 Supported Radio links

Radio links between Wavence devices are autodiscovered by NFM-P. The autodiscovery is supported for the following Radio link types:

- 1+0 radio links; represented by a dashed line on topology maps
- 1+1 radio links; the main link is represented as a dashed green line and the spare links are displayed as dashed blue lines when no alarms exist
- L1 LAG and L2 LAG; represented by a bold dashed line

After the autodiscovery, NFM-P displays the following parameters on the Radio tab of the Physical Port (Edit) form:

- Remote IPv6/IPv4 Address
- Remote Interface
- Remote Port

The Radio interface can be:

- MPT-HC
- MPT-HC-HQAM
- MPT-XP-HQAM
- MPT-HLv1
- MPT-HLv2
- UBT-C
- UBT-m/S/S2
- UBT-T and UBT-T XP
- UBT-I/I2

See the Wavence documentation for a complete list of supported radios.

Radio links between Wavence devices are shown as physical links by NFM-P, with ports as the endpoint type.

To enable Wavence radio link discovery and management, NFM-P requires connectivity between the Wavence NE radio ports, as shown in the following figure. Table 2-1, “Connectivity parameter details” (p. 65) lists the connectivity parameter details for each supported shelf type.

Figure 2-2 Connectivity example for Wavence radio link discovery and management

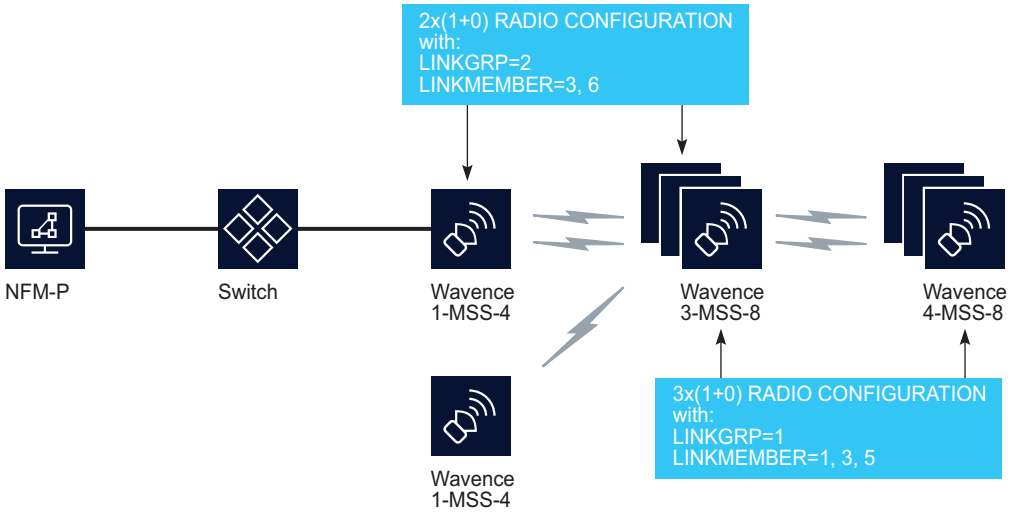


Table 2-1 Connectivity parameter details

Shelf type	1-MSS-4	2-MSS-4	3-MSS-8	4-MSS-4
2-MSS-4	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (as assigned)	—
3-MSS-8	PPPRF Enabled LinkID (23, 23) PPPRF Disabled LinkID (26, 26)	PPPRF Enabled LinkID (as assigned)	—	PPPRF Enabled LinkID (11, 11) PPPRF Disabled LinkID (13, 13) PPPRF Disabled LinkID (15, 15)

To discover multiple radio links, you must provision the radio ports on the Wavence based on the following criteria:

1. Only one radio port can have PPPRF enabled. The far endpoint on the same link must have the same configuration as the first endpoint. PPPRF should be disabled on both endpoints for the second and any subsequent radio links.
2. LinkID requirements include:
   - The LinkID must be enabled for all of the port members of the configuration that have the same LINKGRP, and a different LINKMEMBER that matches the far endpoint.
   - Expected and Sent values must be equal (for example, 11, 11 or 13, 13).
   - For a multiple N × (1+x) radio configurations on the same NE, the LINKGRP must be unique without overlapping (for example, 1 and 2).
   - LinkID should be formatted as LINKGRP:LINKMEMBER in a hexadecimal format where LINKGRP is the first character and LINKMEMBER are the members.

- Any mismatch between the LinkID at the link level (for example, Send is not equal to Expected) mutes the radio connection (MPT case).

3. As a requirement for the first radio link to be discovered, the remote address must be present at both endpoints. For subsequent links, alarms cannot be present on the radio port.
4. When radio link aggregation is enabled for any of the radio links between two Wavences, all radio links must belong to the same LAG.
5. When 1+1 configuration is deleted resulting in two 1+0 radio links, NFM-P can display incorrect information for the remote interfaces. The Remote interface for the previously Spare port can be set to the Main port or 0. The incorrect information occurs because the Wavence node sends incorrect values in the transient phase.
6. When the LAG member links are deleted, NFM-P does not update the display of the link. For example, the LAG configuration with links to two members can display as one link or no link even after the two links are deleted. The incorrect information occurs because the Wavence node sets the remote interface to 0 momentarily.

Note: By default, the PPPRF parameter is enabled and dimmed on the NFM-P GUI. Use the Wavence element manager to disable or enable the PPPRF parameter, if required.

When you configure out-of-band management, the PPPRF and LinkID parameters do not need to be enabled for the Wavence, Release 5.2, 6.0, or later. If the PPPRF and LinkID parameters are disabled on all the radio ports, the radio links are still discovered successfully and the criteria 1 and 2 are not applicable.

When you configure in-band management, the 1+0, 1+1 radio links between two Wavence nodes require the PPPRF parameter to be enabled on the radio ports for NFM-P to discover the far end Wavence node. The 2+0, 3+0, 4+0 radio links between two Wavence nodes require the PPRF parameter to be enabled on one of the radio links at both ends. The PPPRF and LinkID parameters need not be enabled for other radio links.

2.2.4 Wavence radio link protection schemes

You can apply Wavence radio link protection by configuring the Protection Type parameter in the Wavence element manager. Additionally, you can switch between an in-service protected radio link and a standby protected link to perform routine maintenance tasks using the Wavence element manager. See the Wavence documentation for more information.

In-service protected radio links are represented as dashed green links on the physical topology map; standby links are shown as dashed blue links; out-of-service radio links, main or spare, are represented as dashed red links. If a mismatch of active and standby states should occur, main links are represented as dashed green links on the Physical topology map; spare links are shown as dashed blue links on expansion.

Note: The status of a protected link does not have a direct impact on the status of a service. See Table 15-4, “Wavence service status” (p. 215) for more information about the service status.

2.2.5 SNMPv3 authentication and privacy protocol support

Support for authentication and privacy protocols varies by node type and node release. SNMPv3 users are configured using the NFM-P, matching the SNMPv3 configuration on the node, which is configured using WebCT.

SNMPv3 protocol support for Wavence, Release 25 or later

For devices using Wavence Release 25 or later, the following authentication protocols are supported on MSS-8 CorEvo, MSS-E/HE/XE/NIM, and UBT-SA nodes:

- HMAC-SHA-96
- HMAC-SHA2-256
- HMAC-SHA2-384
- HMAC-SHA2-512

Additionally, MSS-8 CorEvo-based nodes also support the HMAC-MD5-96 protocol.

The following privacy protocols are supported on the same nodes:

- AES128 CFB128
- AES192 CFB128
- AES256 CFB128

SNMPv3 protocol support for Wavence, Release 24 or earlier

For devices using Wavence, Release 24 or earlier, the following authentication protocols are supported on MSS-8 CorEvo-based nodes:

- HMAC-MD5-96
- HMAC-SHA-96 (only in combination with a privacy protocol)

Authentication protocols are not supported on MSS-E/HE/XE/NIM or UBT-SA nodes using Wavence, Release 24 or earlier.

The following privacy protocols are supported on MSS-8 CorEvo, MSS-E/HE/XE/NIM, and UBT-SA nodes:

- AES256 CFB128

2.2.6 Wavence backup and restore using NSP Operations

Note: NSP backup file management tools (finding or comparing backup files, for example) are not supported for Wavence backup files. Backup file management requires that the files are stored on the NSP file server, and Wavence backup files are managed through the NFM-P.

You can perform backup and restore operations on one or more Wavence devices using the Device Management view in the NSP. The operation artifacts required to perform backup and restore operations on Wavence devices are included in the Wavence artifact package; this package can be acquired from the Nokia Support Portal or your Nokia support representative. The following pathway describes the high-level steps to prepare for and perform a restore or backup operation on a Wavence node using the NSP. For general information on using operations, see the *NSP Device Management Guide.*

Deploying policies

1

Click on the NSP Menu and select Device Management. In the Configuration Intent Types view, import the following intent types: icm-wavence-backup-restore-policy and icm-wavence-backup-restore-policy-assignment.

2

Create and deploy a configuration template and configuration deployment using the icm-wavence-backup-restore-policy intent. Ensure that the Auto Reboot parameter is enabled, and configure the file transfer settings as required. See the *NSP Network Automation Guide* for information about configuring intents.

Assigning policies

3

Create and deploy a configuration template and configuration deployment using the icm-wavence-backup-restore-policy-assignment intent. In the configuration deployment, select the backup and restore policy you created in Step 2, and select the target NEs. See the *NSP Network Automation Guide* for information about configuring intents.

Performing an operation

4

In the All Operations view, create operations as required, using the following operation types:

- to perform a backup, use the nsp-ne-wavence-backup operation
- to perform a restore, use the nsp-ne-wavence-restore operation

Alternatively, you can perform a backup on a specific node by selecting the node in the Managed Network Elements view and clicking on **(Table row actions), Create an operation, Backup**. You can perform a restore by selecting a previous backup operation in the Operation History view and clicking on **(Table row actions), Restore**.

For information about configuring and scheduling operations, and managing backup and restore operations, see the *NSP Device Management Guide*.

2.2.7 Wavence backup and restore policy requirements for NFM-P

The NFM-P provides backup and restore functions which are supported on some Wavence devices, provided backup and restore policies have been created and distributed to Wavence nodes. See the *NSP Classic Management User Guide* for information about configuring policies and using NFM-P backup and restore. This section describes configuration information for Wavence backup and restore policies.

Auto-reboot configuration

When you configure a backup policy for a Wavence device, ensure the Auto Reboot After Successful Restore option is enabled.

SFTP configuration

Core Evo devices only support software download using SFTP. When configuring SFTP on a policy, the following parameters must be provided:

1. SFTP User ID
2. SFTP password
3. Path to file storage location on the SFTP server
4. Host fingerprint

The SFTP user must have access to the file storage location path. For UBT-SA nodes, the file storage location path must be an absolute path from the / directory. For other nodes, a subjective path can be specified; the root directory for the subjective path is the home directory of the SFTP user.

Note: For nodes other than UBT-SA, if the folder specified in the path does not exist, the SFTP user will attempt to create the required folder structure. The policy may fail if the SFTP user cannot create the folder; for example, a non-administrative user creating a folder in the root directory, or in a location they do not have access to. Ensure that the file storage location exists or that the specified SFTP user has the permission required to create it.

To obtain the host fingerprint, see “To determine a host fingerprint” (p. 102) for information about NFM-P host fingerprints. Some nodes require a specific signature system, as follows:

- **MSS-E/HE/XE and UBT-NIM nodes, Wavence Release 23A** or later, only support using ED25519 fingerprints. Use the following command to obtain the correct fingerprint:

  ```
  ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_ed25519_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'
  ```

  Earlier releases and all UBT-SA nodes only support using RSA fingerprints. Use the following command to obtain the correct fingerprint:

  ```
  ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_rsa_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'
  ```

- **MSS-4/8** nodes only support using ECDSA fingerprints. Use the following command to obtain the correct fingerprint:

  ```
  ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_ecdsa_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'
  ```

- **UBT-SA** nodes only support using RSA fingerprints. Use the following command to obtain the correct fingerprint:

  ```
  ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_rsa_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'
  ```

2.2.8 Wavence log file retrieval

The NFM-P and NSP support the retrieval of log files stored by the Wavence devices.

The logs include:

- all user administration operations and the configuration changes in user activity logs in a user readable format. One entry is captured for each user action.

- all the security-related events in a security audit trail. These events include all security-related settings changes, user accounts management, exporting audit logs, and user login attempt failure.

Three types of log files are stored:

- UAL LOG
- SNMP LOG
- AUDIT LOG

Log file compression

You can use the File Compression parameter on the Log Retrieval configuration form (Administration→NE Maintenance→Log Retrieval) to compress log files before storing. The following compression options are supported: none, ZIP, and GZIP.

See 2.10 “To retrieve log files stored by Wavence devices using the NFM-P” (p. 77) for more information about retrieving logs.

2.3 Pathway to commission and manage Wavence devices

2.3.1 General information

The following pathway describes the high-level tasks required to commission Wavence devices before discovery by NFM-P.

2.3.2 Process

1

Prepare the Wavence for NFM-P management by commissioning the device before NFM-P discovery. See the pathway to commission Nokia devices in the “Device commissioning and management” chapter of the *NSP NFM-P Classic Management User Guide* for the procedures that apply to this device type. In addition, perform the following device-specific procedures as required.

2

Configure an SNMP user, the required security mediation policy, and discovery rule for a Wavence; see 2.4 “To prepare a Wavence NE for NFM-P management” (p. 71).

3

Configure how and when NFM-P polls the device for MIB changes; see 2.5 “To configure polling for a Wavence” (p. 73).

4

Enable the collection of Wavence statistics from the NFM-P auxiliary server; see 2.6 “To collect Wavence statistics from an NFM-P auxiliary server ” (p. 74).

2.4 To prepare a Wavence NE for NFM-P management

2.4.1 General information

The following procedures describe how to prepare Wavence devices (and variants) for commissioning before NFM-P can manage them.

Perform this procedure to configure an SNMP user, the required security mediation policy, and discovery rule for a Wavence NE.

Note: Ensure that you create the mediation policy based on whether the Wavence device supports SNMPv2 or SNMPv3, along with the appropriate Trap mediation policy with community string.

2.4.2 Steps

1

Create an SNMPv3 user on NFM-P.

1. Choose Administration→Security→NE User Configuration from the NFM-P main menu. The NE User Configuration form opens.
2. Click Create. The NE User, Global Policy (Create) form opens.
3. Configure the parameters as required. For the Access parameter, you must choose the SNMP option.
4. Click on the SNMPv3 tab and verify that the SNMPv3 user and user group have been created on the managed NE.

   When a user has been assigned the appropriate SNMPv3 permissions, you can configure the following authentication parameters:
   - Authentication Protocol—Choose an authentication protocol. Protocol support varies by node and release, see 2.2.5 “SNMPv3 authentication and privacy protocol support” (p. 67).
   - Privacy Protocol—Choose a privacy protocol.
   - Set New Authentication Password—enter and confirm a new authorization password.
5. Click OK to close the form and click Search to confirm the creation of the SNMPv3 user.

2

Configure an SNMPv3 mediation security policy for the SNMPv3 user created in Step 1.

1. Choose Administration→Mediation from the NFM-P main menu. The Mediation (Edit) form opens.
2. Click on the Mediation Security tab and click Create. The Mediation Policy (Create) form opens.
3. Configure the Displayed Name parameter to identify the policy and set the Security Model parameter to SNMP v3 (USM).
4. In the SNMP panel, set the Port parameter to 161.

5. In the SNMPv3 panel, click Select and choose the SNMPv3 user created in Step 1 and click OK. The Mediation Policy (Create) form reappears.
6. Save your changes and close the forms.

3

Perform one of the following to configure SNMP management and to create a discovery rule for Wavence devices.

Note: NFM-P uses the default SNMPv2 mediation security policy to discover the Wavence.

a. To configure a discovery rule that uses SNMPv3 management, see the “Device discovery” chapter in the *NSP NFM-P Classic Management User Guide*.

b. To configure a discovery rule that uses SNMPv2 management:

Perform the following steps:

1. Choose Administration→Discovery Manager from the NFM-P main menu. The Discovery Manager (Edit) form opens.
2. Click Create. The Create Discovery Rule step form opens with the Specify General Attributes step displayed.
3. Configure the parameter as required and click Next. The Add Rule Elements step appears.
4. Click Create, configure the required parameters, and click OK. The Create Discovery Rule step form reappears.
5. Click Next. The Add Auto Discovery Rule Elements ACL step appears.
6. Optionally, click Create, configure the parameter as required, and click Next. The Configure Mediation Security step appears.
7. Click Select and choose the mediation security policy created in Step 2 in the Read Access, Write Access, Trap Access, and Security Access Mediation policy panels.
8. Click Finish and close the form. All other steps on the Create Discovery Rule step form are optional for the Wavence.

4

Use the NFM-P client to discover the NE and to verify that the NE configuration allows management of the Wavence; see the “Device discovery” chapter in the *NSP NFM-P Classic Management User Guide*.

END OF STEPS

2.5 To configure polling for a Wavence

2.5.1 Steps

1

In the navigation tree Equipment or Routing view, right-click on a Wavence and choose Properties. The Wavence network element form opens.

2

If required, record the system IP address and management IP address for future configuration requirements.

3

If required, configure the Location and Current OLC State parameters.

Note: While other OLC parameters may be displayed (for example, Lock OLC State), they do not apply to Wavence nodes and cannot be configured.

4

Click on the Polling tab and configure the Scheduled Polling parameter.

5

To determine the current polling status:

The read-only parameters provide the following information.

- Resync Status indicates whether the last poll successfully completed.
- Last Resync Start Time and Last Resync End Time indicate the start and finish of the last poll.
- Scheduled Resync Status indicates whether the last scheduled poll successfully completed.
  Note: Scheduled resynchronization is disabled, by default, for specific MIB entries. Choose the MIB entry policy in the MIB Entry Policies tab of the Administration→Mediation→Mediation (Edit) form, click Properties, then configure the Polling Interval parameter to enable scheduled resynchronization.
  Enabling scheduled resynchronization of the MIB entries for which the scheduled resynchronization is set to disabled by default may have a performance impact.
- Last Scheduled Resync Start Time and Last Scheduled Resync End Time indicate the start and finish of the last scheduled poll.

6

Save your changes and close the form.

END OF STEPS

2.6 To collect Wavence statistics from an NFM-P auxiliary server

2.6.1 Purpose

Perform this procedure if you plan to use an NFM-P auxiliary server to collect Wavence statistics using IPv4 or IPv6.

2.6.2 Steps

1

Choose Administration→System Information from the NFM-P main menu. The System Information form opens.

2

Click on the Auxiliary Servers tab, choose an auxiliary server from the list, and click Properties. The Auxiliary Server (View) form opens.

3

Click on the Auxiliary Services tab, select the STATS_SERVICE entry from the list, and click Properties. The Auxiliary Service - STATS_SERVICE (Edit) form opens.

4

If you are using IPv6, configure the IPv6 Address parameter and click OK.

Note: During the subsequent device discovery, NFM-P registers the IPv6 address of the auxiliary server on each discovered Wavence.

5

Save your changes and close the forms.

END OF STEPS

2.7 To retrieve RSL files, I&C files, or log files stored by the Wavence using the NSP

2.7.1 Steps

Deploying policies

1

Click on the NSP Menu and select Device Management. In the Configuration Intent Types view, import the following intent types: icm-wavence-file-retrieval-policy and icm-wavence-file-retrieval-policy-assignment.

2

Create and deploy a configuration template and configuration deployment using the icm-wavence-file-retrieval-policy intent, configuring the file retrieval settings in the configuration deployment as required. See the *NSP Network Automation Guide* for information about configuring intents.

Assigning policies

3

Create and deploy a configuration template and configuration deployment using the icm-wavence-file-retrieval-policy-assignment intent. In the configuration deployment, select the file retrieval policy you deployed in Step 2, and select the target NEs. See the *NSP Network Automation Guide* for information about configuring intents.

Performing an operation

4

In the All Operations view, create an operation using the nsp-ne-wavence-file-retrieval operation type.

5

In the Operation Inputs panel, select the file types and log types you need to retrieve.

6

Start or schedule the operation. For information about configuring and scheduling operations, see the *NSP Device Management Guide*.

END OF STEPS

2.8 To create or modify a file retrieval policy in the NFM-P

2.8.1 Prerequisites

A file retrieval policy is used to provide the NFM-P with the SFTP configuration required to access log, RSL, and I&C files on a Wavence device. File retrieval policies are created and assigned in the File Retrieval menu, and in the File Retrieval tab under NE Maintenance.

By default, there are three file retrieval policies already configured, one each for RSL, log, and I&C files, assigned to supported Wavence nodes in the network. You can configure the existing policies, or create and distribute any number of new ones, as required.

Note: To configure SFTP you require a host fingerprint. For information about acquiring a host fingerprint, see “To determine a host fingerprint” (p. 102).

2.8.2 Steps

1

Choose Administration→NE Maintenance→File Retrieval from the NFM-P main menu. The File Retrieval form opens.

2

Click on the Retrieval Policy tab. A list of file retrieval policies appears.

3

Select a policy and click on Properties, or create a new policy by clicking on the Create button. The File Retrieval Policy form opens.

4

Configure the parameters in the SFTP Settings panel. Provide the credentials, directory, and IP address of the SFTP server and the host key fingerprint.

5

Click Apply to save and close the form. To assign the policy to a Wavence device, see 2.9 “To assign a file retrieval policy to a Wavence device in the NFM-P” (p. 75).

END OF STEPS

2.9 To assign a file retrieval policy to a Wavence device in the NFM-P

2.9.1 Steps

1

Choose Administration→NE Maintenance→File Retrieval from the NFM-P main menu. The File Retrieval form opens.

2

Click on the Retrieval Policy tab. A list of file retrieval policies appears.

3

Select a policy and click on Properties. To modify a policy or create a new one, see 2.8 “To create or modify a file retrieval policy in the NFM-P” (p. 75).

4

The File Retrieval Policy form opens. Click on the File Retrieval Policy Assignment tab. A popup displays giving you an opportunity to filter for the nodes you need to assign; configure the filter, or click OK to close the popup and continue. You can click on the Filter button to adjust or apply the filter as required.

5

In the Unassigned Sites panel, select the sites to which you need to assign the policy and click on the right arrow. You can continue assigning sites from the list, or use the left arrow to unassign sites.

6

Click Apply to save and close the form. The policy is applied to the selected sites.

END OF STEPS

2.10 To retrieve log files stored by Wavence devices using the NFM-P

2.10.1 Prerequisites

The log retrieval requires the node to be MSS-4/8 release Wavence 19 or later and SNMP mode set as SnmpV2, SnmpV3, Snmpv3_SEC.

Before you can retrieve files from a Wavence device, a File Retrieval Policy must be configured for the device. See 2.9 “To assign a file retrieval policy to a Wavence device in the NFM-P” (p. 76) for information about assigning a policy, and 2.8 “To create or modify a file retrieval policy in the NFM-P” (p. 75) for information about configuring a policy.

Note: Do not perform a file retrieval while a WebCT password reset is in progress. Wavence Nodes with SNMP mode as Snmpv3_SEC are displayed as SnmpV3.

2.10.2 Steps

1

Choose Administration→NE Maintenance→File Retrieval from the NFM-P main menu. The File Retrieval form opens.

2

Select the log retrieval policy configured for the device and click Properties.

3

Confirm the parameters in the SFTP Settings panel. For log file retrieval from CoreEvo nodes, the host key fingerprint must be ECDSA.

4

Click on the File Retrieval Status tab. The Wavence devices that are managed by NFM-P are listed.

5

Choose a device and click Retrieve Logs. The Log Retrieval State column displays the status of log retrieval. The log files are copied from the SFTP server to the NFM-P server. Retrieved logs are displayed in the Logs tab.

Note: Log files are stored on the NFM-P in */opt/nsp/nfmp/nelogs/Wavence/*. Folders are created for each nodeID from which files were retrieved, containing Audit, UAL, and SNMP folders where the respective log files are stored.

END OF STEPS

2.11 To retrieve RSL files stored by Wavence devices using the NFM-P

2.11.1 Prerequisites

RSL file retrieval is supported on MSS-E/HE/XE, UBT-NIM, and MSS-4/8 nodes release Wavence 23A or later, and UBT-SA nodes release Wavence 25 or later.

Before you can retrieve RSL files from Wavence device, a File Retrieval Policy must be configured for the device. See 2.9 “To assign a file retrieval policy to a Wavence device in the NFM-P” (p. 76) for information about assigning a policy, and 2.8 “To create or modify a file retrieval policy in the NFM-P” (p. 75) for information about configuring a policy.

Note: Do not perform a file retrieval while a WebCT password reset is in progress.

2.11.2 Steps

1

Choose Administration→NE Maintenance→File Retrieval from the NFM-P main menu. The File Retrieval form opens.

2

Select the RSL file retrieval policy configured for the device and click Properties.

3

Confirm the parameters in the SFTP Settings panel. For RSL file retrieval from MSS-E/HE/XE and UBT-NIM nodes the host key fingerprint must be ED25519, for CoreEvo nodes it must be ECDSA, and for UBT-SA nodes it must be RSA.

4

Click on the File Retrieval Status tab. The supported Wavence devices that are managed by NFM-P are listed.

5

Choose a device and click Retrieve Logs. The Log Retrieval State column displays the status of log retrieval. The RSL files are copied from the SFTP server to the NFM-P server. Retrieved RSL files are displayed in the Logs tab.

Note: RSL files are stored on the NFM-P in */opt/nsp/nfmp/nelogs/Wavence/*. Folders are created for each nodeID from which files were retrieved, containing a RSLFiles folder where the RSL files are located.

END OF STEPS

2.12 To retrieve I&C files stored by Wavence Release 23A or later devices using the NFM-P

2.12.1 Prerequisites

I&C file retrieval is supported on MSS-4/8 nodes, Wavence Release 23A or later. For older releases, see 2.13 “To retrieve I&C files stored by Wavence Release 22 or earlier devices using the NFM-P” (p. 80).

Before you can retrieve I&C files from a Wavence device, a File Retrieval Policy must be configured for the device. See 2.9 “To assign a file retrieval policy to a Wavence device in the NFM-P” (p. 76) for information about assigning a policy, and 2.8 “To create or modify a file retrieval policy in the NFM-P” (p. 75) for information about configuring a policy.

Note: Do not perform a file retrieval while a WebCT password reset is in progress.

2.12.2 Steps

1

Choose Administration→NE Maintenance→File Retrieval from the NFM-P main menu. The File Retrieval form opens.

2

Select the I&C file retrieval policy configured for the device and click Properties.

3

Confirm the parameters in the SFTP Settings panel. For I&C file retrieval from CoreEvo nodes the host fingerprint must be ECDSA.

4

Click on the File Retrieval Status tab. The supported Wavence devices that are managed by NFM-P are listed.

5

Choose a device and click Retrieve Logs. The Log Retrieval State column displays the status of log retrieval. The log files are copied from the SFTP server to the NFM-P server. Retrieved logs are displayed in the Logs tab.

Note: I&C files are stored on the NFM-P in */opt/nsp/nfmp/nelogs/Wavence/*. Folders are created for each nodeID from which files were retrieved, containing a I and C Parameters folder with the retrieved files.

END OF STEPS

2.13 To retrieve I&C files stored by Wavence Release 22 or earlier devices using the NFM-P

2.13.1 Prerequisites

Use this procedure to retrieve I&C files stored on MSS-4/8 Wavence devices, Release 22 or earlier. For devices using Release 23A or later, see 2.12 “To retrieve I&C files stored by Wavence Release 23A or later devices using the NFM-P” (p. 79).

2.13.2 Steps

1

Choose Administration→NE Maintenance→I&C Parameters Retrieval. The I&C Parameters Retrieval window opens.

2

Click Search. The I&C Parameters Retrieval Status window lists the Wavence nodes. Click the Retrieve Radio RSL button and click Yes on the confirmation window.

3

The RSL File Retrieval Status column is updated with the retrieval status, which is limited to one of the following:

- If the CLI login credentials on the NE does not match the login credentials in CLI panel of the read and write mediation policy, an “Authentication failed” message is displayed.
- If there are no RSL CSV files on the NE, an "RSL Files does not exist on NE" message is displayed. File generation is performed using the WebCT interface.
- If there is an RSL CSV file for a radio port on the NE, the file is retrieved and the RSL status is updated.

END OF STEPS

2.14 To configure Wavence NE mediation for microwave backhaul L3 services

CAUTION

Service Disruption

You need to include the L3 VPN CLI login credentials in the mediation policy.

If the credentials are not included the resync time will be increased exponentially, causing performance impact.

2.14.1 Steps

1

Choose Administration→Mediation from the NFM-P main menu. The Mediation (Edit) form opens with the General tab displayed.

2

Click on the Mediation Security tab and perform one of the following:

a. Click Create to create a new mediation security policy. The Mediation Policy (Create) form opens.

b. Choose an existing policy and click Properties. The Mediation Policy (Edit) form opens.

3

Configure the required parameters.

4

Configure the Communication Protocol as SSH2 and provide the user name and password in the CLI panel.

5

Retain the default values for all other parameters in the Mediation Policy (Create/Edit) form.

6

Save your changes and close the forms.

END OF STEPS

2.15 Pathway to configure MPR system settings on Wavence MSS nodes using the NSP

2.15.1 Purpose

You can use the NSP Device Management view to configure MPR system settings on individual Wavence MSS nodes, or all nodes in a resource group. Before you can configure a Wavence MSS node, an intent type for the node must be imported into the NSP. If you do not have an intent type package for your Wavence MSS node, contact your Nokia support representative.

The following pathway describes the high-level steps required to configure a Wavence MSS node using the NSP; for detailed information on specific steps, see the *NSP Network Automation Guide* and the *NSP Device Management Guide*.

2.15.2 Process

1

Log in to the NSP and select Network Intents from the NSP Menu.

2

Import the intent type package for the Wavence MSS into the Intent Manager.

3

Click on the NSP Menu and select Device Management.

4

Select Configuration Intent Types from the drop-down menu in the banner, and use the Configuration Intent Types view to import the intent type you previously installed.

5

In the Configuration Templates view, create a configuration template using the intent type you imported, configuring the required MPR system setting values.

6

In the Configuration Deployments view, create deployments for the Wavence MSS nodes you need to configure, and deploy the templates to configure the nodes.

2.16 To display Wavence backhaul service status information on the NSP Network Map and Health dashboard

2.16.1 Steps

The NSP Network Map and Health dashboard can display an overview of the status of all Wavence backhaul services in your network using the Backhaul Service Health dashlet. The dashlet is not enabled by default, and the following procedure describes how to add the dashlet to a dashboard. For more information about using dashboards, see the *NSP User Guide.*

1

In the NSP, from the NSP Menu select Network Map and Health > Network Health View.

2

Click on the More Actions button in the upper right and select Edit Dashboard. The dashboard view changes to editing mode.

3

Click on the Add button. The Add Dashlet window opens.

4

Select the Backhaul Service Health dashlet, and click Add. The Backhaul Service Health dashlet appears on the NSP Network Health dashboard.

END OF STEPS

3 Wavence statistics support

3.1 Wavence statistics support

3.1.1 Introduction

The NFM-P supports the collection of network performance, accounting, and flow-based statistics for Wavence devices. NFM-P also provides statistics for monitoring NFM-P processes and functions. These statistics are typically used to monitor or troubleshoot a network, or to perform SLA or billing functions. Statistics collection can be configured with policies that are distributed to specified network objects.

See the *NSP NFM-P Statistics Management Guide* for information about the following for Wavence devices:

- configuring statistics collection
- viewing statistics data in tabular or graphical form
- creating graphical representations of statistics data using the Statistics Plotter
- supported performance and accounting statistics counters for Wavence devices

3.1.2 Optimized historical statistics collection

NFM-P collects historical statistics at 15-minute and 24-hour intervals. The first set of statistics collected after a Wavence device is managed contains all the historical statistics collected during the time interval. The subsequent historical statistics collected only contain the new statistics and the previously collected data is not duplicated. When the Wavence device connectivity is lost, NFM-P collects all of the uncollected records upon restoration of connectivity. When the Wavence device is unmanaged or suspended, no new records are generated. The first set of statistics is collected after the Wavence device is managed again. When error-free statistics data is collected on the Wavence nodes, the hop history data statistics are incremented.

Note: For a newly discovered node that is already suppressed, no missing statistics are displayed for the first interval.

3.1.3 Statistics collection in maintenance mode

While the OLC State of a node is set to maintenance mode, UAS and G826 data is excluded from Hop History statistics, and the Unavailable Seconds parameter is 0.

3.1.4 Elaborated counters and formulas

Table 3-1, “Elaborated counters and formulas” (p. 86), lists the elaborated counters and the formulas.

Table 3-1 Elaborated counters and formulas

Class	Counter	Formula
AggrMaintTxStats	Compressed Tx Throughput [Mbps]	{(Total Transmitted Octets after Compression Periodic × 8)+ (Net bandwidth - Available bandwidth)} / Periodic time in seconds / 10^6
	Tx Compressed Utilization [%]	(Aggregate Compressed Tx Throughput [Mbps] × 100) / Capacity [Mbps]
	Aggregate Tx Throughput [Mbps]	{(Total Transmitted Octets Periodic × 8) + (Net bandwidth - Available bandwidth)} / (Periodic time in seconds) / 10^6
	Tx Utilization [%]	(Aggregate Tx Throughput [Mbps] × 100) / Capacity [Mbps]
	Discarded Frame Ratio [%]	(Total Discarded Frames Periodic) / (Total Discarded Frames Periodic + Total Transmitted Frames Periodic) × 100
	Compressed Gain [%]	(Aggregated Tx Throughput – Compressed Tx Throughput) * 10^2/Compressed Tx Throughput
AggrPerQueueMaintStats	Aggregate Tx Throughput [Mbps]	{(Total number of Confirming Octets Periodic × 8) + (Net bandwidth - Available bandwidth)} / (Periodic time in seconds) / 10^6
	Tx Utilization [%]	(Aggregate Tx Throughput [Mbps] × 100) / Capacity [Mbps]
	Tx Discarded Frame Ratio [%]	(Total Discarded Frames Periodic) / (Total Discarded Frames Periodic + Total Transmitted Frames Periodic) × 100
AggrMaintRxStats	Rx Throughput [Mbps]	(Total Received Octets Periodic) × 8 / (Periodic time in sec) / 10^6
	Rx Utilization [%]	RX Throughput / (Capacity) × 100
	Rx Discarded Frame Ratio [%]	(Total Discarded Frames Periodic) / (Total Discarded Frames Periodic + Total Received Correct Frames Periodic) × 100
PdhFrameHopHistoryDataStats[1, 2] PdhFrameLinkHistoryDataStats	Link Availability [%]	(1 - (Unavailable Seconds Absolute) / (Elapsed time in seconds) × 100

Note:

1. Statistics with a suppressed interval of 0 are only available in historical data if current data statistics are enabled.
2. The Suspect and Suspect Interval Flag attributes are unrelated and may appear independently of each other.
3. Periodic and per second are not applicable for real-time plotting of the elaborated counters.

Note:

- The value of radio port capacity used for computation of relative throughput depends on whether the ACM is preconfigured with or without admission control and chassis types.
- The elapsed time is expressed in seconds. If the elapsed time exceeds 900 s for the 15 min interval or 86400 s for the 24 hour interval, those 900 s or 86400 s are used in the formula, respectively.
- The Wavence automatically suppresses PM on 15 min granularity periods that are classified as "noSuspect" with no errors, and does not store them as history data. In such cases, some of the granularity periods may be missing.
- Link availability counter is 0 in current data classes, for example Hop Current Statistics (15min/24h).
- Net Bandwidth and Available Bandwidth are not applicable for UBT radio ports.

Where:

- Net Bandwidth = radioPDHTTPBidNetBandwidth
- Available Bandwidth = radioPDHTTPBidAvailableBandwidth
- Capacity is:

  - radioPDHTTPBidOperativeAvailableBandwidth - operative bandwidth in Mbps in case of radio LAG L1

  - radioPDHTTPBidAvailableBandwidth - Net bandwidth in Mbps in case of 1+0 and 1+1 systems that are in FCM (Presetting)

  - adaptiveMpdiulationCurrentCapacity - current bandwidth /1000 in Mbps in case of 1+0 and 1+1 systems that are in ACM (Adaptive Modulation)

Note: If the modulation is changed during polling period, it might lead to non-precise values for Link Utilization. As the Attribute Value Change (AVC) notification is not raised by the NE, it is required to consider “Current Capacity” at the end of the polling period.

3.1.5 Wavence-specific statistic usage information

The following provides notable statistic usage information that applies to Wavence devices:

- When the ethAggrMaintTxTTO counter value is zero, no scheduled stats records are collected by NFM-P. This behavior is applicable only to scheduled statistics and not for on-demand statistics.
- The values shown in the real-time plot of the TSL Hop Current Data statistic are multiplied by ten (so a value of 4.0 dBm is displayed as 40 dBm).
- NFM-P supports elaborated counters as an extension to the following classes:
  - AggrMaintTxStats (for radio, Ethernet user ports, and L1 radio LAG)
  - AggrPerQueueMaintStats (for radio ports)
  - AggrMaintRxStats (for Ethernet user ports)

  The elaborated counters are applicable only to scheduled statistics and not on-demand statistics. NFM-P does not support real-time plotting of the elaborated counters. The elaborated counters are supported for Wavence SM, Wavence SA, and Wavence MSS-1c devices. See the Statistics Search Tool for detailed information about the individual statistics counters.
- NFM-P supports the display of the compression gain elaborated counter in Ethernet ports and

radio LAG ports. The compression gain counter shows the difference (%) in bandwidth when packet throughput booster is enabled.

- The granularity period column displays the statistic collection period based on a set time interval; for example, 15 corresponds to 15 min and 24 corresponds to 24 hour.
- NFM-P supports peak and average performance management statistics at LAG level for UBT-SA nodes, and when the radio ports are connected on the EASv2 or CAHD cards and are associated with LAG.
- The radio interface performance management statistics are listed separately for collection intervals of 15 min and 24 hour at the port level. The following table lists the radio interface performance management statistics that are collected at the port level or using the Bulk Operations tool.

Radio interface PM statistic type	Usage notes
Adaptive Modulation Current Data	Statistic is only present when AM is enabled using Adaptive Modulation Mode.
Frame Hop Current Data	Always available for the Radio interface.
Frame Link Current Data	Available for the Radio interface when RPS is enabled. See **Note 1** and **Note 2**.
RSL Hop Current Data	Always available for the Radio interface.
TSL Hop Current Data	Always available for the Radio interface.
RSL Link Current Data	See **Note 1** and **Note 2**. When RPS is present, Hop stats are enabled/disabled on the protecting port along with the active port.
RSL Diversity Link Current Data	Available for Wavence Release 5.1 or later when the space diversity (combiner) is enabled on the Radio interface along with RPS.
RSL Diversity Hop Current Data	Available for Wavence Release 5.1 or later when the space diversity (combiner) is enabled on the Radio interface.
Peak and Average Current Data	See **Note 3** Sstatistics are available for UBT Radio nodes only. Bulk operation is also supported for statistics collection.
Note 1: When RPS is present, you can enable/disable statistics on the protecting port along with the active port. **Note 2:** When RPS is present, do not edit the Radio PM statistic parameters from NFM-P GUI for the spare protecting port. **Note 3:** For UBT-T and UBT-S2, Peak and Average statistics are supported only at the port level and not at the channel level. **Note 4:** For all Radio types, it is recommended to enable the ACM PM when the Radio is in Adaptive Modulation for the bandwidth calculation.	

Note : Only UBT-C 1+0 supported statistics are supported for NFM-P Release 19.3 or later.

- You can enable or disable performance management statistics at port level or using the Bulk Operations tool.
  - **Port level:**

    You can enable or disable individual radio interface performance management statistics that are collected at intervals of 15 min or 24 hour. See 3.2 “To configure radio interface performance management statistics at the port level” (p. 89) for more information.
  - **Bulk Operations tool:**

You can perform bulk changes to enable or disable the applicable incoming and outgoing performance management statistics for statistics collection intervals of 15 min and 24 hour for the radio, STM-1 SDH, E1, and DS1 interfaces. For the E1 interface, the Signal Mode must be configured as Framed before performing the modification. The changes are applicable to the entire list of allowable statistics for statistics collection intervals of 15 min and/or 24 hour. See 3.4 “To configure bulk changes for performance management statistics” (p. 91) for more information; also see the “Bulk operations” chapter in the *NSP NFM-P Classic Management User Guide* for more information.

- Perform the following to plot the statistics for both ends of a physical link traversing between two Wavence NEs, between a Wavence NE and a 7750 SR, or a Wavence NE and a 7705 SAR:
  - Select a supported Radio link on the Administration→Physical Topology map, right-click on the link and choose Plotter→New Plot. The Statistics Plotter window opens to display both link endpoints in the Monitored Object column. Select the appropriate Statistics Group, Statistics Counter, or Data Format, and click the Record/Play buttons to plot the data.
  - You can also plot Radio link statistics at the object level by selecting a supported device port in the navigation tree Equipment view, and choose Properties. The Physical Port — Port (Edit) form opens. Click Plotter→New Plot. The Statistics Plotter window opens to display the selected endpoint in the Monitored Object column. If the port is part of a Radio link, click on the Plot Other Endpoint(s) button to populate/view the other link endpoint. Select the appropriate Statistics Group, Statistics Counter, or Data Format parameters, and click the Record/Play buttons to plot the data.

  See the *NSP NFM-P Statistics Management Guide* for more information about the statistics plotter.

3.2 To configure radio interface performance management statistics at the port level

3.2.1 Before you begin

Configure the radio parameters using the MCT for the newly discovered Wavence SA and Wavence MSS-1c devices, before configuring the radio PM enable and disable parameters on NFM-P.

3.2.2 Steps

1

On the equipment navigation tree, right-click on a Wavence port where a Radio interface is configured, for example, an MPT-MC or MPT-HC unit, and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Radio tab and configure the appropriate PM statistics parameters on the Radio PM panel.

MPRe power levels will be displayed on Radio tab. Dynamic update of the power levels is not supported. Perform a resync or schedule radio analog statistics for the latest statistics values.

END OF STEPS

3.3 To configure link budget calculation statistics

3.3.1 Overview

The link budget calculation report provides the details on radio link deviations, based on the Install/ Design and Actual RSL values per MPT/UBT basis, for selected time range and granularity (15 Min/24 Hr). The report lists the number of deviations and details on the links for Actual vs Design and Actual vs Install percentage values.

Nodes with radio links need to be discovered in the NFM-P. NFM-P will calculate the path distance (user configurable between kilometers) based on the latitude and longitude coordinates on the node properties.

Note: Radio RSL is supported only for MPT/UBT radio ports and not supported for radio modem ports.

I&C Parameters Retrieval is supported on NEs that support secure file transfer.

Receive Signal Level (RSL) indicates the quality of radio transmission.

The following RSL types are supported:

- Design RSL- based on the SLA, the desired RSL values is calculated using complex formulas, considering the receiver sensitivity threshold, output power of the transmitter, loss between transmitter and receiver antenna, gain of the transmitter and receiver antenna and free space loss parameters.
- Installed RSL- is the RSL value after commissioning the Wavence nodes.
- Actual RSL- is the current RSL value retrieved from performance monitoring.

3.3.2 Prerequisites

NE login credentials must be updated in the mediation policy that is used for read and write mediation security in the discovery rule.

- Choose Administration→Mediation→Mediation Security. Select the mediation policy to be updated.
- In the CLI panel, select Communication Protocol as Telnet/SSH.
- Configure the User Name and Password parameters same as the node credentials used for logging into WebCT/NEtO.
- Click Apply.

Before the RSL date can be retrieved, it must be generated using WebCT. See the WebCT documentation for information about generating the I&C parameters file from the Monitoring and Maintenance view. After configuration changes are made to the node, the file should be generated again to ensure the changes are captured.

3.3.3 Steps

1

Retrieve the RSL files. To retrieve files for a CorEvo Wavence node Release 23A or later, see 2.12 “To retrieve I&C files stored by Wavence Release 23A or later devices using the NFM-P” (p. 79) , or for earlier releases see 2.13 “To retrieve I&C files stored by Wavence Release 22 or earlier devices using the NFM-P” (p. 80).

2

With the successful retrieval of the RSL file for any MPT/UBT port, on the equipment navigation tree, right-click on the Wavence port where a Radio interface is configured, for example, an MPT-MC or MPT-HC unit, and choose Properties. The Physical Port (Edit) form opens with the value in the CSV file updated correctly into the Install RSL field in the Radio tab.

3

Click on the Radio tab.

Perform the following:

1. Update the Design RSL value in the Profile panel.
2. Configure the appropriate PM statistics parameters in the Radio PM panel.

4

Click on the Statistics tab and choose Radio Analog Statistics (Radio Equipment) from the Select Object Type contextual menu.

5

Click on the Statistics Policies button and select MIB Entry Policy. Expand the Configuration panel and ensure that the RSL Hop Current statistics are enabled on the radio port.

6

Close the form.

Note: By default RSL file is saved at */opt/nsp/nfmp/nelogs/WavenceRSLFiles/<Node ID>*

END OF STEPS

3.4 To configure bulk changes for performance management statistics

3.4.1 Steps

1

Choose Tools→Bulk Operations from the NFM-P main menu. The Bulk Operations form opens.

2

Click Create. The Create Bulk Change step form opens.

3

Configure the required parameters in the General step and click Next. The Specify the filter step appears.

4

Configure an appropriate filter in the Specify the filter step and click Next. The Specify the attributes step appears.

5

Expand the Attributes drop-down, and click on one or more attributes, as required. The PM properties are displayed on the right panel.

6

Configure the parameters in the right panel.

The following notes apply:

- For radio interfaces, do not use the following attributes:
  - Radio: Radio Port (Radio Equipment)→Radio PM : Radio Port (Radio Equipment)→Radio PM.

    The configured filter lists only the enabled radio PM statistics and not the disabled radio PM statistics.
  - Radio: Radio Port (Radio Equipment)→Radio PM : Radio Port (Radio Equipment)→Radio Bulk Radio PM Enable/Disable 15 Min
  - Radio: Radio Port (Radio Equipment)→Radio PM : Radio Port (Radio Equipment)→Radio Bulk Radio PM Enable/Disable 24 Hrs
- For DS1/E1:
  - PM Enable/Disable for DS1 ports is supported only for Framed and

    Unframed signal mode ports.
  - PM Enable/Disable for E1 ports is supported only for Framed signal mode ports.

7

Click Next, then click Finish, and close the form. The Bulk Operations form reappears.

8

Click Search to locate the Bulk Operation task, choose an entry, and click Properties. The Bulk Change (Edit) form opens.

9

Click on the Batch Control tab and click Generate Batches. The batches are generated.

10

Either click Execute All or choose the required entries and click Execute Selected to enable or disable PM statistics collection intervals of 24 hour and/or 15 min.

11

Close the forms.

END OF STEPS

3.5 RSL Deviation Alerts

3.5.1 Overview

The NFM-P supports raising an alarm when the minimum RSL deviates from the installed RSL by a configurable deviation value. This procedure describes how to configure the deviation value and set up the NFM-P to monitor RSL deviation on a Wavence device by enabling RSL monitoring, and creating a custom Threshold Crossing Alarm rule that alerts the NFM-P when a deviation has occurred.

3.5.2 Steps

1

Click Administration→System Preferences in the NFM-P main menu. The System Preferences form opens.

2

In the Wavence tab, enable the Enable RSL Monitoring And Deviation Alert parameter, and configure the Maximum Allowed Number of Deviations parameter with the number of deviations that must occur before an alarm is raised. Save and close the form.

3

Click Tools→TCA Policies in the NFM-P main menu. The TCA Policies form opens.

4

Click Create. The TCA Policy form opens.

5

Configure the Monitored Object Type parameter as the object type you need to monitor (for example, UBT Channel).

6

Enable the TCA Admin State parameter.

7

In the Custom panel, click Create. The Custom TCA form opens.

8

Configure the following parameter values:

Parameter	Value
Build Formula	rslHopHDStatsDeviation2
Stats Type	RSL Hop History Data Stats- 15Min (Radio Equipment)
Monitored Object	Same as Monitored Object Type above.

9

In the Rules panel, click Create. The Custom TCARule form opens.

10

Create a rule that defines when to raise the Threshold Crossing Alarm. For example, configure the following parameters to trigger an alarm when there is a deviation of more than -1 dB. Then save and close the form.

Parameter	Value
Alarm Severity	Info
Threshold	-1.0
Threshold Direction	Rising Above
Alarm	Enabled

11

In the Custom panel, click Create and create a second rule that defines when to clear the Threshold Crossing Alarm raised by the previous rule. For example, configure the following parameters to clear the alarm when the deviation falls below -1 dB. Then save and close the form.

Parameter	Value
Alarm Severity	Cleared
Threshold	-1.0
Threshold Direction	Falling Below
Alarm	Enabled

12

Click on the Monitored Object tab, and click on Add to add the Wavence network objects that you need to monitor. Save and close the form.

When the Threshold Crossing Alarm is triggered, the NSP raises a RSL Deviation Threshold Crossed alarm against the radio link associated with the monitored object. Both alarms can be viewed and managed in the NSP.

END OF STEPS

3.6 Wavence example object filters for the NSP

3.6.1 Data Collection and Analysis

You can use the NSP to manage YANG-based telemetry from Wavence nodes. When you use the NSP to view indicators, you must use object filters to focus the scope of the indicators to the nodes you need to monitor. This section contains a few example object filters to assist in using the NSP to monitor Wavence nodes.

Finding NE, radio, and lag objects

You can filter for network elements by ID, type, or other attributes. The following examples show how to find NEs, LAGs, and radio ports - either as a broad category, or specific elements:

- Finding an NE:

  ```
  /nsp-equipment:network/network-element[ne-id='203.0.113.169']
  ```

- Finding LAGs on an NE:

  ```
  /nsp-equipment:network/network-element[contains('ip-address',
  '203.0.113.1')]/lag
  ```

- Finding radio ports:

  ```
  /nsp-equipment:network/network-element/hardware-component/port
  [description='Radio']
  ```

- Finding a particular port:

  ```
  /network-device-mgr:network-devices/network-device[name='203.0.113.
  169']/root/nokia-nsp-source:fdn[id='fdn:realm:sam:network:203.0.113.
  169:shelf-1:cardSlot-1:card:port-5']
  ```

- Finding a particular LAG:

  ```
  /network-device-mgr:network-devices/network-device[name='203.0.113.
  169']/root/nokia-nsp-source:fdn[id='fdn:realm:sam:network:203.0.113.
  169:lag:interface-1']
  ```

- Finding channel 1A on a UBT-T:

  ```
  /network-device-mgr:network-devices/network-device[name='203.0.113.
  242']/root/nokia-nsp-source:fdn[id='fdn:realm:sam:network:203.0.113.
  242:shelf-1:cardSlot-4:card:port-5:radio-1']
  ```

- Finding channel 1B on a UBT-T:

```
/network-device-mgr:network-devices/network-device[name='203.0.113.
242']/root/nokia-nsp-source:fdn[id='fdn:realm:sam:network:203.0.113.
242:shelf-1:cardSlot-4:card:port-5:radio-3']
```

You can join together statements in an object filter using the | logical operator, and the filter will return the results of all the joined statements. For example, the following filter returns both NEs that match the specified NE-IDs:

```
/nsp-equipment:network/network-element[ne-id='203.0.113.169'] |
/nsp-equipment:network/network-element[ne-id='203.0.113.170']
```

The same format can be used to combine any of the examples above. For more information about indicators and building object filters, see the *NSP Data Collection and Analysis Guide*.

3.7 Pathway to configure NSP test templates for Wavence CFM Loopback and CFM Stats

3.7.1 Description

You can create test templates using NSP Data Collection and Management to use in the creation of OAM tests. Creating the template requires configuring parameters, and then using the REST API to activate data collection.

3.7.2 Steps

1

In **NSP Data Collection and Management**, create a new test template. See the *NSP Data Collection and Analysis Guide* for information about working with test templates.

2

For a Wavence CFM Loopback test template, specify a name for the template, then configure the parameters as specified in the following table.

Parameter	Value
Destination Type	Enable
Destination Mac Address	00-00-00-00-00-01
Execute Type	On-demand
Priority	Enable
MA Name	srv:${service-id}
MD Name	TEMP_CFM
Reuse existing MEP	Enable
System Type	Enable
System template	Enable

3

For a Wavence CFM DMM Stats test template, specify a name for the template, then configure the parameters as specified in the following table.

Parameter	Value
Destination Type	Enable
Destination Mac Address	00-00-00-00-00-01
Execute Type	Proactive
Bin Group	1
Bulk Result	Enable
MA Name	srv:${service-id}
MD Name	TEMP_CFM
Reuse existing MEP	Enable
System Type	Enable
System template	Enable

4

Use the test templates to create OAM tests, as required. See the *NSP Data Collection and Analysis Guide* for information about performing OAM tests.

5

Using the POST REST API, create the following result-classifier. For information about the API, see the Developer Portal.

```
{
"result-classifier": [
      {
         "name": "wavence_result_classifier",
         "description": "Wavence specific",
         "admin-state": "enable",
         "test-class-mappings": [
            {
               "nsp-class-id": "telemetry:/base/oam-pm/eth-cfm-delay-streaming",
               "pass-func": "function accept(data) { return (data.get('delay') > 0); }"
            },
            {
               "nsp-class-id": "telemetry:/base/oam-pm/twamp-light-delay-streaming",
               "pass-func": "function accept(data) { return (data.get('delay') > 0); }"
```

```
        },
        {
            "nsp-class-id": "telemetry:/base/oam-pm/eth-cfm-delay-session",
            "pass-func": "function accept(data) { return (data.get('two-way-average') >= 0); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oam-pm/twamp-light-delay-session",
            "pass-func": "function accept(data) { return (data.get('two-way-average') > 0); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oam-pm/eth-cfm-delay-base",
            "pass-func": "function accept(data) { return (data.get('frames-
sent') == data.get('frames-received')); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oam-pm/twamp-light-delay-base",
            "pass-func": "function accept(data) { return (data.get('frames-
sent') == data.get('frames-received')); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oampm-accounting/twl-session-acc-stats",
            "pass-func": "function accept(data) { return ((data.get('pdu-
sent').equals(data.get('pdu-received'))) && (data.get('pdu-sent')!=0)); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oampm-accounting/twl-session-loss-acc-stats",
            "pass-func": "function accept(data) { return ((data.get('pdu-
sent').equals(data.get('pdu-received'))) && (data.get('pdu-sent')!=0)); }"
        },
        {
            "nsp-class-id": "telemetry:/base/oampm-accounting/twl-bin-acc-stats",
            "pass-func": "function accept(data) { return true; }"
        },
        {
            "nsp-class-id": "telemetry:/base/oampm-accounting/cfm-dmm-session-acc-stats",
            "pass-func": "function accept(data) { return ((data.get('pdu-
sent').equals(data.get('pdu-received'))) && (data.get('pdu-sent')!=0)); }"
        },
```

```
                {
                    "nsp-class-id": "telemetry:/base/oampm-accounting/cfm-dmm-bin-acc-stats",
                    "pass-func": "function accept(data) { return true; }"
                },
                {
                    "nsp-class-id": "telemetry:/base/oam-result/loopback-result",
                    "pass-func": "function accept(data) { return ('success'.equals(data.get('result-
status')) || 'succeeded'.equals(data.get('result-status'))); }"
                },
                {
                    "nsp-class-id": "telemetry:/base/oampm-accounting/cfm-slm-session-acc-stats",
                    "pass-func": "function accept(data) { return ((data.get('pdu-
sent').equals(data.get('pdu-received'))) && (data.get('pdu-sent')!=0)); }"
                },
                {
                    "nsp-class-id": "telemetry:/base/oampm-accounting/cfm-lmm-session-acc-stats",
                    "pass-func": "function accept(data) { return ((data.get('pdu-
sent').equals(data.get('pdu-received'))) && (data.get('pdu-sent')!=0)); }"
                },
                {
                    "nsp-class-id": "telemetry:/base/oam-result/link-trace-result",
                    "pass-func": "function accept(data) { return ('success'.equals(data.get('result-
status')) || 'succeeded'.equals(data.get('result-status'))); }"
                }
            ]
        }
    ]
}
```


6

After the results classifier is deployed, the results of the tests are displayed in the NSP and the NFM-P.

END OF STEPS

4 Wavence software upgrade

4.1 General description

4.1.1 General description

CAUTION

Service Degradation

Ensure that you regularly remove from NFM-P the device software images that are no longer required; for example, by deleting the images.

An accumulation of device software images can dramatically increase the length of an operation such as an NFM-P database backup, restore, or reinstantiation.

This chapter contains information about how to perform an on-demand software upgrade on Wavence devices and the specific software upgrade policy requirements to perform the upgrade.

See 6.1.8 “Software upgrades on Wavence SCM devices” (p. 115) for information about performing software upgrades on Wavence SCM devices.

To perform upgrades on Wavence devices discovered using the NSP, see the *NSP Device Management Guide*. For upgrades using the NFM-P, see the “NE software upgrades” chapter of the *NSP NFM-P Classic Management User Guide* for general software upgrade requirements and information.

The Wavence software is stored in two banks on a compact flash card:

- The committed bank contains the software that is currently running.
- The standby bank contains downloaded software that has not been activated, or software that was active before the current committed software.

Note:

- A Wavence NE that has never been upgraded displays only the committed bank. The standby bank is not displayed until new software is downloaded for the first time.
- You require an NFM-P user account with an administrator or network element software management scope of command role, or a scope of command role with write access to the mediation package, before you can perform a Wavence software download.

4.1.2 Wavence software upgrade policy requirements

Before performing a software upgrade, you must create a software upgrade policy that specifies the device family, software image, image backup location, and the actions to perform; for example,

image download, activation, or ISSU. Using a software upgrade policy, an NFM-P operator can independently perform the image download, upgrade, and activation tasks.

The following conditions apply to software upgrade policies:

- The policy provides the NE with the location of the software image files on an FTP/SFTP server.
- Select the Forced Download check box on the Software Upgrade Policy (Create) form if you want to make the download forceful.
- The policy is configured with the SFTP transfer protocol specified; determine the following attributes for the transport protocol:
  1. SFTP User ID
  2. SFTP password
  3. Path to file storage location on the SFTP server
  4. Host fingerprint

Note: The file storage location path must be an absolute path from the / directory, and the SFTP user must have access to the location.

To determine a host fingerprint

Determine the version of SSH that NFM-P is using (RSA or ECDSA), using the following command:

`ssh -v localhost`

Example 1: if the output of the command is:

```
debug1: expecting SSH2_MSG_KEX_DH_GEX_REPLY

The authenticity of host 'localhost (::1)' can't be established.

RSA key fingerprint is 89:57:0c:64:63:8c:70:b7:cb:6e:db:33:97:9b:25:32.
[Note the host fingerprint varies from machine to machine]

Are you sure you want to continue connecting (yes/no)?
Use:
```

`ssh-keygen -lf /etc/ssh/ssh_host_rsa_key.pub | sed 's/://g' | awk '{print $2}'`

Example 2: if the output of the command is:

```
debug1: Server host key: ECDSA 71:1a:b1:4e:1c:66:06:0c:a4:bc:dd:c5:fc:29:
b2:70

The authenticity of host 'localhost (::1)' can't be established.
```

```
ECDSA key fingerprint is 71:1a:b1:4e:1c:66:06:0c:a4:bc:dd:c5:fc:29:b2:70.
[Note the host fingerprint varies from machine to machine]

Are you sure you want to continue connecting (yes/no)?
Use:
```

ssh-keygen -l -f /etc/ssh/ssh_host_ecdsa_key.pub | sed 's/://g' | awk '{print$2}'

Example 3: if the output of the command is:

```
debug1: Server host key: ecdsa-sha2-nistp256 SHA256:
RRUksTgiJwIzJeSfs59dCkT+5+50nTs4YN8rLrCi9lM
The authenticity of host 'localhost (::1)' can't be established.

ECDSA key fingerprint is SHA256:
RRUksTgiJwIzJeSfs59dCkT+5+50nTs4YN8rLrCi9lM.

ECDSA key fingerprint is MD5:20:cb:e9:c8:9d:b3:67:99:48:3c:5d:67:7a:8a:
85:f5.
Are you sure you want to continue connecting (yes/no)?
Use:
```

ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_ecdsa_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}

MSS-E/HE/XE and UBT-NIM nodes using Wavence Release 23 or earlier and all UBT-SA nodes support only RSA fingerprint for software download and backup operations. Use the following cipher algorithm to generate fingerprint, irrespective of higher preference algorithm (RSA or ECDSA) on the server:

ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_rsa_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'

Note: For UBT-SA nodes, SSH server configuration (/etc/ssh/sshd_config) must contain following options. Ciphers: aes128-cbc, aes192-cbc, aes256-cbc, blowfish-cbc, 3des-cbc, arcfour128

MSS-E/HE/XE and UBT-NIM nodes using Wavence Release 23A or later support only ED25519 fingerprint for software download operation. Use the following cipher algorithm to generate fingerprint, irrespective of higher preference algorithm (RSA or ECDSA) on the server:

ssh-keygen -E md5 -l -f /etc/ssh/ssh_host_ed25519_key.pub | sed 's/://g' | sed 's/MD5//g'| awk '{print$2}'

4.2 Software upgrade pathway

4.2.1 General information

General pathway to perform Wavence device software upgrades:

4.2.2 Process

Upgrade the device software, as required.

1

Create a software upgrade policy; see 4.1.2 “Wavence software upgrade policy requirements” (p. 101) in this section for the specific conditions that apply to Wavence software upgrade policies, and see “To configure a software upgrade policy” in the *NSP NFM-P Classic Management User Guide*.

2

Download the image package to a directory on the NFM-P client station. Extract the package and ensure that the software description file is in the same directory.

3

Import the software description file; see “To import device software files to the NFM-P” in the *NSP NFM-P Classic Management User Guide*.

NFM-P transfers the description file to a specified FTP server from which the Wavence subsequently retrieves the image files.

4

Perform a software upgrade to transfer the files to the required NEs; see 4.3 “To perform an on-demand Wavence software upgrade” (p. 104) in this guide or “To schedule an NE software upgrade” in the *NSP NFM-P Classic Management User Guide*.

5

Activate the new software as the running software; see 4.4 “To manage the Wavence running software” (p. 106).

4.3 To perform an on-demand Wavence software upgrade

4.3.1 Purpose

Perform this procedure to upgrade the device software on one or more Wavence NEs. Before performing this procedure, review the Wavence software upgrade pathway steps contained in the 4.2 “Software upgrade pathway” (p. 104) for the additional information required to complete this procedure.

4.3.2 Steps

1

Choose Administration→NE Maintenance→Software Upgrade from the NFM-P main menu. The Software Upgrade form opens.

2

Click on the Software Images tab, select the MPR Default software upgrade policy, then the MPR 9500 Software Images tab.

Note: NFM-P performs the upgrade according to the configuration in the software upgrade policy to which the NE is assigned.

3

Click Import and select a software descriptor file. A software descriptor file has a .DSC extension and must be present on the client system. Other software files do not need to be present on the client system.

4

Click Upgrade Sites. A list of NEs opens. The list is filtered to display only the device type that is appropriate for the selected software image.

5

Select one or more NEs and click OK. The software upgrade begins.

6

Perform one of the following to view the status of the software upgrade as it progresses:

a. To view a high-level progress status such as “In Progress”, “Completed”, or “Failed”, click on the Software Upgrade Status tab to view the status.

b. To view the progress of the software upgrade as a percentage of completion:

1. Select the MPR Default software upgrade policy as outlined in Step 1 and Step 2 of this procedure.
2. Click on the Software Upgrade Status tab, select the node on which the software upgrade is being performed, and click Properties. The Software Upgrade Status - MPR Default Policy form opens.
3. Click on the Software Upgrade tab and view the progress of the software upgrade indicated by the Upgrade Percentage Completed (%) parameter.

Proceed to Step 7 after you verify that the files are successfully transferred.

7

Close the Software Upgrade form. After a successful software upgrade, you must activate the software; see 4.4 “To manage the Wavence running software” (p. 105) .

END OF STEPS

4.4 To manage the Wavence running software

4.4.1 Purpose

Perform this procedure to manage the software in the Wavence committed and standby banks. You can upgrade or downgrade the running software release on a Wavence NE.

See “NE software upgrade overview” in the *NSP NFM-P Classic Management User Guide* for information about creating software upgrade policies and performing software upgrades.

CAUTION

Service Disruption

To avoid a service outage:

A Wavence NE may require a firmware upgrade before a device software upgrade. To avoid a service outage, ensure that the device firmware version supports the software upgrade. See the device software Release Notes to obtain information about firmware and software release compatibility.

CAUTION

Service Disruption

Perform this procedure only in a maintenance window:

When you reboot a Wavence SA that is in service, it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

Note: During a software upgrade, the NE audit function is not supported for Wavence NEs.

4.4.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence shelf and choose Properties. The Shelf (Edit) form opens.

2

Click on the Software Bank Details tab. The committed and standby software information is displayed. The committed software is the software currently running on the NE. The standby software is new software uploaded to the NE, or formerly committed software.

3

Verify that the operational state of the standby software is Enabled by examining the Operational State value.

You can also examine the Software Version of the standby and committed software. If the software version of the standby software is more recent than the committed software version, the NE can be upgraded. If the standby software version is older than the committed software version, the NE can be downgraded.

4

Select the standby entry and click Properties. The MPR Software Package (Edit) form opens.

5

Configure the Activation parameter and click OK. The Shelf (Edit) form reappears.

6

Save your changes and close the form. When the standby and committed software versions are different or the forced activation option is selected, the NE reboots using the standby software. If the standby and committed software versions are the same and the activation option is chosen, the NE does not reboot and the Shelf (Edit) form closes.

Note: For nodes with a radio LAG configured, the Activation parameter may take some time to update due to the node enabling all of the associated peripherals.
The Activation Status parameter displays Activated for the committed software package, Not Applicable for the standby software package, and In Progress for a package undergoing activation.

7

After the NE reboots, you can confirm that the NE is running the software stored in the former standby bank. The former standby software is the committed software and the previous committed software is the standby software.

END OF STEPS

5 Wavence migration to revised service model

5.1 Migration pathway

5.1.1 Pathway

Pre-upgrade

1

Perform the pre-upgrade tasks to upgrade from any 5620 SAM releases earlier than 14.0 R7. See 5.2 “To perform pre-upgrade tasks” (p. 109).

NFM-P upgrade

2

See the *NSP Installation and Upgrade Guide* for more information about NFM-P upgrading.

Post-upgrade

3

Perform the post-upgrade tasks to upgrade from any 5620 SAM releases earlier than 14.0 R7. See 5.3 “To perform post-upgrade tasks” (p. 110).

5.2 To perform pre-upgrade tasks

5.2.1 Steps

Clear incomplete deployments

1

Choose Administration→NE Maintenance→Deployment. The Deployment form opens with the Incomplete Deployments tab displayed.

2

Select all entries in the Incomplete Deployments tab and click Clear.

3

Close the form.

Execute script

4

Log in to the NFM-P database station as the Oracle management user.

5

Download the following NFM-P installation script to a local directory in which the Oracle management user has read, write, and execute privileges:

MPR_migrate.bash

6

Use a CLI to navigate to the script location and enter the following:

```
./MPR_migrate.bash
```

Unmanage services from 5620 SAM releases earlier than 14.0 R7

7

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

Note: In the 5620 SAM and in the NFM-P Release 17, the Wavence product is displayed with its former name, 9500 MPR.

8

Click Search, choose the 9500 MPR services, and click Unmanage MPR 9500 Services.

Note: The Unmanage MPR 9500 Services button is only available in 5620 SAM releases earlier than 14.0 R7.

9

Close the form.

END OF STEPS

5.3 To perform post-upgrade tasks

5.3.1 Steps

Discover microwave backhaul services

1

Perform microwave backhaul service discovery. See 15.6 “Microwave backhaul service discovery” (p. 205) for more information.

Migrate service data

2

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

3

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

4

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

5

NOTICE

Service-disruption hazard

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

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

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

6

Locate the following XML tag:

<mprServiceProcessing>

7

Modify the value as follows:

```
enableMigration="true"
```

8

Save and close the nms-server.xml file.

9

Navigate to the */opt/nsp/nfmp/server/nms/bin* directory.

10

Enter the following:

```
bash$./nmsserver.bash read_config ↵
```

Result: Because a one-to-one relationship between 9500 MPR services in 5620 SAM releases earlier than 14.0 R7 and microwave backhaul services in 5620 SAM Release 14.0

R7 does not exist, all of the data may not be migrated from 5620 SAM releases earlier than 14.0 R7 to 5620 SAM Release 14.0 R7.

11

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

12

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

13

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

14

Locate the following XML tag:

<mprServiceProcessing>

15

Delete the following parameter:

`enableMigration="true"`

16

Save and close the nms-server.xml file.

END OF STEPS

6 Wavence SCM device management

6.1 Secure certification mode (SCM)

6.1.1 Introduction

The NFM-P supports the management of the CorEvo-based Wavence, Release 24 or earlier devices that are configured in a secure certification mode and are managed using the secure protocols. The security certification mode is configured in split-mount systems where the encryption block is installed in the radio transceiver connected to the MSS shelf over a Gigabit Ethernet interface.

6.1.2 SCM support deprecation

SCM is not supported in Wavence, Release 25 or later. For nodes using later releases of the Wavence software, use SNMPv3 secure protocols instead. See 2.2.5 “SNMPv3 authentication and privacy protocol support” (p. 67) for information about supported protocols.

6.1.3 Trusted manager

The NFM-P can manage a Wavence SCM device only when the server IP address is configured as a trusted manager in the WebCT. NFM-P generates the PollerProblem alarm when you try to discover the Wavence SCM device without adding the IP address in the trusted manager. You can add a maximum of five IP addresses in the trusted manager. If the limit is exceeded you need to delete an entry to add another trusted manager. See the Wavence documentation for more information about configuring the trusted managers in the WebCT.

6.1.4 Enable HTTPS protocol

NFM-P allows you to enable or disable the HTTPS protocol from the System Settings tab of the Network Element (Edit) form. When you set the HTTPS Protocol parameter as Enabled, you can access the node from NFM-P and from the WebCT.

6.1.5 Disable HTTPS protocol

DANGER

If the Wavence SCM device is unmanaged with the HTTPS Protocol parameter set to Disabled, no other EMS or NMS that does not have the server IP address registered in the trusted manager of the Wavence SCM device can access the Wavence SCM device.

To recover the Wavence SCM device, you must remanage the device in the NMS that has the IP address added in the trusted manager of the Wavence SCM device and enable the HTTPS protocol. If the NFM-P server is not available, you should reset the Wavence SCM device to factory settings.

See the Wavence documentation for more information about resetting the Wavence SCM device to factory settings.

WARNING

Disabling HTTPS protocol

When you set the HTTPS Protocol parameter as Disabled, you can access the node only from NFM-P that has the IP address added in the trusted manager of the Wavence SCM device.

You should ensure that the HTTPS Protocol parameter is set to Enabled in the System Settings tab of the Network Element (Edit) form, before unmanaging the Wavence SCM device.

6.1.6 SCM log file retrieval

The NFM-P supports the retrieval of SCM log files stored by the Wavence SCM devices.

The logs include:

- all user administration operations and the configuration changes in user activity logs in a user readable format. One entry is captured for each user action.
- all the security-related events in a security audit trail. These events include all security-related settings changes, user accounts management, exporting audit logs, and user login attempt failure.

Three types of log files are stored:

- UAL LOG (user activity through WebCT is stored)
- SNMP LOG (users activity through SNMP interface is stored)
- AUDIT LOG (security log is stored)

SCM log file compression

You can use the File Compression parameter on the Log Retrieval configuration form (Administration→NE Maintenance→Log Retrieval) to compress SCM log files before storing. The following compression options are supported: none, ZIP, and GZIP.

For each log file type, the Wavence SCM device stores a maximum of five log files. When the maximum number is exceeded, the oldest log file is deleted. See 2.10 “To retrieve log files stored by Wavence devices using the NFM-P” (p. 77) for more information about retrieving logs.

Exporting SCM log files to an OSS client

You can create and run an XML API script to allow an OSS client to determine the SCM log transfer status, such as when the log transfer request is complete and whether the file is available. The script can be run for the three supported SCM log file types: UAL LG, SNMP LOG, and AUDIT LOG.

The findToFile default location for file retrieval on a local or remote host is used.

For information about creating an XML API script and the findToFile method for retrieving SCM log files, see the *NSP NFM-P Scripts and Templates Developer Guide*.

6.1.7 Backup and restore

The NFM-P does not support the backup and restore function for Wavence SCM devices.

6.1.8 Software upgrades on Wavence SCM devices

NFM-P supports the following two variants of Wavence SCM devices:

- Wavence SCM devices that support software upgrades
- Wavence SCM devices that do not support software upgrades

The Wavence SCM devices that support software upgrades display the “Secure Certificated and Remote Management” value for the SNMP Mode parameter in the System Settings tab of the Network Element (Edit) form. The Wavence SCM devices that do not support software upgrades display the “Secure Certificated” value for the SNMP Mode parameter in the System Settings tab of the Network Element (Edit) form.

The Wavence SCM devices only support SFTP transport protocol. The software upgrade policy for 9500 MPR SCM devices must comply with certain conditions; see 4.1.2 “Wavence software upgrade policy requirements” (p. 101) for more information.

See the NE software upgrades chapter in the *NSP NFM-P Classic Management User Guide* for more information about how to configure a software upgrade policy and how to perform a software upgrade.

6.1.9 Alarms

The following alarms are supported in the SCM:

- CKM (Current Key Mismatch)
- NKM (Next Key Mismatch)
- KeyUnavailable (Key Unavailable)
- ESM (Encryption State Mismatch)
- TrafficDown (Radio Traffic Down)
- AesFipsFailure (MPT AES Engine self-test failure)

6.1.10 ECFM, TACACS+, and IPv6

The Wavence SCM devices do not support ECFM, TACACS+, or IPv6.

6.1.11 Protection configuration

Ensure that you power off the Wavence SCM device after the protection configuration is removed from the Wavence SCM device. Then, power on the Wavence SCM device for the correct protection configuration to reflect in the NFM-P for the Wavence SCM device.

6.2 Pathway to manage Wavence SCM devices

6.2.1 Process

1

Configure the SNMPv3 user in the WebCT. See the Wavence documentation for more information about configuring the SNMPv3 user in the WebCT.

2

Configure the NFM-P server IP address in WebCT trusted managers. See the Wavence documentation for more information about configuring the NFM-P server IP address in WebCT trusted manager.

3

Configure the SNMPv3 user account in the NFM-P; see 6.3 “To configure an SNMPv3 user account on a Wavence SCM device” (p. 116) .

4

Configure the Wavence SCM device mediation policy; see 6.4 “To configure Wavence SCM NE mediation” (p. 117) .

5

Configure the discovery rule; see 6.5 “To configure a discovery rule” (p. 118) .

6

As required, retrieve log files stored by Wavence devices; see 2.10 “To retrieve log files stored by Wavence devices using the NFM-P” (p. 77) .

6.3 To configure an SNMPv3 user account on a Wavence SCM device

Note: Both SNMPv3 and SCM is supported for Wavence, Release 24 and earlier. For nodes using Wavence, Release 25 or later, only SNMPv3 is supported.

6.3.1 Steps

1

Choose Administration→Security→NE User Configuration from the NFM-P main menu. The NE User Configuration form opens.

2

Click Create. The NE User Global Policy (Create) form opens.

3

Configure the User Name parameter as the same SNMPv3 username that you configured in the WebCT.

4

Select SNMP in the Access panel and click on the SNMPv3 tab.

5

Set the Authentication Protocol parameter to SHA.

6

Set the Privacy Protocol parameter to AES 256.

7

Configure the parameters in the Set New Authentication Password and the Set New Privacy Password panels with the same values that you provided in the WebCT.

8

Save your changes and close the form.

END OF STEPS

6.4 To configure Wavence SCM NE mediation

6.4.1 Steps

1

Choose Administration→Mediation from the NFM-P main menu. The Mediation (Edit) form opens with the General tab displayed.

2

Click on the Mediation Security tab.

3

Perform one of the following:

a. Click Create to create a new mediation security policy. The Mediation Policy (Create) form opens.

b. Choose an existing policy and click Properties. The Mediation Policy (Edit) form opens.

4

Set the Security Model parameter as SNMP v3 (USM).

5

Select the SNMPv3 user in the SNMPv3 panel.

6

Retain the default values for all other parameters in the Mediation Policy (Create/Edit) form.

7

Save your changes and close the form.

END OF STEPS

6.5 To configure a discovery rule

6.5.1 Steps

1

Choose Administration→Discovery Manager from the NFM-P main menu. The Discovery Manager form opens.

2

Click Create. The Specify General Attributes step form opens.

3

Configure the required parameters.

4

Select a equipment group.

Note: If the selected equipment group reaches the maximum element limit, any additional discovered NEs are automatically added to the Discovered NEs group.

5

Set the Discovery Protocol parameter as SNMP.

6

Click Next. The Add Rule Elements form opens.

7

Click Create to add a new rule element. The Topology Discovery Rule Element (Create) form opens.

8

Configure the required parameters and click OK.

9

Click Next. The Add Auto Discovery Rule Elements ACL form opens.

10

Retain the default values and click Next. The Configure Mediation Security form opens.

11

Select the SNMPv3 mediation security policy for read, write, and trap access, and the default mediation policy for security access, and click Next.

12

Retain the default values for all other parameters in the remaining step forms.

13

Click Finish.

Result: The Wavence SCM device is discovered in the NFM-P. The device appears on the equipment navigation tree and the topology map.

14

Perform the following to view the device properties:

1. Right-click on the device and choose properties. The Network Element (Edit) form opens.
2. Click on the System Settings tab and the SNMP Mode parameter displays the read-only value as Secured Certified.

15

Save your changes and close the form.

END OF STEPS

7 Wavence object configuration

7.1 Overview

7.1.1 General information

This chapter contains the procedures to configure Wavence device objects using the navigation tree. Device object properties forms, which are used to configure specific parameters for discovered devices, are accessed using objects on NFM-P navigation tree. See the “NFM-P navigation tree” chapter in the *NSP NFM-P Classic Management User Guide* for more information.

The device object is the discovered device at the top of the hierarchy in the navigation tree, directly below the network icon.

7.2 Pathway to configure and manage Wavence device objects

7.2.1 Pathway sequence

The following pathway describes the sequence of high-level tasks required to configure and manage Wavence device objects; see the “Device object configuration” chapter in the *NSP NFM-P Classic Management User Guide* for the generic procedures that apply to this device type. Also, configure the following device-specific tasks and functions.

7.2.2 Process

1

Configure the system settings for a Wavence device; see 7.3 “To configure the system settings on a Wavence” (p. 122).

2

Remove any inconsistencies created due to MIB population failures that can occur during service creation on a Wavence NE; see 7.4 “To resolve Wavence MIB inconsistencies” (p. 122).

3

Update the software activation status for Wavence SA nodes; see 7.5 “To update the software activation status for Wavence SA nodes” (p. 123).

4

Configure a scope of command role for Wavence element manager access; see 7.6 “To configure a scope of command role for NEtO access” (p. 124).

5

Start the Wavence external element manager from NFM-P GUI; see 7.7 “To cross-launch NEtO from NFM-P” (p. 125).

6

As required, review the specific network management features or functions that can be performed on Wavence devices using either NFM-P GUI or using a craft tool such as NEtO.

7.3 To configure the system settings on a Wavence

7.3.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence and choose Properties. The Wavence network element form opens.

2

Click on the System Settings tab, configure the parameters as required, and click OK.

Note: 802.1D bridge type is not supported if a CorEvo card is configured on the Wavence Release 6.0 or later.

3

Save your changes and close the form.

END OF STEPS

7.4 To resolve Wavence MIB inconsistencies

7.4.1 Purpose

Perform this procedure to resolve NE inconsistencies created due to MIB population failures that can occur during service creation on a Wavence NE. If there are NE inconsistencies, the Cleanup Inconsistencies button on the Wavence network element form becomes active to provide a visual cue that action is required to resolve them.

Nokia recommends that inconsistencies be resolved before any service creation. For failures during Wavence service creation, perform a resynchronization of the NE to restore existing NE entries. Inconsistencies are detected during NE synchronization or when opening the NE Properties form. If there are inconsistencies, an alarm with a Warning severity level on the NE appears.

7.4.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence and choose Properties. The Wavence network element form opens.

2

Click Cleanup Inconsistencies. NFM-P attempts to resolve the NE MIB inconsistencies.

3

To verify all MIB NE inconsistencies are resolved, click on the Faults tab to check for any remaining inconsistency alarms.

4

Click on the Abnormal Conditions tab to check for abnormal conditions on the Wavence, such as loopback or TxMute conditions, and to determine the appropriate corrective actions.

Note: You must refresh the Abnormal Conditions tab to ensure the latest content is displayed.

Note: You can clear the abnormal condition alarm after all the individual abnormal conditions are cleared.

5

Close the form.

END OF STEPS

7.5 To update the software activation status for Wavence SA nodes

7.5.1 Purpose

When software activation is performed via an MCT (microwave craft terminal) on a managed Wavence SA node, NFM-P does not indicate whether the software activation was successful. Perform this procedure to update the software activation status by applying a forced activation to the node. This procedure causes the Wavence SA node to reboot.

CAUTION

Service Disruption

Perform this procedure only in a maintenance window:

When you reboot a Wavence that is in service, it is service-affecting. Ensure that the reboot activity occurs during a maintenance window.

7.5.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence SA shelf and choose Properties. The Shelf (Edit) form opens.

2

Click on the Software Bank Details tab, select the Standby bank, and click Properties. The MPR Software Package (Edit) form opens.

3

Set the Activation parameter to Forced Activation and click Apply. The node reboots.

4

Close the form.

END OF STEPS

7.6 To configure a scope of command role for NEtO access

7.6.1 Steps

1

Using an account with an assigned security scope of command role, choose Administration→Security→NFM-P User Security from the NFM-P main menu. The NFM-P User Security - Security Management (Edit) form opens.

2

Click on the Scope of Command tab, click Create, and choose Profile. The Scope of Command Profile (Create) form opens

3

Configure the required parameters.

4

Click on the Roles tab and click Add. The Select Role - Role form opens.

5

Choose one of the following and click OK.

a. Admin NEtO launch to open the NEtO with the administration profile.

b. Viewer NEtO launch to open the NEtO with the viewer profile.

c. Default NEtO launch to open the NEtO with the null profile.

Note: If the option to run TACACS+ in the network is enabled, choose the Default NEtO launch.

6

Save your changes and close the form.

END OF STEPS

7.7 To cross-launch NEtO from NFM-P

7.7.1 Purpose

To cross-launch NEtO, you must belong to a user group that includes one of the following scope of command profiles that is configured with the Administrator role, or another role that has the following permissions set to Update/Execute:

- netw.NetworkElement.method_GUICrossLaunch
- mediation
- security.MediationPolicy

Note:

- Download the NEtO files to the client system under the directory neto within the path: *local_path*\nsp\nms\thirdparty\. For example:
  local_path\nsp\nms\thirdparty\neto
  where *local_path* is the location where the NSP client is installed
- If the NEtO files are not present in that directory, the system displays the error message “NEtO packages are not available. Please download them externally before proceeding.”
- For the Wavence SA, the NEtO cross-launch only occurs if the Wavence SA registration table entry has not reached the limit of 15 entries.
- NEtO cross-launch only occurs on Windows-based NFM-P clients.

For general information about user security, creating a scope of command role, and creating a scope of command profile, see the *NSP System Administrator Guide*. For specific information about creating a scope of command role for NEtO access, see 7.6 “To configure a scope of command role for NEtO access” (p. 124).

7.7.2 Steps

1

Perform one of the following:

a. In the navigation tree Equipment view, right-click on a Wavence and choose External Element Manager.

Note:

- When you launch NEtO for the first time, a confirmation dialog appears with Yes and No options. Click Yes.
  An error message appears if you click No.
- After the NEtO installation completes, the NEtO main view screen appears for all subsequent launches, with the NEtO version adjusted to the NE version from which the NEtO launched.

b. Perform the following for TACACS+:

1. In the navigation tree Equipment view, right-click on a Wavence and choose External Element Manager. A login prompt appears.

2. Type your login credentials. The NEtO main view screen appears.

Note: See the appropriate Wavence guide for information about configuring and using the NEtO external element manager.

END OF STEPS

8 Wavence shelf and card object configuration

8.1 Overview

8.1.1 General information

On the equipment navigation tree, shelf objects are children of device objects. Shelf objects appear below logical group objects in the navigation tree. Card objects are children of shelf objects, and as such appear below the shelf object in the navigation tree.

8.1.2 Wavence shelf information

Shelf objects represent the hardware that is configured on a shelf. When you choose the shelf object in the navigation tree and choose Properties in the contextual menu, you can view the states and conditions of the Wavence shelf including:

- general information
- fan tray state and speed
- card slots
- timing
- faults
- port segregation
- software control module
- software bank information
- cross-connections

For Wavence SA devices, you can view the following states and conditions on the shelf:

- general information
- display
- card slots
- software control module
- software bank information
- faults

The Display tab displays a graphical representation of the device shelf and its equipment components, such as the empty card slots and the cards that are installed on the device. You can double-click on an object in the tab to open its Properties configuration form. Right-click on the object and you have access to the contextual menus for the object and any child objects; for example, the ports of a card (dynamic graphical representation only).

8.1.3 Working with cards and card slot objects on Wavence devices

When you click the plus sign beside a shelf object, the card slots in the shelf appear in the navigation tree. They can appear as empty card slots when a card is not provisioned for the slot.

Card objects for Wavence devices must be configured using a Wavence element manager. See the Wavence documentation for more information.

8.1.4 EPS configuration in Core-E and CorEvo cards

NFM-P supports the configuration of equipment protection switching from main to spare and from spare to main in Core-E and CorEvo cards. See Procedure 8.6 “To perform protection switching in Core-E and CorEvo cards” (p. 137) for more information about configuring equipment protection switching.

Software upgrade

CAUTION

Service Disruption

You need to ensure that the main CorEvo card or Core-E card is active when you perform a software upgrade.

If the spare CorEvo card or Core-E card is active, switch to the main card before performing a software upgrade.

8.2 Supported Wavence device objects and auxiliary equipment

8.2.1 General information

NFM-P supports the following Wavence device shelves, objects, and auxiliary equipment:

- MSS chassis
- radios
- basic and advanced fan trays
- LAG objects

8.2.2 Supported MSS chassis types

The following MSS chassis types can be managed by NFM-P:

- **MSS-1**

  The MSS-1 is a 1 RU, 1-slot shelf. The first four ports of this shelf are Ethernet ports. Ports 5 and 6 are SFP ports. The shelf also supports 16 × DS1 or 16 × E1 ports.

  L1 radio LAG is supported on MSS-1. To be members of the L1 LAG, MPTs must be on port 5 or 6 of the MSS-1. You need to perform L1 radio LAG configuration using the NEtO external element manager before discovery from NFM-P. See the Wavence documentation for more information.

  Note: The equipment tree in the NFM-P GUI displays the MSS-1 shelf as a card slot with Ethernet ports numbered from 1/1 to 1/6 and TDM ports from 1/7 to 1/22.

- **MSS-4 and MSS-8**

  Slots 1 and 2 are reserved for Core-E cards. Each shelf requires a Core-E card in slot 1 and can have an optional spare card installed in slot 2 to protect the main card.

  The MSS-4 shelf supports cards in slots 3 and 4. A card in slot 3 can be protected by an identical card in slot 4.

The MSS-8 shelf supports cards in slots 3 to 8. Protected cards must be installed in slots 3, 5, or 7 and are protected by optional identical cards in slots 4, 6, and 8, respectively.

- **MSS-O**
  The MSS-O is a compact, full outdoor MSS unit. The device provides both optical and electrical Ethernet interfaces and can be installed indoors or outdoors.

8.2.3 Radio support

The microwave radio is a microprocessor-controlled transceiver that interfaces the MSS with the microwave antenna. A radio can be either an outdoor unit (ODU) or an indoor unit (IDU). Each Wavence chassis connects with one radio, either through a radio modem card or a Core card. Radio units can be configured for protection, that is, one radio unit can protect another. In 1+1 configuration the active radio unit is protected by a standby radio unit: in the event of failure of the active radio the standby radio takes over the active role. If there is no standby radio the configuration is called 1+0.

NFM-P can manage the following radio variants:

MPT-HCv2

The MPT-HCv2 ODU transports Ethernet traffic over an RF Radio channel between the MSS and the antenna, according to the configured QoS and to the scheduler algorithms. The input interface is a standard Gigabit Ethernet interface (electrical or optical). The MPT-HCv2 is XPIC-ready by the installation of a dedicated module. The MPT-HC V2 is frequency dependent.

MPT-MC

The MPT-MC is similar to MPT-HCv2 from an architecture standpoint. The differences are:

- MPT-MC is medium capacity
- MPT-MC is natively Ethernet powered through a proprietary PFoE
- MPT-MC has an optical cable length limit of 100 m

MPT-XP

The MPT-XP is a very-high-power version of the MPT-HCv2 and provides +7-8 dB of additional transmit power as compared to the equivalent MPT-HCv2. The MPT-XP is frequency dependent.

MPT-HL

The MPT-HL transceiver card is a microprocessor-controlled RF transceiver that interfaces with the Core-E card or MSS-1 shelf MPT-HL port with an antenna. The MPT-HL transceiver microprocessor manages transmit and receive frequencies, transmit power, alarms, and performance monitoring. The MPT-HL transceiver resides in the MPT-HL shelf.

The following configurations are supported:

- one or two Non-Standby (1+0) radios
- Hot Standby (1+1) and Hot Standby space
- frequency diversity

MPT-HLC

The MPT-HLC transceiver card is a microprocessor-controlled RF transceiver that interfaces with the Core-E card, EASv2 card, CAHD card, or MSS-1 shelf MPT-HLC port with an antenna. The MPT-HLC transceiver microprocessor manages transmit and receive frequencies, transmit power, alarms, and performance monitoring. The MPT-HLC transceiver resides in the MPT-HL shelf.

The following configurations are supported:

- one or two Non-Standby (1+0) radios
- Hot Standby (1+1) and Hot Standby space
- frequency diversity
- single-shelf repeater

MPT-HLS

The MPT-HLS is a fully indoor radio system, for long haul and cabinet requirements, and transports Ethernet traffic over an RF Radio channel. The MPT-HLS transceiver is connected to an MSS-1, MSS-4, or MSS-8. The MPT-HLS can be connected to the Core-E card or to an EASv2 card. The MPT-HLS is a four-rack (2200, 2000, 1700, 1300 mm) unit with two RT subracks. The subracks can be hosted with up to 10 transceivers. The TRU (always protected) is located on the top of the ETSI rack. A fan subrack is configured for each RT subrack. Two types of fan modules are available for configuration, Fan 4 and Fan 8. See the Wavence documentation for more information about configuring the MPT-HLS Radio.

NFM-P supports viewing the adaptive modulation values for the usage time 512 QAM and 1024 QAM in MPT-HLS.

MPT-HQAM

The MPT-HQAM outdoor unit is a microprocessor-controlled RF transceiver that interfaces with the MSS-1/4/8/1c shelf; MPTACC, Core-E, P8ETH, and EASv2 card, or standalone with the antenna. Fixed and adaptive modulation schemes are supported. Channel frequency is software selectable within tuning range of the MPT-HQAM transceiver. The MPT-HQAM transceiver is frequency dependent. An MPT-HQAM connected to a Core-E, P8ETH, or EASv2 card requires a power source. The MPT-HQAM has integrated XPIC and RPS functions.

NFM-P supports two operating modes in the MPT-HQAM:

- Standard mode

  The MPT-HQAM is used with its own capabilities and profiles. The air compatibility with another MPT-HQAM in Standard mode is supported.
- MPT-HC Compatibility mode

  MPT-HQAM is used with the MPT-HC capabilities and profiles. The air compatibility with another MPT-HQAM in MPT-HC Compatibility mode or with an MPT-HC is supported.

The operating modes are configured on the Wavence element manager, and NFM-P supports viewing the MPTHC Compatibility parameter, with the values set to True or False, on the Radio→General tab of the Physical Port (Edit) form.

NFM-P supports viewing 1+1 protection configuration for:

- two MPT-HQAMs, both configured in Standard mode
- two MPT-HQAMs, both configured in MPT-HC Compatibility mode
- two MPT-HQAMs, one configured in Standard mode and one in MPT-HCv2 Compatibility mode
- one MPT-HCv2 (with the main role as protection) and one MPT-HQAM configured in Standard or MPT-HC Compatibility mode
- one MPT-HQAM configured in MPT-HC Compatibility mode (with the main role as protection) and one MPT-HCv2

NFM-P supports the discovery of Radio L1 LAG by adding:

- MPT-HQAM in MPT-HC Compatibility mode to an L1 LAG of MPT-HCv2
- MPT-HQAM in Standard mode to an LAG L1 of MPT-HCv2
- MPT-HQAM in Standard or MPT-HC Compatibility mode to an L1 LAG of MPT-MC
- MPT-HQAM in Standard/MPT-HC Compatibility mode or MPT-MC to an L1 LAG of MPT-HQAM in MPT-HC Compatibility or Standard mode

NFM-P supports the discovery of Radio L2 LAG by adding:

- MPT-HQAM in MPT-HC Compatibility mode to an L2 LAG of MPT-HCv2
- MPT-HQAM in Standard mode to an L2 LAG of MPT-HCv2
- MPT-HQAM in Standard/MPT-HC Compatibility mode to an L2 LAG of MPT-HQAM in MPT-HC Compatibility/Standard mode

See the Wavence documentation for more information about configuring a Radio LAG.

An MPT type conversion procedure allows you to update an MPT-HCv2 to an MPT-HQAM on the node. For the complete procedure, see the Wavence documentation. The node restarts after the conversion and the NFM-P displays the updated MPT-HQAM on the equipment tree and the Port Usage parameter value in the General tab of the Physical Port (Edit) form.

UBT

The UBT outdoor unit is an ultra broadband transceiver. The UBT is supported in split-mount configuration, interfacing with the CorEvo, EAC, EASv2, or MSS-1. Adaptive modulation is supported. The UBT transceiver microprocessor manages transmit and receive frequencies, transmit power, alarms, and performance monitoring. See the Wavence documentation for information about channel spacing, shifter and frequency management, and modem profiles.

The following variants are supported:

- UBT-C: provides a single radio carrier with functionality similar to UBT-S in the frequency band of ≤ 38 Ghz
- UBT-m: provides a single radio carrier in the E-band (80 Ghz) frequency
- UBT-S: provides a single radio carrier in the 5.8 Ghz - 42 Ghz frequency bands

- UBT-S2: provides double radio carrier similar to the UBT-T, on a single radio board
- UBT-I: indoor unit that includes a single radio carrier in the 5.8 Ghz - 42 Ghz frequency bands in addition to a combiner module
- UBT-I2: an evolution of the UBT-I to address long haul needs, UBT-I2 is a single transceiver addressing low frequency bands (5.8GHz to 11GHz). The UBT-I2 has two different versions:
  - UBT-I2 XP which features a high Ptx (~40 dBm @QPSK)
  - UBT-I2 which features the same level of Ptx as the UBT-T XP

  NSP distinguishes between a UBT-I2 XP and UBT-I2 but functionally they are treated the same.
- UBT-T: provides double the radio capacity in the 5.8 Ghz - 42 Ghz frequency bands

  The two radio carriers of UBT-T can be used to aggregate traffic on the same direction (Twin Aggregated Radio). The carrier mode is set during the commissioning phase and cannot be changed later.
- UBT-T XP: provides a 6Ghz and 11GHz dual-band carrier

The UBT is commissioned in the Wavence element manager. The NFM-P will discover the UBT and display the variant in the Port Usage parameter value in the General tab of the Physical Port (Edit) form.

8.2.4 Fan tray support

The Wavence supports two fan tray types: basic and advanced. For the advanced fan tray, you can configure four ports for housekeeping alarms. See the Wavence documentation for more information about configuring a Wavence fan tray.

8.2.5 LAG objects support

NFM-P supports the following LAG objects on Wavence devices:

- L1/L2 Radio LAGs - You must use the Wavence element manager to complete the initial LAG configuration before discovery by NFM-P.
- L2 Ethernet LAGs - You can configure and discover L2 Ethernet LAGs using NFM-P or a Wavence element manager.

See Chapter 10, “Wavence LAG object configuration” for more information about Wavence LAG objects.

8.2.6 XPIC support

The Cross-Polarization Interference Cancellation (XPIC) function doubles the capacity of a single frequency by using both horizontal and vertical electromagnetic polarizations on a path. This increases capacity while also saving spectrum and antenna costs.

XPIC is required on two Radio interfaces in order to provide additional cross-polarization discrimination and to avoid co-channel interference. See the Wavence documentation for more information about radio support of XPIC and how to use the Wavence element manager to configure XPIC.

8.3 Equipment configuration

8.3.1 Physical equipment

Wavence devices can be discovered and managed by the NFM-P, however, devices, cards, and ports must be configured using a Wavence element manager. Depending on the chassis in use, you can configure up to eight cards. See the *Wavence Product Information Manual* for more information about equipment, and the *Wavence WebEML Manual* or *Wavence WebCT Manual* for procedures.

See 8.2 “Supported Wavence device objects and auxiliary equipment” (p. 128) for information about the supported devices and auxiliary equipment on Wavence devices.

EAC cards and its variants are supported from Wavence 18 node version onwards.

8.4 Pathway to manage Wavence devices

8.4.1 Wavence pathway sequence

The following pathway describes the high-level tasks required to commission and discover Wavence devices, configure and manage the device objects, and configure and manage the policies and services associated with the devices.

8.4.2 Process

1

Review the “Pathway to manage network objects” in the *NSP NFM-P Classic Management User Guide* before you use this pathway. The steps in this pathway are common to all NFM-P-managed devices.

2

Commission Wavence devices for NFM-P management; see Chapter 2, “Wavence device commissioning and management”.

3

Use NFM-P to discover Wavence devices; see the “Discovering devices using the NFM-P” chapter of the *NSP NFM-P Classic Management User Guide*.

4

View, manage, and configure Wavence device network objects as required; see the “Working with network objects using the NFM-P” chapter of the *NSP NFM-P Classic Management User Guide*.

5

Modify Wavence device shelf objects; see Chapter 8, “Wavence shelf and card object configuration”. You can only configure cards using a Wavence element manager. See the Wavence documentation for more information.

6

Modify ports on Wavence devices, as required; see Chapter 9, “Wavence port object configuration”. You can only configure ports using a Wavence element manager. See the Wavence documentation for more information.

7

View, manage, and configure Wavence device LAG objects; see Chapter 10, “Wavence LAG object configuration”.

8

As required, perform bulk configuration changes on Wavence devices to change the same configuration on multiple objects at the same time; see the “Bulk operations” chapter of the *NSP NFM-P Classic Management User Guide* for general guidelines. For example, configure a bulk change by choosing Wavence→System Settings - (mpr.MprNeProperties) in the Object Type drop-down menu to specify the bridge type for all Wavence devices. See the XML API Reference for information about all bulk change XML classes associated with the Wavence objects.

9

Create NFM-P policies that define the conditions for NFM-P management functions on Wavence devices.

a. Before creating policies for Wavence devices, review the “Policies overview” chapter of the *NSP NFM-P Classic Management User Guide* for information about NFM-P policy management and the pathway to create and distribute policies.

b. Create QoS device-specific policies as required for Wavence devices; see Chapter 13, “QoS policies”.

10

Before configuring backhaul, or composite services and related functions on Wavence devices, perform the following as required:

a. Review the “Service management and QoS” chapter of the *NSP NFM-P Classic Management User Guide* for information about configuring services on Wavence devices using the NFM-P.

b. Review the “Customer configuration and service management” chapter of the *NSP NFM-P Classic Management User Guide* for information about how to create and manage customers. As required, create customer profiles.

c. Review the Wavence service management and service tunnels chapter for specific information on supported service types; see Chapter 14, “Wavence service tunnels”.

d. Configure service tunnels to carry service traffic on Wavence devices; see Chapter 14, “Wavence service tunnels”.

11

Configure backhaul services for subscribers connected to Wavence devices; see Chapter 15, “Wavence microwave backhaul service management”.

12

Configure composite services to connect the types of services for subscribers connected to Wavence devices; see Chapter 16, “Wavence composite service”.

Fault management

13

Monitor and acknowledge incoming Wavence-specific alarms to check the type and characteristics of the alarms, and to resolve the network problems or physical equipment failures identified by the alarms; see the “Alarm management overview” chapter of the *NSP NFM-P Classic Management User Guide* for more information.

In addition:

- Click on the Abnormal Conditions tab of the Network Element (Edit) form to check for the abnormal conditions on the Wavence, such as loopback or TxMute conditions, to determine the appropriate corrective action. In previous releases of NFM-P, each abnormal condition on the Wavence was reported as an individual alarm on the Faults tab. Abnormal conditions are now reported as a single alarm.
- Refresh the Abnormal Conditions tab to ensure the latest content is displayed.
- Clear the abnormal condition alarm after all the individual abnormal conditions are cleared.

14

Perform specific Wavence device maintenance functions as required:

- configure on-demand or scheduled NE configuration backup and restore device configurations
- perform a Wavence device on-demand software upgrade; see Chapter 4, “Wavence software upgrade”
- monitor deployment of configuration changes to Wavence devices
- configure the OLC state on a Wavence device object to specify whether the object is in maintenance or in-service mode to filter alarms in the alarm window
- perform daily, weekly, monthly, and supplemental routine maintenance to maintain hardware and system integrity and efficiencies of Wavence devices

See the *NSP System Administrator Guide* for more information.

15

Collect NFM-P and NE statistics to monitor NFM-P and Wavence devices, network and service performance, compile equipment usage and billing data, and ensure SLA compliance; see the *NSP NFM-P Statistics Management Guide*.

8.5 Pathway to manage shelf objects on Wavence devices

8.5.1 Pathway sequence

The following pathway describes the sequence of high-level tasks required to manage Wavence device shelf objects. For general shelf object management information, see the “Shelf and card object configuration” chapter of the *NSP NFM-P Classic Management User Guide*.

8.5.2 Process

1

Configure NTP; see the “Shelf and card object configuration” chapter of the *NSP NFM-P Classic Management User Guide*.

2

Configure the card, card slot, and fan objects, and card and port protection using a Wavence element manager; see the Wavence documentation.

3

If required, configure synchronization using SYNC-IO SFPs on the CorEvo card or MSS-1 shelf; see 11.4 “To configure synchronization on a CorEvo card or MSS-1 shelf using SYNC-IO SFPs” (p. 164).

4

If required, configure a 1588 transparent clock; see 11.5 “To configure an IEEEv2 1588 TC on a Wavence shelf” (p. 164).

5

Upgrade the device software, as required; see Chapter 4, “Wavence software upgrade”.

6

As required, migrate a Wavence SA connected to a 7705 SAR from standalone mode to single NE mode; see 8.7 “To migrate the Wavence SA connected to a 7705 SAR from standalone mode to single NE mode” (p. 137).

7

As required, switch between an in-service protected Radio link and a standby protected Radio link for Wavence devices using a Wavence element manager.

8.6 To perform protection switching in Core-E and CorEvo cards

8.6.1 Steps

1

On the equipment tree, expand Network→Wavence→Shelf.

2

Right-click on the main or spare CorEvo or Core-E card slot object for which you need to perform protection switching, and choose Properties. The Card Slot (Edit) form opens.

3

Click on the Protection tab and configure the Commands parameter in the Equipment Protection Scheme Parameters panel.

4

Click Apply.

END OF STEPS

8.7 To migrate the Wavence SA connected to a 7705 SAR from standalone mode to single NE mode

8.7.1 Prerequisites

This procedure assumes you have configured a 7705 SAR MW link and link member before starting this procedure; see the “Shelf and card object configuration” chapter of the *NSP NFM-P Classic Management User Guide*.

Note: If the Wavence SA is discovered as a standalone device on NFM-P, then later changed to single NE mode, you must manually remove the Wavence SA node from the database because it shows as unreachable on NFM-P.

For information about the 7705 SAR and Wavence SA, see the Wavence Release 5.0 or later; and 7705 SAR 6.0 R1 hardware guides.

The following requirements must be met before you change the Wavence SA from standalone mode to single NE mode:

- Ensure that the 7705 SAR is upgraded to Release 6.0 R1 and the Wavence SA is upgraded to Release 5.0 or later.
- Ensure that the MPT software packages are in the cf3:/images/<Timos.xx.xx> directory on the 7705 SAR NE.
- Ensure that the MWA converted database (*.tar) file is in the cf3:<config file path> on the 7705 SAR NE.
- Ensure that the MPT state is operationally up when it is in standalone mode, by connecting it to the 7705 SAR.

8.7.2 Steps

1

On the equipment tree, right-click on a 7705 SAR port that you associated with the MW link and choose Properties. The MW Link Member (Edit) form opens.

2

Configure the parameters as required.

Note: For migration, restart the MPT using the MCT and deselect the Standalone check box within 30 to 60 s of the Radio restart or the MPT may not function as expected. If the restart fails to change the MPT to single NE mode, the MPT must be physically restarted. You can use the MCT only if the Wavence SA is in standalone mode and managed by NFM-P. If the Wavence SA is connected to the 7705 SAR in standalone mode, but not managed by NFM-P, you must use the NEtO/MCT.

3

Click on the Radio tab and configure the parameter as required.

4

Save your changes and close the form.

END OF STEPS

9 Wavence port object configuration

9.1 Overview

9.1.1 General information

Port objects are children of card slot objects. Port objects appear below the card slot after the card is configured. Properties forms for port objects are accessed using the NFM-P navigation tree.

9.1.2 QoS protection schemes for Ethernet ports

You can configure the following QoS protection schemes on Wavence Ethernet ports:

- **traffic storm control**

  A traffic storm occurs when packets flood a LAN creating excessive traffic and degrading network performance. You can use traffic storm control to prevent Ethernet ports from being disrupted by a broadcast, multicast, or unicast traffic storm on the physical interfaces, and limit the impact of VLAN misconfigurations.

  Traffic storm control monitors the incoming traffic levels over a 1-s interval and, during the interval, compares the traffic level with the traffic storm control level that you configure on NFM-P. The traffic storm control level is a percentage of the total available bandwidth of the Ethernet port. For example, if traffic storm control is enabled for ingress traffic and it reaches the configured level on the port with the interval, the traffic is dropped until the traffic storm control interval ends.

- **port rate limiting**

  You can use port rate limiting to protect the Radio-side bandwidth from being overloaded by an ingress or egress port. A common application for port rate limiting is when a Wavence provides the microwave backhaul service for multiple 7705 SAR devices whose queues do not have the visibility of the bandwidth available of the Radio side.

- **dot1q VLAN rate limiting**

  You can use dot1q VLAN rate limiting to protect the Radio side bandwidth on the Wavence from being overloaded by an ingress port when transporting IP/MPLS over MPR transport services on dot1q VLANs. A common application of the VLAN rate limiting feature is to monitor the microwave backhaul services providing transport to multiple 7705 SAR devices whose queues could individually exceed the available Radio bandwidth.

Traffic storm control, port rate limiting, and dot1q VLAN rate limiting are supported on the Core-E and 4+4 × Ethernet (EAS) cards on Wavence nodes. Port rate limiting is supported on MSS-4/8 cards on Wavence nodes Release 23 or later. Up to 1G values are supported on Wavence nodes Release 23 or earlier; 1G, 2.5G, and 10G is supported on nodes Release 23A or later.

See 9.3 “To configure Wavence Ethernet ports” (p. 141) for information about enabling traffic storm control, port rate limiting, and dot1q VLAN rate limiting on the Wavence.

9.1.3 Monitoring Wavence ports using 802.3ah EFM OAM remote loopbacks

You can monitor Wavence Ethernet or SFP ports using the 802.3ah EFM OAM remote loopback diagnostic test on Core-E, CorEvo, EASv1, and EASv2 cards, and on an MSS-1 or MSS-O shelf. See 9.9 “To configure 802.3ah EFM OAM remote loopbacks on Wavence ports” (p. 147).

Note: The link monitoring and fault signaling operational aspects of the 802.3ah EFM OAM diagnostic test are not supported on the Wavence.

When enabled, the remote loopback allows a local DTE to locate a remote DTE and put it into a state whereby all inbound traffic is immediately reflected back onto the link. The 802.3ah EFM OAM remote loopback information is carried by the OAMPDUs. OAMPDUs contain the control and status information to monitor, test, and troubleshoot OAM-enabled links.

9.1.4 2.5 Gb/s SFP port on CorEvo cards

NFM-P supports the configuration of the 2.5 Gb/s speed on the SFP ports of the CorEvo cards. See 9.12 “To configure 2.5 Gb/s speed on the SFP port of CorEvo card” (p. 149) for more information about how to configure 2.5 Gb/s speed on the SFP ports of the CorEvo cards.

9.1.5 UBT-I2 XP power mode support

Three additional power modes are available on the UBT-I2 XP: New HP ACCP, Current ACCP, and Diplexer. These values are displayed in NFM-P but must be configured in WebCT. The power modes appear on the radio tab for a UBT-I2 in XP mode..

9.2 Pathway to manage port objects on Wavence devices

9.2.1 General information

The following pathway describes the sequence of high-level tasks required to manage Wavence ports. See the Wavence documentation for more information.

If a change has been made to an object configuration in a Wavence element manager, you may need to perform a resync to see the correct updated information; see “To partially or fully resynchronize NEs with the NFM-P database” in the *NSP NFM-P Classic Management User Guide*.

Note: Port Mode for Wavence ports is not a configurable parameter, but is based on the overall configuration of the port. Radio ports are displayed as Network ports, and Ethernet ports are displayed as Access ports. An Ethernet port is displayed as a Network port instead if it has a physical link configured using the NFM-P, or an LLDP between two Wavence nodes.

9.2.2 Process

1

As required, configure the ports on Wavence devices using a Wavence element manager:

For Ethernet ports; see 9.3 “To configure Wavence Ethernet ports” (p. 141)

2

As required, configure or perform the following on Wavence device ports:

a. analog performance management on Wavence 1x Radio modem ports; see 9.5 “To collect and view analog radio statistics on Wavence 1x Radio modem ports” (p. 143)

b. power level performance management on Wavence 1x Radio modem ports; see 9.6 “To collect performance management statistics on Wavence 1x Radio modem ports” (p. 144)

c. Wavence port segregation; see 9.7 “To configure Wavence port segregation on an EAS module” (p. 145)

d. synchronization on Ethernet ports; see 11.3 “To configure synchronization on Wavence Ethernet ports” (p. 163)

e. loopback test on a Wavence DS1, ES1, or 1x Radio modem port; see 9.8 “To configure a loopback test on Wavence ports” (p. 146)

f. enable 802.3ah EFM OAM loopbacks on Ethernet or SFP ports; see 9.9 “To configure 802.3ah EFM OAM remote loopbacks on Wavence ports” (p. 147)

g. configure Tx mute on the radio ports; see 9.10 “To configure Tx mute on radio ports” (p. 148)

h. configure WRED QoS on UBT-S/S2 and UBT-T; see 9.11 “To configure WRED QoS on a Wavence MSS” (p. 149).

9.3 To configure Wavence Ethernet ports

9.3.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence Ethernet port and choose Properties. The Physical Port (Edit) form opens.

2

Configure the parameters as required.

Note: The User Label parameter configuration must be limited to a maximum of 15 characters.

3

Click on the States tab and configure the Administrative State parameter.

4

Click on the Ethernet tab and configure the parameters as required.

Note: Before configuring the Advertised Capability parameter, click Turn Up on the Physical Port (Edit) form to display the value of the Egress Rate parameter under the Ethernet tab of the Physical Port (Edit) form.

Check the combinations that are supported for the Advertised Capability parameter in the Wavence documentation.

5

Select the Hold Off check box to enable the hold-off timer.

Note: Hold-off timer can be enabled or disabled only on Ethernet ports that are part of the ERP ring component.

6

Perform the following step if you need to enable one or more protection schemes on the Ethernet port; otherwise, go to Step 7. See 9.1.2 “QoS protection schemes for Ethernet ports” (p. 139) in this section for more information.

a. To enable traffic storm control on the port, configure the parameters in the Storm control panel.

b. To enable port rate limiting on the ports, configure the parameters in the Port Rate Limiter panel.

c. To enable dotq VLAN rate limiting on the port:

Note: When you configure VLAN rate limits, ensure that the combined VLAN rate limits do not exceed the configured port rate limit or the port speed. The PortRateCIROverload alarm is raised when the VLAN rate limits exceed the available port rate, and is cleared when the sum of Ingress CIR on the VLAN rate limiter is less than the port interface speed or the configured Port Rate Limiter value.

You can enable up to eight VLAN rate limits on an Ethernet port.

1. Click on the VLAN Rate Limiter tab, choose an Ethernet port, and click Properties. The VLAN Rate Limiter (Edit) form opens.
2. Configure the parameters as required.
3. Save your changes and close the form.

7

Save your changes and close the form.

END OF STEPS

9.4 To configure LLDP

9.4.1 Before you begin

LLDP is a not a routing protocol, but instead, a neighbor-discovery protocol that allows an NE to advertise its identity and capabilities to other NEs attached to the same physical IEEE 802.1 LAN. As such, it is configured in a different manner than standard routing protocols.

Wavence supports Nearest Bridge LLDP. LLDP timers are not configurable.

LLDP is supported in the SM configuration only. An LLDP link with an SA or Connected node will appear as a link to an unmanaged NE. To avoid this, LLDP Administrative Status should be set to Disabled on SA and Connected NEs.

LLDP is supported on physical Ethernet ports and Ethernet LAG ports.

Note: The prerequisite for LLDP link to be discovered when ports are synchronous, is that the auto negotiation should be true on both end points of LLDP link and speed should be set to 1 Gb/s on both ports.

For more information about LLDP, see the *NSP NFM-P Classic Management User Guide*.

9.4.2 Steps

1

Physically connect the NEs to each other using Ethernet cable.

2

Perform the following on each NE:

1. On the equipment tree, expand Network→Wavence→Card Slot.
2. Right-click on the Ethernet port object and choose Properties. The Physical Port (Edit) form opens.
3. Choose the LLDP tab, then the Nearest Bridge sub-tab, then the General sub-tab. Set the Administrative Status parameter to Tx and Rx to discover the remote peer and link.

   Note: If the Administrative Status is set to Disabled, LLDP will be disabled on the port.
4. Choose the Ethernet tab, then the General sub-tab. Set the Auto-Negotiate parameter to True.

Results:

- The NFM-P discovers the remote peer and adds it to the Remote Peers sub-tab in the LLDP tab.
- The LLDP physical link is discovered and appears in green on the topology map.

END OF STEPS

9.5 To collect and view analog radio statistics on Wavence 1x Radio modem ports

Note:

- When per-queue statistics are collected, Q1 record is not available for the collected statistics.
- When per-queue statistics are collected, nothing is returned by the NE.
- When plotting is performed real-time, a data missing exception occurs for the specific interval.

- The retrieve time is not correctly updated.

9.5.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence 1x Radio modem port and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Statistics tab and choose Radio Analog Statistics (Radio Equipment) from the Select Object Type contextual menu.

3

Click Collect. A statistics record appears in the Physical Port (Edit) form.

4

Select the record and click Properties. The Statistics Record - Radio Analog Statistics form opens.

5

View the read-only analog performance values for the 1x Radio modem port.

6

Close the forms.

END OF STEPS

9.6 To collect performance management statistics on Wavence 1x Radio modem ports

Note:

- When per-queue statistics are collected, Q1 record is not available for the collected statistics.
- When per-queue statistics are collected, nothing is returned by the NE.
- When plotting is performed real-time, a data missing exception occurs for the specific interval.
- The retrieve time is not correctly updated.

9.6.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence 1x Radio modem port and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Statistics tab.

Choose one of the following performance management statistics from the Select Object Type contextual menu:

- Hop Current Data Stats
- Link Current Data Stats
- RSL Hop Current Data Stats
- TSL Hop Current Data Stats

3

Click Collect. A statistics record appears in the Physical Port (Edit) form.

4

Select the record and click Properties. The Statistics Record <*selected performance management stats type*> Current Data Stats form opens.

5

View the read-only performance values for the 1x Radio modem port.

6

Close the forms.

END OF STEPS

9.7 To configure Wavence port segregation on an EAS module

9.7.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence shelf and choose Properties. The Shelf (Edit) form opens.

2

Click on the Port Segregation tab and click Create. The Add Member - Shelf step form opens with the Select From Type step displayed.

3

Configure the From Type parameter and click Next. The From step appears.

4

Click Select, choose a port from the list, and click OK. The Add Member step form reappears.

5

Click Next. The Select To Type step appears.

6

Configure the To Type parameter and click Next. The To step appears.

7

Choose a port, click Finish, then OK. The Shelf (Edit) form reappears.

8

Close the form.

END OF STEPS

9.8 To configure a loopback test on Wavence ports

9.8.1 Supported card ports

You can configure a loopback test on Wavence ports on the following cards:

- UBT variants:
  - UBT-SA
  - UBT-C
  - UBT-I / I2
  - UBT-S / S2
  - UBT-T / UBT-T XP
  - UBT-m
- 1 x Radio modem
- MPT-HLS
- MPT-HLv1
- MPT-HQAM
- STM
- DS1
- ES1
- MPT-HCv2
- MPT-HLC

Note: If the card containing the ports is configured but not equipped, a loopback test cannot be performed on the physical ports of the card.

9.8.2 Steps

1

In the navigation tree Equipment view, right-click on a supported Wavence port and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Loopback tab, select an interface, and click Properties. The Loopback (Edit) form opens.

3

Configure the parameters as required and click OK. The Physical Port (Edit) form reappears.

4

Save your changes and close the form.

END OF STEPS

9.9 To configure 802.3ah EFM OAM remote loopbacks on Wavence ports

9.9.1 Supported card ports

You can configure an 802.3ah EFM OAM remote loopback on an Ethernet or SFP port on Core-E, CorEvo, EASv1, and EASv2 cards, or an MSS-1 or MSS-O unit.

Note: To configure an 802.3ah EFM OAM remote loopback on a port, the administrative state of a port must be up.

9.9.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence Ethernet port and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Ethernet tab, then on the EFM OAM tab.

3

Configure the Mode parameter as Active.

4

Configure the Administrative State parameter as Enabled. The value of the Operational Status parameter changes to Operational.

Note: You must not modify the Mode parameter when the Administrative State parameter is configured as Disabled, even though the Mode parameter is configurable.
The Operational Status parameter has intermediate values, before changing to Operational. The Operational Status can be Operational only when the remote DTE has the same settings as the local DTE for the 802.3ah EFM OAM remote loopback.

5

Perform 9.1.2 a to enable a remote loopback or 9.1.2 b to disable a remote loopback:

a. Select the Set Remote Loopback check box to enable a remote loopback. The value of the Loopback Status parameter changes to Remote Loopback after displaying some intermediate values.

Note: Ensure that the value for the Operational Status parameter is Operational before you select the Set Remote Loopback check box.
When remote loopback is enabled on a port, you cannot modify port segregation of the corresponding card.

b. Deselect the Set Remote Loopback check box to disable the remote loopback.

Note: You can disable remote loopback on a port when the value of the Loopback Status parameter is one of the following:

- Remote Loopback
- Initiating Loopback
- Terminating Loopback

6

Save your changes and close the form.

END OF STEPS

9.10 To configure Tx mute on radio ports

Note: On the UBT-SA S2, muting one channel automatically mutes both channels. The channels cannot be individually muted.

9.10.1 Steps

1

On the equipment tree, expand Network→Wavence→Card Slot.

2

Right-click on the radio port object and choose Properties. The Physical Port (Edit) form opens.

3

Click on the Radio tab and perform one of the following:

a. Set the Manual Local Tx Mute parameter on the Tx Mute panel to On and the transmitter is muted indefinitely.

b. Perform the following to provide a duration during which the transmitter is muted:

1. Set the Manual Local Tx Mute parameter to Timed.
2. Configure the Manual Local Timeout (minutes) parameter. The maximum duration is 2880 min (2 days).

   Note: You cannot set the Manual Local Timeout (minutes) to 0.

Note: It is not possible to change the Tx Mute parameter values from Timed to On or On to Timed. In both cases, change the Tx Mute parameter values from Timed to Off, then to On.

4

Save the changes and close the form.

END OF STEPS

9.11 To configure WRED QoS on a Wavence MSS

Note: You can enable WRED on UBT modules, and color mapping on an MSS-8, MSS-4, or UBT-SA device. When you configure radio queue settings, only select the UBT module which is online.

9.11.1 Steps

1

Enable WRED on the Wavence MSS device by performing the following:

1. On the equipment tree, expand Network→Wavence.
2. Right-click on the Wavence MSS object and choose Properties.
3. Click on the QoS tab, enable the WRED Status parameter, and configure the Color Classification parameter. If required, configure Dot1p forwarding class mapping.
4. Save and close the form.

2

On the equipment tree, expand Network→Wavence→Shelf→Card Slot→Port.

3

Right-click on the UBT port and choose Properties. The Physical Port (Edit) form opens.

4

Click on the Radio Queue tab, then select a queue and click on the Properties button. The QoS Radio Interface Queue Map (Edit) form opens.

5

Configure the parameters as required, then save and close the forms.

END OF STEPS

9.12 To configure 2.5 Gb/s speed on the SFP port of CorEvo card

9.12.1 Steps

1

On the equipment tree, expand Network→Wavence→CorEvo Card Slot.

2

Right-click on the SFP port object and choose Properties. The Physical Port (Edit) form opens.

3

Click on the Ethernet tab, configure the Auto-negotiate parameter as False, and the Advertised Capability parameter in the Capability panel as 2500Mb/s - Full-Duplex.

4

Save your changes and click on the General tab. The Actual Speed (kbps) parameter displays the value as 2500000.

5

Close the form.

END OF STEPS

9.13 To configure bandwidth notification on Wavence nodes

9.13.1 Supported nodes and ports

The bandwidth notification can be enabled on Wavence MSS ports or on the radio port of a Wavence SA.

9.13.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence and choose Properties. The Network Element (Edit) form opens.

2

Click on the Bandwidth Notification tab, and select a port in the Port panel. For a Wavence SA, the port is automatically selected.

3

Configure the Status parameter as Disabled and click Apply, then configure the required parameters in the Settings panel.

Note: The VLAN ID for a Wavence SA ranges from 0 to 4080, whereas for a Wavence SM, it ranges from 1 to 4080.

4

Configure the Status parameter as Enabled.

5

Save your changes and close the form.

END OF STEPS

10 Wavence LAG object configuration

10.1 Overview

10.1.1 Wavence LAGs

Link Aggregation groups (LAGs) are a set of ports used to interconnect network nodes using multiple links to increase link capacity and availability between them. LAGs also provide redundancy between the aggregated links. If a link fails, traffic is redirected onto the remaining link, or links. You can select a LAG as the terminating port when creating a network interface as part of an L3 service.

LAGs on the NFM-P GUI are represented as part of the navigation tree objects and are located below a device icon.

You can configure LAGs using the configuration forms available when you choose Create LAG from the LAG object navigation tree contextual menu. See the “Logical group object configuration” chapter in the *NSP NFM-P Classic Management User Guide* for more information.

10.1.2 Supported LAG types

The NFM-P supports the discovery of the LAG associations from NFM-P or the Wavence element managers for equipment functions on the Wavence.

You can configure the following LAG types for the Wavence:

- L1 Radio LAG (both static and adaptive modulation are supported) using an external element manager
- L2 Radio LAG (only static modulation is supported) using an external element manager
- L2 Ethernet LAG (supported modulation type does not apply to this LAG type) using an external element manager or NFM-P

Service configuration is supported across L1 and L2 Radio LAGs using the suite of current service functionality. For example, support is provided for detection of end-to-end bandwidth on the VLAN path or correlation of link level alarms up to paths that include L1 Radio LAGs.

NFM-P supports:

- discovery of the L1 and L2 Radio LAGs
- configuration and discovery of Ethernet LAGs

L1 LAGs can be created in the following configurations using a Wavence element manager:

- Intra plug-in LAG
- Cross plug-in LAG

An intra plug-in LAG is a LAG with MPT-HLS configured on the same card. A cross plug-in LAG is a LAG with MPT-HLS configured on two EASv2 or CAHD cards on the same MSS row.

10.1.3 L1 Radio port deployment guidelines

An L1 Radio LAG follows a similar deployment model as an L2 Radio LAG except that the L1 Radio LAG functions are deployed at the Radio layer. As a result, the L1 Radio LAG has different port associations, cross-connections, and validations from the L2 Radio LAG. The advantage of an L1 Radio LAG is that highly correlated upper-layer traffic can be hashed. For example, an LSP hashes to the same port in an L2 Radio LAG. Both L1 and L2 Radio LAGs must be configured using a Wavence element manager. See the Wavence documentation for more information.

10.1.4 Applying drop priority to SDH data flow cross-connections on L1 Radio LAGs

You can create a cross-connection of SDH data flow from an SDHACC card to an L1 Radio LAG on an EASv2 or CAHD card. The maximum number of SDH data flow cross-connections to an L1 LAG is 16. The SDH data flow cannot be cross-connected to any other LAG

If the LAG rate drops to less than the bandwidth required by the SDH data flow, congestion and frame loss may occur. To prevent this, you can configure a subset of the SDH data flow cross-connected to the LAG to be dropped to ensure enough bandwidth is available to transmit the remaining flows.

You can use the Drop Priority parameter on the Microwave Backhaul Service GUI forms (at both the service level or individual site level) to define the precedence a flow would take over other flows in the event of congestion. See 15.2 “To configure microwave backhaul services” (p. 195) for information about configuring the Drop Priority parameter.

By default, the drop priority of each SDH data flow is 255 when the cross-connection is created. Drop priority can be configured for each SDH data flow. SDH data flows with the highest drop priority configured are dropped first.

Note: You must create SDH2SDH service before configuring the drop priority value.

Drop priority deployment guidelines:

1. Configuration and reporting of drop priority can be performed at either a service or individual site level.
2. Cross-connections of SDH data flows to Radio L1 Radio LAGs are supported on the following MPT types on the EASv2 or CAHD:
   - MPT-HLS (version 5.2.1 or later)
   - MPT-xC / HQAM (version 6.0 or later)
3. If you configure the drop priority at the service level, this value is propagated to all sites that join the service.
4. On service discovery, if a mismatch is found between the service level and site level drop priority value, a serviceDropPriorityMismatch alarm is raised. You can clear the alarm by:
   - modifying the drop priority at each site to align with the value configured at the service level
   - modifying the drop priority at the service level, which in turn is propagated to all sites
5. If two of more SDH data flows originate from the same site, apply a unique drop priority value to each flow. In the event that the SDH data flows have the same drop priority value, a siteDropPriorityMismatch alarm is raised.

10.2 Pathway to configure and manage Wavence LAG objects

10.2.1 Pathway sequence

The following pathway describes the sequence of high-level tasks required to configure and manage Wavence LAG objects; see the “Logical group object configuration” chapter in the *NSP NFM-P Classic Management User Guide* for the generic procedures that apply to this device type. Also, configure the following device-specific tasks and functions.

10.2.2 Process

1

Configure an Ethernet LAG on the Wavence; see 10.3 “To create an Ethernet LAG on a Wavence” (p. 154).

2

Delete an Ethernet Wavence LAG; see 10.4 “To delete a Wavence Ethernet LAG” (p. 157).

10.3 To create an Ethernet LAG on a Wavence

10.3.1 General information

A LAG is a group of physical ports that form one logical link between two NEs to increase bandwidth, allow load balancing, and provide seamless redundancy. LAG support over multiple devices also provides NE-level redundancy. Use the following procedure to create and manage LAGs on Wavence devices.

Note: By default, an Ethernet LAG is in access mode and can be used as a SAP. If a physical link is created using Ethernet LAGs as the endpoints, the mode automatically changes from access to network mode. If a physical link is created between MPR and non-MPR LAG ports, and the MPR LAG port must be used as a SAP, the user must change the mode to access. See Step 11 for more information about how to change the mode.

Note: An Ethernet member port with a physical link or Radio port with protection cannot be added to a LAG. To add the port, you must delete the physical link, and then add the port to the LAG. See the “Topology map management” chapter in the *NSP NFM-P Classic Management User Guide* for more information about how to delete a physical link.

Note: For Fast Ethernet LAGs, electrical ports cannot be grouped with the optical ports.

10.3.2 Steps

1

In the navigation tree Equipment view, right-click on a Wavence Ethernet LAG and choose Create LAG. The Create LAG step form opens, displaying the Define General Properties step.

2

Configure the parameters as required and click Next. The Configure LAG Parameters step appears.

3

Configure the parameters as required and click Next. The Configure LACP step appears.

Note: The Name parameter configuration must be limited to a maximum of 15 characters.

4

Configure the parameters and click Next. The Configure LAG Members step appears.

5

Click Create to add ports to the LAG. The Create LAG Member form opens, displaying the Only show compatible ports step.

Note: The Show Only Compatible Ports parameter on this form does not apply to the Wavence. The Class parameter depends on the Lag Aggregation Type specified in Step 3.

6

Click Next. The Select Ports step appears.

7

Choose one or more ports from the list and click Finish. The Create LAG step form reappears.

8

Click Finish. The Create LAG - Wizard Completed form opens.

9

If required, select the View the newly created Port Termination check box to view the LAG properties; otherwise, click Close. The LAG appears under the LAGs icon in the navigation tree.

10

Right-click on the LAG, choose Turn Up, and click Yes.

11

As required, right-click on the LAG and choose Properties to view information about the created LAG or to modify the LAG parameters.

The LAG (Edit) form opens and displays the LAG ID and description.

- Choose one of the following Mode parameter values: Access (Ethernet LAG only) or Network.
- The Link Aggregation Group tab displays the Name of the LAG, the number of ports associated with the LAG member ports, and the Lag Aggregation Type. For Ethernet LAG,

choose Hash and Size from the drop-down menu.

- LACP parameters can be modified from the LACP tab.
- LAG member ports can be added from the LAG Members tab.
- The Administrative State parameter can be configured to Up in the States tab, only if at least one port is associated with a LAG. The LAG state cannot be set to Down if a service is associated with the LAG.

END OF STEPS

10.4 To delete a Wavence Ethernet LAG

10.4.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence Ethernet LAG and choose Delete LAG.

2

Click Yes to complete the deletion.

Note: A LAG can be deleted only if a member is not associated with the LAG. To delete the last member from a LAG, the Administrative State of the LAG must be set to Down. A LAG can be shut down only when the LAG is not a part of any service or physical link. Use the Wavence element manager to delete L1 and L2 Radio LAGs and LAG members. See the Wavence documentation for more information.

END OF STEPS

11 Wavence synchronization management

11.1 Introduction

11.1.1 Synchronization — Ethernet ports

PDH and SDH data flow is fragmented and the fragments are transmitted over a packet-switched network. The data rates are controlled by the terminating sites using clocks. The rate at which the fragments are transferred varies, based on the variations in these clocks. By synchronizing the clocks on the terminating devices, the received fragments are reassembled as in the original PDH or SDH data flow at the original bit rate.

You can configure synchronization on the Ethernet ports on the following cards:

- Core-E
- EASv2
- EAC
- CAHD
- UBT-m SA

Before configuring synchronous Ethernet, ensure the following:

- SFP must be configured on ports 5 and 6 on a Core-E card using a Wavence element manager.
- SFP must be configured on ports 5 to 8 on an EASv2 card using a Wavence element manager.
- SFP must be configured on an EAC card using WebCT.
- Ethernet ports and SFPs must be administratively up.

See 11.3 “To configure synchronization on Wavence Ethernet ports” (p. 163) for more information.

11.1.2 Synchronization — CorEvo and MSS-1

The CorEvo card and MSS-1 shelf do not have dedicated synchronization ports. The SFPs configured on the CorEvo card or the MSS-1 provide Sync-In/Out ports. The SFPs are installed in ports 5 and 6 of an MSS-1 and ports 7 and 8 of a CorEvo card. See 11.4 “To configure synchronization on a CorEvo card or MSS-1 shelf using SYNC-IO SFPs” (p. 164) for more information.

Note: The System Quality Level in the NFM-P is referred to as the NEC QL in WebCT.

11.2 IEEE 1588v2 PTP clocks

11.2.1 Introduction

The IEEE 1588v2 standard synchronizes the frequency and time from a master clock to one or more slave clocks over a packet stream. The IEEE 1588v2 is packet-based synchronization that can be over either UDP/IP or Ethernet and can be either multicast or unicast. See 11.4 “To

configure synchronization on a CorEvo card or MSS-1 shelf using SYNC-IO SFPs" (p. 164) for more information about configuring synchronization.

Note: Before configuring synchronization, you must configure the required SFPs on the CorEvo card or MSS-1 shelf with a value of SYNC-IO using a Wavence element manager.

11.2.2 Transparent clock

Transparent clock is a device that measures the time taken for a PTP event message to transit the device and provides this information to clocks receiving this PTP event message. You can enable an IEEE 1588 transparent clock (TC) on a Wavence shelf if the software License parameter value in the System Settings tab of the corresponding Network Element (Edit) form contains the string 1588TC. See 11.5 "To configure an IEEEv2 1588 TC on a Wavence shelf" (p. 164) for more information about configuring the IEEEv2 1588 TC on a shelf.

You can also perform a bulk operation to enable 1588 transparent clock on many shelves at once. Choose Tools→Bulk Operations from the NFM-P main menu and select SONET Sync in the object drop-down menu of the Create Bulk Change form to configure bulk changes for 1588 TC. See the "Bulk operations" chapter in the *NSP NFM-P Classic Management User Guide* for more information.

IEEE 1588v2 PTP support per platform

The platforms that are supported include:

- MSS-O
- MSS-1
- MSS-4
- MSS-8
- MSS-E/HE/XE
- UBT-NIM
- UBT-SA

IEEE 1588v2 PTP support is enabled or disabled at the node level then automatically applied by the node to the following MPT types of the node, if equipped:

- MPT-HC V2
- MPT-HLS
- MPT-HLC
- MPT-MC
- MPT-HQAM

Note:

- IEEE 1588v2 PTP is not supported for MPT-HL v1.
- IEEE 1588v2 PTP is not supported for MPRe and MSS-1c. However, 1588TC fail alarm reporting is supported.

11.2.3 Boundary and ordinary clocks

NFM-P supports the configuration of 1588 Boundary Clock and Ordinary Clock on the CorEvo card for Wavence, and 1588 Boundary Clock for the UBT-m in an SA topology (in both 0+1 and CA configurations).

You need to obtain an IEEE 1588 BC license to configure the 1588 BC and OC. After the license is enabled, the SW License parameter value in the System Settings tab of the corresponding Network Element (Edit) form contains the string 1588BC.

1588 BC and OC parameters are configured at the PTP port level and Wavence device level. The IEEE 1588 PTP object appears below the Synchronization object on the equipment navigation tree. The IEEE 1588 PTP object has the Clock objects as child objects. The ports are also listed at the Wavence device level in the IEEE PTP Clock tab of the Network Element (Edit) form.

See 11.6 “To configure IEEEv2 1588 BC and OC PTP clocks” (p. 165) for more information about configuring the 1588 BC and OC clocks.

Boundary clock

The boundary clock has 16 PTP ports. The boundary clock can be configured as a synchronization source. See 11.7 “To configure the PTP clock as a synchronization source” (p. 167) for more information about configuring the boundary clock as a synchronization source.

For the UBT-m SA, only the Boundary Clock is supported, with two PTP ports.

NEC configuration for UBT-m SA

You can use a UBT-m SA as an EEC node by enabling NEC configuration. Once NEC is enabled, you can configure synchronization settings, SyncE, and SSM options. NEC cannot be disabled unless the PTP clock is disabled.

Ordinary clock, slave

The ordinary clock, slave has a single PTP port. The ordinary clock, slave can be configured as a synchronization source. See 11.7 “To configure the PTP clock as a synchronization source” (p. 167) for more information about configuring the ordinary clock, slave as synchronization source.

Ordinary clock, master

The ordinary clock, master has a single PTP port. The ordinary clock, master cannot be configured as a synchronization source.

Statistics and alarms

NFM-P supports the following IEEE 1588 BC and OC statistics:

- aluPtpPeerPacketStatsTable
- aluPtpPeerClkRecAlgTable
- aluPtpPeerRecClkStatsTable

Note: You can reset all IEEE 1588 PTP statistics counters using the Reset Counters button located on the IEEE 1588 PTP Peer (Edit) form. To access the Reset Counters button, in the

Navigation tree equipment view, expand Network Element→9500 MPR Chassis→Synchronization→IEEE 1588 PTP→Clock→IEEE PTP Port→IEEE PTP Peers and choose Properties. You can confirm that the statistics counters are reset on the Statistics tab.

NFM-P supports the following IEEE 1588 BC and OC alarms:

- 1588AnnouncePktLOS
- 1588SyncPktLOS
- 1588DelayRespPktLOS
- 1588PTPClockclassDEG

11.2.4 1588 ToD

NFM-P supports the configuration of the 1588 ToD SFP in the following cards as noted:

- Port 7 and 8 of the CorEvo card
- Port 1 and 2 of the MSS-E/HE card in Wavence Release 22 or later.
- Port 8 of the MSS-XE card in Wavence Release 22 or later.

The ToD Admin Status and the ToD Message Formats parameters can be configured from NFM-P. See 11.8 “To configure the ToD” (p. 168) for more information about configuring ToD.

11.2.5 Holdover override

NFM-P supports enabling or disabling the Holdover Override parameter on PTP clocks. The parameter is disabled by default, and can only be modified when the PTP clock is administratively disabled. The parameter is supported on the MSS-4/8, MSS-E/HE/XE, and NIM.

11.2.6 PTP statistics naming in Wavence device and NFM-P

Table 11-1, “Mapping of the PTP statistics naming in the Wavence device and the NFM-P” (p. 162) lists the mapping of PTP statistics naming in the Wavence device compared to the naming in the NFM-P.

Table 11-1 Mapping of the PTP statistics naming in the Wavence device and the NFM-P

Wavence device naming	NFM-P naming
Peer packet statistics	
Peer Packets Statistics	**PTPStats (Precision Timing Protocol)**
Alternate Master Packets	aluPtpPeerAlternateMasterDisc
Announce Packets Input	aluPtpPeerAnnounceMsgRx
Announce Packets Output	aluPtpPeerAnnounceMsgTx
Bad Domain Packets	aluPtpPeerBadDomainDisc
Bad Version Packets	aluPtpPeerBadVersionDisc
Delay Request Packets Input	aluPtpPeerDelayReqMsgRx
Delay Request Packets Output	aluPtpPeerDelayReqMsgTx

Table 11-1 Mapping of the PTP statistics naming in the Wavence device and the NFM-P (continued)

Wavence device naming	NFM-P naming
Delay Response Packets Input	aluPtpPeerDelayRespMsgRx
Delay Response Packets Output	aluPtpPeerDelayRespMsgTx
Out Of Order Packets Input	aluPtpPeerOutOfOrderSyncPktRx
Step RM Greater Than 255	aluPtpPeerStepRemovedGreaterThan255Disc
Sync Packets Input	aluPtpPeerSyncMsgRx
Sync Packets Output	aluPtpPeerSyncMsgTx
Recovery Algorithm Statistics	
Peer clock recovery algorithm statistics	**Ptp Clok Recovery Algorithm Stats**
Free-Run	aluPtpFreqRecFreeRunCount
Acquiring	aluPtpFreqRecAcquiringCount
Phase-Tracking	aluPtpFreqRecPhaseTrackCount
Hold-Over	aluPtpFreqRecHoldOverCount
Locked	aluPtpFreqRecLockedCount
Excessive Freq Error Detected	aluPtpFreqRecExcessFreqErrCnt
Packet Loss Spotted	aluPtpFreqRecPacketLossCnt
Excessive Packet Loss Detected	aluPtpFreqRecLossResetCnt
High PDV Detected	aluPtpFreqRecVarTooHighCnt
Excessive Phase Shift Detected	aluPtpFreqRecPdvStepCnt
Sync Packet Gaps Detected	aluPtpFreqRecGapResetCnt
Short Interval Statistics	
Peer internal DPLL statistics	**Ptp Clok Recovery Short Interval Stats**
Phase Error StdDev [ns]	Alu Ptp Peer Intvl Phase Error Std Dev (ns)
Phase Error Mean [ns]	Alu Ptp Peer Intvl Phase Error Mean (ns)

11.3 To configure synchronization on Wavence Ethernet ports

11.3.1 Steps

1

In the navigation tree Equipment view, right-click on a supported Wavence Ethernet port and choose Properties. The Physical Port (Edit) form opens.

2

Click on the Timing tab and configure the SSM parameter to disable or enable the transmission of the synchronization status message over the Radio channel.

3

Save your changes and close the form.

END OF STEPS

11.4 To configure synchronization on a CorEvo card or MSS-1 shelf using SYNC-IO SFPs

11.4.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence shelf equipped with a CorEvo card or the MSS-1 shelf and choose Properties. The Shelf (Edit) form opens.

2

Click on the Timing tab and configure the Secondary Reference Type parameter as Sync-In Port. The Sync In panel is displayed.

3

Select the timing reference in the Sync In panel and click Apply.

4

Click Properties in the Sync In panel. The Physical Port (Edit) form opens.

5

Click on the Timing tab and configure the parameters in the Sync In/Out SFPs panel.

6

Click Apply to save your changes and close the forms.

END OF STEPS

11.5 To configure an IEEEv2 1588 TC on a Wavence shelf

11.5.1 Steps

1

In the navigation tree Equipment view, right-click on a Wavence shelf and choose Properties. The Shelf (Edit) form opens.

2

Click on the Timing tab, select the TC Enabled check box in the 1588 panel, and click Apply to save the changes and close the form.

Note: By default, the 1588 panel is present in the Shelf (Edit) form. However, if the corresponding Wavence device does not have the 1588 TC license, you cannot modify the 1588 on the shelf.

END OF STEPS

11.6 To configure IEEEv2 1588 BC and OC PTP clocks

11.6.1 Before you begin

- To be able to configure PTP clock parameters, you must disable the administrative state of the PTP clock.
- To be able to configure PTP port parameters, you must disable the administrative state of the PTP port.
- For UBT-m SA, to be able to configure PTP clock parameters, you must enable the administrative state of the NEC under Shelf→Timing tab

11.6.2 Steps

1

Configure VLAN elements. See 15.2 “To configure microwave backhaul services” (p. 195) for more information.

Note: Ensure that the adjacencies are configured manually and the path search option is not used.

2

On the equipment tree, expand Network→Wavence→Synchronization→IEEE 1588 PTP.

3

Right-click on the Clock object and choose Properties. The IEEE 1588 PTP Clock (Edit) form opens.

4

Set the Admin State parameter to Disabled.

Note: The parameters in the IEEE 1588 PTP Clock (Edit) form are not editable when the Admin State parameter is Enabled.

5

Perform one of the following to configure the clock type. For UBT-m SA nodes, only boundary clocks are supported.

a. Configure the boundary clock:
   1. Set the Clock Type parameter to Boundary Clock.
   2. Click Apply.
   3. Click on the IEEE PTP Port tab. Sixteen ports are listed. UBT-m SA nodes list two ports.

b. Configure the ordinary clock, slave:
   1. Set the Clock Type parameter to Ordinary Clock, Slave.
   2. Click Apply.
   3. Click on the IEEE PTP Port tab. One port is listed.

c. Configure the ordinary clock, master:
   1. Set the Clock Type parameter to Ordinary Clock, Master.
   2. Click Apply.
   3. Click on the IEEE PTP Port tab. One port is listed.

Note: When you change the clock type parameter, the values that are configured for the respective port parameters are lost and the parameters revert to the default values.

6

Choose a PTP port and choose Properties. The IEEE 1588 PTP Port (Edit) form opens.

7

Configure the VLAN ID parameter with the same value as you configured in Step 1.

Note: The VLAN ID that you assign to one port cannot be assigned to any other port.

8

Configure the remaining parameters, if required.

9

Save your changes and close the form.

10

Repeat Step 3 to open the IEEE 1588 PTP Clock (Edit) form.

11

Set the Admin State parameter to Enabled, save your changes, and close the form.

Result: All the parameters are read-only except Admin State and no further changes can be made to the Clock Type parameter.

End of steps

11.7 To configure the PTP clock as a synchronization source

11.7.1 Steps

1

On the NFM-P equipment navigation tree, expand Network→Wavence→Synchronization→IEEE 1588 PTP→Clock.

2

Right-click on the Clock object and choose Properties. The IEEE 1588 PTP Clock (Edit) form opens.

3

Configure the following parameters:

1. Set the Clock Type to Boundary Clock or Ordinary Clock, Slave.
2. Set the Admin State to Disabled.
3. Set the Frequency Source as Ptp.
4. Set the Admin State to Enabled.

4

Save your changes and close the forms.

5

Right-click on the Shelf object and click Properties. The Shelf (Edit) form opens.

6

Click on the Timing tab and configure the following parameters:

1. Set the Primary Reference Type in the Reference Type panel to 1588 PTP Clock.
2. Set the Secondary Reference Type in the Reference Type panel to Free Run Local Oscillator.

Note: In addition to the synchronization combinations mentioned above, all other supported combination around 1588PTP and other synchronization sources can be configured from NFM-P. See the Wavence documentation for more information.

7

Save your changes and close the forms.

END OF STEPS

11.8 To configure the ToD

11.8.1 Steps

Configure ToD using a Wavence element manager

1

Configure the 1588 ToD SFP on port 7 or 8 of the CorEvo card using WebCT. See the Wavence documentation for more information.

2

On the navigation tree, expand Network→Wavence→Shelf→Card (CorEvo).

3

Right-click on the port 7 or port 8 object and choose Properties. The Physical Port (Edit) form opens.

4

View the value of the Port Usage parameter in the Port Usage panel. The value is TOD-IO indicates whether the ToD SFP is configured successfully.

5

Click on the Time of Day tab and configure the ToD Admin Status and the ToD Message Formats parameters in the ToD SFP panel.

END OF STEPS

12 Wavence inventory management

12.1 Radio port inventory — Wavence SA and Wavence MSS-1c

12.1.1 General information

You can view the inventory of the Wavence SA and Wavence MSS-1c radio ports using the NFM-P Equipment Manager. See 12.4 “To configure radio port inventory for Wavence SA and Wavence MSS-1c devices” (p. 171) for more information about configuring the radio port inventory for Wavence SA and Wavence MSS-1c devices.

12.2 To list and sort inventory information

12.2.1 Steps

1

Choose Manage→Equipment→Equipment from the NFM-P main menu. The Manage Equipment form opens.

2

Perform one of the following to generate a list of equipment.

a. List the equipment on one NE.

1. Choose Network Element (Network) from the object drop-down menu and click Search. A list of NEs is displayed.
2. Select an NE and click Properties. The Network Element (Edit) form opens.
3. Click on the Inventory tab and choose an object type from the object drop-down menu. A list of objects is displayed.

b. List the equipment in the entire network.

1. Choose an object type from the object drop-down menu.
2. Configure the filter criteria and click Search. A list of objects is displayed.

3

Perform one or more of the following to format the results:

a. To display the number of items in the list, right-click on the list heading and view the Count value.

b. To sort the list, click on a column heading. The column heading displays an arrow that indicates the sort order.

c. To move a column, drag the column to a different position.

d. To remove a column, perform the following steps:
   1. Right-click on the column heading and choose Column Display. The Column Display form opens.
   2. Select the columns to remove in the Displayed on Table list, then click on the left arrow. The columns move to the Available for Table list.
   3. Click OK. The columns are removed from the table.

e. To sort multiple columns, perform the following steps:
   1. Right-click on a column heading and choose Show Sorting. The Show Sorting form opens.
   2. Select one or more properties in the Available for Sorting panel, then click on the right arrow button. The properties move to the Used for Sorting panel.
   3. Click Sort Ascending or Sort Descending, as required.
   4. Close the Show Sorting form.

4

Save your column display and sorting preferences:

1. Right-click on any column heading and choose Save Table Preferences.
2. Confirm the action. The configured display preferences are applied whenever you open a list table for the same object type.

5

Save the inventory output, as required. See 12.3 “To save an inventory list” (p. 170).

6

Close the form.

END OF STEPS

12.3 To save an inventory list

12.3.1 Steps

1

Right-click on a column heading of the inventory output and choose Save to File. The Save As file browser form opens.

2

Navigate to the directory in which you want to save the file.

3

Configure the File Name and Files of Type parameters.

4

Click Save. NFM-P saves the inventory list.

END OF STEPS

12.4 To configure radio port inventory for Wavence SA and Wavence MSS-1c devices

12.4.1 Steps

1

Choose Manage→Equipment→Equipment from the NFM-P main menu. The Manage Equipment form opens.

2

Choose Port (Physical Equipment)→Radio Port (Radio Equipment) from the object drop-down menu. A list of radio ports appears.

3

Remove all columns from the list except the following columns, which display the accurate values.

- Radio Interface ID
- Remote Node IPV4 Address
- Remote Node Interface

See 12.2 “To list and sort inventory information” (p. 169) and 12.3 “To save an inventory list” (p. 170) for more information about listing and sorting the inventory information.

Note:

- NFM-P does not support the display of accurate values for those columns other than the parameters displayed in the Physical Port (Edit) form.
- Performance monitoring status and remote inventory data are not part of the inventory report.

END OF STEPS

12.5 Radio port inventory – Wavence devices

12.5.1 General information

You can view the inventory of the Wavence radio ports using the NFM-P Equipment Manager. See 12.6 “To configure radio port inventory for Wavence devices” (p. 172) for more information about configuring the radio port inventory for Wavence SA and Wavence MSS-1c devices.

12.6 To configure radio port inventory for Wavence devices

12.6.1 Steps

1

Choose Manage→Equipment→Equipment from the NFM-P main menu. The Manage Equipment form opens.

2

Choose Port (Physical Equipment)→Radio Port (Radio Equipment) from the object drop-down menu. A list of radio ports and L1 radio LAGs appears.

3

Remove all columns from the list except the parameters that are displayed in the Radio tab of the Network→Wavence→Card Slot→Radio Port→Physical Port (Edit) form.

See 12.2 “To list and sort inventory information” (p. 169) and 12.3 “To save an inventory list” (p. 170) for more information about listing and sorting the inventory information.

Note:

- NFM-P does not support the display of accurate values for the columns other than the parameters that are displayed in the Radio tab of the Network→Wavence→Card Slot→Radio Port→Physical Port (Edit) form.
- The User Label column displays the accurate values for radio ports but not for L1 radio LAGs.
- Performance monitoring status and remote inventory data are not part of the inventory report.

END OF STEPS

12.7 Radio LAG member inventory – Wavence devices

12.7.1 General information

You can view the inventory of the radio LAG member inventory for Wavence devices using the NFM-P Equipment Manager. See 12.8 “To configure radio LAG member inventory for Wavence devices” (p. 173) for more information about configuring the radio LAG member inventory for Wavence devices.

12.7.2 Radio interface IDs

The radio interface IDs are defined as follows:

- Radio LAG – 50122 to 50135
- MPT Port – 500001 to 599999
- ODU Port – 50001 to 59999 except the IDs from 50122 to 50135 that are the radio LAG IDs

12.8 To configure radio LAG member inventory for Wavence devices

12.8.1 Steps

1

Choose Manage→Equipment→Equipment from the NFM-P main menu. The Manage Equipment form opens.

2

Choose Port (Physical Equipment)→Logical Port (Physical Equipment)→Port Group (Network)→Port Group (aggregation)→LAG (LAG) from the object drop-down menu. A list of LAGs appears.

3

Choose a specific radio LAG using the range of radio interface values listed in 12.7.2 “Radio interface IDs” (p. 172) and click Properties. The LAG (Edit) form opens.

4

Click on the LAG Members tab to list the members of the LAG.

Note: Performance monitoring status and remote inventory data are not part of the inventory report.

END OF STEPS

12.9 Inventory list of Wavence system settings

12.9.1 General information

You can view a list of Wavence system settings for all the managed Wavence devices using the System Settings (MPR) option in the object drop-down menu of the Manage Equipment form. See 12.2 “To list and sort inventory information” (p. 169) and 12.3 “To save an inventory list” (p. 170) for more information about listing and sorting the inventory information. You can also retrieve the data using the XML API. See *NSP NFM-P Classic Management User Guide* for more information

13 QoS policies

13.1 Overview

13.1.1 Supported QoS policies

QoS policies define how network traffic is shaped and queued on one or more Wavence device ports and to regulate data throughput. You can use NFM-P to create the following Wavence-specific QoS policies:

- **9500 NE QoS policies**
  9500 NE QoS policies define the QoS classification used for network traffic that traverses Wavence device ports and to apply the 9500 Radio Interface Queue Map policy.
- **9500 Radio interface queue map policies**
  9500 Radio Interface Queue Map policies specify the queue size and queue delay for all queues for the Radio interface that connect to Wavence ports. This policy is applied when the 9500 NE QoS policy is configured.

  The following variants are supported for this policy type:
  - ODU
  - MPT-HL
  - MPT-HC/MPT-MC
  - MPT-HLS
  - MPT-HLC
  - MPT-HQAM

13.2 Pathway to configure Wavence QoS policies

13.2.1 Process

1

Review the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide* for information about NFM-P policy management and for the pathway to create and distribute policies.

2

Review the “QoS policies” chapter in the *NSP NFM-P Classic Management User Guide* for information about how to create and distribute QoS policies.

Note: When you distribute a Wavence QoS policy, you cannot change the QoS Classification parameter and the Queue Mapping parameters in the same distribution. Change the QoS Classification parameter, distribute the policy, then change other parameters as required and distribute the policy again.

The Dot1p Color parameter on local definitions of a QoS policy is configurable, but

changing the value has no effect.

3

Create the following QoS device-specific policies as required:

a. 9500 Radio Interface Queue Map policy; see 13.3 “To configure a 9500 Radio Interface Queue Map policy” (p. 175).

b. 9500 NE QoS policies; see 13.4 “To configure a 9500 NE QoS policy” (p. 177).

13.3 To configure a 9500 Radio Interface Queue Map policy

13.3.1 General information

When configuring a 9500 Radio Interface Queue Map policy, the following QoS variants are supported: ODU, MPT-HL, and MPT-HC/MPT-MC.

13.3.2 Steps

1

Choose Policies→QoS→9500 MPR QoS→ 9500 Radio Interface Queue Map from the NFM-P main menu. The 9500 Radio Interface Map Policies form opens.

2

Perform one of the following:

a. Configure the Policy scope parameter to Global. Go to Step 3.

b. Configure the Policy scope parameter to Local.

If required:

1. Click Select to configure the Local Node IP Address parameter. The Select a Network Element form opens.
2. Choose a device and click OK. The 9500 Radio Interface Map Policies form reappears.

3

Click Create. The 9500 Radio Interface Queue Map, Global Policy (Create) form opens.

4

Configure the parameters as required.

5

Click on the Radio Interface Queue Map tab and click Create. The Radio Interface Queue Map, 9500 Radio Interface Queue Map Global Policy (Create) form opens.

6

Configure the parameters as required and click OK. The 9500 Radio Interface Queue Map, Global Policy (Create) form reappears.

Note: You cannot configure the queue size parameters when the Reset all Queues parameter is selected.

Note: The Queue Size parameter configuration must be limited to a maximum of 4034836 bytes and a minimum of 2480 bytes.

7

Save your changes and close the form. The 9500 Radio Interface Map Policies form reappears.

8

Click Search to display the created policy. To distribute the 9500 Radio Interface Map policy, see the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide*.

END OF STEPS

13.4 To configure a 9500 NE QoS policy

13.4.1 Steps

1

Choose Policies→QoS→9500 MPR QoS→9500 NE QoS from the NFM-P main menu. The 9500 NE QoS Policies form opens.

2

Perform one of the following:

a. Configure the Policy scope parameter to Global. Go to Step 3.

b. Configure the Policy scope parameter to Local.

If required:

1. Click Select to configure the Local Node IP Address parameter. The Select a Network Element form opens.
2. Choose a device and click OK. The 9500 NE QoS Policies form reappears.

3

Click Create. The 9500 NE QOS, Global Policy (Create) form opens.

4

Configure the parameters as required.

The QoS Classification parameter default setting is Disabled. If you configure the QoS Classification parameter to 802.1p, the Dot1p tab appears. If you configure the QoS Classification parameter to DiffServ, the DSCP tab appears.

Note: QoS Classification parameter is not supported for Wavence-SA nodes.

5

Select the Default Type as Core-Enh-Based or Core-Evo-Based depending on the type of nodes this policy is intended to be distributed to.

6

Click on the Queue Map Policy tab, click Select to choose a 9500 Radio Interface Queue Map Policy, and click OK. The 9500 NE QoS, Global Policy (Create) form reappears.

7

Click Apply. The 9500 NE QoS Global Policy (Edit) form opens.

8

Click on the Global Queue Setting tab, choose a Queue number, and click Properties. The RadioQ, Global Policy (Edit) form opens.

9

Configure the parameters as required.

10

Save your changes and close the form. The 9500 NE QoS Policies form reappears.

11

Click Search to display the created policy. To distribute the 9500 NE QoS policy, see the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide*.

Note:

- As a NE behavior, the distribution of classification mode changes the queue size to default a value. After the policy is distributed, repeat Step 8 thru Step 11 to set the required queue size.
- While distributing the policy, you can use the installed filters to filter for Core-Enh-Based and Core-Evo-Based nodes to aid in policy assignment. Do not delete the filters, as they cannot be recovered.

END OF STEPS

14 Wavence service tunnels

14.1 Overview

14.1.1 General information

A service tunnel is an entity used to unidirectionally direct traffic from one device to another device. The service tunnel is provisioned to use a specific encapsulation method, such as GRE or MPLS, and the services are then mapped to the service tunnel. See the “Service tunnels” chapter in the *NSP NFM-P Classic Management User Guide* for the complete list of supported objects that service tunnels can be configured for.

14.1.2 Wavence service tunnel (ERPS) support

You can configure the Wavence using an ERPS topology to create a collection of Ethernet ring nodes to form a closed physical loop. Between two and sixteen Ethernet ring nodes are supported per ERPS topology. The Wavence ERPS support includes tail nodes that connect to ERPS ring nodes. Multiple tail node configurations are supported by NFM-P.

See the “Service tunnels” chapter in the *NSP NFM-P Classic Management User Guide* for information about Ethernet (G.8032) rings and the Wavence ERPS tail node support, and the service types supported. See 14.3 “To create an Ethernet radio ring on a Wavence” (p. 184) for information about how to create an Ethernet Radio ring element on a Wavence.

14.1.3 Ethernet (G.8032) ring support

Ethernet Ring Protection (ERP), as specified in ITU-T G.8032, is a protection mechanism for Ethernet ring topologies that provides a resilient Ethernet network. ERP provides sub-50 ms protection and recovery switching for Ethernet traffic in a ring topology while ensuring that loops are not formed at the Ethernet layer. G.8032v1 supports a single ring topology; G.8032v2 supports multiple rings/ladder topology. For more information about Ethernet (G.8032) rings, see the ITU website at http://itu.int.

14.1.4 ERP topology support

An ERP topology is a collection of Ethernet ring nodes that forms a closed physical loop.

The following are the characteristics of an ERP topology:

- Two to sixteen Ethernet ring nodes are supported per ERP topology.
- A Wavence device can have up to eight ERP topologies.
- Up to eight ERP instances are supported per ERP topology.
- Two adjacent Ethernet ring nodes that are participating in the same ERP topology are connected by Ethernet ring links.

Loop avoidance in the ring is achieved by guaranteeing that, at any time, traffic may flow on all but one of the ring links. This link is called the ring protection link (RPL). One designated node, the RPL Owner (also referred to as the master node), is responsible to block traffic over the RPL.

14.1.5 Wavence ERPS tail node support on Ethernet (G.8032) rings

NFM-P supports configuration of tail nodes on Ethernet rings.

You can create several tail network configurations (see Figure 14-1, “Wavence ERPS tail node configuration (sample 1) ” (p. 179) and Figure 14-2, “Wavence ERPS tail node configuration (sample 2) ” (p. 181) below) on the Wavence including:

- a tail network of one or more MSS-4/8/E/HE/XE or UBT-NIM shelves attached to the ring to create, for example, a tree or linear chain
- a tail network of one Wavence SA attached to the ring to create a Wavence SA extension
- a head-end network of one or more MSS-4/8/E/HE/XE or UBT-NIM shelves

Figure 14-1, “Wavence ERPS tail node configuration (sample 1) ” (p. 179) and Figure 14-2, “Wavence ERPS tail node configuration (sample 2) ” (p. 181) show sample configurations of ERPS tail nodes.

Figure 14-1 Wavence ERPS tail node configuration (sample 1)

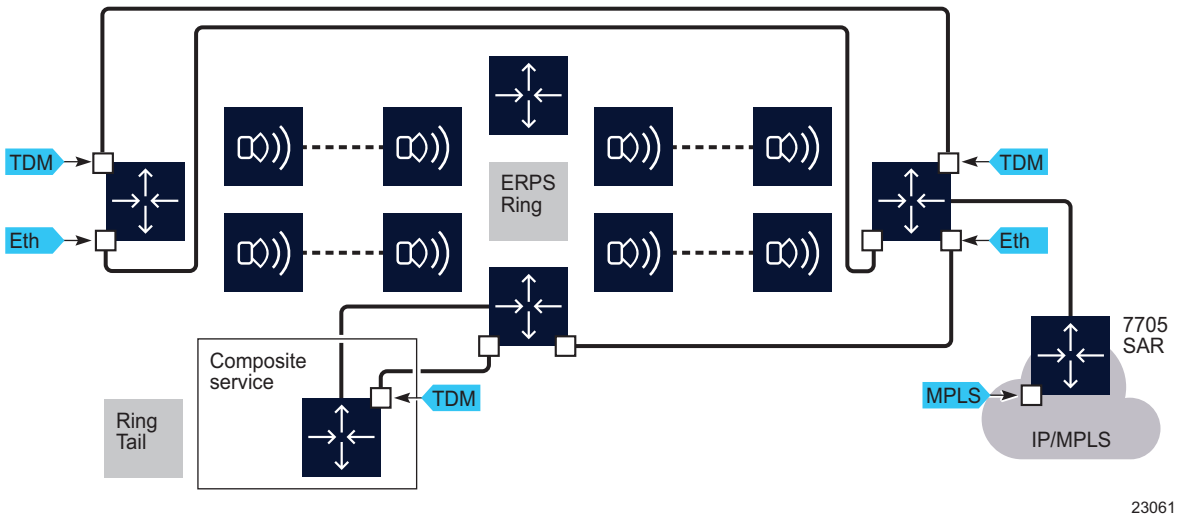
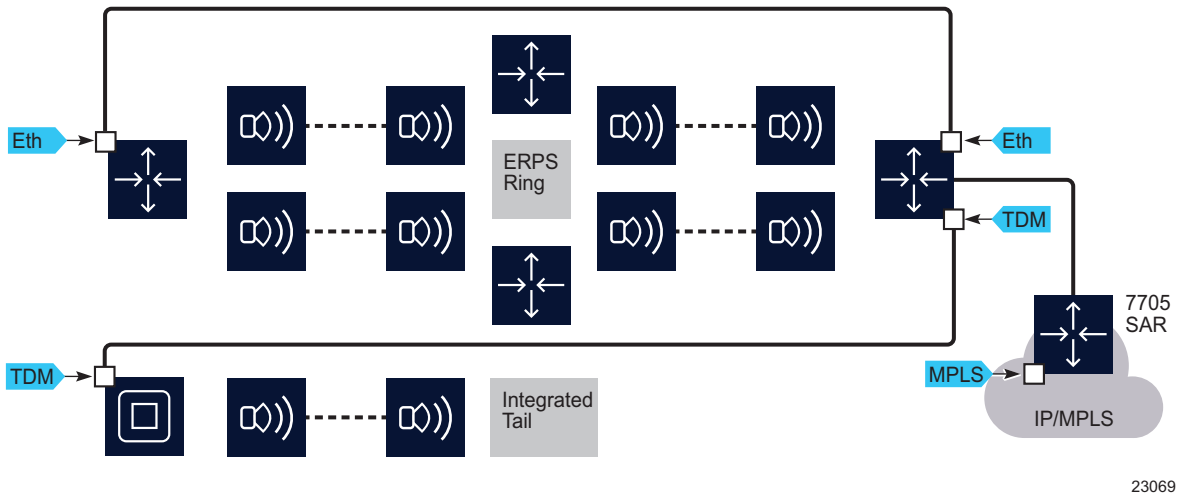


Figure 14-2 Wavence ERPS tail node configuration (sample 2)



14.1.6 Wavence ERPS tail node service provisioning

On supported Wavence MSS-4, MSS-8, and MSS-E/HE/XE shelves, you can provision any service on a tail node; for example, TDM-over-Ethernet using a hybrid path. The services can terminate on a ERPS ring node or on another tail node. For the Wavence SA, a single hop is supported by allowing a service to terminate on a network Radio port. The service terminates on the Radio port as a network attachment with a remote node is the target. You can add a manual link for the Wavence SA on the NFM-P map to provide a representation of the Wavence SA-to-MSS relationship on the ring. A one-hop Wavence SA tail node can also be used in a more traditional Wavence network. See Chapter 15, “Wavence microwave backhaul service management” for the pathway to create microwave backhaul services on Wavence devices.

14.1.7 Wavence ERPS fiber-microwave protection

You can configure fiber-microwave protection for services that traverse Wavence devices, to protect a fiber link with a microwave link when you create the Ethernet Radio ring element for a Radio ring, fiber ring, or mixed ring configuration. See 14.3 “To create an Ethernet radio ring on a Wavence” (p. 184).

The fiber link can be a fiber connection between two Wavence NEs or a wireline network connection between two Wavence devices, where the Wavence access to that wireline network uses a fiber connection.

Figure 14-3 Fiber-microwave protection on the Wavence

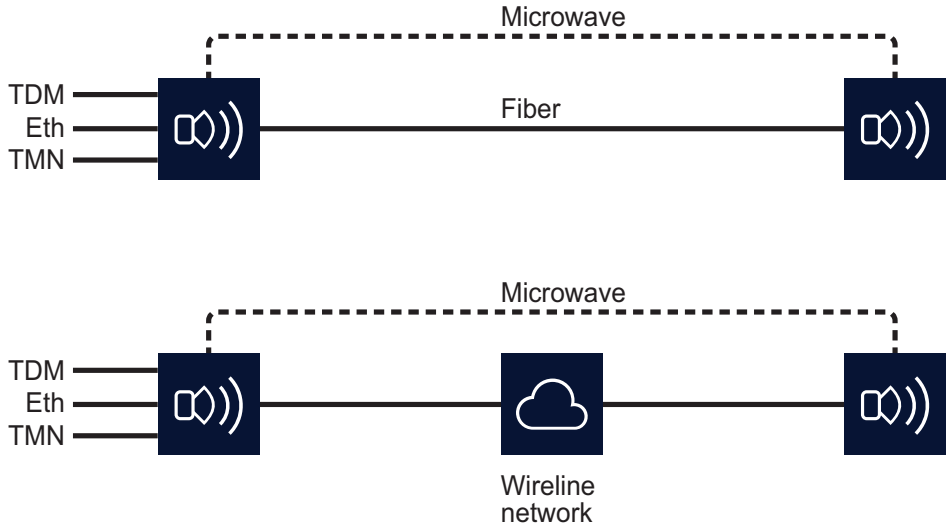


Figure 14-4 Fiber-microwave protection - operation

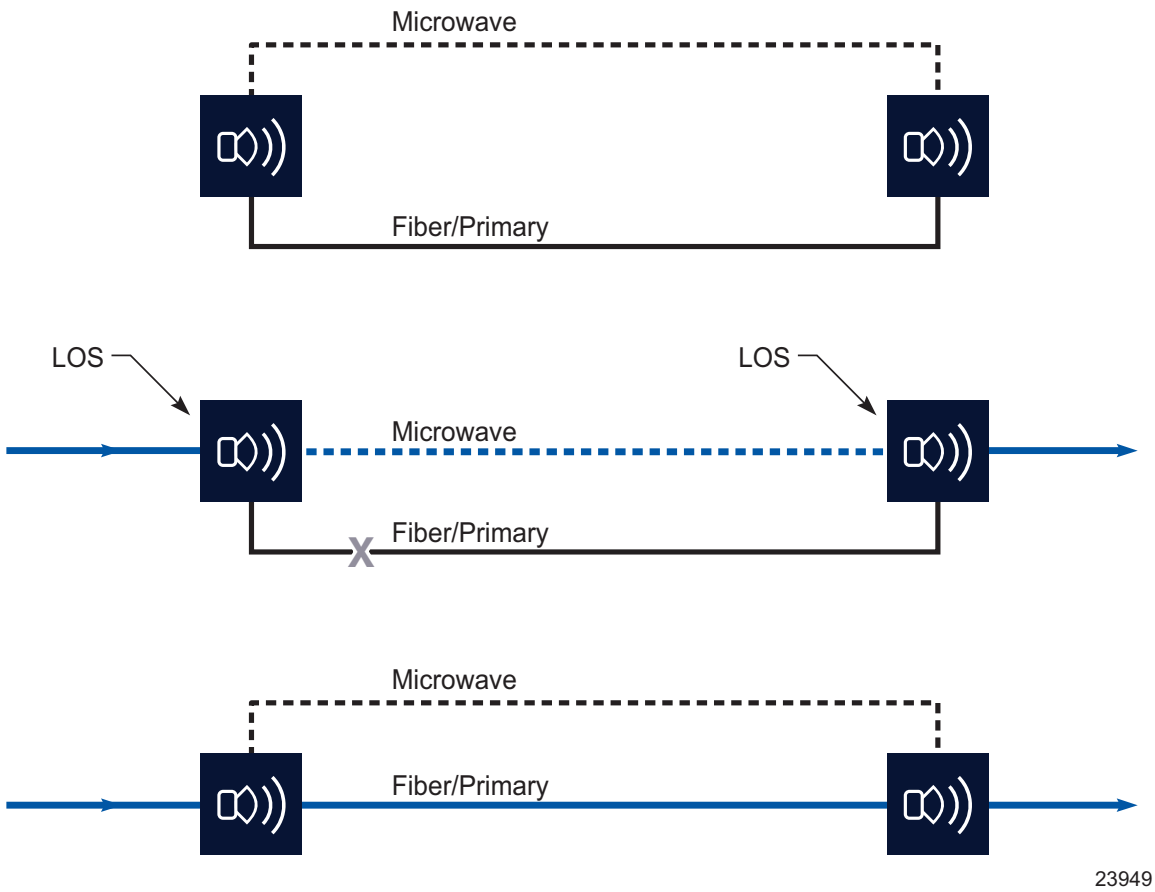
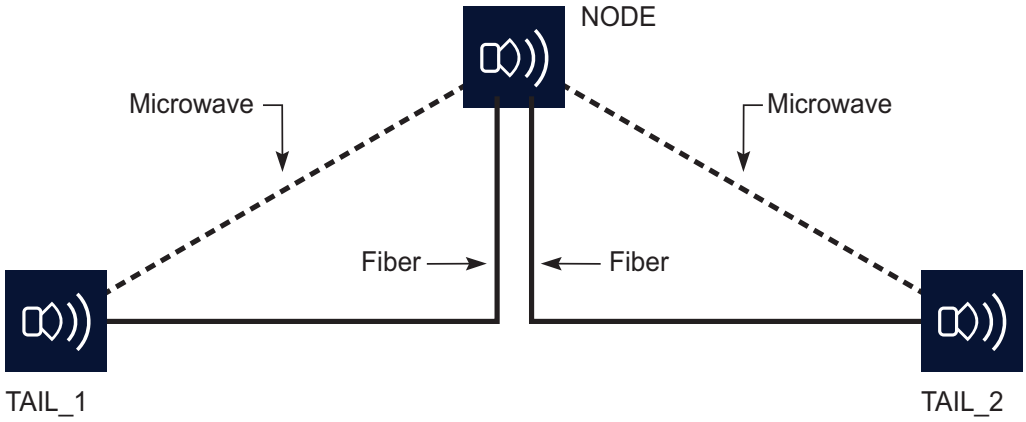


Figure 14-5 Fiber-microwave protection on tail nodes



Daisy chain is supported only for VLAN services. See Chapter 15, “Wavence microwave backhaul service management” for more information about configuring VLAN services on Wavence devices.

14.1.8 Supported ERP service types

You can configure the following service types in an ERP (G.8032) topology using NFM-P on Wavence devices:

- VLAN service
- VLL service (not supported on MSS-E/HE/XE and UBT-NIM)
- Both VLAN and VLL in the same microwave backhaul service

14.2 Configuring service tunnels on a Wavence

14.2.1 Purpose

Use the following procedure to configure service tunnels for Wavence devices. See the “Service tunnels” chapter in the *NSP NFM-P Classic Management User Guide* for the generic procedures that apply to this device type.

14.3 To create an Ethernet radio ring on a Wavence

14.3.1 Purpose

You can use this procedure to create an Ethernet radio ring element for a radio ring, fiber ring, or mixed ring on the Wavence.

Note:

- The radio ring operation status is not correctly displayed when an NE that is part of a ring is not reachable.
- The state cause of Provisioning Mismatch is not displayed for the MEG ID/level mismatch parameter of the Radio ring.
- Ring operation state is not updated correctly when multiple radio links are down.
- The Link Down state cause for Wavence VLL and VLAN services is not displayed when a link in a ring is down.
- The owner of the ring on the NFM-P topology map is labeled and the link that is blocked is highlighted in orange.

14.3.2 Steps

Create the ERP topology

1

On the equipment navigation tree, right-click on a Wavence and choose Properties. The Network Element (Edit) form opens.

2

Click on the Radio Ring Component tab and click Create. The Radio Ring Component (Create) form opens.

3

Configure the parameters in the Radio Ring Component (Create) form.

1. Configure the Topology Name parameter.
2. Click Select, choose an East port, and click OK.
3. Click Select, choose a West port, and click OK.
4. Save your changes and close the form.

   Note: The Type field is updated automatically to Radio or Fiber, based on the selected East Port and West Port.

4

Repeat Step 1 to Step 3 for each Wavence device that you want to add to your ERPS topology.

Create the Radio ring representation

5

Choose Manage→Service Tunnels from the NFM-P main menu. The Manage Service Tunnels form opens.

6

Click Create and choose Radio Ring. The Radio Ring (Create) form opens.

7

Configure the parameters as required and click Apply. The radio ring template is created and searched from the Radio Ring (Ethernet Ring) drop-down menu.

8

Double-click on an entry and the Radio Ring (Edit) form opens.

Define the elements in the Radio ring

9

Click on the Components tab, right-click on the Ring Elements icon in the navigation tree, and choose one of the following:

a. Create Ethernet Ring Element. The Select Network Elements form opens. Go to Step 10.

b. Add Existing Element. Go to Step 22.

10

Double-click on a network element. The Ethernet Ring Element (Create) form opens.

11

Configure the parameters as required.

12

Click Select in Radio Ring Topology panel and choose the appropriate ERP topology created in Step 1 to Step 3. The Ethernet Ring Element (Create) form reappears.

13

Click on the Path Endpoints tab and double-click to select the path A endpoint. The Ethernet Ring Path Endpoint - (Create) form opens.

14

Configure the MEG ID parameter and save the form.

15

Repeat Step 13 and Step 14 to configure the path B endpoint.

Note: The MEG ID parameter for the path B endpoint must be a different value than the one used for the path A endpoint.

16

If required, select the CLE/ODNC check box in the OAM Switch Criteria panel.

Note: If a port with the 802.3ah EFM OAM remote loopback enabled is selected as the endpoint of the ring instance, the OAM Switch criteria panel is displayed.
If the ring instance is in the idle state, the 802.3ah EFM OAM remote loopback enabled, and CLE/ODNC is selected, the ring instance changes to protected state.
If the CLE/ODNC parameter is selected for one ring instance, it is also applicable to other ring instances for that topology.

17

Save your changes and close the form.

Configure a ring protection link for the Radio ring

18

As required, configure a ring protection link for the Radio ring.

Perform the following:

1. Select a site located under the Ring Elements icon on the Radio Ring (Edit) form and choose Properties. The Ethernet Ring Element (Edit) form opens.
2. Set the Ring Protection Link Type parameter to Owner.
3. Click on the Path Endpoints tab and double-click on the endpoint that you want to delegate as the ring protection link. The Ethernet Ring Path Endpoint - Element - Node form opens.
4. Set the Path Endpoint Type parameter to the Ring Protection Link End.
5. Save your changes and close the form.

Note: There can be only one RPL owner in a given ring.

To label and highlight the link from RPL owner

19

In the Microwave Backhaul Service (Edit) form, click Connect Service to connect the microwave backhaul service.

Note: When a new RPL owner is set or after the topology is modified, the Topology Changed check box is selected automatically. The connect service operation must be performed for the changes to be reflected in the Service Topology map.
The microwave backhaul service is configured successfully.

20

Click the Topology View button to navigate to the Service Topology Map for a microwave backhaul service.

The ring owner is labeled on the NFM-P topology map and the link that is blocked is highlighted in orange on the Service Topology Map.

Add other ring elements as required to the Radio ring

21

Repeat Step 9 to Step 17 to create additional new ring elements to add to the radio ring.

22

As required, add existing ring elements to the radio ring.

Perform the following:

1. Right-click on the Ring Elements icon on the Radio Ring (Edit) form and choose Add Existing Element. The Select Elements form opens.
2. Click Search, choose a radio ring element, and click OK. A dialog box opens.
3. Click Yes to confirm.

Turn up all the ring elements

23

As required, turn up the radio ring elements in your Radio ring.

Perform the following:

1. Select all the sites located under the Ring Elements icon on the Radio Ring (Edit) form and choose Turn Up.
2. Click Yes to proceed.

Add the Radio ring to a microwave backhaul service

24

See Chapter 15, “Wavence microwave backhaul service management” to create a microwave backhaul service.

END OF STEPS

15 Wavence microwave backhaul service management

15.1 Microwave backhaul service configuration

15.1.1 Introduction

NFM-P supports the configuration of VLAN, VLL, and composite services on the Wavence devices. The VLAN and VLL services are configured using the microwave backhaul service configuration form. All the microwave backhaul services are identified by a VLAN ID and a service manager ID that are assigned at the time of service creation.

The microwave backhaul service configuration is performed as follows:

- configure the service adjacencies
- connect the service to ensure that the topology is correctly configured
- deploy the service to the Wavence devices
- monitor the service operational state

See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

The NSP supports Wavence service creation using intent-based service management. See 15.14 “Microwave backhaul service creation using NSP Intent-Based Service Management” (p. 218).

15.1.2 VLAN services

VLAN services provide the segmentation services traditionally provided by routers in LAN configurations. VLANs address issues such as scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, address summarization, and traffic flow management.

NFM-P supports the configuration of the following VLAN services on Wavence devices:

- P2P or P2MP (dot1q)
- P2P or P2MP (dot1ad)

The configuration of dot1q and dot1ad parameters is performed at the node level in the System Settings tab of the Network Elements (Edit) form.

See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

15.1.3 VLL services

NFM-P supports the configuration of VLL services on Wavence devices. A VLL service is an L2 point-to-point service that connects backhaul adjacencies. A VLL service is completely transparent to customer or subscriber data and to control protocols. Because of this transparency, the device

performs no MAC address learning in a VLL service. See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

15.1.4 Service objects

See 15.5 “To view the microwave backhaul service objects” (p. 203) for more information about each of the service objects.

15.1.5 Manual adjacency configuration

NFM-P supports the addition of the sites and adjacencies manually when you configure a microwave backhaul service. The physical links need to be configured and Ethernet ring needs to be configured for services that include one or more rings. See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

15.1.6 Automatic adjacency configuration

NFM-P supports adding the sites and adjacencies automatically when you configure a microwave backhaul service. You can configure a service, then perform path search, complete ring, or copy service to add the sites and adjacencies automatically. The physical links need to be configured and Ethernet rings need to be configured for services that include one or more rings.

Path search

A P2MP path is populated automatically by choosing Populate Service→Search For Path menu option on the Microwave Backhaul Service (Edit) form and selecting the source and destination sites. A P2MP path is populated automatically by performing multiple path searches. The P2P path is first configured. Then, the Populate Service→Search For Path option is used multiple times to search multiple paths. Alternatively, the source and destination ports are provided during the path search operation to complete the end-to-end path.

NFM-P supports path search with mixed path types that is, a combination of VLAN and VLL paths when both VLAN and VLL are part of a microwave backhaul service. In the Microwave Backhaul Service Path Search form, the *IsHeterogeneous* parameter is enabled for such mixed paths. Before implementing the path search for heterogeneous services, the MAC address must be calculated and explicitly given by the user for the traffic to flow between the nodes. The path search only lists the shortest paths. See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

Note: During path search, the entirety of the ring is a single hop, so a "longer" ring path may be returned instead of a topologically "shorter" path.

Note: When a configuration file is used to set up carrier aggregation between a Wavence UBT-NIM and a UBT-SM connected to a NIM interface, do not use path search, and instead manually create the service using the NFM-P. Using path search in this circumstance may create duplicate or misleading entries.

Complete ring

You can use the complete ring function in a service that includes one or more rings, which allows you to add all of the sites and adjacencies of the Ethernet ring at the same time. Configure one ring

site first, by providing a suitable adjacency and the ring pointer. Then, use the Populate Services→Complete Ring option on the Microwave Backhaul Service (Edit) form to automatically configure all of the remaining sites and adjacencies of the Ethernet ring. See 15.3 “To complete a ring by automatically adding the ring adjacencies” (p. 198) for more information about how to complete a ring.

Copy services

You can copy sites from an existing microwave backhaul service into a new microwave backhaul service. A new service is first configured, and the existing microwave backhaul service is copied, to create a new microwave backhaul service. All of the sites and ports are copied from the existing microwave backhaul service except the TDM, SDH channelized, and SDH ports that cannot be reused.

Ensure that the existing microwave backhaul service and the new microwave backhaul service:

- are of the same type (VLL or VLAN)
- have different VLAN IDs
- are connected
- are topologically correct

See 15.4 “To copy a microwave backhaul service” (p. 201) for more information about copying a service.

15.1.7 Connect service

Perform the connect service operation to establish links between the service objects. The integrity of the topology is determined when all the service objects are determined and the results are displayed. The incorrect topology is identified by a selected Topology Misconfigured check box and the correct topology is indicated by a deselected Topology Misconfigured check box. NFM-P calculates the operational state after the connect operation only if the topology is correctly configured and deployed on all of the Wavence devices. See 15.2 “To configure microwave backhaul services” (p. 195) for more information about microwave backhaul service configuration.

Incorrect topology

The following are the examples of scenarios that result in incorrect topology:

- physical link missing
- non-MPR sites missing from ring
- radio ring not created in the NFM-P
- ring element not added to radio ring
- missing ring termination site
- two or more disjointed topology services are merged into one service due to having the same VLAN ID

15.1.8 Deploy service

Perform the deploy operation to deploy the microwave backhaul service on the Wavence devices. The deploy operation also allows you to re-deploy failed deployments. You can skip the connect operation, and directly perform the deploy operation, if the connect operation fails even after repeated reconfigurations. NFM-P calculates the operational state only after the connect operation is performed and the topology is correctly configured.

Non-MPR sites

Deploying a microwave backhaul service does not deploy to non-MPR sites. If you add an SR or OEM site to the service, either manually, through path search, or through ring completion, the service configuration is not deployed. You need to configure the corresponding VPRN, VPLS, XC, and VLAN configurations on the non-MPR sites. While configuring such sites in backhaul service, NFM-P automatically deploys the adjacencies on the site.

15.1.9 Service topology map

You can open a service topology map for a microwave backhaul service by clicking Topology View on the Microwave Backhaul Service (Edit) form.

You can perform the following functions from the contextual menu in the service topology map:

- Connect service
- Deploy service
- Create backhaul site

15.1.10 Suppress backhaul service alarms

You can configure the NFM-P to automatically suppress backhaul service alarms on Wavence devices. To suppress these alarms, navigate to Administration→System Preferences and in the Wavence tab enable the Suppress Backhaul Service Alarms parameter. You can use the XML API to clear any existing alarms that have already been raised; see “Clearing suppressed alarms using the XML API” (p. 193).

When this parameter is enabled, the following alarms are suppressed and are not raised by the NFM-P:

- nonDeployedAdjacencyExists
- inSufficientBandwidth
- serviceDropPriorityMismatch
- siteDropPriorityMismatch
- serviceModified
- topologyMisconfigured
- backhaulServiceDown
- connectNotAttemptedOnService
- TestThresholdExceededAlarm2
- TestFailedAlarm2

- ProbeFailedAlarm2
- ServiceSiteDown

ServiceSiteDown alarm suppression

The ServiceSiteDown alarm is a Critical alarm that is used by other nodes in addition to Wavence devices, and by default is not suppressed when backhaul alarm suppression is enabled. To include this alarm in backhaul alarm suppression, you must configure an alarm policy to change the default alarm severity from Critical to Indeterminate. To configure an alarm policy, see the Classic Management chapter of the *NSP System Administrator Guide*.

After you configure the alarm policy, future ServiceSiteDown alarms are raised with a severity of Warning, and if you enable backhaul alarm suppression, then the alarms are suppressed and are not raised.

Default severity of backhaul service alarms

In NSP Release 25.11, the default severity of some backhaul service alarms was changed to Warning. Existing alarms of these types that were raised before you upgraded to Release 25.11 or later are displayed with a severity of Warning after the upgrade. The following table lists the changed alarms, and the previous severity.

Alarm name	Previous severity
backhaulServiceDown	Major
serviceModified	Major
topologyMisconfigured	Major
nonDeployedAdjacencyExists	Major
adjacencyDown	Major

Additionally, the default severity of the following alarms is Info, and the severity cannot be changed:

- connectNotAttemptedOnService

After you enable the Suppress Backhaul Service Alarms parameter, future alarms of these types are suppressed and do not appear in the NFM-P. For already existing alarms, you can use an XML API call to clear the alarms.

Clearing suppressed alarms using the XML API

After you enable the Suppress Backhaul Service Alarms parameter, you can use a POST or XML API call to clear existing backhaul service alarms from the database.

For POST, use the following:

```
<xmlapiRequest xmlns="xmlapi_1.0">

<mpr.MPRManager.deleteServiceAlarms xmlns="xmlapi_1.0">

    <deployer>immediate</deployer>
```

```
  </mpr.MPRManager.deleteServiceAlarms>

</xmlapiRequest>
```

For XML API, use the following:

```
{

"xmlapiRequest": {

   "mpr.MPRManager.deleteServiceAlarms": {

    "xmlns": "xmlapi_1.0",

    "deployer": "immediate"

  }

 }

}
```

15.1.11 Propagate microwave backhaul service names to sites

NFM-P allows you to propagate microwave backhaul service names to sites by selecting the check boxes, “Whenever a site is added to a service in the NFM-P propagate the Service Name to Site Name” and “Propagate Name and Description of Service” in the Services tab of the Administration→System Preferences→System Preferences form. See 15.10 “To propagate microwave backhaul service name to sites” (p. 209) for more information about how to propagate microwave backhaul service names to sites.

Note: Propagation of name from service to service site is supported during the following tasks after the deploy function is performed:

- creation of a new VLAN service
- modification of an already created or deployed VLAN service

Note: Propagation of name from service to service site is only applicable to VLAN service and not to VLL service.

If user enables this option (Administrator→System Preferences→Services) from the NFM-P GUI “Whenever a site is added to a service in the NFM-P propagate the Service Name to Site Name” then NFM-P will propagate the Service Name to Site Name while adding a new site to the existing service or while creating a new service.

If user disables this option (Administrator→System Preferences→Services) from NFM-P GUI “Whenever a site is added to a service in the NFM-P propagate the Service Name to Site Name” then NFM-P will not propagate the Service Name to Site Name during site addition to service.

If user enables this option (Administrator→System Preferences→Services) “Propagate Name and description of Service” then NFM-P will propagate the Service Name and Description of Service to Site Name and Description. This preference is applicable only for an existing service.

If user disables this option (Administrator→System Preferences→Services) “Propagate Name and description of Service” then NFM-P will not propagate Service Name and Description of Service to Site Name and Description. This preference is applicable only for an existing service.

Note: If the “Propagate Name and description of Service” system preference is enabled then NFM-P will be the master; any changes on the site’s Name from a Wavence element manager will be overridden with the Service’s Name in the NFM-P.

15.2 To configure microwave backhaul services

15.2.1 Before you begin

Ensure that:

- the physical links are configured (except for single-site service)
- Ethernet rings are configured, if you are creating a service that includes one or more rings. Only linear VLAN services are supported on ring topology. Linear VLL services are not supported on ring topology.

15.2.2 Steps

1

Perform one of the following to open the Microwave Backhaul Service (Create) form:

a. Choose Create→Service→Microwave Backhaul from the NFM-P main menu. The Microwave Backhaul Service (Create) form opens.

b.

1. Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.
2. Click Create→Microwave Backhaul. The Microwave Backhaul Service (Create) form opens.

2

Configure the parameters in the Customer panel.

3

Perform one of the following to configure the VLAN ID:

a. Retain the default selection in the Auto-Assign ID check box.

b. Disable the Auto-Assign ID and configure the VLAN ID.

4

In the Microwave Backhaul Service panel:

1. Configure the Type parameter as VLAN, VLL, or Unknown.

2. Configure the Drop Priority parameter if you need to define the minimum LAG bandwidth required to support the SDH data flow at the service level. See 10.1.4 “Applying drop priority to SDH data flow cross-connections on L1 Radio LAGs” (p. 154) for more information.

   Note: You can also configure the Drop Priority parameter at the site level; see step Step 6; substep 4.

5

Configure the remaining parameters on the General form, as required, and click Apply. The Microwave Backhaul Service (Create) form is updated as Microwave Backhaul Service (Edit) form and additional parameters appear.

6

Perform one of the following to configure the P2P service path.

a. Perform the following to configure the service path manually from the navigation tree:

1. On the navigation tree, right-click on the Sites object and choose Create Backhaul Site. The Select Network Elements form opens.
2. Choose a Wavence or a non-Wavence (7750 SR or 7210 SAS) site, as required, and click OK. The MBS Site (Create) form opens.
3. Click on the MPR Site tab and configure the parameters based on the service type.

If you set the Type parameter in Step 4 to:	Then the Connection Type parameter in the Service panel is set to:
VLAN	Tagged Ports You can either change or retain the value.
VLL	Cross Connection You can either change or retain the value.
Unknown	unspecified You can configure the value as Tagged Ports, if your service is VLAN, and Cross Connection, if your service is VLL.

4. Alternatively, configure the Drop Priority parameter if you need to define the minimum LAG bandwidth required to support the SDH data flow at the site level. See 10.1.4 “Applying drop priority to SDH data flow cross-connections on L1 Radio LAGs” (p. 154) for additional information.
5. Click on the Adjacencies tab and click Create. The Backhaul Adjacency (Create) form opens.
6. Choose the port, and radio ring, as required, and click OK. The Site, Adjacencies, and Port objects appear below the Sites object on the navigation tree.

   Note: You can also configure the adjacencies by right-clicking the Adjacencies object and choosing Create Backhaul Adjacency.

Note: For non-MPR sites, all radio ring options are listed. You need to select the Wavence radio ring for which the non-Wavence site is part of the topology.

b. Perform the following to populate the path automatically:

1. Click Populate Service→Search For Path. The Microwave Backhaul Service Path Search form opens.
2. Choose the source site and destination site.
3. Choose the source port and destination port, if required, and click Search. The path search results are listed.
4. Choose the required path and click OK. The Site, Adjacencies, and Port objects appear below the Sites object on the navigation tree.

Note: The path search lists either VLL or VLAN path depending on the microwave backhaul service type configured. The path search does not list both VLL and VLAN paths.

7

Configure the Element Instance parameter to select the Ring Element instance (uniformly) in the path search.

For example:

- Element Instance = 0 is given as input in the path search from Endpoint A to Endpoint B involving multiple rings each having more than one ring element instance (maximum 2); all the paths with ring element instance randomly selected in all the multiple rings, and shown as a result of the path search. Use this option for hop-based path searches.
- Element Instance = 1 is given as input in the path search from Endpoint A to Endpoint B involving multiple rings, each having more than one ring element instance (maximum 2); all the paths with ring element instance 1 in all the multiple rings are chosen and shown as result of the path search.
- Element Instance = 2 is given as input in the path search from Endpoint A to Endpoint B involving multiple rings, each having more than one ring element instance (maximum 2); all the paths with ring element instance 2 in all the multiple rings are chosen and shown as a result of the path search.

Note: After choosing a path search result and before applying the changes in the service template, there is an option to clear a ring instance pointer for any ring adjacencies on the Service form.
To change the ring instance pointer for all the ring adjacencies belonging to a specific ring:

1. On the Service form, expand Service→Sites→Site→Adjacenies→Port and choose a ring adjacency.
2. In the Local Adjacency Panel, press the Clear button associated with the Radio Ring parameter to delete the Port.
3. Use the Select button associated with the Local Port parameter to select a new port.

8

Repeat Step 6 and Step 7 to configure a P2MP service path, if required.

9

Click Apply. The Microwave Backhaul Service (Edit) form opens with the updated parameters.

10

Click Connect Service to connect the microwave backhaul service. The Connect Attempted check box is selected automatically.

11

Check whether the Topology Misconfigured check box is selected. If selected, the check box indicates that the topology is misconfigured. The reasons for the topology misconfiguration are provided in the Microwave Backhaul Services panel on the MBS (Edit) form. Take the corrective action to eliminate the errors. The Topology Changed check box is selected automatically after the topology is modified.

Note: See “Incorrect topology” (p. 191) for more information about common causes of incorrect topologies.

12

Click Connect Service again to attempt to connect the MBS. When all errors are eliminated, the Topology Misconfigured check box will be unchecked and the Reason for Topology Misconfiguration information will no longer be present on the form.

Note: You can skip Step 12, and go to Step 13 directly, if the connect operation fails even after the configurations are corrected. The operational state is not calculated in such cases.

13

Click Deploy Service.

Result: The microwave backhaul service is configured successfully.

Note: See “Non-MPR sites” (p. 192) for additional information about deploying a service with non-MPR sites.

END OF STEPS

15.3 To complete a ring by automatically adding the ring adjacencies

15.3.1 Before you begin

Ensure that:

- the physical links are configured
- Ethernet ring is configured

15.3.2 Steps

1

Perform one of the following to open the Microwave Backhaul Service (Create) form:

a. Choose Create→Service→Microwave Backhaul from the NFM-P main menu. The Microwave Backhaul Service (Create) form opens.

b. Perform the following:

1. Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.
2. Click Create→Microwave Backhaul. The Microwave Backhaul Service (Create) form opens.

2

Configure the parameters in the Customer panel.

3

Perform one of the following to configure the VLAN ID:

a. Retain the default selection in the Auto-Assign ID check box.

b. Deselect the Auto-Assign ID check box and configure the VLAN ID.

4

Configure the microwave backhaul service type as VLAN or VLL in the Microwave Backhaul Service panel.

5

Configure the remaining parameters on the General form, as required, and click Apply. The Microwave Backhaul Service (Create) form is refreshed as Microwave Backhaul Service (Edit) form and additional parameters appear.

6

Perform the following to configure one of the sites belonging to the Ethernet ring, along with the corresponding port adjacencies, and the ring pointer:

1. On the navigation tree, right-click on the Sites object and choose Create Backhaul Site. The Select Network Elements form opens.
2. Choose one of the ring sites and click OK. The Backhaul Site (Create) form opens.
3. Click on the Adjacencies tab and click Create. The Backhaul Adjacency (Create) form opens.
4. Choose the port adjacencies and the ring pointer and click OK. The Backhaul Adjacency (Create) form closes and Backhaul Site (Create) form reappears.

   Note: You can also configure the adjacencies by right-clicking the Adjacencies object on the navigation tree and choosing Create Backhaul Adjacency.
5. Click OK. The Backhaul Site (Create) form closes and the Microwave Backhaul Service (Edit) form reappears. The Site, Adjacencies, and Port objects appear below the Sites object on the navigation tree.

7

Perform the following to add the remaining sites and adjacencies of the ERP ring at the same time:

1. Click Populate Services→Complete Ring. The Complete Microwave Backhaul Service Rings form opens.
2. Click Search, choose the ERP ring, and click Complete Ring. The Complete Ring Service form opens with the sites, adjacencies, and port objects that are part of the ERP ring.
3. Click Apply. The Site, Adjacencies, and Port objects appear below the Sites object on the navigation tree of the Microwave Backhaul Service (Edit) form.

8

Click Apply. The Microwave Backhaul Service (Edit) form opens with the updated parameters.

9

Click Connect Service to connect the microwave backhaul service. The Connect Attempted check box is selected automatically.

10

Check whether the Topology Misconfigured check box is selected. If selected, the parameter indicates that the topology is incorrect. Correct the topology. The Topology Changed check box is selected automatically after the topology is modified.

Note: See “Incorrect topology” (p. 191) for more information about common causes of incorrect topologies.

11

Click Connect Service again to connect the microwave backhaul service. If the Topology Misconfigured and the Topology Changed check boxes are deselected, the parameters indicate that the configuration is correct.

Note: You can skip Step 11, and go to Step 12 directly, if the connect operation fails even after the configurations are corrected. The operational state is not calculated in such cases.

12

Click Deploy Service.

Note: See "Non-MPR sites" (p. 192) for additional information about deploying a service with non-MPR sites.

Result: The microwave backhaul service is configured successfully.

END OF STEPS

15.4 To copy a microwave backhaul service

15.4.1 Before you begin

Ensure that the microwave backhaul service that you want to copy has the service type configured as VLL or VLAN and the service is topologically correct. You can copy a VLL service into a microwave backhaul service configured with the service type VLL and a VLAN service into a microwave backhaul service configured with the service type VLAN.

15.4.2 Steps

Create a service

1

Perform one of the following to open the Microwave Backhaul Service (Create) form:

a. Choose Create→Service→Microwave Backhaul from the NFM-P main menu. The Microwave Backhaul Service (Create) form opens.

b. Perform the following:

1. Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.
2. Click Create→Microwave Backhaul. The Microwave Backhaul Service (Create) form opens.

2

Configure the microwave backhaul service type as VLAN or VLL in the Microwave Backhaul Service panel.

Note: Ensure that the Type parameter is not Unknown; the copy function is disabled when the Type parameter is Unknown.

3

Configure the parameters in the General tab, and click Apply to create a service into which the required service can be copied.

Copy service

4

Click Populate Service→Copy Service. The Copy Existing Microwave Backhaul Service form opens with a list of deployed microwave backhaul services that are topologically correct.

5

Choose the microwave backhaul service that you want to copy and click OK. The sites and ports are copied, except the TDM, SDH channelized, and SDH ports that cannot be reused.

Note:

- Ensure that the service that you want to copy has the service type configured and not unknown.
- You can only copy a VLAN service into a microwave backhaul service with service type VLAN, and VLL service into a microwave backhaul service with service type VLL.

Connect and deploy

6

Click Connect Service to connect the topology. The Connect Attempted check box is selected.

7

Check whether the Topology Misconfigured check box is selected. If selected, the parameter indicates that the topology is incorrect. Correct the topology. The Topology Changed check box is selected automatically after the topology is modified.

Note: See “Incorrect topology” (p. 191) for more information about common causes of incorrect topologies.

8

Click Connect Service again to connect the microwave backhaul service. If the Topology Misconfigured and the Topology Changed check boxes are deselected, the parameters indicate that the configuration is correct.

Note: You can skip Step 8, and go to Step 9 directly, if the connect operation fails even after the configurations are corrected. The operational state is not calculated in such cases.

9

Click Deploy Service.

Note: See “Non-MPR sites” (p. 192) for additional information about deploying a service with non-MPR sites.

Result: The microwave backhaul service is configured successfully.

END OF STEPS

15.5 To view the microwave backhaul service objects

15.5.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose Service (Service Management)→Microwave Backhaul Service (MPR) from the object drop-down menu and click Search.

3

Choose a microwave backhaul service and click Properties. The Microwave Backhaul Service (Edit) form opens.

General tab parameters

4

You can view the following parameters on the General tab:

- The Composite Service panel properties appear when the microwave backhaul service is part of a composite service.
- The Operational State parameter is Unknown until the service is connected and the service changes to Up, Down, or Unknown, depending on the factors described in 15.12.5 “Service state” (p. 214).
- The Type parameter in the Microwave Backhaul Service panel can be configured as VLAN, VLL, or Unknown. When you configure a service with the Type parameter set to Unknown, NFM-P automatically sets the service type, if the service is topologically correct, if, depending on the site, the service is set to VLL (at least one site is VLL) or VLAN (all sites are VLAN).
- The Drop Priority parameter in the Microwave Backhaul Service panel defines the minimum LAG bandwidth required to support the SDH data flow at the service level.

Sites tab parameters

5

Click on the Sites tab. The MPR and non-MPR sites are listed.

6

Choose a site and click Properties. The Backhaul Site (Edit) form opens.

7

The General tab provides the System ID of the site.

8

Click on the MPR Site tab and view the following parameters:

- The Connection Type parameter is configured as Tagged Ports for VLAN services and the Service Profile parameter displays the value as VLAN.
- The Connection Type parameter is configured as Cross Connection for VLL services and the Service Profile can be configured as CEM to CEM, CEM to Eth, or SDH to SDH.
- The MAC Address panel appears when the connection type is VLL. The peer and the local MAC addresses are configured manually or automatically, depending on the factors described in 15.12.3 “MAC address” (p. 213).
- The Drop Priority parameter in the SDH Details panel defines the minimum LAG bandwidth required to support the SDH data flow at the service level.

9

Click on the Adjacencies tab. The adjacencies are listed.

10

Choose an adjacency and click Properties. The Backhaul Adjacency (Edit) form opens and the parameters are as follows:

- The Local Port parameter displays the properties of the port that is part of a ring in services that include one or more rings.
- The VLAN Tagging parameter is displayed when the connection type is VLAN.
- The Radio Ring parameter displays the ring pointer.

11

Close the Backhaul Adjacency (Edit) form and the Backhaul Site (Edit) form. The Microwave Backhaul Service (Edit) form opens.

Adjacencies tab parameters

12

Click on the Adjacencies tab, then on the All sub-tab. All of the adjacencies of the microwave backhaul service are listed.

13

Click on the Terminating sub-tab. Only the service endpoint adjacencies are listed.

VLAN Construct tab parameters

14

Click on the VLAN Construct tab. The deployed cross-connects and VLAN elements are listed, depending on the service type configured. You can view the VLAN Construct tab to check whether all the cross-connects and VLAN elements are deployed on the microwave backhaul service.

END OF STEPS

15.6 Microwave backhaul service discovery

15.6.1 Introduction

The microwave backhaul services are discovered automatically when the Wavence devices are managed in the NFM-P and the Resync Status is Done. The physical links and Ethernet rings need to be configured and the discovered microwave backhaul services need to be connected. See 15.7 “To discover a microwave backhaul service” (p. 205) for more information about discovering a microwave backhaul service.

15.6.2 Move microwave backhaul service topologies

The microwave backhaul services that are autodiscovered may have multiple service topologies within a single microwave backhaul service with a single VLAN ID. You need to perform the connect operation on the autodiscovered services, so the multiple service topologies appear with topology IDs in the Sites tab of the Microwave Backhaul Services (Edit) form. The sites belonging to one topology have the same IDs, and such sites can be moved into a new service. Perform the connect operation on both the new service and the original autodiscovered service. See 15.8 “To move Wavence backhaul sites” (p. 207) for more information about moving a service.

15.6.3 Separate microwave backhaul service topologies

You can use the **Separate Topologies** function in the Sites tab of the Microwave Backhaul Services (Edit) form to move the sites belonging to one topology and create separate microwave backhaul services automatically. The microwave backhaul services need to be autodiscovered having a large number of service topologies within a single microwave backhaul service, and with a single VLAN ID. You can use Connect Microwave Backhaul Services→ALL or Connect Microwave Backhaul Services→Selected function to connect the new services. You need to perform the

connect operation also on the original autodiscovered service. See 15.9 “To separate microwave backhaul service topologies” (p. 208) for more information about configuring separate topologies.

15.7 To discover a microwave backhaul service

15.7.1 Before you begin

Ensure that you:

- configure the physical links
- configure the Ethernet ring

15.7.2 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose Service (Service Management)→Microwave backhaul service (MPR) from the object drop-down menu and click Search.

3

Choose the microwave backhaul service that is autodiscovered and click Properties. The Microwave Backhaul Service (Edit) form opens.

4

Click Connect Service to connect the microwave backhaul service. The Connect Attempted check box is selected automatically.

5

Check whether the Topology Misconfigured check box is selected. If selected, the check box indicates that the topology is misconfigured. The reasons for the topology misconfiguration are provided in the Microwave Backhaul Services panel on the MBS (Edit) form. Take the corrective action to eliminate the errors. The Topology Changed check box is selected automatically after the topology is modified.

Note: See “Incorrect topology” (p. 191) for more information about common causes of incorrect topologies.

6

Click Connect Service again to attempt to connect the MBS. When all errors are eliminated, the Topology Misconfigured check box will be unchecked and the Reason for Topology Misconfiguration information will no longer be present on the form.

7

Close the form.

END OF STEPS

15.8 To move Wavence backhaul sites

15.8.1 Steps

Configure a service

1

Perform one of the following to open the Microwave Backhaul Service (Create) form:

a. Choose Create→Service→Microwave Backhaul from the NFM-P main menu. The Microwave Backhaul Service (Create) form opens.

b. Perform the following:

1. Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.
2. Click Create→Microwave Backhaul. The Microwave Backhaul Service (Create) form opens.

2

Configure the VLAN ID with the value of the original service from which you want the sites to be moved, and click Apply, to create a new microwave backhaul service into which you want to move the sites.

3

Save the changes and close the form.

Move the sites to the service

4

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

5

Choose the discovered service containing multiple service topologies and click Properties. The Microwave Backhaul Service (Edit) form opens.

6

Click on the Sites tab and view the Topology column. The sites belonging to one topology will have the same IDs.

7

Choose the sites with the same IDs and click Move to Another Service. The Select Services form opens.

8

Choose the microwave backhaul service created in Step 1 to Step 3 and click OK. The Microwave Backhaul Service (Edit) form opens.

Connect service

9

Click Connect Service to connect the topology. The Connect Attempted check box is selected.

10

Check whether the Topology Misconfigured check box is selected. If selected, the parameter indicates that the configuration is incorrect.

Correct the configuration. The Topology Changed check box is selected automatically after the topology is modified.

Note: See “Incorrect topology” (p. 191) for more information about common causes of incorrect topologies.

11

Click Connect Service again to connect the microwave backhaul service. If the Topology Misconfigured and the Topology Changed check boxes are deselected, the parameters indicate that the configuration is correct.

Note: Ensure that the connect operation is performed on both the moved service and the original discovered service.

END OF STEPS

15.9 To separate microwave backhaul service topologies

15.9.1 Steps

Separate services

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose the discovered service containing a large number of service topologies and click Properties. The Microwave Backhaul Service (Edit) form opens.

3

Click Connect.

4

Click on the Sites tab and click Separate Topologies. New microwave backhaul services are created automatically for each of the topology IDs except the topology ID 1, and the corresponding sites are moved to the respective services.

Note: The Separate Topologies button is dimmed if the connect operation is not performed on the discovered service.
After the connect operation, the Separate Topologies button is enabled for the discovered services that have more than one topology ID.

5

Click Connect to connect the original discovered service, save the changes, and close the form.

Connect separated services

6

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

7

Perform one of the following to connect services:

a. Click Connect microwave backhaul services→All to connect all services.

b. Select the services and click Connect microwave backhaul services→Selected to connect the selected services.

END OF STEPS

15.10 To propagate microwave backhaul service name to sites

15.10.1 Steps

1

Choose Administration→System preferences from the NFM-P main menu. The System Preferences form opens.

2

Click on the Services tab and select the following check boxes:

- Propagate Name and Description of Service
- Whenever a site is added to a service in the NFM-P, propagate the Service Name to Site Name

3

Save your changes and close the forms.

4

Configure a microwave backhaul service. See 15.2 “To configure microwave backhaul services” (p. 195) for more information about how to configure a microwave backhaul service.

Result: The service name is propagated after the deploy function is performed.

Note: See 15.1.11 “Propagate microwave backhaul service names to sites” (p. 194) for more information about the behavior of the “Propagate microwave backhaul service name to sites” function while interworking with a Wavence element manager.

5

Save your changes and close the form.

END OF STEPS

15.11 To list microwave backhaul services

15.11.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Select the appropriate microwave backhaul service to list by choosing Service (Service Management)→<*option from the table below*> from the object drop-down menu and click Search.

To list MBH services by	Choose
Backhaul adjacency	Access interface (Service Management)→Backhaul Adjacency (MPR)
Service type	Service→Microwave Backhaul Service (MPR) or Service→Microwave Backhaul L3 Service (MPR)

Node site name	Site (Service Management)→Backhaul Site (MPR)

3

If required, choose a MBH service and click Properties. The<*selected MBH service*> (Edit) form opens.

4

Close the forms.

END OF STEPS

15.12 Microwave backhaul service associations

15.12.1 Composite services

A composite service is a set of linked services. Composite service functionality supports complex applications that require a combination of services, such as VLAN connections to a VPLS service. The composite service provides the functionality to combine an L2 backhaul service created on the MSS1 Wavence node with an L3VPN service having radio as SAP that was created on the MSS8/4 CorEvo node that has the same VLAN ID.

You can also configure a composite service with a microwave backhaul service on a Wavence, and a VPLS service on a 7210 SAS or 7750 SR. See Chapter 16, “Wavence composite service” for more information about configuring a composite service.

15.12.2 Wavence element manager interworking

Table 15-1, “Wavence element manager interworking” (p. 211) lists the impact on the microwave backhaul services when the modifications are done in a Wavence element manager.

Table 15-1 Wavence element manager interworking

If you modify the	Then
Backhaul adjacency in a Wavence element manager	The serviceModified alarm is generated for the service with no additional text.
Microwave path in a Wavence element manager as part of load balancing	For VLL services: • VLL:serviceModified alarm is generated for the VLL service with no additional text • cross-connect adjacencies are changed on the fly • no need to delete the non-deployed adjacencies • perform the Connect Service action
	For VLAN services: • VLAN:serviceModified alarm is generated for VLAN service with no additional text • delete the non-deployed adjacencies • perform the Connect Service action

Table 15-1 Wavence element manager interworking (continued)

If you modify the	Then
Microwave path in a Wavence element manager as part of error correction	For VLL services: • VLL:serviceModified alarm is generated for the VLL service with no additional text • cross-connect adjacencies are changed on the fly • no need to delete the non-deployed adjacencies • perform the Connect Service action
	For VLAN services: • VLAN:serviceModified alarm is generated for VLAN service with no additional text • delete the non-deployed adjacencies • perform the Connect Service action
VLAN ID in a Wavence element manager as part of error correction	For VLL services: • VLL:serviceModified alarm is generated for the old VLL service with no additional text • a new service with new VLAN ID is autodiscovered with Topology Changed check box selected • perform the Connect Service action for the newly autodiscovered service • delete the old VLL service, if required
	For VLAN services: • VLAN:serviceModified alarm is generated for the old VLAN service with no additional text • a new service with new VLAN ID is autodiscovered with Topology Changed check box selected • perform the Connect Service action for the newly autodiscovered service • delete the old VLAN service, if required
Ethernet path in a Wavence element manager	For VLL services: • VLL:serviceModified alarm is generated for the VLL service with no additional text • cross-connect adjacencies are changed on the fly • no need to delete the non-deployed adjacencies • perform the Connect Service action • perform the Deploy Service action, if required.
	For VLAN services: • VLAN:serviceModified alarm is generated for VLAN service with no additional text • delete the non-deployed adjacencies • perform the Connect Service action

15.12.3 MAC address

Table 15-2, “MAC address” (p. 212) lists the conditions under which the MAC address is automatically calculated.

Table 15-2 MAC address

Connection		MAC Address
TDM port to TDM port connection		NFM-P automatically calculates the MAC address
TDM to Ethernet port connection and the Ethernet access port does not have a physical link in the NFM-P	End node (source or destination node) has LAG to LAG ring port and Ethernet as access port	NFM-P prompts you to enter the peer MAC address
	End node (source or destination node) has LAG to Ethernet ring port Ethernet as access port	NFM-P prompts you to enter the local MAC address
	End node (source or destination node) has Ethernet to Ethernet ring port and Ethernet as access port	NFM-P prompts you to enter the local MAC address
Ethernet access ports have physical link in the NFM-P		NFM-P automatically calculates the MAC address. NFM-P automatically calculates the unicast MAC address of neighboring node, which is not part of service, and populates the MAC address also in the ring nodes.
VLL-VLAN heterogeneous ring configuration		You need to enter the MAC address as NFM-P does not calculate the MAC address for heterogeneous configurations.

15.12.4 Service-in-service

NFM-P supports the association of microwave backhaul services with a service tunnel. See “Service tunnels” chapter in the *NSP NFM-P Classic Management User Guide* for more information about associating a service with a service tunnel.

NFM-P supports autodiscovery for service-in-service associations created with the Wavence. Service-in-service refers to a transport service that carries services for network routers. Autodiscovery allows NFM-P to automatically associate a transport service with a service tunnel when a physical link is created between the Wavence and a non-Wavence NE. Service faults generated on either of the associated services become cross-correlated in the NFM-P.

Note: Service-in-service autodiscovery does not overwrite a service that is already associated with a service tunnel. However, users can manually overwrite an automatic association with another service. Only one service can be associated with a service tunnel.

Note: If the physical link between the Wavence and the network router is removed, the NFM-P automatically disassociates the service from the service tunnel.

15.12.5 Service state

NFM-P calculates the service state under the following conditions:

- All of the service objects are deployed
- Service is connected
- Service is topologically correct

Table 15-3, “Operational state” (p. 213) lists the operational state of microwave backhaul services.

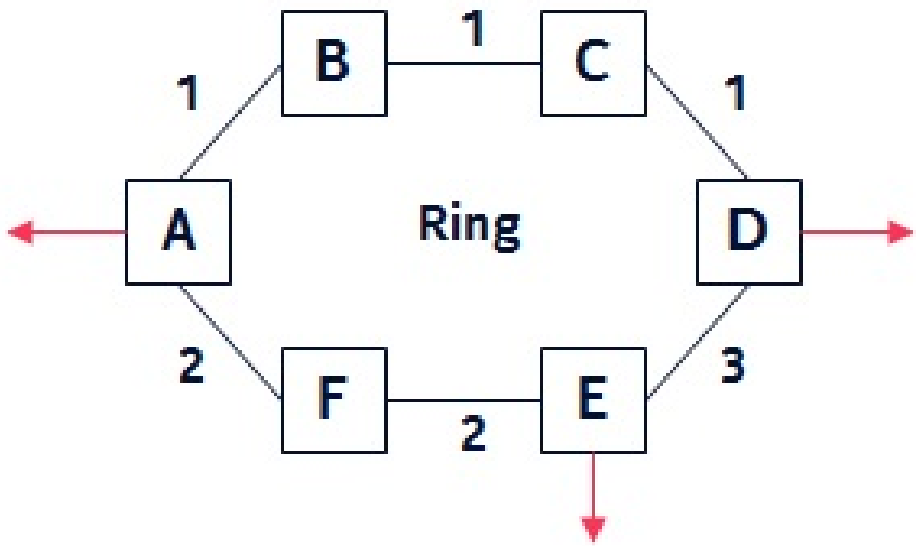
Table 15-3 Operational state

Scenarios	Operational state
No microwave backhaul service is deployed on the Wavence device.	Unknown
One or more microwave backhaul services are not deployed on the Wavence device.	Unknown
Services include no rings where all of the adjacency port states are up.	Up
Services include no rings where one or more adjacency port state is down.	Down
Services include one or more rings. See “Operational state of services that include one or more rings” (p. 214).	

Operational state of services that include one or more rings

The operational state is down when the non-ring adjacencies are down. In Figure 15-1, “Multiple segments on a single ring” (p. 214), if [A, B] and [C, D] go down, the ring is still operational as only one segment is affected. If [A, B] and [F, E] go down, the ring is down as multiple segments are affected and a ring termination site is no longer reachable.

Figure 15-1 Multiple segments on a single ring



Protection types and Wavence service status

In-service protected Radio links are represented as green links on the Physical topology map; standby Radio links are shown as blue links. The status of a Wavence service, spanning over any protected link, does not depend on the status of the link. The status of the service depends on the Radio direction operative status. See the following table for more information about the service status.

Table 15-4 Wavence service status

Protection Type	Main switching criteria / command	Spare switching criteria / command	Main status	Spare status	Radio Direction Operative Status[1]
EPS	Auto (Equipment Failure)	None	Standby	Active	Up
	None	Auto (Equipment Failure)	Active	Standby	Up
	Auto (Equipment Failure)	Auto (Equipment Failure)	Active/Standby	Standby/Active	Down
	Forced Switch	None	Standby	Active	Up
	Forced Switch	Auto (Equipment Failure)	Standby	Active	Down
	None	Lockout	Active	Standby	Up
	Auto (Equipment Failure)	Lockout	Active	Standby	Down
	Manual Switch	None	Standby	Active	Up
	None	Manual Switch	Active	Standby	Up
TPS	Auto (Equipment Failure)	None	Standby	Active	Up
	None	Auto (Equipment Failure)	Active	Standby	Up
	Auto (Equipment Failure)	Auto (Equipment Failure)	Active/Standby	Standby/Active	Down
	Forced Switch	None	Standby	Active	Up
	Forced Switch	Auto (Equipment Failure)	Standby	Active	Down
	None	Lockout	Active	Standby	Up
	Auto (Equipment Failure)	Lockout	Active	Standby	Down
	Manual Switch	None	Standby	Active	Up
	None	Manual Switch	Active	Standby	Up

Table 15-4 Wavence service status (continued)

Protection Type	Main switching criteria / command	Spare switching criteria / command	Main status	Spare status	Radio Direction Operative Status[1]
RPS	Auto (Signal Fail/HBER)	Auto (EW)	Standby	Active	Up
	Auto (Signal Fail)	Auto (HBER)	Standby	Active	Errors
	Auto (Signal Fail)	Auto (Signal Fail)	Active/Standby	Standby/Active	Down
	None	Auto (Signal Fail/HBER/EW)	Active	Standby	Up
	Auto (EW)	Auto (Signal Fail/HBER)	Active	Standby	Up
	Auto (HBER)	Auto (Signal Fail)	Active	Standby	Errors
	Auto (EW)	Auto (EW)	Active/Standby	Standby/Active	Up
	Auto (HBER)	Auto (HBER)	Active/Standby	Standby/Active	Errors
	Forced Switch	None	Standby	Active	Up
	Forced Switch	Auto (Signal Fail/HBER/EW)	Standby	Active	Down
	None	Lockout	Active	Standby	Up
	Auto (Signal Fail/HBER/EW)	Lockout	Active	Standby	Down
	Manual Switch	None	Standby	Active	Up
	None	Manual Switch	Active	Standby	Up

Notes:

1. If the Radio direction operative status is Up, the services are not affected. If the Radio direction operative status is down, the services are affected. The traffic status is Rx operative Up, if the status is Up for all the protection types (EPS and RPS). The traffic status is Tx operative Up, if the status is Up for all the protection types (EPS and TPS).

15.13 Microwave backhaul service management— considerations/ limitations

15.13.1 Wavence-specific service provisioning considerations/limitations

Table 15-5 Microwave backhaul service management — considerations/limitations

Functions	Limitations
Path search	Path search does not work beyond the Wavence realm (that is, IP/MPLS region). Path search does not work when you configure a single site service. Path search through a ring assigns a random radio ring instance if multiple options are available. If you want to use a specific ring instance, it must be done manually. It is the responsibility of the user to check and not to exceed the bandwidth provided by any interface (radio/Ethernet/LAG) involved in the subsequent creation of VLL services.
Ring with L1 radio LAG on CAHD boards	Cross-board CAHD LAG is not supported as a radio ring component TDM cross-connections are not supported. You cannot configure a cross-connection between an ERPS instance with a CAHD L1 LAG as a ring port and any other supported port. EFM OAM or LOC can only be configured as an ERPS switching criteria if the topology includes an optical user EAC port as a ring port. The switching criteria are only active on that EAC port's ring direction.
Ring with L1 radio LAG on electrical interfaces of EAS and EASv2	NFM-P accepts an L1 radio LAG that has radio interfaces configured either as static or adaptive modulation, as a ring port. NFM-P accepts only an active L1 radio LAG as a ring port . NFM-P does not accept an L1 radio LAG as a ring port when MPT-HC, MPT-HLv1, MPT-HLS, MPT-HLC, and MPT-HQAM radio interfaces are provisioned on the same EAS and EASv2 peripheral. NFM-P does not accept an L1 radio LAG as a ring port when electrical user Ethernet interfaces are enabled on the same EAS and EASv2 peripheral. NFM-P does not accept an L1 radio LAG as a ring port when optical user Ethernet interfaces are enabled on the same EAS and EASv2 peripheral. NFM-P does not accept an L1 radio LAG as a ring port when optical user Ethernet interfaces that have SFP provisioned are disabled on the same EAS and EASv2 peripheral. NFM-P does not accept an L1 radio LAG as a ring port when the L1 radio LAG is segregated with: • another L1 radio LAG • an Ethernet interface belonging to the same EAS and EASv2 peripheral • an Ethernet interface belonging to an EAS or EASv2 peripheral provisioned on the same back panel row
Support for MPTs in the same LAG	NFM-P does not support a mix of MPTs (MPT-HL and MPT-HQAM) in the same LAG on anEASv1 card.
EPS protection	NFM-P supports EPS protection on UBT-S/S2 node configured on the EAC card and UBT-T node configured on the Core-EVO and EAC cards.
GUI label in Network Policy window	"Network Policy type for 7705" label is displayed for all node types including Wavence.
ECFM configuration	Wavence ECFM configuration supports L2 Backhaul VLAN service with UBT-SA nodes used as a pass thru node. However, once the UBT-SA nodes are unmanaged and re-managed, the Connect Service operation must be performed to discover the nodes. See 15.1.7 "Connect service" (p. 191).

15.14 Microwave backhaul service creation using NSP Intent-Based Service Management

15.14.1 Intent-Based Service Management

You can use the NSP intent manager and service management functions to create L2 microwave backhaul services for Wavence equipment. Creation and discovery of the following service types is supported:

- VLAN
- VLL
- Composite

The NSP automates service creation through specialized workflows, which must be installed and configured before they can be triggered. This section describes the high-level steps required to install the Wavence backhaul service intent and workflow files, create a service template, and create a service. For more information about using the NSP, see the *NSP Network Automation Guide.*

Before using intent-based service management, ensure the following have been performed:

- the physical links are configured (except for single-site service)
- Ethernet rings are configured, if you are creating a service that includes one or more rings
- the Wavence backhaul service intent package was downloaded from the Nokia Support Portal
- in the NFM-P, the administrator user account has the OSS Management role configured in its Scope of Command

Before starting this process, it will be useful to have the *NSP Network Automation Guide* documentation open or easily available.

Note: Deploying a VLL service with a ring containing a port used for cross-connection creates a service that does not include the node with the cross-connect port. Ensure that ports are not involved in cross-connection before creating a VLL service using the NSP.

15.14.2 Stages

1

In Network Intents, import the wavencebackhaul intent file. See the *NSP Network Automation Guide* for information about installing intent files.

2

In Workflows, import the following workflows included with the Wavence backhaul service intent package:

- Separate_Topology
- Wavence_Backhaul_Service_Connect
- Wavence_Backhaul_Service_Deploy

After the workflows are imported, ensure the Service Life Cycle State is set to Published. See the *NSP Network Automation Guide* for information about importing workflows and setting life cycle states.

3

In Workflows, create a kafka trigger for the Wavence_Backhaul_Service_Connect workflow for when a service is created, using the following parameter values:

Parameter	Value
Kafka Topic	nsp-db-fm
Trigger Name	create_alarm
Trigger Rule	$[?(@.alarmName == ‘connectNotAttempt-edOnService’ || @.alarmName == ‘serviceModified’)]
Kafka Event	CREATE

See the *NSP Network Automation Guide* for information about managing kafka triggers.

4

Create a second kafka trigger for the same workflow for when a service is updated, with the following values:

Parameter	Value
Kafka Topic	nsp-db-fm
Trigger Name	update_alarm
Trigger Rule	$[?(@.alarmName == ‘connectNotAttempt-edOnService’ || @.alarmName == ‘serviceModified’)]
Kafka Event	UPDATE

5

In the NSP application, import the wavencebackhaul intent you installed using the intent manager previously. See the *NSP Network Automation Guide* for information about importing intents.

6

Create a service template, then configure the Service Intent Type to use the wavencebackhaul intent and add the Wavence_Backhaul_Service_Deploy workflow as an assigned workflow. See the *NSP Network Automation Guide* for information about creating service templates.

7

In the Inventory tab, configure Customers as required. See the *NSP Network Automation Guide* for information about customer configuration.

8

In the Services tab, create a service using the Wavence_Backhaul service template. Configure the service as required according to your network. See the *NSP Network Automation Guide* for information about service configuration.

Monitoring created services

9

After creating the service, the Deploy and Connect workflows are automatically launched as required to configure the specified Wavence devices.

You can monitor the progress of the workflows using Workflows, the status of the devices using Device Management, the status of the newly-created service and watch for alarms or faults using the Network Map and Health dashboard. Additionally, Wavence backhaul service status can be monitored using the Network Map and Health dashboard; see 2.16 “To display Wavence backhaul service status information on the NSP Network Map and Health dashboard” (p. 82).

Separating a service

10

After creating a service, you can separate the service using a workflow. Select the service you need to separate, and perform the Execute Workflow action, then choose the Separate_Topology workflow. See the *NSP Network Automation Guide* for more information about executing workflows on a service.

16 Wavence composite service

16.1 Composite service

16.1.1 General information

The following pathway describes the sequence of high-level tasks required to configure a composite service with a microwave backhaul service on a Wavence, and a VPLS on a 7210 SAS or 7750 SR.

Note: If the 7750 SR is configured as the RPL owner in the ERP service, the corresponding RPL link is down.

If one of the backhaul adjacencies on the microwave backhaul service is down, the status of the microwave backhaul service is displayed as down in the service topology map, even though there is an alternate path.

16.1.2 Pathway to configure a composite service

1

Configure an Ethernet Radio ring on a Wavence. See 14.3 “To create an Ethernet radio ring on a Wavence” (p. 184).

2

Configure Ethernet CFM MD, MEG, NE MEG, and MEP. See “To configure an Ethernet CFM MD policy and subordinate objects” in the *NSP NFM-P Classic Management User Guide*.

3

Configure an Ethernet G.8032 ring on the 7210 SAS or the 7750 SR. See “To create an Ethernet G.8032 ring” in the *NSP NFM-P Classic Management User Guide*.

4

Configure a VPLS on 7210 SAS or 7750 SR. See “To create a VPLS” in the in the *NSP NFM-P Classic Management User Guide*.

5

Configure a microwave backhaul service on a Wavence. See Chapter 15, “Wavence microwave backhaul service management”.

6

Configure a composite service between the services created in Stage 4 and Stage 5. See 16.2 “To configure a composite service” (p. 222).

16.2 To configure a composite service

16.2.1 Steps

1

Perform one of the following to open the Composite Service (Create) form:

a. Choose Create→Service→Composite Service from the NFM-P main menu. The Composite Service (Create) form opens.

b. Perform the following:

1. Choose Manage→Service→Composite Services from the NFM-P main menu. The Manage Composite Services form opens.
2. Click Create. The Composite Service (Create) form opens.

2

Configure the required general parameters.

The Composite ID parameter is configurable only if the Auto-Assign ID parameter is disabled.

3

Click Apply.

4

Save the changes and close the forms.

5

Choose Manage→Service→Composite Services from the NFM-P main menu. The Manage Composite Services form opens.

6

Select the composite service and click Properties. The Composite Service (Edit) form opens.

7

In the service navigation tree, right-click on the Services icon and choose Add Services. The Add Services form opens.

Note: You can also configure a service for inclusion in the composite service by right-clicking on the Services icon and choosing Create *Service Type*.

8

Select the VPLS and microwave backhaul services and click OK. The site and adjacencies appear on the navigation tree.

Note: The Composite Service panel parameters are updated on the Microwave Backhaul Service (Edit) form of the selected microwave backhaul services.

9

Right-click on the Connector object on the navigation tree and choose Connect Scp connector. The Scp connector (Create) form opens.

10

Select the microwave backhaul service and the VPLS service in the Service A and B panels and the sites involved in the Site A and B panels.

11

Click on the Service Connection Point tab and select the ports in the Service Connection Point A and Service Connection Point B panels.

12

Perform Step 9 to Step 11 for the remaining connectors.

13

Save the changes and close the forms.

END OF STEPS

17 Wavence microwave backhaul L3 SNMP management

17.1 L3 network interface management

17.1.1 Prerequisites

Before configuring microwave backhaul L3 services, ensure that the NE mediation is configured with the SSH2 communication protocol for L3 VPN Wavence devices.

17.1.2 L3 global routing

The NFM-P supports the configuration of an L3 VLAN with IP/MPLS traffic for a specific Wavence device. The VLAN where the L3 global routing is enabled is unique in the network, that is, all of the IP/MPLS traffic is carried over the same VLAN.

NFM-P manages the L3 VLAN as a backhaul service; for example, discovery, creation, deletion, inventory, and fault reporting are also applicable for L3 VLAN.

The L3 VLAN ID cannot be used for L2 backhaul services.

17.1.3 IP network interface

The NFM-P supports the configuration and discovery of IP network interfaces assigned to Ethernet and radio ports of CorEvo, EASv2, CAHD, EAC, 1+0 radio interface, 1+1 radio interface, L1 LAG radio interface, and Ethernet LAGxcards. You can modify an already configured L3 network interface that is associated with a routing instance.

17.1.4 System interface

The system interface is the default network interface that is configured on the NE.

The user has to assign the address for the interface that will be used for other functionality, such as Static LSP and Static label maps.

17.1.5 Static route

The NFM-P supports the manual configuration of static routes for Wavence devices. The static route configuration requires the system IP address of the node within the network and the next-hop interface IP address through which it is connected. Each node will have the static route information of all the nodes.

17.1.6 MPLS initialization and label distribution

The NFM-P supports the manual initialization of the MPLS (Multi-Protocol Label Switching) at the Wavence device by configuring the following:

- start segment labels (32 to 1023) - the starting label range used to identify the prefix segment

- end segment labels (18432 to 524287) - the ending label range used to identify the prefix segment
- node SID - the value uniquely identifying the Wavence device in the global network

NFM-P displays the MPLS objects as child objects of the routing instance in the network view of the navigation tree. The inventory list of the nodes where the MPLS protocol is initialized is supported at the network level. The MPLS label distribution is achieved by local configuration of the labels associated with each remote system. NFM-P displays the list of remote systems for every Wavence device having MPLS protocol enabled.

17.1.7 Static Label Map

MPLS static LSP feature enable the node to statically assign local labels to an IPv4 prefix. LSPs can be provisioned for these static labels by specifying the next-hop information that is required to forward the packets containing static label.

17.1.8 Static LSP

Wavence can be used to support L3 IPv4 data routing services using the capabilities of the MPLS networking using LSPs. L3 IPv4 data plane routing and static LSPs are required in Wavence to support static LSP. These enable the user to create and configure static IP routes by creating network interfaces. The MPLS static LSP feature enables the product to statically assign local labels to an IPv4 prefix. All the IPv4 Data Plane and MPLS (LSP and L3VPN) related configuration in the Wavence will be static configuration provisioned by the operator or user and by the NMS or Carrier SDN controller.

Swap and Pop operations can be created either using the static label maps from MPLS interface properties window or while configuring the static LSP paths.

17.1.9 Segment Routing Traffic Engineering LSP

Segment Routing Traffic Engineering (SR-TE) LSPs forward traffic along a network chain different than the one at the lowest cost, for the purposes of network optimization. BE SPF might not consider the convergences of several LSP via the same set of links, creating congestion. By the same token, some links might be under utilized since they are not involved in the SPF. Via the joint usage of BE and TE LSPs, a centralized SDN controller can optimize the network usage balancing flows across them.

For information about configuring SR-TE LSPs, see the *NSP Classic Management User Guide*. For considerations when using SR-TE with Wavence, see 17.33 “Wavence VPRN service — considerations/limitations” (p. 254).

17.1.10 SDP tunnel

The Service Distribution Point (SDP) is a logical representation of the transport tunnel that is used to deliver the service data to the egress PE. For Wavence NEs, the transport tunnel to be associated with the SDP is the static LSP able to reach the PE (or P node able to reach the PE). An SDP is locally unique within the NE and represented by an SDP ID. The same SDP ID can appear on other NEs. An SDP uses the system IP address to identify the far-end NE.

The SDP provides the binding between the service labels and the transport tunnel. To make a VPRN service to use an SDP for distribution, the service should be joined to the SDP using SDP binding, that is, spoke-SDP.

The operational and administrative states of the SDP control the state of the VPRN services bound to the SDP. The operational state of SDP is a result of the operational state of the underlying static LSP.

17.1.11 Black-hole routes

The black-hole feature configures a static route in the routing table (VRF), which drops all the traffic matching with this destination system IP address. A black-hole route can be created with the intended destination IP address whose next hop is 0.0.0.0, by default.

17.1.12 VPRN ping

The VPRN ping OAM diagnostic test determines the existence of the far-end egress point of the service. This allows testing of whether a specific destination can be reached. VPRN pings can be sent in-band or out-of-band. When a VPRN ping test packet is sent, a reply is generated if the targeted prefix is reachable over a VPRN SAP or VPRN spoke interface; otherwise the test packet is dropped in CPM. This also applies in the case of a routed VPLS interface. See 17.31 “To create and run a VPRN Ping test from a service manager form” (p. 252) and 17.32 “To create and run a VPRN Ping test on a SAP” (p. 253).

See the *NSP Classic Management User Guide* for information about configuring and using STM tests.

17.2 Pathway to configure L3 VPN transport setup

17.2.1 Stages

Perform the following stages to configure a microwave backhaul L3 service:

1

Initialize an L3 VLAN. See 17.4 “To initialize an L3 VLAN ID” (p. 229).

2

Configure a routing instance. See 17.5 “To configure a System and Network interface” (p. 230).

3

Perform manual initialization of the MPLS protocol. See 17.6 “To initialize the MPLS protocol” (p. 231).

4

Perform manual configuration of the remote system. See 17.7 “To configure an MPLS interface” (p. 231).

Configure OSPFv2 based L3 VPN

5

Configure an OSPFv2 Router ID. See 17.22 “To configure OSPFv2 Router ID” (p. 246).

6

Configure a dynamic LSP. See 17.23 “Pathway to configure OSPFv2” (p. 246).

7

Configure an IP/MPLS service tunnel. See 17.30 “To configure IP/MPLS Service Tunnel” (p. 251).

Configure Static L3 VPN

8

Configure a static route. See 17.8 “To configure a static route” (p. 232).

9

Configure a static LSP. See 17.9 “To configure a static LSP” (p. 233).

10

Configure an SDP tunnel. See 17.14 “To create an SDP Tunnel” (p. 237).

Note: On the Manage VLAN Groups form, you can automate static routing configuration (static routes and MPLS) using the Transport Setup button and dynamic routing configuration (MPLS and OSPF) using the Dynamic Transport Setup button. Also, the Enable MPLS interfaces must be selected to enable all MPLS interfaces on the nodes involved in VLAN group. The Transport Setup button automates the initialization of MPLS, and configuration of the remote system and static routes. The Dynamic Transport Setup button automates the initiation of MPLS, configuration of the remote system, initialization of OSPF, configuration of OSPF areas, instances, interfaces, and deletes static routes on the configuration, as this is the preferred option for dynamic routing configuration.

From the Transport Setup and Dynamic Transport Setup windows, you can manage incremental or decremental changes in the network. If an L3 node is added to the network, routes will be updated on all the nodes to reflect the addition of an L3 node. Similarly, if a node is deleted from the network, routes will be deleted relevant to the deleted node.

In case of conversion of the network configuration from linear to ring topology, transport setup is not supported due to limitation from the wavence node. In this scenario, dynamic transport setup option can be used for the required configuration. The routes are based on best available path.

The Dynamic Transport Reset (removes OSPF objects) and Transport Reset (removes MPLS objects) buttons in the Manage VLAN groups window can be used to remove one or more nodes from an L3 VPN. However this action does not delete the node from the VLAN group.

17.3 Pathway to configure a VPRN service using the Service Management view

17.3.1 Intent Manager view

You can use NSP Service Management and Intent Manager to automatically create a VPRN service and service objects using automated workflows and scripts. This section describes the prerequisite tasks that must be performed in the NFM-P. For more information about using NSP Service Management, see the *NSP Service Mangement Guide*.

17.3.2 Stages

1

Discover and manage Wavence nodes in the NFM-P, and configure VLAN IDs. See 17.4 “To initialize an L3 VLAN ID” (p. 228).

2

Configure system and network interfaces for the service. See 17.5 “To configure a System and Network interface” (p. 230).

3

Configure a VLAN group for the managed Wavence nodes, including transport and dynamic transport configuration. See 17.21 “To configure a VLAN group” (p. 245).

17.4 To initialize an L3 VLAN ID

17.4.1 Steps

Using Bulk Operation

1

Choose Tools and select Bulk Operations. The Bulk Operations form opens.

2

Click Create. The Create Bulk Change (New) form opens.

a. Type the VLAN ID name.

b. Expand the Admin State drop-down menu and select Enable.

c. Expand the Object Type drop-down menu, expand the MPR tree, and select System Settings.

d. Click Next and on the Specify the Filter window, click Next.

e. Expand Attribute, then General, and then IP Data Plane Settings.

f. Double-click on L3 VLAN ID and enter the VLAN ID to be created. Click Next.

Note: VLAN ID should be the same across all the L3VPN nodes configured in the specified network or cluster.

g. Change review window displays the configured attributes along with the VLAN value.

h. Select the View newly created bulk change check box and click Close.

The Bulk Change (Edit) form opens.

3

Select the VLAN attribute you created and click Batch Control tab.

4

Click Generate Batches to generate the first set of 20 VLAN IDs, and click Execute.

5

Double-click on the Batch ID row to view the Batch Items.

Configure individually

6

In the navigation tree equipment view, right-click on a Wavence device object in the equipment tree and choose Properties. The Network Element (Edit) form opens.

7

Click System Setting tab and configure the L3 VLAN ID under the IP Data Plane Settings.

8

Click OK to save and close the form.

END OF STEPS

17.5 To configure a System and Network interface

Note: By default, a system interface is created when the node is added. However, the user has to set the IP address.

17.5.1 Steps

1

In the navigation tree routing view, expand Network→Wavence→Routing Instance.

2

Right-click on the Routing Instance object and choose Create Interface. The Create Network Interface step form opens and the Define General Properties step appears.

3

Configure the required parameters and click Next. The Select Port form opens.

4

Select a specific port, click Finish to save and close the forms.

END OF STEPS

17.6 To initialize the MPLS protocol

17.6.1 Steps

1

In the navigation tree routing view, expand Network→Wavence→Routing Instance.

2

Right-click on the Routing Instance object and choose Properties. The Routing Instance (Edit) form opens.

3

Click on the Protocol tab and select the MPLS Enabled check-box.

4

Click OK to save your changes and close the form.

END OF STEPS

17.7 To configure an MPLS interface

17.7.1 Steps

1

In the navigation tree routing view, expand Network→Wavence→Routing Instance.

2

Right-click on the MPLS, and click Create Interface. The MPLS Interface (Create) form opens.

3

Configure the required parameters.

4

Click OK to save and close the form.

END OF STEPS

17.8 To configure a static route

17.8.1 Steps

1

Right-click on the Static Routes object on the navigation tree and choose Create Static Routes. The Static Route (Create) form opens.

2

Configure the required parameters.

Perform one of the following based on whether you need to create a next hop or black-hole static route:

a. To configure next hop:

- Configure the Destination IP address, then select Next Hop from the drop-down menu, and configure the next hop IP address. Click OK to save and close the form.
- Configure the System parameter as Local for local static routes, then configure the Next Hop IP parameter.

Note: You can configure IPv6 destination IP address only when the IPv6 Allowed check-box is enabled on the associated L3 access interface, on the General tab of the VPRN L3 Access Interface (Edit) form.

Note: If an IPv6 address is configured under destination IP address parameter, you can either provide an IPv6 IP address without selecting the L3 access interface or select the created L3 access interface to provide link local address under the Next Hop IP address.

b. To configure black-hole static route, see 17.15 “To create a black-hole route” (p. 238) .

3

Configure the remaining parameters.

4

Save your changes.

The Remote System or Next-Hop objects are displayed on the navigation tree below the Static Routes object for each site.

5

Close the forms.

END OF STEPS

17.9 To configure a static LSP

17.9.1 Overview

A static LSP is always unidirectional. Static LSPs are configured on the all the sites to determine PUSH, SWAP and POP. SWAP and POP operations are defined once we set the PUSH configuration. On the network, each node is explicitly defined as a Swap or Pop NE. These operations are defined at the MPLS interface level.

17.9.2 Steps

1

Choose Manage→MPLS→Static LSP. The Manage Static LSP window opens.

2

Click Create. The Static LSP (Create) form opens.

3

Click the General tab.

Configure the required parameters.

4

Click the Static Hops tab and configure the following parameters:

- Click Create. The Static Hop (Create) form opens.
- Double-click on the Site ID. The Static Hop (Create) form with additional parameters opens.
- Type the Egress Label that was calculated in the General tab and set the Next Hop IP address.

5

Repeat Step 2 to Step 4 to configure the number of static hops required.

Note: Swap and Pop operations can also be created using the static label maps from the MPLS interface properties window. See 17.10 “To create static hops from an MPLS interface properties window” (p. 234) for the procedure to create static hops from MPLS interface properties window.

6

Click OK to save the changes and close the forms.

END OF STEPS

17.10 To create static hops from an MPLS interface properties window

Note: SWAP and POP operations are defined once the PUSH configuration is set. On the network, each node is explicitly defined as a Swap or Pop NE.

17.10.1 Steps

1

In the navigation tree routing view, expand Network→Wavence→Routing Instance→MPLS.

2

Right-click on the Interface INTF and choose Properties. The MPLS Interface (Edit) form opens.

3

Click Static Label Maps and click Create. The Static Label Maps (Create) form opens.

4

Based on the Label Action selected, set the required parameters.

5

Click OK to save and close the forms.

END OF STEPS

17.11 To configure static routes on a VPRN site

17.11.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Choose a VPRN service and click Properties. The VPRN Service (Edit) form opens.

3

On the service navigation tree, expand the Sites icon, right-click on a routing instance and choose Properties. The VPRN Site (Edit) form opens.

4

Click on the Routing tab, then on the Static Routes tab.

5

Define a static route that the PE VRF is to exchange with the CE:

1. Click Create. The Static Route (Create) form opens.
2. Configure the required general parameters.
3. Configure the parameters in the Destination panel.

   The IP Address parameter is configurable when the Type parameter is set to an option other than Black Hole.
4. Select an interface for the static route in the Destination panel.
5. Configure the parameters in the Other panel.
6. Save the changes and close the form.

6

Save the changes and close the forms.

END OF STEPS

17.12 To create and configure a Two-Way Active Measurement Protocol Light reflector

17.12.1 Overview

You can enable or disable Two-Way Active Measurement Protocol (TWAMP) on a server, and view session and connection statistics. A TWAMP Light test needs to be pointed at a reflector on the correct UDP port in order to execute properly and generate valid results. A TWAMP Light reflector can be configured on a base routing instance or on a site. There can only be one reflector on a particular base routing instance or a site.

17.12.2 Steps

1

Choose Manage_Service_Services from the NFM-P main menu. The Manage Services form opens.

2

Choose Service (Service Management) Microwave Backhaul Service (MPR) from the object drop-down menu and click Search.

3

Choose a microwave backhaul service and select the Site for which you want to configure the reflector. The Microwave Backhaul Service (Edit) form opens.

4

Click the OAM tab, then the TWAMP tab.

5

Click Add. The TWAMP Light Reflector (Create) form opens.

6

Configure the required parameters.

Note: To make changes to TWAMP server parameters, or to delete a TWAMP reflector, the Administrative Status parameter must be set to Disabled.

7

Click Create in the Reflector Prefixes panel. The Prefix TWAMP Light Reflector (Create) form opens.

8

Configure the required parameters.

Prefixes are added to the reflector to determine which Sessions can target the reflector. You should specify the prefix address and length if you require masking. Only those TWAMP Light test sessions with a Source IP matching a prefix will be valid.

9

Click on the Statistics tab.

10

Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.

11

Click Statistics Policies and select Statistics Policy from the menu. The Statistics Policy form opens, with the General tab displayed.

12

Configure the required parameters.

13

Save the changes and close the forms.

14

To view TWAMP statistics on a server:

1. Perform Step 1 to Step 4 of this procedure.
2. Select the required record from the table and click Properties.
3. The TWAMP Light Reflector (Edit) form opens, with the General tab displayed.
4. Click on the Statistics tab.
5. Select either Past 4 Hour(s) or No Filter, as required, from the filter selector.
6. Click Collect or Collect All. The system compiles the statistics and displays the available records in the table.
7. Select the required record from the table and click Properties. The Statistics Record is displayed.
8. Save your changes and close the forms.

END OF STEPS

17.13 To view all the configured TWAMP Light reflectors

17.13.1 Steps

1

Click Tools→Service Test Manager (STM) on the NFM-P main menu. The Service Test Manager (STM) form opens.

2

Choose TWAMP Light Reflector (Assurance) from the drop-down menu and click Search.

The list of all the configured TWAMP reflectors are displayed.

END OF STEPS

17.14 To create an SDP Tunnel

17.14.1 Steps

1

Choose Manage→Service Tunnels from the NFM-P main menu.. The Manage Service Tunnel form opens.

2

Click Create→IP/MPLS Service Tunnel (SDP). The IP/MPLS Service Tunnel (SDP) wizard opens.

3

Configure the required parameters.

4

Click OK to save and close the form.

End of steps

17.15 To create a black-hole route

17.15.1 Steps

1

In the navigation tree routing view, expand Network→Wavence→Routing Instance→Static Routes.

2

Right-click on Static Routes and Click Create Static Route. Static Route (Create) form opens.

3

Enter the destination system IP address in the Destination field. The Prefix Length must always be set to 32.

4

Choose Black Hole from the Type drop-down menu.

5

The IP Address field, which is the next hop IP address, must always be set to 0.0.0.0.

6

Click OK to save and close the form.

End of steps

17.16 To configure a SAP access ingress policy

17.16.1 Steps

1

Choose Policies→QoS→SROS QoS→Access Ingress→SAP Access Ingress from the NFM-P main menu. The SAP Access Ingress Policies form opens.

2

Click Create or choose a policy and click Properties. The SAP Access Ingress Policy (Create|Edit) form opens.

3

Configure the required general parameters.

Note: For some of the general parameters, additional fields will be displayed when certain selections are made. For example, when setting the IP Criteria Type and IPv6 Criteria Type to VXLAN-VNI and then clicking Apply, the Match Criteria field is displayed, and shows a value of None.

Note: NEs that support next-generation CLI use the policy name as the key identifier for internal system reference. For policies on these NEs, you must configure a policy name (typically the service name or a numerical string). Policy IDs are also supported. You must configure a numerical range on the NE for auto-assigned policy IDs; see 17.19 “To configure an Auto-ID range for policies” (p. 242).

Note: For some of the following steps, the tabs are not available until after the policy is created. Click Apply if required to create the policy and make all tabs available.

4

Map ingress dot1p bits.

1. Click on the Dot1p tab.
2. Click Create or choose a Dot1p entry and click Properties. The Dot1p (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

5

Map ingress DSCP bits.

1. Click on the DSCP tab.
2. Click Create or choose a DSCP entry and click Properties. The DSCP (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

6

Click OK to save the policy and close the form, or click Apply to save the policy. To distribute the SAP access ingress policy, see the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide*.

END OF STEPS

17.17 To configure a SAP access egress policy

17.17.1 Steps

1

Choose Policies→QoS→SROS QoS→Access Egress→SAP Access Egress from the NFM-P main menu. The SAP Access Egress Policies form opens.

2

Click Create, or choose a policy in the list and click Properties. The SAP Access Egress Policy (Create|Edit) form opens.

3

Configure the required general parameters.

Note: For some of the following steps, the tabs are not available until after the policy is created. Click Apply if required to create the policy and make all tabs available.

Note: NEs that support next-generation CLI use the policy name as the key identifier for internal system reference. For policies on these NEs, you must configure a policy name (typically the service name or a numerical string). Policy IDs are also supported. You must configure a numerical range on the NE for auto-assigned policy IDs; see 17.19 “To configure an Auto-ID range for policies” (p. 242).

4

Configure forwarding classes. You can create up to eight forwarding classes.

1. Click on the Forwarding Classes tab.
2. Click Create, or choose a forwarding class and click Properties. The Forwarding Class (Create|Edit) form opens.
3. Configure the Forwarding Class parameter.
4. Configure the required parameters in the Dot1p panel.
5. Save your changes and close the form.

5

Click OK to save the policy and close the form, or click Apply to save the policy. To distribute the SAP access egress policy, see the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide*.

End of steps

17.18 To configure a QoS network policy

17.18.1 Steps

1

Choose Policies→QoS→SROS QoS→Network→Network from the NFM-P main menu. The Network Policies form opens.

2

Click Create, or choose a policy and click Properties. The Network Policy (Create|Edit) form opens.

3

Configure the required general parameters.

Note: To view or configure the NE policy name parameter, the Show Display Name of Form system preference must be enabled. See the section on configuring NFM-P system preferences in the *NSP System Administrator Guide*.

Note: NEs that support next-generation CLI use the policy name as the key identifier for internal system reference. For policies on these NEs, you must configure a policy name (typically the service name or a numerical string). Policy IDs are also supported. You must configure a numerical range on the NE for auto-assigned policy IDs; see 17.19 “To configure an Auto-ID range for policies” (p. 242).

4

Configure the parameters in the Ingress panel and Egress panel.

5

Configure egress forwarding classes.

1. Click on the Egress Forwarding Classes tab. Eight default FCs are displayed.
2. Click Create, or choose an FC and click Properties. The Egress Forwarding Class (Create|Edit) form opens.
3. Configure the required parameters.

   Select the Use check box to configure the Queue ID and Policer ID parameters. A valid entry for the Queue ID parameter must be specified in the queue group template policy.
4. Save your changes and close the form.

6

Configure ingress forwarding classes.

1. Click on the Ingress Forwarding Classes tab. Eight default FCs are displayed.

2. Click Create, or choose an FC and click Properties. The Ingress Forwarding Class (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

7

To configure the mapping of ingress or egress traffic markings to FCs and profiles, click on the appropriate tab. Mapping is optional and is based on combinations of customer QoS marking for LSP EXP, DSCP, Dot1p, and Precedence. Table 17-1, “Network policy traffic-mapping options” (p. 241) describes the options.

Table 17-1 Network policy traffic-mapping options

Tab	Mapping
Ingress LSP EXP Bits	LSP EXP bits of the ingress traffic to an FC and profile
Ingress DSCP	DSCP of the ingress traffic to an FC and profile
Ingress Dot1p	Dot1p tag of the ingress traffic to an FC and profile
Egress DSCP	DSCP of the egress traffic to an FC and profile
Egress Precedence	Precedence value of the egress traffic to an FC and profile

Perform the following steps for each mapping that you want to configure.

1. Click on the required tab.
2. Click Create, or choose an entry and click Properties. A (Create|Edit) form opens.
3. Configure the required parameters.
4. Save your changes and close the form.

8

Click OK to save the policy and close the form, or click Apply to save the policy. To distribute the QoS network policy, see the “Policies overview” chapter in the *NSP NFM-P Classic Management User Guide*.

END OF STEPS

17.19 To configure an Auto-ID range for policies

17.19.1 Before you begin

NEs that support next-generation CLI use the policy name as the key for internal system reference. For these NEs, a policy ID is also configurable. If a policy ID is not configured, the system auto-assigns a numerical policy ID. When the policy is distributed to an NE, the auto-assigned ID is generated from a specified range of values.

Perform this procedure to configure a numerical range on the NE for auto-assigned policy IDs.

Before you change an existing range configuration on an NE, you must delete any policies on the NE that have IDs within the existing range.

If you configure a range that comprises a policy ID that already exists on the NE, deployment fails.

17.19.2 Steps

1

On the equipment tree, right-click on a supporting NE and choose Properties. The Network Element (Edit) form opens.

2

Click on the Globals tab, and then the Policies tab.

3

For each policy type, configure the start and end values for the ID range.

4

Save your changes and close the form.

END OF STEPS

17.20 To configure a VPRN service

17.20.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Manage Services form opens.

2

Click Create→VPRN. The VPRN Service (Create) form opens.

3

Configure the parameters in the Customer panel.

4

On the navigation tree, right-click on the Sites object and choose Create VPRN Site. The Select Network Elements form opens.

5

Choose the required Wavence sites, and click OK. The site objects are displayed on the navigation tree.

6

Perform the following to configure the L3 access interfaces:

1. Right-click on the L3 Access Interfaces object on the navigation tree and choose Create L3 Access Interface. The VPRN L3 Access Interface (Create) form opens.
2. Configure the parameters in the General tab.
3. Click on the Port tab and select the terminating port.
4. Configure the VLAN ID parameter.
5. Click on the Addresses tab and click Create. The IP Address (Create) form opens.
6. Configure the required parameters and click OK.
   - If it is required to provide IPv4 address, you can provide the IPv4 IP address on the L3 access interface.
   - If it is required to provide IPv6 address, enable the Allow IPv6 check-box. With IPv6 allowed check-box enabled, you can either specify linked local address manually or Use Self-Generated check-box for the system to generate an IP linked local address.

     It is required by the user to provide a valid IPv6 IP address and prefix length under addresses tab and routing tab of VPRN service to avoid any deployment errors.

     There is no MIB mapped to show "Use Self-Generated" in the NFM-P GUI from the Wavence NE. Once you have set the "administrative" Link Local address by VRtrIfAdminLinkLocalAddr, you cannot go back to a self-assigned IP linked local address.
7. Save your changes.
8. Repeat sub-steps 1 to 7 to add multiple L3 access Interfaces, if required.

Result: The SAP objects are displayed on the navigation tree below the VPRN L3 Access Interfaces object for each site.

7

Configure a static route on all the SAP objects.

Two types of VPRN services are supported on SAP nodes. Full mesh, see 17.11 “To configure static routes on a VPRN site” (p. 234) and Hub and Spoke method, see 17.15 “To create a black-hole route” (p. 238).

Result: The Remote System or Next Hop objects are displayed on the navigation tree below the Static Routes object for each site.

8

Click Apply to deploy all of the L3 SAPs and routes on the Wavence devices.

9

Close the forms.

END OF STEPS

17.21 To configure a VLAN group

17.21.1 Steps

1

Choose Manage→VLAN Group. The Manage VLAN Group form opens.

2

Click Create. VLAN Group, (New Instance) (Create) form opens.

3

Configure the required parameters.

4

Select Wavence from the Node Type drop-down menu.

5

Configure the VLAN ID parameter.

Note: The VLAN ID must be the same as the VLAN ID that is used while initializing the L3 VLAN. See 17.4 “To initialize an L3 VLAN ID” (p. 229).

6

Click Apply to save the changes.

7

Click on the Group Members tab and click Create. Select the NEs that you want to be part of the VLAN group and click OK.

8

Click OK to save the changes and close the form.

9

In the Manage VLAN Groups form, select the VLAN group and click Transport Setup. Click Yes. The NFM-P automatically performs the following tasks on NEs in the VLAN group:

- creates static routes
- initializes the MPLS protocol
- configures MPLS interfaces

10

Click Dynamic Transport Setup, and then click Yes. The NFM-P automatically performs the following tasks on NEs in the VLAN group:

- initializes the MPLS protocol
- configures MPLS interfaces
- enables OSPF protocol
- creates an OSPF instance with area 0.0.0.0
- creates OSPF interfaces corresponding to MPLS interfaces on all nodes in the VLAN group
- configures all created interfaces and instances to be administratively up
- discovers dynamic LSPs after they are created on the nodes as a result of OSPF configuration

END OF STEPS

17.22 To configure OSPFv2 Router ID

17.22.1 Steps

1

In the navigation tree equipment view, right-click on a Wavence device object in the equipment tree and choose Properties. The Network Element (Edit) form opens.

2

Click System Settings tab.

3

Configure the Base Virtual Router IP Address parameter under the IP Data Plane Settings panel.

Note: By default, the OSPFv2 router IP address is the system interface IP address.

4

Click OK to save the changes and close the form.

END OF STEPS

17.23 Pathway to configure OSPFv2

17.23.1 Stages

Note: Segment Routing cannot be enabled if Static LSP or Label Maps are present on node and vice-versa.

1

Enable OSPF on a routing instance; see 17.24 “To configure OSPFv2 instance on a Routing instance” (p. 247) .

2

Create at least one OSPFv2; see 17.27 “To create an OSPF area” (p. 249) .

3

Assign Layer 3 interfaces to the routers in the OSPFv2 area; see 17.28 “To add a Layer 3 interface to an OSPF router” (p. 249) .

4

Configure LFA and remote LFA as required; see 17.26 “To enable LFA and remote LFA on an OSPF instance” (p. 248).

5

Configure OSPF segment routing as required; see 17.29 “To configure OSPF segment routing and discover dynamic LSPs” (p. 250).

17.24 To configure OSPFv2 instance on a Routing instance

17.24.1 Steps

1

In the navigation tree Routing view, expand Network→*NE*→Routing Instance→OSPFv2 Instance.

2

Right-click OSPFv2→Create OSPFv2 Instance. The OSPF Site, OSPFv2 Instance (Create) form opens.

Note: Wavence supports creation of only one OSPFv2 instance.

3

Click Apply. OSPF Site, OSPFv2 Instance (Edit) form opens with all the mandatory parameters.

An OSPFv2 instance is created with a default area 0.0.0.0.

Note: By default OSPFv2 is enabled and displayed on the NE.

4

Click OK to close the form.

END OF STEPS

17.25 Pathway to configure OSPFv3

17.25.1 Prerequisites

OSPFv3 is supported on the MSS-4/8, MSS-E/HE/XE, and UBT-NIM using Wavence Release 23 or later. OSPFv3 is configured using the WebCT interface for each node, and OSPFv3 configuration parameters are read-only in the NFM-P.

17.25.2 Steps

1

Open the WebCT interface for the Wavence node, and perform the following tasks in Networking Configuration:

- Enable TMN/PPP
- Configure the OSPFv3 router ID
- Configure OSPFv3 areas and area IDs as required
- Configure OSPFv3 area stub flags

See the Wavence documentation for information about configuring OSPFv3.

2

In the navigation tree Routing view of the NFM-P, expand Network→*NE* and click on Polling→OSPFv3 Details to confirm the configuration.

END OF STEPS

17.26 To enable LFA and remote LFA on an OSPF instance

17.26.1 Steps

1

In the navigation tree Routing view, expand Network→*NE*→Routing Instance→OSPFv2 Instance.

2

Right-click on the OSPFv2 instance and select Properties. The OSPFv2 Instance (Edit) form opens.

3

In the LFA tab, enable Loop-free Alternate and configure the parameters as required.

Remote loop-free alternate uses segment routing by default. To configure segment routing, see 17.29 “To configure OSPF segment routing and discover dynamic LSPs” (p. 250).

4

Click OK to close the form.

End of steps

17.27 To create an OSPF area

17.27.1 Steps

1

In the navigation tree OSPF view, right-click on the OSPFv2 instance and click Create Area. The Area Site (Create) form opens.

2

Configure the required general parameters.

3

Configure the Area ID parameter and click Apply.

Note: You can create up to four areas on an OSPFv2 instance. Default is Area0 with IP address 0.0.0.0.

4

Repeat Step 1 to Step 3 to configure multiple areas.

5

Save your changes and close the form.

End of steps

17.28 To add a Layer 3 interface to an OSPF router

17.28.1 Purpose

Perform this procedure to allow an OSPF-enabled router to participate in area discovery and share routing information with other area members. On configuring the OSPFv2 routing instance, L3 interface and area on an OSPFv2 router which are operationally up, the OSPF neighbors gets discovered under OSPF instance.

Note: This action assigns an existing Layer 3 interface to the router in the OSPF area rather than creating a new Layer 3 interface.

17.28.2 Steps

1

In the navigation tree OSPF view, expand Network→Instance.

2

Right-click on an Area icon and choose Create Interface. The OSPF Interface (Create) form opens.

3

Configure the required general parameters.

4

Choose an interface in the Interface panel.

5

Click on the Protocol Properties tab and configure the required parameters.

6

Based on the configuration select the Type parameter from the Type drop-down menu (Broadcast and Point-to-Point).

Default type is Broadcast.

7

Save your changes and close the form.

END OF STEPS

17.29 To configure OSPF segment routing and discover dynamic LSPs

17.29.1 Steps

1

In the navigation tree Routing view, expand Network→*NE*→Routing Instance→OSPF Instances.

2

Right-click on an OSPF Instance object and choose Properties. The OSPF Site, Routing Instance, OSPF Instance (Edit) form opens.

3

Click on the Segment Routing tab.

4

Set the Administrative State parameter to Up and configure the required parameters.

The Prefix SID Type parameter can be either Local or Global. The default is None.

Note: The segment routing administrative state can be enabled only if the prefix SID type is either Local or Global.

The minimum value for the Prefix SID Start Label parameter depends on the value of the Start Segment Routing Label parameter on the MPLS instance. See 17.7 “To configure an MPLS interface” (p. 231) .

5

Click OK to save your changes and close the form.

Note: Upon enabling segment routing with administrative state UP and Prefix SID parameter to Local or Global the Dynamic LSPs gets discovered.
The path to view the discovered dynamic LSPs, Manage→MPLS→Dynamic LSPs.
Dynamic LSPs form opens with the list of discovered dynamic LSPs.

END OF STEPS

17.30 To configure IP/MPLS Service Tunnel

17.30.1 Steps

1

Choose Manage→Service Tunnel from the NFM-P main menu. The Manage Service Tunnel form opens.

2

Click Create→IP/MPLS Service Tunnel (SDP). The IP/MPLS Service Tunnel (SDP) wizard opens.

3

Configure the required parameters.

4

Click Next. The Pick Source Node step is displayed.

5

Select a source site or enter its IP address.

6

Click Next. The Pick Destination Node step is displayed.

7

Select a destination site or enter its IP address.

8

Click Next. The Specify Transport step is displayed.

9

Specify MPLS for the Underlying Transport parameter and configure the required parameters.

10

Enable the SR-OSPF check-box.

11

Click OK to save the changes and close the form.

END OF STEPS

17.31 To create and run a VPRN Ping test from a service manager form

17.31.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Service Manager form opens.

2

Choose a service from the list and click Properties. The *Service* (Edit) form opens.

3

Click on the Sites tab.

4

Choose a site or sites from the list and click Properties. The Site (Edit) form opens.

5

Click on the OAM tab, then the Tests tab.

6

Configure and run a VPRN ping OAM diagnostic.

To create and run a VPRN ping:

1. Click on the VPRN Ping tab. A list of VPRN diagnostics appears.

2. Double-click on a row in the list to edit an existing test, or click Create to create a new test. The VPRN ping form opens.
3. Configure the required parameters.
4. Select a VPRN site.
5. Click on the Test Parameters tab and configure the required parameters.

   The Probe History parameter is only configurable when the NE Schedulable parameter is enabled.
6. Click on the Results Configuration tab and configure the required parameters.
7. Click Apply to save the changes and confirm the action.
8. Click Execute. A deployed test is created and run. Open the deployed test from the Deployed Tests tab to view its current state. When the test is complete, the deployed test is removed, and you can view the results.

7

View the test results on the Results tab. The results depend on the type of test.

Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

END OF STEPS

17.32 To create and run a VPRN Ping test on a SAP

17.32.1 Steps

1

Choose Manage→Service→Services from the NFM-P main menu. The Service Manager form opens.

2

Choose a service from the list and click Properties. The *Service* (Edit) form opens.

3

Click on the Sites tab.

4

Select one or more SAPs within the sites in the service, then right-click on a SAP and select Run OAM Tests. The OAM Contextual Test form opens.

5

Configure the test parameters as required, and click on the Execute button.

6

View the test results on the Results tab. The results depend on the type of test.

Result information includes:

- Number of Probes Sent
- Time Last Response
- Number of Responses Received

END OF STEPS

17.33 Wavence VPRN service — considerations/limitations

17.33.1 Wavence-specific service provisioning considerations/limitations

Table 17-2, “Wavence VPRN service — considerations/limitations” (p. 253) lists the notable services provisioning considerations and limitations for Wavence devices.

Table 17-2 Wavence VPRN service — considerations/limitations

Functions	Limitations
L3 VPRN services	• Non-default customer assignment are not supported for Wavence domain. • Consider two VPRN (PE) sites A and B, if the spoke-SDP binding from A to B goes down (admin/operational) then spoke-SDP binding from B to A will remain admin and operational up (but will contain alarms related to spoke SDP binding from A to B on the "Affected Alarms" tab of spoke-SDP binding from B to A). • VPRN SAP related statistics show field names that are common across multiple domains (for example, SR, SAR, and so on). • IP stats are applicable only to the network interface and the same is displayed for Wavence nodes. • VPRN interface creation via the routing sub-tree view in the NFM-P is not supported. • The creation of L3 SAP requires IP address assignment. • The System IP address of NEs managed in the NFM-P should be unique (/32 subnet mask).
L3 VLAN ID	• The range of the L3VLAN IDs configured on the NE should 0 and 2 to 4080. • VLAN IDs present in the NE VLAN Table cannot be selected as IP Data Plane L3VLAN ID and IP Data Plane L3VLAN ID cannot be used to the NE VLAN Table. • When the L3VLAN ID is set to 0, it is not allowed to create network IP interfaces and administratively enable the system IP interfaces and modify any L3 VPN related parameters. • The IP Data Plane L3VLAN ID can be changed only when all the created network IP interfaces and the System IP interface are administratively disabled. Setting VLAN ID to 0 after having created network IP interfaces will not allow to administratively enabling these interfaces.

Table 17-2 Wavence VPRN service — considerations/limitations (continued)

Functions	Limitations
IP network creation/configuration	• Ports involved in the network interface cannot be reused for another network interface creation. • The network interface cannot be administratively enabled if the port and address are not assigned to the interface. • The system interface cannot be modified or deleted when the interface administrative state is enabled.
Static LSP	• Static hops (Swap, Pop) configured under a static LSP will be listed only in the case of creation. If a discovered node has a static LSP along with static hops (Swap, Pop) already configured, then static hops are not listed as these are NFM-P only attributes and there are no common parameters to associate them. Because of this limitation, a “MissingHopConfiguration” warning alarm is raised on the Static LSP. • Destination IP address will not be assigned to static LSPs in the NFM-P if they are created from WebCT. It is required to assign complete static LSP parameters (Source IP, Destination IP, Next Hop and labels) if the user is configuring static LSPs from WebCT. • When LSP is created with static hop entries (SWAP/POP), end to end LSP path will be created in the NFM-P. The hop (SWAP/POP) objects are associated to LSP through static hop entries. If the user tries to delete the LSP, it will delete the associated static hop entries (SWAP/POP). • For discovered static LSP, static hop entries (SWAP/POP) are not listed as these objects are not related. If the user tries to delete LSP, the hops are not deleted as they are independent objects. The user has to delete static labels (SWAP/POP) from slabel maps tab of MPLS interface. • User encounters deployment error if static LSP's are deleted with "Turn Up" Administrative state, it’s always required to shut down the static LSP before attempting to delete it.
SR-TE LSP	• When creating an MPLS Path, use the System Interface IP address instead of the Network Element IP address for network elements on the path. • When creating an SR-TE LSP, the Source and Destination IP should use the respective node System Interface IP.
SDP tunnels	• SDP tunnels cannot reuse LSP that are already configured under other SDP tunnels. • SDP Tunnel page show some irrelevant tabs or attributes for Wavence, which are relevant across SR/SAR nodes. • SDP Tunnel creation form requires source and destination node IPs.
Network QoS	The node will accept the configuration only if the LSP EXP in profile and LSP EXP out profile bits are same.
Transport setup	Transport setup is not supported for disjoint topology. If any discrepancies are detected, transport setup will display an error and it is the responsibility of the user to delete such configurations.

A NEtO, WebCT, and NFM-P management comparison

A.1 Overview

A.1.1 Purpose

Appendix A illustrates the Wavence management features supported by other element managers as compared with NFM-P.

A.1.2 Contents

A.1 Overview	257
A.2 Support for Wavence management features across element managers	257

A.2 Support for Wavence management features across element managers

A.2.1 NEtO, WebCT, and NFM-P management feature support

This topic provides the management features for Wavence devices and shows which are supported by each element manager.

Table A-1, “Legend for feature support tables” (p. 257) is a legend that describes the meaning of annotations used in Table A-2, “NEtO, WebCT, and NFM-P management feature support” (p. 258).

Table A-1 Legend for feature support tables

Annotation	Meaning
N	Not supported
N*	Not supported, settings affecting NFM-P only
N**	Not supported, thresholds (through policy) affecting NFM-P only
NS	No plan to support
R	Read only
Y	Supported
Y*	Supported with similar functionality
Y**	Supported for IPv4 only
Y1	PM current data
Y2	Supported via Radio dashboard

Table A-1 Legend for feature support tables (continued)

Annotation	Meaning
Y3	Supported only for Radio G.826 PM
Future	Candidate features

Table A-2, "NEtO, WebCT, and NFM-P management feature support" (p. 258) lists the management features for Wavence devices and shows which features are supported by each element manager.

Table A-2 NEtO, WebCT, and NFM-P management feature support

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
Maintenance & Monitoring				
Alarms	Current Alarms reporting	Y	Y	Y
	Alarms Log (Alarm History)	Y	Y	Y*
	Alarms Severities Settings (ASAP)	Y	Y	Y
	Alarms Synthesis	Y	Y	N
Events	Events LOG	Y	NS	N
Current Configuration View	CCV file	Y	Y	N
Abnormal Conditions	Abnormal Conditions Synthesis	Y	Y	Y
	Abnormal Conditions List	Y	Y	Y
Restart commands	Restart NE	Y	Y	Y
	Restart MPT	Y	Y	N
EFM (802.3ah)	Ethernet First Mile / OAM Settings	Y	Y	Y
	Ethernet First Mile / OAM Remote Loopback	Y	Y	Y
ECFM (802.1ag)	Ethernet Connectivity Fault Management	CLI	Y	Y
Neighbors	Link Layer Discovery Protocol (Ethernet)	N	Y	Y
	Radio Neighbors discovery	Y	Y	Y*
Protections commands	Lockout / Forced Switch / Manual Switch EPS	Y	Y	R
	Lockout / Forced Switch Core EPS	Y	Y	Y
	Lockout / Forced Switch / Manual Switch RPS	Y	Y	R
	Lockout / Forced Switch / Manual Switch TPS	Y	Y	R
Protections status	EPS	Y	Y	R
	RPS	Y	Y	R
	TPS	Y	Y	R

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
Ethernet Statistics	Ethernet Statistics per Ethernet port (Tx/Rx)	Y	Y	Y
	Ethernet Statistics per Radio port (Tx only)	Y	Y	Y
	Ethernet Statistics per Radio queue (Tx only)	Y	Y	Y
Performance Monitoring	Radio PM activation / de-activation	Y	Y	Y
	Radio G.826 PM	Y	Y	Y
	Radio Tx/Rx Power PM	Y	Y	Y
	Radio Rx Diversity Power PM	Y	Y	Y
	Radio Adaptive Modulation PM	Y	Y	Y
	E1 / DS1 PM activation / de-activation	Y	Y	N
	E1 PM	Y	Y	Y
	DS1 PM	Y	Y	Y
	STM.1 RS PM activation / de-activation	Y	Y	Y
	STM-1 RS PM (SDH Transparent)	Y	Y	Y
	Threshold Data	Y	Y3	N**
Radio Statistics	Analogue Measurements (RSL, TSL, XPD)	Y	Y	Y
	Equipment Measurements (Temperature, Power, Current, Voltage)	N	Y2	Y
RSL History	RSL History file	Y	Y	Y
Tx Diversity Antenna	Tx Diversity Antenna	Web Server	Y	N
MPT/EASv2 replacement	MPT/EASv2 replacement	Web Server	NS	N
L3 Routing	IP Data Plane Routing	N	Y	Y
	Label Forwarding Table	N	Y	Y
	VPRN Routing	N	Y	Y
L3 Statistics	IP Data Plane Statistics	N	Y	Y
	MPLS Instance Statistics	N	Y	Y
	VPRN Statistics	N	Y	Y
L3 Access	Service Access Point Configuration	N	Y	Y
	Service Tunnel Spoke Binding	N	Y	Y
	Access Routing Configuration	N	Y	Y
Administration				
License Management	Licence info & upgrade	Y	Y	Y

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
NE Info	Site Name	Y	Y	Y
	Site Location	Y	Y	Y
	Latitude	Y	Y	Y
	Longitude	Y	Y	Y
	Node MAC Address	Y	Y	Y
Software Package	SW Package download	Y	Y	Y
	SW Package Activation	Y	Y	Y
	SW Packages/SW Units Management	Y	Y	Y
User Profiles & Access management	Users configuration	Y	Y	N
	Users Profile management	Y	Y	N
B&R	Backup & Restore	Y	Y	Y
System Settings	Date/Time Settings	Y	Y	Y
	DHCP Enabling/Disabling	Y	Y	Y
SNMP Settings	SNMP Community String	Web Server	Y	N*
	SNMP Version	Web Server	NS	Y
TACACS	Authentication & Authorization	CLI / SNMP	NS	R
	Accounting	CLI / SNMP	NS	R
CFNR (Configuration File)	Configuration File Download	Y	NS	N
CorEvo Upgrade	CorEvo Upgrade	Web Server	Y	N
LAC	Local Access Control settings	Y	Y	Y
	Local Access Control status	Y	Y	Y
Networking				
Networking IPV4/IPV6	NE Local Address	Y	Y	R
	Local TMN Ethernet port	Y	Y	R
	TMN Ethernet port#4	Y	Y	R
	TMN In-Band	Y	Y	R
	PPP RF	Y	Y	R
	OSPF	Y	Y	R
	Static Routing	Y	Y	R
	Routing Table	Y	Y	R

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
IPv6	IPv6 Pre-Provisioning	Y	NS	N
	IPv6 Activation	Y	Y	N
NTP	NTP servers setting	Y	Y	Y
	Inventory	Y	Y	Y
Equipment				
Equipment	MSS slots configuration	Y	Y	R
	MPT-HLS subracks	Y	Y	R
MSS Protections	Core board Protection	Y	Y	R
	PDH board Protection	Y	Y	R
	SDH board Protection	Y	Y	R
	Static LAG for Core Protection	Y	Y	R
	Ethernet Loss as Core Protection switch criteria	Y	Y	R
Radio Protections	1+1 HSB	Y	Y	R
	1+1 FD	Y	Y	R
	Virtual RPS enabling	Y	Y	R
	CLA Reset command	Y	Y	N
Remote Inventory	Remote Inventory	Y	Y	Y
Power	Power Source (PoE / QMA)	Y	Y	R
Housekeeping	Housekeeping on AUX board	Y	Y	Y
	Housekeeping on A-FAN board	Y	Y	Y
	Housekeeping on E-FAN board	Y	Y	Y
Interfaces				
PDH	E1 Settings	Y	Y	Y
	DS1 Settings	Y	Y	Y
	DS3 Settings	Y	Y	Y
	E1 Node Timing	Y	Y	Y
	CES Settings (TDM2TDM / TDM2ETH Service Profiles)	Y	Y	Y
	Loopbacks	Y	Y	Y

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
SDH Transparent	STM-1 / OC3 Settings	Y	Y	Y
	CES Settings (SDH2SDH Service Profile)	Y	Y	Y
	Loopbacks	Y	Y	Y
SDH Channelized	STM-1 Settings	Y	Y	Y
	E1 Channelized Node Timing	Y	Y	Y
	CES Settings (TDM2TDM / TDM2ETH Service Profiles)	Y	Y	Y
Radio	User Label	Y	Y	R
	Channel Administrative State (UBT-T and UBT-S2)	N	Y	R
	Capacity License (UBTs)	N	Y	R
	Coding Modulation (FCM/ACM)	Y	Y	R
	Modem Profile (Channel Spacing, Modulation, Supported Modulations in ACM, Option, Net BW)	Y	Y	R
	XPIC Polarization & Associated Channel	Y	Y	R
	Space Diversity	Y	Y	R
	Shifter & Frequency	Y	Y	R
	Power (RTPC/ATPC)	Y	Y	R
	Link Identifier	Y	Y	R
	Encryption	Y	Y	R
	Packet Throughput Booster	Y	Y	R
	Low DC Voltage Alarm Threshold	Y	Y	R
	Branching Loss	Y	NS	R
	Loopbacks	Y	Y	Y
	Radio Equipment Measurements (Temperature, Power, Current, Voltage)	Y	Y	R
	Tx Mute (manual, timed, auto)	Y	Y	Y
	Current Modulation & Net BW in ACM	Y	Y2	R
	Freeze & Force command in ACM	Y	Y	R
	Squelch command in Space Diversity	Y	Y	R

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
Ethernet	Speed & Duplex Settings w/ Autonegotiation Disabled	Y	Y	Y
	Speed & Duplex Settings w/ Autonegotiation Enabled	Y	Y	Y
	Flow Control	Y	Y	Y
	Autonegotiation Restart command	Y	Y	Y
	Port Rate Limiter Settings	Y	Y	Y
	Storm Control Settings	Y	Y	Y
LAG	Ethernet LAG L2	Y	Y	Y
	Radio LAG L2	Y	N	R
	Radio LAG L1	Y	Y	R
	Radio LAG L1 with electrical interface	N	Y	R
IP Data Plane	IP Data Plane VLAN ID	N	Y	Y
	System IP Interface	N	Y	Y
	Network IP Interfaces	N	Y	Y
	IP Data Plane Static Routing	N	Y	Y
Services				
TDM Services	Cross Connections (TDM2TDM / TDM2ETH / SDH2SDH)	Y	Y	Y
	Admission Control	Y	NS	Y
	Cross Connections recovery	Y	NS	Y
	Admission Control enabling (ODU 300 only)	Y	NS	Y
	SDH Flow Drop Priority (in LAG)	Y	Y	Y
Port Segregation	Ports Segregation	Y	Y	N
Ethernet Services	Bridge Type	Y	Y	Y
	802.1q Virtual Bridge	Y	Y	Y
	802.1ad Provider Bridge	Y	Y	Y
	VLAN Rate Limiter	Y	Y	Y
	Per VLAN per COS Rate Limiter	Y	Y	Y

Table A-2 NEtO, WebCT, and NFM-P management feature support (continued)

Domain	Feature	NEtO	Web CT	NFM-P 19.3 or later
Ring	Ring Radio-Radio	Y	Y	Y
	Ring of L1 LAG	Y	Y	Y
	Ring Radio-Ethernet	Y	Y	Y
	Ring Ethernet-Ethernet	Y	Y	Y
	Mixed Ring XCs Pre-configuration tool	Y	NS	Y*
Synchronization	Synch Role (Master/Slave)	Y	Y	Y
	Primary / Secondary Synch sources	Y	Y	Y
	Synch-E for Ethernet ports	Y	Y	Y
	Synch-in / Synch-out	Y	Y	Y
	SSM	Y	Y	Y
1588	1588 TC enabling	Y	Y	Y
	1588 BC/OC Settings (Ring included also)	Y	Y	Y
	VLAN Settings	Y	Y	Y*
	1588 BC/OC Statistics	Y	Y	Y
	ToD	Y	Y	Y
QoS	Classification Criteria (802.1p / DiffServ) Setting	Y	Y	Y
	Forwarding Class - Queue mapping	Y	Y	Y
	Scheduler Setting	Y	Y	Y
	Queue Size Setting	Y	Y	Y
MPLS QoS	SAP Ingress QoS	N	Y	Y
	SAP Egress QoS	N	Y	Y
	Network QoS	N	Y	Y
Bandwidth Notification	Bandwidth Notification	N	Y	Y
AUX Channels	Auxiliary Channels configuration (ODU300 only)	Y	NS	N
	Auxiliary Channels Cross-Connections (ODU300 only)	Y	NS	N
L3 Services	MPLS Instance	N	Y	Y
	MPLS Interfaces	N	Y	Y
	Static LSPs	N	Y	Y
	VPRN Services	N	Y	Y
	SDPs	N	Y	Y

Table A-3, “WebCT and NFM-P management feature support on the UBT-SA” (p. 265) lists the management features for UBT-SA and shows which features are supported by each element manager.

Table A-3 WebCT and NFM-P management feature support on the UBT-SA

Domain	Feature	Web CT	NFM-P 19.6 and later
Administration			
NE Info	Site Location	Y	Y
	Latitude	Y	Y
	Longitude	Y	Y
B&R	Backup & Restore	Y	Y
Equipment			
Equipment	Slots configuration	Y	Y
Maintenance & Monitoring			
Alarms	Current Alarm reporting	Y	Y
	Alarm Log (Alarm History)	Y	Y
Restart Command	Restart NE	Y	Y
Performance Monitoring	Radio PM activation / de-activation	Y	Y
Networking			
Networking IPV4/IPV6*	NE Local Address	Y	Y
	Local TMN Ethernet port	Y	Y
	TMN Ethernet port#4	Y	Y
	TMN In-Band	Y	Y
	Routing Table	Y	Y
IPv6*	IPv6 Pre-Provisioning	Y	Y
	IPv6 Activation	Y	Y
* IPv6 is applicable from NFM-P 19.9 or later			