HITACHI
Inspire the Next

PRODUCT GUIDE

FOXMAN-UN
System Description

Hitachi Energy

Document ID	1KHW002415-R18	
Document edition	FOXMAN-UN System Release:	R18
	Revision:	A
	Date:	2025-08-14

Copyright and confidentiality

Disclaimer

This document contains information about one or more Hitachi Energy products and may include a description of or a reference to one or more standards that may be generally relevant to the Hitachi Energy products. The presence of any such description of a standard or reference to a standard is not a representation that all the Hitachi Energy products referenced in this document support all the features of the described or referenced standard. In order to determine the specific features supported by a particular Hitachi Energy product, the reader should consult the product specifications for that Hitachi Energy product. In no event shall Hitachi Energy be liable for direct, indirect, special, incidental, or consequential damages of any nature or kind arising from the use of this document, nor shall Hitachi Energy be liable for incidental or consequential damages arising from the use of any software or hardware described in this document.
Hitachi Energy may have one or more patents or pending patent applications protecting the intellectual property in the Hitachi Energy products described in this document. The information in this document is subject to change without notice and should not be construed as a commitment by Hitachi Energy. Hitachi Energy assumes no responsibility for any errors that may appear in this document.
All people responsible for applying the equipment addressed in this manual must satisfy themselves that each intended application is suitable and acceptable, including compliance with any applicable safety or other operational requirements. Any risks in applications where a system failure and/or product failure would create a risk for harm to property or persons (including but not limited to personal injuries or death) shall be the sole responsibility of the person or entity applying the equipment, and those so responsible are hereby requested to ensure that all measures are taken to exclude or mitigate such risks.
Products described or referenced in this document are designed to be connected and to communicate information and data through network interfaces, which should be connected to a secure network. It is the sole responsibility of the system/product owner to provide and continuously ensure a secure connection between the product and the system network and/or any other networks that may be connected.
The system/product owners must establish and maintain appropriate measures, including, but not limited to, the installation of firewalls, application of authentication measures, encryption of data, installation of antivirus programs, and so on, to protect these products, the network, its system, and interfaces against security breaches, unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
Hitachi Energy performs functionality testing on released products and updates. However, system/product owners are ultimately responsible for ensuring that any product updates or other major system updates (to include but not limited to code changes, configuration file changes, third-party software updates or patches, hardware change out, and so on) are compatible with the security measures implemented. The system/product owners must verify that the system and associated products function as expected in the environment in which they are deployed. Hitachi Energy and its affiliates are not liable for damages and/or losses related to security breaches, any unauthorized access, interference, intrusion, leakage, and/or theft of data or information.
This document and parts thereof must not be reproduced or copied without written permission from Hitachi Energy, and the contents thereof must not be imparted to a third party nor used for any unauthorized purpose.

Contents

1 Network Management with FOXMAN-UN

The FOXMAN-UN manages dedicated Network Elements (NEs) according to ISO FCAPS network management model and framework. It supports the following management functional areas:

- Fault Management,
- Configuration Management,
- Performance Management,
- Security Management.

FOXMAN-UN integrates into a larger overall Operations Supports System (OSS) by providing northbound interfaces (NBI) to several higher level management (HLM) systems.

This chapter provides a high level description of how FOXMAN-UN fits into the network. The main sections are:

- 1.1 "Server Redundancy",
- 1.2 "FOXMAN-UN Architecture",
- 1.3 "FOXMAN-UN Key Functionality",
- 1.4 "FOXMAN-UN Deployment Scenarios",
- 1.5 "The Managed Network Environment".

1.1 Server Redundancy

FOXMAN-UN can be deployed with server redundancy. A main server provides the default FOXMAN-UN base and core services, and the database to which a client can connect. A warm standby or cold standby server is configured and is activated in case of non-availability of the main server.

With warm standby the services on the standby server are started automatically when switching over. With cold standby the services on the standby server need to be started manually.

A periodic database backup and replication ensures that main and standby servers have an up-to-date database.

1.2 FOXMAN-UN Architecture

The key to the deployment of FOXMAN-UN is its architecture, which is designed with distributed management in mind and is based on a modern hardware platform and object oriented technology.

FOXMAN-UN architecture consists on the following components:

- NEM Core including database,
- Agents (southbound interfaces),
- NEM Client (Main GUI includes NEM Desktop, NEM Configurator, NEM Network Browser),
- Northbound Interfaces (e.g. SNMP, CLI).

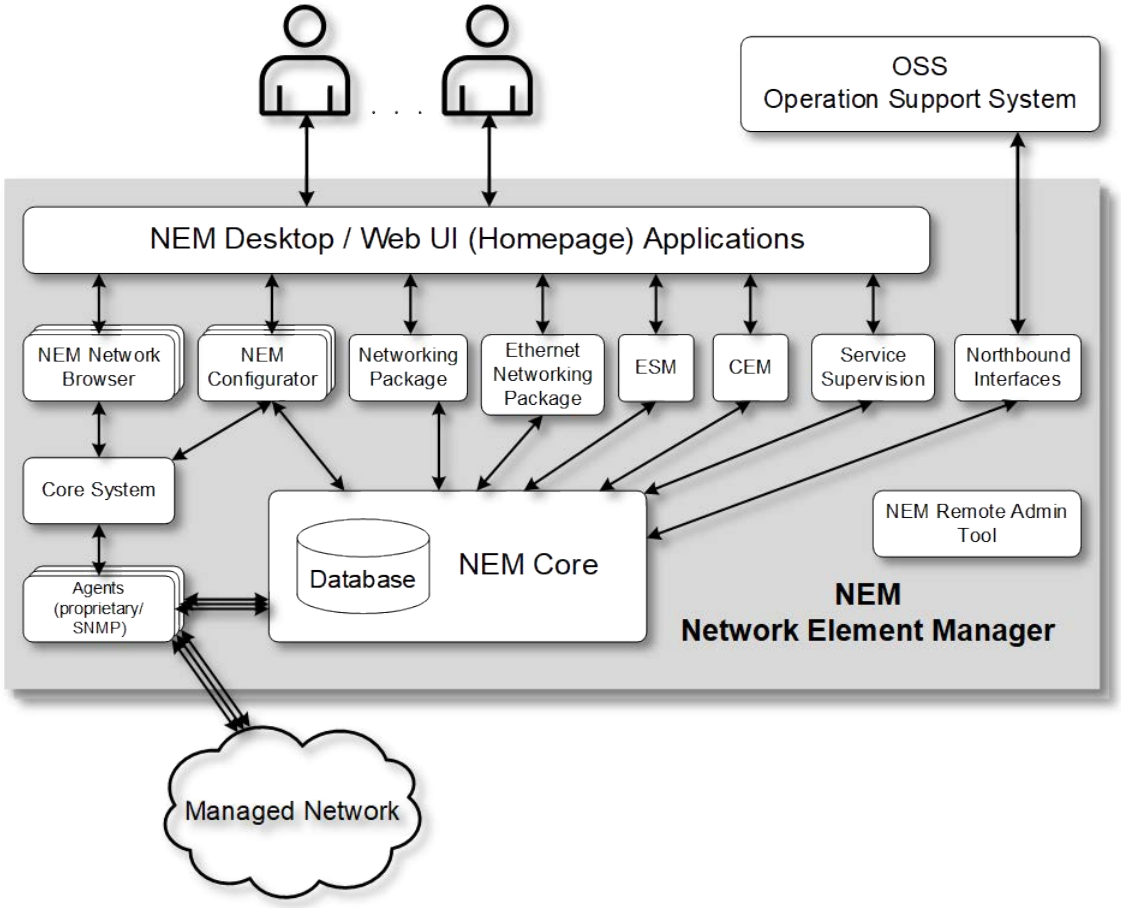


Figure 1: FOXMAN-UN Architecture

1.2.1 NEM Core and Database

FOXMAN-UN is built around a database. This database stores all the relevant information:

- For management:
  - Agents and supervised network elements.
- At the element level:
  - configuration,
  - alarm,
  - inventory,
  - performance counters (if enabled).
- At networking level:
  - Services (Service Supervision),
  - End-to-end MPLS services (Ethernet Networking Package),
  - End-to-end TDM services (Networking Package).
- For security access:
  - users and roles,
  - domains,
  - profiles.
- Maps and sections;
- SW management for managed nodes (FOX61x):
  - Network overview,
  - Distribution wizard,

  - Task and job management.
- Credentials distribution:
  - Scheduled tasks for distribution of passwords to managed nodes (FOX61x),
  - management and download to managed nodes (FOX61x) of SSH keys;
- Events.

The core component contains the software necessary for managing this information as well as for handling the communication with the other processes.

1.2.2 Agents

The agent handles the communications with the network elements.

In a multi-tasking operating system, several agent processes can be running depending on the number of sub-networks connected to the workstation.

The agent can:

- upload and download configurations from and to the NEs,
- poll NEs for alarms,
- collect inventory data from NEs,
- retrieve and set status information.

1.2.3 Managed Network Elements

Hitachi Energy FOX61x platform has a native integration into FOXMAN-UN including:

- Full Graphical User Interface (GUI) and Management Support;
- All NE information completely uploaded into the FOXMAN-UN database.

Hitachi Energy FOX51x platform has a native integration into FOXMAN-UN including:

- Full Graphical User Interface (GUI) and Management Support via the FOXMAN-UN client for Windows®;
- All NE information completely uploaded into the FOXMAN-UN database.

FOXMAN-UN offers southbound interfaces enabling the integration of Hitachi Energy and third party SNMP devices into the network for:

- Inventory,
- Alarming,
- Cross-launch of management software,
- Full NE support in FOXMAN-UN network browser (network map).

Each of the network elements contains managed objects such as:

- attributes (system options and settings),
- parameters (options and settings of interfaces),
- network connections (interconnections of the interfaces).

All NEs are interconnected to form a management network containing managed objects such as:

- subunits,
- circuits.

Please note:
Refer to FOXMAN-UN Release Note for the latest updated list.

1.2.3.1 FOX61x and FOX51x Families

FOXMAN-UN manages the following Hitachi Energy NEs:

FOX61x shelves:

- FOX615,
- FOX612,
- FOX611.

FOX610

FOX51x shelves:

- FOX515 (local craft terminal in FOXMAN-UN client for Windows® only),
- FOX512 (local craft terminal in FOXMAN-UN client for Windows® only),
- FOX-U (existing setups supported, but not creation of new NEs),
- FOX-U/E (existing setups supported, but not creation of new NEs).

1.2.3.2 SNMP Devices

FOXMAN-UN manages the following SNMP devices:

- Hitachi Energy EDS500 series switch 500NMDxy,
  - For the full list of supported EDS500 series devices refer to the FOXMAN-UN R18 release note.
- DTM-M SHDSL Router,
- Hitachi Energy Scada NG,
- Hitachi Energy LRIS-34xx:
  - LRIS-3410,
  - LRIS-3420,
  - LRIS-3430,
  - LRIS-3440.
- Hitachi Energy LRIS-32xx:
  - LRIS-3230,
  - LRIS-3260.
- AKCP SensorProbe 2,
- Alcatel-Lucent OmniSwitch 6450 / 6860,
- Benning Power D400,
- Billion BIPAC 8500 / 8501 / 8520,
- BKtel Optical Amplifier/Sender (OAS),
- Ciena 6130,
- Cisco 3845/2811 Integrated Services Router,
- Cisco Catalyst 2960 Switch,
- CXR FOE1T1 (TNLO),
- Delta Power Supply DPS 600B-48-2/4,
- Elcon BIG 10 (1022 / 1024),
- Elcon FOS 100 CPE,
- Ericsson Mini-Link TN R4,
- FortiGate 100D / 300C / 311B,
- NEXANS iSwitch G1043,
- NEXANS FibreSwitch BM100,
- Plisch DAB TDA3000 series,
- Proscend 5600 / 6200,
- SAIA-PCD.

Other devices:

- FOX660 (read-only functionality).

Please refer to FOXMAN-UN Release Note for the latest updated list.

1.2.4 NEM Client (Graphical User Interfaces)

The NEM Desktop provides the menus for calling all FOXMAN-UN functions, applications, the NEM Help, and the new browser-based Homepage (Web UI).

The NEM Desktop itself is started by connecting it to an active NEM core via the login procedure.

The NEM Desktop provides the user with the legacy application interfaces. The main applications are the NEM Configurator and NEM Network Browser.

The NEM Configurator provides access to the NE configuration management, whereas the NEM Network Browser provides graphical view of the network.

The Homepage, introduced with release R16B, is the browser-based home for all applications. It includes new applications that are not available from the NEM Desktop. It also provides links to all legacy applications.

Please refer to 2.3 "NEM Desktop" for further details and information regarding the other FOXMAN-UN applications.

1.2.5 Northbound Interfaces

FOXMAN-UN offers several northbound interfaces, which can be activated via the FOXMAN-UN license. These interfaces enable the FOXMAN-UN integration into the following Higher Level Management (HLM) systems:

- SNMP for fault management;
- XML or CSV (file based) for inventory management
- Command line interfaces for inventory data retrieval and POTS line test in FOX51x NEs;

  A terminal in the OSS is connected to a specific TCP port in the FOXMAN-UN core for each CLI interface. A special set of commands is available for the execution and the retrieval of results.

FOXMAN-UN supports the following HLM applications:

- SNMP, IBM Netcool certified (FM).

Additionally, FOXMAN-UN can be integrated into almost any HLM application providing SNMP based (southbound) interface.

For support of any other HLM software, please contact Hitachi Energy.

1.3 FOXMAN-UN Key Functionality

FOXMAN-UN provides Basic Package (BP) and Network Services for TDM (PDH/SDH)-based, and MPLS-TP based networks. These services are subdivided into major functional areas which interact with each other:

- Fault,
- Configuration,
- Performance,
- Security.

1.3.1 Fault Management

FOXMAN-UN offers alarm management, which ensures that operator can quickly locate, analyze and correct network problems. The Alarm Manager is mainly responsible for:

- alarm list,
- alarm summary,
- alarm customization,
- alarm history,

- alarm escalation.

1.3.2 Configuration Management

FOXMAN-UN's Configuration Management is divided into distinct parts, listed below

- Network element configuration

  The configuration of NEs are done via dedicated configuration tools:

  - FOXCST for FOX61x NEs,
  - UCST for FOX51x NEs,
  - craft terminals, web interfaces for 3rd party devices.

  FOXMAN-UN provides basic operations such as changing the NE's name and password.
- Network wide configuration to:
  - discover the network inventory including NE, unit, port, configuration or service inventory;
  - manage the interconnection between NEs via Section Management sub-system;
  - display the selected network's graphical view via NEM Network Browser;
  - perform bulk configuration to simplify tasks on several NEs like modification or distribution of Passwords, Profiles, Custom Parameter Sets and Embedded software.

1.3.3 Performance Management, Diagnostics and Status

FOXMAN-UN allows collecting and reporting of the NEs, networks and services performances through the following:

- Performance Data Collection:

  Elements in the managed network can be specified for performance monitoring. The performance data of these elements are continuously collected and saved in a separate database.

  Collected performance data from NEs, the FOXMAN-UN server, or basic OS statistics can be displayed via customizable dashboards in the Metrics Database application.

  From there, the performance information can be exported for integration into an OSS (Operation Support System).
- Health Monitoring:

  Some specific performance data, such as RX/TX errors, RX/TX throughput, NE uptime, NE temperature, CPU load, SFP temperature, SFP RX/TX power, memory usage, is used to indicate network, network element, and section health in the Network Monitoring application.
- Service Supervision and Reporting:

  This allows FOXMAN-UN to measure the end-to-end service delivery quality. It ensures that end-to-end applications are flowing across the network and are being delivered to the end users according to the agreed service level metrics.
- Synchronization maps:

  Synchronization map graphically displays the actual clock propagation of the SDH or PDH of the managed network. This facilitates identifying synchronization problems such as:

  - 'clock islands', where a network element clock is generated locally and is not propagated to any other network element,
  - 'timing loops' which may have inadvertently been created by propagating the clock from a network element back to a network element which is providing the clock source.

  PTP synchronization map graphically displays the PTP clock distribution in the Ethernet / MPLS-TP network with clock mode, ID, class, accuracy, and source for each NE.
- NE Synchronization:

  FOXMAN-UN allows synchronizing the alarms, inventory and service of all or a selection of the NEs in the managed network with the database. In addition date and time of the NEs can be synchronized with the workstation date and time.

1.3.4 Security Management

FOXMAN-UN's security management ensures only authorized FOXMAN-UN users can access the system. It includes proper configuration of management rights, privileges and permission of authorized FOXMAN-UN users based on users and roles definition. It ensures that the network administrators can control what each of these users and roles are allowed to.

FOXMAN-UN security elements consists of connection management, domains, users, roles, and profiles.

The FOXMAN-UN connection manager requires username and password to authenticate a FOXMAN-UN user. A domain containing a number of elements (NEs, security profiles, agents, services, etc.) is assigned to a FOXMAN-UN user via a role (predefined system role or user-defined role) which determines the FOXMAN-UN functions the user has a right to execute. For example, a FOXMAN-UN user with a specific role can manage specific nodes without knowing the nodes' passwords. It's the user's role(s) that defines whether or not the user can access the configuration of specific nodes.

Please note:
For details, please refer to 3 "Security Administration".

1.4 FOXMAN-UN Deployment Scenarios

1.4.1 General

Depending on the network size and the operation & maintenance organization, the various FOXMAN-UN components can be distributed on different workstations / PCs, and different locations. The appropriate license options must be ordered to enable the appropriate functionality.

FOXMAN-UN is implemented to run under the following operating systems:

- Red Hat Enterprise Linux,
- Microsoft Windows® (client installation with GUIs only, i.e. NEM Desktop, NEM Configurator, and NEM Network Browser, plus Help).

For the specific hardware and OS requirements refer to the FOXMAN-UN Release Note.

FOXMAN-UN under Linux can be ordered and installed as:

- Full version (Core/Agent/GUIs),
- GUIs only (NEM Desktop, NEM Configurator, NEM Network Browser, plus Help, No Element Agent or Core Server functionalities).

FOXMAN-UN under Microsoft Windows® can replace a GUIs only installation or it can be used instead of any X-Terminal solution as e.g. !M, X2Go, Reflection-X, XMing, XManager as a faster solution.

The following examples are described below:

- Single user working on a single workstation,
- Multi-user environment (optionally with core redundancy),
- Network partitioning & regionally organized O&M (optionally with core redundancy),
- Integration to higher order management systems.

Please note:
In the context of the following deployment examples, the term Workstation (WS) is used for LINUX system, while the term Personal Computer (PC) stands for a Microsoft Windows® system.

Please note:
In the scenarios below, the NEM services on “Main” or “Standby” WS are active exclusively, i.e. WS A (Main) is active per default, and WS B (Standby) will only get active when the NEM services on WS A (Main) are down or WS A (Main) is unreachable.

1.4.2 Single User - Single Workstation

For small to medium size networks only one operator needs to work at any one time and all management functions can be performed from a single workstation.

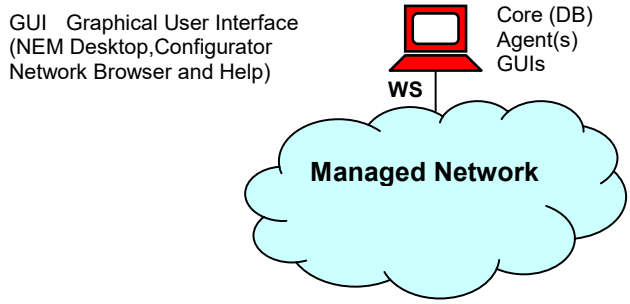


Figure 2: Single User - Single Workstation

1.4.3 Multi-User - Single / Redundant Workstation with Agent(s)

If more than one operator needs to work simultaneously with the FOXMAN-UN, each additional workplace can either be equipped with a workstation running GUIs only, or with a Windows PC.

The additional workstations / PCs can be connected via a LAN sharing the same infrastructure, such as a printer, CD drive, etc.

In the following example, WS A (Main) runs the core with the database, agent(s), and GUIs; WS B (Standby) runs the core services, agent(s) and GUIs in case WS A is down or unreachable. WS C (LINUX) and the PC (Windows) run GUIs only.

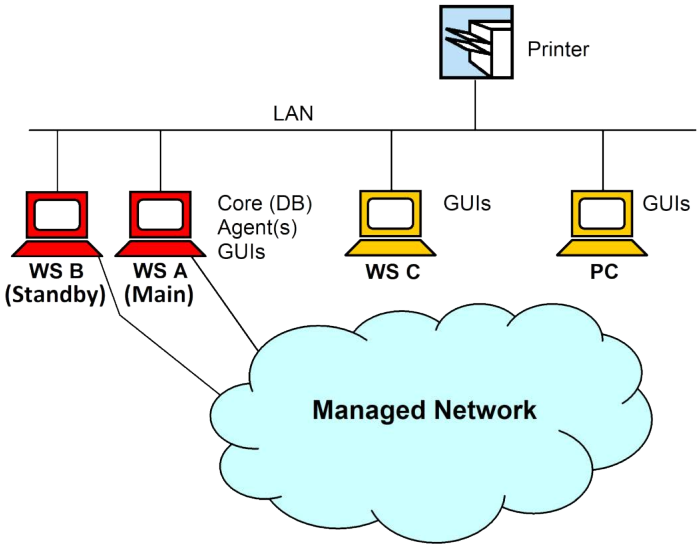


Figure 3: Multi- User - Single Workstation with Agents

In that example, three operators, one on WS A (WS B as optional standby), WS C, and the PC, can work on FOXMAN-UN simultaneously.

Additional PCs or workstations running the GUIs can be added to the LAN as required. Such a configuration is useful for middle sized networks.

The FOXMAN-UN administrators, using the available access administration features can define responsibilities separately for each operator.

1.4.4 Regionally Organized O&M with Network Partitioning

The example below shows an operation & maintenance organization that is regionally distributed.

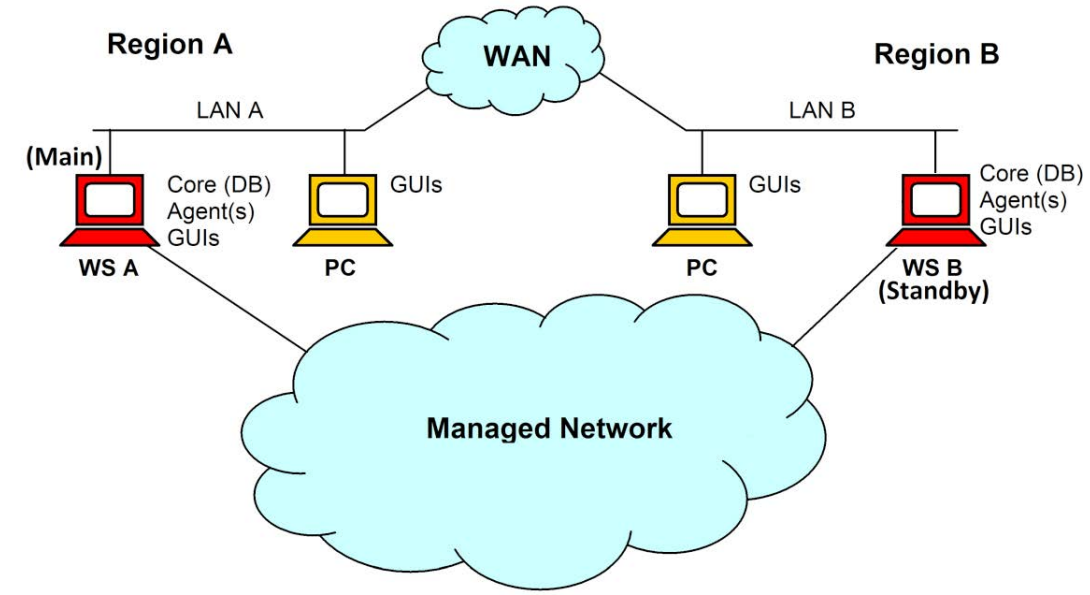


Figure 4: Regionally Organized O&M

When managing a network that covers a large geographic area, it is often advisable to partition the managed network into sub-networks.

Each region can have a part of the FOXMAN-UN infrastructure with core and GUIs, and sharing a central database (on the Main server, with the Standby server as redundancy). For access to the core and the database the different regions are connected via a WAN.

FOXMAN-UN Security Administration provides the administrator with the tools to define which network elements an operator can access. These access rights can be segregated according to the defined regions. They are valid regardless of which WS or PC an operator is working on.

1.4.5 FOXMAN-UN in a Multi-Vendor Environment

In a multi-vendor environment, FOXMAN-UN takes the role of a vendor specific network element manager that supports the FOX61x and FOX51x families of products.

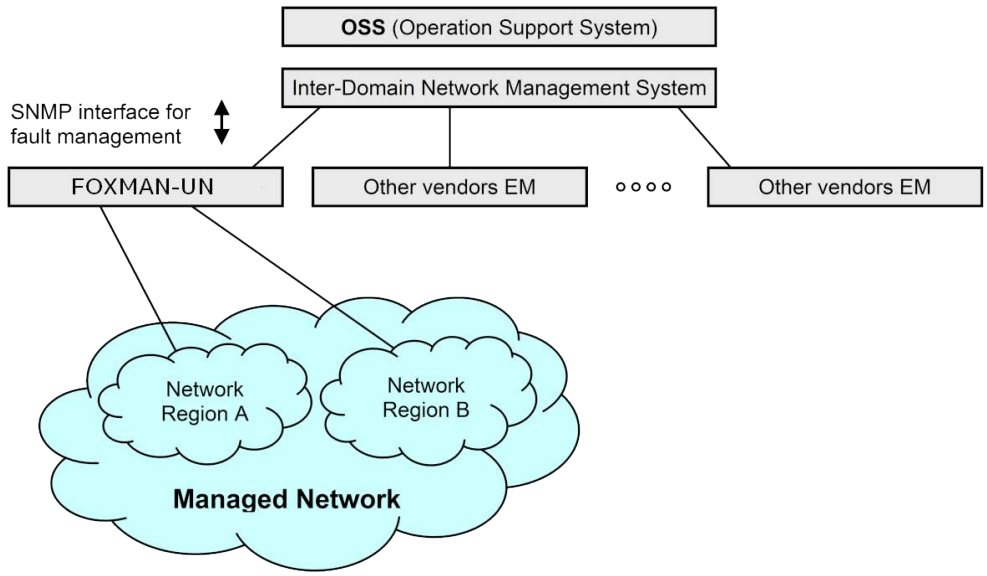


Figure 5: FOXMAN-UN in a Multi-vendor Environment

The above diagram shows the basic management concept envisioned for the management of a heterogeneous network.

In this model the position of FOXMAN-UN is as an Element Manager for the FOX61x and FOX-51x NEs in network regions A and B.

Here the main tasks of the various managers are as follows;

OSS (Operation Support System):

- Handling of customer management,
- Service management,
- Billing & service level reporting,
- Order handling.

Inter-Domain Manager (IDM):

- Common graphical representation of the domains and NEs within the network,
- Inter-domain capacity management,
- Common fault management,
- Common performance management,
- Seamless end-to-end management across the domains.

Element Manager: (e.g. FOXMAN-UN):

- Configuration of the network elements in its domain, including end to-end provisioning within the domain,
- Fault management of the NEs,
- Security management of the NE and domain access,
- Performance monitoring, initiation, collection of data,
- Interface to a higher level manager (e.g. IDM or OSS) to provide the necessary information to enable them to fulfill their tasks. This allows a mediation function between the Higher Level Manager (HLM) and the domain which the Element Manager is controlling.

FOXMAN-UN fulfills the functionality of an Element Manager. In this respect it contains an SNMP proxy agent which provides the interface to a HLM.

1.4.6 Simple Network Management Protocol (SNMP) Proxy Agent

In order to communicate to the Higher Level Managers (HLM), that is the IDM and/or the OSS, FOXMAN-UN provides an SNMP proxy agent as a licensed option. This proxy agent provides a mediation device function for fault management, based on SNMP v1/v2c/v3.

Using the trap mechanism of SNMP, FOXMAN-UN informs the HLM about the following:

- Information on alarms (new, outstanding, acknowledged and cleared alarms), which includes the alarm text, identification, time and date of alarm, and the severity;
- Notification of the addition and deletion of network elements and units within it;
- Changes in operational state of the network element.

The possibility for sending traps to two different HLM systems is supported. This is required in a redundant system, where one HLM system protects the other one.

A standard SNMP «get» request from the HLM provides inventory information such as the lists of installed NEs and their configured units.

1.4.7 Reach Through

With SNMP proxy agent it is possible for the IDM or OSS to keep track of the major changes which are happening in real time in the managed network. If the IDM wants to make NE configuration changes, a proxy server in the FOXMAN-UN provides a reach through functionality to:

- Login from the HLM using a Unix remote shell mechanism.
- As Login parameters the HLM provides:
  - NE ID (based on the ID given in the information reported by the SNMP Agent from the NE list),
  - Login type (prompted login will prompt for a username and password).
- Once the user is logged in, a single graphic will be displayed at the HLM; this graphic will show the NE shelf. The operator may then proceed to carry out any configuration changes he wishes for the NE on the FOXMAN-UN.

In this way the HLMs do not need to keep a database and can concentrate on the inter domain and service management.

1.5 The Managed Network Environment

1.5.1 FOX61x Management Environment

1.5.1.1 General

The FOX61x management network is based on Ethernet. The local management port (Ethernet for FOX61x) is used solely for local connection and initial configuration of the NE.

1.5.1.2 Management Interfaces

The FOXMAN-UN accesses the NE via an Ethernet network (optical 1/10/40 GbE or electrical 10Base-T, 100Base-TX, 1000Base-T).

FOX61x NEs offer a connection to a dedicated Ethernet management interface of the core unit (CESM1, CESM2, CESM3), or via an in-band connection. The NE management communication is based on TCP/IP.

Please note:
When using OSPF in the management network of FOX61x nodes make sure to configure the source IP addresses for the different applications on the “managementNetwork” access point of the FOX61x nodes. We recommend the use of loopback interfaces for this purpose.

If these source IP addresses remain unconfigured the FOXMAN-UN will not be able to assign some of the notifications received from FOX61x nodes to the correct node. This will result in messages of the type “Missing Multiple Notification Messages” in the FOXMAN-UN event log.

1.5.1.3 In-band Management

NEs can also be managed in-band via a trunk Ethernet interface (optical GbE or electrical 10Base-T, 100Base-TX, 1000Base-T) with VLAN tagged management traffic. The management VLAN can be configured in the FOX61x.

1.5.2 FOX51x Management Environment

1.5.2.1 General

Before being able to manage a network of FOX51x network elements, it is necessary to establish a management network and define the approach in which the FOX51x network is to be managed.

The following sections describe how the management network is established and the possibilities that the FOXMAN-UN provides.

1.5.2.2 Management Interfaces

The FOX51x network elements provide 3 different types of management interfaces. These are summarized in the table below, along with the various possibilities to establish the management network.

Table 1: Management Interfaces

Network Elements		FOX515	FOX512	FOX-U	FOX-U/E
Management Interface	F(RS232)	X	X	X	X
	Q1(RS485)	X	X	X	X
	Qx (10BaseT)	X	X		
In-Band Communication Channel	EOC (Embedded Operations Channel)	X	X	X	X
	ECC (Embedded Communication Channel)	X	X		
Out-of-Band Management	Management via Terminal Server and Router	X (1)	X (1)	X (1)	X (1)
	Management via LAN	X (2)	X (2)		

(1) Connection directly from a terminal server or router to the F interface.
(2) Connection to the Qx interface (10BaseT) of the control card of FOX515/FOX512.

1.5.2.3 In-band ECC sub-networks for FOX515/FOX512

With the FOX515/FOX512 a communication concept based on the Embedded Communication Channel (ECC) is used.

In the case of FOX515, the connectivity of the ECC sub-network is carried out internally. In this way there is no need to extract the management channel and connect it to the Qx Interface.

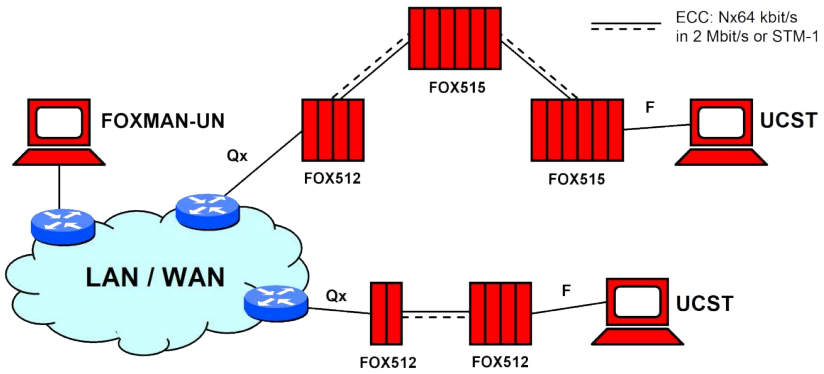


Figure 6: In-band ECC subnetworks for FOX51x

1.5.2.4 Mixed Networks and Interworking of ECC & EOC Sub-networks

FOXMAN-UN caters for networks consisting of FOX-U, FOX-U/E, FOX515, and FOX512. In this case FOXMAN-UN can communicate with both ECC.

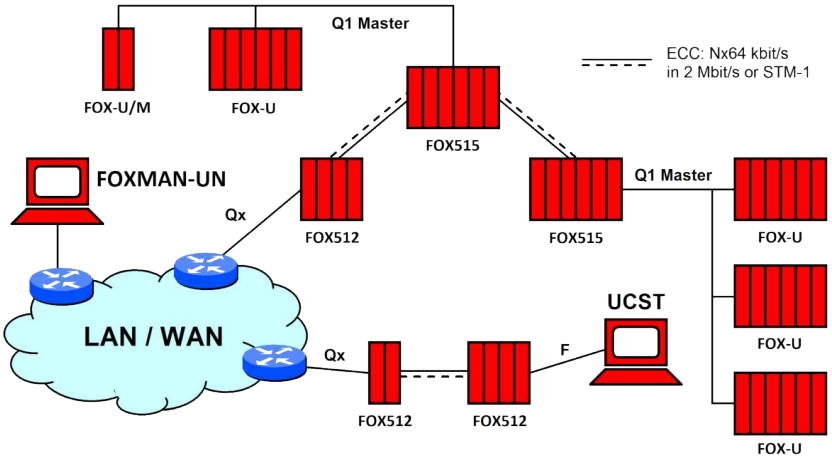


Figure 7: Mixed Networks and Interworking of ECC & EOC Sub-networks

1.5.2.5 Out-of-band Router Management Sub-network

Out-of-band router functionality should be used if it is necessary to separate the management sub-network from the transport network. FOXMAN-UN provides a possibility for the management communication data to be transported over a Data Communications Network (DCN), e.g. LAN, X.25 or frame relay network, etc., using routers.

In the case of FOX515/FOX512, a router at the remote site is not necessary, as the Qx interface of the FOX515/FOX512 can be connected directly to the LAN.

The management sub-network can be implemented as a mixture of both in-band ECC sub-network, and out-of-band router management sub-network.

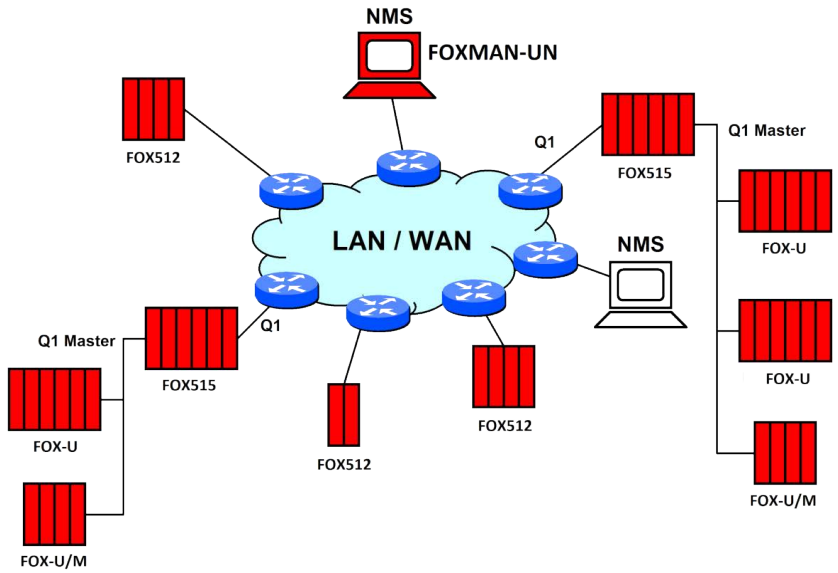


Figure 8: Out-of-band Router Management Sub-network

1.5.3 “FO” NEs Management Environment

NEs of type FO (foreign object) can be integrated into the management network. They require their own agent of type FO. Usually, they are managed with their own craft terminal, or via their built-in browser-based application that can be cross-launched from the NEM Configurator or from the NEM Network Browser.

1.5.4 SNMP Management Environment

1.5.4.1 General

FOXMAN-UN offers a southbound SNMP interface to cater for the management of suitable third party devices.

A FOXMAN-UN element agent can be configured to provide a SNMP agent manager. This agent manager supports SNMP v1, v2c and v3. SNMP devices can be assigned to such an element agent.

Management of SNMP devices is based on Ethernet.

1.5.4.2 Management Interface

The FOXMAN-UN accesses the SNMP devices via an Ethernet network. The SNMP device management communication is based on TCP/IP.

2 NEM Graphical User Interface

2.1 NEM Login

The NEM Login dialog allows starting the NEM Desktop while connecting it to the NEM server (core). It is also used to set up server redundancy, i.e. the main/standby functionality.

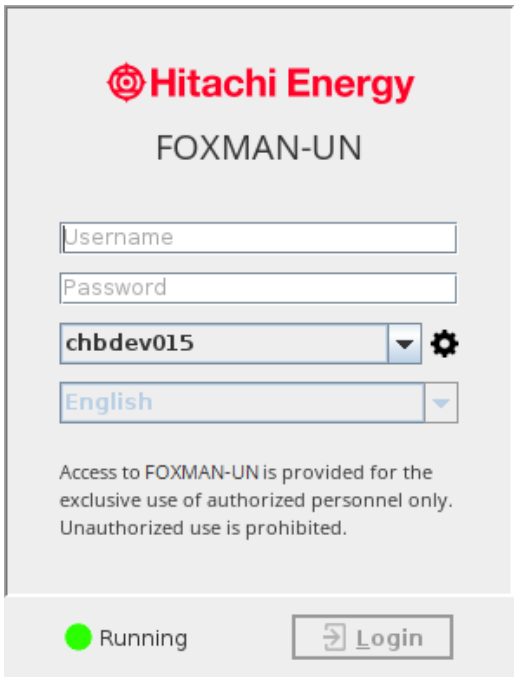


Figure 9: NEM Login

The username and password will authenticate a user. The username must be an authorized FOXMAN-UN user.

When logging in for the first time, the client user needs to accept the server certificate to enable login.

The Language option field is only selectable when language packs are installed on the server.

2.2 Host Manager

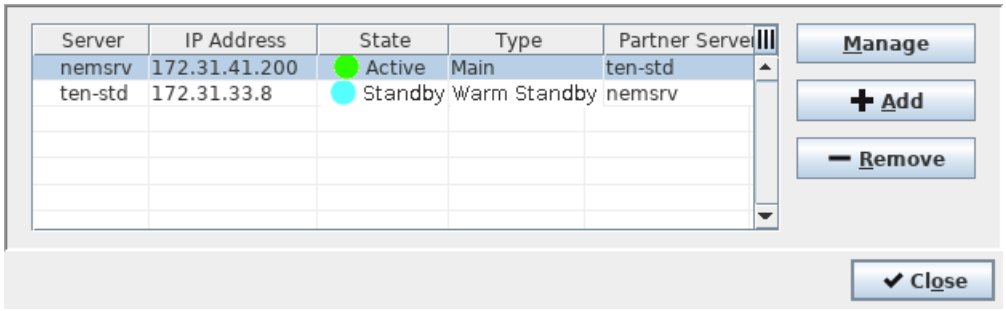


Figure 10: NEM Login

The Host Manager dialog is called from the settings icon in the NEM Login dialog. It is used to add and remove NEM servers, and to set up server redundancy via the NEM Remote Admin Tool.

2.3 NEM Desktop

The NEM Desktop is the control panel from where all the FOXMAN-UN functions and access to the NEM Help System are started.

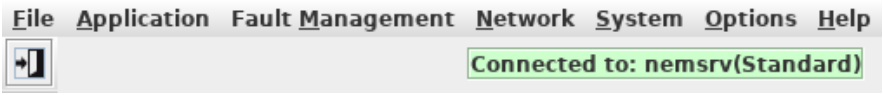


Figure 11: NEM Desktop GUI

2.3.1 File

The File menu allows the user to exit (log out) from the NEM Desktop.

2.3.2 Applications

Applications are started from the NEM Desktop “Application” menu.

- Homepage

  The homepage is the **browser-based home for all UI applications** provided with FOX-MAN-UN, i.e., all browser-based applications and legacy applications. At startup, it shows an overview with
  - Alarms summary,
  - Services Supervision summary,
  - Clock synchronization information,
  - Servers information,
  - System host information, and
  - Application shortcuts.

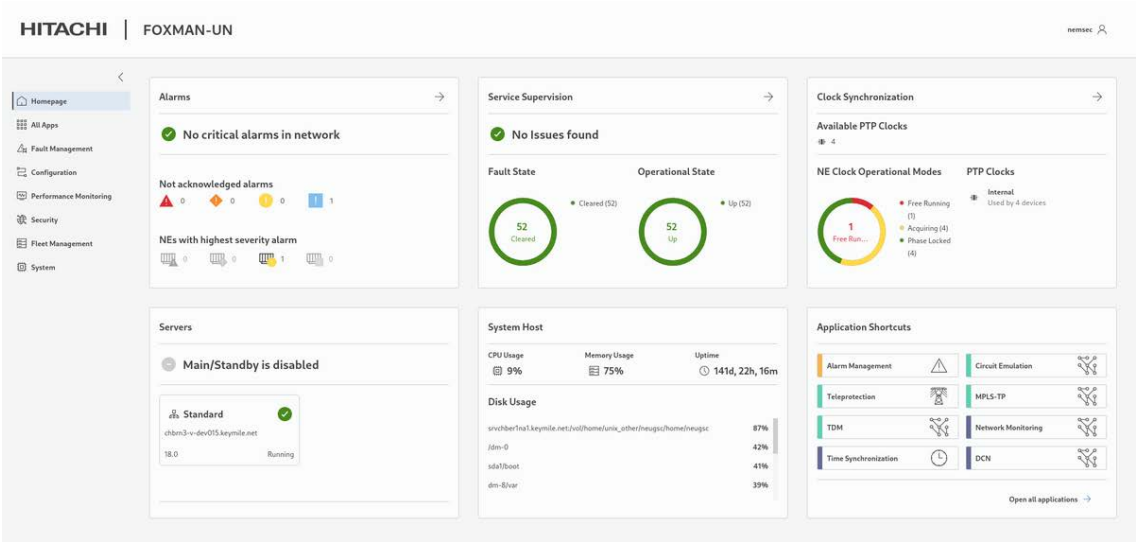


Figure 12: Browser-based homepage with basic network and system information (sample)

The homepage includes links to
- all Web UI applications and
- all legacy applications that can also be reached from the NEM Desktop menu.

The applications are listed as tiles with an icon and their respective name. They are grouped by the categories:
- All Apps (with tiles to start each application),

- Fault Management,
  - Service Supervision
  - Alarm Management
- Configuration,
  - Circuit Emulation,
  - Teleprotection,
  - MPLS-TP,
  - TDM,
  - Spanning Tree,
  - Element Management,
- Performance Monitoring,
  - Network Monitoring,
  - Time Synchronization,
  - DCN,
- Security,
  - Credential Distribution,
  - DIRAC & FU Credential Management,
  - Ethernet Security Manager,
  - User and Role Management,
- Fleet Management
  - Inventory,
  - Profile & CPS Tasks,
  - ESW Network Overview,
  - ESW Distribution Wizard,
  - ESW Task Management,
  - ESW Job Management,
- System,
  - System Event List,
  - Remote Executor.

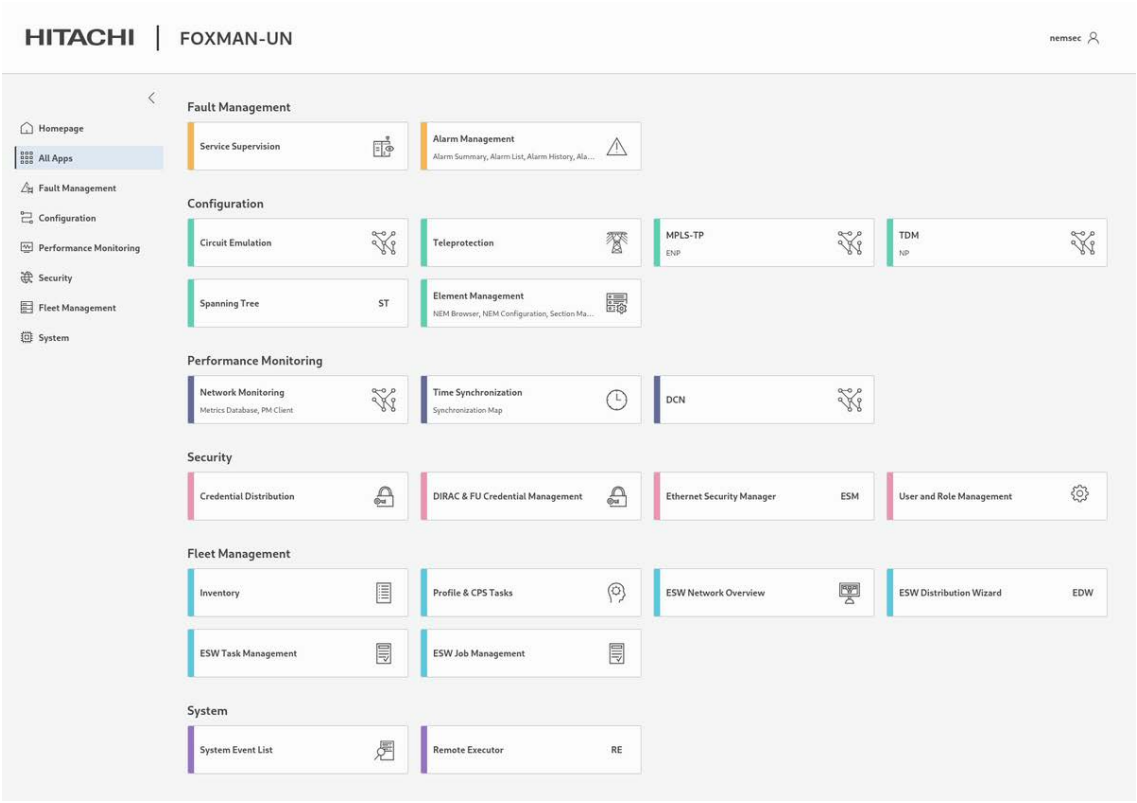


Figure 13: Browser-based homepage with application overview “All Apps”

- The main applications available from the NEM Desktop menu are listed below:
  - NEM Network Browser:

    The Network Browser provides the operator with a graphical view of the network in the form of maps to supervise the network and carry out the day to day management of the network elements.
  - NEM Configurator:

    The Configurator allows setting up all the details of the management network and defining the security aspects. In addition it provides access to the NE configuration management and limited access to the fault management.
  - Section Management:

    The Section Management allows creation, modification or deletion of section(s) and launch of the NP GUI for the specific section. The dialog likewise displays all sections of the managed network, regardless of any map that may be opened.
  - Networking Package (NP):

    The Networking Package provides an end-to-end provisioning of circuits and trails across FOX51x or FOX61x TDM-based legacy networks.
  - Ethernet Networking Package (ENP):

    The Ethernet Networking Package provides an end-to-end provisioning of MPLS-TP tunnels, pseudo wires, VPLS, and VPWS services across FOX61x networks.
  - Ethernet Security Manager:

    The Ethernet Security Manager provides all controls for managing Ethernet security like MPLS-TP encryption, setting up Crypto Engines, and defining mappings of encryption termination points and ports for MPLS-TP tunnels.
  - Service Supervision:

    The Service Supervision and Reporting allows end-to-end network services monitoring. It runs regular reports regarding end-to-end service availability, particularly related to any

Service Level Agreements that may exist. In the current release, System Services and Advanced Services are distinguished.

- Circuit Emulation

  The Circuit Emulation Manager (CEM) provides an overview of Circuit Emulation Services (CES) in FOX61x networks, including alarm monitoring, a list of possible issues, graphics on clock operation modes, Pseudo Wire (PW) protocols, CES profiles, packet traffic statistics and alarm history. It also lists end-to-end TDM services, CES, and VPWS in separate tables.

- Homepage

  The Homepage is described at the beginning of this section “Applications”.

The following application provides system administration options:

- Remote Admin Tool:

  The Remote Admin Tool is available for the FOXMAN-UN Linux client only. It is not available for the FOXMAN-UN client for Windows®.

  It provides access to all other administration sub-areas:

  - License Information:

    The NEM License Information is used to display and monitor the License Key required for running the application. In addition, a license file can be uploaded from a file system.

  - Manage Authentication Keys:

    This dialog is used to create, activate, delete, and export authentication keys for the secure FOXMAN-UN to FOX61x management communication.

  - Start/Stop Services:

    The Start/Stop Services dialog offers a graphical interface for monitoring the status of NEM base and core services, starting and stopping the NEM core services, restarting selected services, performing a resynchronization of NP data, and showing the status of Element Agents.

  - Show Element Agents:

    The Element Agent window is used to display status information of the agent processes supporting the communication to the Network Elements.

  - Inventory Information:

    Used to display server related inventory information, such as disk mount points and usage, memory usage, and CPU usage information.

  - Database Backup:

    Provides three separate GUI dialogs to:

    - Schedule periodic, daily, weekly. and/or monthly database backups,

    - Create and delete manual database backups,

    - Restore manually or automatically created database backups.

  - Main/Standby Configuration:

    Provides GUI dialogs to configure server redundancy via the setup of main and standby server types, assign these servers to each other, and make one of the servers the active one.

2.3.3 Fault Management

The Fault Management menu provides access to the following alarm management functions:

- Alarm Summary:

  Calls the network alarm summary showing the currently active alarms of all NEs, FOs and Services managed by the FOXMAN-UN,

- Alarm List:

  Calls the alarm list containing the currently active alarms of all NEs, FOs and Services managed by FOXMAN-UN.

- Alarm History:
  Calls the dialog for the retrieval of cleared and acknowledged alarms. In the default setting, alarms of the fast 30 days are stored in the history files.
- Alarm Customization:
  Calls the dialog for the modification of the alarm criteria on a global or NE basis.

2.3.4 Network

The Network menu provides access to the following functions:

- Performance Management
  Opens the user interface for the configuration of the performance data collection.
- Inventory Request
  Calls the Request Inventory Report dialog where a report can be configured by selecting the report type and either the relevant NEs or NE types. The report can be displayed on the screen and/or saved as XML or CSV file.
- Synchronization Map (for TDM based services)
  Calls a dialog where a map of the synchronization paths for a selectable number of NEs can be generated.
- PTP Sync Map
  Opens a map displaying the PTP synchronization network diagram, based on the selected managed network similar to the NEM Network Browser. The PTP related information is shown for each of the NEs in the network.
- Spanning Tree
  Displays a map of STP or RSTP instances in Ethernet networks.
- Task View
  Displays an overview of existing tasks. Selected tasks can be executed, aborted, resumed, retried or deleted.
- NE Password Tasks
  Calls a list of the current NE Password tasks. Existing tasks can be monitored, modified or deleted. From this dialog, new tasks can be added.
- Profile and CPS Tasks
  Calls a list of the current Profile/CPS tasks. Existing tasks can be monitored, modified or deleted. From this dialog new tasks can be added. Importing and exporting Profiles and CPS as well as creation of new Profiles are likewise possible.
- ESW Tasks
  Calls a list of the current legacy ESW tasks related to FOX51x-based legacy networks. Existing tasks can be monitored, modified or deleted. New tasks can be added
- Credential Distribution
  Calls the Network Credential Distribution dialog that supports password change on supported NE types, management of SSH keys for secure authentication on supported NE types, and a task manager for password distribution and creation, download, activation, and deletion of public / private keys.
- ESW Management
  Provides a number of Embedded Software (ESW) Management related features such as an overview of all ESW installed in the network, an ESW distribution wizard to allow easy ESW distribution and upgrade to new releases, a job management definition dialog, and a task management dialog to supervise scheduled, running, and finished ESW distribution tasks.

2.3.5 System

The System menu calls

- the Event List (legacy application) table, which lists all major system events and activities carried out by the FOXMAN-UN applications kept in the FOXMAN-UN database. Up to 100,000 events can be stored. The overflow is saved into history files.
- the Remote Admin Tool; this tool is used to set up redundancy by activating a main/standby setup. Also refer to Standby System.
  It is also used to:
  - manage server machines to connect from the client,
  - define database backup plans,
  - manage database backups,
  - manage licenses,
  - manage authentication keys for secure connection to FOX61x nodes,
  - start and stop FOXMAN-UN services.
- the Remote Executor; this tool is used to execute scripts for various administration functions.
- the Metrics Database, an integrated third party application that provides you with means to create a variety of graphs out of collected performance monitoring data.

2.3.6 Options

The Options menu provides access to the following functions:

- Preferences (Global Preferences)
  Provides a number of preferred GUI parameters that can be set for
  - Maps: use of new map and graphic symbols style;
  - Colors: use of a new color scheme, and selection of colors for alarm categories;
  - Tunnel Editor: enable or disable the option to show LSP graphs;
  - Tables: Enable or disable automatic column resizing;
  - Look & Feel: select a GUI theme, and enable or disable enhanced contrast.

2.3.7 Table Filters

Any table present in the GUI has either a filter feature built in by default, or the filter can be enabled/disabled by pressing “CTRL-F” (STRG-F) on the keyboard. The filter feature supports wildcards and regular expression patterns, which the user can select by pressing the search filter icon on the left hand side of the filter field.

2.3.8 Help

The Help menu provides access to the FOXMAN-UN Help viewer (Help) and displays the software version of the installed FOXMAN-UN (About).

2.4 NEM Configurator

2.4.1 General

The NEM Configurator allows defining the network to be managed as well as setting up the security system.

The NEM Configurator is implemented in the style of a browser showing a **tree panel** on the left and a **details panel** on the right. Below is the **Activity List.**

All configuration functions can be accessed via context menus either from the tree or the details panels.

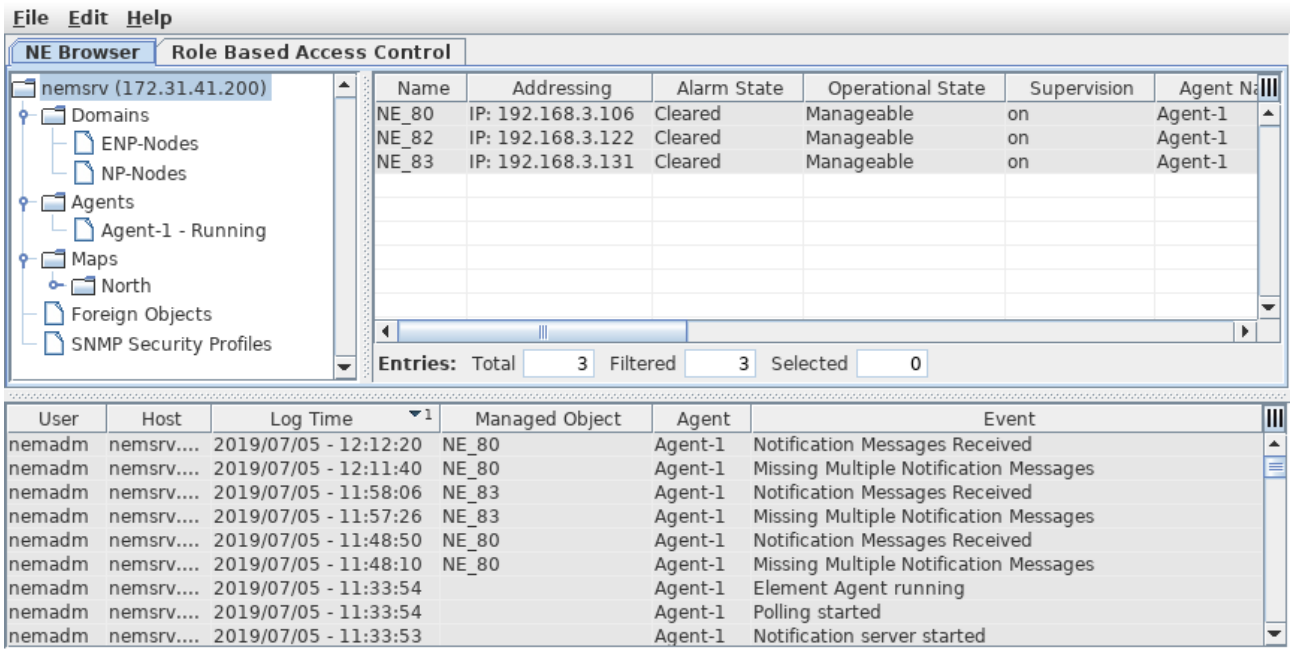


Figure 14: NEM Configurator

In a second tab, the NEM Configurator provides the means for management of role-based access control (RBAC). This dialog provides

- management of security domains,
- predefined security profiles,
- user creation and management and roles assignment, and
- roles management for system roles and user-defined roles.

Also refer to section 3 "Security Administration" for more details.

2.4.2 NE Browser

2.4.2.1 General

Defining the managed network consists of configuring the **agents** which are responsible for the communication with the network elements and then assigning the **NEs** to them. If required, Foreign Objects have to be created.

2.4.2.2 Standard Procedure

Usually the specific details of the management network have been compiled in the form of name lists and address lists for agents and for their network elements. It is then a matter of entering these data while creating the agents and assigning the network elements.

2.4.2.3 NE Discovery

For the instances where the network elements in the field are not known, FOXMAN-UN offers a discovery tool.

For a selected agent, this tool scans the specified address range and automatically creates the discovered NEs in the FOXMAN-UN database. It generates a name that contains a date / time stamp. This name can then be modified as required.

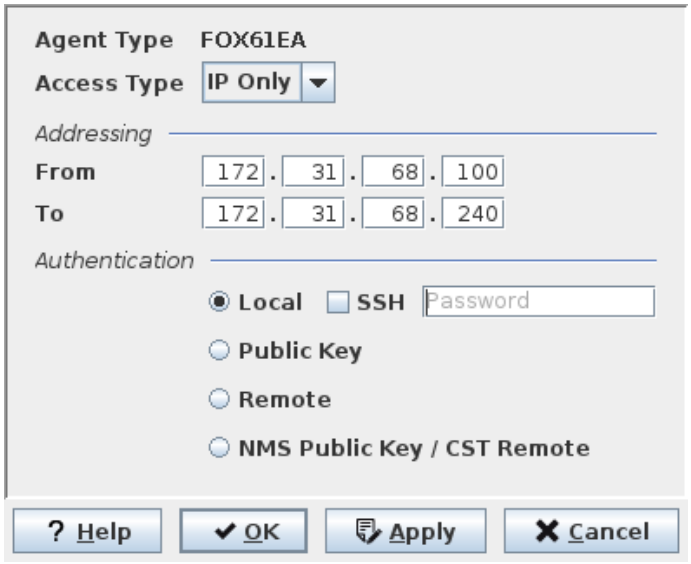


Figure 15: NE Discovery Request

This way the FOXMAN-UN operator can quickly populate the database. The remaining task is the renaming of the network elements.

2.4.2.4 NEs of Type 'Foreign Objects'

NEs of type Foreign Object are defined by name, description (Location and Tag) and TTPs (Trail Termination Points) which are required if sections have to be terminated at the FO.

If alarms are to be associated with a FO,

- in a FOX51x NE, use an ALCAR unit as physical alarm input, and configure alarms via the FOX51x local craft terminal UCST;
- use alarm customization functionality with Port scope.

2.4.3 Security Configuration

Security elements to be configured consist of **Domains**, **Users** and **Roles**. For details about the security concept refer to 3 "Security Administration".

2.4.4 Fault Management

The NEM Configurator gives limited access to the alarm situation in the managed network. The following functions are available if the appropriate access rights exist:

- Alarm Status per NE or for the complete managed network
- Alarm List per NE or for the complete managed network
- Alarm acknowledgment

For FOX51x NEs, alarms can also be accessed via the Hardware Views.

For FOX61x NEs, currently active alarms can also be accessed via the Alarm tab of the FOXCST GUI.

2.4.5 NE Configuration Management

The relevant configuration tool (FOXCST or UCST) can be opened for any NE in the managed network. Configurations can be modified if the appropriate access rights exist.

Please note:
FOXCST and UCST are configuration tools for NE types FOX61x and FOX51x, respectively.

2.4.6 Operational Aspects

The following actions are possible if the appropriate access rights exist:

- Stopping and starting of agents,
- Stopping and starting the polling of specific NEs,
- Request forced polling of specific NEs.

2.5 NEM Network Browser (legacy application)

2.5.1 General

The NEM Network Browser is used to create a set of graphical representations of the managed network called **maps**. Each network element, Foreign Object or System NE is shown as a symbol. Traffic and clock connections between the elements can be shown as lines and are called «Sections».

2.5.2 Maps - Group Maps

A hierarchy of maps can be built by using group maps. A group symbol on a map represents a sub-map that can contain again all types of symbols. Double clicking a group symbol opens up the group map in an additional window. In this way a large network can be structured and the elements on a map can be limited to a reasonable number. Such a map structure could start at a national level containing only group symbols of the regions, continuing with groups showing cities and finally NEs.

There is no practical limitation to the number of levels that can be defined, or to the number and type of symbols used on each level.

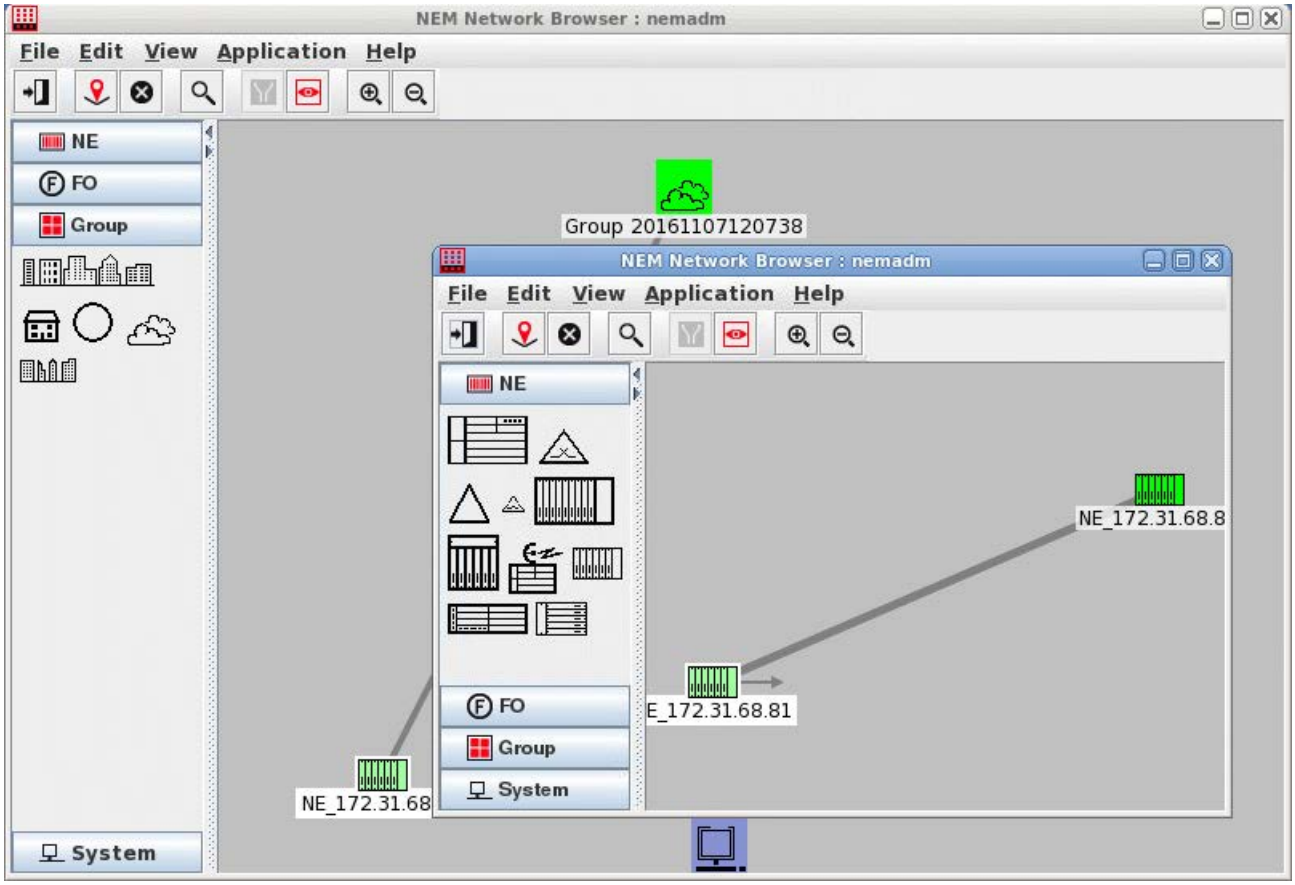


Figure 16: Maps - Group Maps

It is possible to define several maps for the same network according to topology, application, NE type, or any other criteria. Any NE can be placed in more than one map.

2.5.3 Symbols

2.5.3.1 Standard Symbols

The set of symbols is part of the FOXMAN-UN standard installation. Further customized symbols can be created by the user and imported. The symbols to be imported have to be created in the PNG format. A new map style provides additional, new symbol graphics in addition to the legacy graphics of earlier FOXMAN-UN versions.

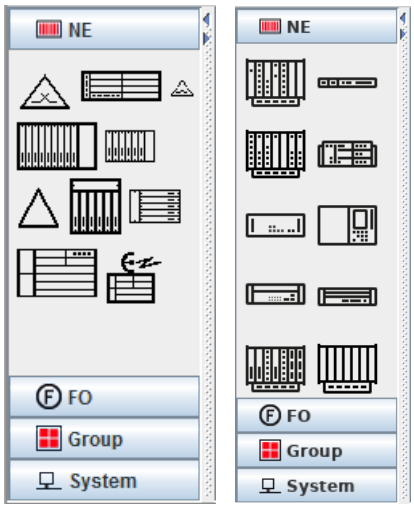


Figure 17: Standard legacy and new NE Symbols

Once placed on a map, each symbol is shown in one of several colors representing its alarm state. The alarm colors of all types of symbols are propagated to their group symbol if it exists. If for instance all group symbols on the main map are shown in green, this means that no element contained in that map structure has active alarms.

For more information on the display of alarm information refer to 4 "Fault Management".

2.5.3.2 Cut and Paste

The operator can, in the map “Edit” mode, using just the mouse, move symbols between main and group maps with a «Cut and Paste» function.

2.5.3.3 Find Symbol Facility

In a large map structure containing many levels of group maps it can be difficult to find a specific symbol. The «Find Symbol» function locates a symbol (NE, FO, group or system) anywhere in a map structure by opening the relevant group map if required and scrolling the view till the symbol is in focus.

2.5.3.4 Alarm Indication

The highest severity of all currently active alarms in a network element is indicated by its color. There are five different severities, with the color green showing a no alarm situation in legacy style.

With the new map style, a no alarm situation is indicated with a non-colored node or NE.

Additionally three flags show a «Polling stopped» situation, a «NE unmanageable» situation and the highest severity of all unacknowledged alarms. With the new map style, the flags have a slightly different graphical design; e.g. the highest severity of all unacknowledged alarms is shown with a specific symbol and color. The figure below shows examples of NE alarm flags for the severities “None”, “Warning”, “Minor”, “Major”, and “Critical”.

Figure 18: Examples of Alarm Flags and Message Flag

The map style and the alarm colors can be determined in the global preferences (see 2.3.6 "Options").

2.5.4 Messages

NEs and FOs can have messages attached to them, e.g. for passing information from one operator to the next. Symbols that have a message attached are marked with an asterisk beside their name. The marking is propagated upwards through the map structure. Group symbols show an asterisk and the number of messages present in the structure below. With the new map style, messages are indicated with a balloon icon (also see Figure 18).

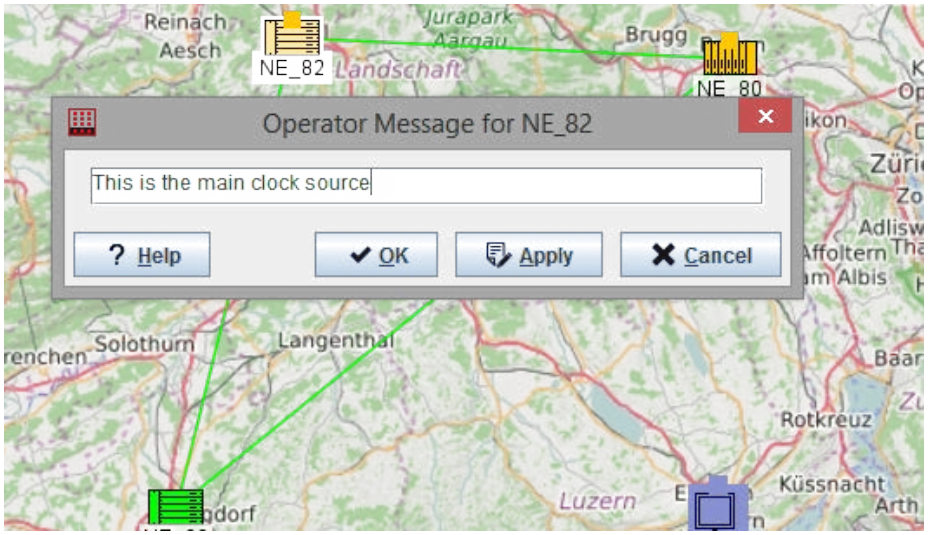


Figure 19: NE Message

2.5.5 Sections

A section represents a physical interconnection between two NEs or between an NE and a FO (foreign object). It is based on the configuration data of the NEs and FOs.

A section is shown as a colored line on a map. Sections are created using the «Section Management» dialog, which lets you fill in all the details.

The line color indicates either inactive operational state (gray) or when active, the highest alarm severity of the sections.

Please note:
The file /opt/nem/etc/sectionalarmmapping.cfg is a NEM configuration file which allows customer-specific section alarm mapping. It allows you to specify if an alarm affects or does not affect a section. For details, please refer to section 11.3 “FOXMAN-UN Configuration Files” of the user manual “FOXMAN-UN under Linux”.

Please note:
The section status is not immediately updated with alarms, e.g. it may take a delay.

The operator can display the section details including circuits or trails running over the specific section simply by double clicking with the mouse to call the «Section Management» dialog. The dialog displays details of the section showing:

- User-defined section name,
- Transmission capacity (layer rate),
- Cost,
- Type of media,
- A and Z end NEs,
- A and Z end TP labels,
- section ID,
- Alarm state (via coloring).

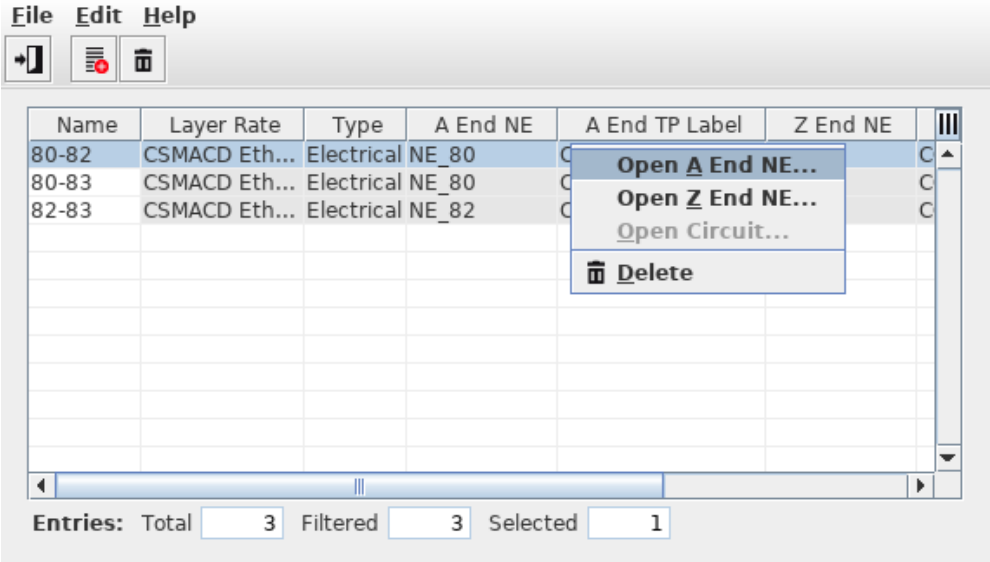


Figure 20: Section Management

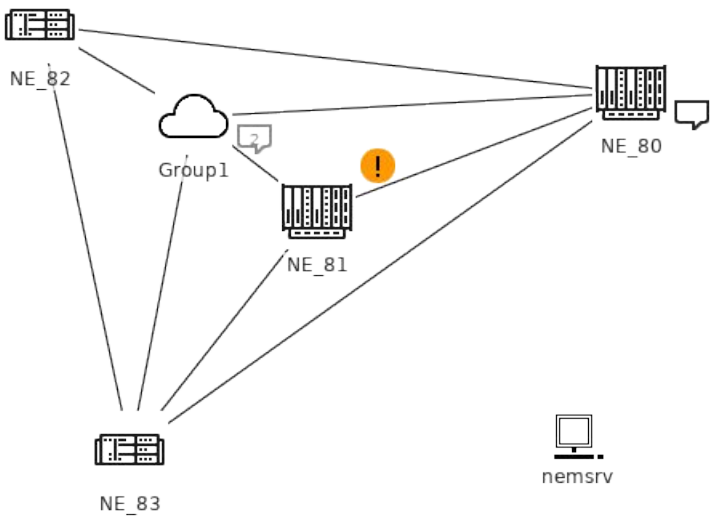


Figure 21: Map Sections

2.5.6 Map Background

The default map background is no image. A customer specific high resolution background images can be added by the operator. The background images to be imported must be presented in the JPG format.

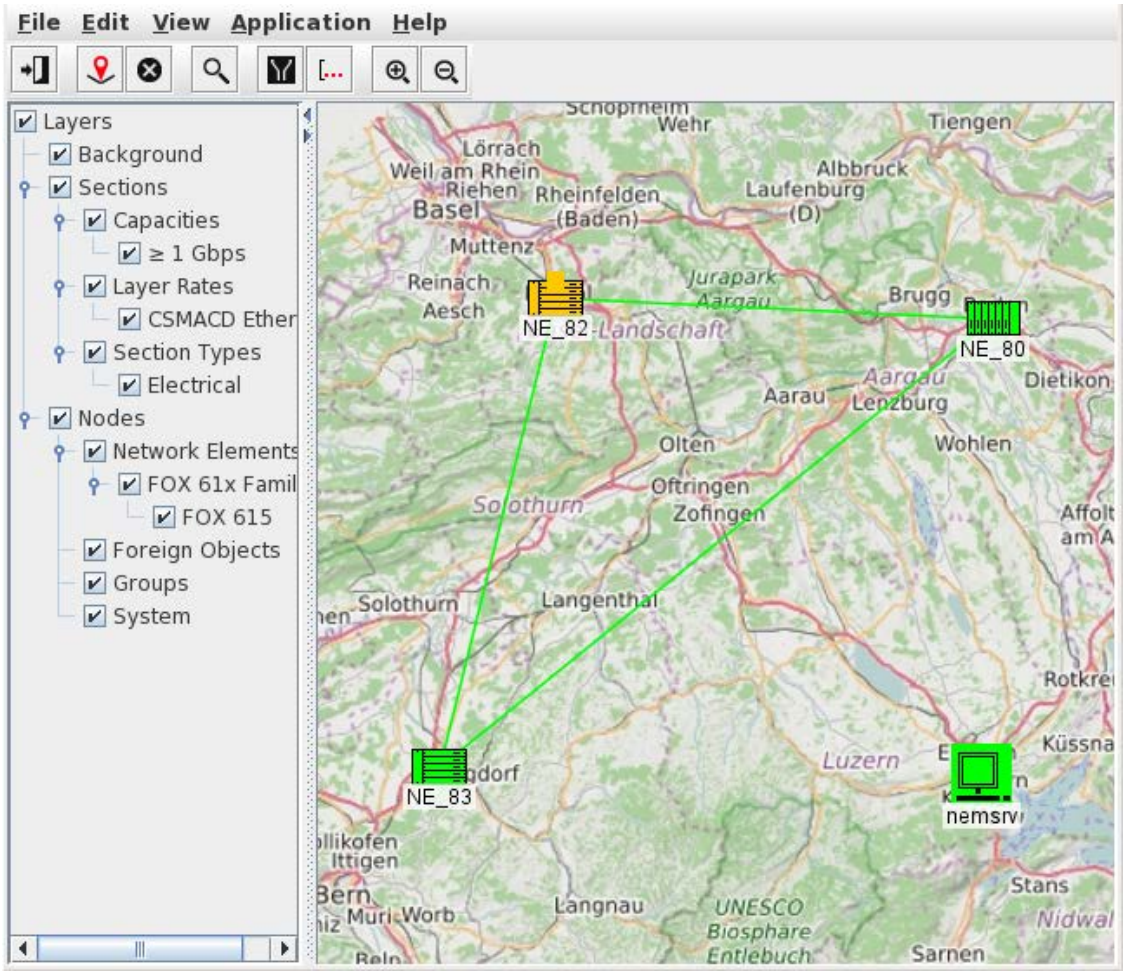


Figure 22: Imported Map Background

2.5.7 Security

User access to individual maps, to individual elements on a map as well as authorized functions for a user are defined by the security system. This is configured using the NEM Configurator.

2.5.8 Fault Management

The NEM Network Browser gives access to the alarm situation in the managed network. The following functions are available if the appropriate access rights exist:

- Alarm status per NE or for the current map,
- Alarm list per NE or for the current map,
- Alarm acknowledgment,
- Alarm summary for the current map.

For FOX51x NEs, alarms can also be accessed via the Hardware Views. For FOX61x NEs, the alarm list of a specific NE is accessed via the context menu of that NE in the map.

2.5.9 Configuration Management

The relevant configuration tool (FOXCST or UCST) can be called for any NE in the current map. Configurations can be modified if the appropriate access rights exist.

2.6 Managed Objects

2.6.1 FOX51x Hardware Views

The FOX51x hardware views are supported only with the FOXMAN-UN client for Windows®.
FOXMAN-UN provides several levels for the visualization of alarms in the FOX51x NEs.

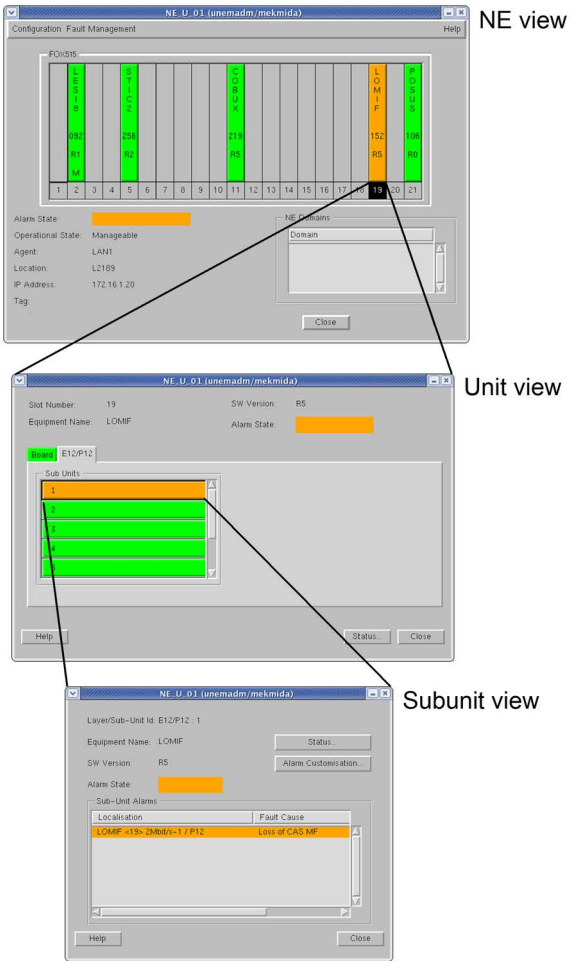


Figure 23: FOX51x Hardware Views

2.6.1.1 Hardware View NE

The operator can display the FOX51x hardware view by double clicking on the corresponding FOX51x symbol.

The hardware view displays the NE subrack with the appropriate units inserted in the appropriate slots as it is actually installed giving:

- NE attributes,
- NE alarm state (color),
- NE alarm text,
- The alarm state (color) of each individual unit.

2.6.1.2 Hardware View Unit

By double clicking on a specific unit, the operator gets all details for the selected unit such as:

- Unit attributes,
- Unit SW Version,
- Unit alarm state (color),

- Unit alarm text,
- The alarm state (color) of each individual subunit.

2.6.1.3 Hardware View Subunit

By clicking on a specific subunit, the operator gets:

- Subunit alarm state (color),
- Subunit alarm text,
- Access to all subunit status information like slip counters and status of signaling bits.

2.6.2 FOX61x Views

FOXMAN-UN provides several levels for the visualization of alarms in the FOX61x NEs.

The NE level alarms are shown in the AP tree of the FOXCST with an NE icon color that corresponds to the alarm severity.

Please refer to FOXCST User Manual for details. The FOXCST User Manual is part of the FOX-61x technical documentation.

2.6.3 NEs of Type Foreign Object

Foreign equipment is not managed by FOXMAN-UN, but can be displayed as NES with foreign object symbols on the maps.

Using a special alarm collecting unit ALCAR in a FOX51x NE, alarms and also commands can be associated with foreign objects. These alarms will then not be treated as belonging to the NE where the unit is located, but are shown as part of the relevant FO. The alarms can be customized to be visible on FO.

2.7 Event List (legacy application)

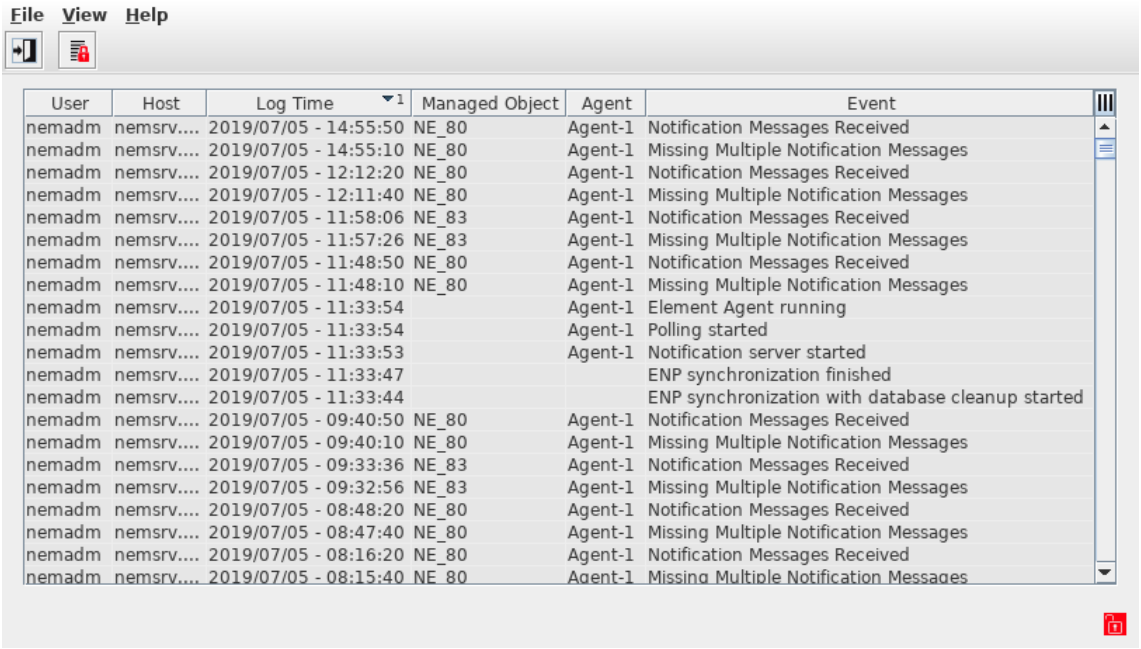


Figure 24: Event List (legacy application)

The Event List provides a list of all the activities being carried out by the FOXMAN-UN application, and events that have occurred. It provides details of all actions and responses which have occurred between the FOXMAN-UN and the network. For each action initiated by the applica-

tion, an indication is provided as to the type of action, the user and workstation where the action was initiated and the time/date stamp when the action occurred.

The information displays in the NEM Configurator's Activity List at bottom panel is the same as the information displays in the NEM Desktop - System - Event List.

Entries in the Event List can be sorted, filtered, searched, exported, and printed.

A System Events list is also available in the browser-based UI. It can be opened in browser-based applications from the "System Events" icon in the top selection bar.

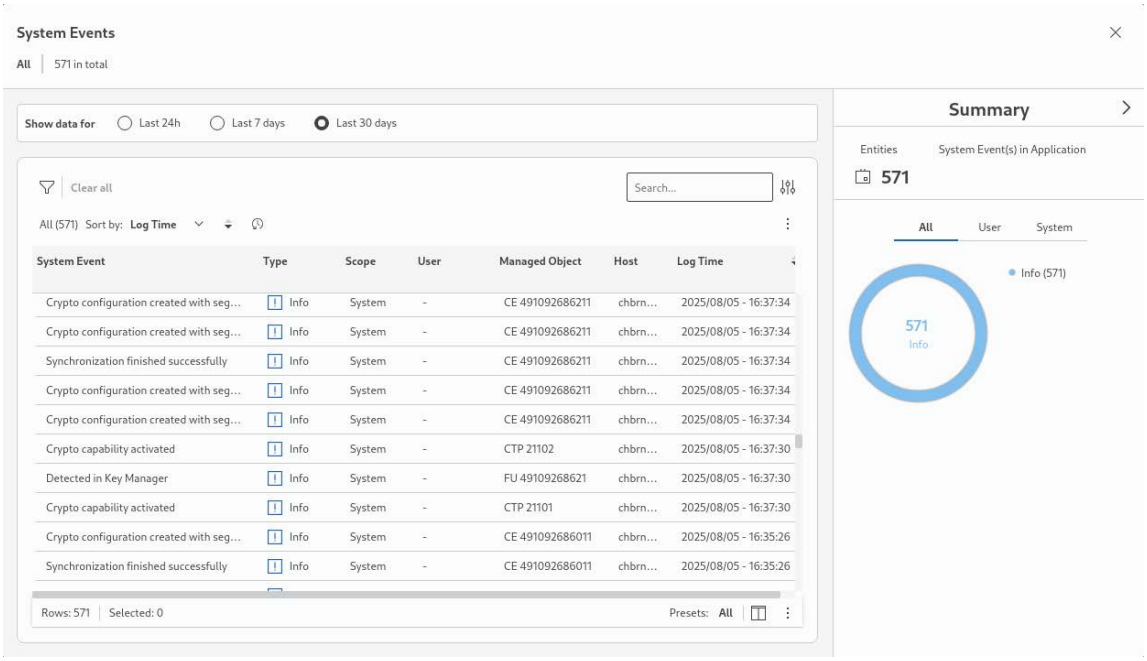


Figure 25: System Event List (browser-based application)

3 Security Administration

3.1 General

FOXMAN-UN security is a very flexible system based on identity and access control commonly known as AAA (Authentication, Authorization and Accounting).

Authentication is based on the operating system as well as on the FOXMAN-UN application. A user is identified on logging into the workstation or PC. A second identification takes place before a GUI can be connected to the FOXMAN-UN database.

Authorization occurs by the means of roles assigned to each FOXMAN-UN user (RBAC), or user privileges and profiles (DAC, legacy). A user is authorized or not authorized to perform the defined FOXMAN-UN functions.

Accounting consists of the activity logging capabilities of FOXMAN-UN. All security operations (amongst others) are logged and stored in history files for later auditing.

Please note:
FOXMAN-UN Security elements are described in details in the following sections of the “FOXMAN-UN NEM Help System” User Manual:

→ chapter “NEM Configurator - Role Based Access Control”,

→ chapter “SNMP Security Profile - Create/Properties,

→ chapter “Security Configuration”.

3.2 Role-based Access Control (RBAC)

RBAC has been introduced with system release R17A. It provides user permission control via roles assigned to a user.

3.2.1 System Roles

The following system roles are predefined:

- Viewer,
- Operator,
- Engineer,
- Installer,
- Secadm (Security administrator),
- Rbacmnt (RBAC management).

Each of these roles has an access permission level assigned for each specific function category.

Access permission levels include:

- No access,
- Read access,
- Full access,
- Disabled,
- Enabled.

Function categories include the following areas:

- Network engineering:
  - Section management,
  - Network design,
  - Traffic engineering,

  - Node aggregation,
  - Ethernet security management,
  - Remote execution.
- Network monitoring:
  - Service supervision,
  - Performance monitoring,
  - Alarm configuration,
  - Alarm management.
- System management:
  - Role based access control,
  - Credential management,
  - Remote administration,
  - Administration.
- Node management:
  - Node restore configuration,
  - Profile & CPS management,
  - Software management,
  - Node access Information,
  - Node access maintenance,
  - Node access manager,
  - Node access session manager.

3.2.2 User Defined Roles

Individual user-defined roles can be added with a name and description, and with access permission levels for function categories and areas in accordance with the operator’s specific requirements.

3.3 Administrators

FOXMAN-UN has two types of administrators who can set different levels of user security.

- Workstation & Linux System Administrator

  Is typically from the computer systems department and has the responsibility for creation and deletion of workstation users at the Linux level.
- FOXMAN-UN Administrator

  In general, FOXMAN-UN administrators are responsible for:
  - Defining the domains and their managed objects;
  - Defining the user roles;
  - Assigning roles to FOXMAN-UN users created by the Linux system administrator.

  Using the system roles and user-defined roles, the security administrator can create various function levels for administrators and operators and make them valid for all or only part of the managed network via the domains.

3.4 Network Partitioning

Using the domains, the network can be divided into a number of security areas. Users can be allocated one or several domains for specific functions.

The domain allocations can be made for a limited period. This feature can be used to cross network partitions for backup purposes, holiday assignments, and so forth.

4 Fault Management

4.1 Introduction

The key requirement of any Network Management system is to detect any faults, inform the operator, and provide the means to take appropriate actions to remedy the fault.

Fault Management in FOXMAN-UN can be subdivided into two areas:

- Alarm Handling,
- Status Monitoring.

Fault Management is one of the main menu entries in the NEM Desktop. The fault management menu provides the functions:

- Alarm Summary,
- Alarm List,
- Alarm History,
- Alarm Customization.

The resulting lists from each of these functions can be filtered/sorted as well as printed or exported for further analysis if required.

The Alarm List can also be called from both the NEM Configurator and the NEM Network Browser from a specific NE.

4.2 Alarm Handling

4.2.1 General

The first instance in the handling of alarms is the NE. Alarms are generated there and then handed over to the FOXMAN-UN.

The NE continuously monitors its input signals and detects if any of them are missing or faulty. Any alarms that are generated as a result of this supervision are stored in the on-board **Logbook**. They are then uploaded from there by FOXMAN-UN during the next poll of the NE and presented to the operator.

4.2.1.1 Alarm Notification

The FOX61x and FOX51x families have the capability to signal to the FOXMAN-UN the presence of a new alarm. Upon generation of a new alarm the NE sends a notification to the FOXMAN-UN, which in turn polls the NE out of sequence. This speeds up the reporting of alarms while at the same reducing the amount of traffic in the management network.

FOXMAN-UN likewise can handle alarms that include delayed creation, external indication via an external device, and sending alarm notifications via email.

4.2.1.2 Main Functions

Alarm handling in FOXMAN-UN provides the following main functions:

- Alarm Summary,
- Alarm List,
- Alarm filtering,
- Alarm acknowledgment,
- Alarm localization,
- Section alarms,
- Alarm notification for Foreign Object alarms,
- Alarm notification via E-mail,

- Alarm Escalation,
- Work Instructions,
- Alarm printout,
- Alarm Customization:
  - Changing of fault cause text and severity for all or selected NEs, for all or selected units and /or subunits,
  - Intermittent alarm blocking,
  - Alarm OFF setting for undesired alarms.
- Alarm history,
- Activity history,
- Logbook function,
- Loss of communication alarm (Network Management System to NE).

4.2.2 Alarm Summary

4.2.2.1 Alarm Summary Display

The Alarm Summary gives an overall view of the alarm situation for the total network (from the NEM Desktop) or within a map (from the NEM Network Browser, or from the expanded Alarm Summary). It shows the number of currently active alarms for each severity as well as the number of cleared but not acknowledged alarms.

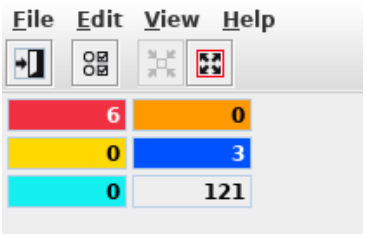


Figure 26: Alarm Summary, Shrunk Display

When the network elements are polled, or if notifications are received from the network elements, the operator is notified of any new alarms via the Alarm Status as follows:

- Increase of the counter for the appropriate severity;
- Blinking of the appropriate counter and colored toggle;
- Audible alarm (if enabled).

For each alarm counter the appropriate alarm list can be called with a double click of the mouse.

The alarm summary window can be shrunk or expanded. When expanded, it shows the alarm counts including the severity labels.

Figure 27: Alarm Summary Full

4.2.2.2 Alarm Status Filter

The blinking of counters and the audible alarm can be customized via the alarm summary options. Blinking and audible alarm can be enabled down to and including a user definable threshold severity.

Default is blinking enabled for all severities included «Cleared» and audible alarm disabled.

4.2.2.3 Alarm Severities

FOXMAN-UN supports five alarm severities according to TMN standards. They are indicated using the following colors:

Table 2: Alarm Severities

Severity	Displayed Colour
Critical	Red
Major	Orange
Minor	Yellow
Warning	Blue
Indeterminate	Light Blue

In addition green is used for a no alarm situation and for alarms with customized severity «Off». «Cleared» alarms are colored pink in the alarm summary.

4.2.3 Alarm Customization

4.2.3.1 Global

The alarm behavior can be adapted to the requirements of the network operator.

A customized alarm can be defined for the following scopes:

- on a Network level (a customization is valid for the selected unit in the entire managed network);
- on a Domain level (a customization is valid for a selected unit in a domain);
- on an NE Type level (a customization is valid for a selected unit in all NEs of one type);
- on an NE level (a customization is valid for the selected unit of one or several NE(s));
- on a Port level (a customization is valid for the selected unit in a specific slot of an NE).

The customized alarms (including those generated via the hardware views) are listed at the top of the dialog indicating

- Scope,
- Selection,
- Unit,
- Location,
- Old Alarm Text (FOXMAN-UN default alarm text),
- Old Severity (FOXMAN-UN default severity),
- New Alarm text (modified alarm text if applicable),
- New Severity (modified severity if applicable),
- Transfer to FO (applicable to Port Scope only),
- Intermittent Period,
- Work Instructions.

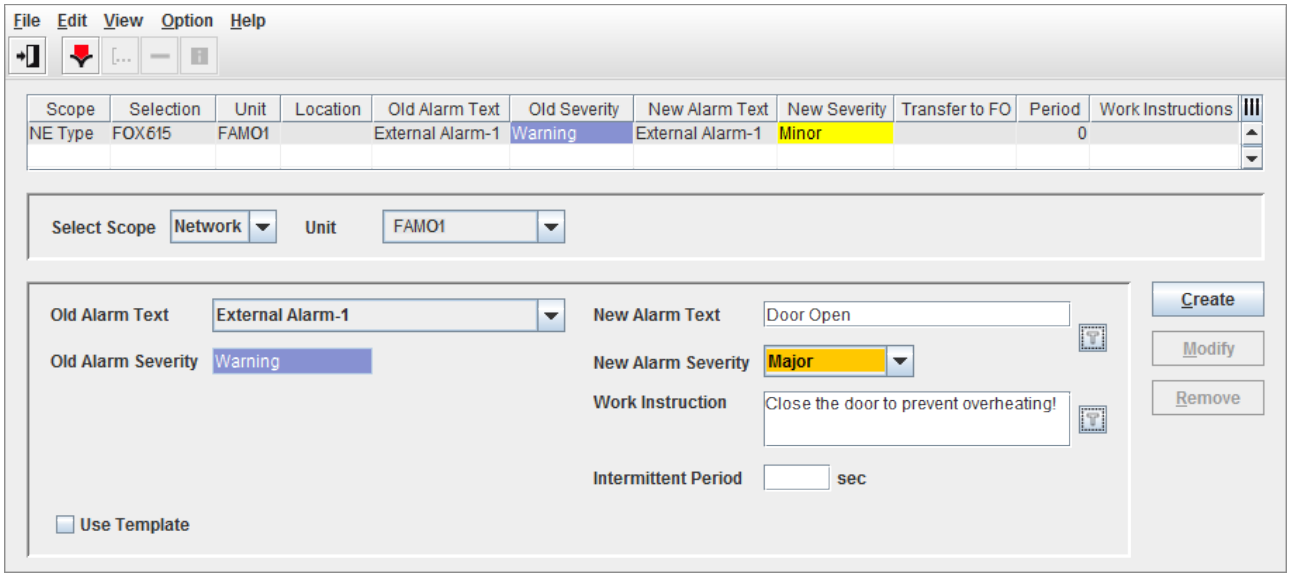


Figure 28: Alarm Customization - Global

The Alarm Customization templates ease the creation steps of Alarm Customization. There are 4 types of templates that the operator can create:

- Alarms & Severity,
- Work Instructions,
- Unit Alarms,
- Unit Port Alarms.

The operator can use these templates when creating customized alarms. The Unit Alarms and Unit Port Alarms templates can be used to create multiple customized alarms for a specific unit or port.

4.2.3.2 Units/Subunits

The default settings for fault cause text, severity and intermittent alarm blocking can also be modified individually for each alarm on a unit and subunit level. The customization dialog is called from the hardware views (FOX51x network elements only; FOXMAN-UN client for Windows® only).

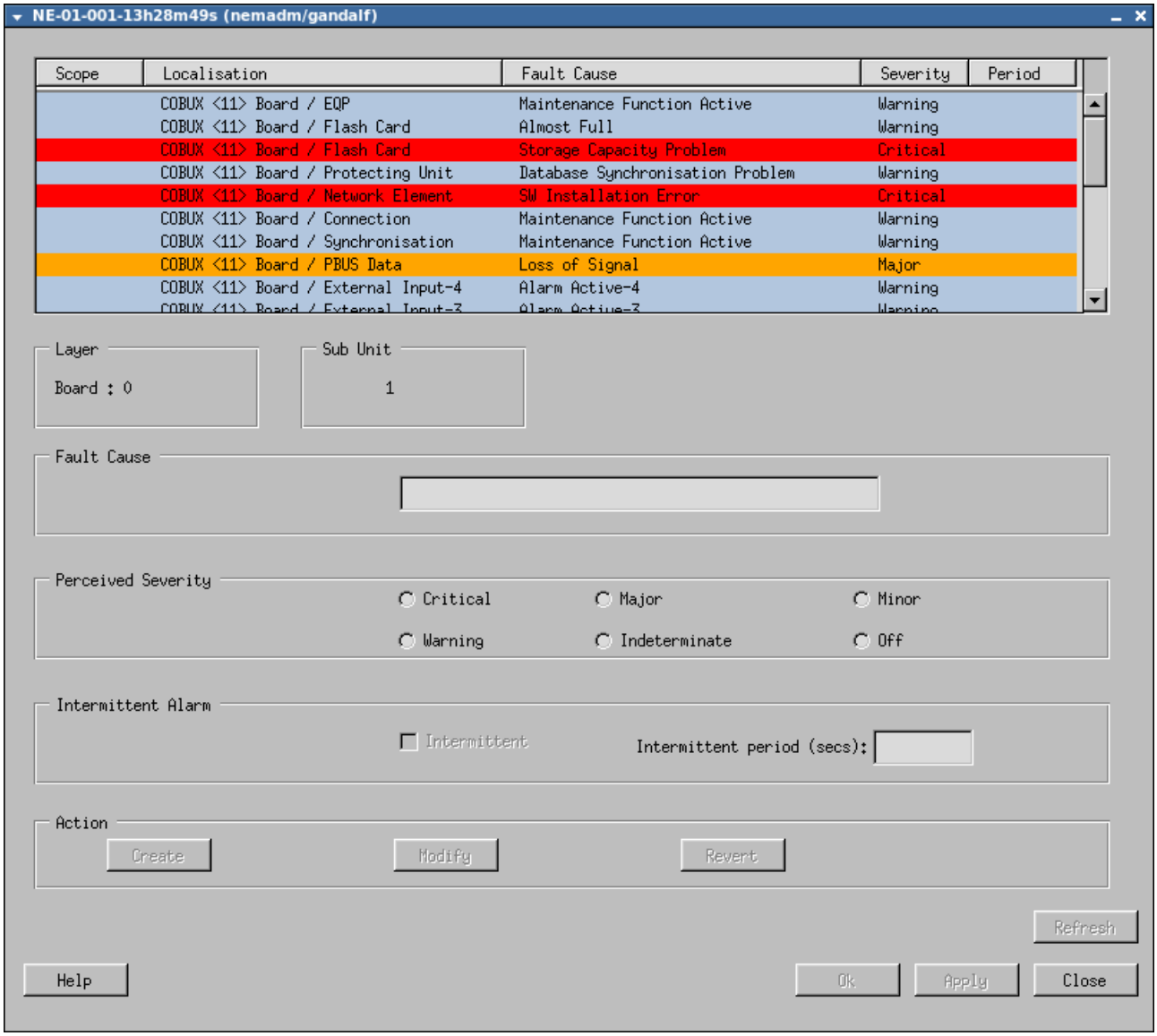


Figure 29: Alarm Customization - Unit and Subunit Level

Alarm customizations are clearly marked in the list and can be easily found again. They can be returned to default settings by the push of the Revert button.

Intermittent alarm setting

The FOX51x family of network elements register any alarm lasting more than 200 ms. During the commissioning phase or while field work is in progress a lot of intermittent alarms may be created which disturb the routine supervision of the network. For such situations, FOXMAN-UN allows filtering the alarm so that only one occurrence during a user definable period can be reported.

The hardware views show all units and subunits which contain customized alarms marked with an «M». This applies also if the customization has been done on a global or NE level (see below).

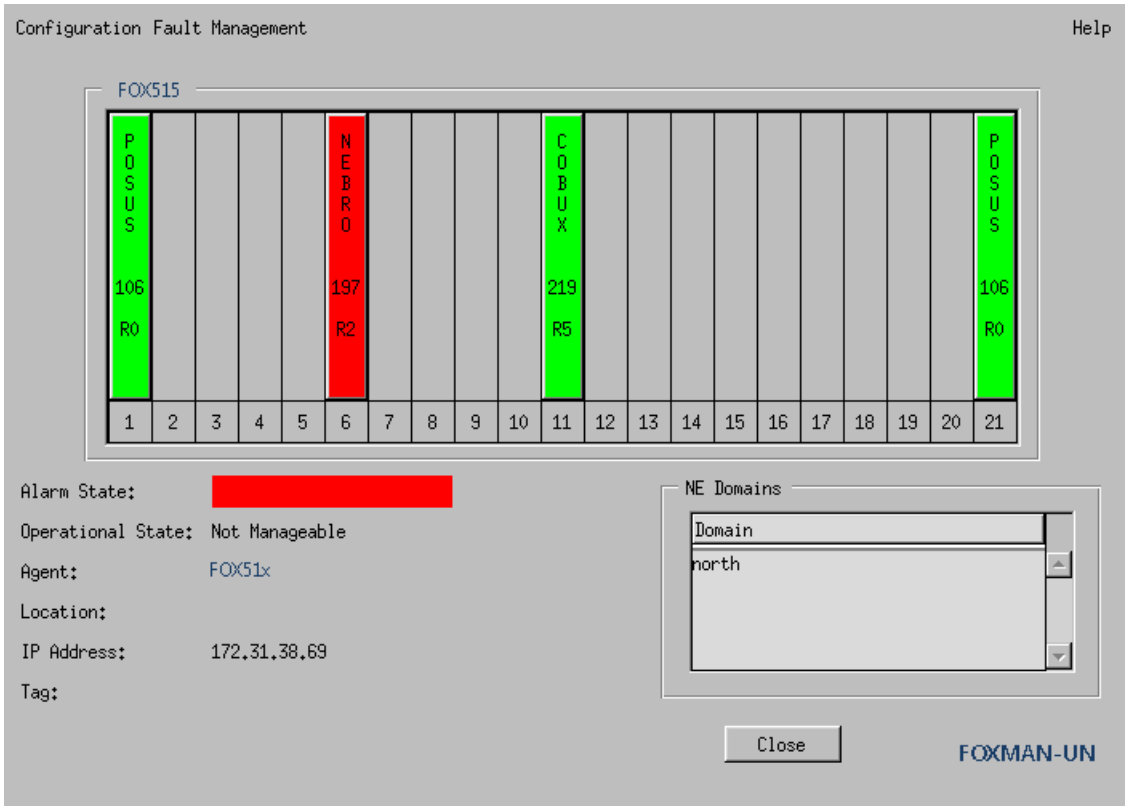


Figure 30: Alarm Customization - Hardware View

Please note:
Customizations created from hardware views take precedence over those created via the global customization.

4.2.3.3 Severity «Off»

During installation and commissioning it can be desirable to temporarily to prevent certain alarms from being reported. This is achieved by modifying the default alarm severity to «Off».

FOXMAN-UN can be configured to either completely ignore alarms which have their severity set to «Off» (default configuration), or to indicate and log them as normal alarms with the severity «Off».

4.2.4 Alarm Flooding Protection

As a protection from a build up of outstanding unacknowledged alarms or from sudden surge of intermittent alarms, FOXMAN-UN can auto acknowledge alarms.

In auto acknowledge mode, cleared alarms are automatically acknowledged and then moved from the database to the alarm history.

It is also possible to define the maximum number of alarms per NE to be held in the database. If this number is exceeded, any cleared alarms are written to the alarm history and removed from the database. In this way the application can protect itself from overload conditions.

4.2.5 Foreign Object Alarms

Foreign Objects can be assigned alarms generated at the inputs of a special FOX51x unit called ALCAR. These alarms are not reported as belonging to the FOX51x, they are directly associated with their foreign object. Fault cause text and severity and alarm input number are defined via the FOX51x configuration.

Foreign object alarms are handled the same way as alarms of the NE type FOX51x.

FOX61x NEs do not offer a corresponding alarm collection unit.

4.2.6 Alarm Localization

When an alarm appears, the operator can easily and quickly localize the fault on the graphical representation of the network. The NEs and sections (links between NEs) reflect their alarm state by the color of their symbols on the map.

The color propagation of an alarm through the hierarchy of the maps allows the operator to intuitively follow the alarm down to the lower maps and finally, via the hardware views, to the channel, port and card level.

4.2.7 Alarm List

By default the alarm list displays all outstanding, acknowledged and unacknowledged alarms except those with severity.

The Alarm List dialog displays all outstanding, acknowledged and unacknowledged alarms except those with severity «Off».

The alarms of the current FOXMAN-UN user's managed network are filtered according to where the alarm list is called from:

- All alarms of the total managed network;
- All alarms of all NEs belonging to a specific map;
- All alarms of selected service(s);
- All alarms of a single severity in the total network;
- All alarms of a single severity belonging to a specific map;
- All alarms of a single NE;
- All alarms of the system.

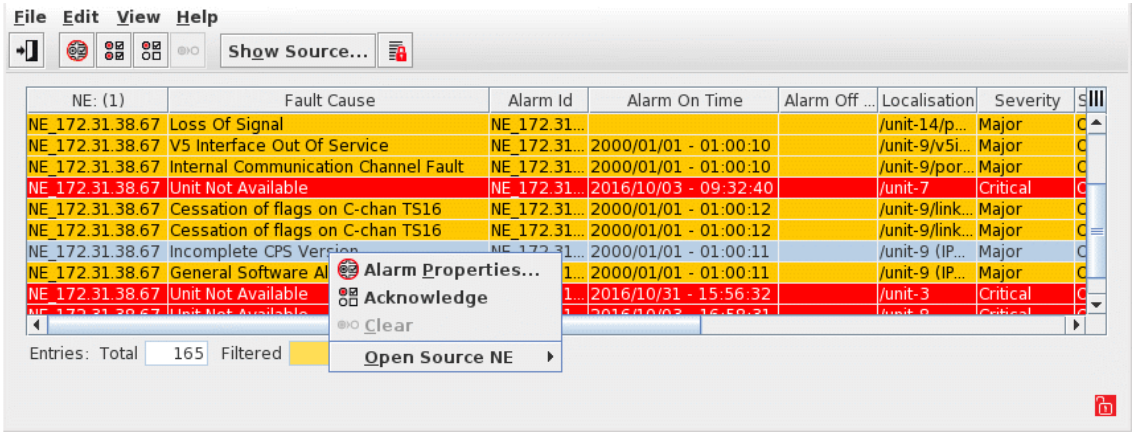


Figure 31: Alarm List

4.2.7.1 Alarm Acknowledgment

Single alarms or a group of alarms can be acknowledged in a single step. Acknowledging a cleared alarm will remove it from the database and write it into the alarm history.

4.2.7.2 Alarms Properties

Alarm properties are available for each individual alarm, providing information such as:

- Fault Cause,
- Work Instructions,
- Comments/Predefined Comments,
- Location of a fault down to subunit level,

- Severity,
- Alarm Status,
- Alarm Type,
- Alarm On/Off Time,
- Alarm On/Off Acknowledge (by whom and when it was acknowledged).

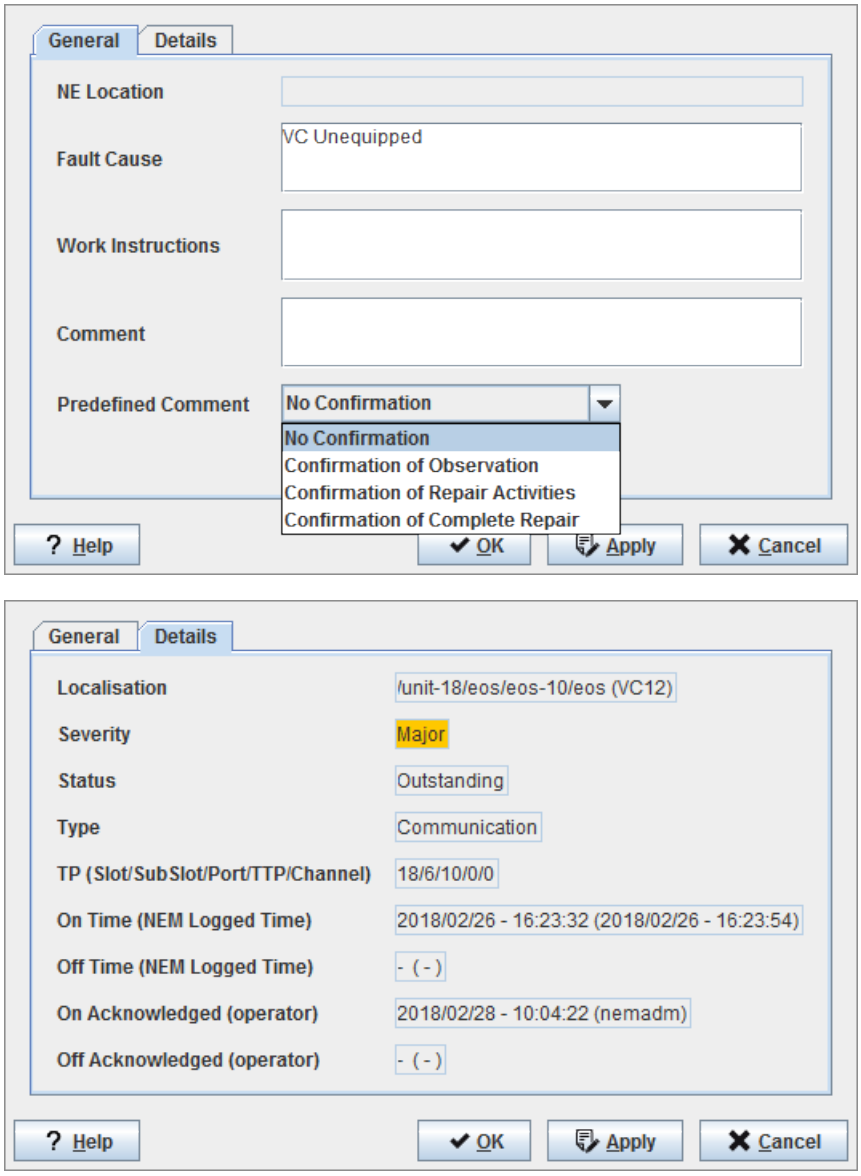


Figure 32: Alarm Properties

The operator can acknowledge each alarm individually and add a comment or select from one of the Predefined Comments, to give other operators further relevant information of the problem, and the steps that were already taken, or are being taken.

4.2.7.3 Alarm List Printout

FOXMAN-UN allows an operator to send selected or filtered alarms of an alarm list either to a printer or to a file. Files are text files of the type CSV containing separators which can be opened and analyzed further using a spreadsheet application.

4.2.8 Section Alarms

Sections display selected alarms generated by the subunits of their endpoints. The color of the section is modified to reflect the highest severity of the active alarms. Only alarms indicating affected traffic are shown, e.g. «AIS received» (minor), «BER > 1E-3» (major), «BER > 1E-5» (minor), «Loss of Signal» (major).

4.2.9 Alarm Email Notification

For each domain, alarm notification can be done to a email address specified in the domain properties. The operator can specify whether he wants to include system alarms, and the minimum level of severity to be notified.

4.2.10 Alarm Escalation

The FOXMAN-UN's special handling of alarms include creation of delays from the alarm occurrence before activating the alarm, turning on an external alarm indicator or sending alarm notifications via emails.

4.2.11 Alarm History

To analyze the network quality over a long period, FOXMAN-UN generates appropriate alarm and activity histories.

All acknowledged and cleared alarms that are deleted from the Alarm List are written to the Alarm History, which can be analyzed and archived.

Similarly, all activities displaying successful or unsuccessful FOXMAN-UN procedures are written to the activity history which can be analyzed and archived.

4.2.11.1 History File Cycling

To prevent history files from growing too large and slowing down overall system performance, one file is created per 24 hour period. A maximum of 30 history files (covering a period of 30 days) are kept in the system. History files older than 30 days are automatically removed.

FOXMAN-UN allows modification of the length of the standard history period of 30 days.

4.2.11.2 History Data Retrieval

Alarms or activities can be retrieved from the history for a user definable date and time period which can span the whole of the 30 day history. In addition, filters can be set to efficiently handle analysis tasks. The resulting filtered lists can be printed or saved to file.

4.2.12 Logbook Function

Each NE keeps a limited local history of its alarms in the alarm logbooks. FOXMAN-UN automatically collects the alarms from these logbooks and presents them to the users.

The NE alarm logbooks can also be uploaded and displayed at the FOXMAN-UN workstation using the respective configuration tool (FOXCST or UCST).

4.2.13 NE Alarm Synchronization

The FOXMAN-UN also provides the capability to automatically synchronize the contents of the database with the current alarm situation of the network elements. The synchronization can be performed for all or only a selection of the managed network elements.

4.2.14 System NE

A number of system alarms generated by the FOXMAN-UN management communication (via the agents), the SNMP interface, the file system of the workstation (via the smtool) or the FOXMAN-UN Networking Package (if activated in the license key) can be displayed via the System NE.

This pseudo NE can be placed on a map like a normal symbol. Its default name is the name of the workstation where the FOXMAN-UN core is installed. Its color and blinking state are modified according to the system alarm state.

Please note:
Some of the system alarms cannot be cleared automatically. They have to be removed manually by the FOXMAN-UN user.

4.2.15 Trouble Ticketing

FOXMAN-UN allows referencing a trouble ticket on a per alarm basis. Each alarm in the alarm list offers a comment field for this purpose, which can also be used for conveying further messages. The comment field is accessed via the alarm details menu in the alarm list.

5 Configuration Management

5.1 Introduction

Configuration is clearly an important feature of any management system. The ease of use is paramount if the efficiency and responsiveness of an operator to create, modify and expand the network is to be guaranteed.

Configuration management is divided into 2 distinct parts:

- Network element configuration,
- Network configuration.

Network elements (NEs) are presented to the operator by a set of views through which he has access to all the parameters, status monitoring, and diagnostic functions at the element level.

More than one network element can be accessed and worked on at the same time on the same screen.

Bulk configuration tasks can be executed with the built-in task dialogs. For the following tasks a separate dialog is available:

- NE password changes,
- Profiles and CPSs,
- ESW installation.

The automated network and service provisioning features are discussed separately under 7 "Networking Package" and 8 "Ethernet Networking Package".

5.2 FOX61x NE Configuration

5.2.1 FOXCST / FOXMAN-UN Look and Feel Similarities

The configuration dialogs for the FOX61x NEs are the same as the dialogs of the standalone FOXCST GUIs. This permits an operator familiar with the standalone FOXCST GUIs to do NE configurations from FOXMAN-UN without additional training.

The screenshot below shows an example of the FOXCST GUI connected to a FOX61x NE. The NE is shown in the shelf view, with a presentation of the physical arrangement of the units in the subrack.

Further views of the FOX61x NEs are:

- Tree view,
- Commissioning,
- Alarms,
- Cross Connections,
- Switching,
- MPLS-TP,
- Management Interfaces.

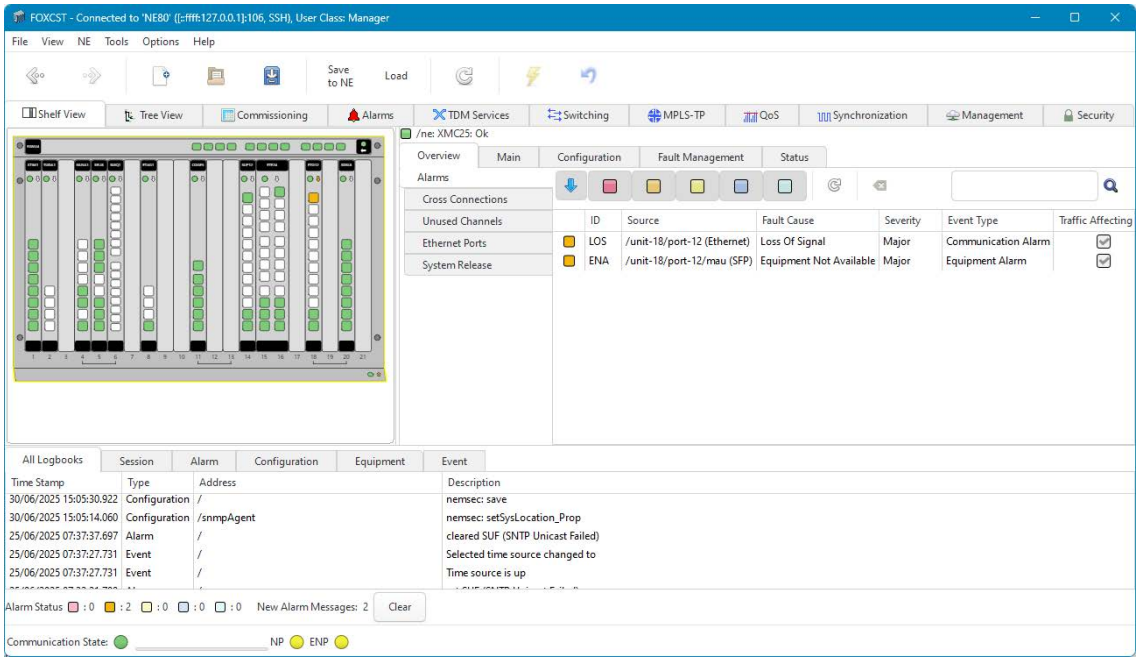


Figure 33: FOX61x NE Configuration (Shelf View)

5.2.2 Configuration Changes

The FOXCST GUI is called via the context menu of an entry in the NE list of NEM Configurator or a symbol on a map. The FOXCST is started and automatically connected to the NE using the selected user class.

Once connected, the configuration of the NE can be examined and modified if required. A «Save to NE» command stores the configuration in the NE. Depending on the settings in the “database.conf” and “tasks.conf” files a modified NE configuration is backed up immediately or in regular intervals.

As a default, a maximum of five configuration backups are kept for each NE. If required, any of these can be used for restoring a previous NE configuration. Restoring a previous NE configuration can be initiated from the NEM Network Browser (legacy application) or from the NEM Configurator.

5.2.3 Simultaneous Access

A FOX61x NE allows up to 16 simultaneous management sessions. One session is always reserved for the session manager, the other 15 sessions can be used by other user classes in any distribution, but only one session of class “Session Manager” is allowed at a time. More than one simultaneous session of class “Manager” is thus accepted. It lies in the responsibility of the connected users to avoid configuration conflicts.

However the acceptance of multiple manager sessions is essential in order not to block service provisioning by FOXMAN-UN, i.e. FOXMAN-UN must be allowed to start a manager session to any NE at any time. The session manager has the authority to terminate all active sessions except his own.

5.2.4 NE Profiles

NE profiles are used to simplify the configuration of large numbers of units by using predefined parameter sets with identical values. There are a number of different profile types available.

FOXMAN-UN provides a profile tool which allows creating or importing new profiles and downloading them to selected FOX61x NEs. Profiles can also be uploaded from NEs.

5.3 FOX51x NE Configuration

5.3.1 UCST/FOXMAN-UN Look and Feel Similarities

All configuration dialogs in FOXMAN-UN have exactly the same layout as the standalone UCST dialogs. This ensures that an operator who knows how to configure NEs using the standalone UCST is able to make the same configuration using FOXMAN-UN with a minimum of re-training.

The FOX51x hardware views are supported only with the FOXMAN-UN client for Windows®.

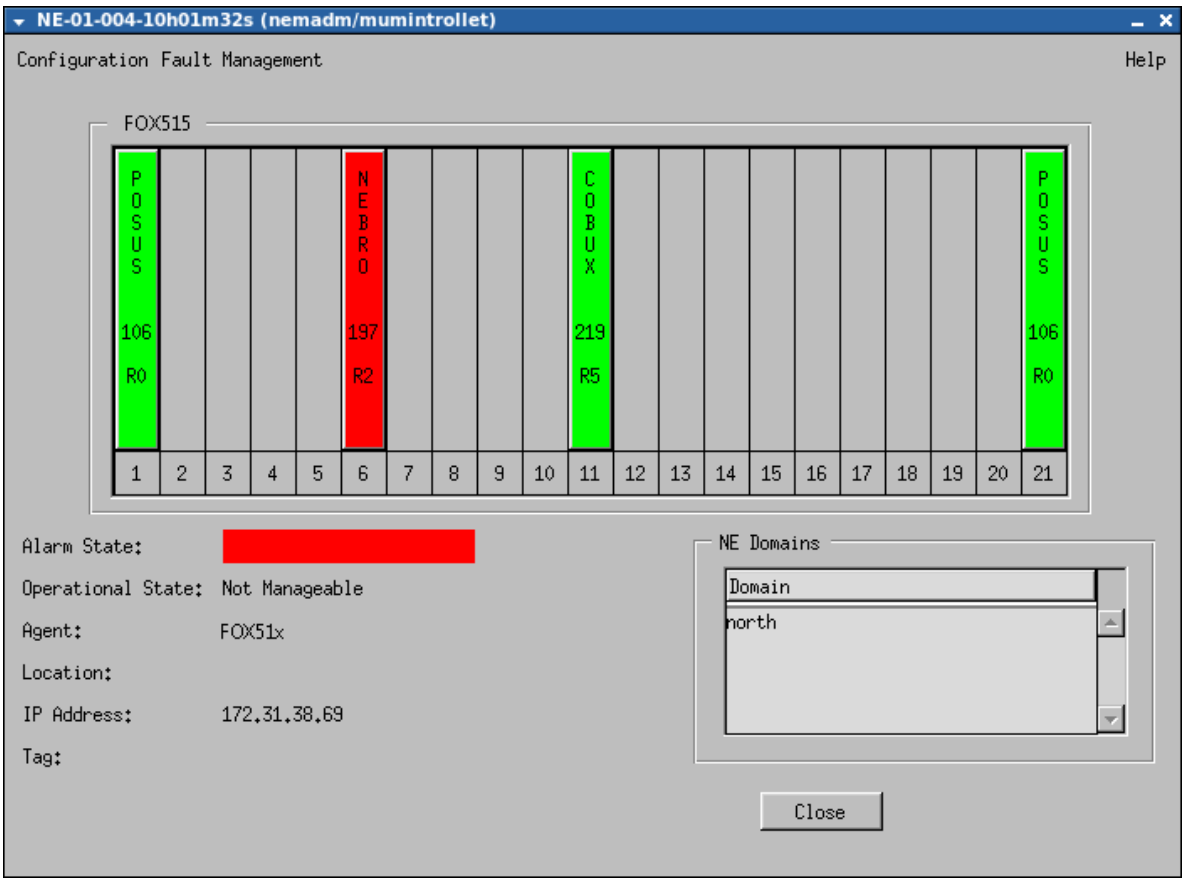


Figure 34: FOX51x NE Configuration

Amongst others, the configuration functions permit the operator to:

- see the function of a given unit (card) by placing the mouse pointer on it;
- set parameters of the Interface units (analogue, data, or transmission), down to what signal level is to be defined or metering pulse, speed, etc.;
- configure cross-connections;
- establish conferences;
- define clock sources;
- define and initiate diagnostic functions (e.g. manual or periodic self tests, etc.);
- define equipment protection;
- define configuration profiles.

5.3.2 Configuration Changes

5.3.2.1 General

To call the configuration tool UCST for a particular NE, the mouse pointer is placed over the NE symbol and the context menu displayed via the right mouse button. Selecting «Configuration» calls the UCST and opens the appropriate configuration file.

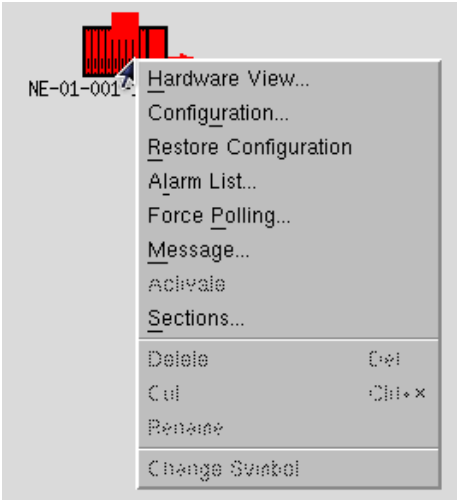


Figure 35: UCST Configuration Tool- NE Menu

Updating the configuration

Once the network element configuration has been updated the operator has the following choices:

- **Full Download**: Download the entire configuration to the network element, to change the actual configuration with the newly defined one. This function is only used if the configuration identifier or the configuration data in FOXMAN-UN differs to that in the network element. This may occur if a field engineer has locally changed the FOX51x configuration.

  A full download can disturb the traffic of some older UBUS units (bit errors, loss of frames, etc) even if the relevant configurations remain unchanged.
- **Partial Download**: Download only the units that contain configuration changes to the network element without disturbing traffic.
- **Upload**: Loads the current configuration from the NE and loses the configuration changes.
- **Reset Configuration**: Loads the configuration from the FOXMAN-UN database and loses the configuration changes.

5.3.2.2 Simultaneous Access

More than one user can access the configuration of the same NE simultaneously. If any one of them performs a download, all other users receive a warning message. It shows the identity of the user responsible for the change:

Figure 36: UCST: Configuration Mismatch

5.3.2.3 Local Configuration Change

A system alarm «Automatic Configuration Upload Performed» is raised if the configuration of an NE is changed locally and, as a consequence, is uploaded automatically to synchronize the database.

5.3.3 Profiles

Profiles have been introduced to simplify the procedure of configuring many subunits with an identical set of parameters across an entire network. Profiles are predefined structures with a defined subset of parameters for functions of units. Profiles are managed via FOXMAN-UN and CST for use in units with DSL or Ethernet functionality.

5.3.4 Inventory for FOX51x

FOX515, FOX512 provide detailed information on the units installed. The inventory view provides the units part number along with the Hardware and Software versions as follows:

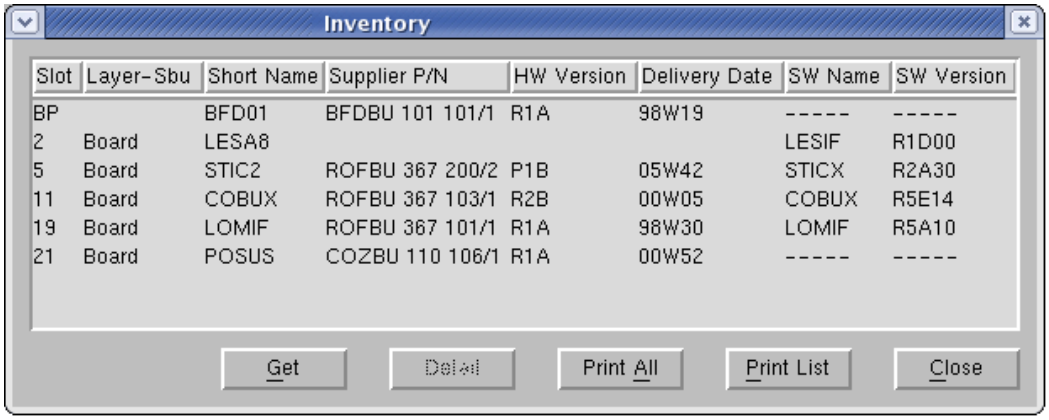


Figure 37: FOX51x Inventory

The operator can get further details on a given unit by choosing the unit and pressing on the Details button.

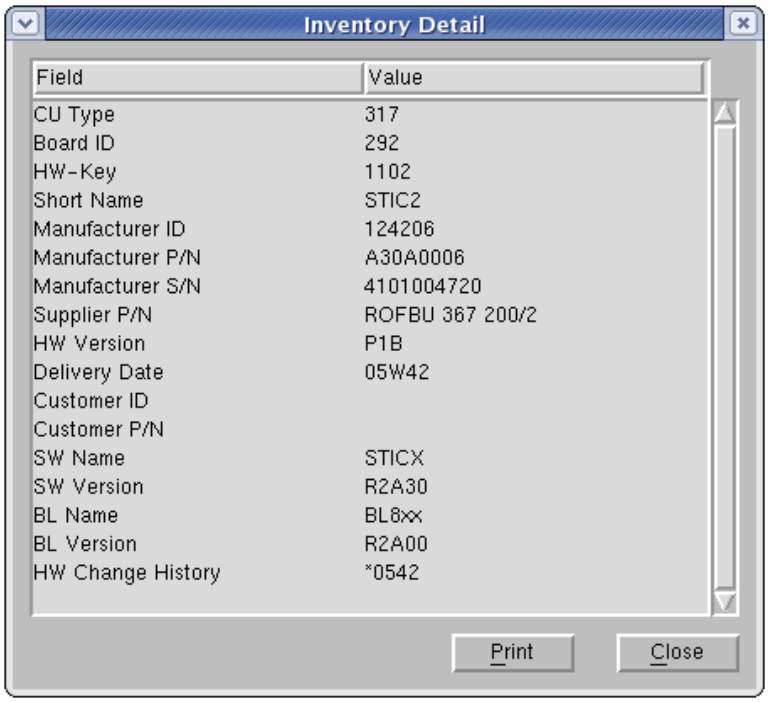


Figure 38: FOX51x Unit Detail Inventory

5.4 Network Configuration

To provision a network service, it is necessary:

- to change the configuration of 1 or more NEs in the network, and
- to ensure that the resulting configurations are mutually consistent.

5.4.1 Section Definition

To create trails from one end of the network to another, it is necessary to define sections between network elements. These represent the actual physical connections between two network elements, within which logical connections can be defined.

Sections between network elements can be defined for different types of end node combinations:

- NE to NE,
- NE to Foreign Object (FO),
- FO to FO.

The operator can define the sections using the Section Editor:

The operator can define, modify, delete sections and launch the NP GUI for the specific section using the «Section Management». This dialog gives a list of all existing sections.

For a new section, the «Create Section» dialog allows choosing the endpoints (NE and termination point), the layer rate and cost as well as specifying section name.

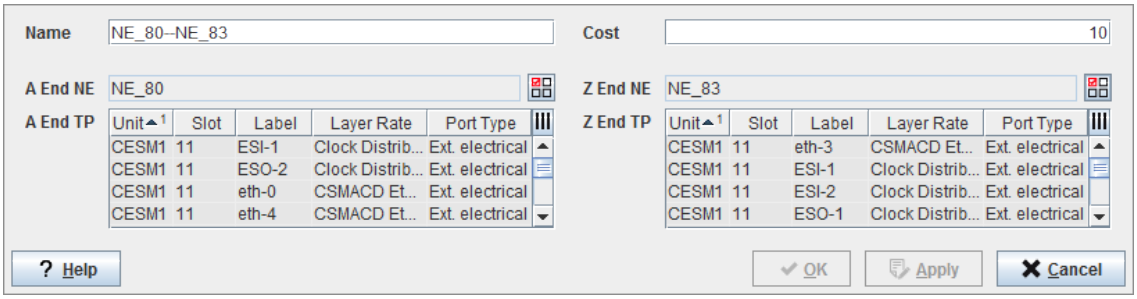


Figure 39: Network Configuration: Section Creation

On a map, a section can be comfortably created in Edit mode using the NE context menu «A-End Section» or «Z-End Section», which calls the Create Section dialog.

Once sections are defined these can be displayed and alarmed.

The “Open-Circuit” context menu launches the NP GUI for the specific section. The NP GUI will show the circuits or trails going over the section.

By double clicking on a section on the Map the operator can obtain a detailed information of the section.

5.4.2 End to End Configuration

By using the «Section Management» the operator can create the connections between the network elements (including NEs of type Foreign Object). Once the sections have been established, the operator can create end-to-end circuits configuring the network elements involved on this circuit and make sure that the internal connection points over the cross connect are established.

Creation of services (in the packet word, such as for MPLS-TP) or circuits (in the TDM world) is supported by the respective network applications:

- MPLS-TP application (browser-based application) or Ethernet Networking Package (legacy application) for VPLS and VPWS service creation, see 8 Ethernet Networking Package (on page 81).
- Networking Package (legacy application) and TDM (browser-based application) for TDM service creation and view, see 7 Networking Package (on page 73).
- Circuit Emulation (browser-based application) for ciruit emulation service creation and view, see 9 Circuit Emulation (on page 100).
- Teleprotection (browser-based application) for teleprotection service creation and view, see 10 Teleprotection (on page 101).
- DCN (browser-based application) for management access and data communication network manegement.

To ease this process, FOXMAN-UN allows the operator to configure several network elements simultaneously. The input and output circuits and their characteristics can be defined, such that the circuit can be established from one end to the other.

5.5 Configuration Tasks

5.5.1 General

Network-wide tasks as

- NE password tasks,
- Profile and CPS tasks,
- Credential Distrubution,
- ESW Management,

- ESW tasks (legacy),

are collected in an overview after having been defined in a task specific dialog (see below). From this overview, existing tasks can be aborted, restarted, paused, resumed, or deleted. Tasks can be executed immediately after task creation, or they can be scheduled to a specific point in time.

The overview shows property and status information of all created tasks.

The tables from each of these tasks can be filtered/sorted as well as printed or exported for further analysis if required

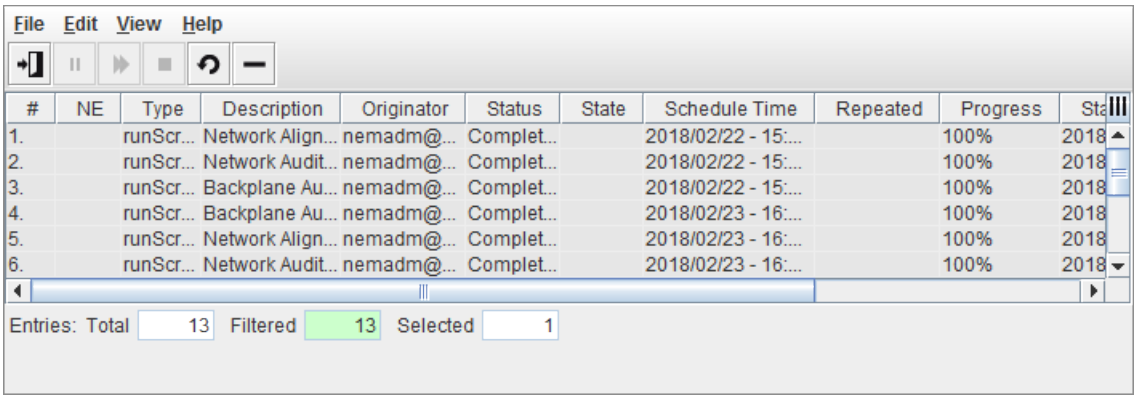


Figure 40: Task View

5.5.2 NE Password Tasks

Passwords for NE access can be set or modified for selected NEs or for all NEs in a network. This allows setting passwords for the different user classes.

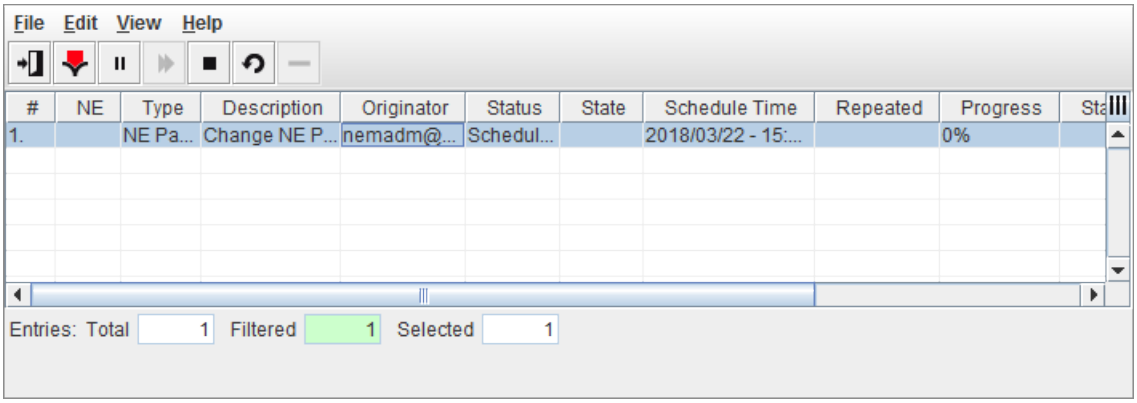


Figure 41: NE Password Tasks

5.5.3 Profile & CPS Tasks

Profiles and customer parameters sets (CPS) can be loaded to selected NEs or to all NEs in a network (FOX61x NE type only). Profiles and CPS are part of an NE configuration, but must be loaded to the NE in order to fully configure the NE.

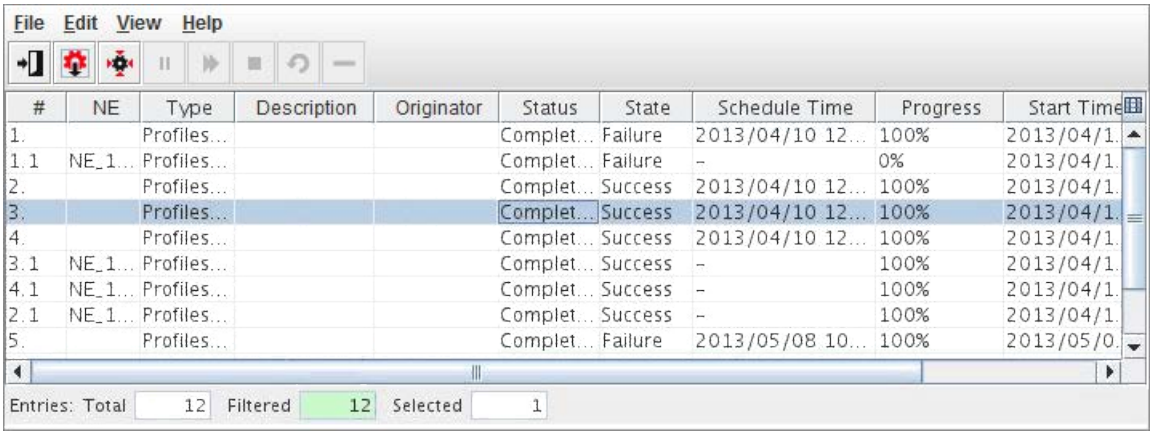


Figure 42: Profiles & CPS Tasks

5.5.4 ESW Management

Embedded Software (ESW) running on units of Network Elements can be loaded from a file system to the FOXMAN-UN database. From the database, ESW can be distributed to selected NEs or to all NEs in a network via an ESW task based on a specified ESW distribution job definition.

This task distributes and/or installs ESW to the network elements.

A network overview lists all ESW installed in the network and allows the user to group the listing by ESW name and version, by unit type, or by NE.

ESW distribution jobs and related tasks are created in a wizard providing different installation or ESW upgrade options, including scheduled distribution, scheduled installation, and NE ESW upgrade with minimized service interruption.

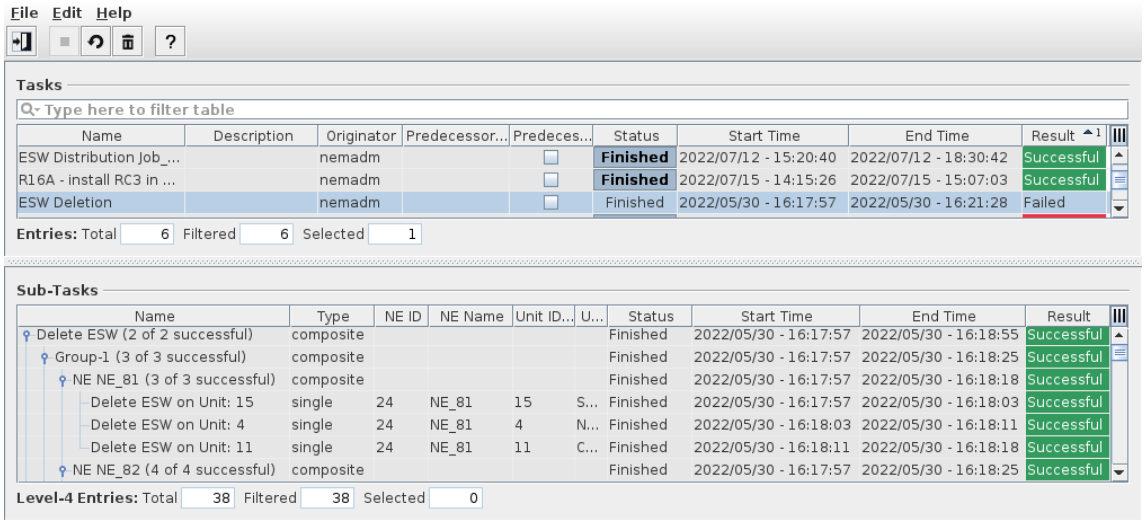


Figure 43: ESW Task Management

6 Performance Management, Diagnostics, and Status

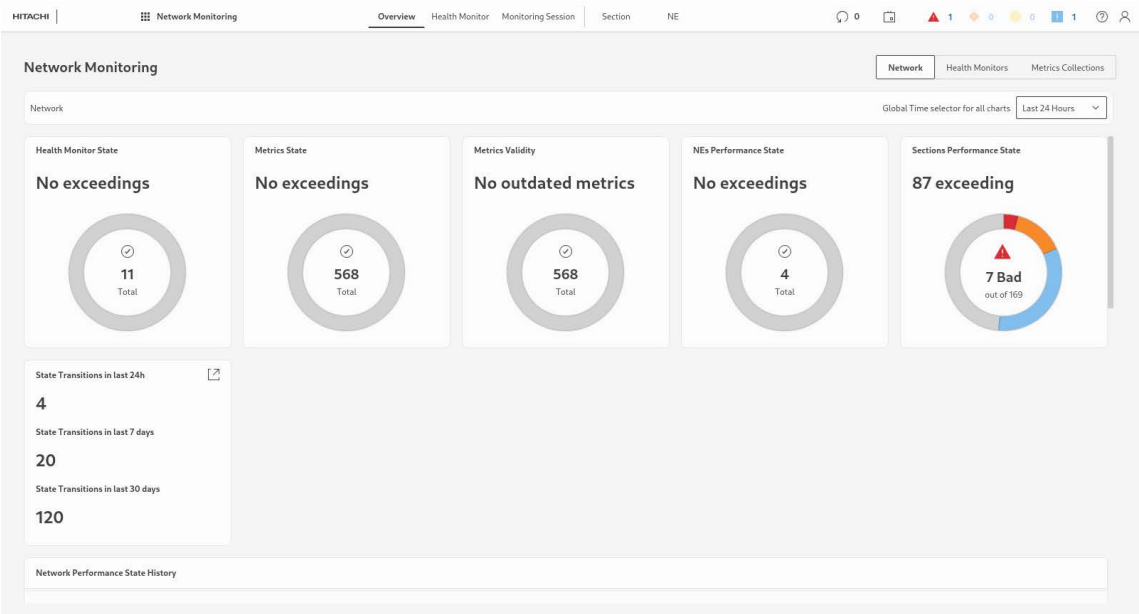
6.1 Network Monitoring

The Network Monitoring application provides a map or table view with all relevant information on the following tabs:

- Overview,
- Health Monitor,
- Monitoring Session,
- Section,
- NE,

related to the network health and performance. For detailed information on the Network Monitoring application, refer to the user manual “Network Monitoring” [1MRC000115].

6.1.1 Overview



The overview tab is the dashboard for a quick overview of the network performance status and history. Overviews and diagrams, where appropriate, are shown for the selected time. The overview provides the following graphical views:

- Network,

  An overview page with widgets providing graphical overviews on various aspects of network performance, network elements performance, and sections performance.
- Health Monitors, including the tabs
  - Performance State,

    displaying collected performance data for all Health Monitors,
  - Values,

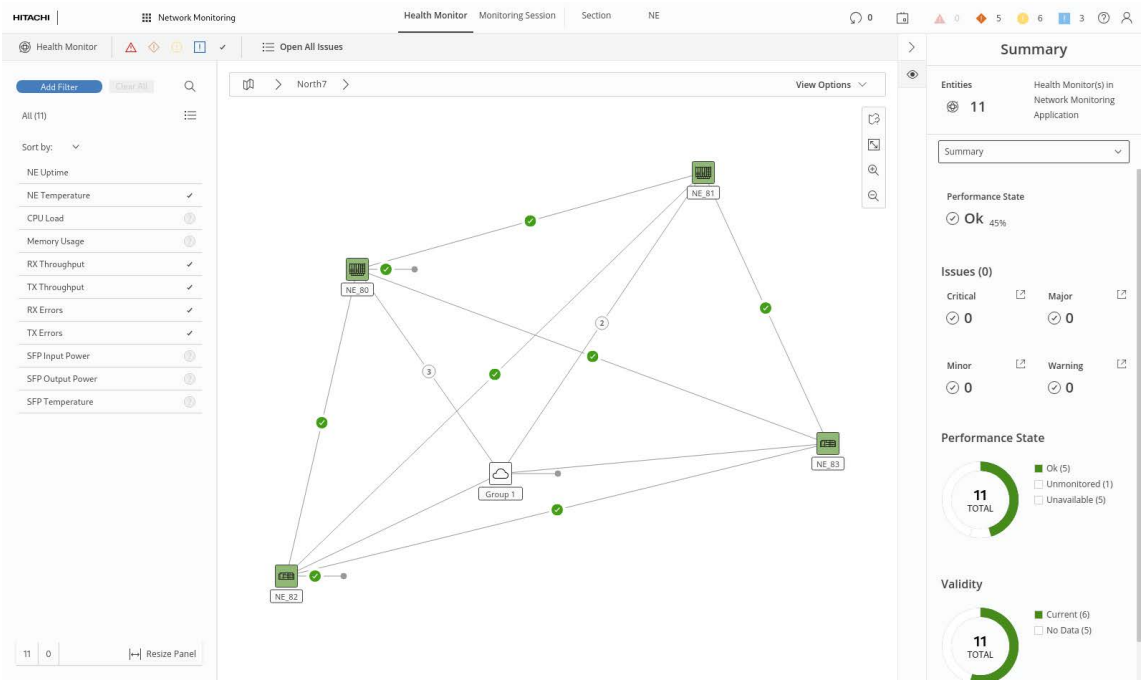
    displaying charts for the selected time span (via Global Time Selector) for all Health Monitors,
- Metrics Collections,

  providing a chart of the NEs health monitoring status.

Flexible options allow selection of history intervals via the “Global Time selector for all charts”, such as

- Last 24 Hours,
- Last 7 Days,
- Last 30 Days.

6.1.2 Health Monitor



Under the Health Monitor tab, the monitoring session collects health data from all elements of the network that provide appropriate data and presents the data on the network map and in a table in the entity browser (left panel). In the Summary (right panel) an overview on all monitored elements in the network is presented. It includes various monitored parameters, such as

- TX Errors,
- RX Errors,
- NE Uptime,
- NE Temperature,
- CPU Load,
- SFP Temperature,
- SFP Output Power,
- SFP Input Power,
- RX Throughput,
- TX Throughput,
- Memory Usage.

Upon selecting a specific monitor in the entity browser (left panel), the related health status is shown in the right panel.

Metrics

When opening ‘Metrics’ from the ribbon or the context menu for a selected Health Monitor, a table with all the metrics of the given monitor is displayed.

The four predefined state filters

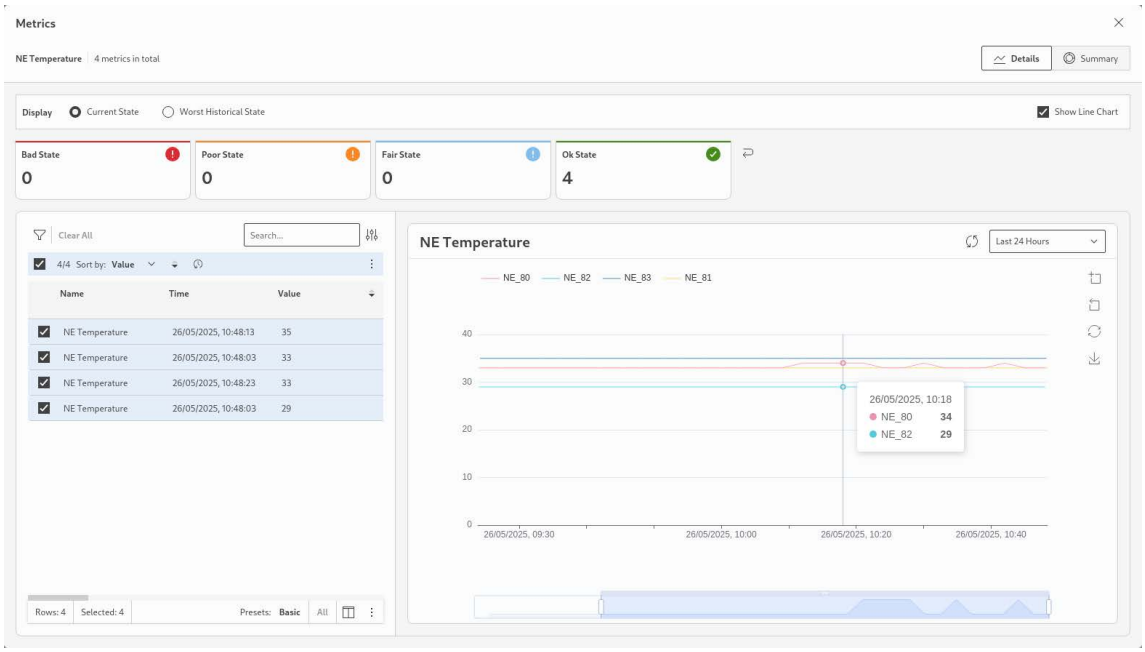
- Bad State,

- Poor State,
- Fair State,
- Ok State

can be set or reset by clicking any of them.

The selectable option “Show Line Chart” activates a line chart view of a single or multiple selected metrics.

An example for the NE temperature line chart details of four NEs is given below:



The drop-down list in the line chart title bar provides different default time periods. Two rulers (start date&time, end date&time) below the line chart allow you to adjust the time span shown in the chart. You can also zoom into the chart clicking on the “Zoom” icon and using the pointer device to select a span within the chart.

When placing the pointer into the chart, details on the captured metrics samples are shown in a tooltip window.

6.1.3 Monitoring Session

Information on the related monitoring session, including a detailed view, are presented under the Monitoring Session tab. In the details view, among others, General information, and Threshold Configuration with defaults and overrides are available.

The Threshold Configuration page lets you

- under Defaults,
  - view default thresholds for defined metrics,
  - edit default thresholds by selecting an existing entry and clicking on Edit ;
- under Overrides,
  - add a new override for defined items,
  - edit an existing override,
  - remove an existing override.

6.1.4 Section

Health information on sections is presented under the Section tab with a summary or individual details for a selected section.

6.1.5 NE

Health information on NEs is presented under the NE tab with a summary or individual details for a selected NE.

6.2 Performance Management

6.2.1 General

Performance monitoring in FOXMAN-UN provides Quality of Service evaluation of the data transmission media.

For the FOX61x NEs performance data is produced for Ethernet interfaces (trunk ports and user ports) as well as for all other trunk and user ports (packet-based and TDM-based performance data, as available).

For the FOX51x NEs it is implemented according to ITU-T recommendations G.826 for event calculations.

Performance monitoring with the FOX51x is available for all ABUS/SBUS and PBUS units with traffic signal layers and the new UBUS units. The parameters are evaluated according to ITU-T G.826.

Legacy UBUS units (e.g. MEGIF, UNIDA, TUNOP) have no performance monitoring.

The diagnostic function of the control unit COBUX, COBUV provides performance monitoring for the channel under test. The monitoring complies with ITU-T G.821.

Performance data is generated and stored at the unit themselves. After initialization the unit automatically starts counting the required events and stores the results in its memory.

Upon operator request, the CST can perform the function to retrieve the data from the unit and display it. For UCST it is possible to print the retrieved data.

FOXMAN-UN offers also an automatic performance data collection function. This allows collecting performance data over an extended period of time for a selected number of items in the managed network.

6.2.2 Recommendation ITU-T G.826

Recommendation G.826 defines error performance parameters for networks supporting paths which are independent of the physical layer.

Performance Measurement results are divided into Events and Parameters:

Events:

- Errored Block (EB),
- Errored Second (ES),
- Severely Errored Second (SES),
- Background Block Error (BBE),
- Unavailable Time (UT).

Parameters:

- Errored Second Ratio (ESR),
- Severely Errored Second Ratio (SESR),
- Background Block Error Ratio (BBER).

6.2.3 Performance Data Retrieval

The performance data from specific units can be retrieved and displayed via CST.

The operator can request the data for two measurement intervals:

- 15 min intervals (some legacy units use a variable length interval);
  History usually covers a 24 h period.
- 24 hour intervals (from midnight to midnight);
  History covers one 24 h period.

6.3 Automatic Performance Data Collection

6.3.1 General

FOXMAN-UN offers a performance data collection tool. Via collection schedules, a selection of elements in the managed network can be specified for performance monitoring. The performance data of these elements are continuously collected and saved in database tables, according to the kind of performance (G.826, MIB2, Ethernet, etc).

From third party software like PGAdmin or InfluxDB, the performance information can be exported in for integration into an OSS (Operation Support System).

6.3.2 Collection Schedules

From the NEM Desktop-Network, the «Performance Management Client» GUI can be called, which lets you define the desired collection schedules.

The example below shows the lists of all the defined PM collection jobs with their corresponding information. These include the Name, Data counter periodicity: 15min and/or 24h,Time and Date of last modification and Description of the collection job.

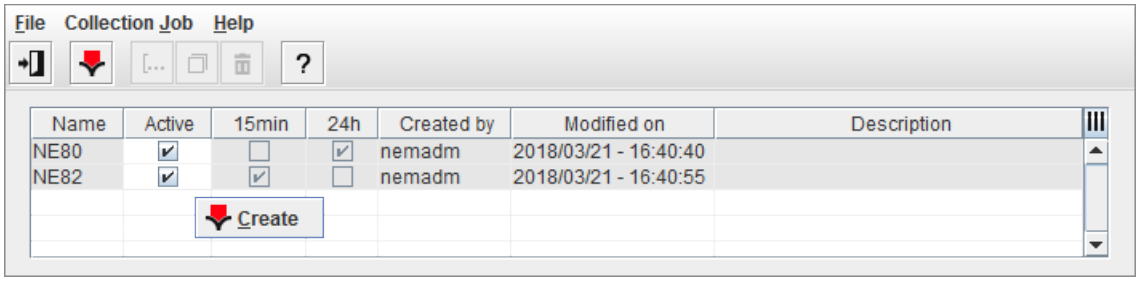


Figure 44: PM Client

The PM Collection Wizard lets you create new PM collection job as well as modify or duplicate an existing job.

For each schedule or job, it is mandatory to define the Name of the collection job, the definition of the type of data to be collected (15 minute interval and/or 24 hour interval), and a list of collection targets. These targets are determined with the help of the Wizard's Selection panel, which lets you easily step from the Network level down to the desired subunit(s).

6.3.3 Results

The collected Performance Management data is stored in the PostgreSQL database: PM_DATABASE. The PM_DATABASE can be administered with the command-line tool psql or more conveniently via more familiar graphical tools, such as PGAdmin III.

Please note:
These tools should only be used for connecting to and examining the PM_DATABASE. The users must not make any changes directly to the database, including adding new tables, entering or updating data.

6.4 Metrics Database

The system and network performance metrics database is a third party application that provides you with means to create a variety of graphs out of collected monitoring data, including system OS and NE performance data.

From ENP, new boards for VPWS or MPLS links can be created in the monitoring dashboard for any of the VPWS services or MPLS links.

6.5 MPLS-TP Diagnostics

In MPLS-TP networks built with FOX61x nodes, tunnels provide diagnostics features such as

- LSP Ping (evaluating the number of replies and the round trip delay),
- LSP Trace Route (evaluating the route to the tunnel end), and
- Delay Measurements.

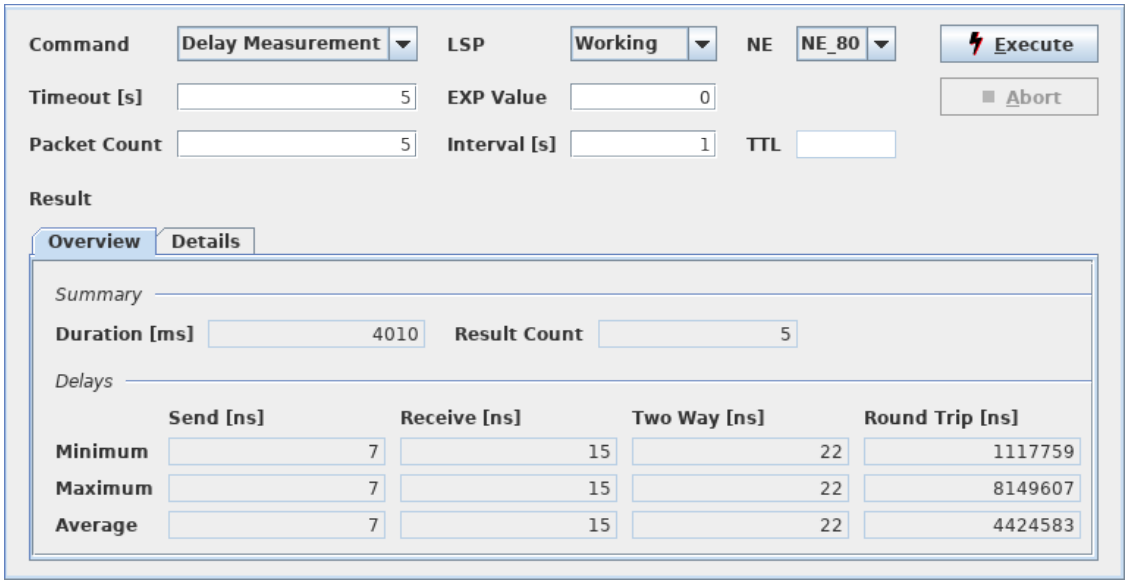


Figure 45: LSP Delay Measurement Results (example)

The delay measurements have a resolution of 1 ns if the Precision Time Protocol (PTP) is applied for node synchronization.

6.6 TDM Diagnostics

6.6.1 Pattern Generator

FOX61x, FOX515, and FOX512 provide a pattern generator on the control unit. The pattern generator can be cross-connected to any PDH unit in the FOX51x or to TDM units with PDH signals in FOX61x. This allows diagnostics on transmission links connected to the given NE.

In the FOXCST GUI connected to an FOX61x the TDM diagnostics function with a pattern generator and analyzer is accessed under the “TDM Services - Diagnostics” tab and provides settings and status display for bit error and delay measurements based on different patterns. The sample dialog below shows the setup of the pattern generator for an FOX61x.

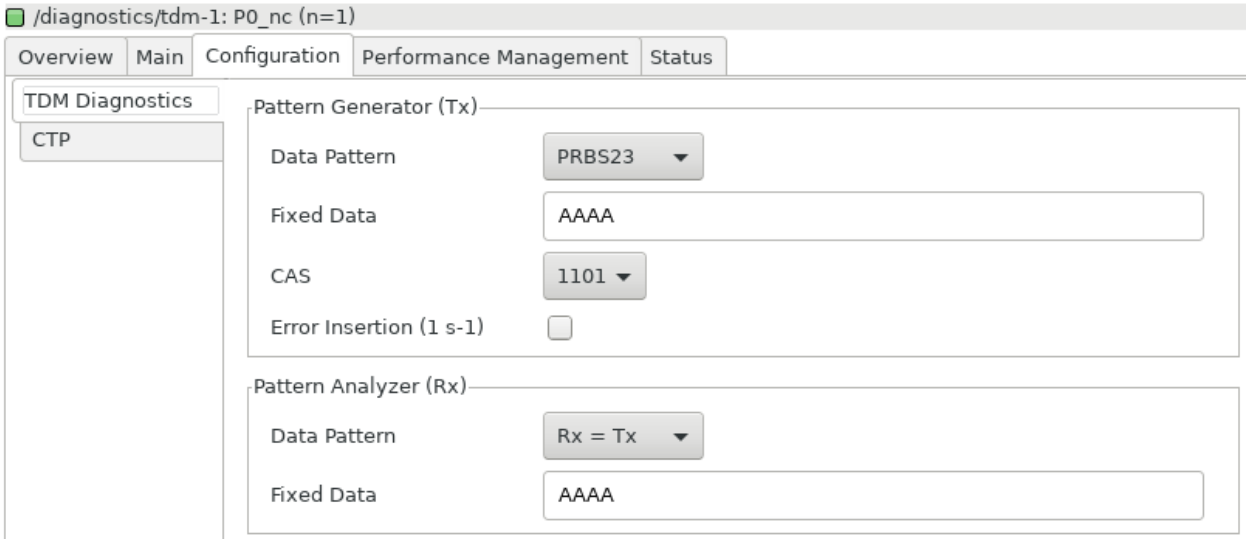


Figure 46: FOX61x Pattern Generator

6.6.2 FOX51x Diagnostics

6.6.2.1 Loop Activation

Various diagnostic loops can be activated on the units.

6.6.2.2 Integrated Testing of Subscriber Lines

If the FOX51x is equipped with SULIC, SUBH1, SUBH3, the following in-service line tests are available:

- subscriber loop characteristics.

With ISBUx the following in-service line tests are available:

- subscriber loop characteristics,
- activation tests.

6.6.2.3 Status Monitoring

The previous chapters have shown how FOXMAN-UN handles the alarms and monitors their status. Another aspect of managing a network is the ability to monitor the status of the access lines at customer sites or at the remote NE. This is useful both as a measure to prevent faults as well as to improve localization of faults that are already alarmed.

The following status monitoring functions are available:

- Monitor Signaling bits;
- Activation/deactivation states of ISDN and HDSL lines;
- Idle/busy states of POTS lines;
- Remote alarms and remote loops;
- Controlled slip counts of data channels and 2 Mbit/s signals;
- Performance information based on G.826.

6.6.2.4 Signaling Bits

The following signaling bits used in the G.704 2 Mbit/s frame can be monitored:

- The signaling bits (E/M and E'/M' or bits a, b, c and d of TS16) of PCM channels (NEMCA, SUBLx, EXLAx, SUBUK).
- bits (C/I) of V11 channels (SIFOX, UNIDA).
- TS0 spare bits in the 2 Mbit/s signals.

- TS16 spare bits in the 2 Mbit/s signals.
- CRC4 Error bits (E13 and E15) in the 2 Mbit/s signals.

6.6.2.5 Activation / Deactivation States

For all ISDN and xDSL units, activation and deactivation states of the DSL transmission lines can be called up and displayed.

6.6.2.6 Idle / Busy States of POTS Lines

For all units containing POTS interfaces, the idle and busy states of subscriber lines can be displayed.

6.6.2.7 Remote Alarms

The following remote alarms can be displayed:

- Status of the LEDs of the NTU connected to the SULIC.
- Alarms from the remote 8 Mbit/s optical ports (TUNOP / TUNOS / TUNOL and TUPON).

6.6.2.8 Controlled Slip Counts

Network synchronization problems can cause controlled byte/frame slips on data channels and the 2 Mbit/s signals. These controlled slips are counted and the slip counters are available for monitoring.

6.6.2.9 Network Element Timing Source Status

Via UCST the current timing source status of any network element can be displayed. The availability off all configured timing sources is shown as well as the currently active one.

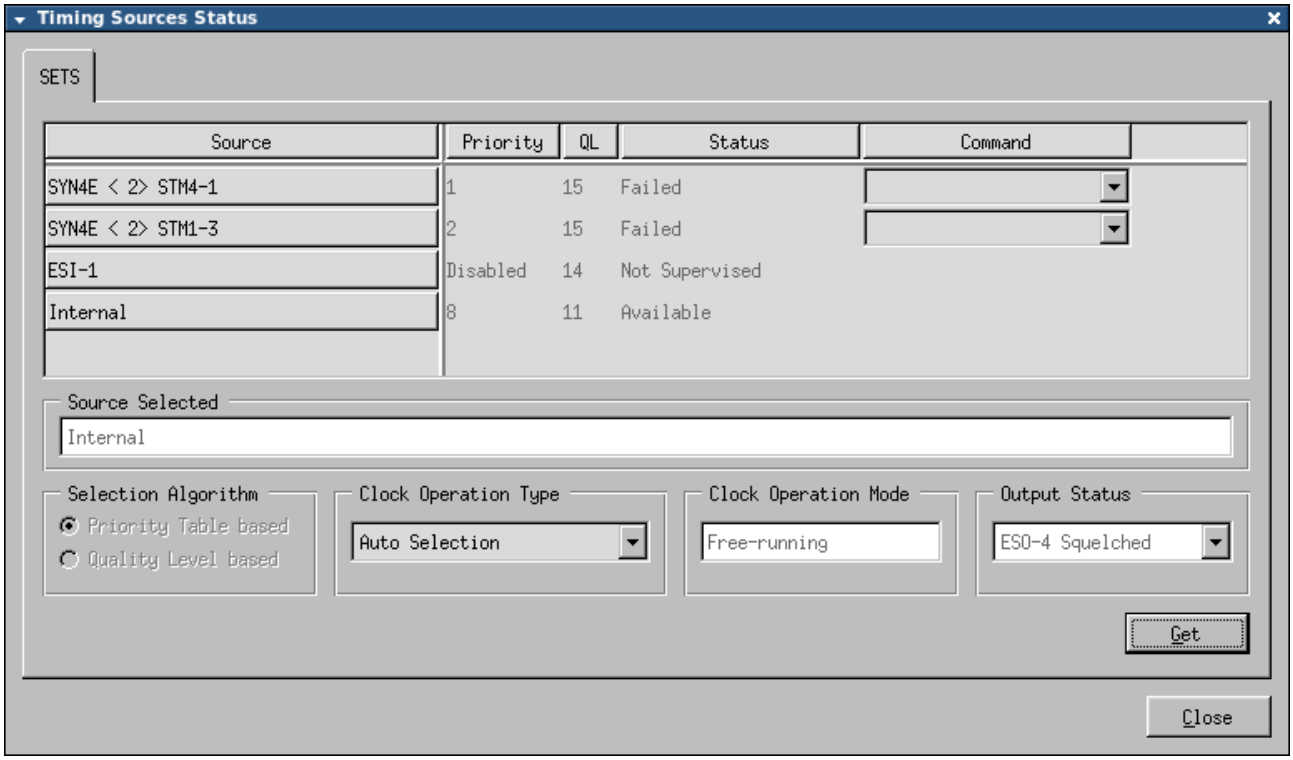


Figure 47: Timing Sources Status

6.7 Synchronization Map

Synchronization of network elements and how the clock information is propagated through the network, determine the integrity of information transmission through the network.

To ensure that this operates correctly, FOXMAN-UN provides the SDH and PDH Synchronization Map functionality.

This facility helps the operator to trace the clocking information through the managed network, and identify:

- which network element in the network is supplying the clock;
- any 'clock islands', where a network element clock is generated locally and is not propagated to any other network element;
- Any 'timing loops' which may have inadvertently been created by propagating the clock from a network element back to a network element which is providing the clock source.

With the synchronization map the operator can graphically display the actual clock propagation of either the SDH or PDH part in the managed network.

A synchronization map can be generated for all or for a user defined selection of the managed network elements.

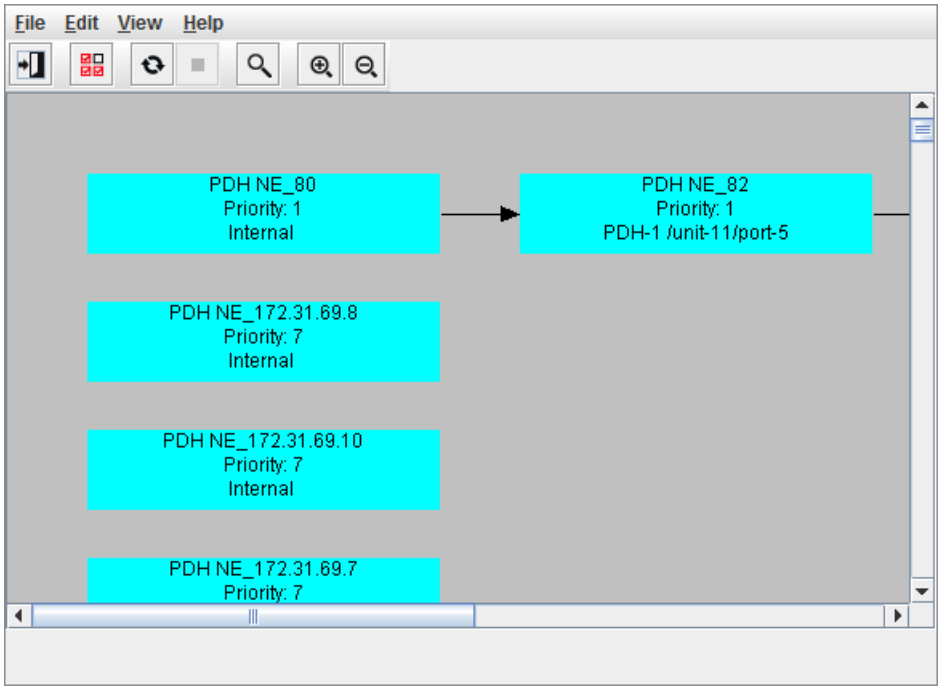


Figure 48: Synchronization Map

The current timing source information is collected from all the FOX61x and FOX51x network elements through the polling mechanism. Therefore the synchronization map reflects the timing situation at the moment of the poll of each network element. The map can be updated manually.

6.8 PTP Sync Map

For PTP-enabled FOX61x nodes FOXMAN-UN provides a sync map with an overview on the clock regions, clock labels, sync modes, clock operation modes, clock sources, clock accuracy, and node details.

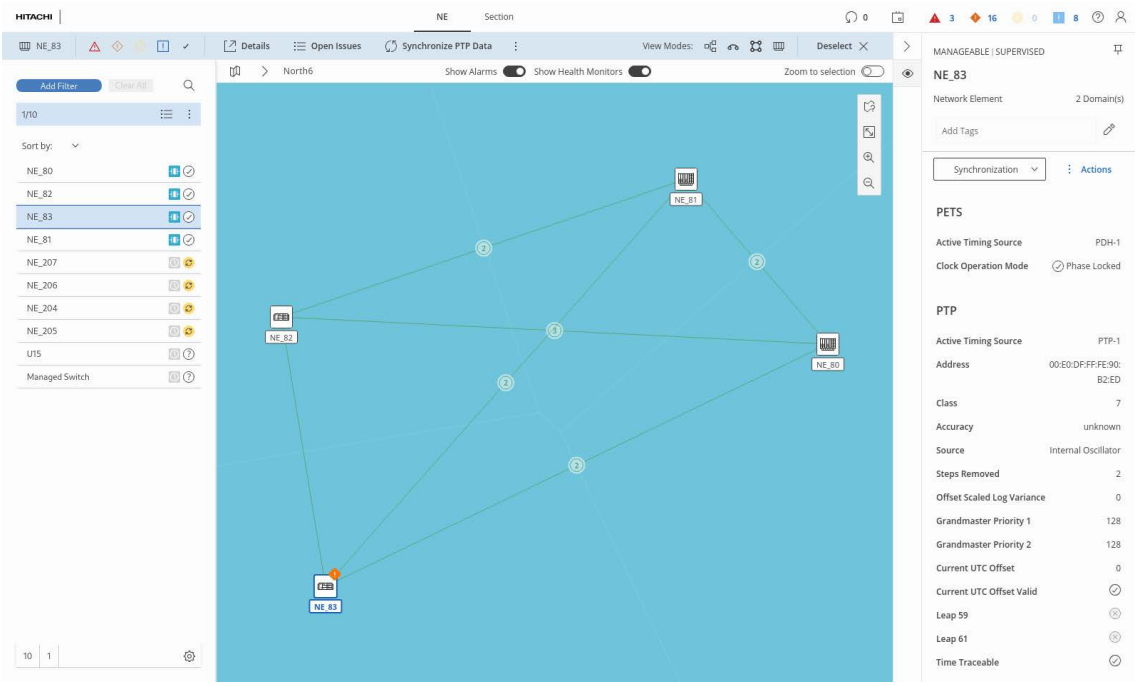


Figure 49: PTP Synchronization Map

6.9 Network Element Synchronization

FOXMAN-UN allows synchronizing the alarms, inventory and service of all or a selection of the NEs in the managed network with the database. In addition date and time of the NEs can be synchronized with the workstation date and time.

Date and time synchronization is also performed automatically for all network elements at 03:01 every morning. This function can be modified or deleted if required.

6.10 Ethernet Traffic Protection Maps

FOXMAN-UN provides maps that allow identifying the network protection topologies and their components, such as:

- Rapid Spanning Tree,
- Ethernet Ring Protection Switching (ERPS).

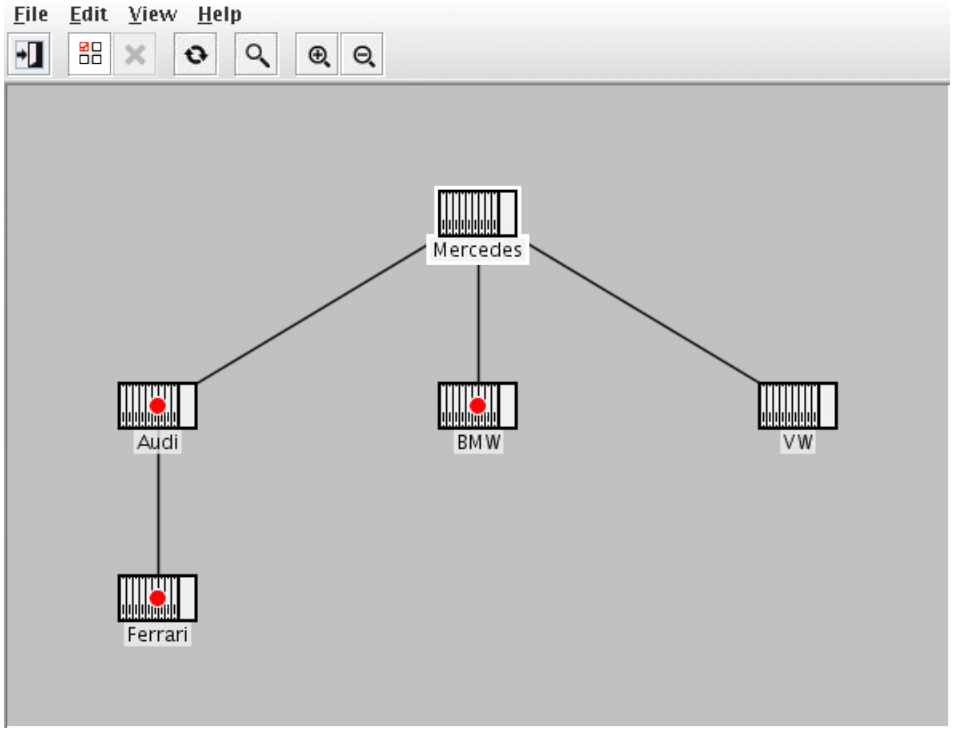
Please note:
The Ethernet traffic protection maps are applicable only for the networks' FOX61x R1C or R1D NEs.

Detailed information regarding provisioning are available at the following FOX61x document:

→ User Manual «Ethernet Switching».

6.10.1 Spanning Tree Map

The spanning tree map displays the spanning tree view of the selected NE with STP configured.



- All bridge nodes show the bridge name (the NE name known in the FOXMAN-UN). If the bridge has a port with status Blocking, this is indicated by a red circle marker.
  - A tool-tip on the bridge node shows additional information of the bridge:

Table 3: Bridge node (RSTP)

Parameter	Description
Name	The RSTP Bridge Name. Note: Currently “Customer Bridge” is the only bridge.
Priority	The configured Local/Root bridge priority.
Own MAC Address	The Local bridge MAC address.
Root MAC Address	The Root bridge MAC address.
Blocking ports	The slot/port# of ports which are in Discarding state.

  - a double click on bridge node opens the FOXCST of the corresponding NE with user class “Information”.

Please note:
Verify that the FOXCST is defined in the “client_cst_doubleclick_default” parameter of /opt/nem/etc/cst.conf.

- Links
  - Links are represented with dark gray lines between bridge nodes. Only links with forwarding endpoints are shown.
  - a double click on a link opens the Section Manager and the section on which the link relies is shown.
  - a tool-tip on the link shows additional information of the link end ports

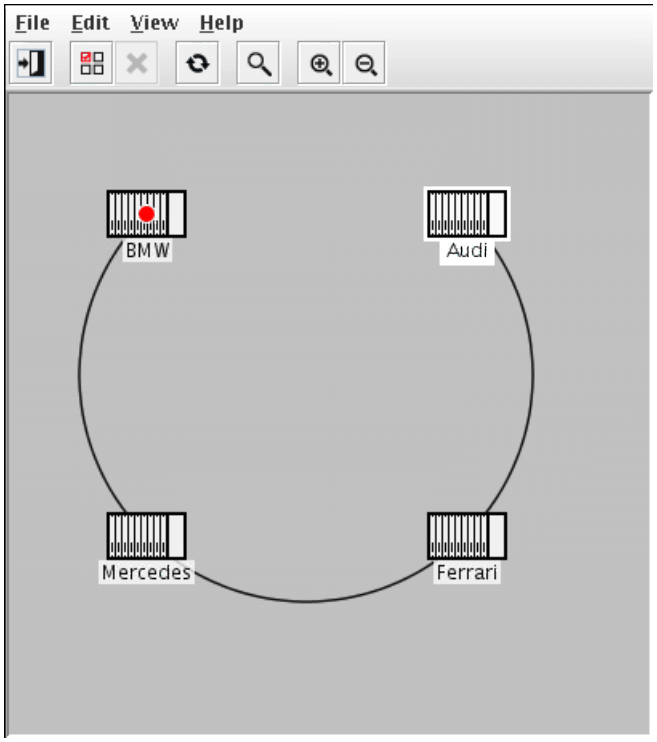
Table 4: Link end ports

Parameter	Description
Port Roles	Shows the link end port's role. Note: In RSTP, the port role is not applicable and will be shown as "N/A".
Priorities	Shows the configured port priority.
Port State	Shows only the Forwarding port state (since only forwarding links are shown in the map)
Path Cost	Shows the administratively assigned value for the contribution of this port to the path cost towards the spanning tree root.

6.10.2 Ethernet Ring Protection Switching (ERPS) Map

Please note:
This feature is not available for ERPS configured on EoS ports.

The ERPS map displays the ERPS ring view of a selected NE with ERPS configured.



- Bridge node
  - All bridge nodes show the bridge name (the NE name known in FOXMAN-UN). If the bridge has a port with status Blocking, this is indicated by a red circle marker.
  - a tool-tip on the bridge node shows additional information of the bridge:

Table 5: Bridge node

Parameter	Description
Name/IP Address	The ERPS Bridge Name /IP Address
MAC Address	The Local bridge MAC address
Blocking ports	The slot/port# of ports which are blocked

  - a double click on bridge node opens the FOXCST of the corresponding NE with user class “Information”.

    Verify that FOXCST is defined in the “client_cst_doubleclick_default” parameter of /opt/nem/etc/cst.conf.

- Links
  - Links are represented with dark gray lines between bridge nodes. Only links with forwarding endpoints are shown.
  - a double click on a link opens the Section Manager and the section on which the link relies is shown.
  - a tool-tip on the link shows additional information of the link end ports:

Table 6: Link end ports

Parameter	Description
Name/IP Address	Shows link end’s NEs Names/IP Addresses
Port	Shows link end ports’ /unit-slot/port#
Port Role	Shows the link end port role. Currently displays only “None” as port role.
Port State	Shows the link end port states. Currently displays only “Unblocked” as port role.

7 Networking Package

7.1 Introduction

Today telecommunication network operators face unprecedented pressure to embrace operating efficiency. Fast service provisioning together with lean operation and maintenance crews providing a high quality of service have become crucial objectives for service providers. Cost, pressure and lack of experienced network design engineers are other problems operators have to deal with.

By automating the network and service provisioning processes the Networking Package (NP) provides the necessary features to fulfill the above mentioned customer demands. This application provides a superior solution that satisfies the needs of network operators in their daily work - configuring and maintaining their network. Both service provisioning and capacity planning – supported by the powerful reporting capability – across multiple transmission technologies provided by the FOX61x and FOX51x platforms.

The Networking Package (NP) provides an end-to-end provisioning of circuits and trails across FOX61x or FOX51x networks (excluded from the NP are MPLS-TP circuits which are managed by the ENP, see 8 "Ethernet Networking Package").

As access networks are located in the periphery of operator networks, connecting the subscribers to the various services located on servers or switches in the central offices, it is necessary to create circuits starting in a FOX61x or FOX51x network and terminating in the equipment delivered by another vendor. These types of applications are well supported in the Networking Package.

The NP offers a faster and much more convenient solution for the user, compared to the circuit configuration based on the FOXCST or UCST, where the cross-connects have to be configured for each network element individually. In addition, operators have the possibility to document the circuits according to their company internal standards.

The ability to create all types of protected end-to-end connections supported by the hardware of the FOX61x/FOX51x allows the operator to provide services with a high reliability. The switchover to the protected circuit in case of failure is done by the hardware in less than 50 ms.

The Networking Package is offered as a separate option to the FOXMAN-UN Basic Package.

It does not require installation as it is installed when the Basic Package itself is installed.

The Administrator can grant access rights to the Networking Package for other operators from the main Security menu.

It is enabled if ‘Networking Package’ option is activated in the License Key.

Please note:
For detailed information, please refer to the “FOXMAN-UN Networking Package” User Manual.

7.2 Terminology

Before describing the features of the Networking Package it is useful to gain an overview about the terms and objects used in the Networking Package software. The design of the object model and the implementation of the various transmission layers are following the ITU-T recommendation G.805. This allows presenting the connections in the FOX51x or FOX61x network in a manner which is familiar to the operators of network management systems in the telecommunication industry.

The following table gives an overview about the most often used terms:

Table 7: NP Terminology

Functions	Descriptions
Application	The application is the main object in NP. Any creation, modification or deletion of connections is done within an application. An application contains Transport Entities (TE): circuits, trails or sub-network connections. The user manages the connections of the network through applications.
Transport Entity (TE)	A transport entity is a connection through the network connecting two termination points on the same layer rate. It is the collective term in NP for circuits, trails, sub-network connections and Unknown.
Circuit	A circuit connects the subscriber at the border of the network with either another subscriber at the other end of the network or with a server or switch in the central office. The circuit is the end-to-end connection through the network. The major task of NP is the handling of circuits.
Trail	A trail is a connection within a network carrying circuits or other trails. Every circuit has to be created over a trail. A trail is representing a connection between two trail termination points (routed over a part of the network) with a certain bandwidth. A good example is the VC-12 trail created over several STM1 sections providing 2 Mbit/s. This VC-12 trail will be used to route and transport circuits through the network.
Subnetwork Connection (SNC)	A subnetwork connection represents a connection between two points inside the network, usually to connect two border points of a sub-network managed by another group of the network operation center. A SNC will be used to carry trails or circuits.
Unknown	An Unknown represents a Transport Entity not recognized by the Networking Package as one of the above described TEs. Such transport entities require actions to be taken by the operator for further analysis.
Matrix Connection (MC)	A Matrix Connection is a connection between two connection points of two units in a network element. In the FOX51x/FOX61x documentation and in the other chapters of this document they are referred as cross-connections.
Link Connection (LC)	The Link Connection is a logical connection within a trail. In other words, a trail provides one or several link connections, which will be used to carry circuits or other trails.
Sections & Topological Trails	Sections are physical connections between two network elements (refer to «2.5.5 "Sections". In Networking Package Sections are called Topological Trails.

7.3 Functionality

The Networking Package comprises the software that provides the functionality to:

- semi-automatically or automatically provision trails and circuits;
- scan an existing FOX51x or FOX61x network and determine the existing end to end connectivity (Support of complex constructs such as Broadcast, Data Multi-Point and Voice Conference);
- manage any connections that are discovered;
- generate reports of the network;
- provision a network made of FOX51x NEs, FOX61x NEs and Foreign Objects (FOs are defined as network elements that are not managed by FOXMAN-UN Basic Package but are represented in it as part of the network).

7.4 Configuration

7.4.1 Main Window

The main Window displays the list of all existing Application Filters, Applications and Transport Entities (TEs). Each Application displays details of all its TEs.

There is likewise an event logger at the bottom, which can be cleared as required.

The Main Window allows to:

- Create/Edit/Delete Filter;

- The Filter is used to retrieve and display only a specific list of Applications or Transport Entities (TEs);
- Refresh Filter List;
- Create/Edit/View Application;
- Create/Edit/View TEs;
- View the Application Mgr. list, which displays all currently on-going Application Edits;
- Displays the “Out of Synch” and “Pending Changes” indications.

  The “Out of Sync” indication means the NP/BP Databases are de-synchronized. The NP User has to run “npresynch”.

  The “Pending Changes” indication displays the number of pending changes or downloads of changes to the NE(s). The user has to wait until this indication is cleared before he can continue with Application Edit.

Please note:
For detailed information on User Workflow and NP troubleshooting, please refer to the User Manual “FOXMAN-UN Networking Package”.

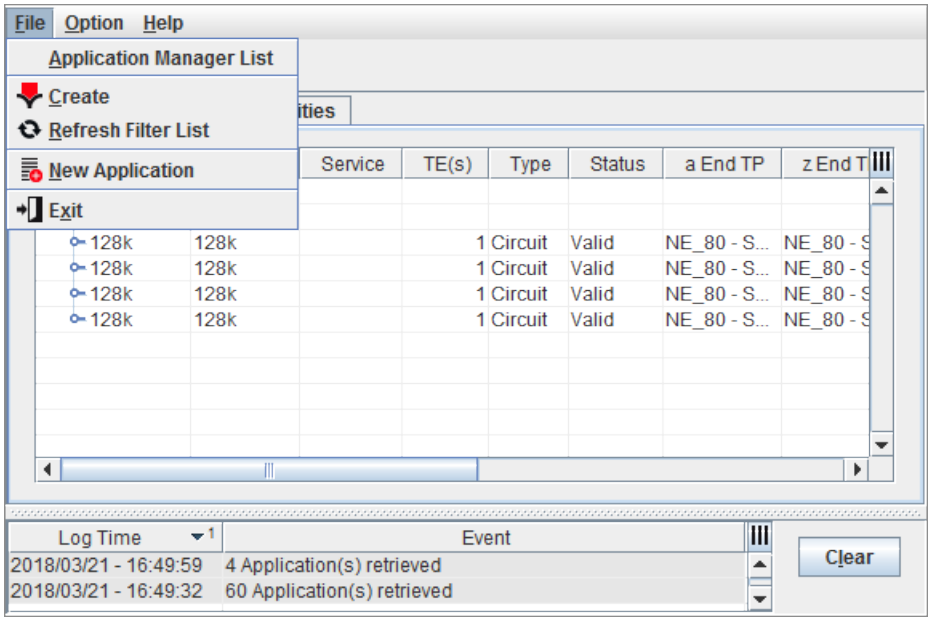


Figure 50: Networking Package (NP) Main Window

The TE is a connection that is created utilizing existing network configuration information such as cross connections and Sections, also known as Topological Trails. The TE brings data from one source termination point to one or more sink termination points in the network at various physical (STM-1, E12, E-DSL, …) and logical rates (P0, P12, VC12, …). The recognition of the TE requires a global view of the network as opposed to an element view.

Four TE types are supported in NP:

«Circuit», «Trail», «SNC» (Sub-Network Connections) and «Unknown».

The TE is built into an Application so that it can be managed in FOXMAN-UN NP. All the user actions are performed through the Application. The Application itself is downloaded to the network and saved in the database in its entirety.

If required the TE can be modified.

7.4.1.1 Status Indications

The most demanding task of FOXMAN-UN NP is to keep the network configuration up-to-date with the network elements configurations. This is in particular the case when concurrent users are doing changes with multiple networking instances or changes the network element directly via FOXCST or UCST.

Due to the nature of concurrent changes (race condition when changes common objects) in the NE and NP, the de-synchronization of NP Data with BP /NE Data cannot be avoided.

To easily detect these situations, the following visual indications on the Main NP User interface are implemented:

Out of Synch Indication

- NP/BP Databases are de-synchronized or the NP is waiting for network element configuration change confirmations
- The NP User has to run “npresynch”

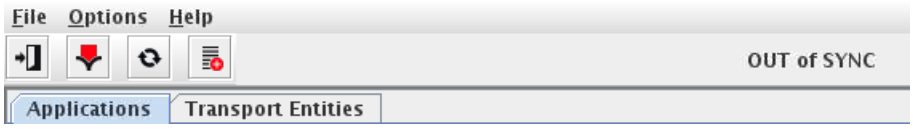


Figure 51: Out of Synch Indication

Pending Changes Indication

- Indicates the number of pending changes or downloads of changes to the NE(s)
- The NP User has to wait until all the pending changes indications are cleared before he can continue with Application Edit

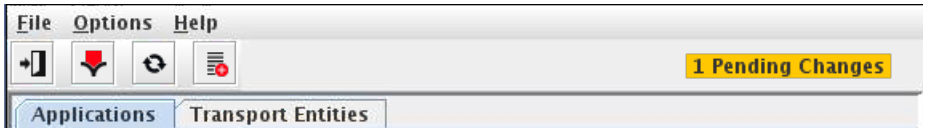


Figure 52: Pending Changes Indication

Refresh of the Filter List Indication

The “Refresh Filter List” button becomes active when

- the object download is terminated, the “Pending Changes” indication cleared. This indicates that the changes caused updates in the database.
- when BP trail information changes e.g. creation/deletion of TDM cross connection via FOXCST/UCST

7.4.2 Defining End Point of an Application

The Endpoints A End NE and Z End NE have to be specified first before FOXMAN-UN NP can start to search for all possible hops having enough capacity to carry the P0_nc service.

In the example below the data service provisioned is based on the «Type» of «Circuit» and uses a bandwidth of a P0_nc «Layer» structure with the application being bi-directional indicated in the «Direction» field.

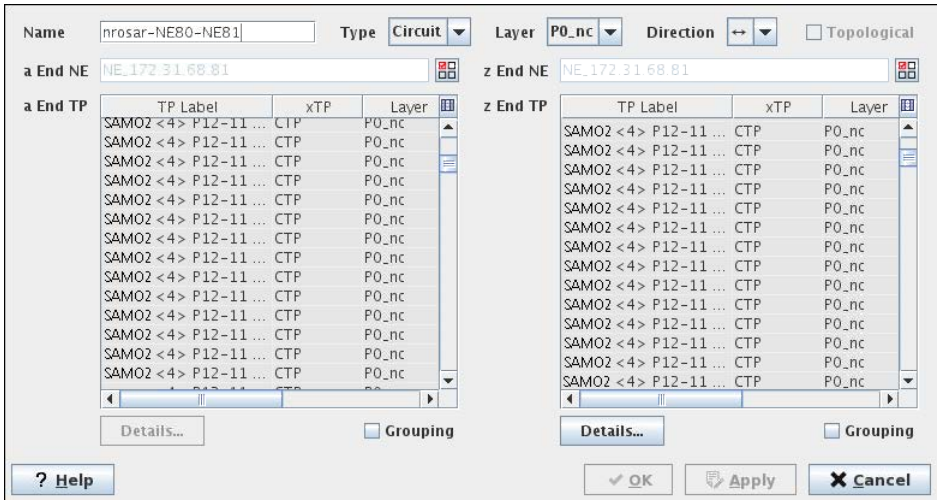


Figure 53: NP: Defining End Point of an Application

The a End Terminating Point (TP) and the z End TP can be selected via the TP Browser Table.

The detailed information of the selected or highlighted TP is called by clicking on “Details” button, which calls the TTP dialog.

The TTP dialog below provides useful information such as:

- the Layer rate of a TTP,
- the Signaling (‘CAS’),
- protection modes supported,
- etc.

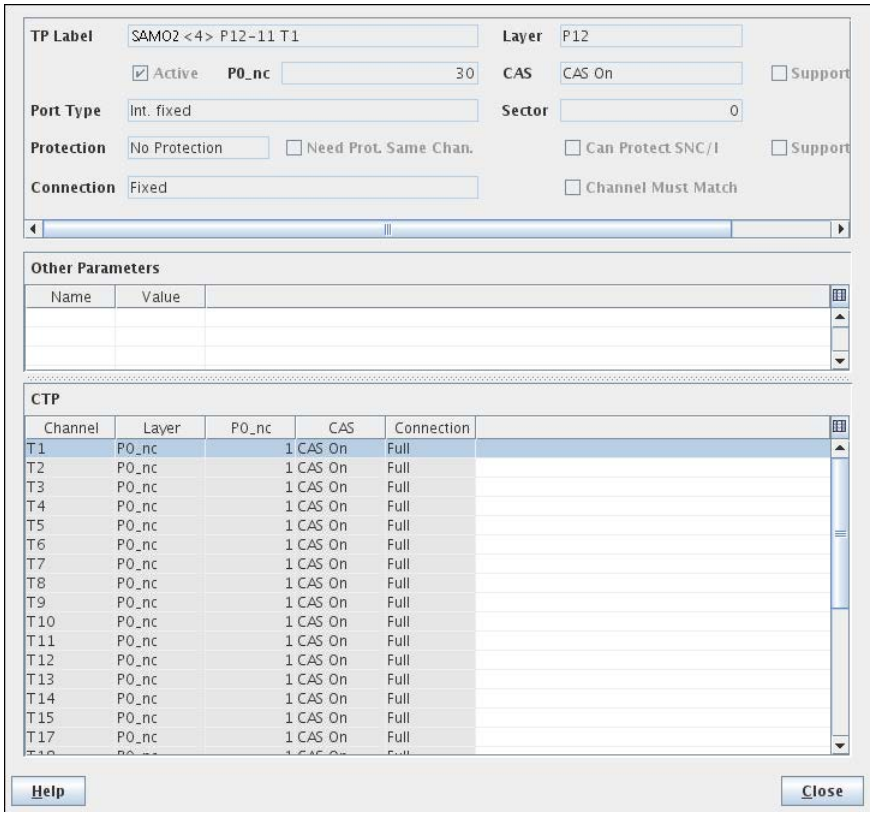


Figure 54: NP: TTP Dialog

7.4.3 Manual Circuit Configuration

The configuration of circuit provisioning is less time consuming when using the NP as it is all done in the one mask. Manual routing is done on a 'hop-to-hop' basis. The operator sequentially selects the involved NEs offered by the routing algorithm, starting from the A endpoint, till the Z endpoint is reached.

Basically there are five easy main steps for the provisioning of an end to end circuit:

1 Choose the End point (the NE and Termination Point).

2 Define the path through the network (FOXMAN-UN provides available choices at each end).

3 Choose the Channel or Timeslot to be used (per section).

4 Document the Endpoint of the circuit.

5 Activate the Configuration in the Network.

Circuits and the Network are documented at the same time.

7.4.4 Automatic Circuit Configuration

With the automatic routing FOXMAN-UN NP offers are more efficient way to provision an end-to-end circuit. The optimal route is automatically calculated and selected by the software. In order to influence the routing algorithm the operator can configure the automatic routing parameters.

The following parameters can be configured:

Table 8: Automatic Circuit Configuration Parameters

Parameters	Description
Max hop	Allows the selection of a number of hops (network elements) within a path.
Max cost	Defines the maximum costs a route may cost (based on the cost factor associated to each section).
Routing order	The routing order can be specified. This applies only if more than one route has been found between the two selected end-points. The following parameters can be specified: - Shortest (with regards to the number of network elements) - Cheapest (lowest overall costs)
Select NEs	The route **should not** go through specific network elements (FOX51x, FOX61x or Foreign)
Server rates	The route should not use Trails of a specific layer rate. Examples of layer rates are: P12 and VC12.

Furthermore, one out of three path cost calculation models can be selected by specific settings in the NP configuration file /opt/nem/etc/np.conf.

7.4.5 Protection

All types of protection schemes implemented in the FOX51x or FOX61x platforms are supported:

- End-to-end 1+1 path protection,
- 1+1 section protection,
- 1+1 multiplex section protection on SDH,
- Linear trail protection on VC-12 layer.

When NP sets up the protection paths, it automatically avoids using the same NE for passing the direct and the protected path.

In case of a failure in the working path the switchover to the protecting path is done in the hardware of the corresponding network elements, which leads to a very short traffic interruption time.

7.4.6 NP Usage

For any Transport Entity (TE), the usage of channels or containers can be shown as a property of the TE.

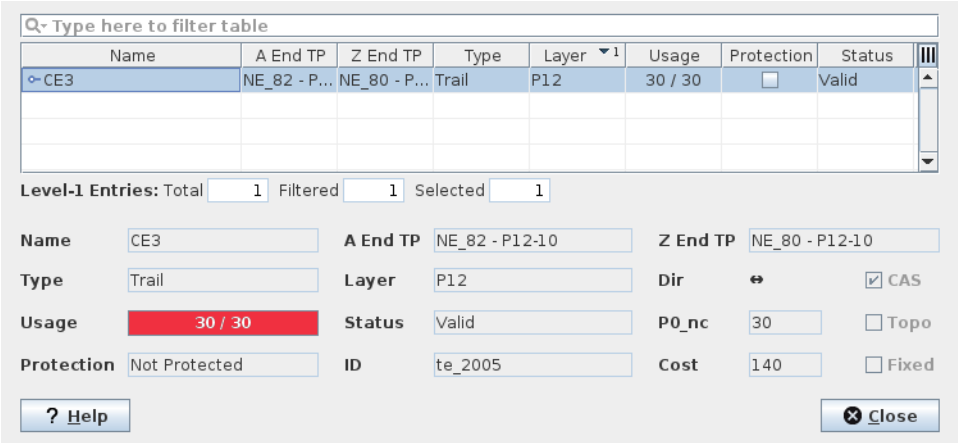


Figure 55: NP Usage Example

7.4.7 TE Graph

For any Transport Entity (TE), the network graph can be shown as logical and/or physical diagram within the same window. When selecting a TE, the graph is calculated based on the TE characteristics, and displayed in a built-in, zoomable browser window. Beside several view options, a list of possible issues can be displayed. The graphs can be saved to a png or svc file.

The logical graph shows all logical layers of the selected TE. Working and/or protecting paths, fixed TEs, TE labels, NE IDs, shared resource counts, and other view options can be set via an options menu.

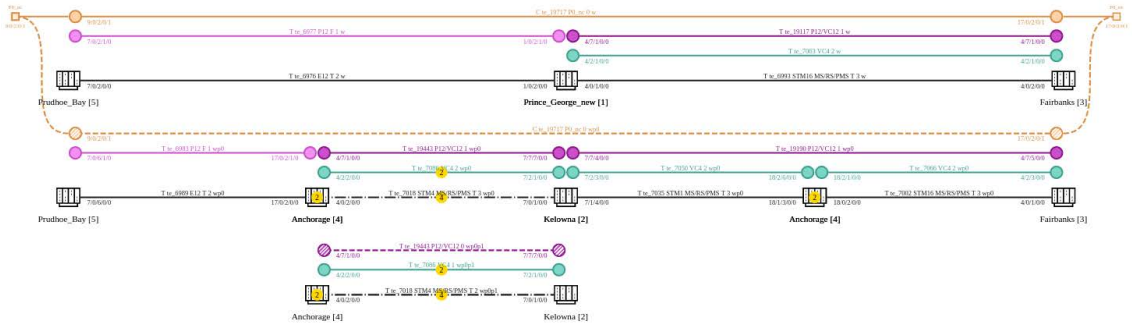


Figure 56: TE Graph - logical, Example

From the TE Graph window, the following context sensitive options are available:

- Open an NE's configuration with selectable user class;
- Open the list of active alarms for a selected NE;
- Open the NP Usage dialog for a selected section, trail, or circuit;
- Open the Application dialog for a selected element to show details on the application and the TE.

The physical graph shows the physical arrangement of NEs, sections (including working and protection), and circuit access points. Among others, working and/or protecting paths, and fixed TEs can be selected as view options. The NEs in the physical graph can be rearranged when in the edit mode.

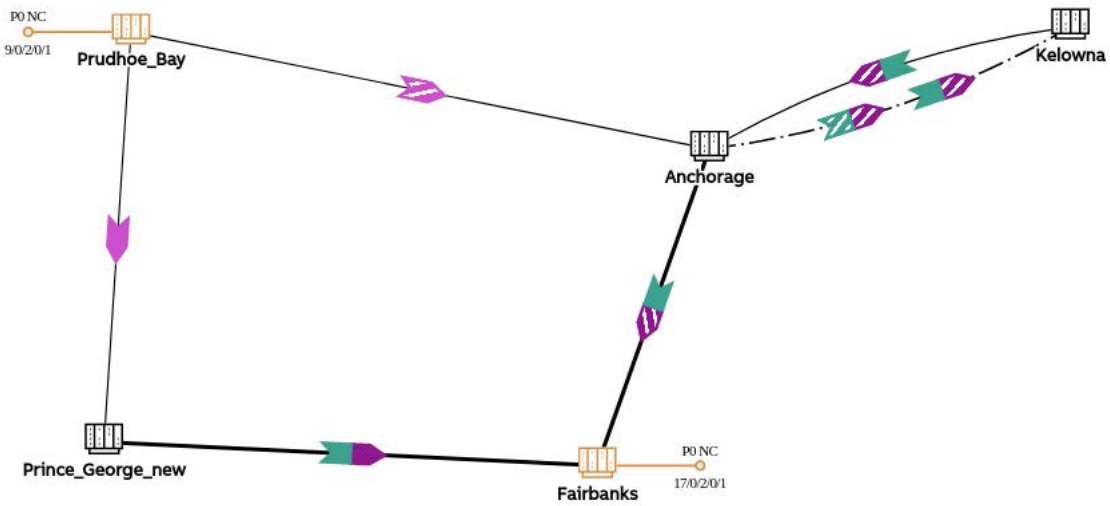


Figure 57: TE Graph - physical, Example

7.5 NP Reporting Tool

7.5.1 General

The documentation of established networks is often a time consuming and manual task. It requires a big effort to keep documentation up-to-date with the changes applied to the network.

The Reporting is basically used to generate information needed to document the existing network.

7.5.2 NP Reporting Tool

The NP Reporting Tool is part of the licensed option «FOXMAN-UN Networking Package». This powerful tool generates a set of ten report files in CSV format containing information on NEs, units, ports, applications, customers, sections and transport entities. These files can be analyzed offline by any suitable third party tool (e.g. MS Excel).

Reports are generated on the same workstation where the FOXMAN-UN core is installed. The tool can be started at any time during normal FOXMAN-UN operation.

Please note:
The NP Reporting Tool gives the possibility to edit large reports without disturbing the FOXMAN-UN NP core.

The following information is collected and stored in the report files:

- List of all network elements and foreign objects in the network with their names and types;
- List of units and software versions in each network element;
- List of all ports of all units for each network element with their names, used status, free bandwidth and time slot occupation;
- Application list with the status of each application;
- List of all Transport Entities with path details;
- List of all sections at the E12, O22 and STM-1 layer with the status of all sections;
- List of circuits per customer;
- List of trails.

Further information can be found in the “FOXMAN-UN Networking Package” User Manual.

8 Ethernet Networking Package

8.1 Introduction

The Ethernet Networking Package (ENP) handles the FOXMAN-UN MPLS-TP network functionality.

Multiprotocol Label Switching - Transport Profile (MPLS-TP) enables MPLS to be deployed in transport network and operated in a similar manner to existing transport technologies, e.g. SDH. The objective is to achieve the transport characteristics of SDH that are connection oriented, a high level of availability, quality of service, OAM capabilities[1].

MPLS-TP network provisioning can be achieved via a centralized Network Management System (NMS) for static provisioning and/or a distributed control plane for dynamic provisioning. FOXMAN-UN current version supports static provisioning.

The main characteristics of MPLS-TP are:

- Connection oriented: MPLS-TP uses Label Switched Paths (LSPs) and Pseudo Wires (PW) to deliver services.
- MPLS-TP can carry any type of client traffic such as ATM, SDH, Ethernet, etc.
- Provides network-wide Hierarchical QoS (HQoS).
- Transport layer agnostic: MPLS-TP can run over Ethernet, SDH, OTN, Generic Framing Procedure (GFP) and Wavelength Division Multiplexing (WDM).
- Provides OAM capabilities similar to those provided by SDH and OTN.
- Provides end-to-end protection and restoration mechanisms including:
  - supports 1+1 protection and 1:n protection;
  - LSP and PW protection:

    FOXMAN-UN supports 1:1 bidirectional LSP protection;
  - guaranteed 50 ms recovery time;
  - MPLS-TP restoration mechanisms support revertive and non-revertive behavior.

8.1.1 MPLS-TP Architecture and Operations

This section provides an overview of MPLS-TP forwarding mechanism as well as the major components of an MPLS-TP network.

The figure below illustrates the MPLS-TP operation as connection-oriented transport system for packets. Traditionally packet transport switches each packet independently. However, with MPLS-TP, the connection is first set up.

Beside Tunnel protection also H-VPLS Provider Edge (PE) dual homing protection is supported. With this VPLS can be protected from a failure of a node or a link at the PE.

1. Networks and Services: Carrier Ethernet, PBT, MPLS-TP and VPLS, M. Toy

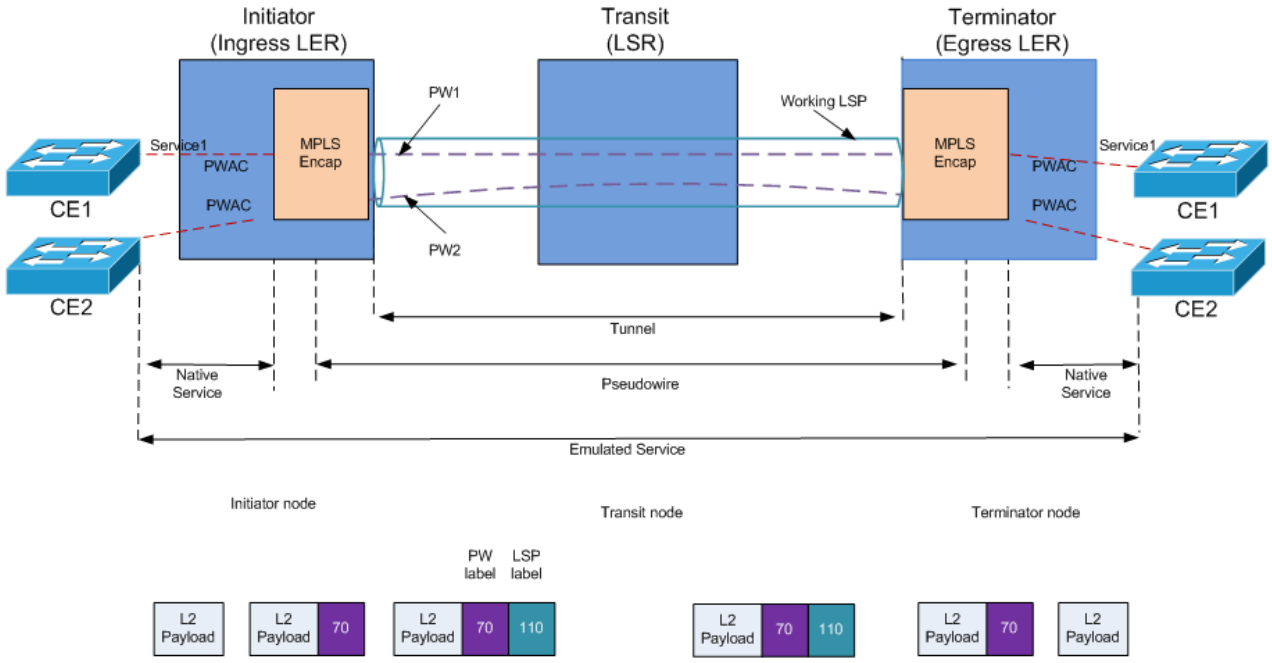


Figure 58: Simplified MPLS-TP Architecture

8.2 ENP Main GUI

The main window displays the list of all existing VPWS and VPLS Services, Pseudo Wires, Tunnels, Links, NEs, and Service Profiles or Templates. It likewise allows the operator to:

- Create/Edit/Delete
  - Class Types (as Traffic Engineering base),
  - QoS Reference Tables,
  - Services (VPWS, VPLS, H-VPLS),
  - Tunnels (protected / unprotected; encrypted / unencrypted),
  - Links (Sections),
  - Service Profiles or Templates.
- Add / Remove NEs to / from the ENP domain.
- Split existing Link and insert NE,
- Reroute existing Tunnels,
- View Details of Services, Pseudo Wires, Tunnels, Links, NEs, and Service Profiles or Templates.

8.2.1 Hierarchical QoS

The HQoS Configuration Manager provides all required settings for the implementation of HQoS in the MPLS-TP network, such as

- Class Type definition,
- Selection of allocation model: RDM (Russian Doll Model) or MAM (Maximum Allocation Model),
- Service Category definition,
- HQoS Profile definition and allocation of Class Type Shapers to links and/or nodes of the complete network or to parts of it,
- HQoS Constants definition,

allowing the operator to implement and apply Class Type shapers and bandwidth enforcement throughout the network.

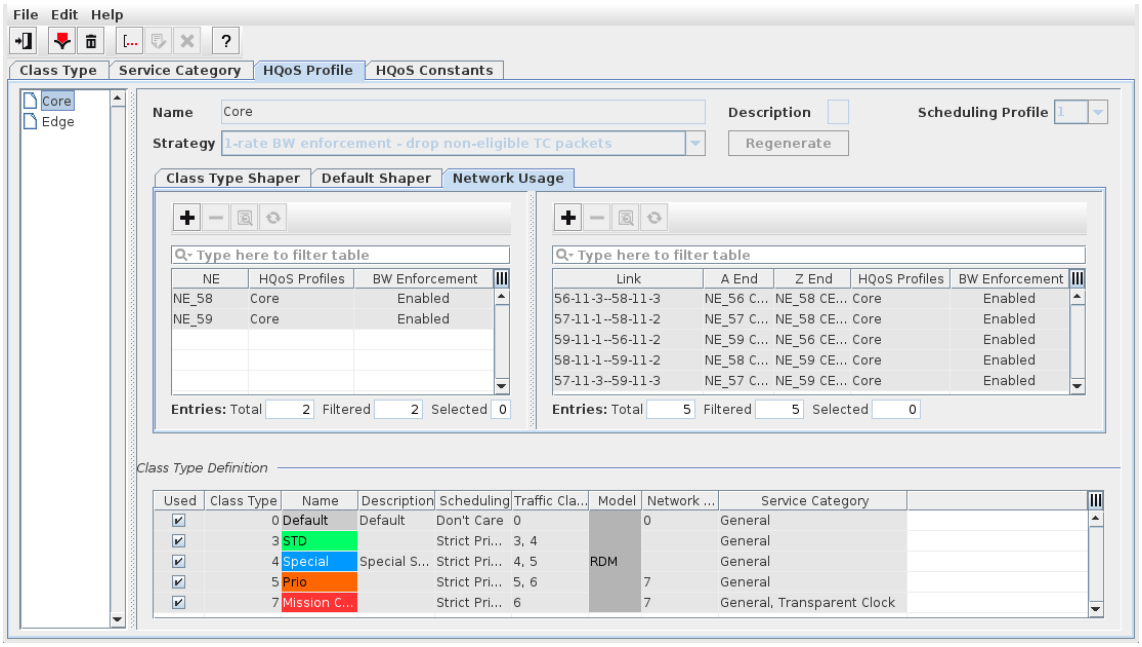


Figure 59: HQoS Configuration Manager Dialog (Expert Mode View)

8.2.2 Class Types

Both basic QoS and HQoS use Class Types for bandwidth and traffic classes control.

Class-Types are required during creation of Service Profiles, and applied to services (VPLS, VPWS), Pseudo Wires, and Tunnels. The Class-Type definition - available in the “Tools” menu of the ENP main window - is therefore the basis for the complete MPLS-TP network and needs to be done as a first step during network configuration & commissioning.

Class-Types can be exported and imported.

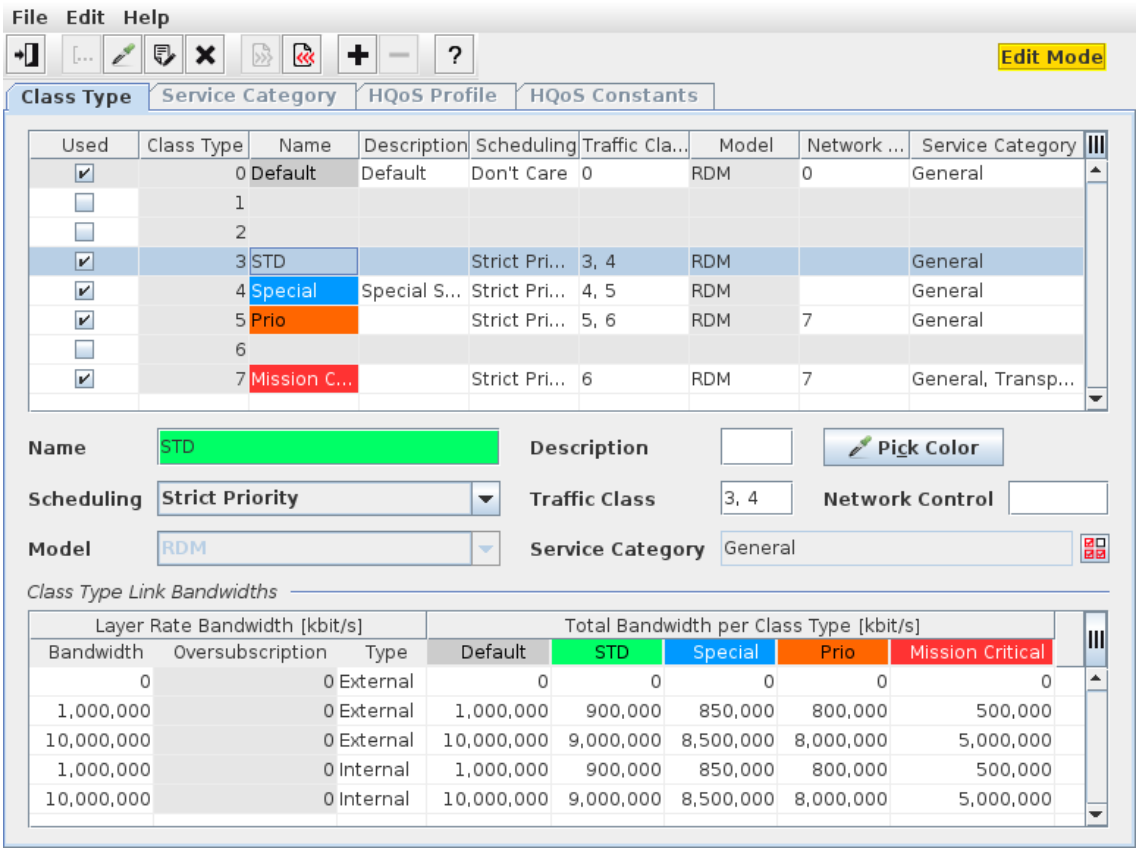


Figure 60: ENP Class Type definition dialog

With basic QoS, the alignment of the NE's QoS reference tables throughout the network is done via the "Schedule Network Alignment" dialog.

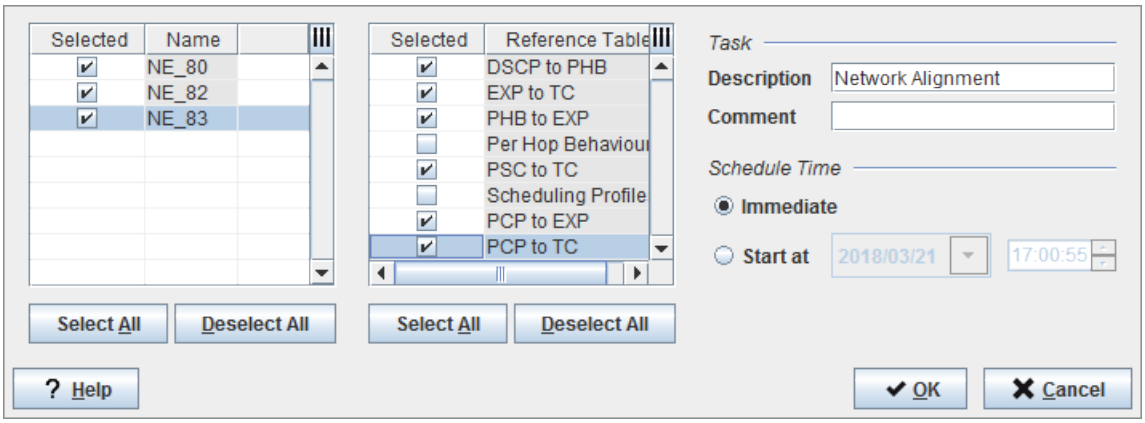


Figure 61: ENP "Schedule Network Alignment" task creation dialog

An audit function verifies the alignment of QoS reference tables in the network. Audits can be initiated immediately or on a scheduled, regular basis.

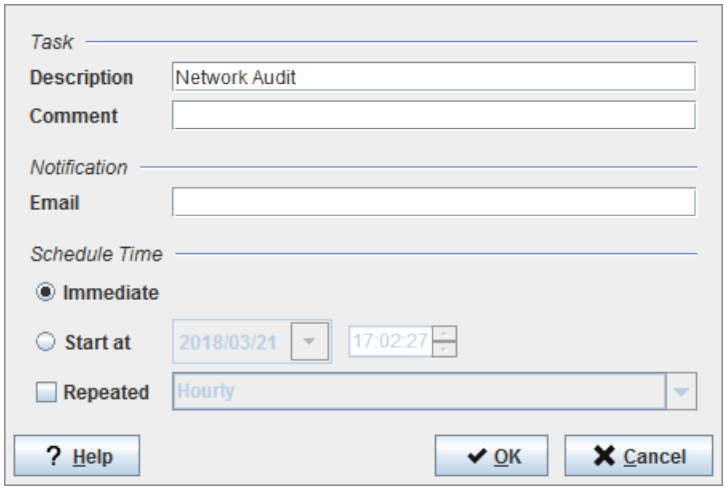


Figure 62: ENP “Schedule Network Audit” task creation dialog

Audit results can be displayed, and the corresponding audit reports are stored in the NEM database. The reports can be exported for further processing.

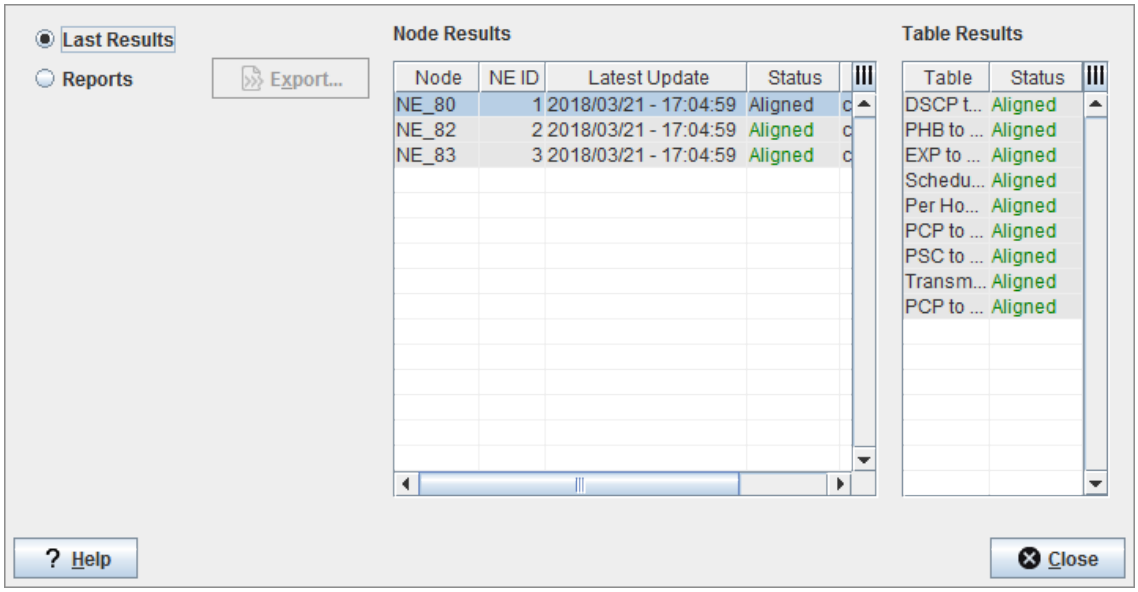


Figure 63: ENP “Network Audit Last Results” dialog

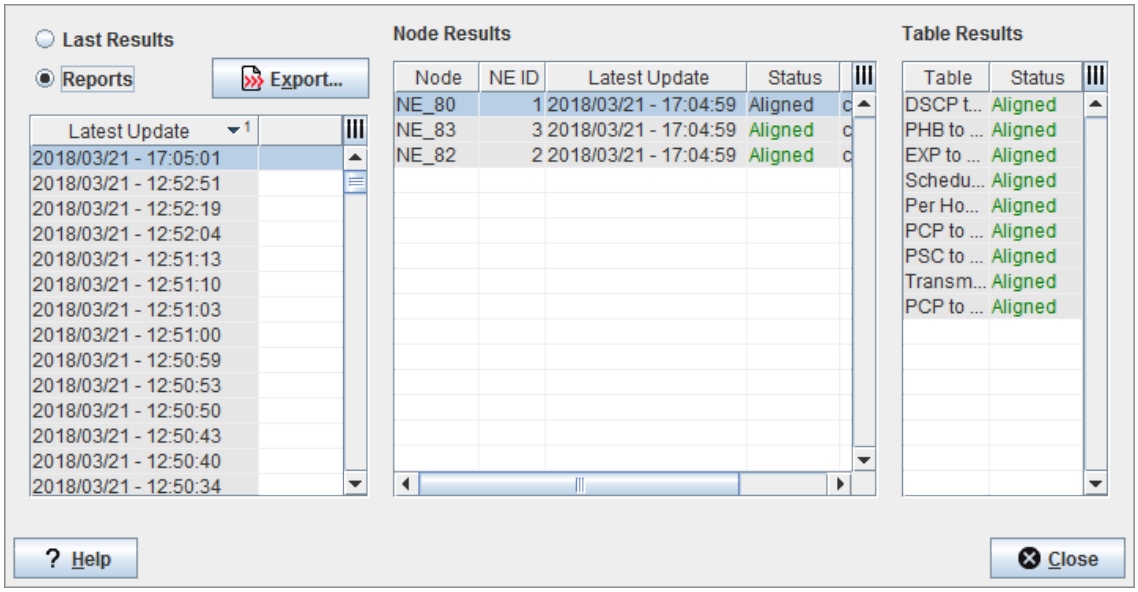


Figure 64: ENP “Export Network Audit Results / Report” dialog

8.2.3 VPLS Tab

A Virtual Private LAN Service (VPLS) is a multipoint-to-multipoint Ethernet bridging service. Within the VPLS instance, all member nodes of the mesh type are connected with Pseudo Wires in a full-mesh topology.

The VPLS creation also supports H-VPLS, i.e. mesh/spoke network topologies, and PE Dual Home topologies, i.e. H-VPLS PE dual-homing protection.

On each node, the Pseudo Wires are connected to a Switching Virtual Interface (SVI). A local VLAN of the node is associated to the SVI. Bridge ports are attached to the VPLS if they share the same VLAN ID with the SVI.

The VPLS Tab displays all the saved and/or deployed VPLS. It likewise allows you to create, modify, see details, deploy or delete VPLS.

The VPLS are listed in a hierarchical table that can be expanded or collapsed. The top level displays all VPLS Services. The second level displays all member VPLS NEs. Under each NE, all member ports, Pseudo Wires, and tunnels are displayed. Details of every VPLS can be shown via the “Details VPLS...” menu option.

VPLS can be modified or deleted from this tab.

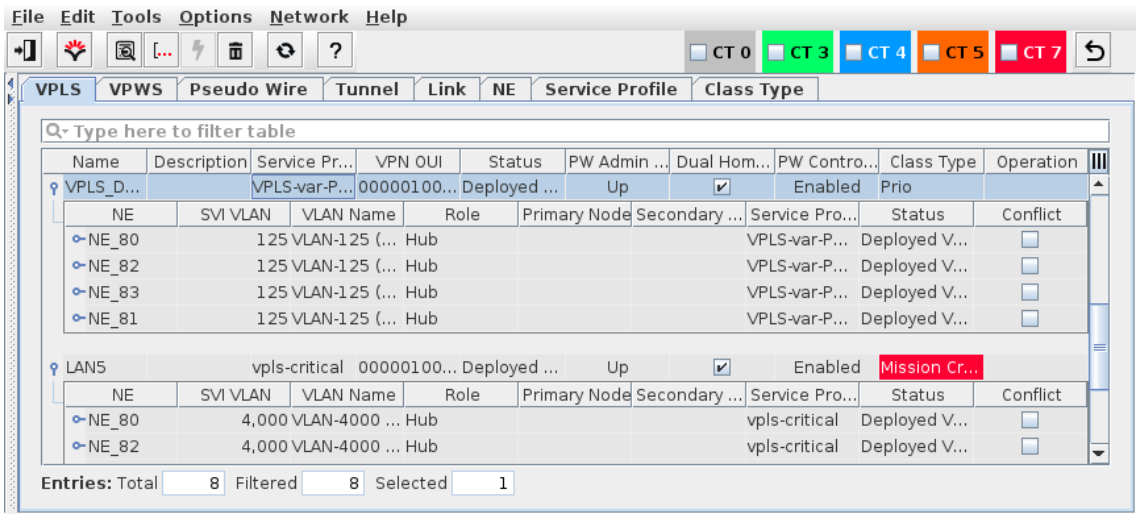


Figure 65: ENP VPLS Tab

Any VPLS that is saved in the database or deployed to the network can be visualized in a graphical viewer with many view options.

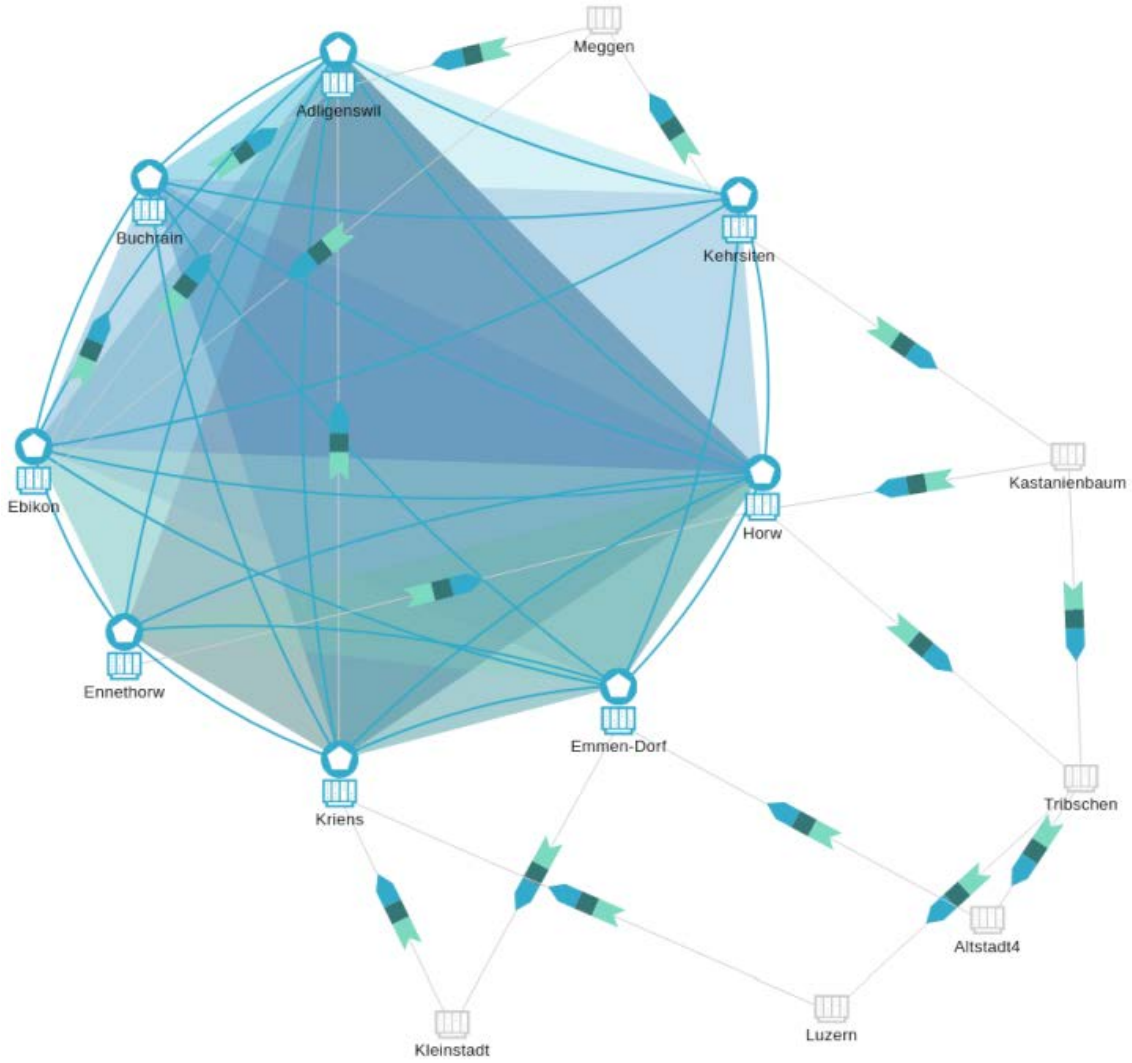


Figure 66: VPLS Graph - physical, Example

8.2.4 VPWS Tab

Displays all the existing VPWS Services

Allows you to create, modify, deploy or delete VPWS Services, or to see details of already created VPWS Services.

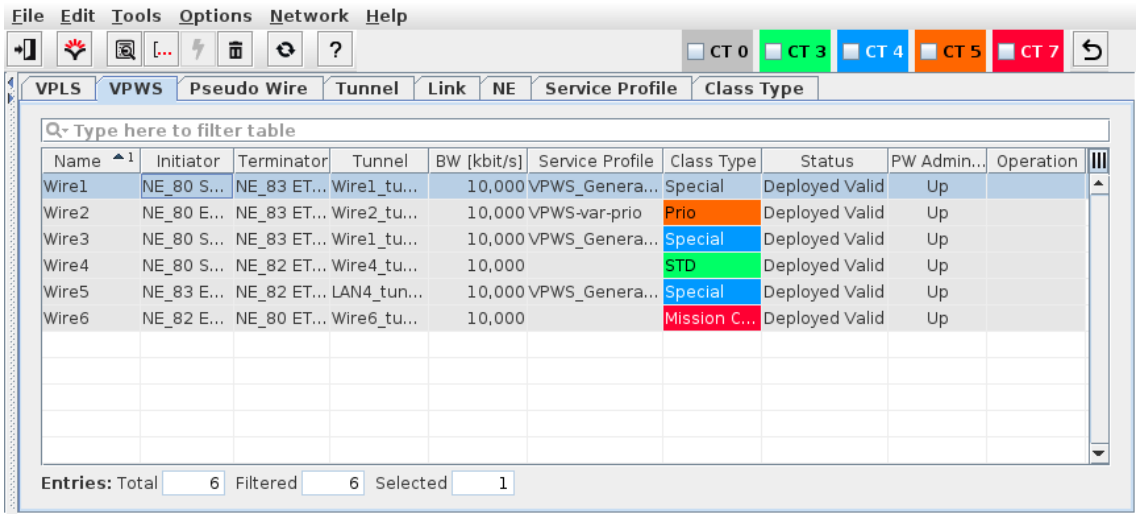


Figure 67: ENP VPWS Tab

Any VPWS that is saved in the database or deployed to the network can be visualized in a graphical viewer with many view options.

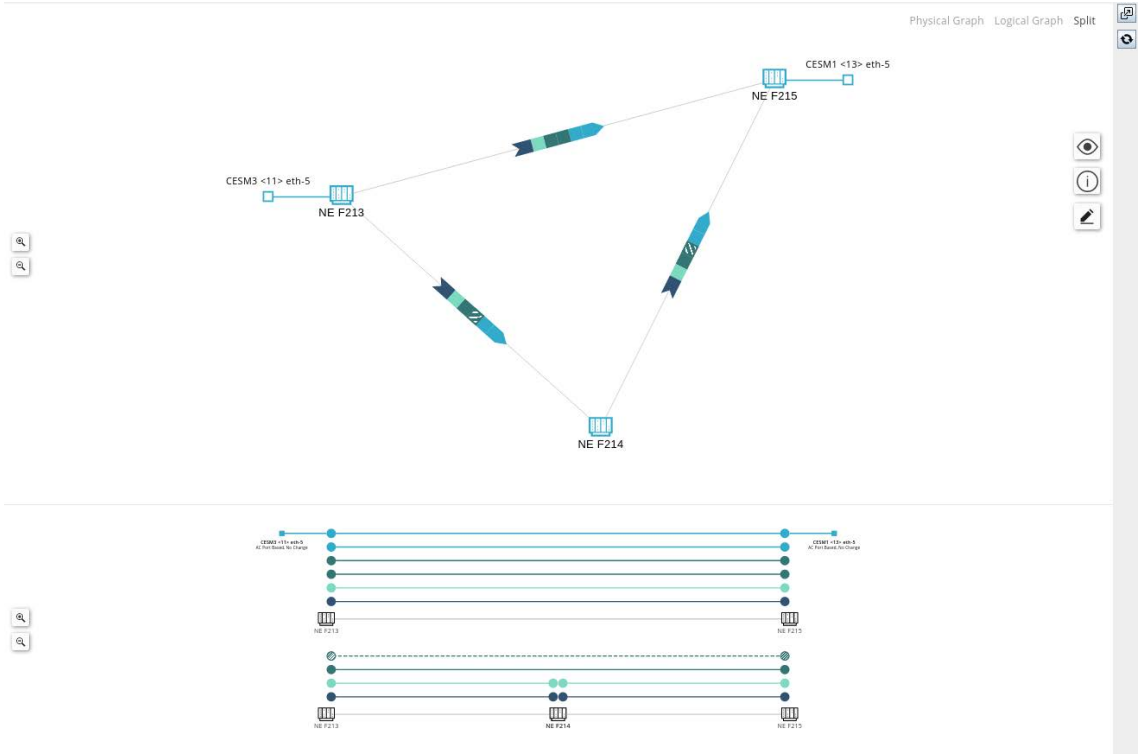


Figure 68: VPWS Graph - physical and logical in split view, example

8.2.5 Pseudo Wire Tab

Displays all the existing Pseudo Wires in the ENP.

Allows you to see details of existing Pseudo Wires.

From the details view, allows you to deploy PWs that are not yet deployed.

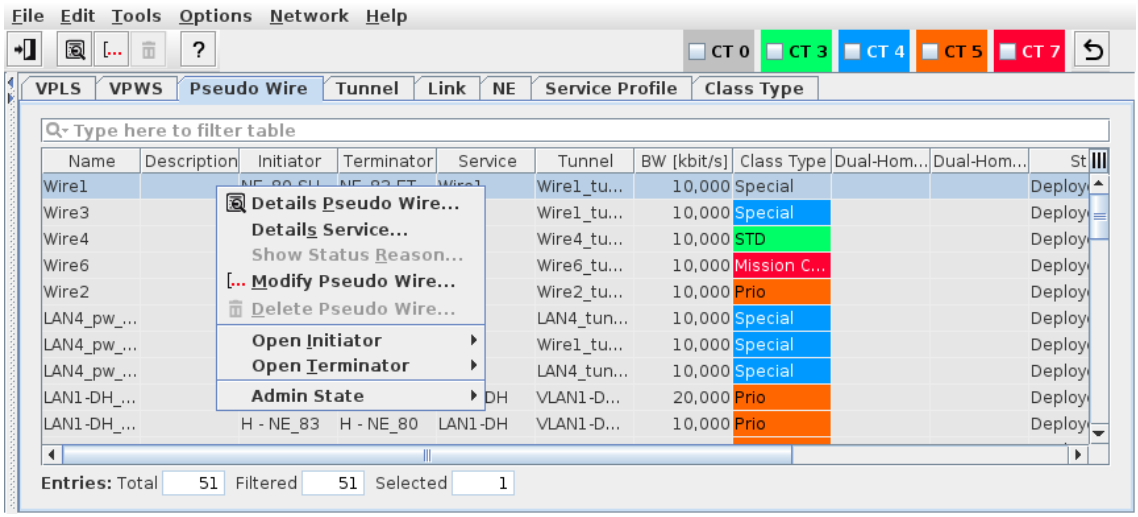


Figure 69: Pseudo Wire Tab

8.2.6 Tunnel Tab

Displays all the existing Tunnels in the ENP.

Allows you to create, see details, modify some parameters, deploy or delete Tunnels. When ENP Expert Mode is activated, Tunnels can be set to unprotected mode, or tunnel LSP element can be deleted, replaced, or rerouted.

Allows you to create Services within a Tunnel.

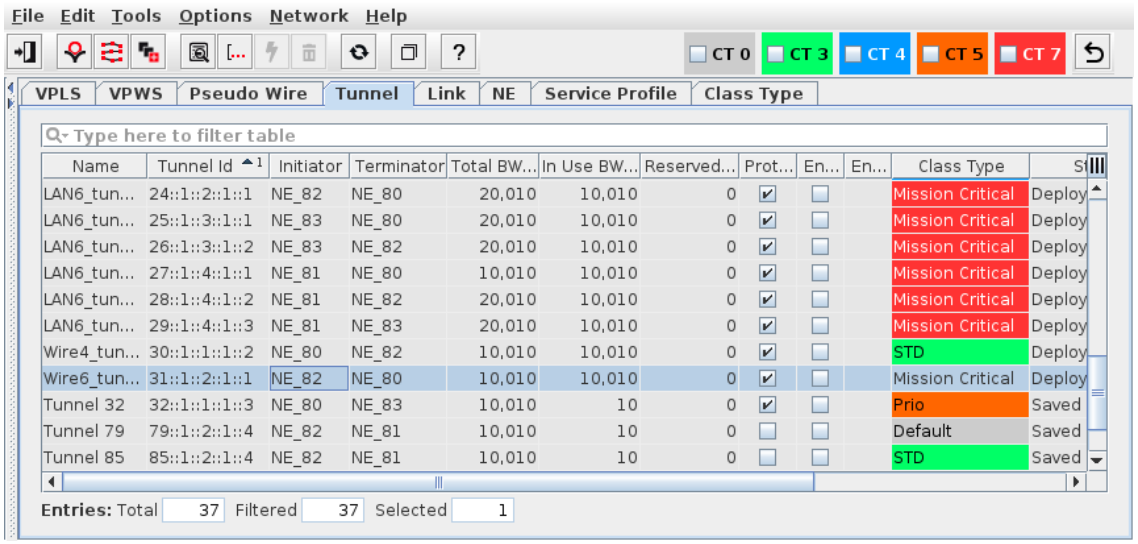


Figure 70: Tunnel Tab

8.2.7 Link Tab

Displays all MPLS or ENP links. These links are sections created via the Section Management whose endpoints are MPLS interfaces.

An ENP link has a bandwidth attribute (Available BW) used for the LSP path computation. The default Total bandwidth is computed from the physical port characteristic of the end points. The user can overwrite this default bandwidth per Class-Type for the LSP path computation and therefore applying an over-subscription to the link if required.

Allows you to modify the following parameters:

- Name,

- Total Bandwidth (per Class-Type),
- Use for Routing,
- Cost.

The Link's Name and Cost are synchronized with the Section's Name and Cost.

A link can be expanded / collapsed in the Link list. When expanded, the link's Class-Types with their related bandwidths and further parameters are displayed.

A link can be split for insertion of a new NE. The tunnels that were carried over the previous tunnel are re-routed over the two new links and the inserted NE. This procedure requires activation of the ENP Expert Mode.

A graphical view shows the bandwidth usage for every Class-Type when selected in the expanded view.

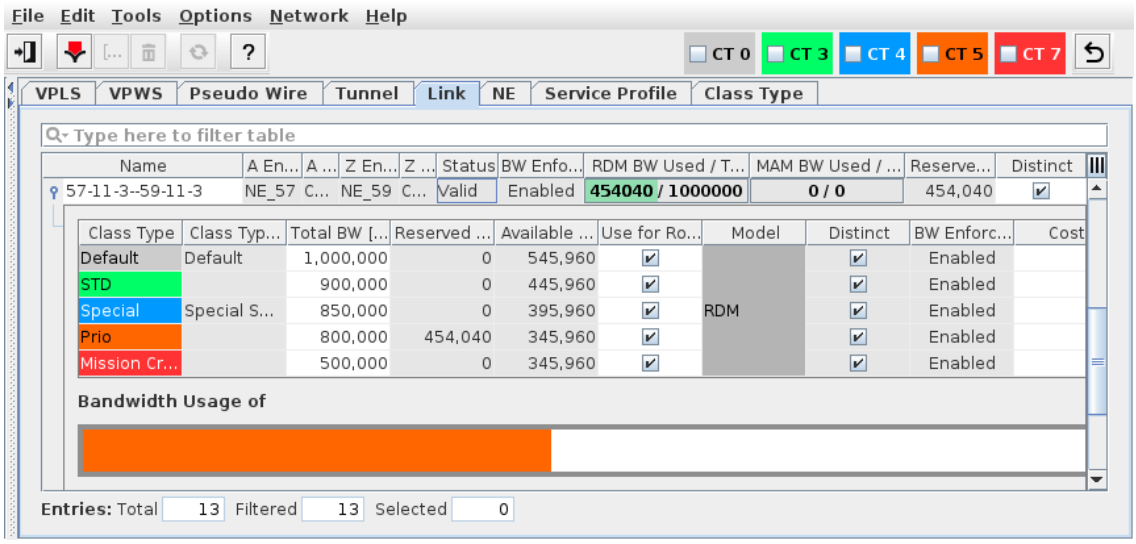


Figure 71: ENP Link Tab

8.2.8 NE Tab

Displays the ENP-Nodes domain's member NEs.

Allows you to add/remove NEs to the ENP-Nodes domain.

Allows you to set/modify the Global ID, Node ID and Description of NEs not yet added to the ENP-Nodes domain.

Displays the selected NE details, which include the following information:

- MPLS details including the node's Global ID, Node ID, and Description.
- Lists of VPLS/VPWS and tunnels in which the NE is involved.
- List of the NE's available bridge ports and VLANs.The bridge port is the Port attached to the bridge on the node with type CVP.

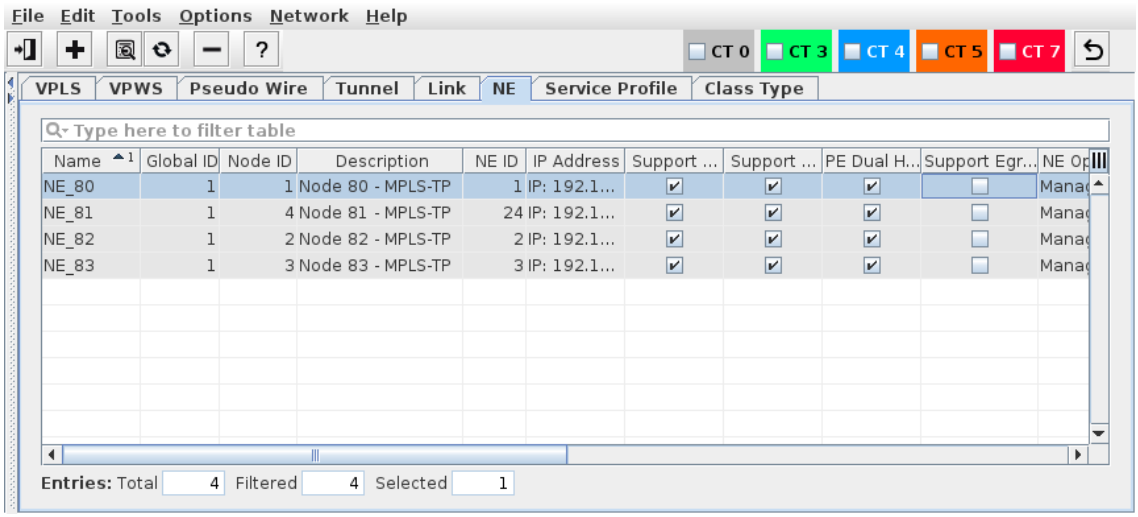


Figure 72: ENP NE Tab

8.2.9 Service Profile Tab

Displays all the existing Service Profiles.

Allows you to create, edit and delete Service Profiles.

Service Profiles are required for consistent Class Types over the MPLS network. The use of Service Profiles requires a valid license option. Service Profiles are based on the Class-Type definition available in the “Tools” menu of the ENP main window.

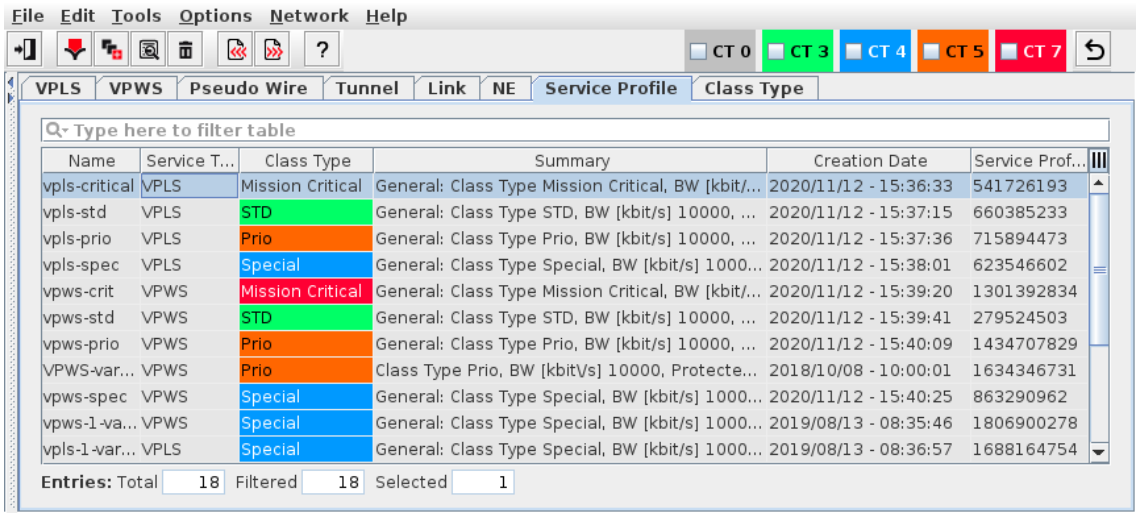


Figure 73: ENP Service Profile Tab

8.2.10 Class Type Tab

Displays the active Class Types that have been configured via the “Tools - Edit Class Types” dialog.

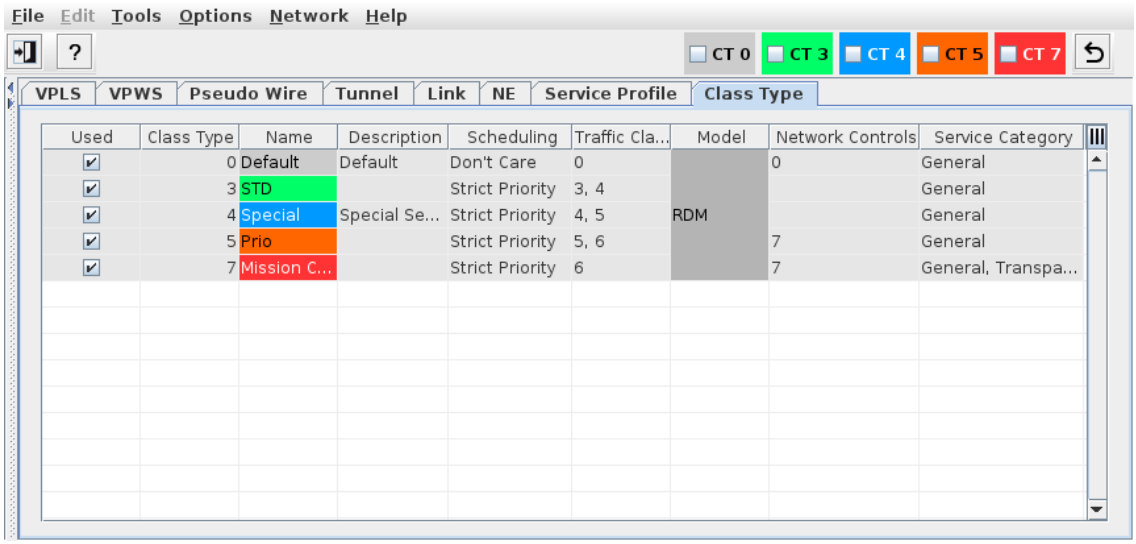


Figure 74: ENP Class Type Tab

8.3 Create Service Profile

Allows you to create or modify VPLS or VPWS Service Profiles.

The service profile provides initial settings when creating or modifying Services and Tunnels.

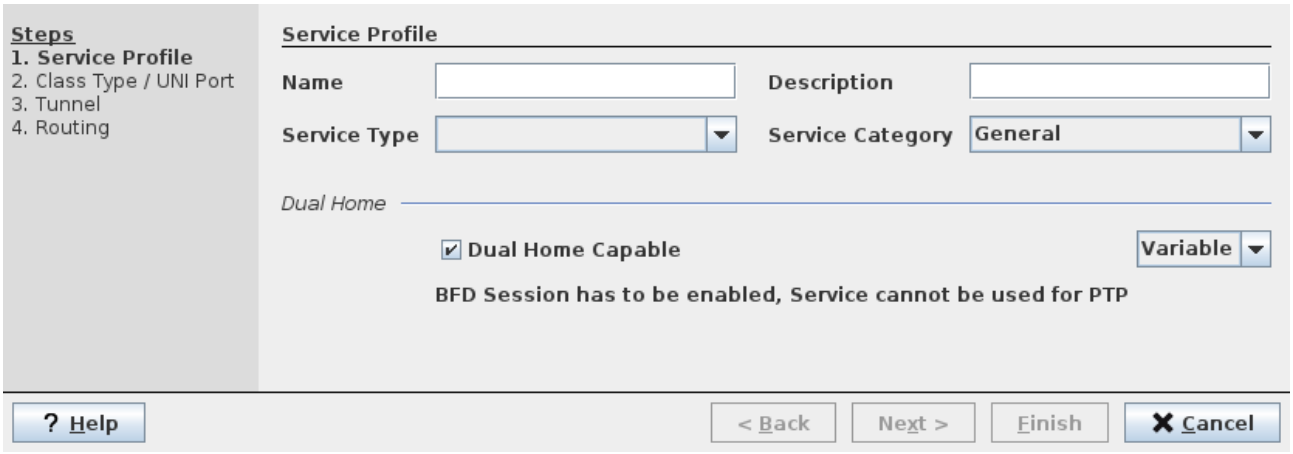


Figure 75: “Create Service Profile” Wizard (step 1)

The wizard includes four steps with the following subjects:

- Service Profile main characteristics, including the selection of the service type (VPLS, VPWS) and of the PE Dual Home option,
- Class Type / UNI Port specification,
- Tunnel details,
- Routing details.

Service Profiles are stored in the NEM database. They can be exported and imported.

8.4 Create Service

The Create Service Wizard allows the user to create services of type Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS) and save these to the database. Saved services can be applied to the network by deploying them.

The Create Service wizard contains a maximum of six (6) steps:

Create VPWS

1 Define Service;
2 Define Attachment Circuit;
3 Define Tunnel(s);
4 Create Tunnel(s) Manually;
5 Summary (Save).

Create VPLS

1 Define Service;
2 Define VPLS NEs;
3 Define VPLS Topology;
4 Define Tunnels;
5 Create Tunnel(s) Manually;
6 Summary (Save).

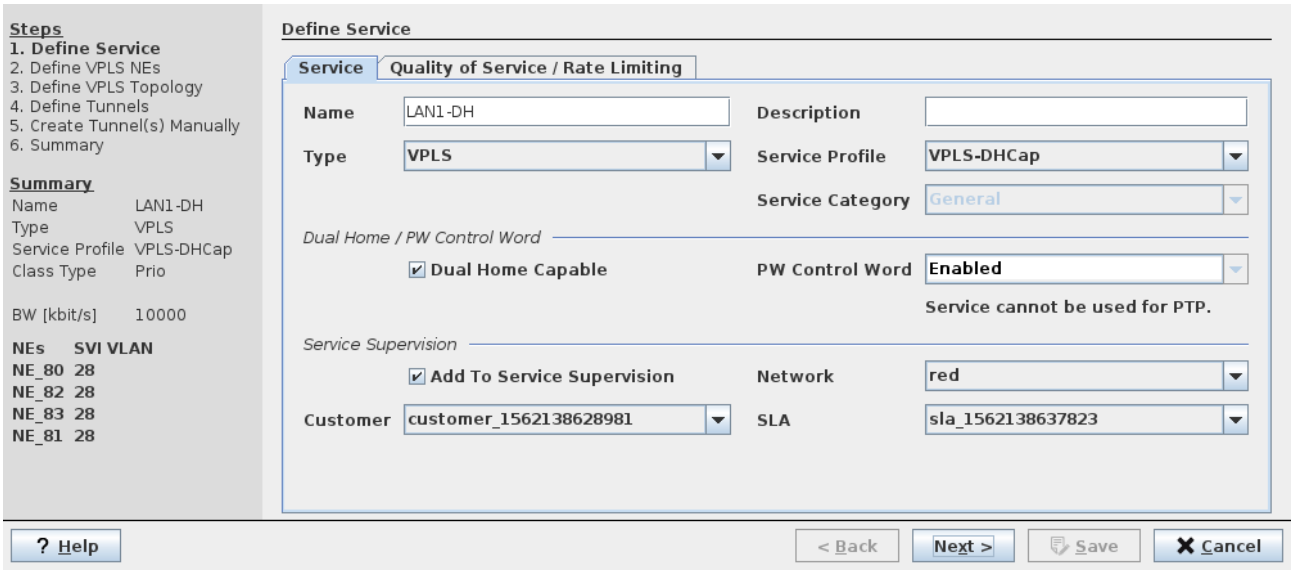


Figure 76: “Create Service” Wizard (VPLS, step 1)

8.5 Create Tunnel

Allows creation of Tunnel with working and optionally protection LSP. The LSPs can be created via Manual or Automatic Routing.

The created LSPs are co-routed bidirectional LSP. This means the forward and reverse directions of a bidirectional LSP follow the same path, that is the same nodes and links from nodes A to Z or from nodes Z to A.

During Tunnel configuration, the path bandwidth, Bidirectional Forward Detection (BFD) session to detect failure condition on the path, and the path protection parameters can also be configured.

When Service Profiles are used some of the settings applied during tunnel creation are predefined in the profile.

The same dialogs are used in view only mode for the “Tunnel Details” view that is available for existing tunnels.

In the tunnel graph, details of an LSP element can be displayed in an informative tool-tip, Link details can be shown, and the A End NE or Z End NE configuration can be opened with the required user class.

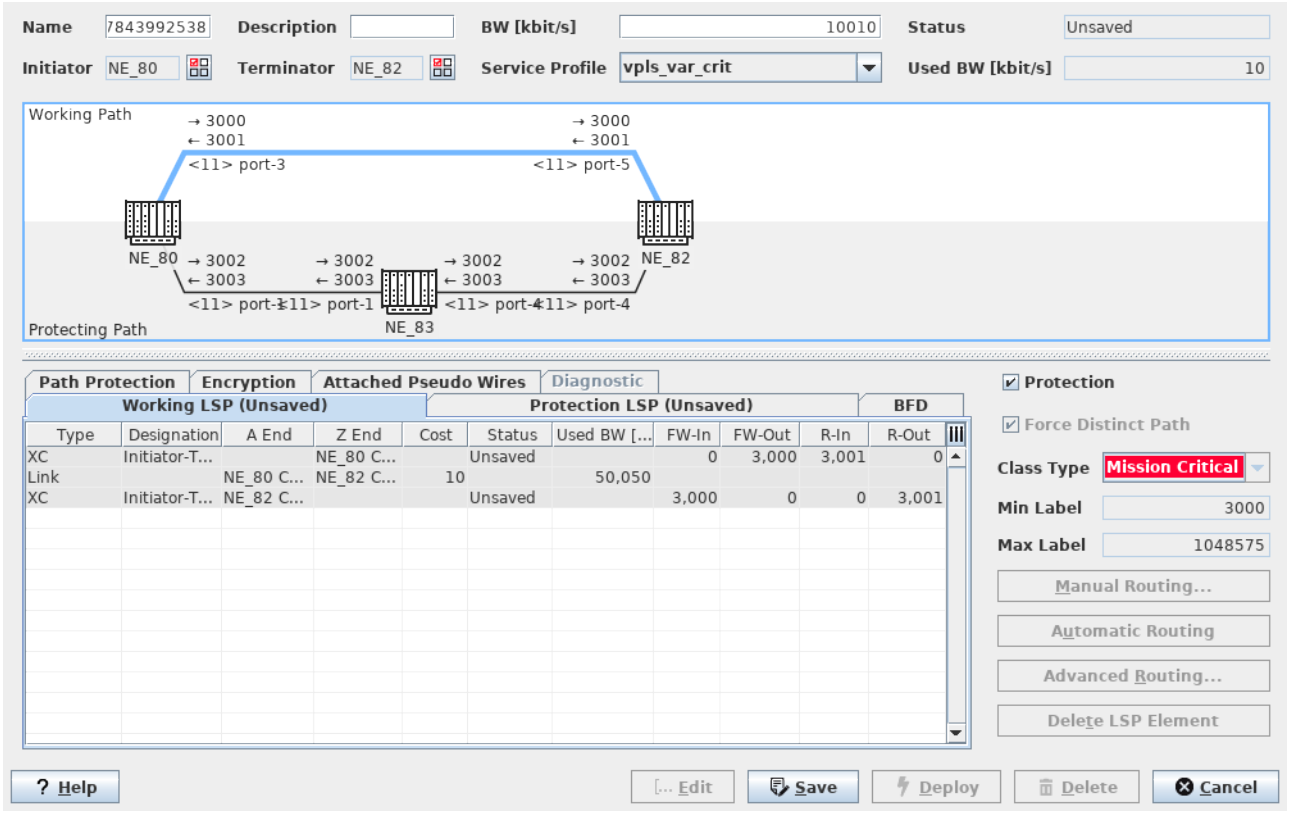


Figure 77: Create Tunnel, with Tunnel Graph

8.5.1 Manual Routing

When a Tunnel is created, the route has not been defined thus the Path contains a “Hole”. The user can select Manual, Automatic or Advanced Routing to complete the route.

The Manual Routing window returns a list of possible MPLS links with enough available bandwidth to reach the Next-Hop MPLS node. The user has to manually select each “Hop” until the path is complete.

The listed next-hop links must fulfill several constraints:

- the links must have enough Available bandwidth
- to prevent loops, the links leading to nodes already in the path are not listed. This implies that a link can only be used once.

8.5.2 Automatic Routing

Automatic Routing creates a complete LSP automatically based on the cheapest route. This means the routing engine takes into account the administrative cost of the link, which is set via section management or via NE Tab. The selected path between Initiator and Terminator, therefore has the lowest overall link cost in the network.

If Tunnel template is used, the automatic routing engine completes the path based on the template’s configured Automatic Routing Parameters. Please refer to Advanced Routing for details.

8.5.3 Advanced Routing

Advanced Routing creates a complete LSP automatically based on the configured values of the Automatic Routing Parameters.

If Tunnel template is used, the advanced routing engine will override the template’s configured Automatic Routing Parameters in completing the LSP.

Note:

The Advanced routing engine, however, will not change the Tunnel template's configuration.

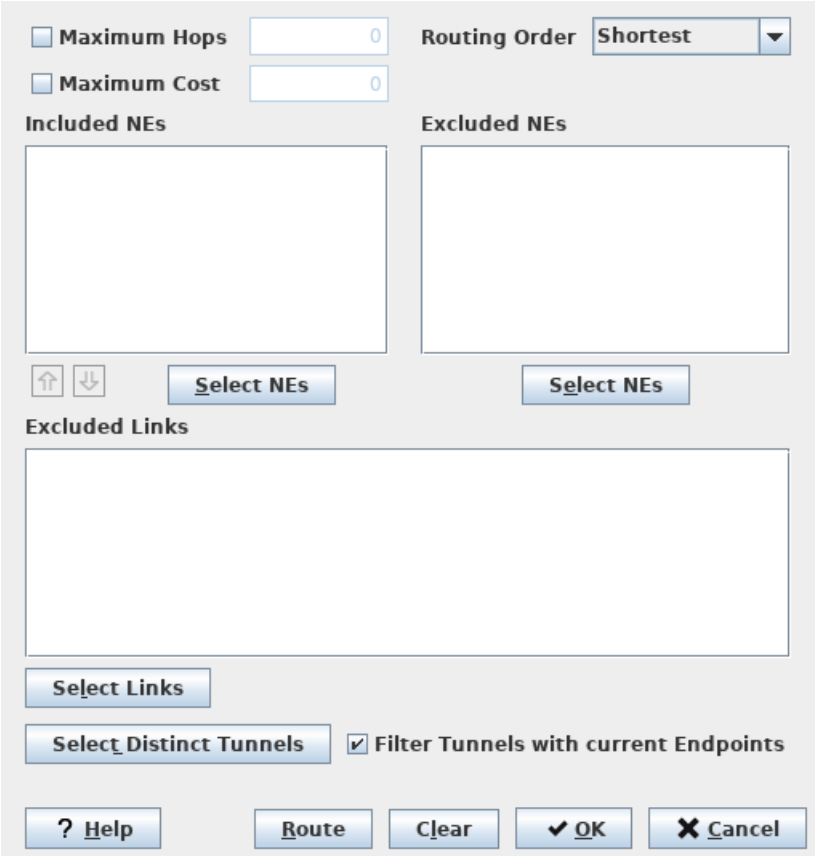
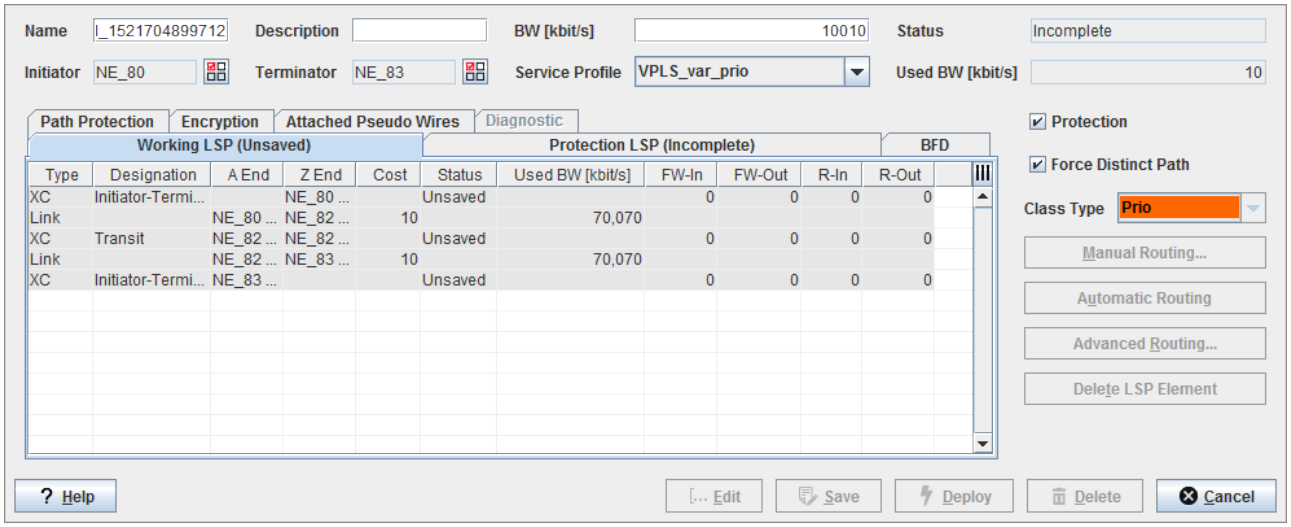


Figure 78: Set Automatic Routing Parameters

8.5.4 Working and Protecting LSP

When the routing is completed, the Working LSP and Protection LSP tabs display the Working and Protection Paths respectively.

The tabs allow to delete LSP elements of the type "Link", and to set Protection or to set Unprotected a working or protection LSP.



Type	Designation	A End	Z End	Cost	Status	Used BW [kbit/s]	FW-In	FW-Out	R-In	R-Out
XC	Initiator-Termi...		NE_80 ...		Unsaved		0	0	0	0
Link		NE_80 ...	NE_82 ...	10		70,070				
XC	Transit	NE_82 ...	NE_82 ...		Unsaved		0	0	0	0
Link		NE_82 ...	NE_83 ...	10		70,070				
XC	Initiator-Termi...	NE_83 ...			Unsaved		0	0	0	0

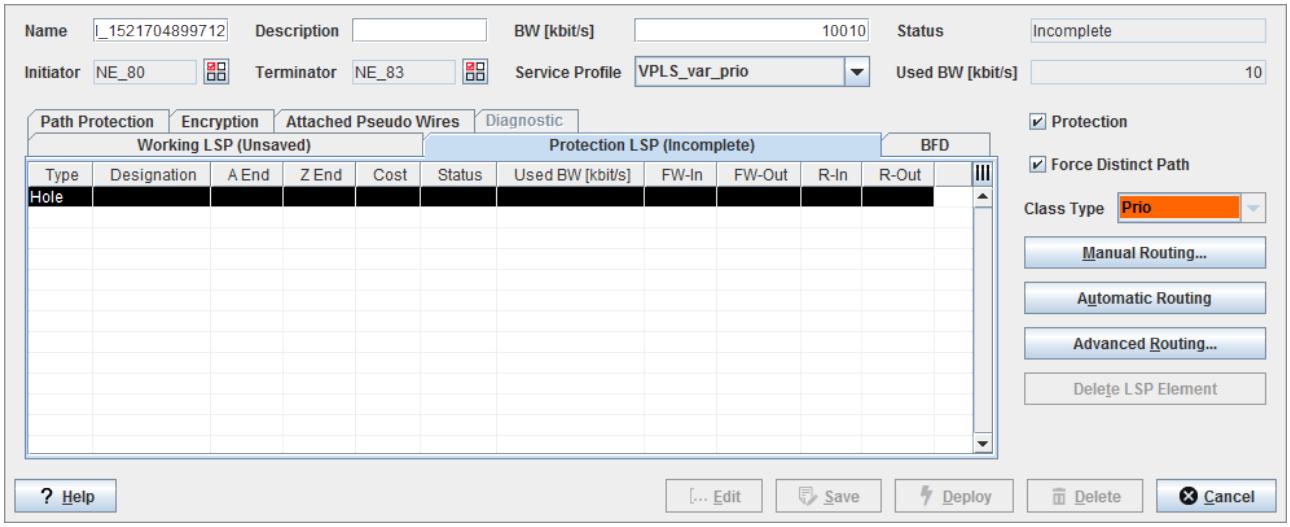


Figure 79: Working and Protection LSP

8.5.5 OAM Bidirectional Forwarding Detection (BFD)

Bidirectional Forwarding Detection (BFD) is a network protocol used to detect faults between two MEP endpoints connected by a link. The BFD establishes a session between these endpoints over a particular link by exchanging control packets.

Both MEPs exchange BFD control packets at a regular interval. The local MEP sends Continuity Check (CC) packets at a defined “CC Interval” and the remote MEP monitors the arrival of the CC packets and detects loss of Continuity (LOC) if the packets fail to appear over a certain time period.

If the link or path is protected, separate BFD sessions (BFD CC Supervision) are automatically established in the working and protection LSP to monitor both links.

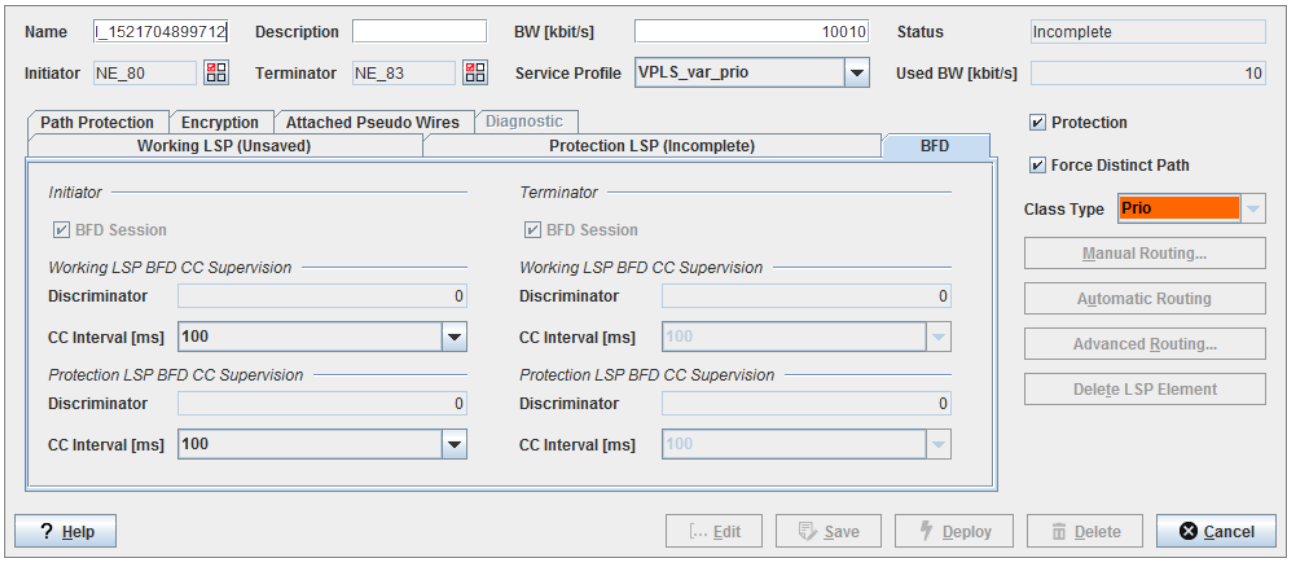


Figure 80: OAM Bidirectional Forwarding Detection

8.5.6 Path Protection

Allows you to define the notification frequency of the path state as well as the restoration actions once the working path is repaired or restored. The protection mode defines whether or not the traffic is switched back from protection path to the working path. There are two modes of operation:

- Revertive mode

  The traffic is automatically switched back from the protection path to the working path after the expiration of the Wait-to-Restore (WTR) timer.

- Non Revertive mode

  The traffic is not automatically restored to the working path, even if the working path is repaired. Thus, administration form of intervention, i.e. a “Manual Switch” is needed to invoke restoration action if required.

  This mode is employed if the administrator wants to gain assurances about the integrity of the path before switching path or if it is acceptable to continue operation without the (protection) path being protected.

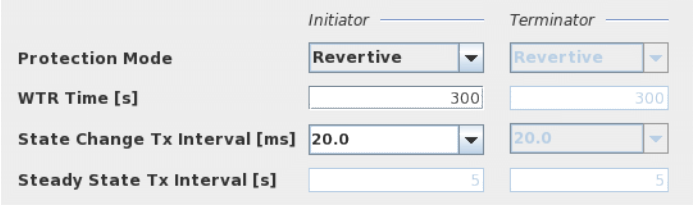


Figure 81: Path Protection Parameters

In the graphical view of the Path Protection tab the currently active path is colored in gold while the inactive path is black.

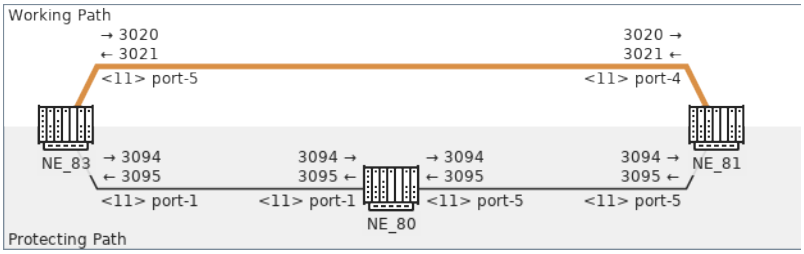


Figure 82: Path Protection - Active Path

8.5.7 Encryption

During Tunnel creation lets you select an encryption profile to be applied to the tunnel (end-to-end), or to segments of the tunnel (hop-by-hop). Also, encryption can be applied separately for working and protection LSPs.

In “Tunnel Details”, displays encryption status of the working and protecting tunnel on both the initiator and the terminator side. The graphical view shows encrypted segments of working and protection LSPs.

Allows you to select the encryption profile for the working and protecting tunnel on both the initiator and the terminator side.

The selection of the encryption profile is managed by a specific security manager.

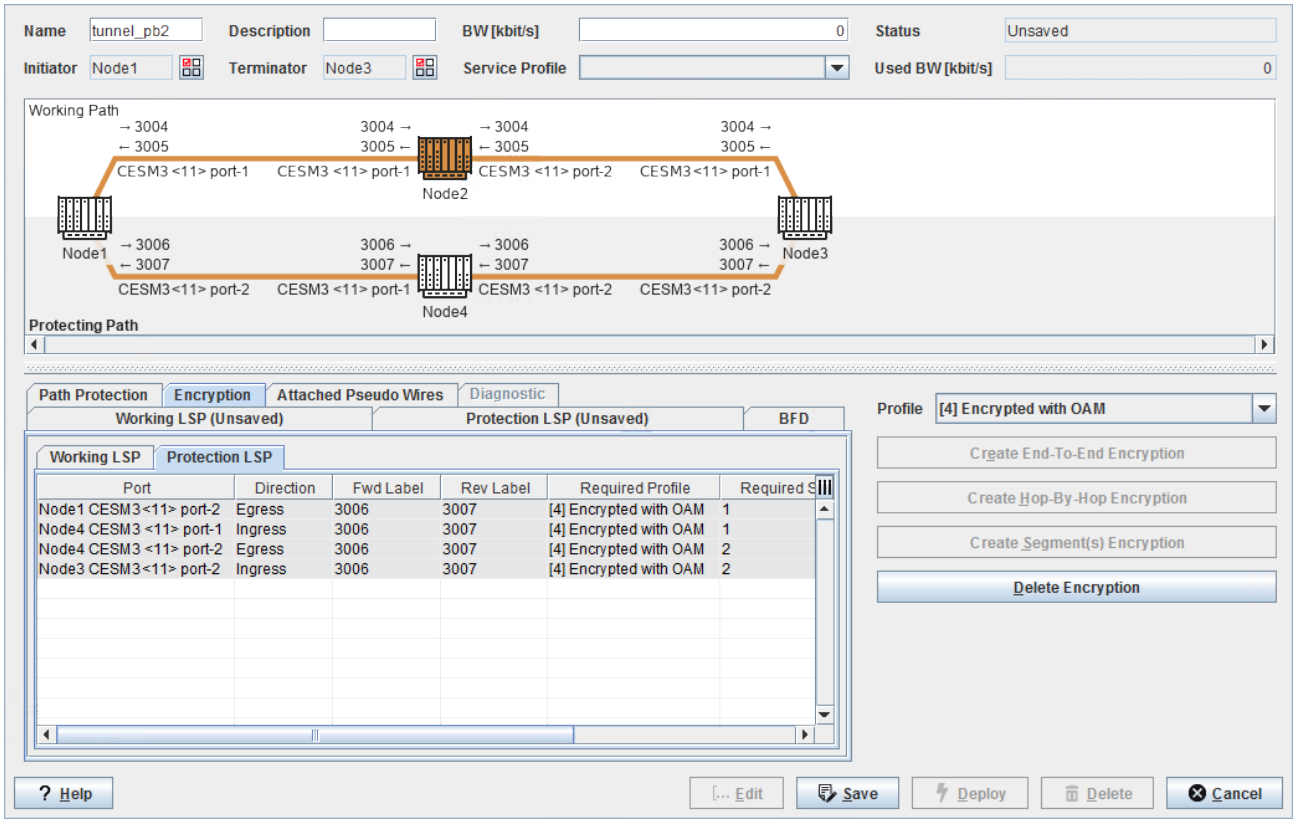


Figure 83: Encryption

8.5.8 Attached Pseudo Wire

Displays all the Pseudo Wires attached to a Tunnel (where available).

Allows you to open the VPWS and VPLS dialogs in details view mode where services are available already. During tunnel creation usually no attached Pseudo Wires are defined yet for that tunnel.

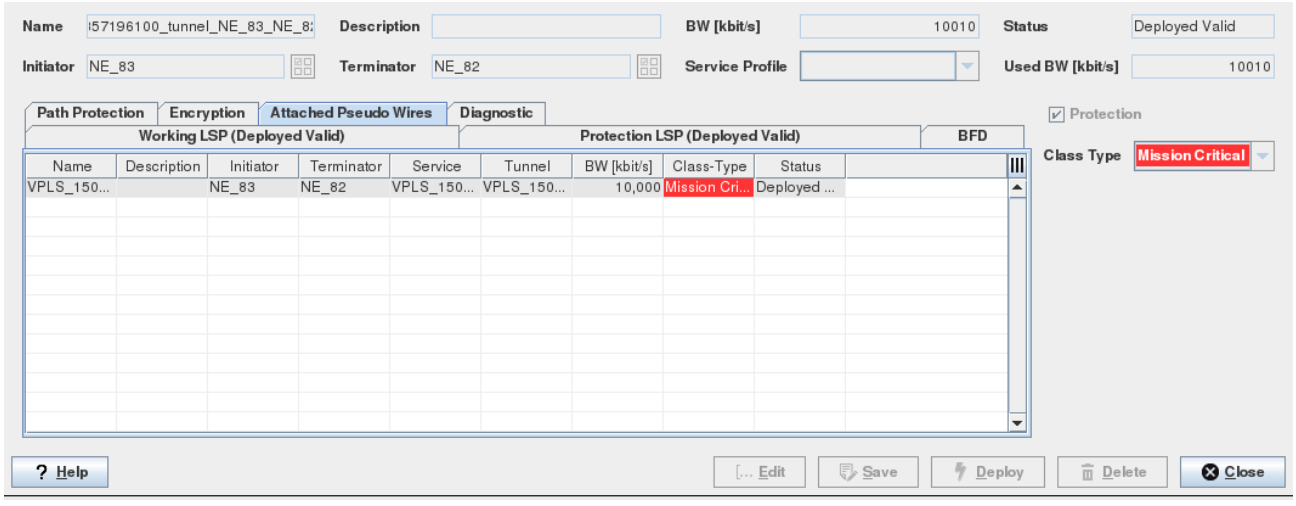


Figure 84: Attached Pseudo Wire

8.6 Tunnel Details

8.6.1 Path Protection

Displays path protection information and allows you to execute switch-over commands.

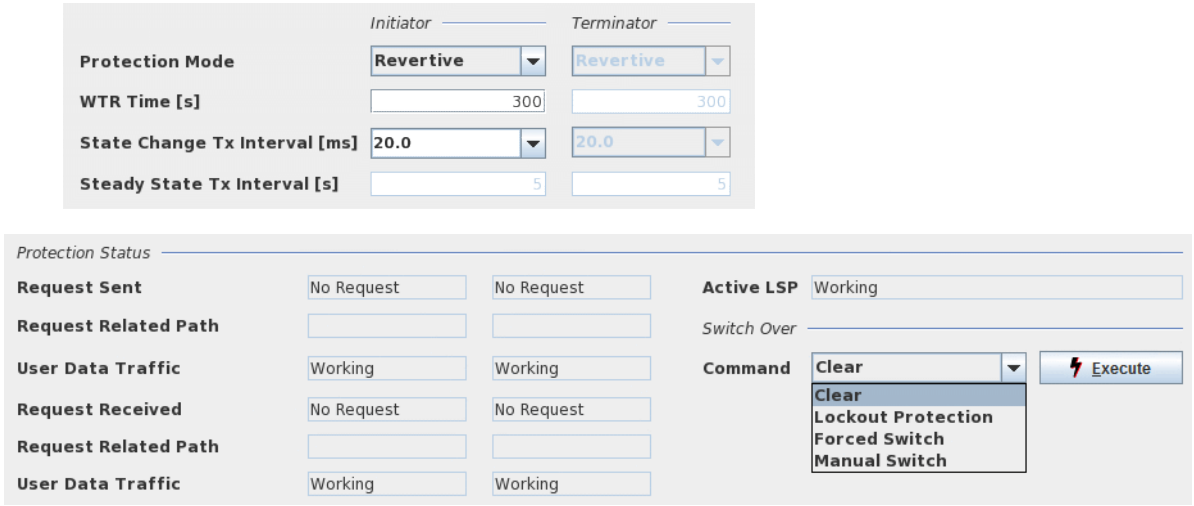


Figure 85: Tunnel Details, Path Protection

8.6.2 Diagnostic

Displays tunnel diagnostic information and lets you execute Ping, Trace Route and Delay Measurement commands. With the use of PTP for node synchronization the delay measurement allows for nanosecond resolution.

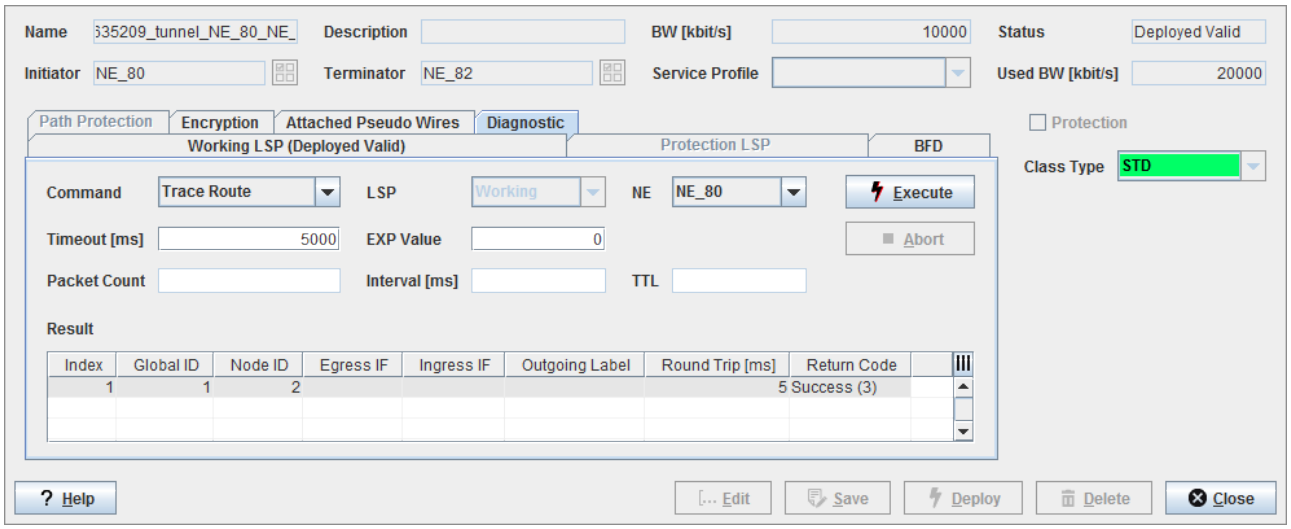


Figure 86: Tunnel Details, Diagnostic

9 Circuit Emulation

The Circuit Emulation application is the browser-based graphical user interface for creating and monitoring Circuit Emulation Services (CES) in FOX61x networks.

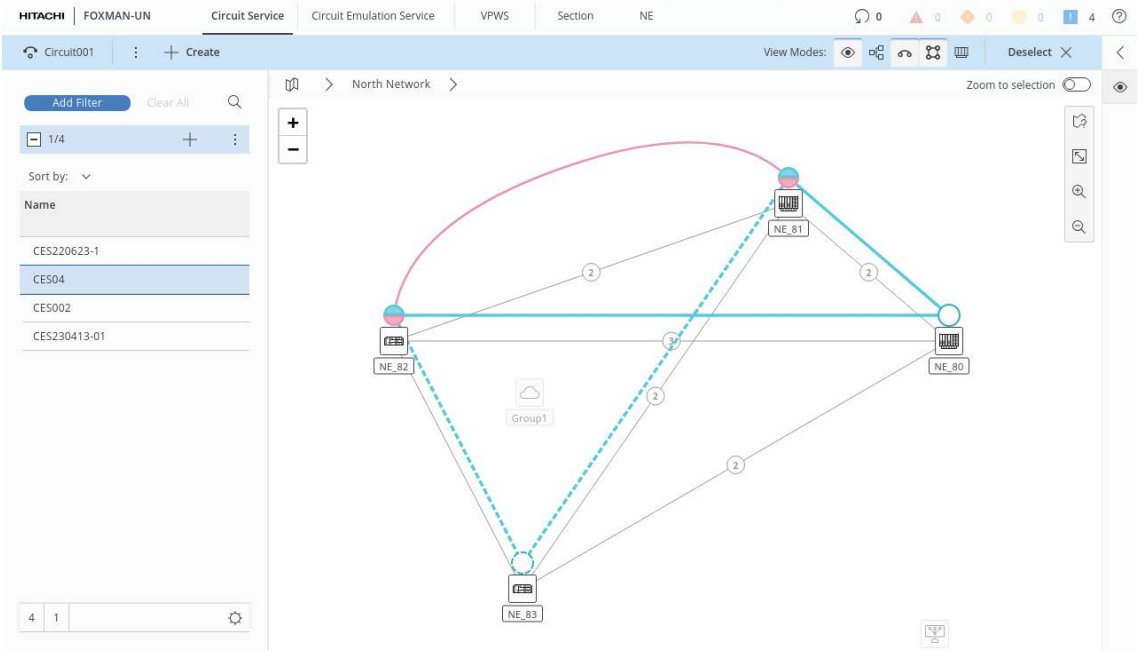


Figure 87: Sample CEM Overview Dialog with service list and service map

The CEM GUI dialog provides the following main tabs:

- **Circuit Services**

  Lists all TDM Circuit services that make use of CES in the network;

  Provides a service creation wizard guiding through all required steps to create and deploy a Circuit Service.
- **Circuit Emulation Services**

  Lists all CES services in the network;

  Provides a service creation wizard guiding through all required steps to create and deploy a CES.
- **VPWS**

  Lists all Virtual Private Wire Services (VPWS) that are required for providing circuit emulation services and teleprotection services.
- **NE** (Network Elements)

  List all network elements and their key characteristics, including their support for CES services;
- **Section** (physical links)

  Lists all sections in the managed network and their key characteristics.

List entries can be filtered, and single or multiple entries can be selected and more detailed properties can be displayed for any selected entries.

Various context menu options are available, such as opening initiator or terminator NE configuration directly from the service, NE, or section, opening a details view, deleting a service, changing admin states, opening the alarm list.

10 Teleprotection

The Teleprotection application is the browser-based graphical user interface for creating and monitoring Teleprotection Services in FOX61x networks.

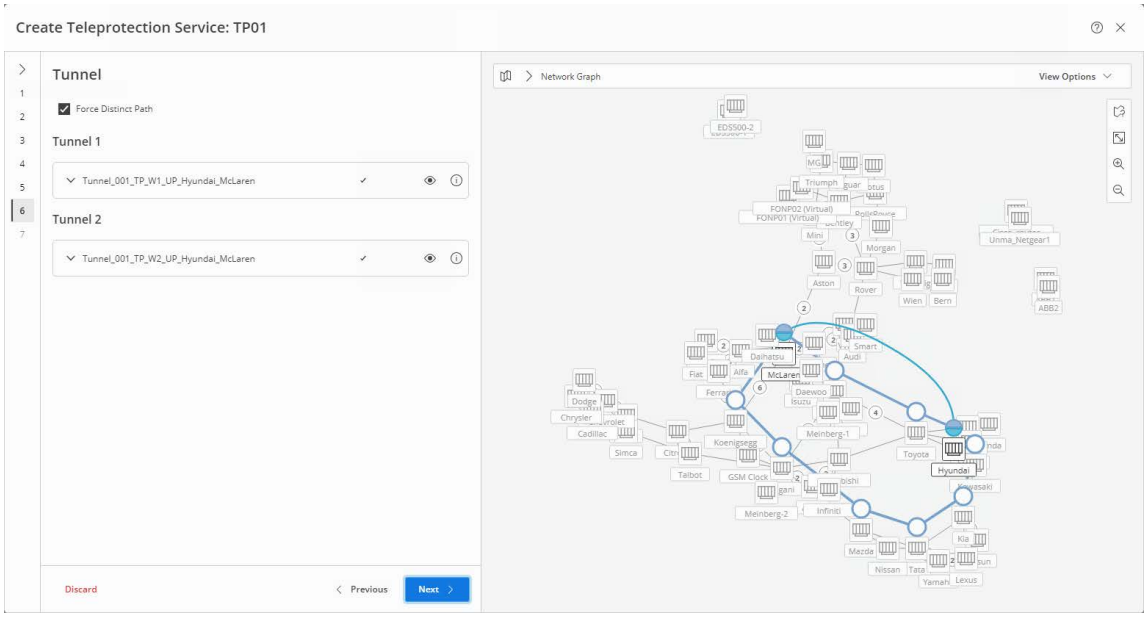


Figure 88: Sample Teleprotection Service Creation Wizard View

The Teleprotection GUI dialog provides the following main tabs:

- **Circuit Service**

  Lists all TDM Circuit services that make use of CES in the network;

  Provides a service creation wizard guiding through all required steps to create and deploy a Circuit Service.
- **Teleprotection Service**

  Lists all teleprotection services in the network;

  Provides a service creation wizard guiding through all required steps to create and deploy a teleprotection service.
- **VPWS**

  Lists all VPWS in the network that are relevant for teleprotection services;

  Provides detailed, structured information on every VPWS, their configuration, issues, related items, and more.
- **Section** (physical links)

  Lists all sections in the managed network and their key characteristics.
- **NE** (Network Elements)

  Lists all network elements and their key characteristics, including their support for teleprotection services;

11 Service Supervision and Reporting

11.1 Introduction

Service Supervision provides Service Level Management by monitoring “Services” and presents Service operational state and fault state. In addition, it generates reports for “Services” that present availability over time.

The sample EoS network diagram below illustrates the boundary of the FOXMAN-UN’s end-to-end service monitoring and an overview of the Service Path.

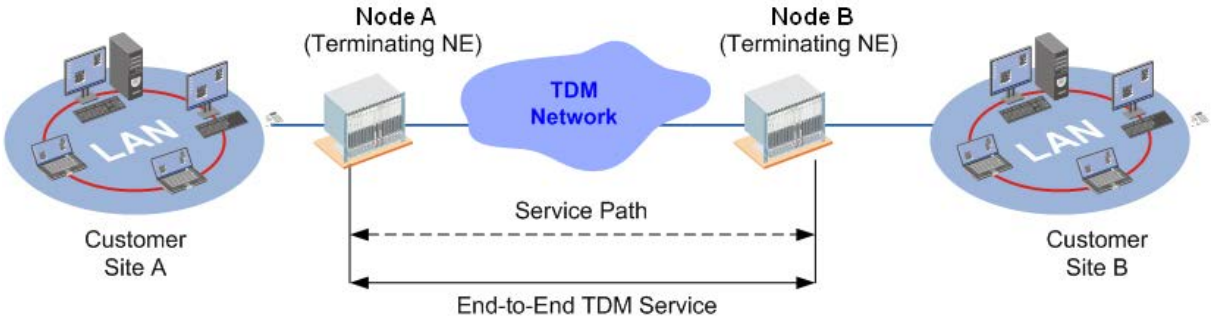


Figure 89: End-to-End TDM Service Supervision

- Service

  A Service is a a collection of Service Paths, where a Service Path provides one complete “channel” of the intended service. A Service must have at least one Path.
- Path

  A Service Path or transport route defines one complete channel of the Service. It is a combination of Service Components.
- Service Components

  A Service Component, which represents a physical or logical elements in the network, can be:
  - Port
  - Circuit

    The Networking Package (NP) must be enabled for Circuits to be part of a Service. If NP is disabled, the operator can use only the Ports, Sections and Service Points for creating a Service Path.
  - Section
  - Service Point

    A FOXMAN-UN object, where key service control and configuration resides. For example, an EoS Service Point represents the point where EoS is enabled/disabled and where EoS specific alarms would be addressed.

    The other supported Service Point types are as follows: X21, RS232 (V24/V28), E&M and E1).

The diagram below illustrates a single end-to-end service with two different Paths (or transport routes).

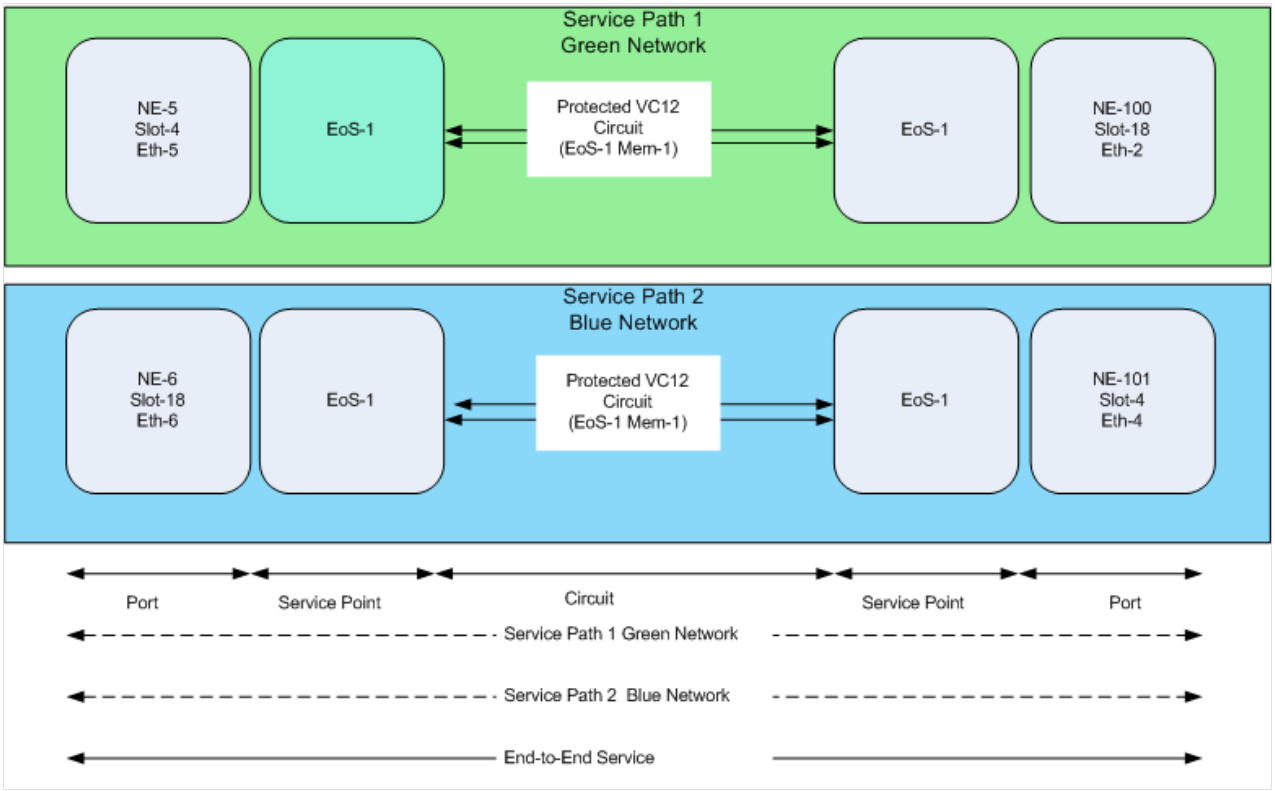


Figure 90: End-to-End Service Paths

11.2 Adding Services to Supervision

There are two basic ways to add services to Service Supervision:

a adding System Services directly from ENP or NP application,

b adding Advanced Services by manually creating service supervision entries.

The Service Supervision main window displays details of all the configured Services with their corresponding paths and components, divided into the two groups in their respective tabs (System Services and Advanced Services).

It is likewise the main dialog to call the relevant dialogs such as:

- Alarm List of the Service(s);
- Create/Edit Services;
- Manage Customer;
- Manage SLA;
- Manage NE Maintenance Mode;
- Manage Report Profile;
- Generate Report.

11.3 System Services

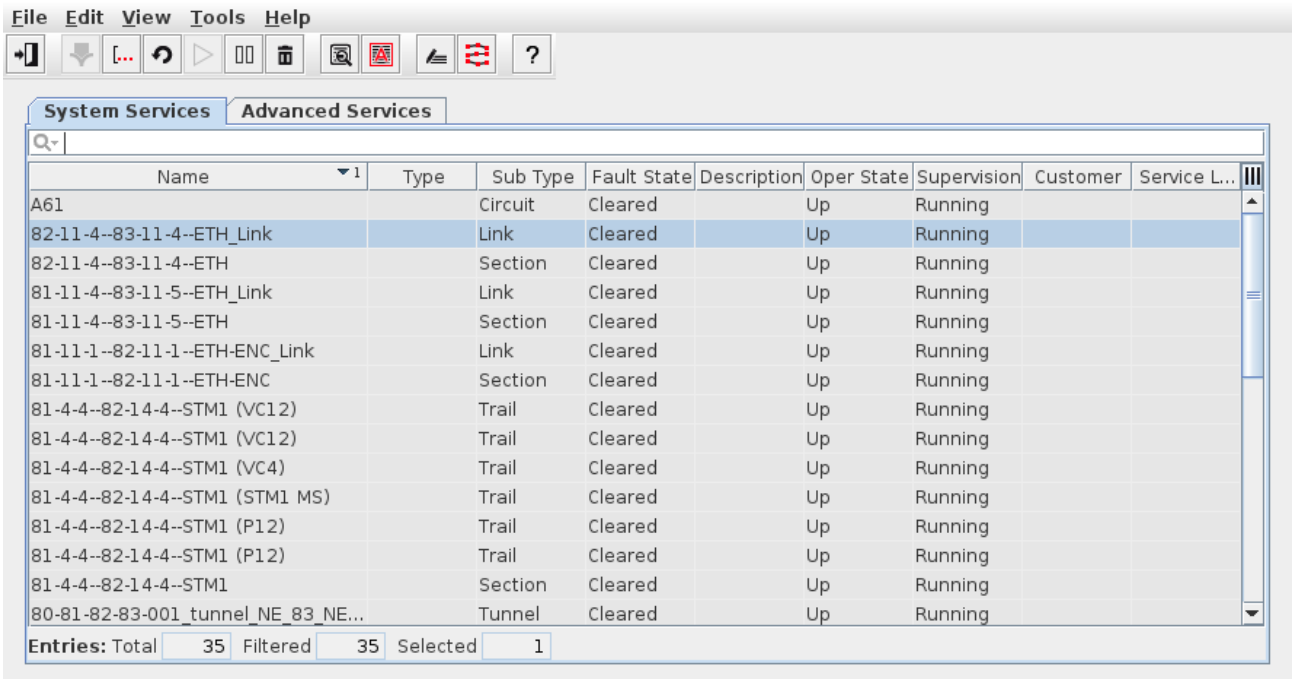


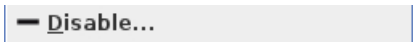
Figure 91: Service Supervision Main Window, System Services

11.3.1 Adding Services

System Services are added to Service Supervision via the context menu of an ENP or NP service. The context menu of a service in ENP or a TE in NP includes the option “Supervision” with the following commands:

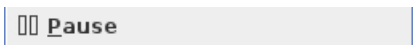
- Enable

- Disable

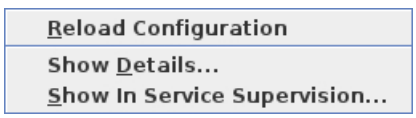


- Resume

- Pause



In addition to these commands, service configuration can be reloaded, details can be shown, and the service can be shown in the Service Supervision dialog via the following further “Supervision” commands:



Reload Configuration will reload the configuration from the network (NEs) to make sure the information in the database is up to date in case of recent changes to the service.

Showing details opens a hierarchical view of the service structure in the Service tab and related alarms in the Alarm tab.

When “Show In Service Supervision...” is selected, the service is shown in a filtered view of the System Services tab of Service Supervision.

11.4 Advanced Services

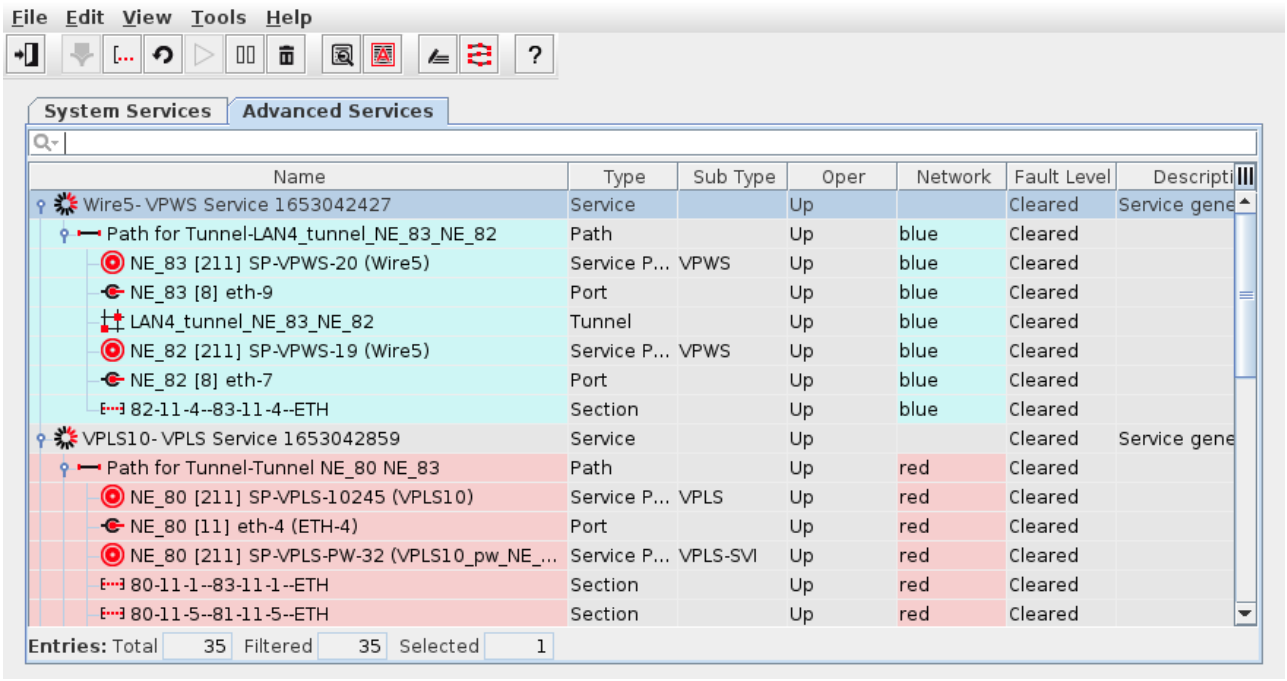


Figure 92: Service Supervision Main Window, Advanced Services

11.4.1 Creating Services

The Service Editor dialog is launched from the Service Supervision main dialog to create or edit Services. It looks similar to the main dialog, with the following differences:

- Displays only the details of the current Service being created or edited;
- Does not show the status and alarms;
- Allows deleting the current Service;
- Allows adding or deleting Service Path(s), Service Component(s);
- Allows editing the existing Path and Service attributes of the current Service.

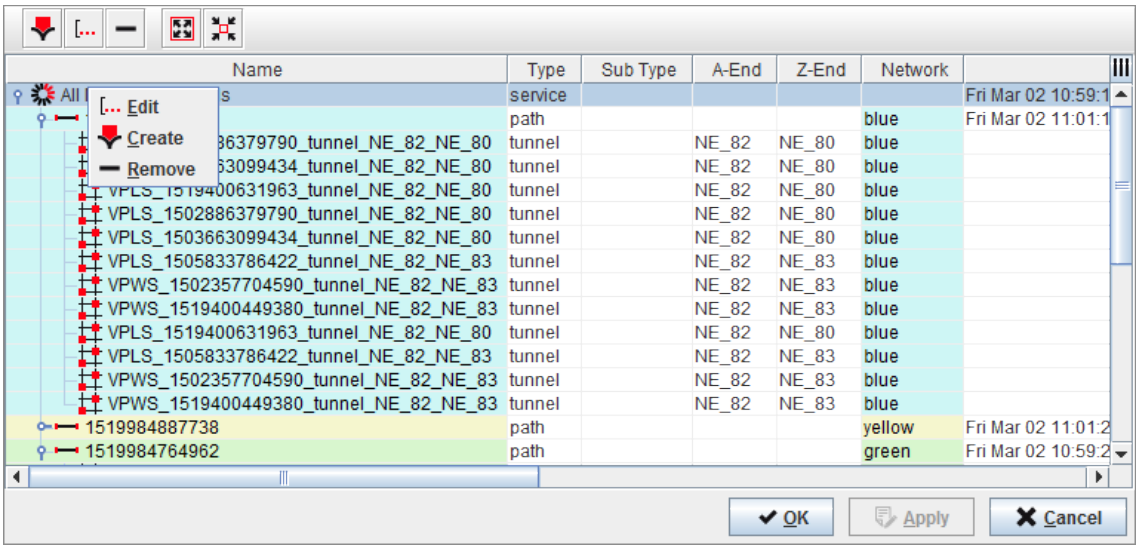


Figure 93: Service Editor

11.5 Service Supervision Tools and Options

11.5.1 SLA Manager

The Service Level Agreement (SLA) contains the service reliability/performance metrics that can be negotiated between the service provider and a customer to guarantee levels of quality for traffic transiting the network.

The current implementation monitors only the actual Service Availability and compares it against the Service Availability threshold set in the SLA. If this threshold is crossed, an SLA violation is reported in the Service Reporting dialog. The SLA manager is only applicable to Advanced Services.

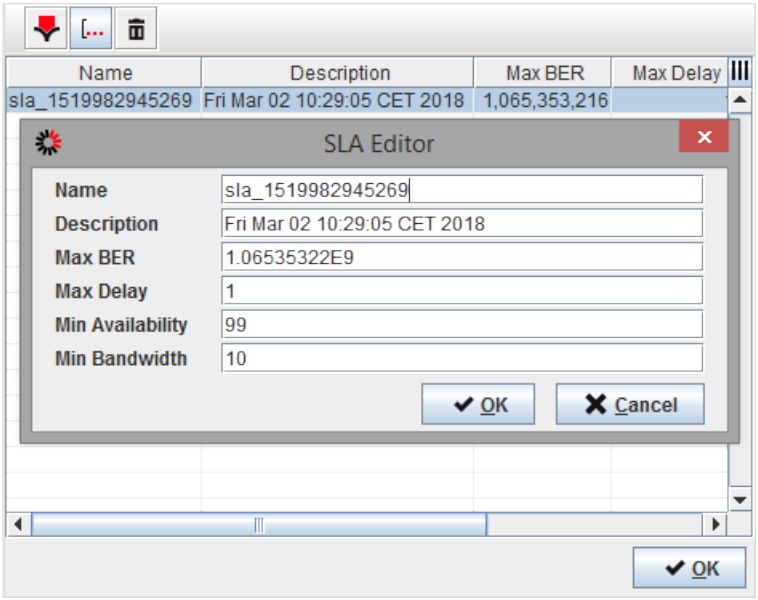


Figure 94: SLA Manager / SLA Editor

11.5.2 Service Alarms

The key piece of functionality in the Service Supervision is identifying which Services are impacted by traffic affecting equipment alarms. This feature is useful when troubleshooting a service problem.

The **Alarm List** dialog filters the alarms based on the selected element(s), e.g. list only the Service Alarm of the selected service(s) or list all the alarms of the service(s), service path(s) and service components.

Please note:
Important points about Service Alarms:

→ Only one Service Alarm active per Service;

→ If a Service Alarm changes severity, the active alarm is cleared and a new alarm is raised;

→ Only traffic affecting equipment alarms are monitored for Service Alarms.

→ To prevent service alarms from being activated during NE maintenance, a maintenance flag can be set on the NE. This will suppress all service alarms during the maintenance.

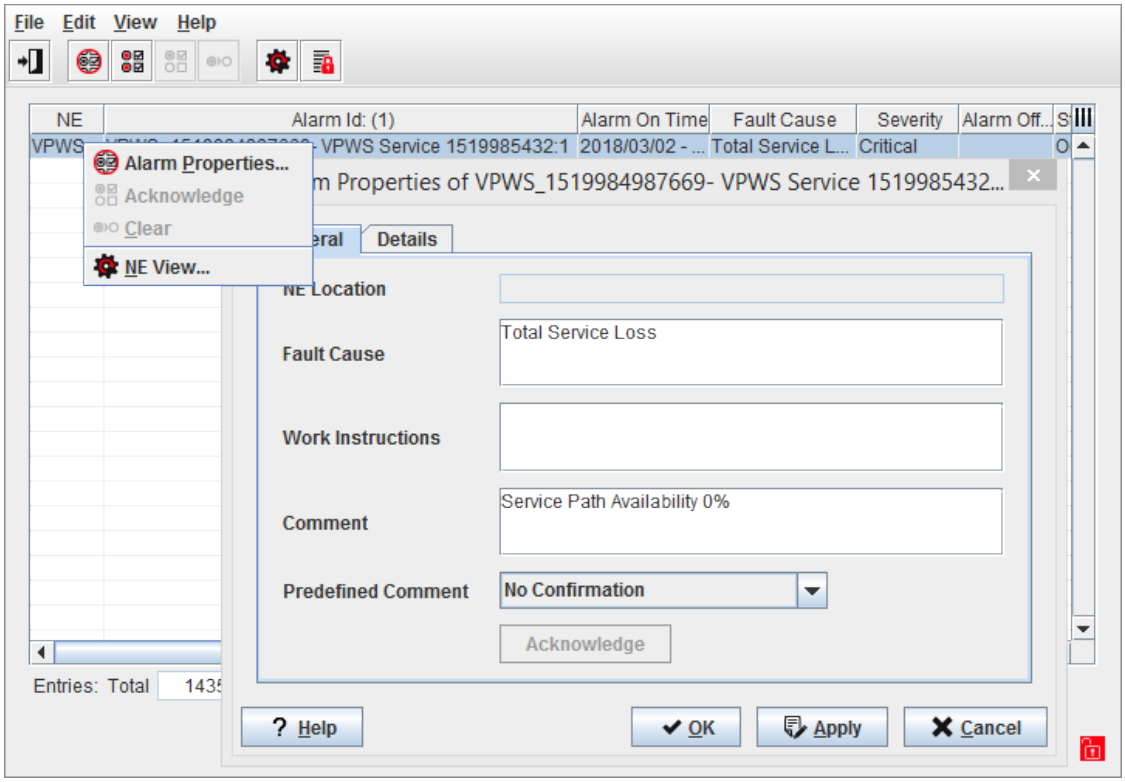


Figure 95: Service Alarms, Alarm List and Alarm Properties

Service Alarm Severity

The mapping of equipment alarms to service fault state is configurable via:

`/opt/nem/etc/singlePathServiceAlarmMapping.cfg`

and

`/opt/nem/etc/multiPathServiceAlarmMapping.cfg`

NE Alarm Filter

The customer-specific mapping for alarms to be processed or ignored by Service Supervision is configurable via:

`/opt/nem/etc/neAlarmFilterServices.cfg`

For details, please refer to chapter “FOXMAN-UN Configuration Files” of the “FOXMAN-UN under Linux” User Manual.

11.5.3 Service Reporting

Service Reporting is only available for Advanced Services. It displays the Service end-to-end performance monitoring information as listed below:

Service Events

Lists the service events within the specified reporting period (1 to N days).

In the daily reports, the “Event Start Time/Event Start Off” indicate:

- from the event ON to the event OFF in case both events are during the reported day;

- from the event ON to the end of the day, if there is no OFF period event during the reported day;
- If there is no ON, but the OFF event, the time until OFF is reported.

The “Event Duration” indicate:

- If the ON event persists during the day, the full day is reported (86400 seconds);
- Note for the daylight saving, the duration of a day is adjusted (23 or 25 hours).

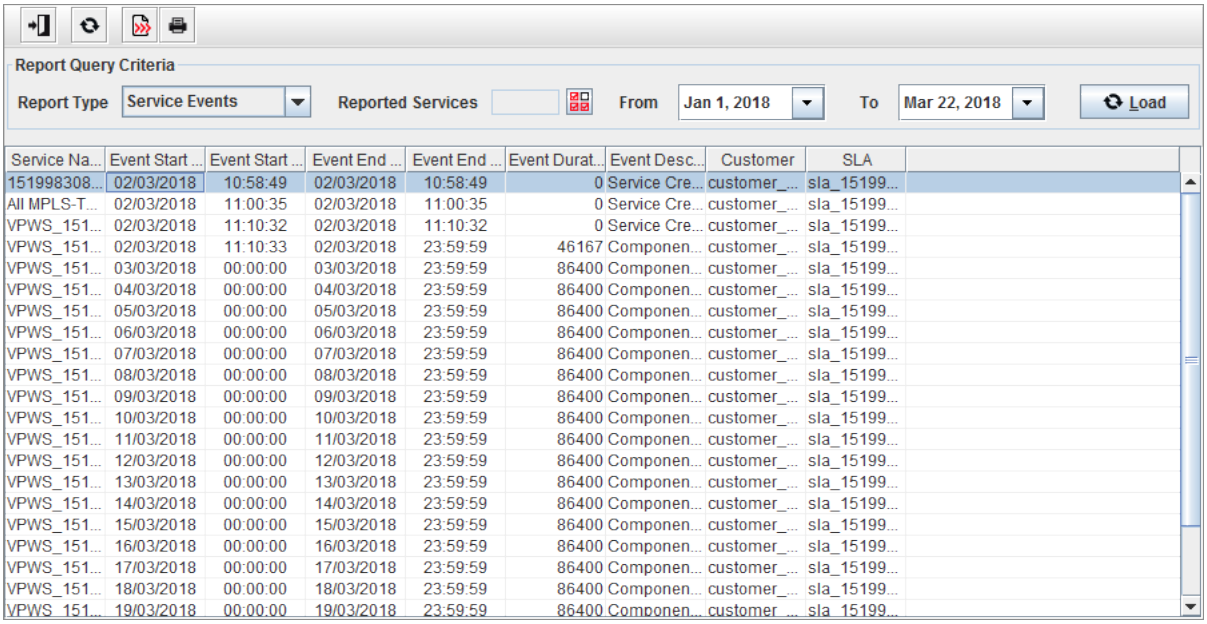


Figure 96: Service Events Report (Report Viewer)

Service Outage Daily Statistics

Displays the Service unavailability instances count and time intervals for the 24h period.

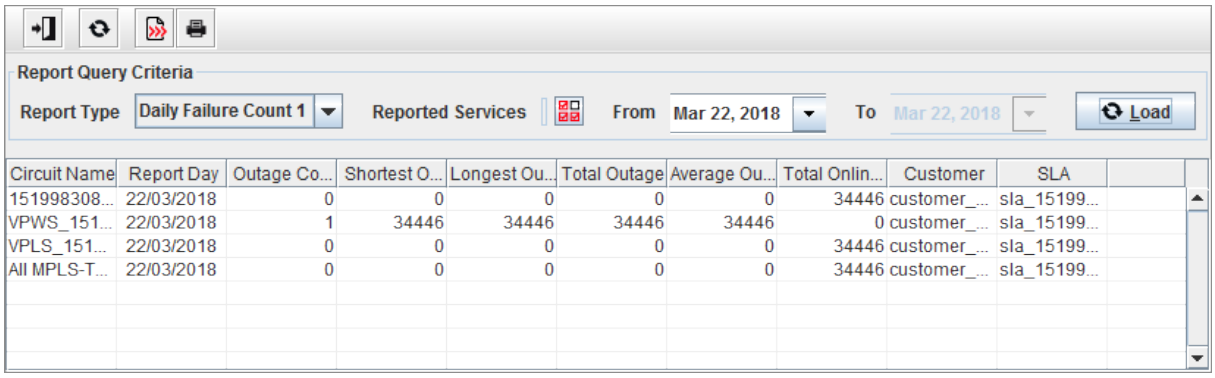


Figure 97: Daily Failure Count 1 Report (Report Viewer)

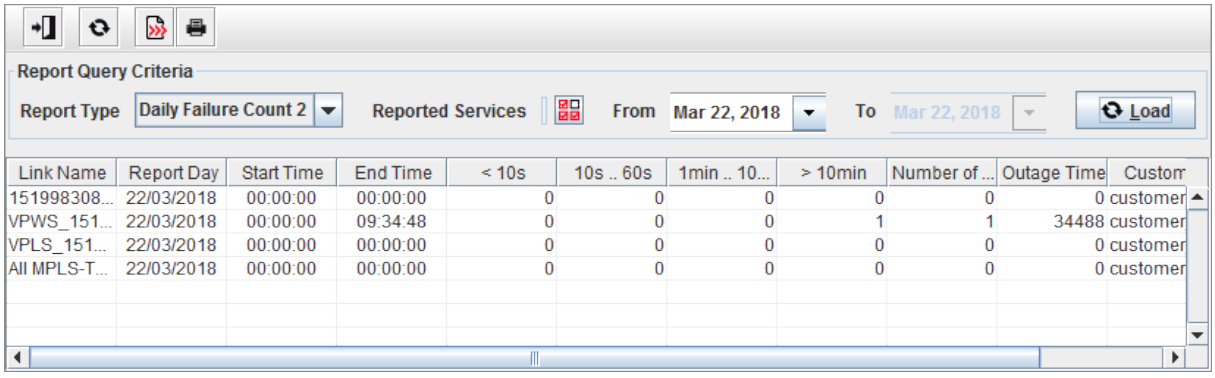


Figure 98: Daily Failure Count 2 Report (Report Viewer)

Service Monthly Availability

Displays the calculated Service end-to-end Availability per month. It likewise detects threshold violations against the Availability QoS metric set in the SLA.

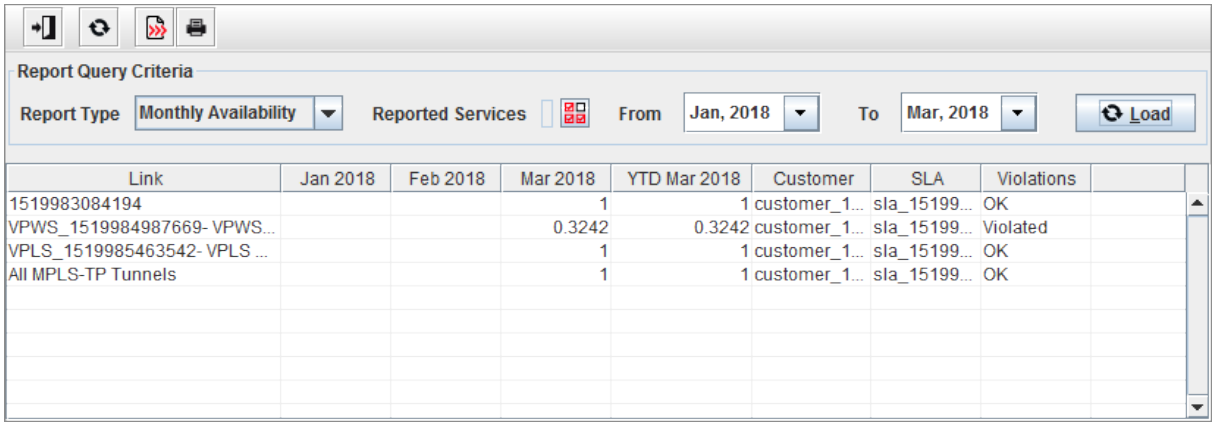


Figure 99: Monthly Availability Service Report (Report Viewer)

11.5.4 Service Report Manager

Allows the creation of Service Report Profile to:

- Schedule report creations;
- Send generated reports to an email or save in a local directory.

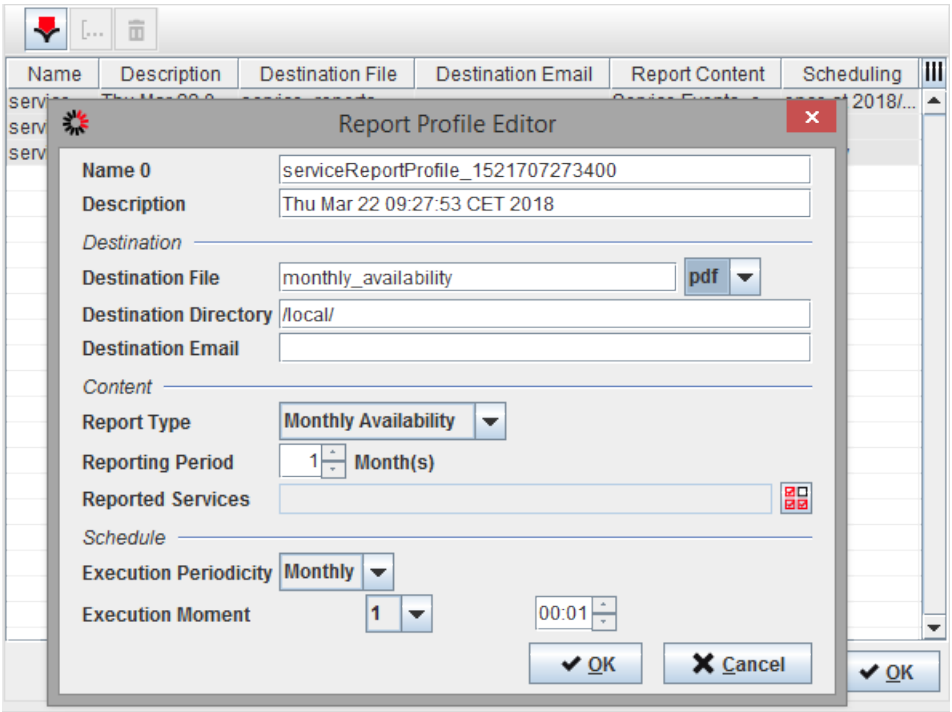


Figure 100: Service Report Manager

The dialog lists the Reports Profile, showing the Report Type (Service, Daily Statistics Count 1, etc.), the Schedule of the report generation and the Destination of the generated report(s).

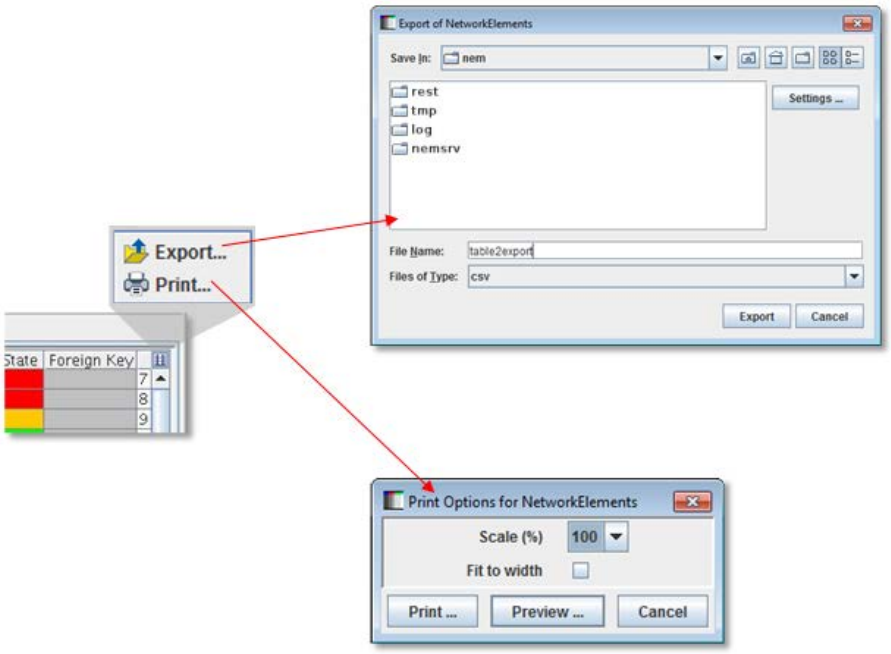
12 Print & Information Export

Documenting the network is an essential part of managing the network. FOXMAN-UN provides help to keep track of changes and allows an operator to print where required the necessary information for network operation. Amongst the possibilities available, the operator can print or save to a file.

12.1 Table Print /Export

FOXMAN-UN dialogs represent data and information in table form. This allows the user to:

- sort, filter and re-organize the table's rows and columns to help manage the data effectively;
- export and save the table's contents to a csv or xml file;
- print the table's contents.



12.2 NE Reports

On a per network element basis it is also possible to print or save to a file in CSV format via UCST (FOX51x NEs only):

- Log Book;
- Inventory;
- via the «File > Print» menu the following:

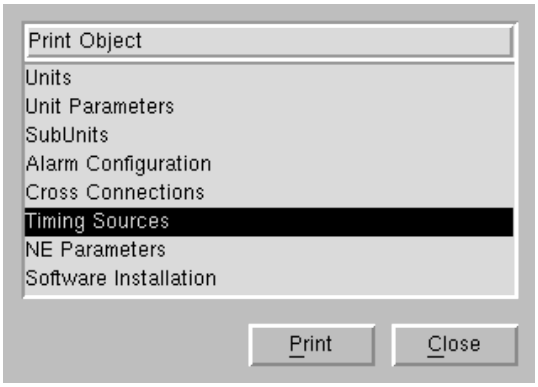


Figure 101: NE Reports

12.3 Inventory

The inventory of the managed network is periodically collected and saved in the FOXMAN-UN database.

Inventory reports of different types can be generated and either sent to the screen or saved as a CSV or a XML file for integration into an OSS (Operation Support System).

A «Request Inventory Report» dialog is provided for the configuration of the required report.

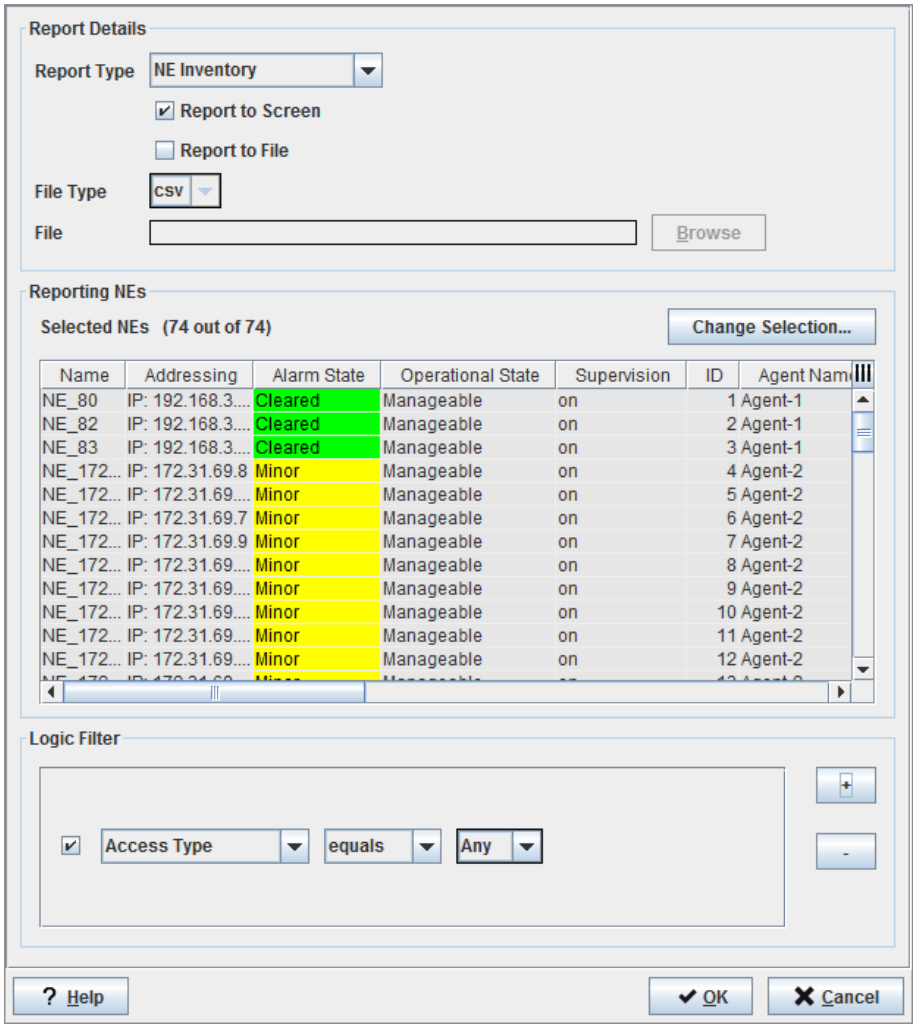


Figure 102: Print - Inventory (Request Inventory Report)

The following types of reports can be generated:

- NE Inventory:
  NE properties and relevant agent properties.
- Unit Inventory:
  Hardware and ESW properties of all units in the selected NEs.
- Port Inventory:
  All ports per unit, with their label, layer rate, activity status and service type.
- Configuration Inventory (for FOX51x NEs):
  - NE inventory:
    NE properties and relevant agent properties.
  - TTP:
    TTP properties and relevant agent properties.

- Matrix connections:

  All cross-connections with their group label, layer rate, directionality and protection as well as their a and z end identification and trail termination point data.
- Software:

  Software installation configuration and relevant agent properties.
- Timing source.
- NE parameters.

13 Installation, Administration & Help Tools

13.1 Installation

13.1.1 General

Simplicity of use is the prime objective of the FOXMAN-UN design. This starts with the installation of the application. It has been designed to be as simple as possible, and assumes a minimum knowledge of the workstation and operating system.

13.2 System Administration

13.2.1 Remote Admin Tool

This tool provides a number of system functions via the NEM Remote Admin Tool GUI. Using these functions does not require essential Linux knowledge.

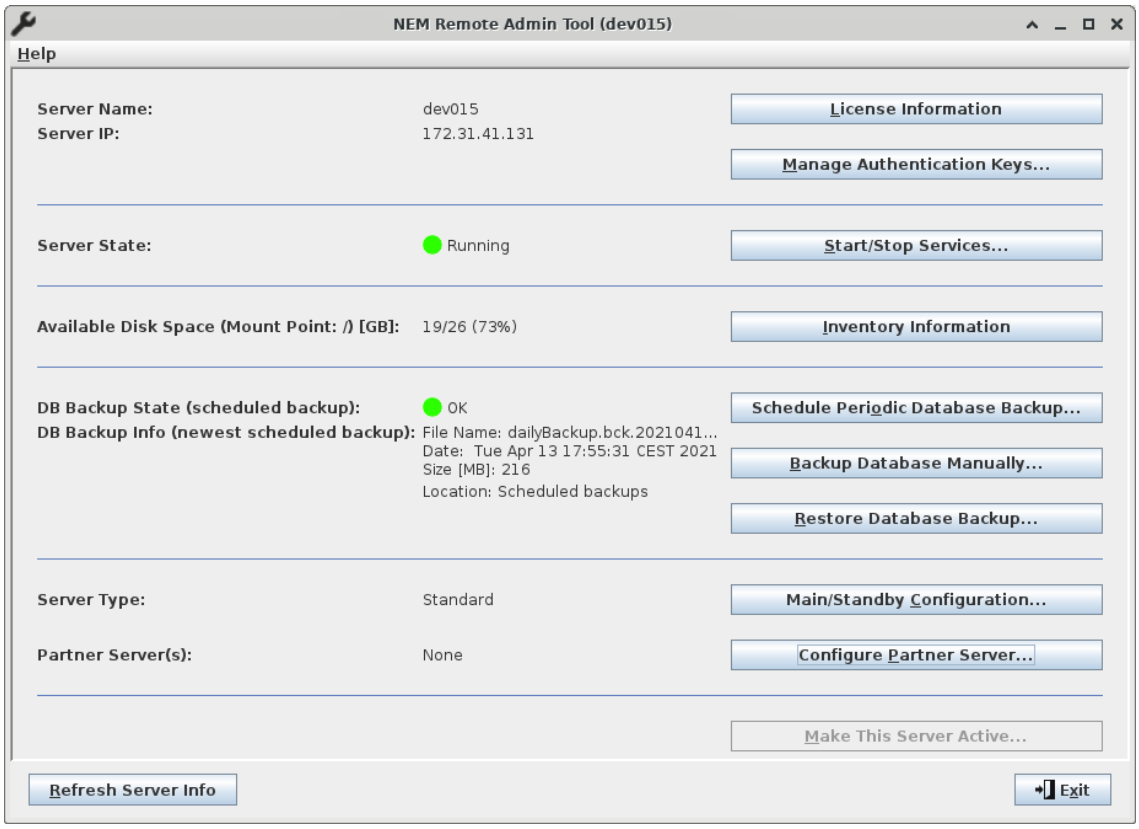


Figure 103: NEM Remote Admin Tool

Once installed, FOXMAN-UN provides the FOXMAN-UN administrator with a simple administration tool to help carry out the basic tasks of:

- Viewing and loading the license key,
- Managing authentication keys,
- Starting/restarting and stopping FOXMAN-UN services,
- Re-synchronizing NP objects with BP NE data,
- Viewing the Element Agents status,
- Viewing server inventory information,

- Scheduling periodic database backups,
- Performing a manual database backup,
- Restoring a database backup manually,
- Providing redundancy via main/standby configuration.

13.2.1.1 License Information

The License Info dialog shows the details of the currently active license keys. Depending on the licensed options, one or more tabs are provided in the dialog. As a default, the NEM license tab includes the workstation identification number and the LAN interface ID, followed by the various licensed options.

Via the command button “Upload NEM License File...” menu it is possible to select a new license key file.

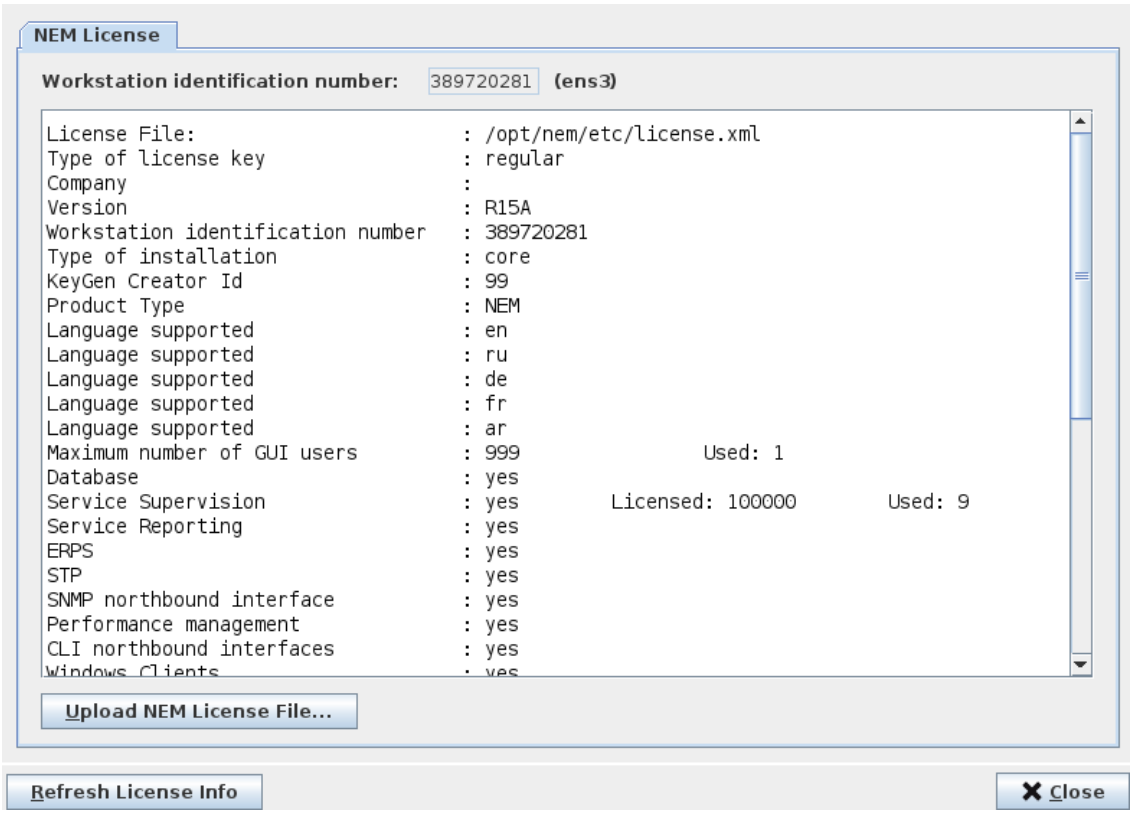


Figure 104: NEM License sample

13.2.1.2 Managing Authentication Keys

The tool to manage authentication keys is provided in the “Manage Authentication Keys” dialog. It allows you to create, activate, and delete authentication keys. Such keys are used e.g. for secure access to FOX61x nodes.

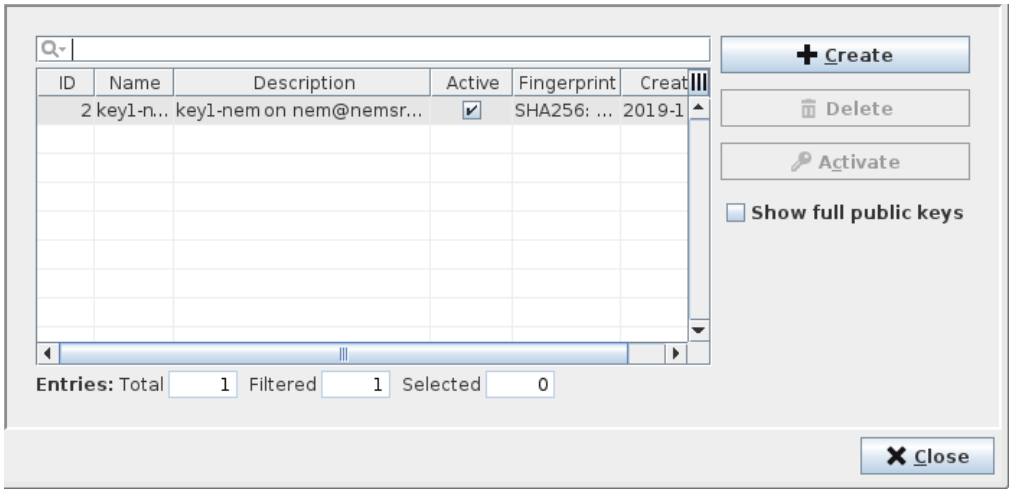


Figure 105: Manage Authentication Keys sample dialog

13.2.1.3 Start/Stop Services

This function reports the status of the FOXMAN-UN services and provides commands to start and/or stop services. It allows you to:

- Show all FOXMAN-UN services (i.e. base services, core services, and additional services like e.g. DIRAC services, depending on license options) with their name, description, selection for restart, restart indication, state, start date, and run time;
- Restart selected services;
- Start NEM core services;
- Stop NEM core services;
- Execute NP Resynchronization with BP NE data;
- Show Element Agents.

You can refresh the services status via the “Refresh Services Info” button.

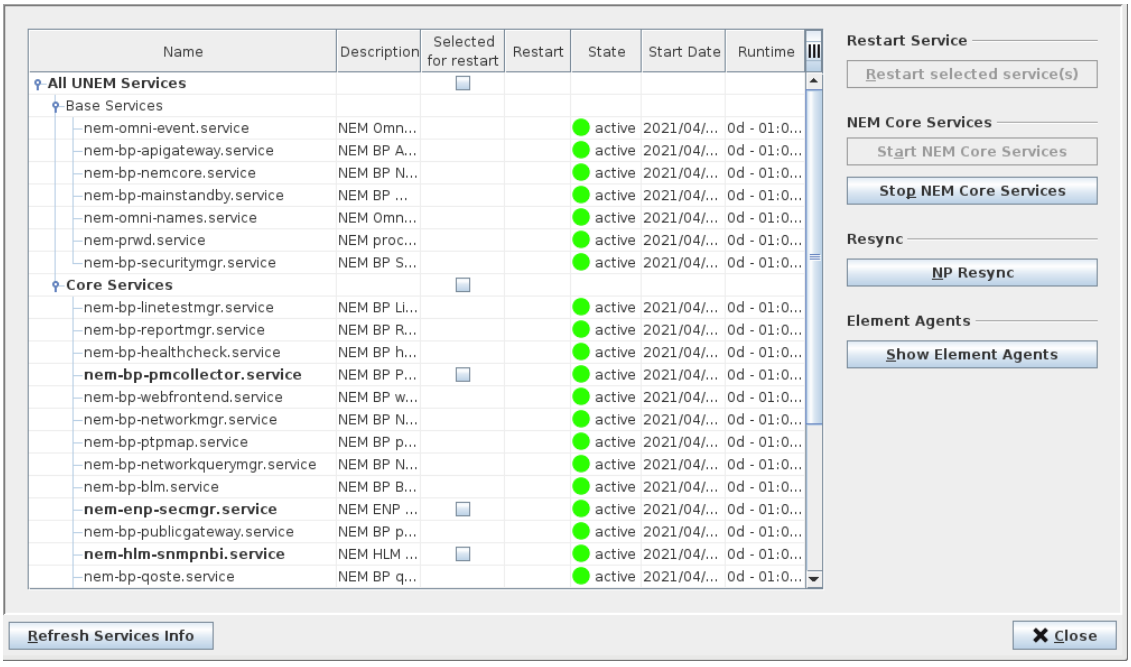


Figure 106: Services Management dialog

The most likely reasons for using the “Start/Stop Services” function are:

- To display the current status of the FOXMAN-UN system (the command “lsnem” also shows these status indications).

- To stop the FOXMAN-UN system for restoring the database from the backup (the FOXMAN-UN core must be inactive for this process).
- To stop and restart just the core for the purpose of activating changes made to the configuration file “nem.conf”.
- To try and recover from some error conditions (indicated for instance by deteriorated performance) by stopping and restarting the system or selected services.

13.2.1.4 Element Agents

Element Agent (EA) information is provided in the “Services Management” dialog, which is called via the “Start/Stop Services” button. Click the “Show Element Agents” button to open the dialog.

EA Name, Host Name, Server Name, Port, Manager ID, NAT Manager ID, Process ID (PID), Admin status, current status, and EA ID in the database are shown for each Element Agent.

13.2.1.5 Inventory Information

Disk Information

This information is provided in the “Inventory Info” dialog. The disk information is provided in raw format, i.e. for each of the logical/physical disk devices it shows the device name, mount point, total size, available size, and usage.

Memory Information

Information on memory is provided in the “Inventory Info” dialog as follows:

Total, used, free, shared, cached, and available memory is shown for both RAM and swap space.

CPU Information

CPU information is provided in the “Inventory Info” dialog as follows:

For each of the CPU cores, CPU information is displayed similar to the Linux command “vmstat”.

13.2.1.6 Database Backup and Restore

For description of how to use the DB Backup and Restore functions, refer to the user manual “FOXMAN-UN Main/Standby Solution” [1KHW029097].

13.2.1.7 Managing Main/Standby Configuration

Detailed information on the setup and configuration of server redundancy, i.e. the Main/Standby configuration, is provided in the two documents

- User manual “FOXMAN-UN Main/Standby Solution” [1KHW029097],
- Application note “FOXMAN-UN Main/Standby Solution” [1KHW029089-R18].

13.3 NEM Help Viewer

Also provided with the application is a context based on-line help which provides the necessary information associated with every dialog. This ensures that the operator always has at hand the necessary help to manage the network.

The help viewer offers a table of contents that is grouped logically. It allows navigating through all the help pages. Additionally the help pages themselves contain links to related pages. There is also a search function incorporated.

The help viewer can be started as a separate application anytime, either from the menu or via command line.

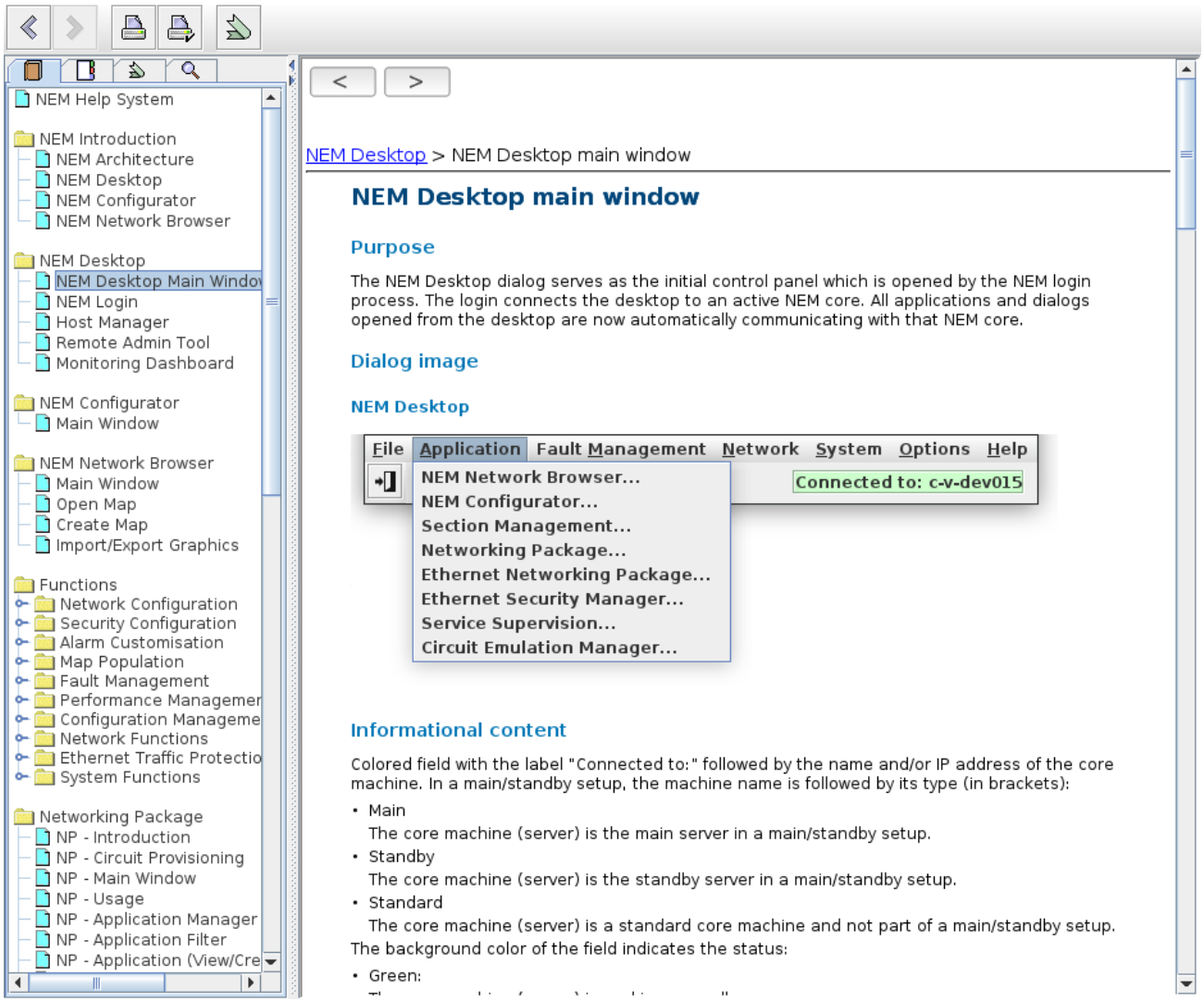


Figure 107: NEM Help Viewer

13.4 Remote Executor

Under the “System” menu of the NEM Desktop an option is provided for executing scripts. The dialog is called Remote Executor. It allows you to import, execute, and delete scripts for execution of specific tasks in your network.

13.5 Technical Documentation

The FOXMAN-UN documentation (NEM DOC Viewer) is delivered together with the FOXMAN-UN system software. The documentation is installed on the core machine via an install script:

```
[root@ host] # <LocalDrive>/Documentation/install.sh
```

Once installed, the documentation can be called from the menu or via command line. It opens up a navigation page from where all available documents can be accessed.

14 FOXMAN-UN Standby & Recovery Concepts

14.1 Introduction

From the perspective of management of a network, a key consideration is how one recovers from a disaster situation. The main disaster situations are related to:

- Loss or suspected corruption of database,
- Hardware failure.

In both cases it is necessary to recover the data and ensure that FOXMAN-UN is up and running again in the shortest possible time.

The following chapters cover how the FOXMAN-UN application can be protected against these types of unforeseen situations and recover from them.

14.2 Database Backup

The first aspect of data integrity for FOXMAN-UN is to ensure that regular backups are taken of the critical data. FOXMAN-UN provides the necessary tools for regular backups, and subsequent restoration of the database, alarm history, activity history, along with user-selected files (these have to be copied into a special directory for this purpose).

In addition the network elements store their configuration and alarm information locally. This means that the NEs are not dependent on the manager for their normal operation.

Hence, in case of a manager (FOXMAN-UN) failure the network elements will continue to function and the network traffic is not affected. Furthermore, if there have been any network changes since the last backup, it is always possible to upload the information from the network elements themselves.

14.3 Standby System

Backup of the database only protects the data used for the management of the network. However, this does not provide any failsafe or graceful rollover mechanism in case of a failure of the hardware on which the application is operating.

By failsafe, it means that there is no possibility that an error can occur. The typical hardware configuration being used for FOXMAN-UN to manage the network could be:

- a single workstation to manage the whole network (user interfaces, agents and database installed on the same machine);
- a server with the central database.

In each of the above cases it is absolutely paramount to be able to recover the data and bring the manager back into operation in the shortest possible time, with a graceful switch over to another workstation or server.

14.3.1 Standby Concept for FOXMAN-UN

The FOXMAN-UN standby concept provides different possibilities. Standard options:

- Cold standby: a standby machine is used to take over the management from the working (main) machine in case of an error. While in cold standby, the standby server regularly fetches the database from the main server to keep its database synchronized.
- Warm standby: The main FOXMAN-UN server and the standby server machines are connected to the network, and backing up their database in regular intervals. In case of a failure of the main server, the warm standby server takes over automatically. While in warm standby, the standby server regularly fetches the database from the main server to keep its database synchronized.

Please note:
The term machine represents either a workstation or a server.

The criteria of all recovery methods are based on the importance of speed of return to normal operation.

14.3.2 Cold Standby

Under normal operation it is expected that the database and system files are backed up on a regular basis. In case of failure of the main workstation or server, the operator must:

- Make sure that the workstation ports are connected to the management network (i.e. the LAN port is connected).
- Manually start the core services on the cold standby system.
- Connect the clients to the cold standby system once it is up and running.

The requirements for this solution are:

- A second workstation or server – with the same Hardware configuration as the main one, with FOXMAN-UN installed;
- A second FOXMAN-UN license & key for the new hardware.
- Setting up the Main/Standby configuration with the two servers, and selecting “Cold Standby” for the standby server.

This solution is sufficient to provide a standby concept with a recovery time of approximately 10 min. It requires manual intervention.

14.3.3 Warm Standby

This option is supported via the Main/Standby option. When the core services on the main server are down, or when the main server is not reachable, the standby server starts its services automatically after a predefined timeout and is available during the unavailability of the main server.

The requirements for this solution are:

- A second workstation or server – with the same Hardware configuration as the main one, with FOXMAN-UN installed;
- A second FOXMAN-UN license & key for the new hardware.
- Setting up the Main/Standby configuration with the two servers, and selecting “Warm Standby” for the standby server.

This solution provides a faster switch-over than the cold standby, and the standby server activation is done automatically with configurable timeouts.

14.4 Internal Process Recovery

14.4.1 Watch-Dog Processes

FOXMAN-UN has two watchdog processes, which ensure that critical processes stay active. In case of failure of a process, it is automatically restarted and appropriate indications are provided to the operator via the Alarm list.

The watchdog mechanism is automatically initiated upon installation and reboot of the workstation. In this way FOXMAN-UN looks at the recovery from a critical situation by itself before involving the operator.

15 HW and OS Requirements

The FOXMAN-UN application is offered in different versions for the following platforms:

- Red Hat Enterprise Linux (RHEL),
- Microsoft Windows® based PCs (Client only, i.e. GUI and NEM Help).

15.1 RHEL Platform

The FOXMAN-UN application can be installed on Red Hat Enterprise Linux (RHEL) versions as given in the Release Note for the current FOXMAN-UN release.

For more details on operating system and hardware requirements refer to the FOXMAN-UN Release Note under «Hardware and OS Requirements».

15.2 Microsoft Windows Platform

For details on operating system and hardware requirements for the FOXMAN-UN client for Windows® refer to the FOXMAN-UN Release Note under «Hardware and OS Requirements».

16 License Concept

For details on the FOXMAN-UN licensing model please refer to the document:

- “FOXMAN-UN Licensing Model” [1KHW029143].

17 Glossary

17.1 General FOXMAN-UN Expressions

Table 9: General FOXMAN-UN Expressions

FOXMAN-UN Expressions	Description
Action Buttons	On the bottom of dialogs, used to [Save (Apply)] or [Cancel] changes made and to [Close] the dialog.
Agent	Identifies an EOC or ECC subnetwork or an Ethernet port that is used to communicate with the NEs via one of the communication ports of the WS.
Alarm cleared	Fault condition disappears. This causes an alarm off event to be generated.
Alarm off event	Clearing of an alarm either as a result of operator repair action, or self-correction.
Alarm on event	Occurrence of a new alarm.
Alarm outstanding	Active alarm
BP	Basic Package of FOXMAN-UN.
Dialogs	The FOXMAN-UN operator’s windows for displaying and setting the parameters of the network, and parameters of the NEs and FOs that it contains. Dialogs contain Fields, Menus, and Push Buttons.
Dialog Menus	Always present at the top of the maps and dialogs
Domain Name	Identifies a grouping of NEs. (e.g. all NEs with the same Domain Name are identified as all managed by the same operator.
ENP	Ethernet Networking Package of FOXMAN-UN.
Lower level maps (group maps)	Represent parts of the network. Display symbols optionally placed over city maps, floor plans and/or cabinets.
Maps	The FOXMAN-UN operators' windows for visually representing the network. Maps are organized into a hierarchy. The root map can contain group symbols representing a lower level map which can again contain group symbols. The bottom level group map then shows the individual NEs. Each map contains a menu bar and navigation buttons.
Menus	2 types of menus are available allowing the operator to easily select (using the mouse) commands from a roll down list: Dialog menus and Symbol menus (context menus).
NE	Network Element, a network node managed by FOXMAN-UN.
NE Address	Identifies an NE within a Management Network (e.g. the Ethernet address or IP address of an NE).
NP	Networking Package of FOXMAN-UN.
Parameters	Any settable attributes of Units/SbUs (options, modes of operation, signal levels, etc.).
Context menus	Selective menu depending on the cursor position, popping up when the RIGHT mouse button is pressed.
Symbols	Graphic representations of network elements, groups of NEs, foreign objects, system NE on maps.

Hitachi Energy Ltd
Bruggerstrasse 72
5400 Baden - Switzerland

Phone: please refer to https://www.hitachienergy.com/contact-us/Customer-Connect-Center (Customer Connect Center)
Email: communication.networks@hitachienergy.com

www.hitachienergy.com/communication-networks

Document ID: 1KHW002415 R18 Rev. A