AXX 9840 INSITE

R2.0

User Guide

ERICSSON

ERICSSON

1 INTRODUCTION

2 STARTING THE AXX 9840 INSITE

4 MCN SETUP

5 ETHERNET SERVICES MANAGEMENT

2/1553-2/ZAN 601 13/1 Uen A 2006-10-16

1 Introduction

1.1 Contents at a glance

"Report tool"

The report feature helps you to get an overview of configuration and data that are currently implemented in the managed network. The reports can be used for general analysis of the state of the management system and managed network, or for providing an overview on configured services in the network.

"Layer 2 Configuration"

Describes management of the bridging service (L2 forwarding) with Bridge, MAC Multicast and IGMP Snooping, Spanning tree protocol (STP), Rapid STP (RSTP), Traffic control and VLAN.

"Layer 3 - configuration"

Management of the IP service with Layer 3 IP forwarding, IP interfaces, RIP and OSPF,IP redundancy, DHCP and QoS.

"Management of AXX10 and AXX11" - "Management of AXX10 and AXX11"

Describes management alarm handling, performance management and settings of the units.

1.2 AXX 9300 METRO management tasks

The links below guide you to the main AXX 9300 METRO related management tasks.

- **"AXX 9300 METRO User Management" on page 14**
- **"The Commissioning Wizard" on page 17**
- **"The MCN Wizard" on page 169**
- **"AXX 9300 METRO Shelf Management" on page 359**
- **"AXX 9300 METRO Cross Connection Management" on page 436**
- **"L1 Ethernet Service over SDH" on page 566**

2 Starting the AXX 9840 INSITE

2.1 Logon

The purpose of this chapter is to describe the tasks involved in starting up the program and connecting to a TMN server and the managed network.

2.1.1 Preconditions

2.1.1.1 The User

The user is provided with a valid User ID and password, set by the system administrator.

AXX 9840 INSITE

The AXX 9840 INSITE system is installed, the name of the host is known and the server is running.

2.1.1.2 The Network

Network Elements are available in the network and communicate with the system, see “The Commissioning Wizard” on page 17

2.1.2 Start the program

Procedure: **START THE PROGRAM ON WINDOWS**

1. Select Programs from the Start menu.
2. Locate and select the AXX 9840 INSITE program.

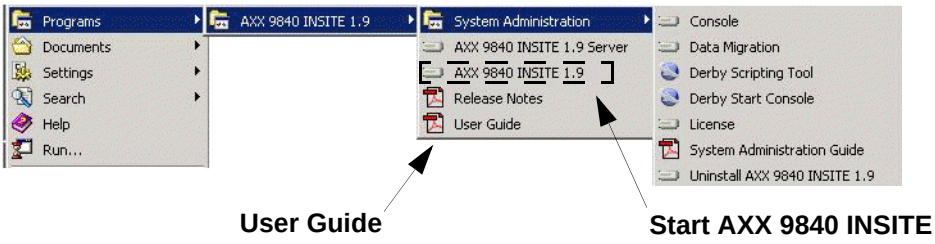


Figure 1 AXX 9840 INSITE program menu on Windows

The system presents the AXX 9840 INSITE logon window with information about the product name and release edition. See “Logon AXX 9840 INSITE” on page 6.

Procedure: **START THE AXX 9840 INSITE ON UNIX (SOLARIS)**

1. Open a shell window.
2. Navigate to the link directory.
3. Enter and execute the command: /**`AXX 9840 INSITE_x.y_client`**

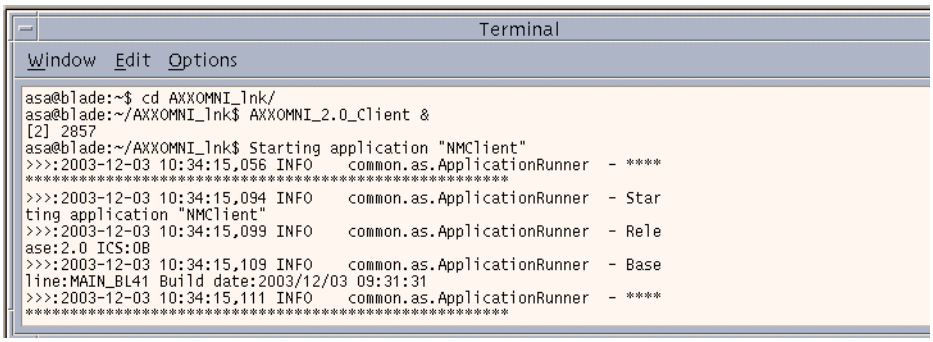


Figure 2 Program menu on UNIX- example.

2.1.3 Logon AXX 9840 INSITE

2.1.3.1 Logon screen.

The layout supports new NEs with other authentication mechanism than SNMP.

- IP: The address of the NE.
- User: Field used for AXX 9300 METRO. Enter your user-name (users are configured on the NE, see ref.“AXX 9300 METRO User Management”.)
- Password: For AXX 9300 METRO enter the password For non-AXX 9300 METRO NEs, enter the SNMP community string.

Procedure: `LOGON`

1. Enter the IP address or select from the pulldown menu.
2. Enter your User id.
3. Enter the **Password. (Not required the first time you login)**
4. Enter name of the host as **Server** (localhost = default).

Figure 3 Logon window- example

5. Click **Logon.**

Community access levels:

The network element supports three community access levels:

- ReadOnly - only read access to the whole MIB
- ReadWrite - read and write to the MIB, but can not change community strings
- Super - read and write to the complete MIB.

6. The system validates the logon input and opens the AXX 9840 INSITE Desktop.

You can now navigate in the topology and perform network element management from the Desktop. Your Desktop will have a view predefined according to your role.

Logon failed

If the logon input is not valid, the system will ask you to try again.

Figure 4 Logon message- example

2.2 Edit User settings

2.2.1 Enter User profile

You can enter your user profile from the Desktop.

Procedure: **ENTER USER PROFILE**

1. From the **Tools** menu, select **User settings**.

The system opens the dialogue box.

Enter your name and contact information
Click OK

Figure 5 User Settings dialog box

NOTE! UserId and Role are read - only, except for the System Administration.

2.2.2 Change Password

Procedure: **CHANGE YOUR PASSWORD FROM THE DESKTOP.**

From the **Tools** menu, select **User Settings**.

The system opens the dialogue box.

Open the password dialogue
Type the new password
Retype the new password
Click OK

Figure 6 User Settings- example

TIP! Select a password to remember, one that you do not have to write down

2.3 Log off

Procedure: **EXIT THE PROGRAM**

1. Select **Exit** from File menu or press **Alt and F4**

Figure 7 Exit

The system will update any changes to your user profile.

NOTE! You will be prompted to save any unsaved changes.

2.4 Initialisation Of Network Elements

A local terminal with VT100 emulation is required during the first commissioning of the network element in order to set up the necessary communications parameters enabling access to the element via AXX 9840 INSITE over the Management Port.

After the first commissioning, the VT100 interface can be used for modifying the communications parameters and perform some status checks of the network element.

The VT100 interface is password protected.

2.4.1 Commissioning of IP address via VT100 Interface

AXXCLI is a line-oriented ASCII-based management interface embedded in the AXX network element.The AXXCLI is accessed via the VT100-port. The serial connection communications parameters are fixed:

- 19200 bit/s,
- no parity,
- 8 bits,
- 1 stop bit,
- and no hardware flow control.

VT100 terminal codes are used.

The VT100-port (Console port) for the AXX network element is provided using an RJ-45 connector. The cable for connecting the VT100-port to the serial-port on the PC can be provided. The specification of this cable is the following:

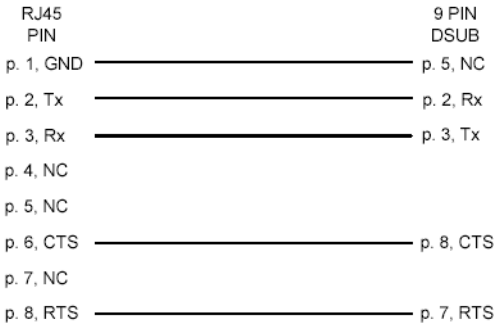


Figure 8 VT100-CABLE (Console cable)

NOTE! Pin 4,5 and 7 are only used for debug purposes.

Procedure: **INVOKE CLI**

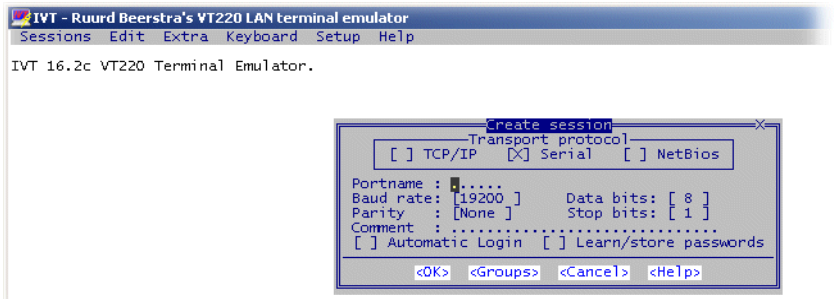
1. Connect the VT100 interface of the network element to a free COM port of the PC running the AXX 9840 INSITE application.

2. A VT100 terminal application is available from the AXX 9840 INSITE Logon window.

3. Double-click the VT100 icon in the lower right corner of the Logon window.

Figure 9 Start VT100 terminal application

4. The terminal application launches.



5. Enter **COM port** name and select **OK**.

6. An AXXCLI session is invoked by typing **axxcli** in terminal window. User authentication (password, 8-12 ASCII characters) is required, as the following session start-up sequence shows. Default password is AXXCLI.

```
>axxcli

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

        AXX 9200 EDGE Command Line Interface

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


Enter AXXCLI password: ******
```

AXXCLI>

7. You will find the AXXCLI commands in the NE Quick Reference Guide.

It is sufficient to type leading characters of the command name to avoid ambiguity – the same applies to keywords.

The BACKSPACE or DELETE key may be used to edit the command line. Commands and keywords are not case-sensitive.

The Management Port IP address is a compulsory parameter, and must be specified by you. All the other parameters (except default gateway) are defaulted to predefined values if they are not specified.

Configuration of VT100 terminal

The VT100 terminal can be launched from the desktop as well as from logon window, see Figure 9

You may change the terminal SW to be launched.

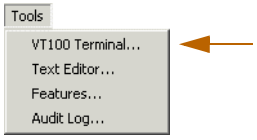


Figure 10 Start VT 100 from desktop

This is done by editing the VT 100 path description in the **ExternalApplications.xml** file, found in the folder:

installdir\AXX 9840 INSITE**res\config**
Example of the ExternalApplications.xml:

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<ExternalApplications>

  <vt100       file="../external/IVT_VT220_Telnet/ivt.exe"/>
<exec        file="rundll32 url.dll,FileProtocolHandler"/>

  <editor       file="notepad.exe"/>
<fileexplorer file="explorer.exe"/> <companyweb   file="rundll32
url.dll,FileProtocolHandler" params="http://www.ericsson.com"/>
<web          file="rundll32 url.dll,FileProtocolHandler"/>
<help         file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/AXX9840INSITE_UserGuide.pdf"/>
<alarmhelp    file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/AXX_ALARMS_ED01.pdf"/>
```

```
<alarmhelp2   file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/AXX9300METROAlarmEvent.pdf"/>
<maphelp      file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/MapDesigner.pdf"/>
<sysadm       file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/SystemAdministration.pdf"/>
<releasenotes file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/AXX9840INSITE_ReleaseNotes.pdf"/>
<pmhelp file="rundll32 url.dll,FileProtocolHandler"
params="../res/help/PMTools_UserGuide.pdf"/>

</ExternalApplications>
```

2.5 AXX 9300 METRO User Management

The AXX 9300 METRO User Management application allows system administrators to add and remove users on an AXX 9300 METRO network element. Other users may only change their own settings.

Procedure: **START THE APPLICATION**

1. From the **Equipment** menu, select **NE User Management**.

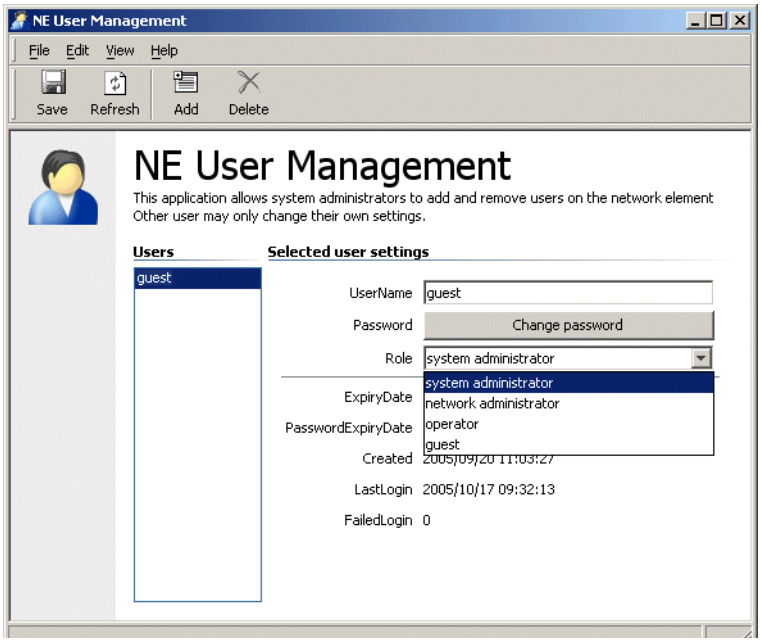


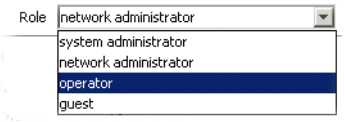
Figure 11 AXX 9300 METRO User Management application ()

Procedure: ADD A USER

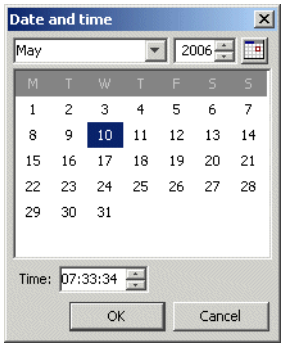
1. In the toolbar click 

.
2. Enter **User Id** and initial **password**.

3. Click **OK**.
4. Select desired **role** for the new user.



5. Optionally you **can change default** user and password **expiry dates**.



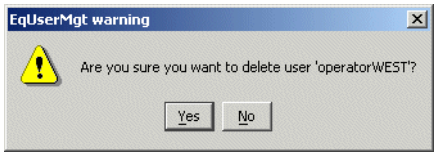
6. Press 

to add the new user.

Procedure: DELETE A USER

1. **Select** desired **user** and press 

2. Click **Yes** in the dialog box appearing.



2.5.0.1 Feature Permission

The role associates users with permissions on identified system features in a feature-to-role matrix. The roles are predefined and can not be edited.

If the feature under security management is associated with a system application, the permissions is used to control the execution of the application, the access to reading attributes and changing attributes.

If the feature under security management is associated with accessing network elements, the permissions is used to control the capability to monitor the network element, commission the network element or manage services provided by the network element.

If the feature under security management is associated with accessing the system information model, the permissions is used to control the creation, modification and deletion of objects within the model.

	System Administrator	**Network Administrator**	**Operator**	**Guest**
Security Management				
Audit Trail report	x			
Manage Users	x	r		
Network Element Management				
Slot configuration	x	x	r	r
MCN configuration	x	x	r	r
NE restart	x	x	x	
SW download	x	x	r	r
Configuration backup/restore	x	x	r	r
Port enable/disable	x	x	x	r
Bandwidth Management	x	x	x	r
VLAN Management	x	x	x	r

	System Administrator	Network Administrator	Operator	Guest
Notification Management	x	x	x	r
Cross Connect setting	x	x	x	r

2.6 The Commissioning Wizard

2.6.1 Introduction

The Commissioning Wizard is an interface for setting-up an unconfigured network element. A set of limited but important features can be configured with the wizard. Everything that the can be configured, can also be configured from a management station's Desktop. So the Commissioning Wizard isn't a necessary tool, but one of convenience. For a preconfigured network element, the Desktop, and not the Commissioning Wizard, is recommended for additional configuration.

NOTE! This chapter explains the use of the Commission Wizard to configure an unconfigured network element. Configuration concepts, access limitations, and the alike, are beyond the scope of this chapter.

NOTE! This chapter is applicable to the AXX 9300 METRO, the AXX 9100 CONNECT and the AXX 9200 EDGE network element types.

NOTE! An AXX 9300 METRO's active Aggregate Module (AM) must have its Expected Mode properly configured before the Commissioning Wizard will work properly.

2.6.2 Starting the Commissioning Wizard

PROCEDURE: **STARTING THE COMMISSIONING WIZARD**

The Commissioning Wizard is a pop-up window started from the management station's Desktop.

Select **Equipment > Commissioning Wizard** from the Desktop's menu bar.

2.6.3 Welcome to the Commissioning Wizard

The Commissioning Wizard is split into two panes, one left and one right. The wizard begins by introducing itself with a welcome message on the right side panel.

The left side panel contains a list of the setup steps. The user is prompted for information at each step. To move from one step to the next, click "Next" on the lower right side of the window. There are slight differences in the left side panel depending on the NE type.

The wizard only makes changes to the network element after all steps are completed.

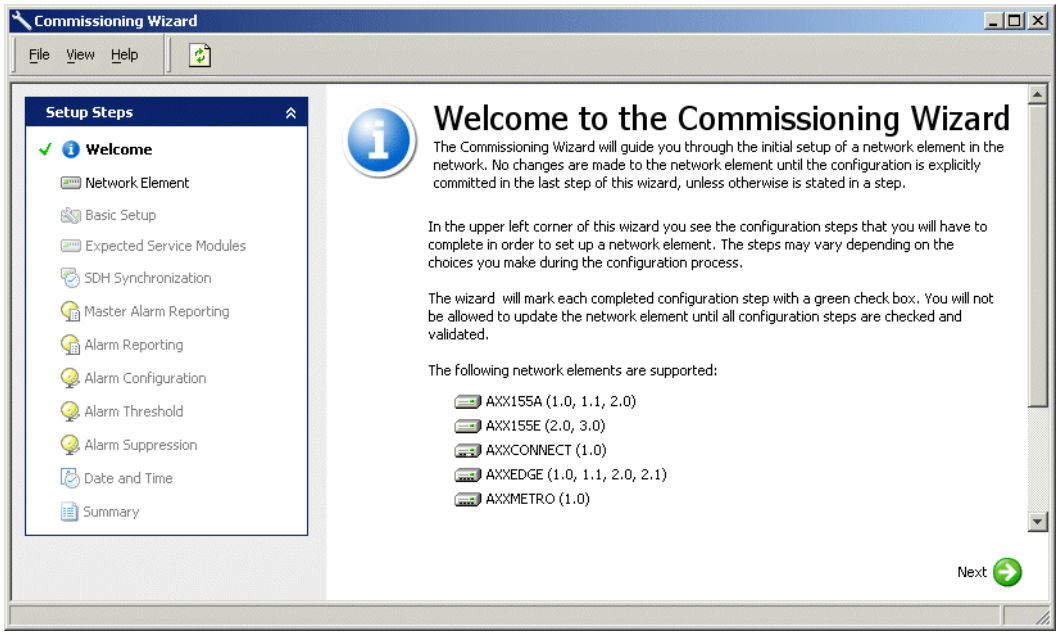


Figure 12 Welcome to the Commissioning Wizard

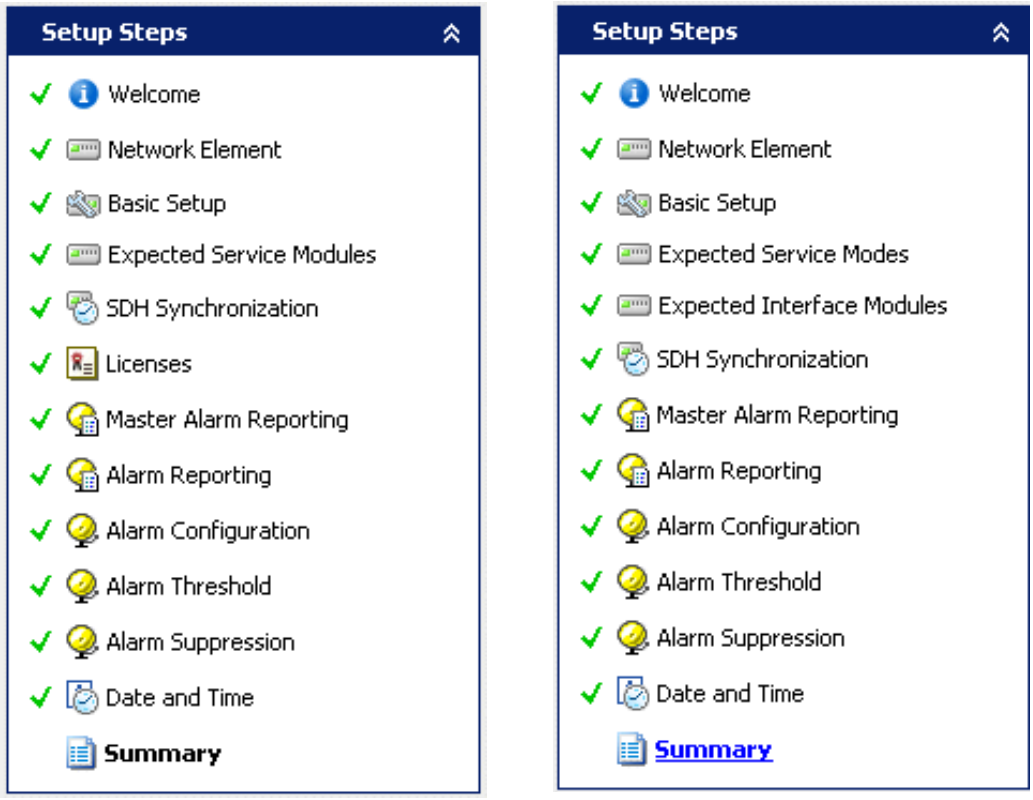
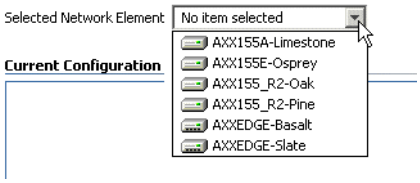


Figure 13 Setup Steps
The AXX 9100 CONNECT and the AXX 9200 EDGE (left), and the AXX 9300 METRO (right)

2.6.4 Setup Step - Network Element

The Network Element setup step lists information about the NE. It is mostly about the installed hardware for the network element. The exact information shown, varies with network element type.

Select the **Network Element** to be configured from the pull-down menu



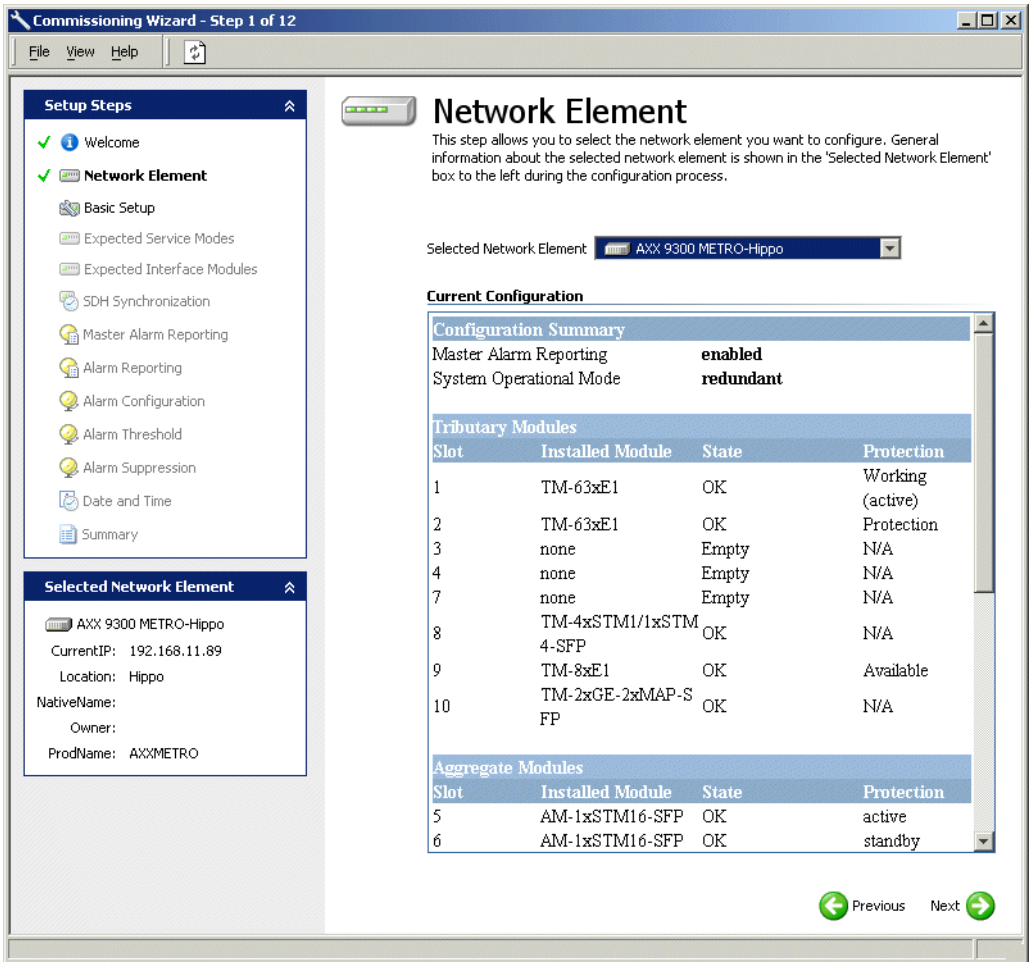


Figure 14 AXX 9300 METRO - Network Element

2.6.5 Setup Steps - Basic Setup

Name, Location and Owner identify and describe a network element. They serve no technical purpose, but are helpful for management. Minimally, it is recommended to set Location, which is used to label the network element in the Management Tree.

NOTE! For more information see “Network element information” on page 33.

The remainder of Basic Setup varies the with network element type. However, regardless of type, the information provided configures access to the NE for management. It identifies hosts (IP addresses), user names, and passwords that are allowed to make changes to the NE.

The Basic Setup step is identical for the AXX 9200 EDGE and the AXX 9100 CONNECT. “SNMP Users and Access Rights” identifies hosts from where remote management will be allowed by the NE. The associated password is actually an SNMP (Simple Network Management Protocol) community string. For users with SNMP experience, the majority of fields will be self explanatory. Further explanation beyond the scope of this chapter.

For the AXX 9300 METRO, “User Management” identifies individual user accounts. Most of the fields are self explanatory. The meaning of the specific fields and the values they can accept is beyond the scope of this chapter.

The AXX 9300 METRO section “Notification Subscribers” identifies IP addresses where SNMP traps will be sent. When the AXX 9820 CRAFT is used for management, entries will automatically be added and removed when users login, and there is generally no need to explicitly add entries. When the AXX 9840 INSITE is used, the IP address of the server should be added.

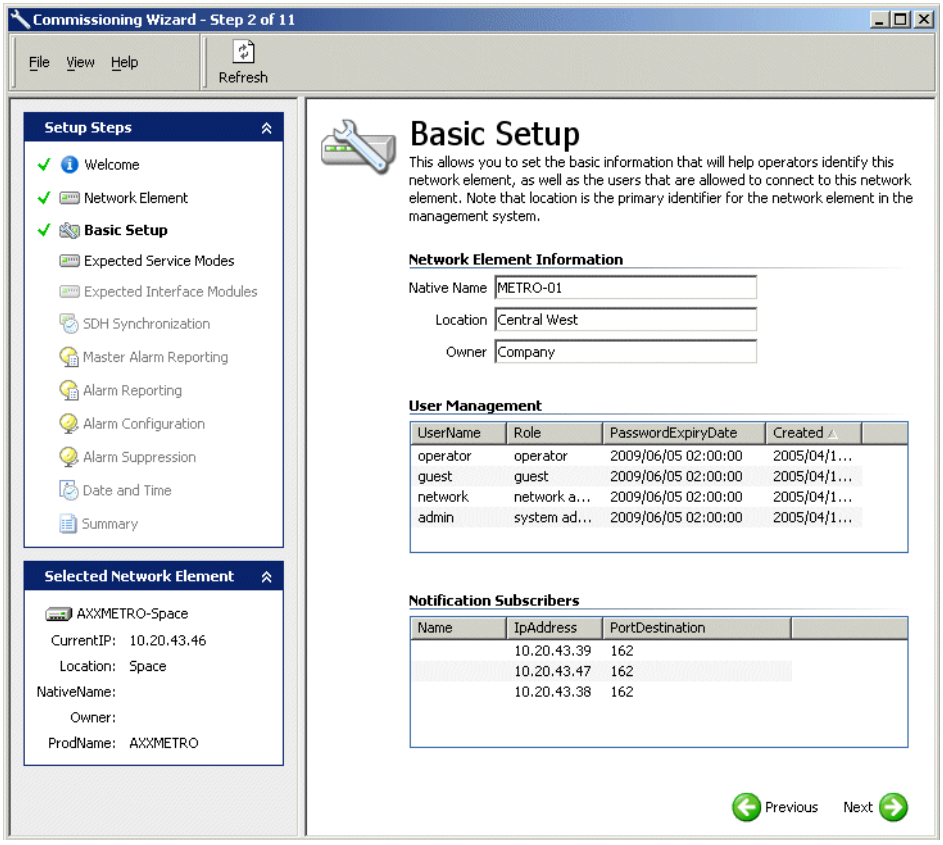


Figure 15 AXX 9300 METRO - Basic Setup

2.6.6 Setup Step - Expected Service Modes or Expected Service Modules

Expected Mode or Expected Module identifies the module that will be configured in a slot. In almost all cases, this is set to match the physically installed module. The physically installed modules are shown (Installed Module), and the Expected Mode/Module can be set.

Some modules have multiple modes, supporting different functionality. For example, the AXX 9300 METRO's TM-4xSTM1/1xSTM4-SFP can be configured for either four STM-1 ports or one STM-4 port. On the AXX 9300 METRO, the mode is selected together with the module (Expected Mode). On the AXX 9200 EDGE and the AXX 9100 CONNECT the module (Expected Module) and the mode (Config Mode) are configured separately.

Depending on the setting of Expected Mode or Expected Module, additional configurable attributes will become available. For users familiar with the network elements, these attributes will be self explanatory. An explanation of these attributes is beyond the scope of this chapter.

Notice that the first two tabs for the AXX 9100 CONNECT aren't slots, but "Aggregate Interfaces," and "pdh." The Aggregate Interface's attribute Aggregate Mode is basically equivalent to Expected Mode. There is no mode to configure for under the pdh tab.

The remainder of the information in the window identifies information about the module installed in the slot and the software installed on the module.

TIP! For more information see “Slot attributes” on page 34.

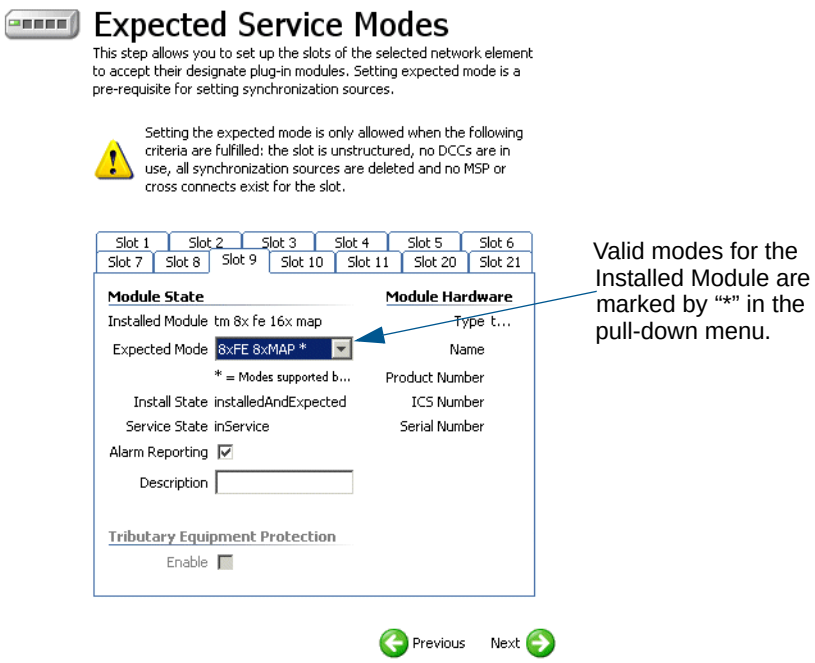


Figure 16 AXX 9300 METRO - Expected Service Modes

2.6.7 Setup Step - Expected Interface Modules (AXX 9300 METRO)

SFPs offer flexibility in the selection of physical interfaces. Ethernet ports can be configured to use fixed interfaces or SFPs. SDH fiber ports must use SFPs. The attribute Expected Port Interface indicates the type of interface that will be configurable, either an SFP type or a fixed interface. Most commonly, Expected Port Interface is set to match the physically installed SFP type (Installed Interface field).

The values for Expected Port Interface are beyond the scope of this chapter.

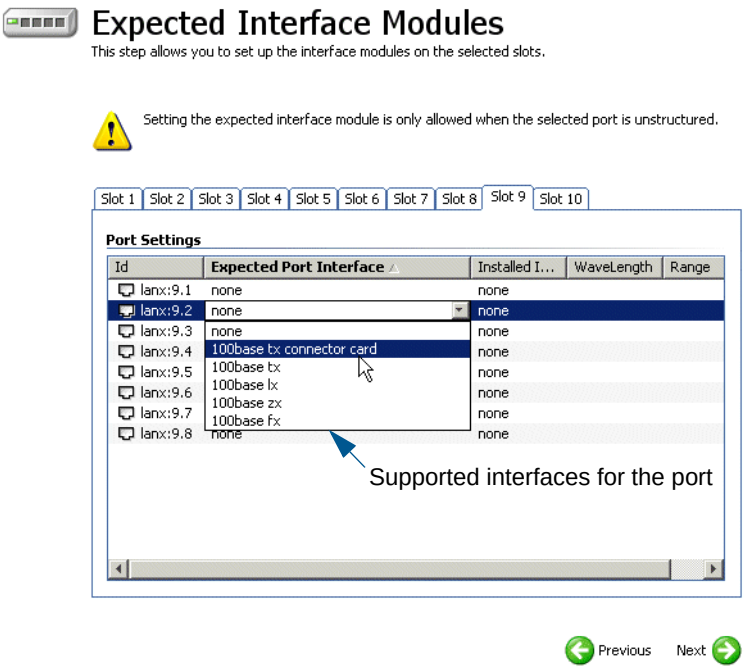


Figure 17 Expected Interface Modules

READ MORE: See “Physical Interfaces” in the AXX 9300 METRO Technical Reference for more information.

2.6.8 Setup Step - SDH Synchronization

All SDH equipment requires a synchronization signal. The signal is referred to as T0. A variety of sources can provide T0. If multiple sources are identified, the additional ones are backups should the primary fail. If T0 sources are not provided, the NE will use its internal clock. Although this can work, it is generally not recommended. Setting T0 sources is recommended.

Network elements have a SYNC port that can be used to send a synchronization signal to external equipment. (The AXX 9300 METRO can have two.) The signal, T4, is configured from the SDH Synchronization setup step. Unlike T0, T4 is not a critical setting and is unused in many networks.

Further explanation is beyond the scope of this chapter.

TIP! For more information see “SEC (T0) synchronization” on page 35 and “2048 kHz Output (T4) synch - AXX 9200 EDGE - parameters” on page 36.

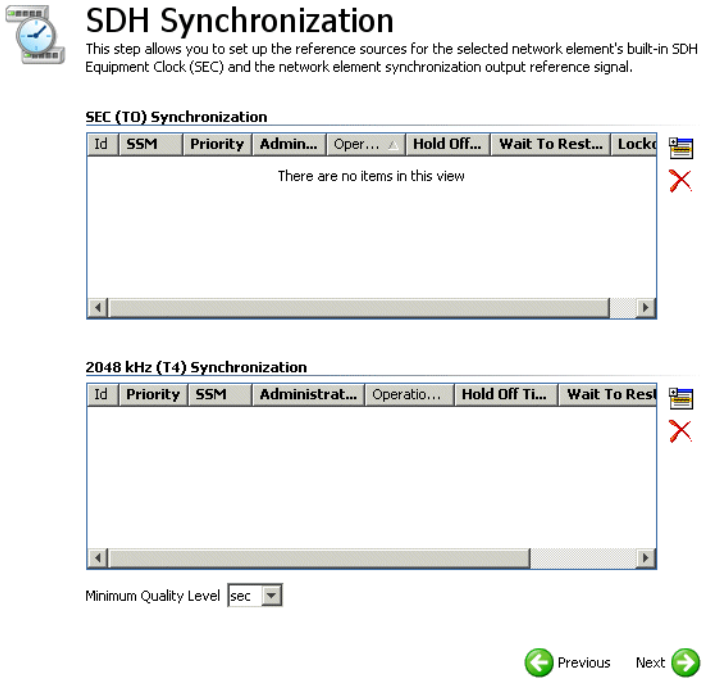


Figure 18 SDH Synchronization

2.6.8.1 Adding Entries to the Synchronization Tables

The button is used to add a synchronization source to the table. After the entry has been added, the fields can be set to identify and configure the source.

Highlighted entries can be deleted with the button.

2.6.9 Setup Step - Licenses (AXX 9100 CONNECT and AXX 9200 EDGE)

A license provides access to a feature in a network element. Without a license, the feature is unavailable. Licenses are network element specific (i.e. node locked). They are provided as files that must be uploaded to the NE. The Licenses setup step indicates if a license is already installed and, through the “Package Installer,” can be used to install licenses. The Package Installer allows the license file to be identified, uploaded and automatically installed.

TIP! For more information see “Licenses installed - parameters” on page 47 and the Chapter , “NE updates and upgrades.”

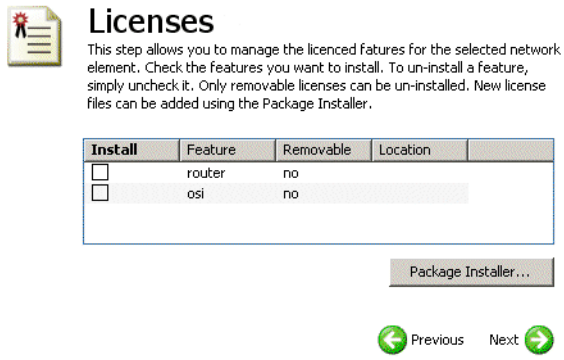


Figure 19 AXX 9200 EDGE - Licenses

2.6.10 Setup Step - Master Alarm Reporting

This setup step allows global network element alarms to be enabled or disabled. A brief description of each alarm type is provided by the wizard. For users without experience or guidance, it is recommended to enable Master Alarm Reporting and Pointer Justification Event, and to disable Non-Intrusive Monitoring and Link Capacity Adjustment Scheme during commissioning. Additional information about these alarms is beyond the scope of this chapter.

TIP! For more information see “Master Alarm Reporting strategies” on page 38.

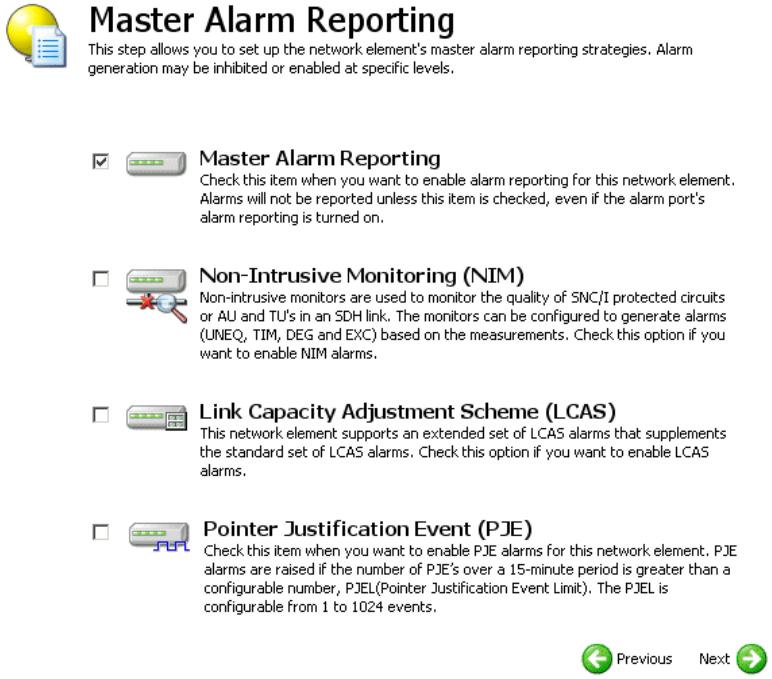


Figure 20 AXX 9300 METRO - Master Alarm Reporting

2.6.11 Setup Step - Alarm Reporting

A network element has inputs for external alarms. If an external alarm is triggered, a message can be sent to the management stations. Most commonly, environmental conditions such as air conditioning failure, UPS power loss, or temperature of range, are set to trigger external alarms.

Alarms can be triggered closed or open loop, and each alarm’s message is configurable (Description attribute). Configuring of external alarm is not crucial, and they are unused in many networks.

From the Alarm Reporting setup step, alarms for an AXX 9200 EDGE’s power ports can also be enabled or disabled. The power port alarms are always enabled for the AXX 9100 CONNECT and AXX 9300 METRO. It is recommended to enable them for the AXX 9200 EDGE.

.

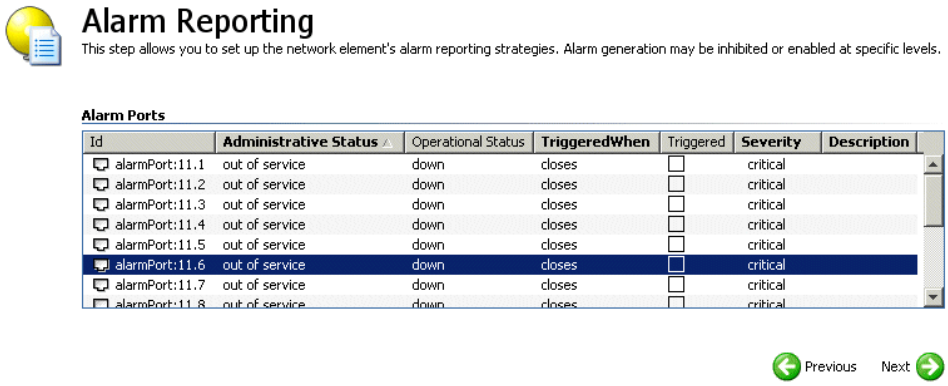


Figure 21 Alarm Reporting

2.6.12 Setup Step - Alarm Configuration

The Alarm Configuration setup step is split into two parts. The upper part, Alarm Configuration, provides a list of alarms that the network element can raise. It allows each alarm's description (Probable Cause Qualifier attribute) and each alarm's Severity to be modified. Modifying these fields is seldom required.

The lower part, Alarm Persistency, defines how long a problem must be present before an alarm is raised, and how long the problem must be corrected before an alarm is cleared. Understanding these settings require SDH/PDH experience, and should only be modified by knowledgable users. In many networks, the defaults are left unchanged.

TIP! For more information see “Alarm configuration (severity list)” on page 39 and “Alarm persistency” on page 39.

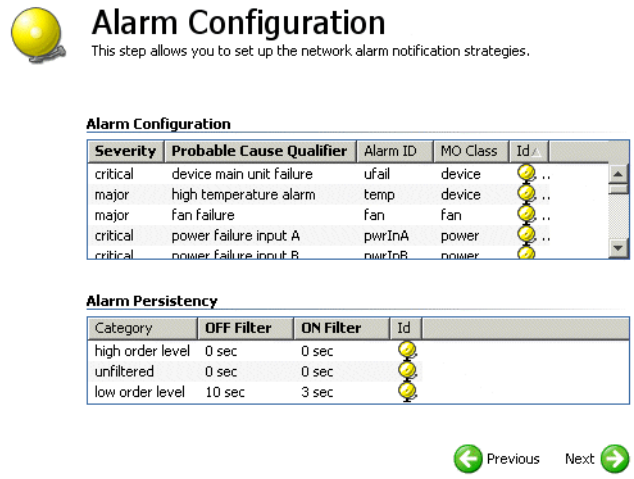


Figure 22 Alarm Configuration

2.6.13 Setup Step - Alarm Threshold

Alarm Thresholds are specific levels that set the requirements for a signal to be in range. When a signal is out of range, an alarm is raised. Understanding the thresholds require SDH/PDH experience, and should only be modified by knowledgable users. In many networks, the defaults are left unchanged.

TIP! For more information see “Alarm thresholds” on page 40.

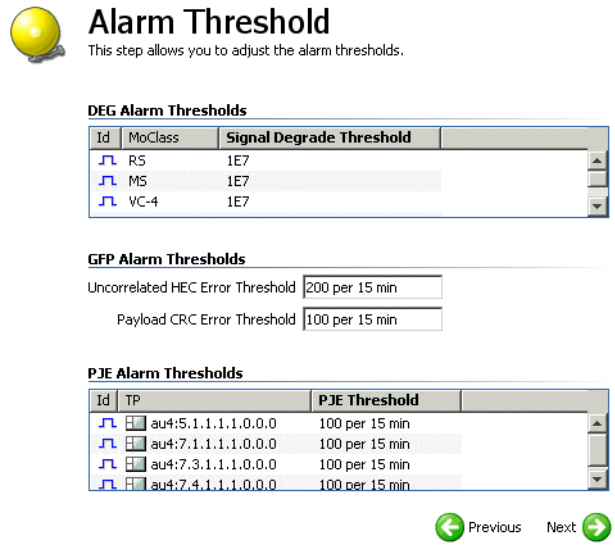


Figure 23 Alarm Threshold

2.6.14 Setup Step - Alarm Suppression

Individual alarms can be suppressed. Alarm suppression requires SDH/PDH experience, and should only be done by knowledgable users. In many networks, the defaults are left unchanged. If changes are made, a common one is to enable the AIS alarm, which is disabled by default.

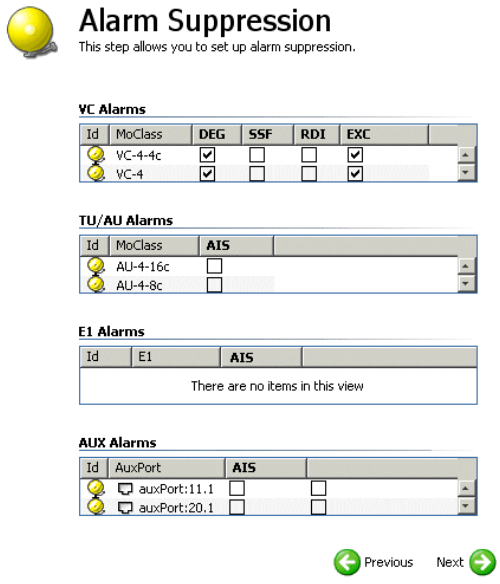


Figure 24 Alarm Suppression

2.6.15 Setup Step - Date and Time

NEs do not need to know the proper date and time. However, various happenings, such as the raising of alarms, are assigned time stamps. Having accurate time stamps simplifies management.

The date and time can be kept local in the network element. Alternatively, if a time server is available, the NE can be configured to keep itself synchronized with the server.

Using the Commissioning Wizard the time cannot be randomly assigned. Setting the time will match the NEs clock to the clock on the computer where the wizard is running. If it is necessary to set a random time and date, use the management station's Desktop.

The bottom of the window shows the NE's clock. Additionally, if the NE is already configured to synchronize with a time server, the server's IP address is also listed. However, when the wizard is used for its most common purpose, to configure an unconfigured NE, the NE will not be preconfigured to synchronize with a server.

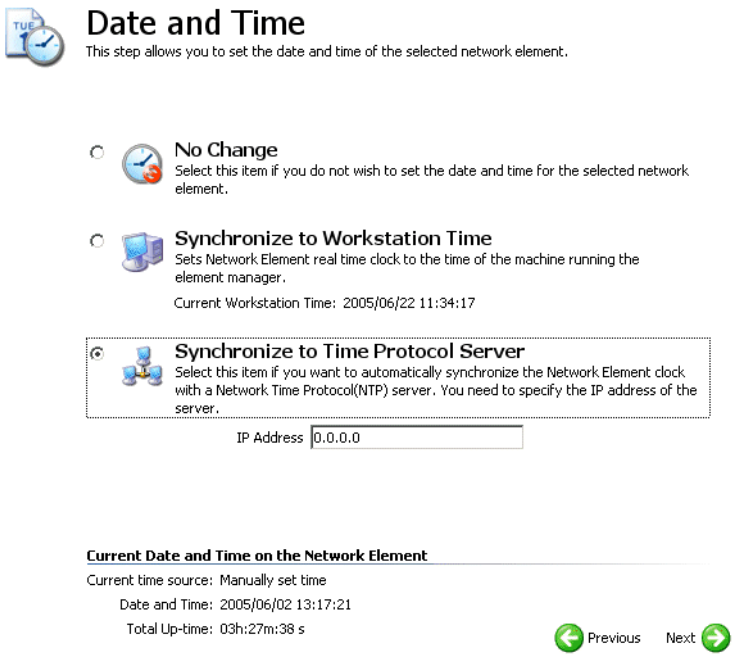


Figure 25 Date and Time

- **No Change**
  No Change leaves the NEs clock settings unchanged.
- **Synchronize to Workstation Time**
  Synchronize to Workstation Time synchronizes the NEs clock to match the clock on the computer where the Commissioning Wizard is running.

- **Synchronize to Time Protocol Server**
  Synchronize to Time Protocol Server configures the NE to work with a server. The IP address of the server must be provided. Additionally, for the AXX 9100 CONNECT and AXX 9200 EDGE the Synchronization Interval is required. More information about the meaning of these fields is beyond the scope of this chapter. Note that the AXX 9100 CONNECT and AXX 9200 EDGE use a different protocol then the AXX 9300 METRO for communicating with a time server.

2.6.16 Setup Step - Summary

The summary shows the changes that have been planned. If the configuration is not correct, the user can click on any setup step in the left side panel and modify the planned configuration.

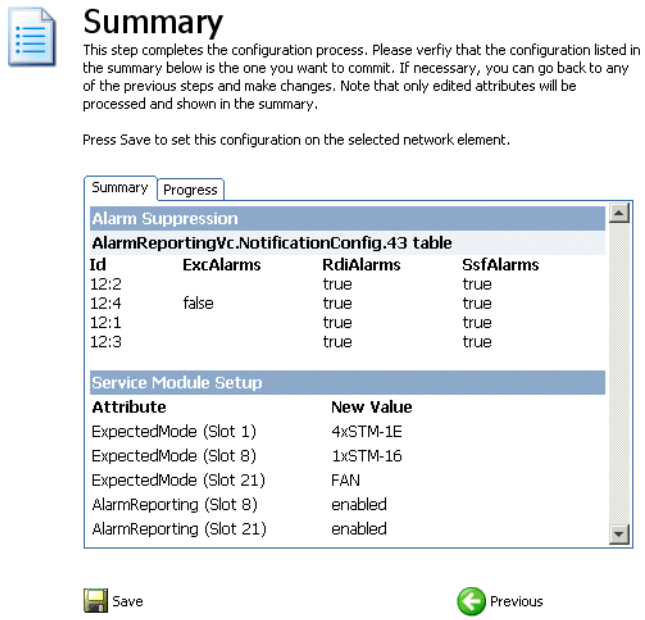


Figure 26 Summary

If the configuration is correct, click 

Save to commit the changes to the network element.

NOTE! Because multiple changes are being committed, saving can take several minutes.

2.6.16.1 Feedback as the changes are committed to the NE

After **Save** is selected, the wizard switches over to the Progress tab to describe each change as it is completed. Additionally, a **Stop** button appears

next to **Save**. Stopping will not leave the NE is an unusable state, but it may leave it in a state unknown to the user.

The messages in the Progress tab can generally be ignored by less experienced users. Most importantly, when all the changes are committed, a message will state if the changes were successful, and how long they took to complete.

In the unlikely event that a change was not successfully committed to the network element, the failure will be reported in the Progress tab. The failure is also recorded in the management stations error log.

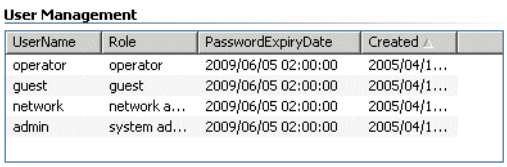
2.7 Select Attributes from the Commissioning Wizard

2.7.1 Network element information

The system presents the current network element instance description (default: blank text fields). Edit the network element description attributes;

Table 1 Network element description attributes

Parameter	Purpose	Comment
Native Name	Administratively assigned name for this managed NE.	0-160 characters.
Location	The physical location of NE.	Anything written in this field will replace the associated IP-address in management tree and graphical presentations. 0-160 characters.
Owner	Contact person for this managed NE.	0-160 characters.



2.7.2 SNMP Users table

2.7.2.1 Notification Subscribers

.

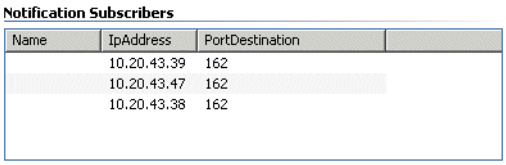


Figure 27 Notification subscribers list

Table 2 Slot attributes

Parameter	Purpose	Comment
Slot ID	Selectable tabs for each available slot.	
Installed Module	Displays currently installed module.	
Expected Mode	To select desired service mode from pull down menu.	Supported modes for the installed module are marked by a “*”.
Install State	Displays install state.	Possible states: - Empty - InstalledAndExpected - ExpectedAndNotInstalled - InstalledAndNotExpected - MismatchOfInstalledAndExpected
Service state	Displays service state.	Possible states: - InService - OutOfService (Fault condition present in service slot) - OutOfServiceByMaintenance (Module shutdown via HW switch or software) - NA (empty) - OutOfServicePending (Shutdown in progress)
Alarm Reporting	Option to enable alarm reporting of module.	If disabled this will suppress alarms related to this module.
Description	Administratively assigned name for this service module.	0-63 characters.

Parameter	Purpose	Comment
HW Inventory	Display HW serial no., product no., version (ICS) and type.	
Tributary Equipment Protection	Enable to protect the module	The adjacent module is set to protection, and is not configurable.
Power Configuration	Select DC Voltage source 48 or 60V	
AGGREGATE MODULES:		
System mode		REDUNDANT -Equipment protection is installed and works. DUPLEX - Probable network release mismatch - Equipment protection not working. - Update network release to match. SIMPLEX - Only one active Agg module LOCKED - Manually forced to active,
Slot state		ACTIVE WARM_STANDBY COLD_STANDBY BOOTING ERROR UNKNOWN NOT_PRESENT

Table 3 SEC (T0) synchronization

Parameter	Purpose	Comment
SynchPort	Identifier of the originating source port position.	
Source Type	Type of synchronization source. STM-n, E1-port or External Synch-port.	Notice, if desirable to use an E1-port as sync. source, PRA mode is required.
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type.
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.

Parameter	Purpose	Comment
Hold Off Time	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait To Restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
Administrative Quality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SSUT - PRC
Priority	Source priority.	1-5.
Operational Quality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC

Table 4 2048 kHz Output (T4) synch - AXX 9200 EDGE - parameters

Parameter	Purpose	Comment
Synch Port	Identifier of the originating source port position.	
Source Type	Type of synchronization source. STM-n or Internal Clock	
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type. STM-n port will by default send DoNotUse. Consider this parameter changed to fit your configuration.

Parameter	Purpose	Comment
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.
Hold Off Time	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait to restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
Administrative Quality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SUT - PRC
Priority	Source priority.	1-5.
Operational Quality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC

Table 5 Master Alarm Reporting strategies

Type	Description
Master Alarm Reporting	Enable alarm reporting for this NE. Alarms will not be reported unless this item is checked, even if the alarm port's alarm reporting is turned on.
Non Intrusive Monitoring	NIM monitors the quality of SNC/I protected circuits or AUs and TUs in an SDH link. The monitors can be configured to generate alarms (UNEQ, TIM, DEG and EXC) based on the measurements.
Link Capacity Adjustment Scheme	This NE supports an extended set of the standard LCAS set.
Pointer Justification Event	Raises an alarm if the number of PJEs over a 15 min period is greater than a configurable from 1 to 1024 events. This is the PJE Limit or PJEL.

NOTE! AXX 9300 METRO Non Intrusive Monitoring.
When creating non-intrusive monitors in AXX 9300 METRO, the PM counters are not cleared. If there are any non-zero counters in the current counter arrays before a NIM create, the counting continues from these values. Counters used for calculating DEG/EXC alarms are cleared, and all the valid-flags are cleared at NIM create.

Due to the number of possible NIM instances, the counters are only updated while the object exists. This applies for all VC-levels, and for BBE, ES, SES and UAS.

:

Parameter	Values	Comment
ID		
Administrative Status	- In service - Out of service	
Operational Status	- Down - Up	The operational status of the alarm port.
TriggeredWhen	- Opens - Closes	Choose if you want the alarm to be triggered when the alarm loop opens or closes.
Triggered	Ticked/unticked	
Severity	- critical - major - minor - warning	
Description	Enter text string	Optional

2.7.2.2 Alarm configuration (severity list)

Parameter	Purpose	Comment
MoClass	Display object type	
AlarmId	Abbreviation of alarm type	Identified as "ProbCause" in alarm table.
Severity	Set alarm severity	minor-major-critical
Description	Provide explanatory text for alarm.	Identified as "ProbCauseQ" in alarm table.0-64 characters.

2.7.2.3 Alarm persistency

Alarm persistency defines how long time an alarm has to be stable until the network element will generate an alarm notification, or how long time an alarm situation must have ceased until the network element will generate an alarm cleared notification. Persistency is configured separately for alarm and alarm clear situations, and is implemented by two filters:

Table 6 Alarm persistency - parameters

Parameter	Purpose	Comment
PersistencyCategory	Displays category	Applicable categories: - highorderlevel - unfiltered - loworderlevel
OnFilter	Seconds to wait until an alarm is raised.	0 - 30 seconds.
OffFilter	Seconds to turn off an alarm when cleared.	0 - 30 seconds.

Table 7 Persistency category

Persistency category	Alarm types	Managed objects
	LOS	SDH Port, PDH Port
	LOF	RS
	AIS	MS
	EXC,DEG	RS, MS
	TIM	RS
	RDI	MS
	CDF	RS, MS
	AUX	Aux Port
Unfiltered	LOP	TU4, TU3, TU12
	LOM	VC4
	LOF-RX, LOF-TX	E1
Low order level	AIS	TU4, TU3, TU12, E1, E3
	EXC, DEG	VC4, VC3, VC12
	SSF	VC3, VC12
	TIM, RDI, UNEQ, PLM	VC4, VC3, VC12

2.7.2.4 Alarm thresholds

Some alarms are generated when a performance measurement crosses a predefined threshold. In the Ericsson AXXESSIT network elements this threshold is configurable. Quality measurements on the SDH frames are associated with alarm threshold according to the listing below:

Table 8 Alarm threshold - parameters

Parameter	Purpose	Comment
MoClass	Display object type	
SD Threshold	Threshold for a DEG alarm to be reported.	10E-6 to 10E-9. For example, if set to 10E-7 , an alarm is raised when BER exceeds this threshold. To clear, the BER level must be improved by a factor 10.

2.7.2.5 Pointer Justification Event (PJE) Alarm Threshold

You can edit the number of PJEs inside a 15min period required to generate a PJE alarm.

The number can be from 1 to 1024 events.

2.7.2.6 VC alarms

Table 9 Alarm suppression - VC

Parameter	Purpose	Comment
MoClass	Display object type.	
DEG	Suppress or allow BER-DEG alarms to be reported.	
SSF	Suppress or allow signal server failure to be reported.	
EXC	Suppress or allow BER-EXC alarms to be reported.	10E-5 threshold level for the EXC alarms to be reported.
RDI	Suppress or allow RDI alarms to be reported.	

2.7.2.7 TU/AU alarms

Table 10 Alarm suppression - TU/AU

Parameter	Purpose	Comment
AIS	Suppress or allow AIS alarms to be reported.	

2.7.2.8 E1 alarms

Table 11 E1 Alarms

Parameter	Purpose	Comment
Id	Identifier of the E1 slot position.	
MoClass	Display object type.	
AIS	Suppress or allow AIS alarms to be reported.	

2.7.2.9 AUX alarms

Table 12 AUX Alarms

Parameter	Purpose	Comment
AIS	Suppress or allow AIS alarm to be reported.	Alarm Indication Signal

2.7.3 AXX 9300 METRO CommWiz

Network element information

The system presents the current network element instance description.

1. Edit the **network element description attributes**.

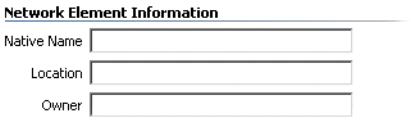


Figure 28 Network element information

Table 13 Network element description attributes

Parameter	Purpose	Comment
Native Name	Administratively assigned name for this managed NE.	0-160 characters.
Location	The physical location of NE.	Anything written in this field will replace the associated IP-address in management tree and graphical presentations. When entering value for location, avoid special characters such as apostrophe and quotation marks. Only use letters. 0-160 characters.
Owner	Contact person for this managed NE.	0-160 characters.

SNMP users and access rights (Community table)

In the Basic Setup windows you can also define the TMN managers (AXX 9820 CRAFT, AXX 9840 INSITE) that are allowed to access the network element.

The system presents the currently defined SNMP users defined in the network element.

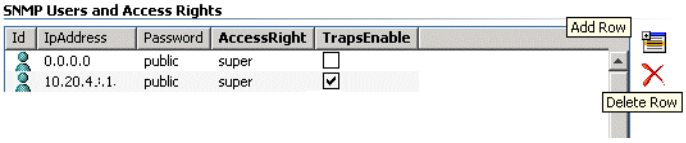


Figure 29 SNMP Community table

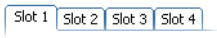
You edit (create, delete, modify) each user by the following attributes:

Table 14 SNMP attributes

Parameter	Purpose	Comment
IpAddress	IP address of manager / trap receiver.	IP address <0.0.0.0> for an instance in community table, means that any host can connect only limited by password. Removing this address will increase security in open networks.
Password	This is a selectable password to be decided by the operator.	1-20 characters.
AccessRights	This controls the access to MIB attributes: "readOnly", "readWrite" and "super".	At least one instance in the table should have "super" access to be able to maintain SNMP permissions for NE. Otherwise, if this is not desirable, you may configure the SNMP community table via commands in CLI via local console or Telnet.
TrapsEnable	Option to enable traps to be sent continuously to a specific host.	Current products and SW versions limit the maximum of instances in community table to 16. It is recommended no more than 3-4 with trap=enabled.

The slot attributes available for presentation are:

Table 15 Slot attributes

Parameter	Purpose	Comment
Slot ID	Selectable tabs for each available slot. 	Slot 1-4 for AXX 9200 EDGE Slot for AXX155A
Installed Module	Displays current installed module.	
Expected Module	To select desired service module from pull down menu. Enumerated list.	
Install State	Displays install state.	Possible states: - Empty - InstalledAndExpected - ExpectedAndNotInstalled - InstalledAndNotExpected - MismatchOfInstalledAndExpected

Parameter	Purpose	Comment
Service state	Displays service state.	Possible states: - InService - OutOfService (Fault condition present in service slot) - OutOfServiceByMaintenance (Module shutdown via HW switch or software) - NA (empty) - OutOfServicePending (Shutdown in progress)
Alarm Reporting	Option to enable alarm reporting of module.	If disabled this will suppress alarms related to this module.
Description	Administratively assigned name for this service module.	0-63 characters.
HW Inventory	Display HW serial no., product no., version (ICS) and type.	
SW Inventory	Display loaded SW versions in respective banks and administratively used bank.	Notice that not all Ethernet service modules have software loaded on the module itself, and hence not an applicable view for all modules.
Config Mode	Select mode 8xFE+SMAP: 8xWAN or 14xWAN ports 2xGE+SMAP: One or none WAN ports	Possible states: - 8xFE+SMAP(8xWAN) - 2xFE+SMAP(14xWAN) - 2xGE+SMAP(1xWAN) - 2xGE(0xWAN)

2.7.3.1 AXX 9200 EDGE/AXX155A

- Define a number of synchronization sources. Parameters per source are:

Table 16 SEC (T0) synchronization - AXX 9200 EDGE/AXX155A - parameters

Parameter	Purpose	Comment
Slot	Identifier of the originating source slot position.	
Port	Identifier of the originating source port position.	
Type	Type of synchronization source. STM-n, E1-port or External Synch-port.	Notice, if desirable to use an E1-port as sync, source, PRA mode is required.
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type.

Parameter	Purpose	Comment
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.
HoldOffTime	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait-to-restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
AdminQuality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SSUT - PRC
Priority	Source priority.	1-5.
OperQuality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC
PortDescription	Displays description assigned the port.	

Parameter	Purpose	Comment
Slot	Identifier of the originating source slot position.	
Port	Identifier of the originating source port position.	
Type	Type of synchronization source. STM-n or Internal Clock	
SSM	Activation of Synchronization Status Messaging.	Only applicable for STM-n type. STM-n port will by default send DoNotUse. Consider this parameter changed to fit your configuration.
Lockout	Set / Clear	Set - This command is used to temporarily exclude a specified synchronization source from the selection process. Clear - This command is used to re-include a previously locked out reference source.
HoldOffTime	SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected sync. reference. After the Hold-Off time the selection process will switch to the error free reference with the highest QL.	Range 300 - 1800 ms.
Wait-to-restore Time	When a nominated synchronization source recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process. WTR timer is configurable in the range 0-12 minutes (one minute step).	The WTR time does not apply to changes in the QL reflected by the received SSM-value (QL-PRC, QL-SSU-T, QL-SSU-L, QL-SEC, QL-DNU).
AdminQuality	Assigned quality for this reference.	Not applicable when SSM is used. Options available: - SEC - SSUL - SSUT - PRC
Priority	Source priority.	1-5.

Parameter	Purpose	Comment
OperQuality	Actual state for the reference.	States: - Failed - DoNotUse - SEC - SSUT - SSUL - PRC
PortDescription	Displays description assigned the port.	

2048 kHz Output (T4) synch - AXX 9200 EDGE/ AXX155A - parameters

:

Parameter	Purpose	Comment
Install	Install state.	Ticked if features license installed.
Feature	Feature description.	Available licenses: - Routing - OSI
Removable	Indicates whether the license can be removed or not.	All features loaded may be removed. This requires a special file downloadable from web.
Location	Indicate the directory on the PC where you have the license file saved and available for installation.	

Table 17 Licenses installed - parameters

Parameter	Purpose	Comment
Type	-48VDC or 230 VAC.	Read only
Alarm Reporting	Enable/disable alarm reporting	Master Alarm per power module
Input A	Enable/disable alarm reporting from input A	
Input B	Enable/disable alarm reporting from input B	

AXX 9200 EDGE Alarm reporting - power modules

Table 18 Alarm reporting - alarm ports

Parameter	Purpose	Comment
Alarm Reporting	Alarm port enable/disable	
Triggered When	Alarm when alarm loop opens/closes	Alarm triggering strategy
Description	Alarm port description	0-63 characters

2.7.3.2 Alarm configuration (severity list)

Table 19 Alarm severity - parameters

Parameter	Purpose	Comment
MoClass	Display object type	
AlarmId	Abbreviation of alarm type	Identified as "ProbCause" in alarm table.
Severity	Set alarm severity	Warning-minor-major-critical
Description	Provide explanatory text for alarm.	Identified as "ProbCauseQ" in alarm table.0-64 characters.

2.7.3.3 Alarm persistency

Alarm persistency defines how long time an alarm has to be stable until the network element will generate an alarm notification, or how long time an alarm situation must have ceased until the network element will generate an alarm cleared notification. Persistency is configured separately for alarm and alarm clear situations by two filters:

Table 20 Alarm persistency - parameters

Parameter	Purpose	Comment
PersistencyCategory	Displays category	Applicable categories: - highorderlevel - unfiltered - loworderlevel
OnFilter	Seconds to wait until an alarm is raised.	0 - 30 seconds.
OffFilter	Seconds to turn off an alarm when cleared.	0 - 30 seconds.

Table 21 Persistency category

Alarm types	Managed objects
LOS	SDH Port, PDH Port
LOF	RS
AIS	MS
EXC,DEG	RS, MS
TIM	RS
RDI	MS
CDF	RS, MS
AUX	Aux Port
LOP	TU4, TU3, TU12
LOM	VC4
LOF-RX, LOF-TX	E1
AIS	TU4, TU3, TU12, E1, E3
EXC, DEG	VC4, VC3, VC12
SSF	VC3, VC12
TIM, RDI, UNEQ, PLM	VC4, VC3, VC12

Alarm thresholds

Some alarms are generated when a performance measurement crosses a predefined threshold. In the Ericsson AXXESSIT network elements this threshold is configurable. Quality measurements on the SDH frames are associated with alarm threshold according to the listing below:

Table 22 Alarm threshold - parameters

Parameter	Purpose	Comment
MoClass	Display object type	
SD Threshold	Threshold for a DEG alarm to be reported.	10E-6 to 10E-9. For example, if set to 10E-7 , an alarm is raised when BER exceeds this threshold. To clear, the BER level must be improved by a factor 10.

Pointer Justification Event (PJE) Alarm Threshold

You can edit the number of PJEs inside a 15min period required to generate a PJE alarm. The number can be from 1 to 1024 events.

2.7.3.4 VC alarms

Table 23 Alarm suppression - VC

Parameter	Purpose	Comment
MoClass	Display object type.	
DegAlarms	Suppress or allow BER-DEG alarms to be reported.	
SsfAlarms	Suppress or allow signal server failure to be reported.	
ExcAlarms	Suppress or allow BER-EXC alarms to be reported.	10E-5 threshold level for the EXC alarms to be reported.
RdiAlarms	Suppress or allow RDI alarms to be reported.	

2.7.3.5 TU/AU alarms

Table 24 Alarm suppression - TU/AU

Parameter	Purpose	Comment
AisAlarms	Suppress or allow AIS alarms to be reported.	

2.7.3.6 E1 alarms

Table 25 Alarm suppression - E1

Parameter	Purpose	Comment
MoClass	Display object type.	
Slot	Identifier of the E1 slot position.	
Port	Identifier of the E1 port position.	
AisAlarms	Suppress or allow AIS alarms to be reported.	

2.7.3.7 AUX alarms

Figure 30 Alarm suppression - AUX

Parameter	Purpose	Comment
RaiAlarms	Suppress or allow RAI alarm to be reported.	Not supported by AXX155E.
AisAlarms	Suppress or allow AIS alarm to be reported.	Not supported by AXX155E.

2.8 IP Unnumbered mode

2.8.1 Introduction

This chapter focuses on using AXX155E, AXX155A and AXX 9200 EDGE in IP un-numbered mode.

The following examples are valid for these NE releases:

- AXX155E R3.0
- AXX155A R2.0
- AXX 9200 EDGE R2.x

In the traditional IP numbered mode, each DCC connection is an IP network, and both ends of the DCC connection have an IP address in that network.

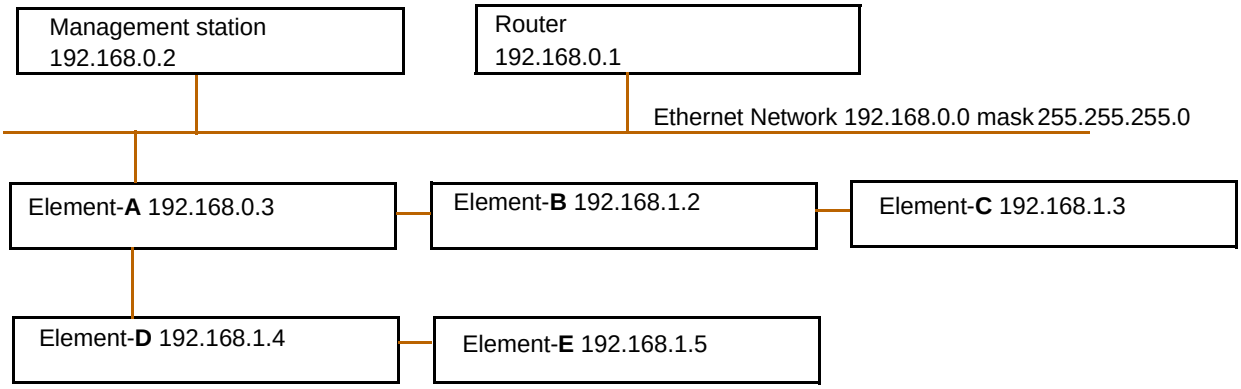
In IP-unnumbered mode, all management interfaces of an element will have the same IP address. The DCC interfaces inherit the address of the management interface. This makes configuration of a set of elements connected via DCC simpler.

Routing between the elements will be taken care of by the OSPF routing protocol, using host routes pointing to the interfaces.

2.8.2 Planning the network

In a typical IP-unnumbered network, one element will be connected with the outside world via the management port. This is the IP unnumbered gateway. The other elements are connected to the first element via DCC channels. As an alternative to DCC channels, it is possible to use LANx ports in layer 1 mode.

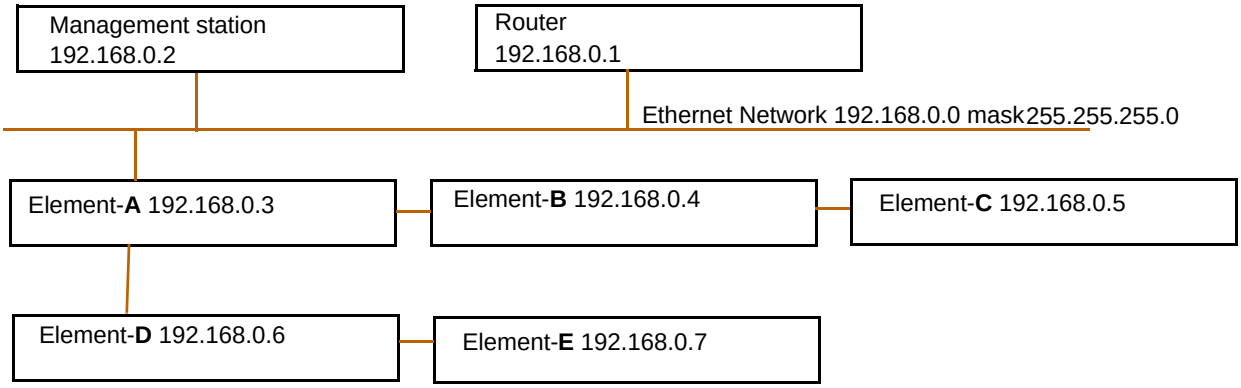
2.8.2.1 Example 1



In this configuration, the network elements, except the gateway element, will have an IP address on a separate network.

The management station and the router will have a static route for all the elements in the 192.168.1.0 network via 192.168.0.3.

2.8.2.2 Example 2



In this example, all elements, including the gateway element, will have addresses on the same network as the other hosts on the Ethernet. The gateway element acts as an ARP proxy. That is, when a host, for instance the router, broadcasts a "who has address 192.168.0.7" on the Ethernet, the gateway element, Element-A, responds on behalf of Element-E. The following IP packets from the router to Element-E is sent to Element-A's hardware address.

2.8.3 Set up the element for IP unnumbered, overview

Procedure: **SET UP THE ELEMENT FOR IP UNNUMBERED**

1. Connect to the element via the serial port
2. Clear the configuration with AXXCLI function **erase cdb** (configuration database), unless the element is a new, not configured element.
3. Set the **system mode** via AXXCLI.

Optionally, set the IP unnumbered gateway to true, if the element is going to be the gateway element.

4. Set an **IP address** via AXXCLI.
5. Add a **user** in the community table
6. **Connect** to the element with the Management Tree
7. Use the Management Tree to configure the **DCC interfaces**
8. Create an **OSPF area**
9. Assign the **OSPF interfaces** to the OSPF area.

Add static route entries (if needed).

Set LeakStaticRoutes (if intended).

Set LeakExternalDirectRoutes (if intended).

10. Enable **OSPF globally** for the element.
11. **Remove** the management port cable.

The above steps are explained more detailed in the following sub-sections.

Connect to the element via the serial port

Connect the elements serial port (marked VT100) to a management station with the supplied serial cable. Use a terminal emulation program to connect to the elements command line interface.

Clear the configuration with AXXCLI.

If the element has been configured in IP numbered mode, the configuration has to be reset.

At least, all OSPF-related entries must be removed, and all static routes, including the default route, must be deleted.

Procedure: **ERASE CDB**

1. Enter the AXXCLI menu
2. Enter the **erase cdb** command.

The element will now restart.

Setting the system mode.

When the element is unconfigured or the element has been cleared with the function "erase cdb", it initially is in IP numbered mode. Changing the system mode to IP unnumbered is done via the command line interface.

2.8.3.1 Optionally set gateway enable.

If the element is the gateway element, consider setting the gateway enable to true. The effect of this variable is to create a route for the local network on the management port, and to leak this route via OSPF to the other ip unnumbered elements. Also, it ensures that static routes to gateways on the Ethernet are pointed to the correct interface.

This provides connectivity from all IP unnumbered elements in to any host on the Ethernet, see “Example 1” on page 52 or “Example 2” on page 52 configurations.

See also “Using the LeakDirectExternalRoutes variable.” on page 59.

Set an IP address via AXXCLI

Use the AXXCLI to set an IP address. If this is the gateway element, a default gateway can also be set. If this is not the gateway element, a default route need not be set, as the proper routes will be configured by OSPF.

Add a user in the community table

Use the command line interface to add a line in the community table. In the AXX 9200 EDGE, the community table is found in the "Community table" menu directly below AXXCLI.

Enter this command:

add manager=0.0.0.0 community=public access=super traps=disable

Connect to the element with the Management Tree

The network element must now be connected to a management station running the Management Tree using the management port. The easiest way is to use a straight unshielded twisted pair cable with RJ45 connectors in each end, and connect it directly between the element and the management station.

Configure the management station's interface to have a static IP address in the same network as the element. For instance, if the elements IP address is 192.168.1.5 and the netmask is 255.255.255.0, select for example address 192.168.1.100 for the management station (select an unused address).

Alternatively, if example 2 configuration is used, the element can be temporarily connected to the Ethernet with a cable from the management port to the switch representing the Ethernet. If this method is chosen, special care must be taken when the cable is removed after the configuration is complete. At this time, the IP traffic that till now have used the management port, is supposed to continue using the gateway element's management port.

But the other hosts, like the management station in the example and the router, will continue to send to the mac-address of the management port, now unsuccessfully.

Therefore the ARP-tables of the management station and the router have to be manually deleted.

After that, the gateway element will answer the ARP requests for the elements, and communication can continue. The ARP command is for instance **arp -d 192.168.0.5** in MS Windows and the same in Solaris.

Alternatively, if a configuration like example 1 is used, the management port of the element can be connected to the Ethernet, then the management stations interface is changed to an unused address in the same IP network as the element.

2.8.3.2 Example

The element to be configured is 192.168.1.3, it's management port is connected to the switch representing the Ethernet. The management stations IP address is changed to 192.168.1.100.

Now we are running two IP-networks on the same Ethernet. There will be no connectivity to the router when this is going on, and the ARP table on the management station will be reset when it's IP address is changed back to the normal, 192.168.0.2, so there will be no problems with ARP tables in this case.

If the element to be configured is the gateway element (Element-A in both examples), the management port is supposed to be connected permanently, and connectivity should be ensured with no special arrangements.

Configure the DCC interfaces

Use the Management Tree to configure the DCC interfaces (alternatively, the DCC interfaces can be configured in AXXCLI).

- Find the SDH port you are going to use
- Find rs
- Find dccR
- Set the variable **Mode** to **ipOverDcc**.
- The IpEncapsulation should be set to ppp/crc32, which is the default for AXX 9200 EDGE R 2.0.

Alternatively, find the dccM interface under ms under rs, and set Mode to ipOverDcc.

The DCC interfaces are also available in table form in **ManagementInterfaces**, DCC.

Unless the optical cables are connected to the SDH ports, and the DCC interfaces at the other ends are configured accordingly, the DCC interfaces will have OperStatus "down". This is ok for the moment, but the interfaces will have to be brought "up" for the OSPF interface configuration in a later step.

Create an OSPF area

In the Management Tree,

- Find ManagementInterfaces
- Then DCNRouter
- Then OSPF
- Then AreaOSPF. In this table, add a row, accept all the default entries
- Then save. This will create an area with id 0.0.0.0.

Assign the OSPF interfaces to the OSPF area

The OSPF interfaces for the DCC channels will automatically be created when the DCC channels are in "up" operational status. At this point, it is therefore necessary to connect the optical cables, where the DCC channels of the other ends of the cables are configured accordingly.

If this is not practical, it is possible to temporarily interconnect two ports on the same element, configuring the DCC channels of each port. The DCC interface will then reach "up" OperStatus, and the OSPF interfaces are visible in the AreaInterface table.

In the Management Tree,

- find **managementInterfaces**,
- then DCNRouter
- then OSPF
- then **AreaInterface**. For each of the interfaces, select the area to which the interface attaches, 0.0.0.0 in our example.

A third possibility is to skip this step entirely, deploy the element to its final location, connect the cables and restart the element. When the element is restarted and the DCC interfaces have **OperStatus** up, the startup procedure will assign each OSPF-interface to the first area it finds. If this method is used, it is still necessary to enable OSPF globally for the element (see “Enable OSPF globally for the element.” on page 58).

Set LeakStaticRoutes

If this is the gateway element (Element-A in the examples), the variable **LeakStaticRoutes** should be set to **true**. The default route, or any other static routes set in the element will then be announced to all the other elements in the IP unnumbered network, enabling connectivity outside the network. If this is not the gateway element, this variable should normally be set to **false**.

Enable OSPF globally for the element.

In the Management Tree,

- find managementInterfaces
- then DCNRouter
- then OSPF
- Change variable AdminStatus to "enabled".

Remove the management port cable.

Unless this is the gateway element, remove the management cable.

If a separate IP network was used, as in example 1, the hosts on the Ethernet should have a route to the elements via the gateway element.

Example, MS Windows

route add 192.168.1.0 mask 255.255.255.0 192.168.0.3

Example, Solaris:

route add -net 192.168.1.0/24 192.168.0.3

Delete ARP entries in the management station or the router, if appropriate, see “Connect to the element with the Management Tree” on page 55.

Verify connectivity

It should now be possible to ping the element from anywhere, and to connect AXX 9840 INSITE to the element.

All the elements should now have a route to the new element, see managementInterfaces, DCNRouter, RoutingTable.

The gateway element Element-A, should now answer ARP requests for the new element, see

Element-A's **ArpProxy** table found under management interfaces, DCNRouter.

Using the LeakDirectExternalRoutes variable.

Consider one of the example networks. If a management station is connected to any element in the network, for example Element-E, and the management station's IP-address is configured with a compatible IP address, connectivity to the first element is enabled.

If, in addition, the LeakDirectStaticRoutes in Element-E is set to "enabled", the direct route to the workstation is announced through OSPF to the other elements in the network, enabling connectivity between the directly connected workstation and all the elements in the IP unnumbered network.

A direct static route is created when the element receives an ARP-request on the management port.

Connectivity without OSPF

For the first elements behind the IP-unnumbered gateway, Element-B and Element-D in the above examples, OSPF is strictly not necessary to enable connectivity. A simple routing protocol called IPCP (IP Control Protocol) that works over PPP, will ensure connectivity to neighbouring elements. The router or the management station in the examples will be able to connect to Element-B and Element-D without OSPF, but a static route in Element-B and Element-D is necessary.

Consider also a situation with many CPE (Customer Premises Equipment) elements connected to one node at the edge of the network. OSPF can be turned off on each of the CPE elements, the neighbour has LeakDirectExternalRoutes turned on. This will reduce the number of nodes running OSPF, and therefore also the OSPF traffic.

Changing the IP address

To change the IP address of an element, the global OSPF must first be turned off using the Management Tree, variable AdminStatus in OSPF. After that, the IP address has to be changed via AXXCLI using the serial cable. Alternatively, the IP address could be changed via the Management Tree, if routes are in place to cover both addresses. After that, AXX 9840 INSITE has to be reconnected using the new address.

2.8.4 IMPORTANT - System mode from IP to IP un-numbered

Products affected

The IP un-numbered feature was introduced in AXX 9200 EDGE Network Release (NR) 2.0. This field notice will apply for this and future releases.

Problem description

Changing system mode from IP (default) to IP un-numbered may imply problems.

Problem symptoms

Experiences from field (labs) tell us that current implementation have limitations in software for changing system mode from IP (default) to IP un-numbered.

Even though there are IP addresses and routing protocols configured on NE the operator does not receive any notification, which could have prevented the change until necessary configuration changes have been maintained.

From a software design point-of-view, the configuration of system mode for DCN routing is seen as a strategically choice, which the operator should configure prior to configure IP address and protocols on the device.

The reason for this is because the network design is different for each of the system modes.

The consequence for changing the system mode from IP to IP un-numbered is complicated and you may experience severe problems. Worst-case scenario is not being able to re-obtain IP connectivity to NE.

Workaround

Generally the safest alternative is to erase the configuration prior to change the system mode. We are aware that this is an unpopular alternative, and have performed some testing to find a more proper workaround.

NOTE! The following guidelines can not guarantee successful change from IP to IP un-numbered System mode. It is

recommended that the configuration is tested on NEs in lab prior to performing the changes in a live environment.

Till now we have tested some different configurations, and the following steps were successful:

Procedure: **SYSTEM MODE FROM IP TO IP UN-NUMBERED**

1. **Locally connect to MNGT-port** and connect with **AXX 9820 CRAFT**.
2. **Remove all IP addresses** in the IP interface table **except** for the MNGT-port address (IF=1000).
3. **Remove** all static configured **routes** (even the 0.0.0.0 route).
4. **Disable** active **routing protocols** (RIP and/or OSPF).
5. **Locally** connect to device **via CLI** (VT100).
6. Remove **IP address assigned to management port** (AXXCLI>ip ip=0.0.0.0 sub=0.0.0.0).
7. **Set** system **mode** to IP unnumbered (**IPUN**) and **reset** the device.
8. **Change** the **IP address** (MNGT-port) to fit your new network design and **re-configure** the **SNMP community**.
9. **Re-connect** to device with AXX 9820 CRAFT.
10. **Commission IP un-numbered configuration**. IP over PPP (DCC), OSPF, etc.

2.9 DCN routing and networking (IP Unnumbered)

2.9.1 Introduction

This section briefly explains the components of the DCN IPUN router. Furthermore, it is shown some examples how to set up Ericsson AXXESSIT nodes for DCN routing and networking in an IP unnumbered topology.

By illustrating some basic network topologies with related configurations, the reader should hopefully be able to build more complex network topologies for a particular purpose. It is assumed that the reader is familiar with basic IP networking concepts and terminology.

It should be emphasized that the basic intention with the DCN network is to provide management connectivity to the Ericsson AXXESSIT nodes in the network topology.

The DCN traffic is encapsulated in IP frames transported to the router nodes through two types of media:

- The management port (Ethernet 10/100 Mbps). This port is always available at the NE, and can be connected directly to a DCN management LAN, alternatively through a switch or IP router.
- SDH DCC channels. These are point to point channels (DCC/L1CC) terminated at adjacent SDH nodes and with bandwidth 576/192 kbps respectively. On these PTP channels, the IP datagrams are encapsulated in PPP framing running over HDLC/DCC or L1CC.

An IP packet arriving at a node is either terminated locally (if the packet is destined for the node) or routed to another router node (nexthop), reachable over one of the PTP (DCC/L1CC) channels or the management port.

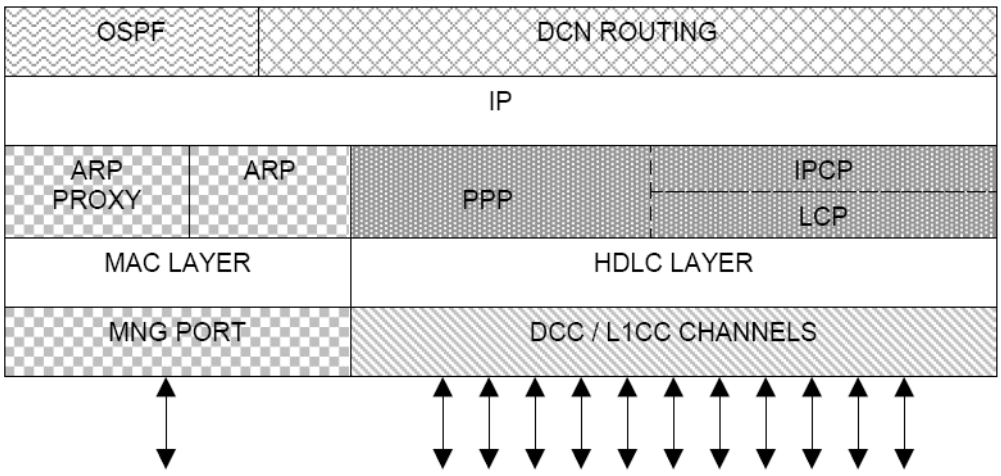


Figure 31 DCN router - main components

The main components of the DCN router is illustrated in Figure 31 The main components are described in the following subsections.

List of abbreviations used in this section

Table 26 List of abbreviations

Abbreviation	Description
ABR	Area Border Router
ARP	Address Resolution Protocol
AS	Autonomous System
ASBR	Autonomous System Border Router
BBA	BackBone Area
BDR	Backup Designated Router
DCC	Digital Communication Channel
DCN	Digital Communication Network
DR	Designated Router
IPCP	IP Control Protocol
IPUN	IP UnNumbered
LCP	Link Control Protocol
LSA	Link State Advertisement
LSDB	Link State Data Base
NH	NextHop
NE	Network Element
OSPF	Open Shortest Path First
RO	Read Only
RW	Read Write
SR	Static Route
PPP	Point to Point Protocol
PTP	Point To Point

2.9.2 Supported functionality

Here is a brief description of some of the functionality supported by the DCN router. Having this in mind, you should be able to follow the examples/scenarios described throughout this section.

2.9.2.1 IP unnumbered

The proprietary DCN router is based on the IP unnumbered concept. This implies that there is only one IP address to be configured per node. The nodes IP address applies to the management port, but is also adopted by all PTP channels (unnumbered links). Hence, IP configuration is simpler and IP address space is saved.

2.9.2.2 PPP

On the PTP channels (DCCR/DCCM), the DCN router runs the PPP (Point To Point Protocol). PPP is encapsulated in HDLC framing with configurable checksum, either CRC32 or CRC16. CRC32 is default. PPP must be enabled for all PTP channels intended for transport of DCN traffic.

2.9.2.3 IPCP

On the PTP channels, the IPCP (Internet Protocol Control Protocol) runs on top of PPP. Through IPCP, the DCN router learns the IP (unnumbered) addresses of its adjacent neighbours (also denoted as peer IP addresses). This information (together with the corresponding channel metric) applies to selection of interfaces to the NH routers. The IPCP information is also relevant to the advertisement (leaking) of routes into OSPF.

2.9.2.4 OSPF

OSPF (Open Shortest Path First) is a routing protocol running directly on IP. Via OSPF, the DCN routers exchange link state information which is distributed (flooded) throughout the OSPF domain. This link state information contributes when the DCN router builds its routing table.

2.9.2.5 ARP

The ARP (Address Resolution Protocol) applies to broadcast media, i.e. the DCN routers management port. ARP matches higher-level IP addresses to the physical addresses of the destination hosts. ARP uses a lookup table (called ARP cache) to perform the translation. When the address is not found in the ARP cache, a broadcast is sent out on the network with a special format called the ARP request. If one of the machines on the network recognizes its own IP address in the request, it sends an ARP reply back to the requesting host. The reply contains the physical hardware address of the receiving host. The requesting host stores this address in its ARP cache so that all subsequent datagrams (packets) to this destination IP address can be translated to a physical address.

2.9.2.6 PROXY ARP

Proxy ARP enables one LAN connected AXX node to respond to ARP requests on behalf of SDH nodes not connected to the LAN. For this to occur, the DCC connected SDH nodes must reside on the same subnet as the LAN connected node. When a LAN host sends an ARP request to a node that is not connected to the LAN, the proxy node returns its own MAC address to the host. The host then sends the IP datagram for the destination node to the MAC address of the proxy node, which in turn routes the datagram according to its routing table. Proxy ARP is always enabled and does not require any user configuration.

2.9.3 DCN network topology examples

2.9.3.1 IP Subnet Gateway

A DCN IP network may consist of a management LAN and several SDH nodes. The following figure shows a network where all router nodes reside in the same IP subnet.

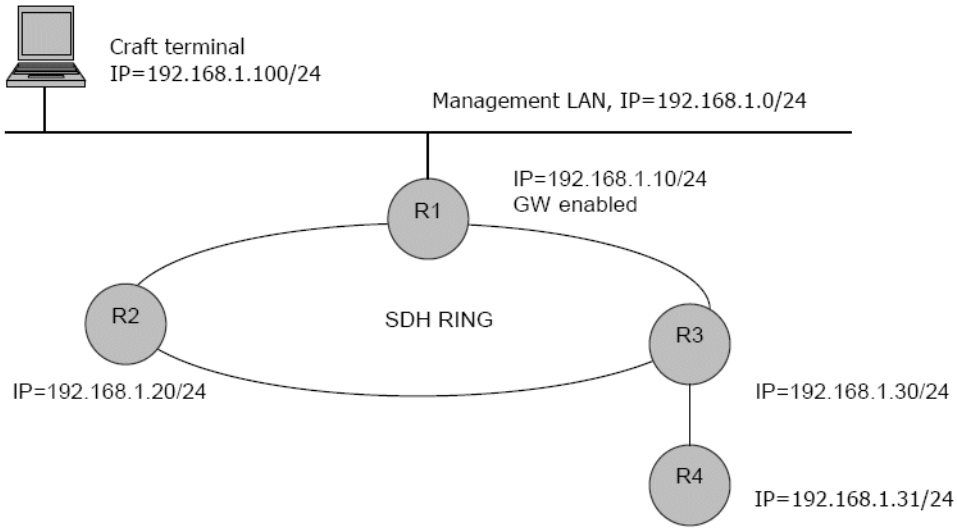


Figure 32 IP Subnet gateway - example

In this network, only a few IP addresses are used by the router nodes. All unresolved IP addresses within the DCN subnet are assigned to the default gateway interface (reachable via R1s management port).

- How do we get connectivity from the craft terminal to the nodes in this subnet?

One solution is to add static routes at all router nodes. In simple networks, this may be a satisfactory solution. But as the network grows, it will be cumbersome to maintain the routing tables in all the nodes. A more automatic and flexible solution is to let OSPF distribute the information needed to build the routing tables. For this network, we have to set up the following configurations at the router nodes.

- The PTP (DCC) interfaces of R1, R2, R3 and R4 must be configured for OSPF (see section § 3.3).
- R1 must be enabled as gateway for the IP subnet.

- How does it work?

Through OSPF, the DCN routers exchange the necessary information needed by each router to build its routing table. OSPF is also needed for R1 to tell the other nodes that it acts as a default gateway node for the IP subnet. Finally, as R1 also learns how to reach R2, R3 and R4 it will operate as proxy ARP for them at the management LAN (since they are all within the same subnet as R1).

2.9.3.2 Volatile Host Routes

Look at Figure 32 We now want temporary to connect another management terminal to the management port of R4. As R1 and R4 are on the same IP subnet, they cannot both be configured as IP subnet gateway. Hence, R4 must be configured for GW disabled, which implies that all unknown subnet destinations are still routed to R1. The situation is illustrated below.

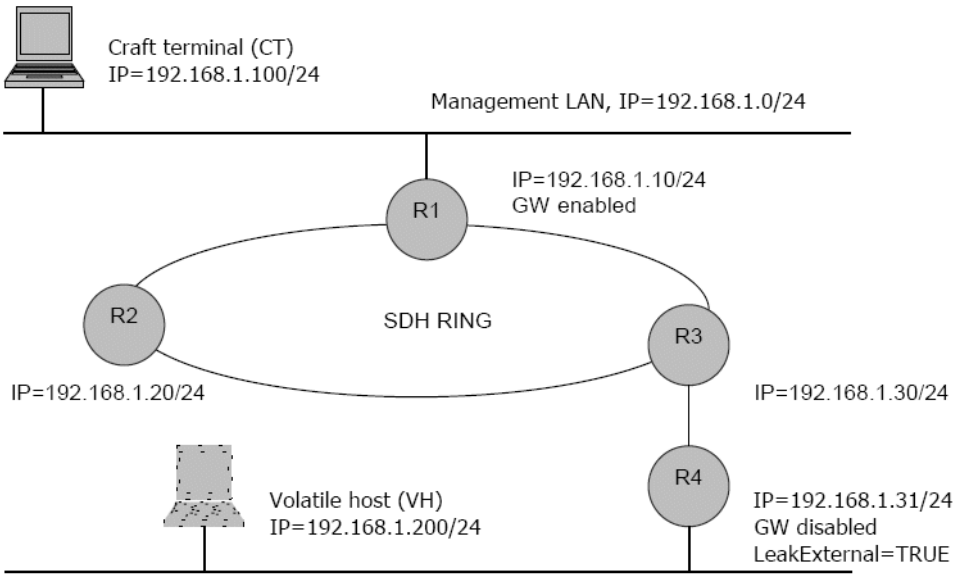


Figure 33 Volatile Host Routes - example

- So, how do we obtain connectivity from the volatile host to the router nodes?

We start with R4. The clue here is ARP. When the host tries to reach R4, it will issue an ARP request at R4s management port. This ARP request reveals the host (as the ARP request contains VHs IP address). R4 now knows that the host is locally connected and adds a route to it. Hence, all IP packets to the host is now routed to R4s management port, and not to the subnet gateway at R1.

- But what about connectivity to the other nodes?

If the host tries to reach one of the other router nodes (R1, R2, R3), it will again issue an ARP request at R4s management port. As R4 will be ARP proxy on behalf of the other nodes, an ARP reply is returned from R4 with is own MAC address. The host continues by sending the IP packet to R4, which in turn routes the packet correctly to the destination node. But what about the opposite direction (from R1, R2, R3 back to the host)? As R1, R2 and R3 have no specific route to the host, these will route the reply packets onto the subnet gateway.

So how do we getR1, R2 and R3 to know that the host is at R4? The clue is leaking of external direct routes into OSPF. By enabling R4 to leak the host route to the other routers, they will know that the host is now reachable via R4, and not at the subnet gateway.

Comments:

- If there have not been exchanged any IP traffic with the host for some time (5-10 minutes), R4 will delete the host from its ARP table, and the host route will be flushed from the OSPF domain as well.
- If you cannot obtain connectivity from the host, a possible reason may be that the host does not issue any ARP request (as it already has R4 in its ARP cache). In such cases, flushing the hosts ARP table will have immediate effect. This should always be done if you have changed from GW enabled

2.9.3.3 Multiple management ports connected to the same DCN management LAN

The following example shows a topology where multiple DCN routers are physically connected to the same DCN management

LAN. This network can be considered as “parallel” DCN networks terminated into the same LAN.

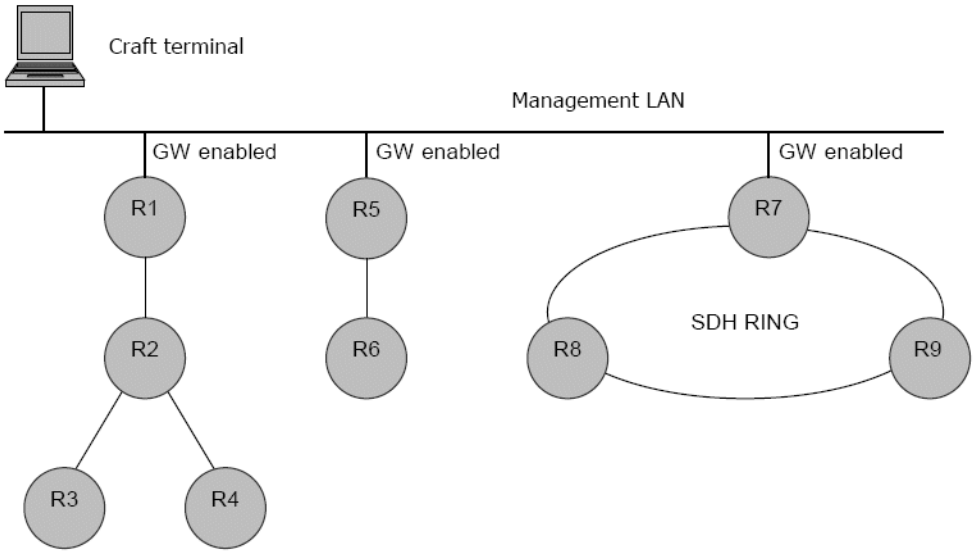


Figure 34 Management ports connected to the same DCN management LAN

In this network, R1, R5 and R7 are obviously part of the same IP subnet. These routers are also enabled as IP gateways for their corresponding PTP networks. All router PTP interfaces are enabled for OSPF.

In the following, we assume that the other routers also belong to the same IP subnet (for simplicity, although this is not required).

As the gateway routers operate as ARP proxies for their corresponding PTP topology, it is important that the PTP topologies are separated from each other. This means, that it is NOT allowed to open a DCN link for routing between for instance node R2 and R6. This has to be provided by the network operator in order to avoid routers at the management LAN who compete about being ARP proxy for the network.

Comments:

- Although DCN routing has to be avoided between “parallel” DCN topologies, other SDH (user) traffic can of course be passed through. The operator must only remember to keep the PPP links in the disabled mode.

2.9.3.4 Router nodes at different IP subnets

In IP unnumbered, having router nodes at different IP subnets is quite normal. The subnets must be separated from each other via

PTP links. The following figure illustrates two IP subnets, with addresses 192.168.1.0/24 and 192.168.2.0/24 respectively. Both have separate management LANs as indicated.

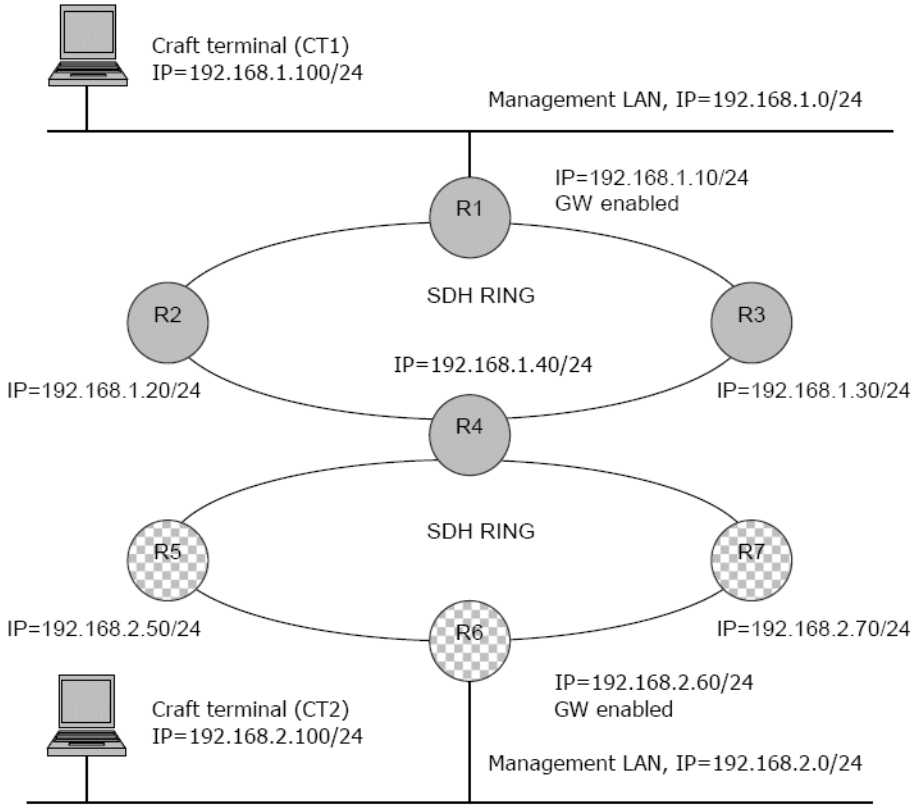


Figure 35 Router nodes at different IP subnets

- How do we obtain connectivity from the craft terminals to the nodes in this DCN network?

We start by enabling OSPF at the routers PTP interfaces (see section § 3.3). Additionally, we configure R1 and R6 as IP subnet gateways. Via OSPF, the DCN routers will now learn how to reach the other router nodes (in both subnets). Additionally, all router nodes will know how to reach the 192.168.1.0/24 subnet at R1 and the 192.168.2.0/24 subnet at R6.

However, the craft terminals (CT1 and CT2) does not know how to reach anything else than its local subnet. So, we have to add a static route at CT1 to the 192.168.2.0/24 subnet with R1 as nexthop. Likewise, we must add a static route at CT2 to the 192.168.1.0/24 subnet with R6 as nexthop.

Comments:

- Although not intended (from a DCN networking point of view), this DCN network will also provide IP connectivity between CT1 and CT2. (That is, CT1 and CT2 will both be able to “PING” each

2.9.3.5 Using Static routes in an IP unnumbered topology

Although we enable OSPF in the DCN network, there are still cases where we have to supplement with static route entries in one or more of the nodes in order to reach external networks. Consider the following network topology.

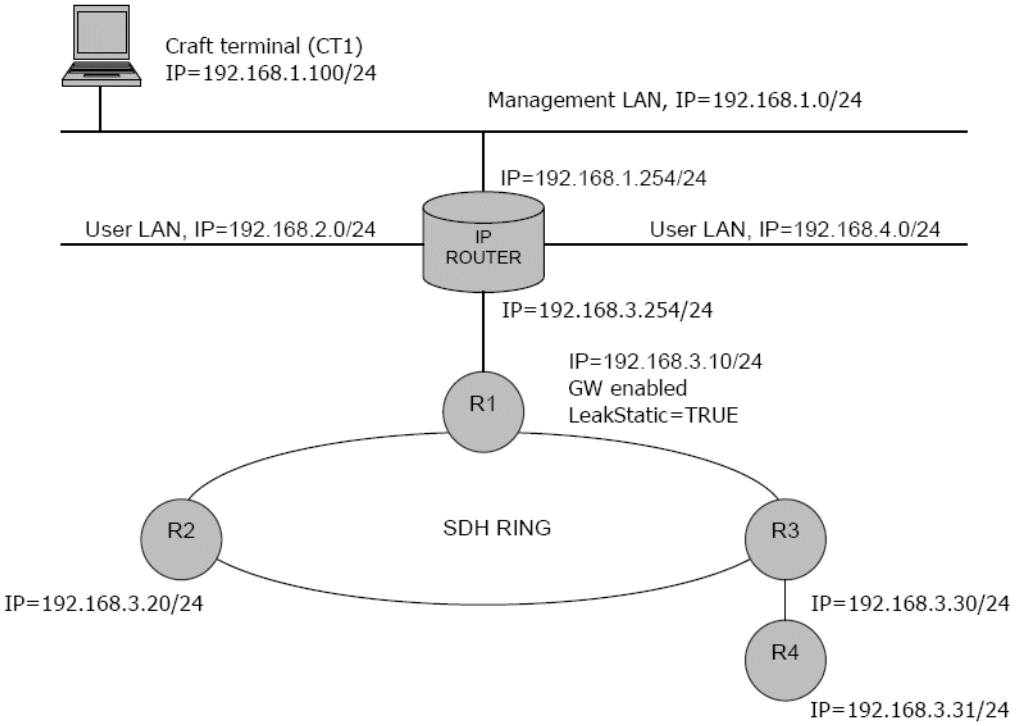


Figure 36 Using Static routes in an IP unnumbered topology - example

The DCN network (IP=192.168.3.0/224) is connected to the management LAN through an IP router with multiple Ethernet LAN interfaces. The other LANs connected to the IP router can serve traffic which is (more or less) separated from the DCN network.

- What do we have to do here to obtain connectivity from the management LAN to the DCN network?

We start again by enabling OSPF at the DCN routers PTP interfaces (see section “DCN router configuration and monitoring” on page 72) and enables R1 as IP subnet gateway. The DCN routers will now learn how to reach the other router nodes and the subnet gateway (IP=192.168.3.0/24) at R1.

However, the DCN routers still don't know how to reach the management LAN at address 192.168.1.0/24. In order to tell them, we add a static route at R1 to IP=192.168.1.0/24 with nexthop IP=192.168.3.254.

This tells R1 how to reach the management LAN. But what about the other DCN nodes? They must also be told how to reach the management LAN. The clue is again OSPF, this time we must allow R1 to leak the static route to the other nodes. This is done by configuring R1 for leaking of static routes into OSPF.

Finally, we have to configure a static route at CT1 to the DCN subnet at IP=192.168.3.0/24 with nexthop IP=192.168.1.254. If we don't, CT1 will not know how to reach the DCN network.

Another (somewhat rare) example where static routes are required, is shown in the following figure.

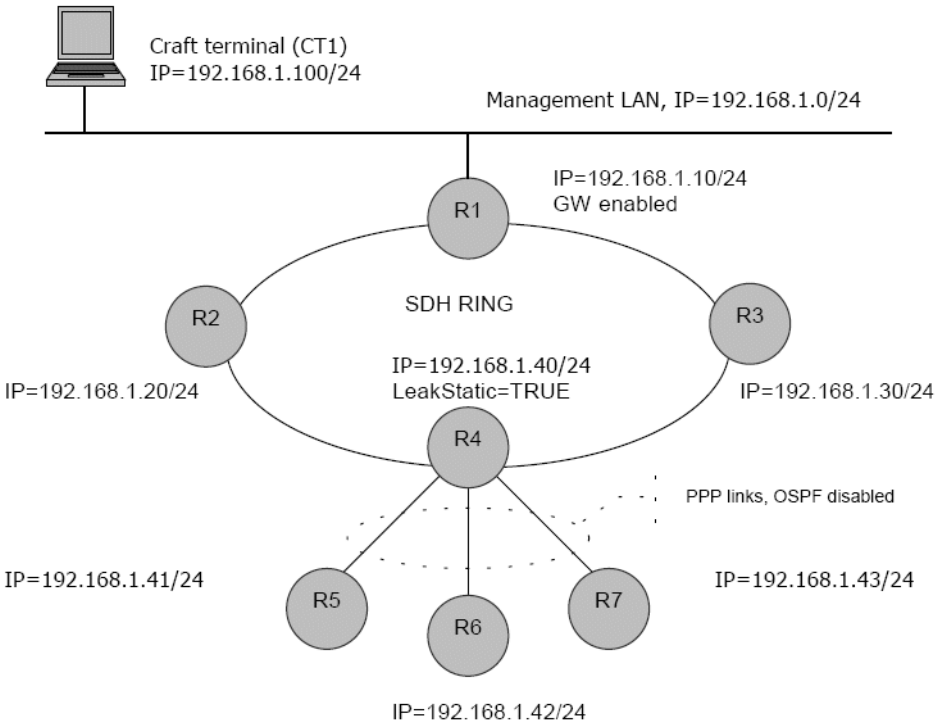


Figure 37 Static routes - example #2

The DCN routers reside in the same IP subnet. The PPP links part of the SDH ring are enabled for OSPF. However, the PPP links from R4 to R5, R6 and R7 does not support OSPF (of some reason).

- In order to obtain connectivity from CT1 to all the router nodes, we have to do the following.

Enable OSPF at the DCN routers PTP interfaces (see section § 3.3) except for those from R4 to R5, R6 and R7. Enable R1 as IP subnet gateway. The DCN routers R1, R2, R3 and R4 will now learn how to reach each other and the subnet gateway (IP=192.168.1.0/24) at R1.

However, we still have no connectivity to R5, R6, and R7. In order to reach them, we have to leak routes to them into the OSPF domain. These routes have to be added as static routes in R4 as follows:

Destination IP=192.168.1.41/32, nexthop IP=192.168.1.41
Destination IP=192.168.1.42/32, nexthop IP=192.168.1.42
Destination IP=192.168.1.43/32, nexthop IP=192.168.1.43

Although these routes seems strange and useless (as R4 already knows the routes to R5, R6 and R7 via IPCP), this is the way to get them advertised into the OSPF domain. Consequently, R4 also has to be enabled for leaking of static routes into OSPF.

Finally, R5, R6 and R7 all have to add a static route to the DCN subnet via R4 as follows:

Destination IP=192.168.1.0/24, nexthop IP=192.168.1.40

Comments:

- One should expect that R4 would leak the routes to R5, R6 and R7 provided that IPCP is UP and R4 is enabled for leaking of external directly connected routes. However, LeakExternalDirect=TRUE applies to host routes at the management port only.

2.9.4 DCN router configuration and monitoring

This subsection describes the user interface of the DCN router, regarding configuration and monitorable parameters and data. The user interface of the DCN router is presented as a separate folder which resides under the item “ManagementInterfaces” in the management tree.

NOTE! To make the DCN router folder appear in the GUI, the device must first be configured for system mode “IP unnumbered”. This selection is only available through the local terminal interface (CLI/AXXCLI).

Warning!

Selection of system mode “IP” or “IP unnumbered” shall be done as the very first DCN configuration. If you change system mode after having performed other DCN related configurations, these get lost and the behaviour is unpredictable. Do NOT change system mode remotely (via Telnet) as you will lose connectivity to the device!

2.9.4.1 The user interface for the DCN router

The user interface is divided in the following sections:

ARP TABLE

This table contains the current ARP entries (ARP cache) used by the router. The table applies to translation between IP addresses and physical (MAC) addresses when IP packets are sent to the management port.

ARP PROXY TABLE

This table contains the IP addresses for which the router is a proxy on the management port. The IP addresses seen in the ARP proxy table are IP addresses reachable via the PTP (DCC) links.

IPUNNUMBEREDGW

This parameter configures whether or not the routers management port shall operate as a subnet gateway. The role of the subnet gateway router is explained in previous sections.

ROUTING TABLE

This table contains the route table currently used for routing of DCN IP packets. Each route entry has the following attributes:

- Destination IP address
- Destination IP mask
- Nexthop router IP address
- Outgoing interface index
- RouteType
- Protocol How the route is learnt
- NexthopAS ASBR router id. (OSPF routes only)

- Metric OSPF metric
- TOS Type of service (always 0)

In this screen, the operator is free to add static routes to the DCN router. It is sufficient to specify the

destination IP address and mask together with the IP address of the nexthop router. Static routes (added by the network manager) appear with RouteType=Remote and Protocol=netmgmt.

OSPF

Regarding OSPF configuration, it is assumed that the operator has some knowledge about OSPF.

Furthermore, it is assumed that the operator has decided the OSPF network with respect to routers, areas and interfaces.

NOTE! OSPF routing on the MNGT-port is only supported when node operates as IPUN GW. Enabling OSPF routing on MNGT-port will only be successful for NE's configured as IP unnumbered gateway. This is a limitation in IP unnumbered router design. Workaround; Enable IPUN gateway. Be aware that several IPUN gateways in one IP segment may cause suboptimal routing. Consider assigning unique IP segments to each IP unnumbered router in the topology. This will provide an expandable network configuration.

AdminStatus

This parameter configures whether the router shall enable OSPF in general. It can be considered as the “main switch” for turning OSPF on or off.

AreaOSPF

This is where to create the OSPF areas wherein the router shall participate. You simply “add” an area, specify its area identifier and “save”. All areas will be created as regular (non-stub) areas by setting ImportAsExternal=”true”.

Comments:

OSPF areas must be created before interfaces can be configured, as these have to be attached to a legal area. If you have a small router topology (less than 30-40 router nodes), it should suffice with one area (backbone). Also remember that an IP subnet must reside within one and only one area.

AreaInterface

This is where to configure the routers OSPF interfaces. The following parameters are configurable:

AreaId
The OSPF area wherein the interface shall be attached.

AdminStatus
Whether or not the interface shall be enabled for OSPF.

RouterPriority
Applies to DR/BDR election. Only relevant for the management interface.

RouterDeadInterval
Time before the neighbour router is declared in-operational.

HelloInterval
Time between Hello packets are sent out on the interface.

TransitDelay
The transit delay for LSAs to reach the neighbours.

RetransmitInterval
Time before re-transmitting unacknowledged LSAs

It is recommended to leave most values at their default values (as most OSPF routers use default settings). It should not be necessary to change anything else than the AreaId, AdminStatus and perhaps the RouterPriority.

Interfaces to be configured must be brought into operational status UP. For the PTP interfaces, this means that PPP must be up (I.e. DCC must be configured to IpPpppCrc16/IpPppCrc32 and the optical fibre must be physically connected). In order to change the interface parameters, AdminStatus of the interface must first be set to “disabled”. When the interface parameters are properly set, AdminStatus can be set to “enabled”.

Comments:

By default, all PTP interfaces have their AdminStatus=“enabled”, whilst the management port has AdminStatus=”disabled”. When an interface comes up (and there exist a configuration setting for the interface), it will be attached to the area to which it is configured. However, if there does not exist any interface configuration, the interface will be attached to the lowest existing area (if any). Hence, if you intend to have all PTP interfaces enabled for the same area, you can simply create the area and skip the interface configuration.

However, it should be good practice to configure the interfaces individually and attach them to their intended areas.

In addition to the configurable parameters listed above, an OSPF interface entry has the following readonly attributes:

IfIndex
The interface index of the OSPF interface

IpAddress
The IP address of the OSPF interface. In IPUN, this is equal for all interfaces.

IfType
PointToPoint or Broadcast Refer to RFC 2328 § 9

IfState
Down/Waiting/PointToPoint/BR/BDR/DROther. Refer to RFC 2328 § 9.1

OspfEvents
OSPF interface state changes Refer to RFC 2328 § 9.3

DR
The router id. of the designated router (Broadcast networks only)

BackupDR
The router id. of the backup DR (Broadcast networks only)

LeakExternalDirectRoutes
This parameter configures whether or not the router shall leak routes related to “volatile hosts” into the OSPF domain.
Leaking of such routes is explained in more details in a previous section.

LeakStaticRoutes
This parameter configures whether or not the router shall leak its static routes into the OSPF domain.Leaking of such routes is explained in more details in a previous section.

2.9.5 Device Restart requirements

If you have performed any of the actions listed below, make sure to restart (reboot) the device when you have completed your DCN configurations. This has to be done in order to take the configurations properly into effect:

- Changed the OSPF administrative state
- Created or deleted an OSPF area
- Configured or reconfigured any of the OSPF interfaces

3 Using AXX 9840 INSITE

3.1 Introduction

This chapter presents the AXX 9840 INSITE desktop with its tools, menu items, views and general editing functions.

The AXX 9840 INSITE desktop is built on the AXX 9800 TMN Graphical User Interface framework, consisting of the Management Tree, Attributes Viewer, Notification List and the Map Viewer.

3.2 AXX 9840 INSITE desktop

The Management Tree is a topology browser and presents all Network Elements (NEs) in the managed network and management system. Attributes show values of a specific managed object. The Notification List presents all notifications in AXX 9840 INSITE. The Map Viewer is a graphical presentation of network elements and their managed objects. Statusbar displays a description of the selected item on desktop.

The Management centre map has short-cuts to main views and functions.

.

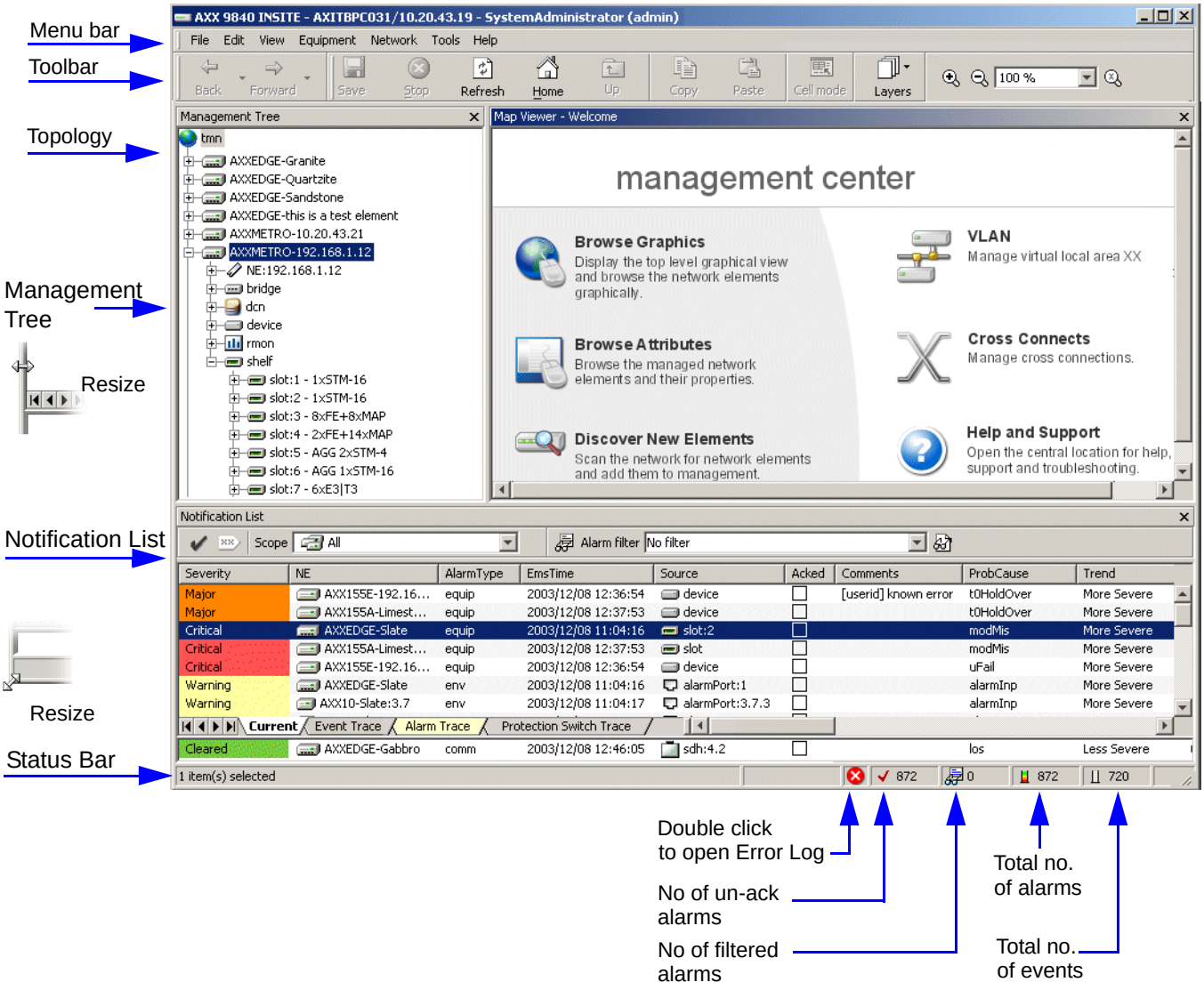


Figure 38 AXX 9840 INSITE Desktop

3.2.1 Toolbar navigation

You can at any time rearrange the given layout of the Toolbar. Your dedicated Toolbar will have the same layout regardless of the logon location.

3.2.1.1 Toolbar buttons

Name	Icon	Description
Back/ Forward		Navigate in Topology - back or forward in navigation history (only to main view; attributes and maps)
Stop		Stop the current operation
Refresh		Refresh the active view
Home		Return to root node from current view
Up		Move up one level in Management Tree
Paste		Paste content current on the clipboard. See “Copy and paste” on page 88
Cell mode		By default, entire rows are selected in table, but single cells can easily be selected using the cell-mode toggle button
Copy		Copy selected item(s) to the clipboard. See “Copy and paste” on page 88
Save		Save
Add		Add new row
Delete		Delete selected item(s)
Views		Selected view (default) or viewing Children See page 3-93

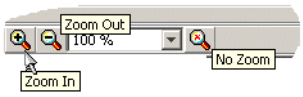
Name	Icon	Description
Layers		See Map Viewer
Zoom		See Map Viewer

Table 27 Toolbar buttons

3.2.1.2 Lock Toolbars

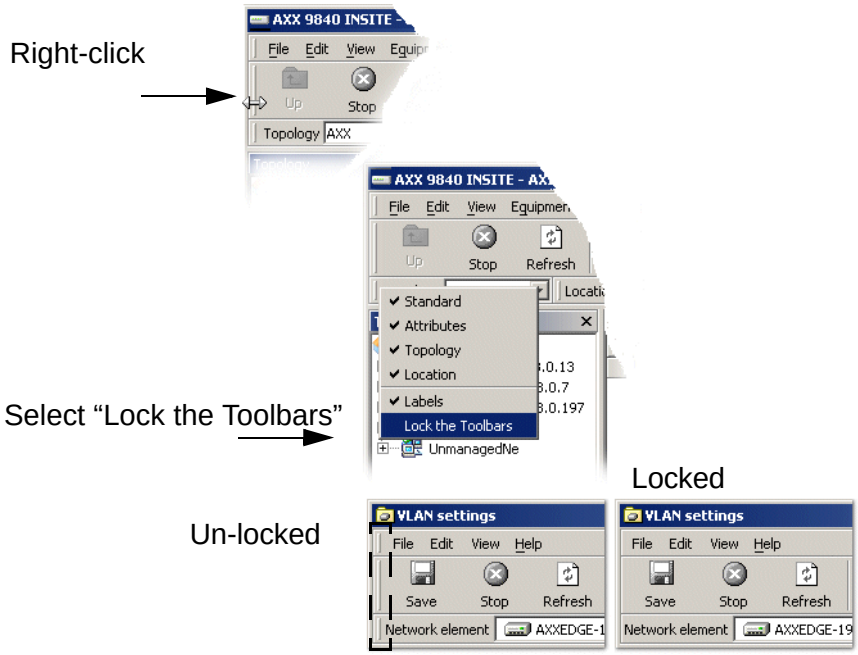


Figure 39 Lock Toolbar - overview

3.2.1.3 Move Toolbars

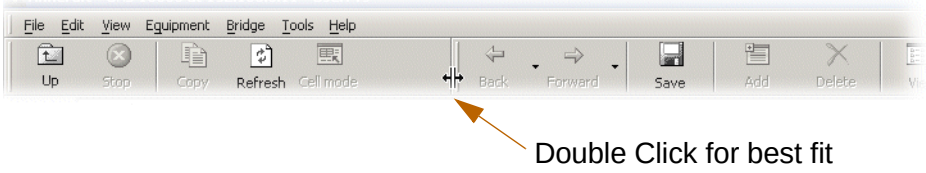


Figure 40 Move Toolbar - Example

3.2.2 Menu items

3.2.2.1 File

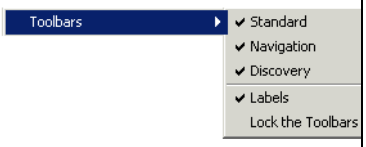
Menu item	Action
Save	Save.
Exit	Exit AXX 9840 INSITE.

3.2.2.2 Edit

Menu item	Action
Copy	Copy selected items to system clipboard.
Paste	Paste content current on system clipboard
Add	Add row
Delete	Delete selected item(s).
Select all	Select all items in the active view.
Invert selection	Invert current selection in the active view.
Clear selection	Clear current selection.

3.2.2.3 View

.

Menu item	Action
Toolbars 	Standard: Check to make Standard toolbar active. Navigation: Back/ Forward Attributes: Check to make Attributes toolbar active. Map Viewer: Check to make Map Viewer toolbar active Zoom: Toggle the zoom tool Location: Check to make visible Labels: Check to make labels visible on toolbar buttons Lock the Toolbars
Status bar	Check to make Status bar visible in the bottom of AXX 9840 INSITE desktop.
Management Tree	Check to make Management Tree an active application on the desktop.

Menu item	Action
Notification List	Check to make Notification List an active application on the desktop.
Last alarm	Check to view latest received alarm in separate window in the Notification List.
Back	See “Toolbar buttons” on page 81
Forward	
Up	
Home	
Stop	
Refresh	
Error Log	Open Error log. Log is also available from the statusbar directly.

3.2.2.4 Equipment

Menu item	Action
VLAN Settings	Open VLAN Settings GUI. Please see “VLAN provisioning” on page 547.
Cross Connection manager	See “SDH Cross Connection Management” on page 451.
Notification History	Open Notification History. See “Notification History List” on page 149.
Commissioning Wizard	Open the Commissioning Wizard. .
MCN Wizard	Open Management Communication Network. Wizard. Please see the “The MCN Wizard”chapter.
NE Maintenance	Open Software Download and Configuration Restore. Please see the “NE updates and upgrades”chapter.
NE User Management	Restricted access according to user rights
PM Viewer	Open the Performance Management GUI. See.

3.2.2.5 Tools

Menu item	Action
VT 100 Terminal	The VT100 terminal launches (only visible if configured). Please see “Configuration of VT100 terminal” on page 12 for details.
View Running Configuration	Opens a text based report about System Status info such as: Total memory, Used memory,Free memory, Ics, Uptime Server hostname and address
Text Editor	Open Text Editor to create, open and save text file.
Features	Open list of supported features for selected Network Element.
Protocol Viewer	View the protocol scheme for the various Network Elements
Repository browser	View and publish Maps, Images and templates
User Settings	Open User Settings to change password.
User Manager	Open User Manager Tool. NOTE! Access Control feature.
Audit Log	Open Audit Log NOTE! Access Control feature.
Map Viewer	Open Map Viewer Tool in new window.
Map Designer	Open Map Design Tool. See Map Designer User Guide

3.2.2.6 Help

Menu item	Action
Online Help	Launches AXX 9840 INSITE User Guide online.
Alarms and Events	Launches an Alarms and Events description document
AXX 9300 METRO Alarms and Events	Launches an Alarms and Events description document specific to AXX 9300 METRO (Only active when logged on to an AXX 9300 METRO NE)
Map Designer Help	Launches the Map Designer User Guide.
PM Tools	Launches the PM Tools User Guide.
System Administration Guide	Launches the System Administration Guide.
Release Notes	Launches release notes for installed AXX 9840 INSITE software.

Menu item	Action
Ericsson Web	Open Ericsson Internet site.
About	Launches information of installed AXX 9840 INSITE software. See Figure 41

Figure 41 The About box- Example

3.2.2.7 Log Viewer

The Log Viewer contains a list of error messages reported in AXX 9840 INSITE according to level settings. If the log contains messages, this is displayed in the status bar with symbols indicating severity of the message:

Error

Warning

Information

Unmappped severity

- Double-click symbol to view log.
- Messages marked with the Note- icon contains additional information.
- Click Note- icon to view link.

NOTE! Logs can be saved to file, opened in, and deleted from the Log Viewer. ‘Clear’ will remove all messages from the Log Viewer.

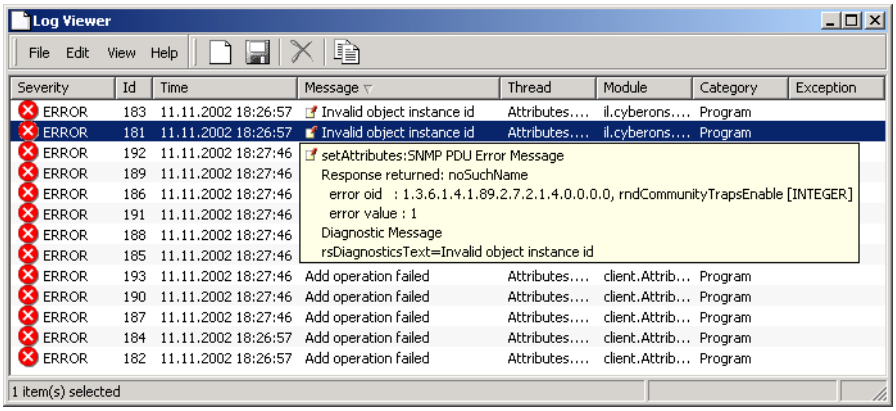


Figure 42 Log Viewer

Tooltip shows the entire value, if it does not fit inside the cell:

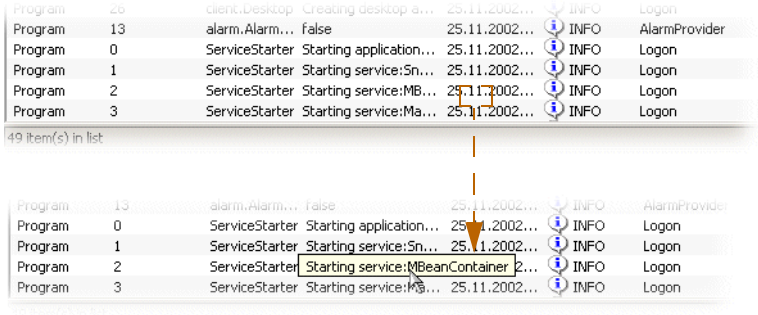


Figure 43 Log Viewer - tooltip

3.2.3 Other desktop features

3.2.3.1 Copy and paste

All AXX 9840 INSITE applications supporting table entry editing have a copy and paste feature. When pasting, AXX 9840 INSITE will verify that selected columns have the same data type as the cells copied from. If not, you are asked if you would like to copy the data based on the column names. Only editable columns with the same name and data type will be then be pasted. This enables copying and pasting between tables with the same data but with different column order.

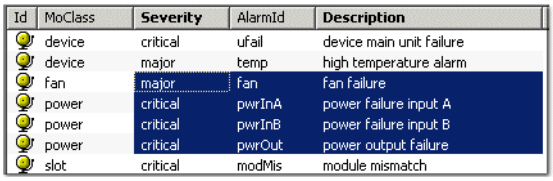


Figure 44 Example - copy data from an AXX 9840 INSITE application

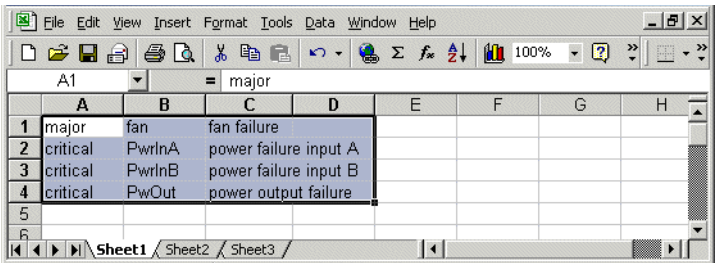


Figure 45 Example - paste data to 3.rd party program

3.2.3.2 Cell-selection mode

By default, entire rows are selected in table, but single cells can easily be selected using the cell-mode toggle button. 

The feature enables copying one table cell, selecting the entire column, press Paste and copying the value into all selected cells. Copy and paste of ranges are also supported. Thus you can copy values A and B and paste them into a large range in order to get the A and B values repeated throughout the range.

Copy and paste to external applications such as MS Excel and MS Word, is supported.

3.2.3.3 Navigation in tables using the keyboard.

Cell in focus is easily spotted and the arrow-keys can be used to move the cursor (applies for editable tables only). Editing of selected cell is easily available via Enter or F2. The Tab-key can be used for moving to the next editable cell (from left to right and top to bottom). The selection is circular, meaning when last editable cell on the last row is reached, the first editable cell in the first row will be activated.

In order to move to first editable cell in a table, activate the window and press the Tab-key twice.

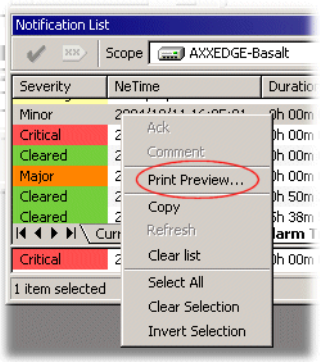
See “Notification List” on page 128

3.2.3.4 Auto fit column width

Double-clicking on the resize-area in the column header will resize the column so that it is wide enough to show all values in the column. By default, the column name is not taken into consideration, but this can be achieved by holding down the Shift key while double-clicking.

3.2.4 Print preview of the Notification list

At any time you can open a Print Preview, and create a report from the collected data for example in the Notification list. Right click on an item in the list and select Print Preview.



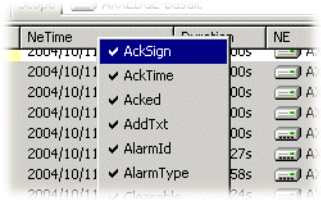
Right click

Figure 46 Print preview

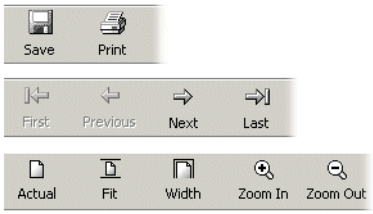
The report preview reflects the order which the columns in the list are arranged and sized, so you can re-arrange and adjust the width of the columns to fit the data you want to present in the table.

Dependant on the number of columns set up in the Notification List, the right part is truncated.

Right click in the Notification List and uncheck columns not needed for the print-out. Print to PDF file format and then use a PDF reader to print the file.



Save the report to PDF for the best print and electronic handover format.



Report viewing options	
Open	Opens a dialog where you can browse and open previously stored reports of the format JasperReports(*.jrprint)
Print	Opens a standard system print dialog
First	Jumps to the first page
Previous	Shows the previous page
Next	Shows the next page
Last	Jumps to the last page
Actual	Scales the page to actual size
Fit	Scales the page to fit inside the active window
Width	Scales the page to fit the width in the active window
Zoom in	Enlarges the text
Zoom out	Reducers the text

NOTE! The Print Preview is also available from the Audit log and the PM viewer.

3.3 Management Tree

The Management Tree is a topology of managed objects, and presents managed Network Elements (NEs) and objects in a hierarchy. The Attributes Viewer shows values to the managed objects.

A set of network elements can be grouped into domains. A default domain lists the managed NEs directly in the Management Tree. You can view the entire hierarchy, or use any of the predefined views to only view managed entities of a certain type. You can choose to view the LAN ports only.

Whenever an item in the Management Tree is selected, the topology and/ or Attributes list the children objects to this parent item.

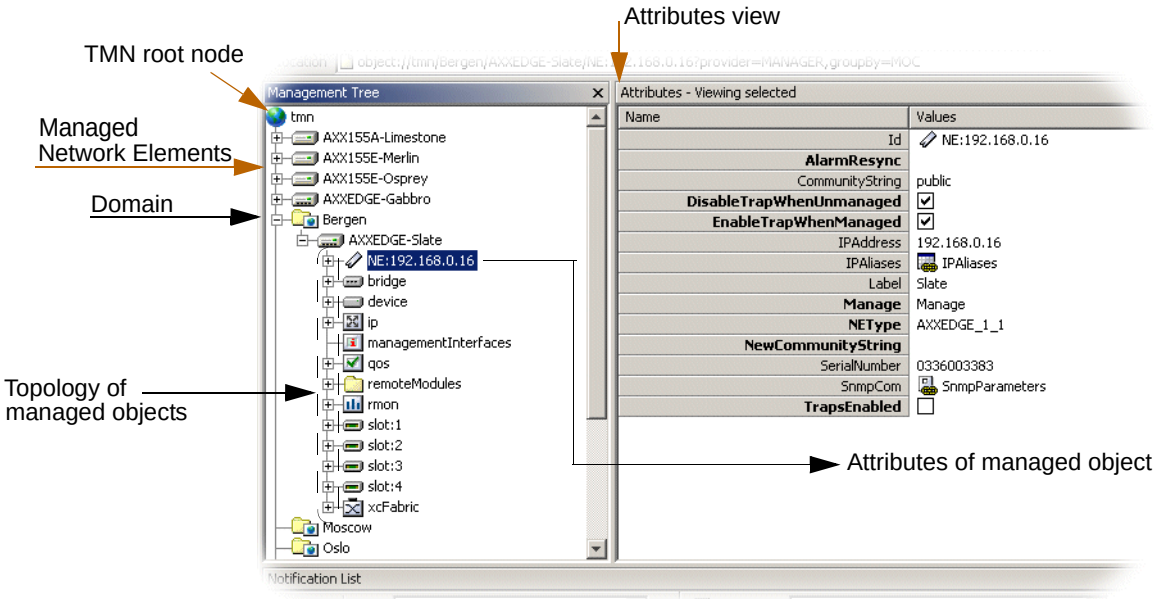


Figure 47 Management Tree- Example

Clicking on a managed object in Management Tree, will display all attributes to that specific object.

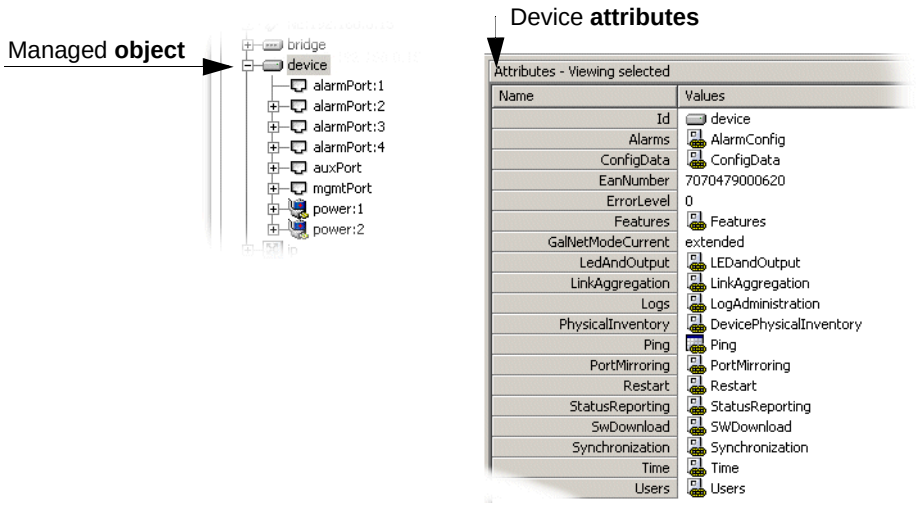


Figure 48 View device attributes

NOTE! All links to editable complex types and tables are visualized as hyperlinks. The different configuration tasks using the Management Tree are thoroughly shown in the following chapters.

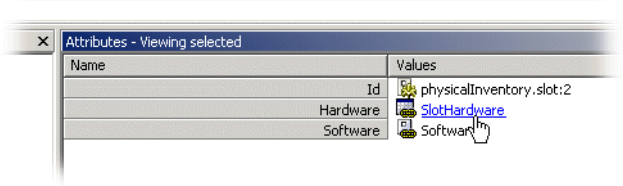


Figure 49 Editable types and tables - hyperlinks

Although changing attribute values can carry all necessary configurations, more complex configuration is handled using wizards or custom user interfaces.

3.3.0.1 State indication to managed NEs

The Management Tree also provides a graphical state indication on the managed NEs. See example in Figure 50

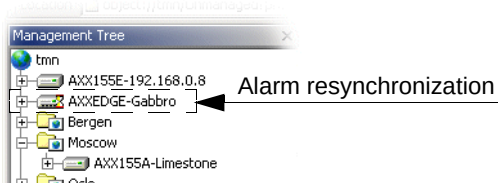


Figure 50 Example of state indication on a network element

3.3.0.2 Symbols

An **hourglass** 

This symbol indicates initialization and alarm resynchronization when objects are added to management.

A **white cross on red** 

The symbol indicates a lost connection between the management system and the network element.

3.3.1 Attributes

Attributes are essential supplements to the Management Tree and apply to managed network elements and to each of the managed objects.

Attributes have two optional views, and values can be edited for some of them.

3.3.1.1 Viewing selected and children

Selected

Attributes to the managed objects are listed on a top- level in this default view.

Children

The children to a managed object can be presented in both the Management Tree and the Attributes Viewer. See Figure 51

Configurations however can only be edited in Attributes, see “Attribute values” on page 94.

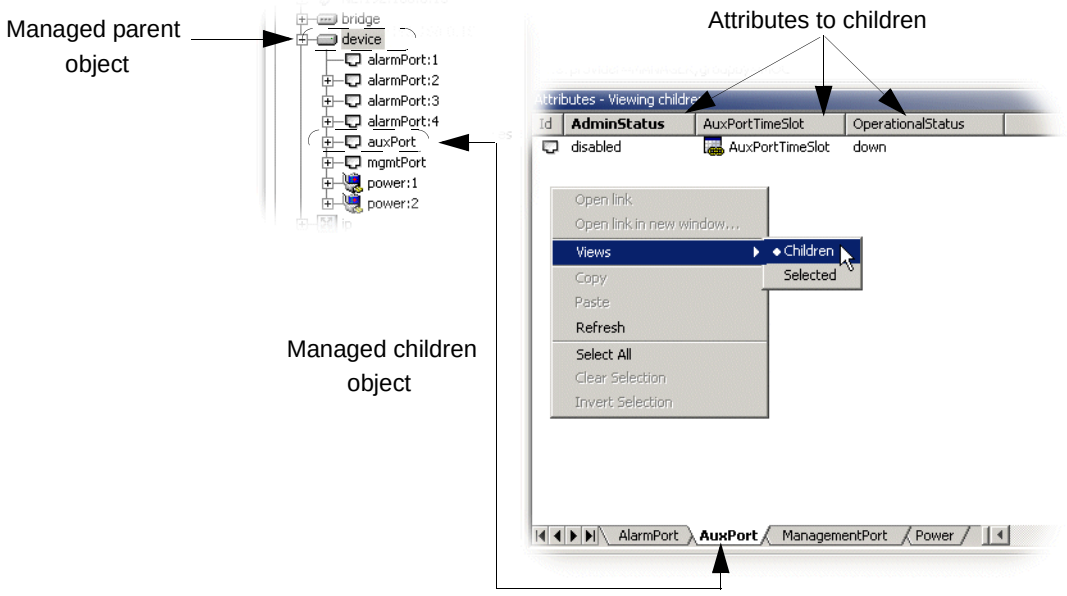
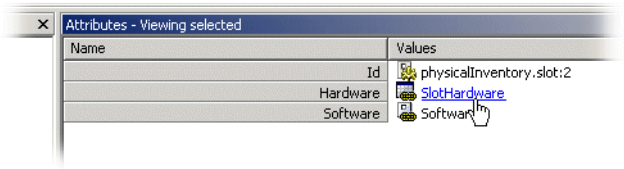


Figure 51 Attributes of selected object - viewing children objects

Attribute values

Attribute values can carry all necessary configurations to the managed objects.

Editable attributes are shown with **bold** attribute name. Such attributes can be edited in the table directly or through custom user interfaces. All links to complex types and tables are visualized as hyperlinks.



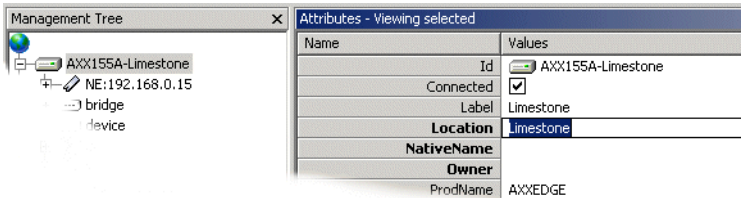


Figure 52 Hyperlinks and editable attribute values

The example shows a Network Element labelled ‘Limestone’ in the Management Tree. This attribute can be edited along with Native Name and Owner. A change in Location is a change of Label. ProdName however is a non-configured attribute.

Procedure: **OPEN ATTRIBUTE LINKS**

You have two options to view attribute links:

1. Click **the link** directly to view attributes in the same window. See Figure 53

or:

1. Select a **managed object** in Management Tree
2. Right- click **link** to children object in Attributes
3. Choose **Open link in new window**

A new window shows attributes to the managed object.

TIP! Right click and hold inside the Attributes window and move the mouse to the left and then release to go back to the last view. Move to the right to go forward again.

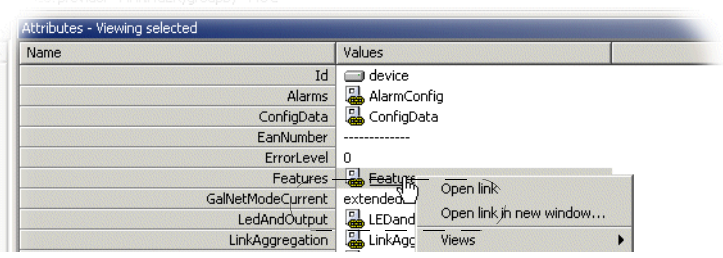


Figure 53 Attribute view options

TIP! With separate windows you can compare attribute values on different managed objects.

3.4 Manage Domains

A domain is defined as a set of network elements. Domains present a way of organizing access to the network through a logical grouping of managed objects. AXX 9840 INSITE updates all user profiles that are associated with the domain.

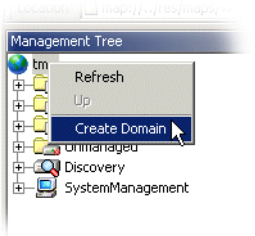
NOTE! Domain is part of access control. Network Administrator and System Administrator have access to manage domains.

The default domain is the TMN root node in Management Tree. It lists all managed network elements that do not belong to a domain. A network element can only belong to one domain.

3.4.1 Domain set up

Procedure: **CREATE A DOMAIN IN THE MANAGEMENT TREE**.

1. Right- click **TMN root** in the Management Tree.



2. Select **Create Domain.**

The Create Domain dialog box opens.

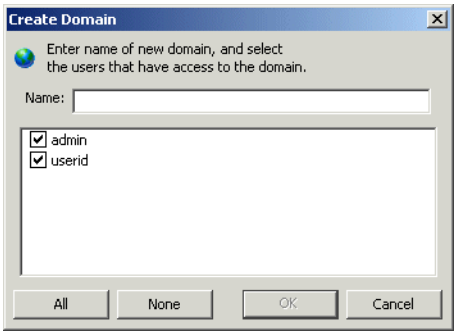


Figure 54 Create domain dialog box- example

3. Enter **Name** of the domain.

4. Check **<UserId>** in list for domain access right.

NOTE! Press None to clear list, and press All to check list of users.

5. Click **OK.**

A new domain will appear with name in Management Tree to users with domain access rights. See Figure 56

NOTE! *Figure 55 The domain has not yet any managed network elements.Add network element(s) to domain*

This procedure applies to existing network elements in the managed list in the Management Tree. For undiscovered network elements, see “Add and Remove NE to management” on page 102 and “Add to Domain” on page 112.

1. Select and drag **network element** from the managed list in the Management Tree.

2. Drop network element to selected **domain.**

The network element is grouped in domain.

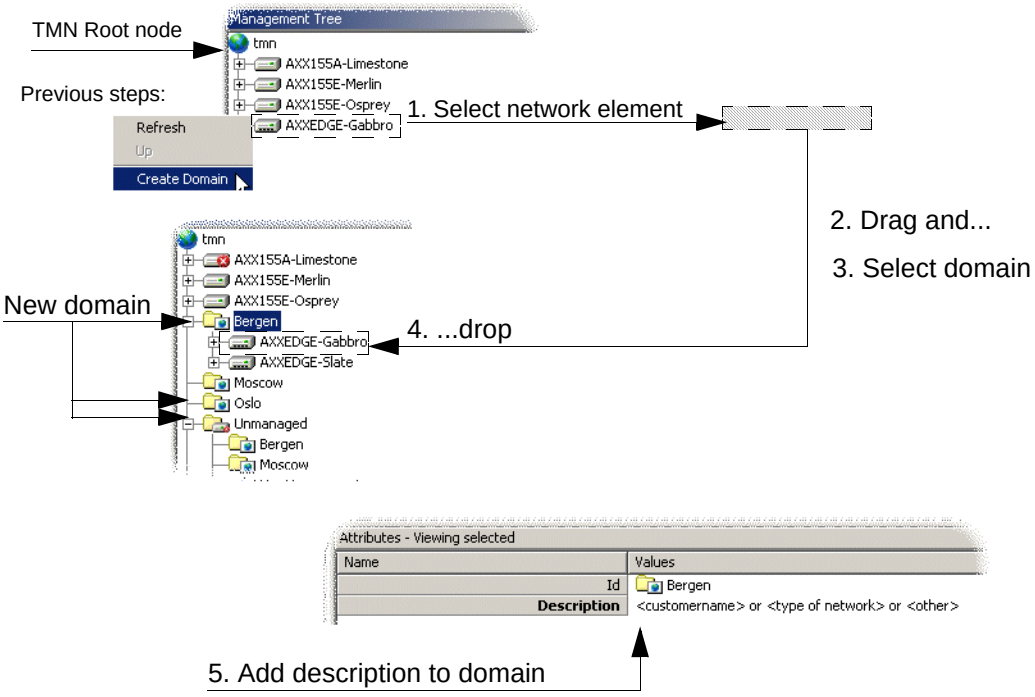


Figure 56 Domain set up- example

3. Repeat in order to **group a set of network element** in managed domain.

A failure in drag- drop operation is announced as an error message:

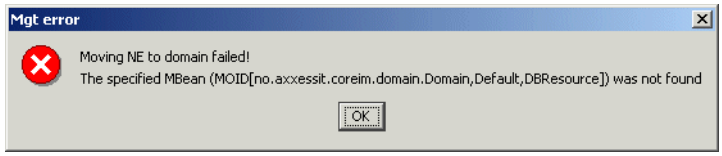


Figure 57 Error message- example

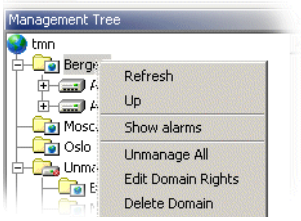
4. Add **description** to domain in Attributes.

5. Press **Save**.

Procedure: **EDIT DOMAIN RIGHTS FROM THE MANAGEMENT TREE**

1. Right- click targeted **Domain** in the Management Tree.

2. Select **Edit Domain Rights.**



The Edit Domain dialog box opens.

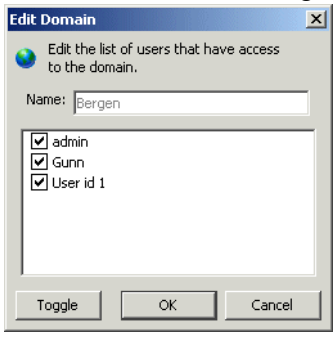


Figure 58 Create domain dialog box- example

3. Uncheck and/ or check **<UserId>** in list for domain access right.

NOTE! Press None to clear list, and press All to check list of users.

4. Click **OK.**

The domain will appear with name in the Management Tree for users with domain access rights, and will be removed from those users without access rights.

NOTE! This procedure is also available in the User Manager, (see the System Administration Guide.

3.4.2 Remove a domain from the Management Tree

Procedure: **REMOVE NETWORK ELEMENT(S) FROM MANAGED DOMAIN**

1. Select desired managed **domain** in Management Tree.

2. Select and **right-click** desired network element**.**

3. Select **Unmanage.**

The NE is removed from the domain, and is listed as unmanaged.

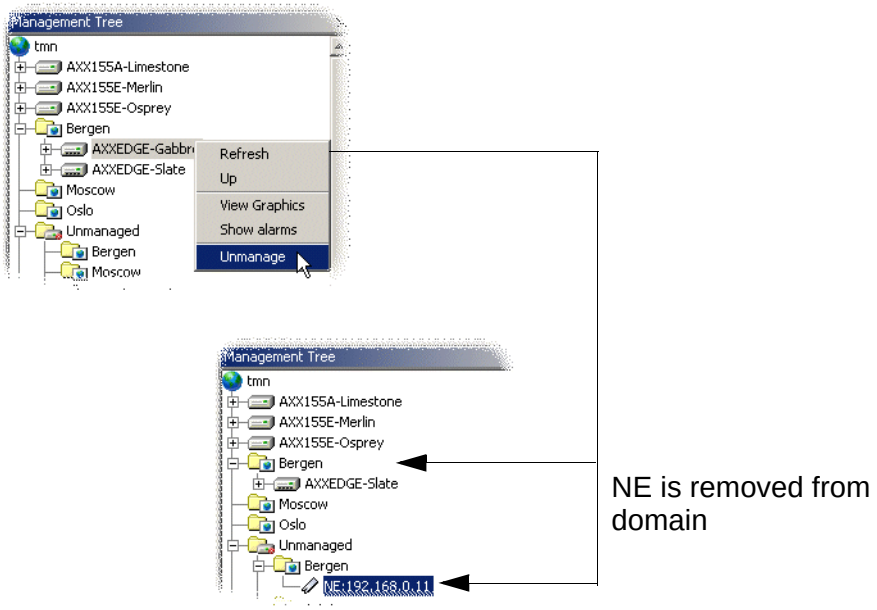


Figure 59 Remove network element from domain

NOTE! The NE is still part of the unmanaged list in the topology. See “” on page 127

Procedure: DELETE A DOMAIN

The domain must be empty in order to delete it from the Management Tree, see “Remove a domain from the Management Tree” on page 99.

1. Right-click selected domain.

2. Choose **Delete Domain.**

AXX 9840 INSITE removes the domain from the Management Tree.

NOTE! AXX 9840 INSITE deletes the domain entry from the repository and updates all entities that have an association with the deleted domain.

You will see an error message if the domain is not empty.

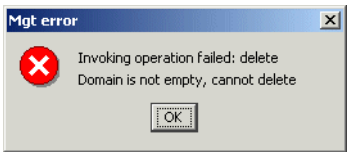


Figure 60 Error message - domain not empty

3.5 Add and Remove NE to management

3.5.1 Introduction

The purpose of this section is to describe the process of how network element instances in the managed network are discovered and added to, or deleted from management through identification criteria of the network element(s).

The section also describes how to use the AXX 9840 INSITE to change the management state of discovered network elements.

NOTE! This is an access control feature. The system administration represented by the Network Administrator and the System Administrator have access to Discovery.

3.5.1.1 Overview

The following overview applies when initiating an auto-discover session:

- Define the auto-discovery strategy
- Detection criteria specification (address range, network element type etc.)
- Define the initial management state for undiscovered network elements when detected
- Define the management strategy for discovered network elements
- Initiate the auto-detection session.
  AXX 9840 INSITE initiates an auto-discovery session according to the specified strategy, see Figure 61 The discovered network elements are registered in AXX 9840 INSITE according to the state change strategy, see “Network element states” on page 102.

The order of the steps is insignificant, except for the initiation, which must be the last.

3.5.1.2 Network element states

The network elements can be in three different logical states, as presented in Figure 61

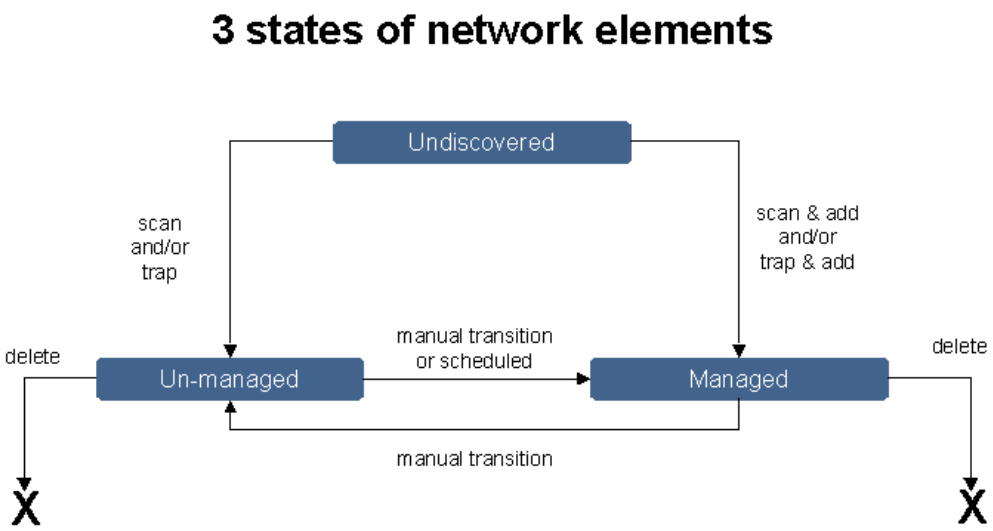


Figure 61 NE State transitions related to discovery and management.

You can configure AXX 9840 INSITE to initiate these transitions.

Unmanaged

A network element is unmanaged when it exists in the managed network and is identified by AXX 9840 INSITE, but AXX 9840 INSITE is prohibited from performing management tasks on the network element.

If a network element is in the unmanaged state:

- Can partly browse in topology.
- Can not be configured.
- Alarms are not reported.
- Part of unmanaged domain.

Undiscovered

A network element is undiscovered when it exists in the managed network, but is not identified by nor visible in AXX 9840 INSITE.

The network element is neither in “Unmanaged” nor “Managed” state.

Managed

A network element is managed when it exists in the managed network and is identified by AXX 9840 INSITE. AXX 9840 INSITE performs management tasks on the network element.

If a network element is in the managed state:

- Can browse in Management Tree
- Can be configured
- Alarms are reported if AXX 9840 INSITE is registered as trap receiver on the element
- Part of managed domain

3.5.2 Detection Criteria Specification

You configure AXX 9840 INSITE to discover network element instances on one or more sub nets according to different criteria; the network element characteristics used when scanning.

3.5.2.1 IP address, or subnet mask

If you know the exact IP address or host name of the network element, this can be specified, i.e., a pre-configured network element list. The alternative is to specify a network[1] where the element belongs. A restriction is put on the network mask to avoid flooding of the Internet with broadcast messages.

See “Discovery entry attributes” on page 109 and “Network” on page 110.

3.5.2.2 Network element type

You can optionally specify the type of the network element(s) from a list of network elements, a specific network element type, or all element types the management system is able to manage.

See “Discovery entry attributes” on page 109 and “Element Type” on page 112

3.5.2.3 Community string

The community string of the management system must be specified in order to receive traps from the network elements. When the management system connects to the network element the first time,

1. network = network address + network mask

the IP address of the management system is not defined in the community table.

- If the management system is not defined in the community table, the user specifies an initial community string. A second community string for insertion in the community table if the element is added to management can also be specified.
- If the management system is defined in the community table it needs to know the community string in order to possibly manage the network element.

See “Community String” on page 110 and “How to specify the community string” on page 118

3.5.3 Define auto-discovery strategy

You select the discovery methods to inspect the managed network to find network elements and register them into AXX 9840 INSITE. The auto-detection strategies are:

3.5.3.1 Manual scan discovery

New network elements are physically added to the network and the field operator notifies the operator on duty about the changes, i.e., on which subnets and what criteria. The operator can then manually initiate a scan limited to the known IP address(es) of the new network element(s). You can specify whether the network element shall go into the managed state or into unmanaged (default) state if discovered during a scan.

See “Discovery of single network element” on page 113.

3.5.3.2 Manual rescan discovery

AXX 9840 INSITE scans the managed network once to find network elements.

If the network element on a scanned IP address matches the auto-discovery criteria, it is discovered and registered in AXX 9840 INSITE as a managed or unmanaged network element.

If no network elements are found that meets the characteristics the scan is not repeated automatically. A manually rescan of the existing discovery setup is provided, see “Rescan discovery entry” on page 111.

3.5.3.3 Scheduled scan discovery

You specify a scan interval to make AXX 9840 INSITE perform periodic scans of the managed network to identify new network elements according to the “Detection Criteria Specification” on page 104.

If the network element on a scanned IP address matches the auto-discovery criteria, and the network element is not already registered in AXX 9840 INSITE as a managed object, it is discovered and registered in AXX 9840 INSITE as a managed or un-managed network element.

3.5.3.4 Trap discovery

When a trap from an un-discovered network element is received by AXX 9840 INSITE, and the network element matches the auto-

detection criteria, the element is discovered and registered in AXX 9840 INSITE as a managed or un-managed network element.

The initial trap and other traps that are received during evaluation of the trap sender, is collected and stored by the management system. If the element is added to management, the traps are mapped to notifications and presented in the management system. See “Notification List” on page 128.

NOTE! You can disable scans (try-and forget and scheduled scans) without affecting the trap detection.

3.5.4 Management strategy for network elements

Validation of found network element instances

AXX 9840 INSITE scans the sub net(s) for network elements fulfilling the specified criteria. Depending on the state transition value AXX 9840 INSITE moves the found network elements fulfilling the criteria to:

- List of managed (TMN domain root node = default)
- List of unmanaged (TMN domain root node = default)

The default set domain lists, i.e., network elements in the states ‘managed’ or ‘Unmanaged’, of known elements consist of elements that are found earlier through a scan and are added to management manually or automatically.

Un-discovered network elements

You can specify the initial management state of a network element when discovered. The choices are managed (default) or un-managed. You may optionally specify the target domain of the discovered network element. The intention of an un-managed state is to evaluate the discovered network element prior to manually releasing it for management.

Depending on the state transition value the management system moves the found network elements fulfilling the criteria to:

- List of managed
- List of unmanaged

The lists of known elements consist of elements that are found earlier through a scan and are added to management manually or automatically.

The lists of "Managed" and "Unmanaged" elements are stored persistently.

State Change strategy for discovered network elements

You can change the management state of discovered network elements manually. The alternatives are:

- Change from un-managed to managed state
- Change from managed to un-managed state
- Delete from un-managed state

See “” on page 116

When the user defines the strategy for state management, the following choices are available:

- When changing from un-managed to managed, the target network element trap generation is enabled by AXX 9840 INSITE.
- When changing from managed to un-managed, the target network element trap generation is disabled by AXX 9840 INSITE
- No changes to target network element trap generation when changing between managed and un-managed state.

When a network element is added to management manually, AXX 9840 INSITE possibly asks the system administrator for more configuration needed to be able to add the network element to management.

3.5.5 Presentation of the Discovery

Open The Discovery

Open the Discovery from the Management Tree or from the Management Centre.

The Discovery GUI

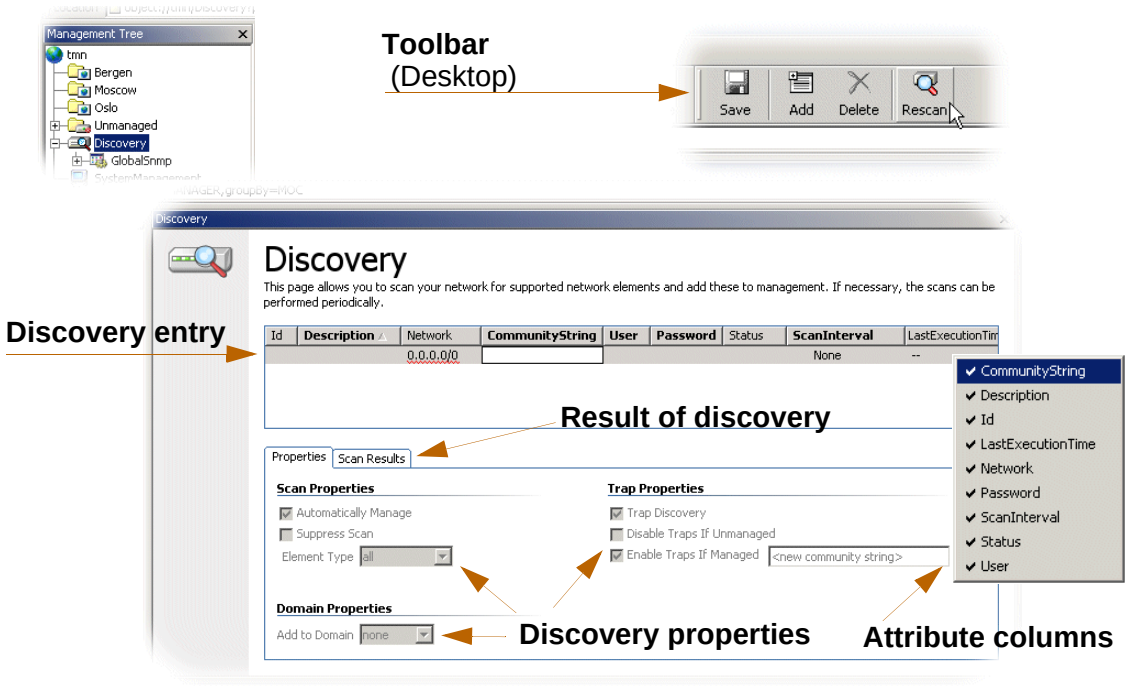


Figure 62 Discovery view

Discovery entry attributes

The following attributes can be found in the Discovery view. Some attributes are read only.

3.5.5.1 Id and Description

An identification is automatically displayed for a discovery entry. A description field is provided for manually added information to the different entries.

3.5.5.2 Network

Network Address formats:

The IP Address can be entered as a specific, known network address:

192.168.0.8

or as a network range:

192.168.0.0/24

About using **/**<prefix length> notations

You can use the extended network prefix length rather than a subnet mask. The prefix length is equal to the number of continuous one-bits in the traditional subnet mask. For example, this means that specifying the network address 130.5.5.25 with a subnet mask of 255.255.255.0 can also be expressed as 130.5.5.25**/24**

130.5.5.25	10000010.	00000101.	00000101.	00011001
255.255.255.0	11111111.	11111111.	11111111.	00000000

130.5.5.25**/24**	10000010.	00000101.	00000101.	00011001
24 bit Extended Network Prefix				

3.5.5.3 Community String

The community string is a password that must be specified in order to discover and manage network elements.
'Public' is default password for IP=0.0.0.0.

NOTE! If your AXX 9840 INSITE workstation is not defined in the community table, see "Community string" on page 104 for system administration.

3.5.5.4 User and Password

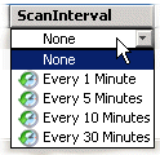
When you want to include AXX 9300 METRO NEs in the discovery, you need to enter the user and password for these NEs in your network.

3.5.5.5 Status

The different Discovery status are OK and Error for the process. A progress bar is displayed with status information in percentage.

3.5.5.6 Scan Interval

A discovery operation will be repeated when you select a periodic rescan with or without interval. Available intervals are as shown below:



NOTE! Make sure that Suppress Scan is un-checked, when using Scan Interval.

3.5.5.7 Rescan discovery entry

Scan Interval is default set to no rescan, thus AXX 9840 INSITE will try- and- forget discovery, see “Define auto-discovery strategy” on page 106.

You can rescan an existing discovery entry by using the rescan button on the toolbar.

3.5.5.8 Discovery properties

Automatically manage

Check Automanage to automatically add discovered NEs to domain of managed elements. An uncheck will register discovered NEs to unmanaged domain. It is recommended to use this function when

the network element is known (Network format = IP address/ Element Type).

Suppress Scan

This is a supplementary function to Scan Interval and Trap Discovery.

Check Suppress Scan to:

- set the rescan on hold in network element discovery (for later use)
- turn off the network element scan

Element Type

Select desired network element type to be target for scan, using the pull-down menu. Choosing ‘All’ includes all supported network elements types.

Add to Domain

Use Domain menu to group new network element(s) to predefined domains directly in Discovery. See.“Domain set up” on page 96

3.5.5.9 Trap properties

Trap Discovery

Check Trap Discovery in order to receive traps from discovered NEs in given subnet.

NOTE! AXX 9840 INSITE can discover traps on network elements even if they are manually removed from management, and can automatically add such NEs to management. The combination of Automanage, Trap Discovery, Enable Trap When Managed and Re-scan should be used with caution.

Disable Traps When UnManaged

Check to disable trap-receiving when managed NEs are set to unmanaged.

Enable Traps When Managed

Check to enable trap-receiving when discovered NEs are set to managed.

New Community String

A second community string should also be specified for insertion in the community table when the element(s) is added to management.

The new community string is added to the community table, when *Enable Traps When Managed* is checked and enables your AXX 9840 INSITE workstation to receive traps from the network element(s) added to management.

Scan Results

The result of the discovery is displayed with status for the discovered network elements and IP addresses, see Figure 66

3.5.6 Recommended discovery setup

The automatically manage feature is a default setting. If you prefer to manually set discovered network element(s) to managed state, uncheck this property and see “” on page 116.

NOTE! You must manually register AXX 9840 INSITE as a subscriber to alarms and events from the network element, see “Subscription of alarms” on page 121.

Procedure: **DISCOVERY OF SINGLE NETWORK ELEMENT**

We recommend you to use this procedure when you know the network elements IP address and type. See “Define auto-discovery strategy” on page 106.

1. Open **Discovery.**
2. Click **Add** on Toolbar.
   - A new discovery entry appears.

3. Enter **Description**.

4. In **Network** enter the **IP address** for target NE or range of NEs.

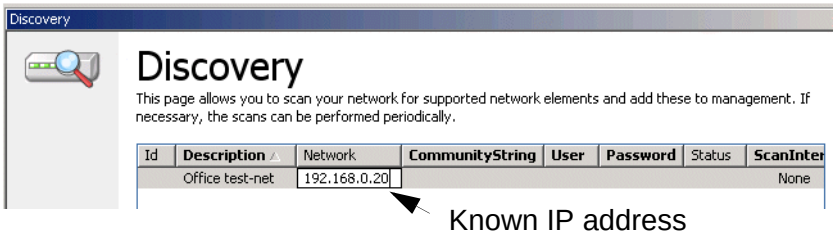


Figure 63 Discovery entry- example

5. Enter initial **CommunityString** for non-AXX 9300 METRO NEs.

6. Enter **User** and **Password** for AXX 9300 METRO NEs

7. Check **Automatically Manage** (default as scan property).

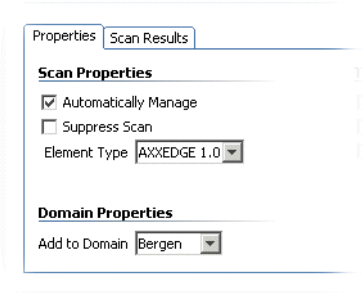


Figure 64 Discovery properties- example

8. Select **Element Type** from menu.

9. Select **Domain** for targeted network element.

10. Check **Trap Discovery**.

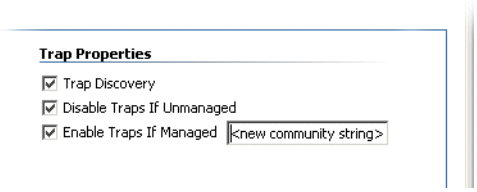


Figure 65 Trap properties

11. Check **DisableTrapsWhenUnmanaged**.

12. Check **EnableTrapsWhenManaged.**

13. Enter **NewCommunityString** as Trap property.

14. Click **Save** on toolbar to execute Discovery settings.

15. View the **Status** for Discovery progress.

The discovery result is displayed as shown in Figure 66

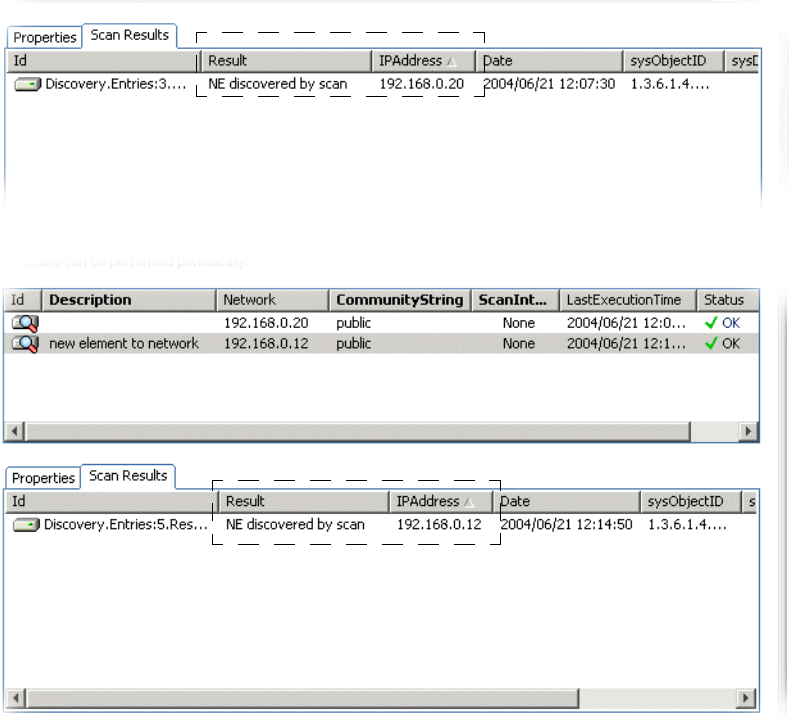


Figure 66 Discovery result- example of single network element discovery

Procedure: NETWORK SCAN

READ MORE:E “Define auto-discovery strategy” on page 106.

1. Open **Discovery.**
2. Click **Add** on Toolbar.
3. Enter **Description**.
4. In **Network** enter network range.
   (see “Network” on page 110)

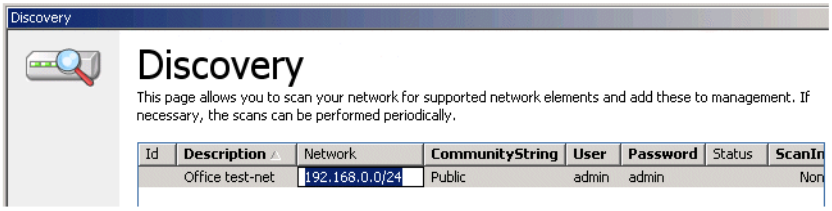


Figure 67 Discovery- example of network scan

5. Enter initial **CommunityString** for non-AXX 9300 METRO NEs.
6. Enter **User** and **Password** for AXX 9300 METRO NEs
7. Check **Automatically Manage** (default).
8. Set **Element Type** to All (default).
9. Check **DisableTrapsWhenUnmanaged**.
10. Enter **NewCommunityString**.
11. Click **Save** to execute network scan.
12. View the **Status** for Discovery progress.

Procedure: MANUAL TRANSITION TO MANAGED STATE

READ MORE: See “Unmanage single network element” on page 126.

1. Select **desired NE** from unmanaged domain in Management Tree.

2. Click **Manage** and select **Manage**.

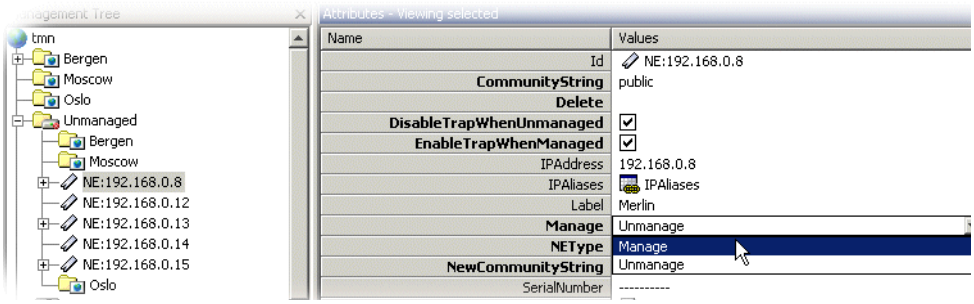


Figure 68 Manage state- example

3. Click **Save** on Toolbar.

The selected NE is part of the managed list in Management Tree.

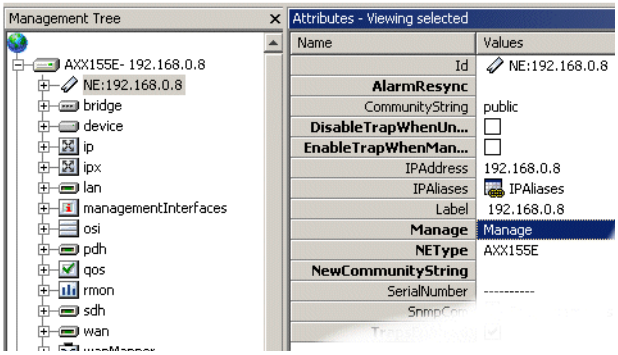


Figure 69 Managed object to root node

Procedure: **SET MANAGED STATE TO MULTIPLE NETWORK ELEMENTS**

1. Select **Unmanaged** domain in Management Tree.
2. Right-click and select **Manage All**.

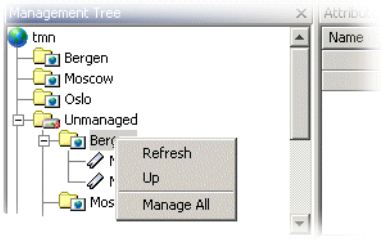


Figure 70 State transition from Unmanaged domain

Multiple NEs are now part of the managed domain in Management Tree. The unmanaged domain is cleared for any unmanaged network elements.

NOTE! When the network element is set to managed state and the Enable Trap When Managed is checked, remember to re synchronize alarms. See “Subscription of alarms” on page 121 and “Resynchronize Alarms (optional)” on page 125.

3.5.7 How to specify the community string

After having performed discovered and added a network element to the managed network you must specify the community string. When AXX 9840 INSITE connects to the network element the first time, the IP address of AXX 9840 INSITE may not be defined in the community table. If this is the case, AXX 9840 INSITE is not able to receive traps from the element. See *“Subscription of alarms” on page 121*.

- If your AXX 9840 INSITE workstation is not defined in the community table, the system administration specify an initial community string. A second community string for insertion in the community table if the element is added to management can also be specified.
- If AXX 9840 INSITE is defined in the community table it needs to know the community string in order to possibly manage the network element.

1. Select **desired NE.**
2. Click **Device.**
3. Select **Users** in Attributes.
4. Select **Snmp.**
5. Click **Add** and **enter/select**:
   - IpAddress
   - Password
   - Access Right
   - TrapsEnable
6. Click **Save**.

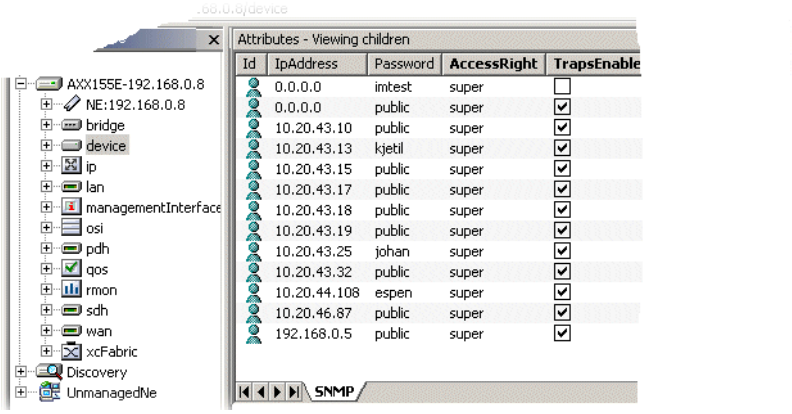


Figure 71 Community table

3.5.8 SNMP Communication Parameters

This section describes Global Settings to the SNMP communication between AXX 9840 INSITE and the network elements.

1. Navigate to Discovery->**GlobalSnmp**.

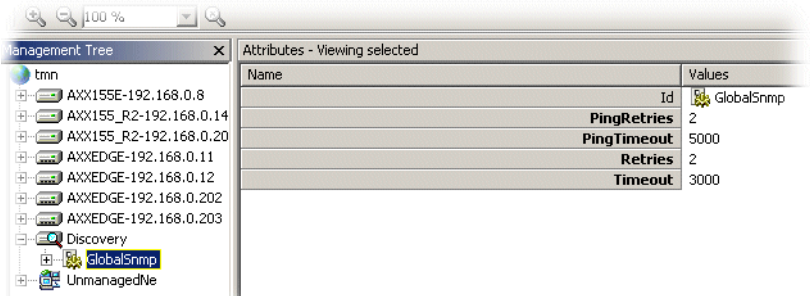


Figure 72 SNMP global settings

Attributes control the communication parameters of the snmp resource (snmp adapter).

Time-out and Retries applies to normal management traffic like getting and setting attributes.

PingTimeout and PingRetries apply to the connection polling that results in Connection Lost events. The time-out values for Ping are normally set higher than for normal traffic in order to report network element connection status with a higher degree of certainty.

Default time out values in milliseconds are:

- Time-out 3000
- Retries 2
- Ping Timeout 5000
- Ping Retries 2

The default values are established persistently when a fresh copy of AXX 9840 INSITE is installed.

The parameter values are constrained according to the following list:

- Time-out and PingTime-out 100..15000
- Retries and PingRetries 0..3

Override global settings on a per-network-element basis

The global settings are possible to override on a per-network-element basis.

2. Navigate to [NE-root]->NE and further down to the attribute **SnmpCom**.
3. Press **SnmpParameters.**
4. **OverrideGlobal** determines if local values for timeout and ping are used.
   If un-checking the **OverrideGlobal** attribute, the **Timeout** and **Retries** parameters are **reset** to the global settings.

It is possible to enable simple response time statistics (for snmp tuning purposes).

5. To enable the function, check the **RegisterStatistics** attribute.
   The snmp response values are read from the Statistics attribute.

3.5.9 Subscription of alarms

To view current alarms you must manually register AXX 9840 INSITE as a subscriber to alarms and events from the network element.

Procedure: **REGISTER AS A SUBSCRIBER OF A NETWORK ELEMENT**

1. Select targeted **NE** in Management Tree.
2. Check **TrapsEnabled** in Attributes.

3. **Save.**

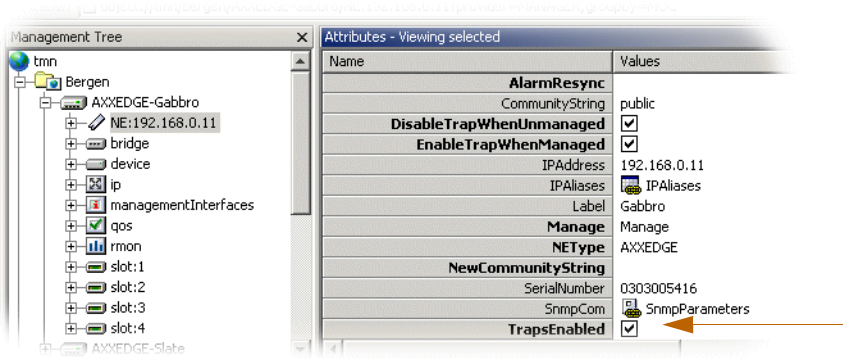


Figure 73 Setting TrapsEnabled in Attributes -1-

Or:

1. Select targeted **NE.**
2. Select **device.**
3. Choose **Users** and click **Snmp.**

AXX 9840 INSITE presents the community table.

4. Select **TrapsEnable** for network element, with reference to **IpAddress.**

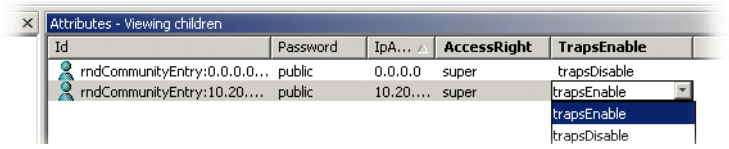


Figure 74 Setting TrapsEnable in community table

5. **Save.**

With this registration, AXX 9840 INSITE can poll the element for all current alarms and report alarms and events to the IP address of AXX 9840 INSITE. The SNMP traps are mapped to Notifications in AXX 9840 INSITE.

The community table on network elements allows 16 instances of traps receivers (users) to exist at the same time. The network element will always attempt to send the traps to all the configured traps receivers.

In some situations, the network element may generate a large number of traps ("alarm storms"). Under these special circumstances, the transmit buffers of the network element may become overloaded, and it may not be possible to send all traps as intended. This problem increases with the number of configured traps receivers and when the MCN capacity is low.

To prevent loss of traps towards traps receivers, we recommend no more than 3 instances configured as traps receivers. The MCN should also be designed with sufficient capacity. The traps receivers may also poll the network element to check for updates the alarm states, but note that this causes further traffic increase in the MCN.

Alarm notification severity

The severity of an alarm notification can either be reported from the network element or must be defined in the notification mapping.

Trap to notification mapping

The interpretation of alarm and event is slightly different in the network element and AXX 9840 INSITE. The mapping rules applied to the SNMP traps are illustrated in Figure 75

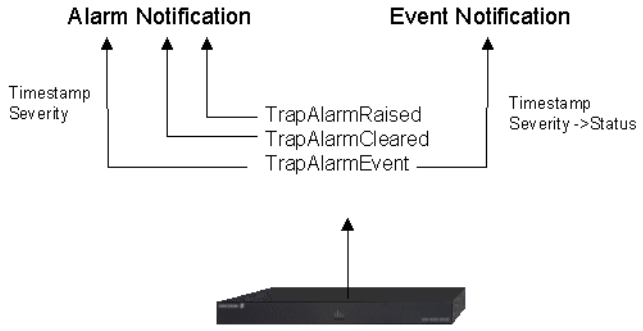


Figure 75 Trap to notification mapping

The TrapAlarmRaised and TrapAlarmCleared traps are mapped to Alarm Notification. The timestamp in the trap will be used together with the severity. AXX 9200 EDGE and AXX155E have severity in the trap. This severity is used in Notification.

One attribute in an Alarm Notification is called "Clearable". If set to TRUE, this attribute indicates that the management system should expect a TrapAlarmCleared for this alarm.

Those TrapAlarmEvent traps that indicate an error/failure in the network element will be mapped to an Alarm Notification with the

attribute "Clearable" set to FALSE. The severity and timestamp from the trap are used in the Alarm Notification.

Other TrapAlarmEvents will be mapped to Event Notifications. These have no severity, but a Status defining the type of event, e.g. info, confirm etc. The severity in the trap might be used as the Status in the Event Notification.

Unknown traps

If AXX 9840 INSITE receives a trap and there exists no mapping to any type of notification, a notification will be generated. The notification contains all the information as it was received in the trap.

3.5.10 Resynchronize Alarms (optional)

If you suspect discontinuity between traps received and alarms displayed in the Notification List, its recommend to re synchronize the alarms.

1. Select managed **NE.**
2. Select **AlarmResync.**
3. Select **Resync** and click **Save.**

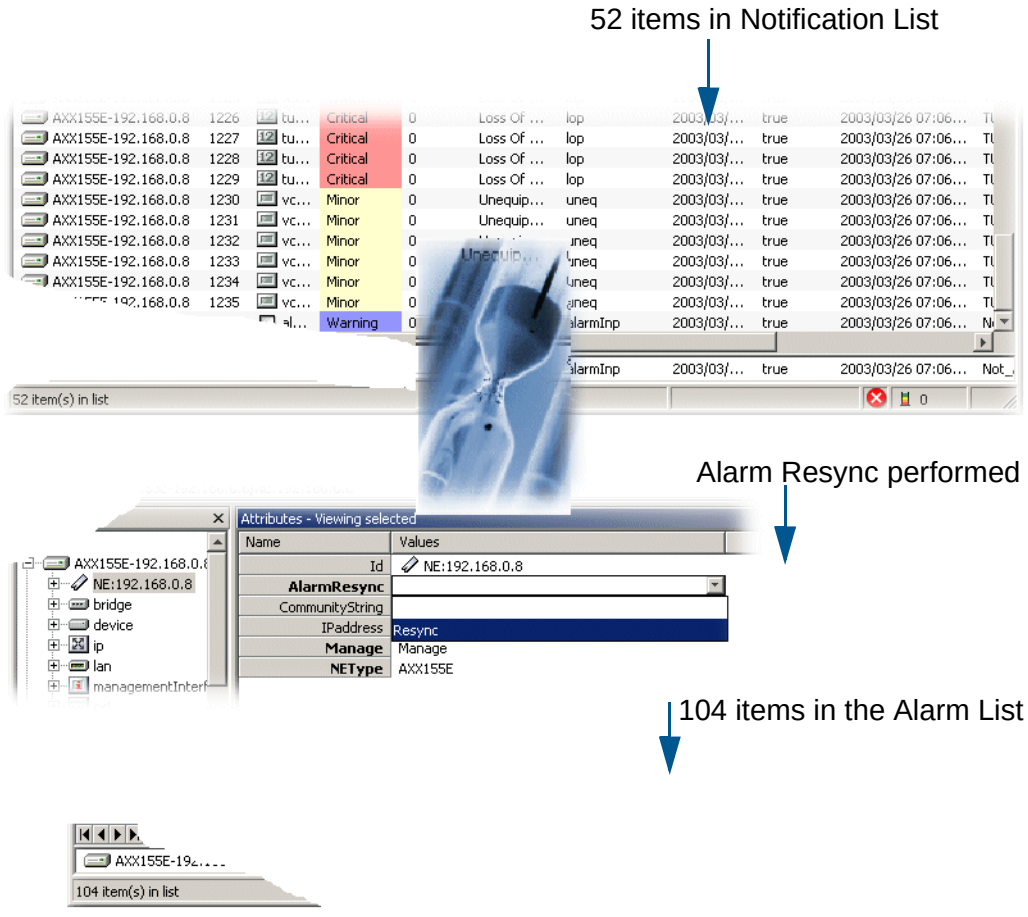


Figure 76 Resynchronize alarms- example

3.5.11 Remove network elements from management

The purpose of this section is to describe how network elements are removed from management.

NOTE! Make sure that any rescan are deleted.

Unmanage single network element

1. Select **NE** from Management Tree.
2. Click **Manage** and select **Unmanage** in Attributes.
3. Click **Save** from Toolbar.

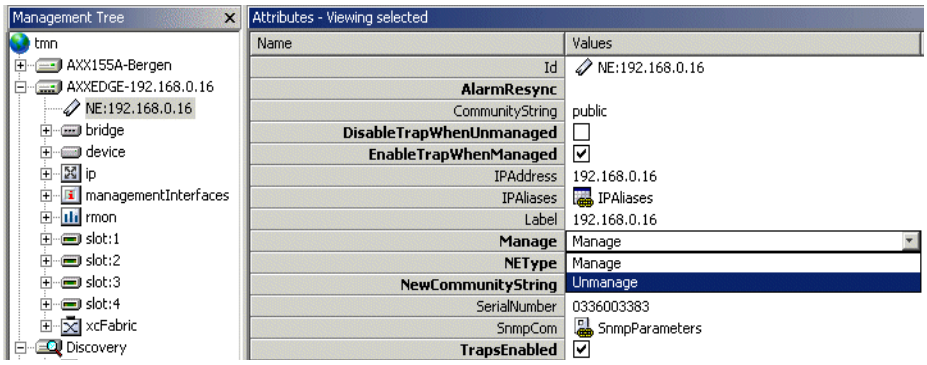
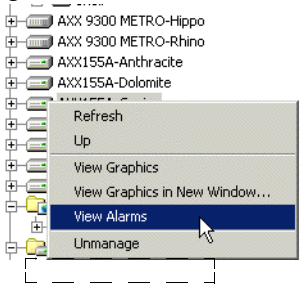


Figure 77 Manual state transition -1-

Alternative method

1. Select **NE** from Management Tree.
2. Right-click and choose **Unmanage**.



The selected Network Element is removed from management and is part of unmanaged domain in Management Tree. The Notification List no longer receives alarms for removed network element.

NOTE! Be aware of the combination of checked Automanage, unchecked ‘Disable when Unmanaged’ together with an active rescan in Discovery. If a trap is received by AXX 9840 INSITE, NE will not be removed from topology, but have an automatic state transition and move to managed domain in Management Tree.

Procedure: **UNMANAGE MULTIPLE NETWORK ELEMENTS**

1. Select desired managed **domain.**
2. Right-click and select **Unmanage All.**

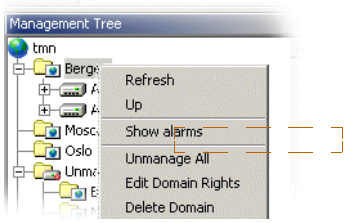


Figure 78 Unmanage multiple NEs

The managed domain is cleared for every managed network element. They are part of unmanaged list in Management Tree.

Procedure: **DELETE SINGLE NE FROM TOPOLOGY**

1. Select the desired **Network Element** from list of unmanaged.
2. Click and select **Delete** in Attributes.
3. Click **Save** from Toolbar.

The network element is no longer present in Management Tree.

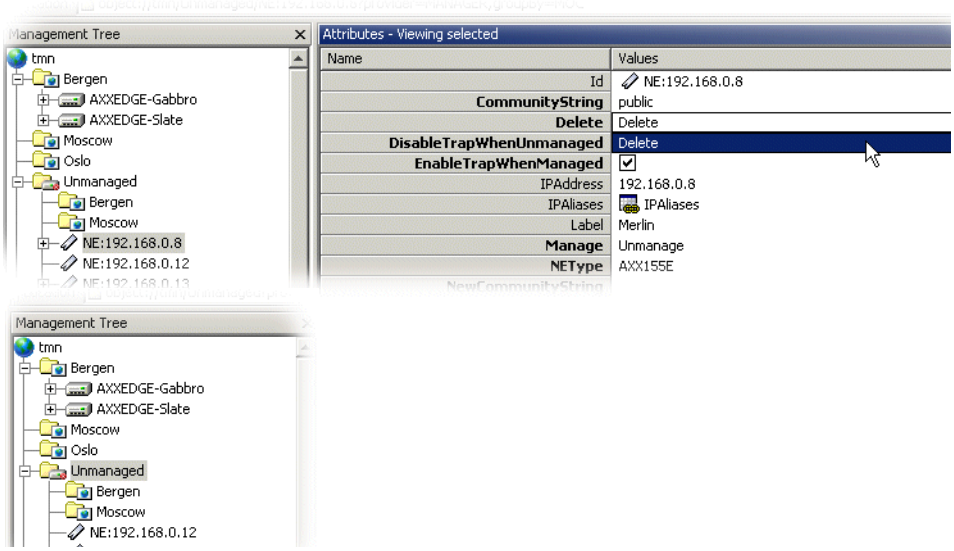


Figure 79 NE removed from Management Tree

3.6 Notification List

This section presents the Notification List, its views and functions. The purpose of the Notification List is to present the current alarm and event notifications. In addition the history of all alarms are presented.

Alarms reports failures in the network element. Events report other situations in the network element that are not failures.

Notifications are presented in various types of list views:

- The Current Alarm List: List current state of managed network element
- The Trace Lists: Chronological list of received notifications (alarm, protection switch and event)
- The Historical Lists: Chronological, static log stored in AXX 9840 INSITE

The dynamic lists are updated every time a new notification is received, unless the notification is suppressed by any selection.

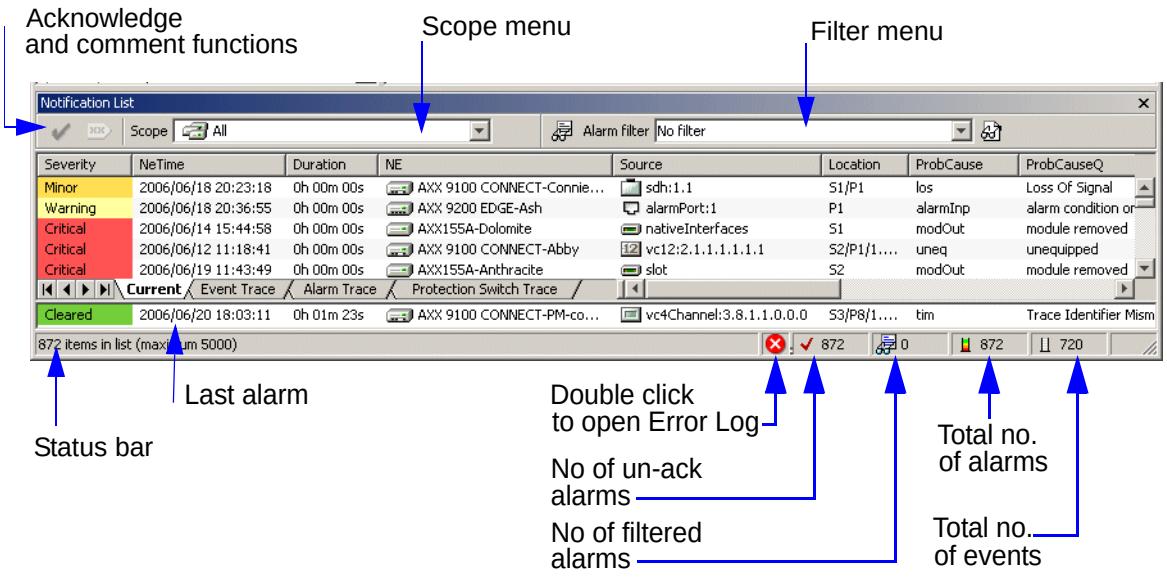


Figure 80 Notification List View

You can comment, acknowledge and select notification records, scope and filter notification selections, and rearrange and sort alarm columns in the Notification List.

NOTE! The maximum number of current alarms is 5000. Trace lists have a maximum of 1000 notifications.

3.6.1 Notifications

A notification is a message informing of a specific occurrence, such as an alarm situation or a state change.AXX 9840 INSITE support alarm notification and event notification see Table 28 and Table 29 notification.

3.6.1.1 Steady State notification / clearable alarms

A notification informing on an occurrence that indicates a steady state change. There are associated notifications that informs on changes to other steady states in the originating object. Specifically for alarm notifications, such alarms are called "clearable", as there will always be an "alarm cleared" notification associated with the "alarm" notification from the same object.

3.6.1.2 Stateless notification / non-clearable alarms

A notification informing on a transient occurrence. There are no associated notifications that informs on a transient occurrence with the reverse effect. Specifically for alarm notifications, such alarms are called "non-clearable" as such an alarm is not associated with an "alarm cleared" notification.

3.6.1.3 Alarm lifecycle

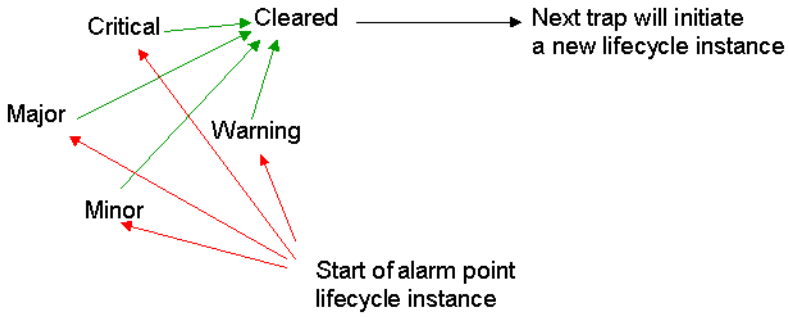


Figure 81 Lifecycle instance of alarm point

The Notification list presents one row for each alarm point, like an alarm source and alarm identification combination. When a new alarm notification for the same alarm point is being presented, the row is possibly updated with the severity of the new alarm and new timestamp(s) unless the alarm has been cleared. A new row is created if the alarm point starts a new lifecycle instance, see Figure 81 Each new alarm notification might cause a transition from one severity to another or to the Cleared severity which ends the lifecycle.

NOTE! No traps are sent to the IP address of AXX 9840 INSITE if you have de-registered as trap receiver. See “Subscription of alarms” on page 121.

3.6.2 Alarm notifications

Alarm notification is a notification type to report a fault condition. A clearable Alarm Notification has an associated alarm clear event, otherwise non-clearable.

The lists contains notification records with a set of information. Alarm attributes are listed in alphabetical order.

Table 28 Alarm notification attribute values

Attribute		
Name	**Description**	**Legal Values**
AckSign	Acknowledge signature	Userid (automatic)
AckTime	Acknowledge time	yyyy/mm/dd hh:mm:ss (server time)
Acked	A check when alarm is acknowledged	Checked/ Unchecked
AddTxt	Additional text (free form text description)	
AlarmId	Unique identification of alarm	
AlarmType	Alarm grouped into categories	Equip(-ment), env(-ironment), comm(-unication), process
Clearable	Boolean value to indicate if the alarm can be cleared or not. Some alarms does not have duration and therefore no Cleared severity	Checked/ Unchecked
Comment	Manual added text as comment to alarm	Text (latest only) (appear in history log)
DefAggr	N/A	
Duration	Time interval: From alarm was received to cleared alarm	hh:mm:ss
Ems Time	Timestamp set by AXX 9840 INSITE when the alarm was received	yyyy/mm/dd hh:mm:ss (server time)
Id	Unique sequence number to identify the alarm	
Layer rate	The layer rate in which the managed object belongs if applicable.	Not Applicable (any other layer rate supported by the network element) See Map viewer and Map Designer
Link	Alarm is associated with a link hence the alarm e.g color maps	user defined names on configured links
Location		

Attribute		Legal Values
Name	**Description**	
NE	Identification of the network element	
NativeValues	Unmapped trap data	(legal values depends on the network element)
NeTime	Timestamp from network element (if available)	yyyy/mm/dd hh:mm:ss
NumUpdated	How many times the alarm has been updated from a given Alarm Point (defined by Source and Alarm Identifier)	Numbers (1- n)
ProbCause	The probable cause of the alarm	(legal values depends on the network element)
ProbCauseQ	A probable cause qualifier if the probable cause itself is not sufficient to determine the exact error and source	(legal values depends on the network element)
PrvId	Previous Identification of notification	Sequence number
Severity	Severity of alarm	Critical, Major, Minor, Warning, Cleared, Indeterminate
Source	Identification of the network element that contains the source of the alarm.	Every managed objects available in Management Tree
Trend	Indication to report trends on severity change.	No Change, Less Severe, More Severe

3.6.3 Event notification

Event notification is a notification type that reports state change to managed objects.

The lists contains notification records with a set of information. Attribute names are listed in alphabetical order.

Table 29 Event notification attribute values

Attribute		
Name	**Description**	**Legal Values**
AddTxt	Additional text to explain the event	
Description	Additional text	
Ems Time	Timestamp set by AXX 9840 INSITE when the alarm was received	yyyy/mm/dd hh:mm:ss (server time)
EventId	Unique identification of event	
EventType	Event grouped into categories	Equip(-ment), env(-ironment), comm(-unication), process
Id	Unique sequence number to identify the event	
Moid	Identification of the network element that contains the source of the event.	A M.O in the Information Model for the equipment
Native Values	Unmapped trap data	(legal values depends on network element)
NE	Identification of the network element	
NeTime	Timestamp from network element (if available)	yyyy/mm/dd hh:mm:ss

3.6.4 Current alarm list

The Current Alarm List is a specialized dynamic view. This list presents alarm notification records, and present alarms in an active state, not cleared nor acknowledged.

You can scope, filter and sort the views. See “Notification Filter” on page 138 and “Rearrange views” on page 152.“Scope and filter notifications” on page 138.

Procedure: **VIEW CURRENT ALARMS**

1. Click on the **Current** tab to view current alarms.

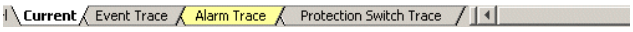


Figure 82 Current tab - Notification List

The **latest received alarm** is visible in the lower part of the Notification List.

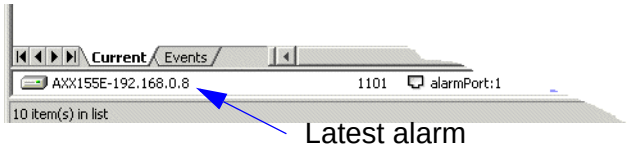


Figure 83 Latest alarm received

2. Click Refresh to update the Current List.

3.6.4.1 Select alarm(s)

Single selection

- Click on desired **single** alarm.

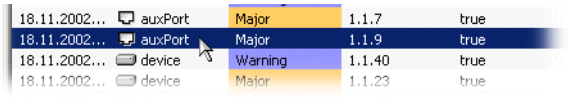


Figure 84 Select single alarm

Select all alarms

- Right- click in the list and choose **Select all**.

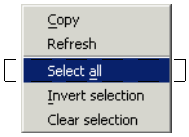
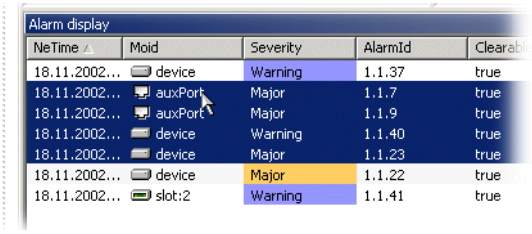


Figure 85 Select all alarms

Select alarms using keyboard

- Click on first alarm in a continuous range, **hold Shift- key** and click on last alarm in desired range.



Shift-key

Figure 86 Select alarms - continuos range

or,

- **Click** on first alarm, **hold Ctrl- key** and click on desired alarms to make none continuous selection.

.

Ctrl-key

Figure 87 Select alarms - none continuos range

You can also choose **Invert selection** or **Clear selection.**

Procedure: **COPY ALARM(S)**

1. Select desired alarm(s).
2. Click 

The contents of your selection is copied to the clipboard.

3. Select Text Editor from Tools menu**.**
4. Paste content from the clipboard.

NOTE! From the clipboard, paste the content to 3.rd party applications, such as Notepad or MS Excel.

3.6.5 Notification Trace List

The Trace Lists are dynamic views that present notifications from the moment the view is opened. Events, Alarms and Protection switches(AXX 9300 METRO) are reported and listed chronologically as messages from the network element state. The view contains no history, but is continuously updated whenever new notifications are received and/ or updated.

You can scope, filter, sort and clear the views. See “Notification List” on page 128.

Procedure: **VIEW TRACE LISTS**

- To view events reported from the network element, you select desired **Trace** tab in the Notification List.

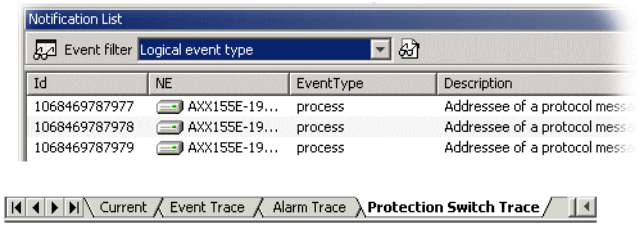


Figure 88 Events Trace Tab

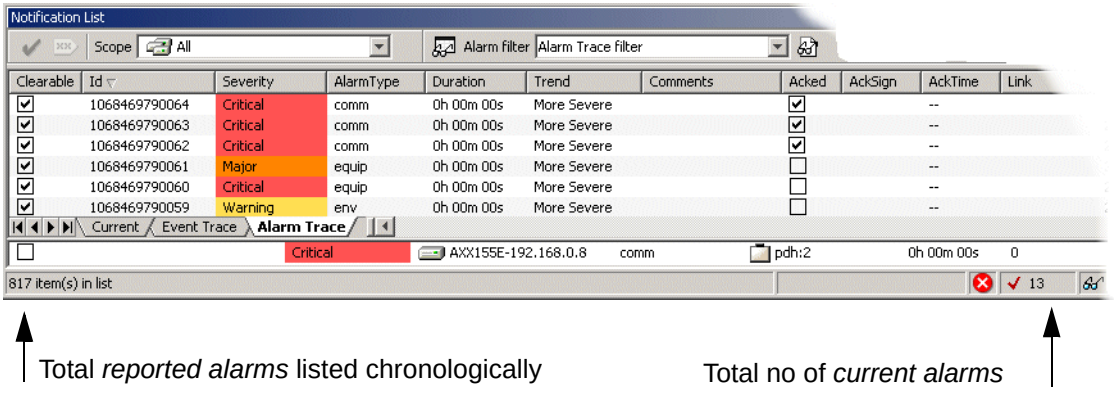
For details on the notification attributes, see “Event notification” on page 132.

Procedure: **VIEW ALARM TRACE LIST**

One alarm in Current alarm list may represent multiple alarms (items) in the Alarm Trace list.

1. Select **Alarm Trace** Tab in the Notification List.

2. View **all alarms** reported from the network elements.



Total *reported alarms* listed chronologically

Total no of *current alarms*

Figure 89 Alarm Trace Tab- example

Procedure: **CLEAR TRACE LISTS**

1. Select Trace Tab.
2. Right- click in the Trace list.
3. Choose **Clear list.**

The list is cleared and will be empty until new items are received.

3.6.6 Notification Filter

3.6.6.1 Scope and filter notifications

This section presents how to see a subset of notifications in the Notification list display, and introduces scope and filter to create such a notification selection.

You can at any time create, delete and modify a notification selection to all Notification List views.

TIP! The recommended way to make a selection: Scope the Notification List first to limit the selection. Then filter the list, to sort notifications in scope.

3.6.6.2 Scope setup

The scope is already set when a managed network element is selected in the Management Tree. A manually set Scope can result in a domain or a network element (Default scope = All)

Procedure: **SINGLE NE SCOPE**

1. Select **managed NE** in Management Tree.
2. **Right-click** in Management Tree.

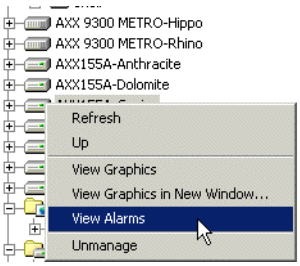


Figure 90 Management Tree - View alarms

3. Choose **View alarms**

AXX 9840 INSITE updates the Notification list with alarms for selected NE only.

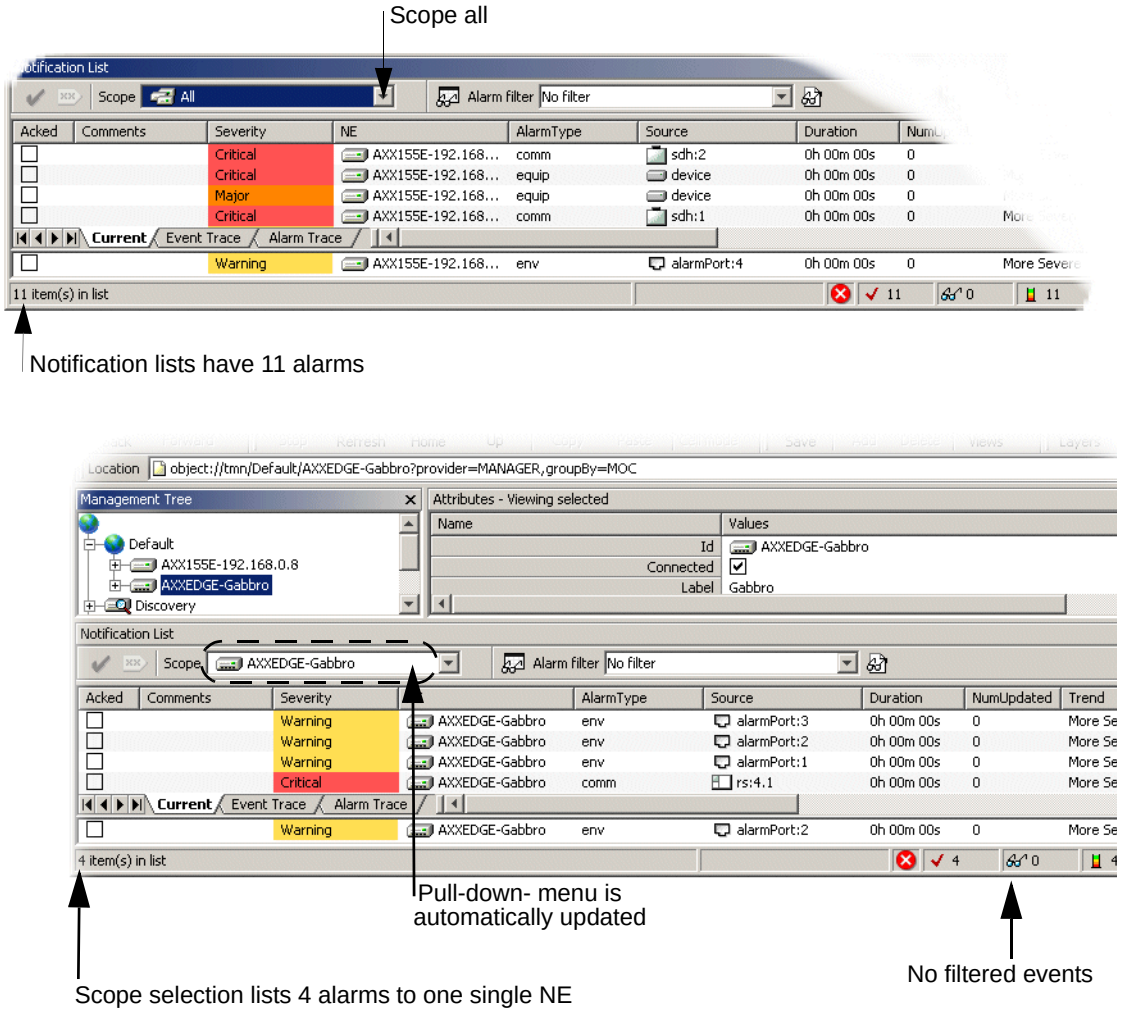


Figure 91 A single NE scope -1-

NOTE! The alternative method to make a scoped notification selection to one single NE is shown in Figure 92 The result is the same.

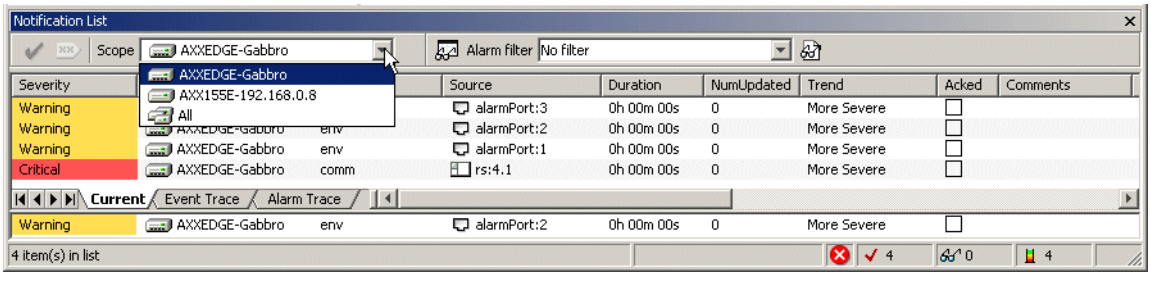


Figure 92 Single NE Scope -2-

Scope domain

1. Select **domain** from the **Scope menu** in the Notification List.

AXX 9840 INSITE scope list to a group of NEs (Domain), and Current List presents alarms to scope only.

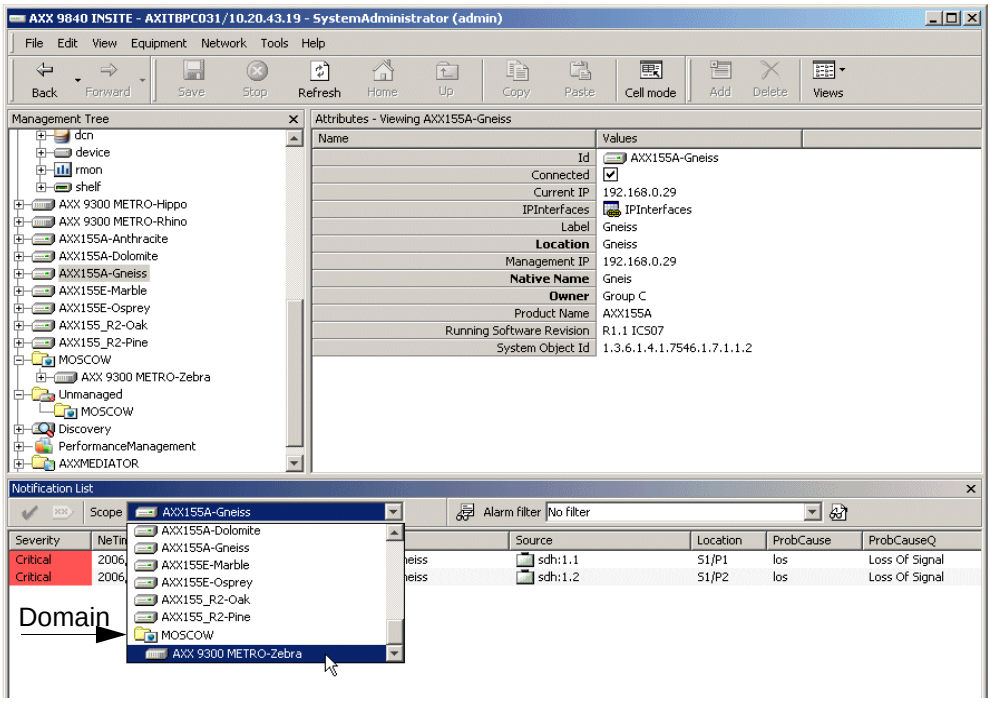


Figure 93 Scope Domain

3.6.6.3 Filter setup

Examples of filter criteria

- The notifications generated in a specific time interval
- Only alarms with a specific severity
- Only acknowledged alarms
- Alarms with a specific probable cause
- Events with a specific status
- Alarms from only one managed object

Table 30 Filter expressions

Expression	Description
AND	choose value and add as second criteria[a]
OR	choose value instead of first criteria if no response[b]
NOT	exclude value from list
>	value larger than...
<	value less than...
>=	value larger or equal to...
<=	value less or equal to...

a. AND: All of the criteria must be fulfilled or the filter will not return any items

b. OR: If you do not choose any expression when adding criteria, AXX 9840 INSITE will automatically use OR

Procedure: **CREATE A SINGLE FILTER**

1. Click the **Configure filter** icon in Notificatior

AXX 9840 INSITE opens the Alarm Notification List Filter.

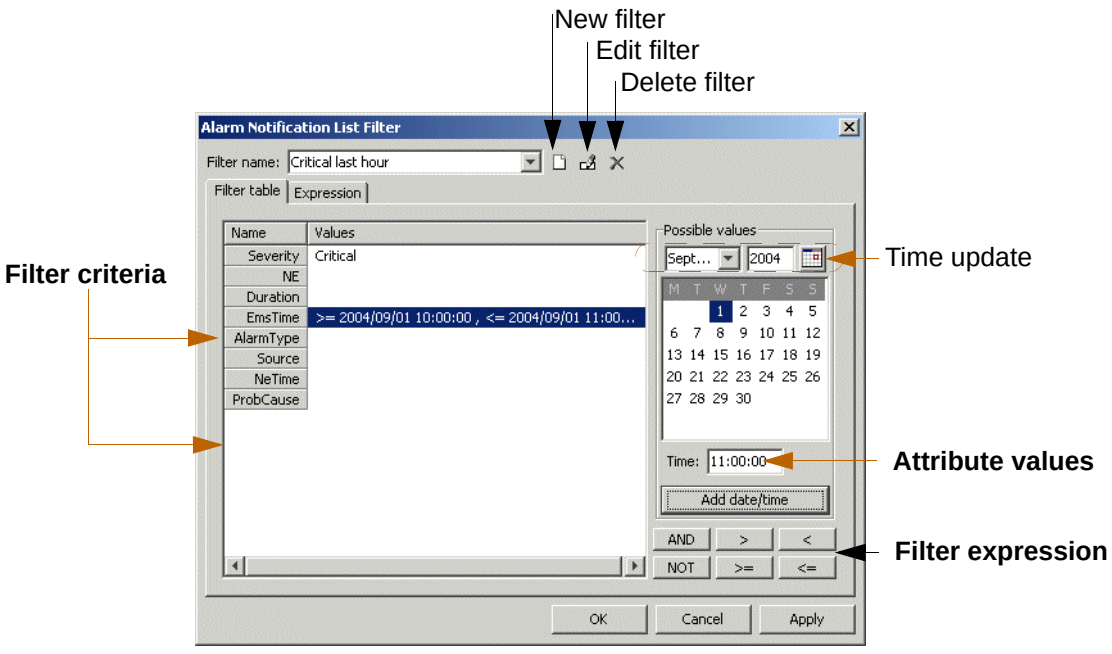


Figure 94 Filter menu- example

Example of time interval: Critical alarms latest hour (10:00 to 11:00)

Select type of time criteria (EMS time), set time value to larger or equal to 10:00, press AND and press expression less or equal to 11:00.

2. Click **New** filter icon in Filter menu.
3. Enter **Name** to filter and press enter.
4. Select **Criteria** to filter from Filter table.

Possible values are listed in window to the right.

5. Select **Value** and double-click.

Value is added to selected filter criteria.

6. Select a **new** filter criteria and value.
7. Click **OK.**

AXX 9840 INSITE adds the filter to Filter list.

Procedure: **VIEW FILTERED NOTIFICATION LIST**

1. Select **Filter** from pull-down menu in **Notification List.**

AXX 9840 INSITE presents a filtered notification list.

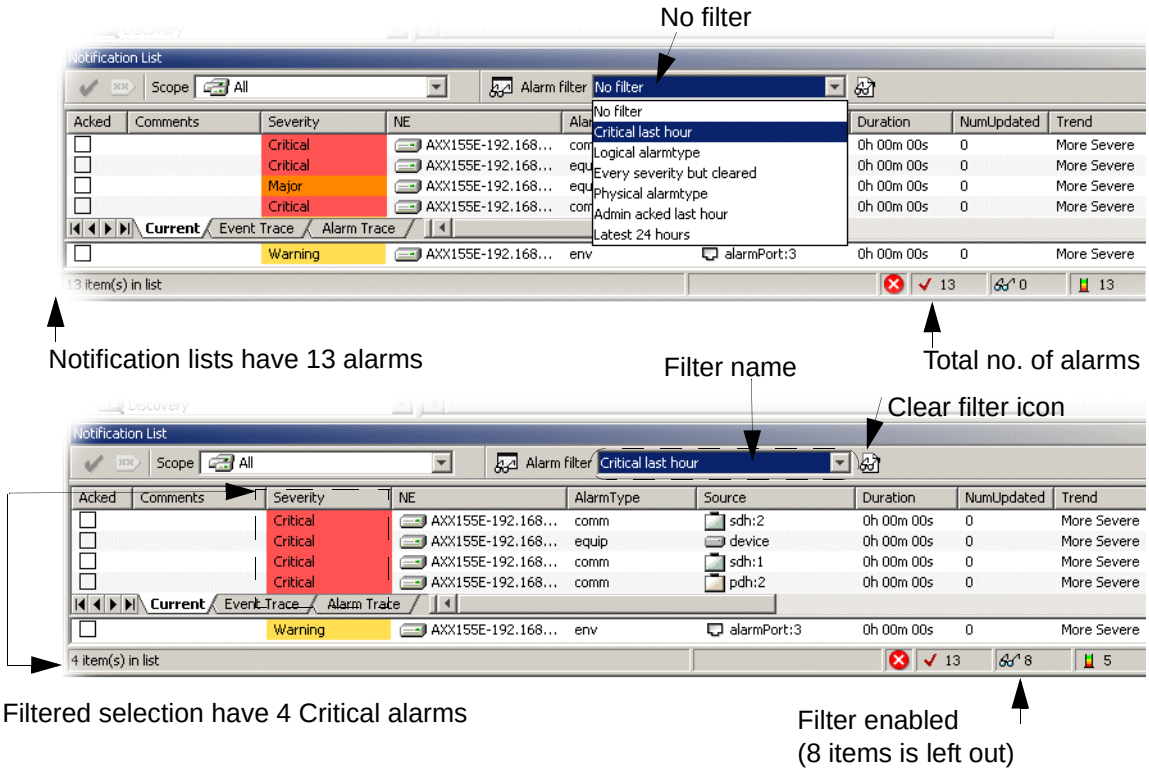


Figure 95 Filter selection in Current alarm list

NOTE! Latest alarm is displayed in the Notification List independent to any filter.

Procedure: **MODIFY FILTER NAME**

1. Open **Alarm Notification List I**
2. Select **Filter**.
3. Click **Edit** icon.
4. **Rename** filter selected and press **Enter**.
5. Click **OK**.

The selected filter has a new name. No changes have been made to the filter setup.

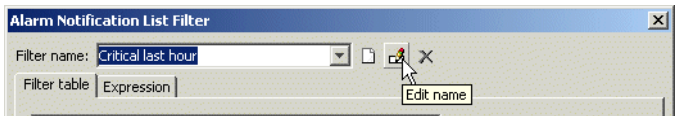


Figure 96 Modify filter name

Procedure: **MODIFY FILTER CONTENT**

1. Open Alarm Notification List Filt
2. **View** filter setup in Expression table.
3. **Modify** content (attribute values).
4. Click **OK**.

NOTE! The selected filter has a new content. Be aware of the filter name.

Procedure: **DELETE FILTER SELECTION**

1. Open Alarm Notification List F
2. Select **desired filter** from menu.

3. Click **Delete**.
4. Click **OK**.

The Filter is removed from Filter pull-down menu in Notification List.

Recommended selection to Notification List

You can create and present an effective notification list with a combination of scope and filter selection.

1. Choose **Scope** from pull-down menu.

2. Choose **Filter** from pull-down menu.

AXX 9840 INSITE presents a selection of notifications to the given scope and filter.

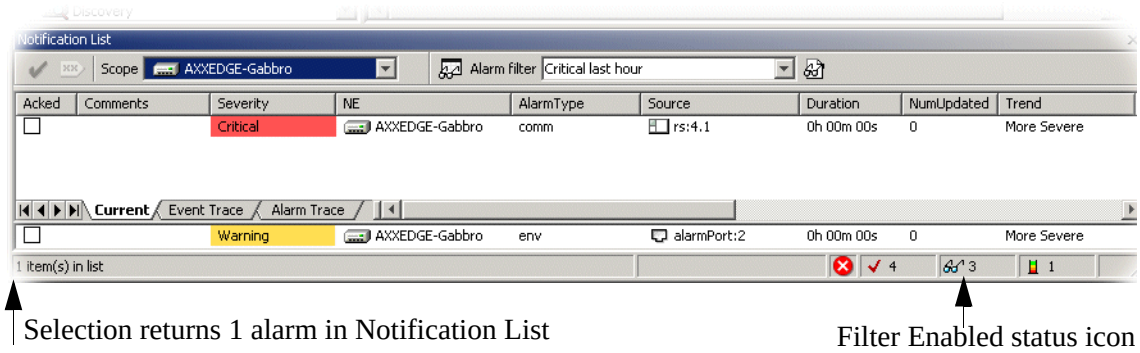


Figure 97 Example of combined notification selection

3.6.6.4 Clear filter and scope in Notification List

Clear Filter

1. Click **Clear filter** icon in Notification List. 

The Notification List is unfiltered.

NOTE! Be aware of possible Scope. The Notification list may not be complete.

Clear Scope

1. Select **All** in **Scope** pull-down menu

The Notification list is unscoped.

NOTE! Be aware of possible Filter. The Notification List may not be complete.

3.6.7 Acknowledge and comment notifications

This section describes how you can acknowledge and comment notifications presented in the Notification List. All users will be notified of such actions.

Use the Current Alarm List to comment and/ or acknowledge any alarm notification(s). Acknowledged alarms are removed from this list. You can trace alarms and view acknowledgements and comments in the Alarm Trace and the Notification History.

Procedure: **ACKNOWLEDGE CURRENT ALARM NOTIFICATION**

1. Select **desired alarm** from the Current Alarm List.
2. Click the **Acknowledge**- icon from Notification List.

The notification is tagged with an acknowledgement mark, userid and timestamp.

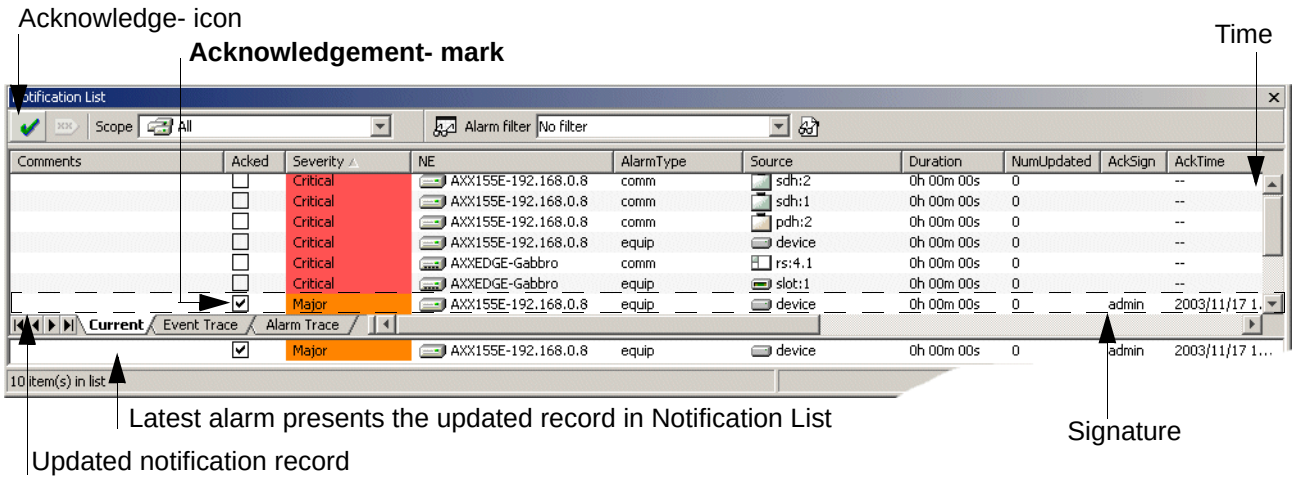


Figure 98 A single acknowledged notification

See “Select alarm(s)” on page 134 for multiple acknowledgements.

NOTE! Existing acknowledgements cannot be cancelled.

Procedure: ADD COMMENT TO CURRENT ALARM NOTIFICATIONS

1. Select **desired alarm** from Current Alarm List.
2. Click the **Comment** icon from Notification List.

AXX 9840 INSITE opens the comment text box.

3. **Enter** a comment **text**.

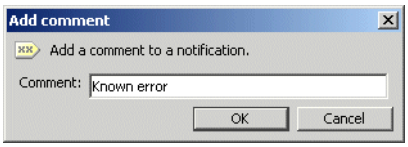


Figure 99 Comment text box

4. Click **OK.**

The Notification List updates the notification record with the comment text and your user-id.

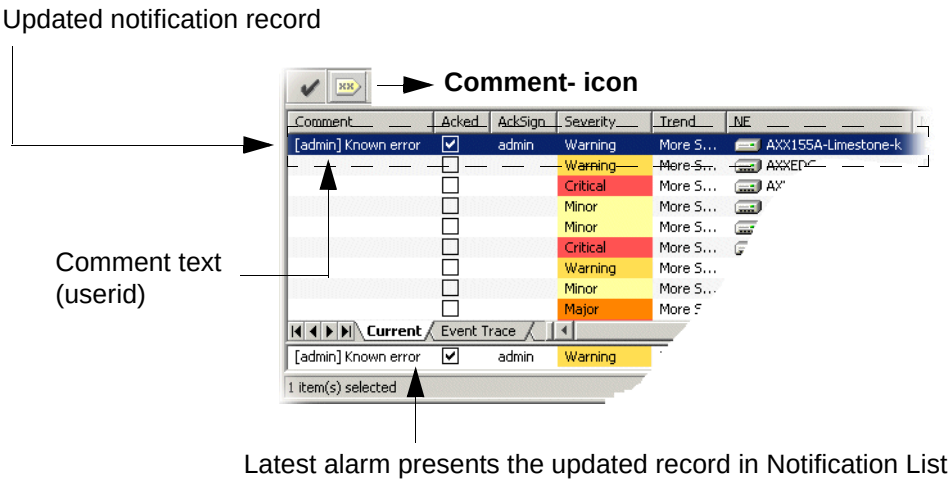


Figure 100 Notification comment

Comments to more than one alarm notification results in the same comment to all the notifications. See “Select alarm(s)” on page 134 for multiple notification comments.

NOTE! Existing comments cannot be edited or removed. Click Cancel to close dialog box.

Procedure: **VIEW ACKNOWLEDGEMENTS AND COMMENTS**

READ MORE: See “” on page 141 and “Rearrange views” on page 152

Procedure: **TRACE ACKNOWLEDGEMENTS AND COMMENTS**

1. Select **Alarm Trace Tab** in Notification List.
2. **Click** the **Acked** and/ or **Comment column**(s) **heading**(s).

The list is sorted by your choice.

3. Select predefined filter.
4. View selected alarm trace.

NOTE! Please see “” on page 149 to view the history list.

3.6.8 Notification History List

The Historical Lists present the notifications received from the network elements up to the time the view is opened. You can scope, filter and sort the lists.

NOTE! Click Refresh to load the recent history. The view might be empty until a load is yet to be performed.

The history log on the network element can be cleared through an action on the Log Administration attribute of the device.

Procedure: **VIEW ALARM HISTORY**

To get a list of all alarm notifications reported on the network element since the last restart of the network element, or the last clear of the history list in the network element:

For attribute details, see “Alarm notifications” on page 130

1. Select **Notification History** from **Equipment menu**.

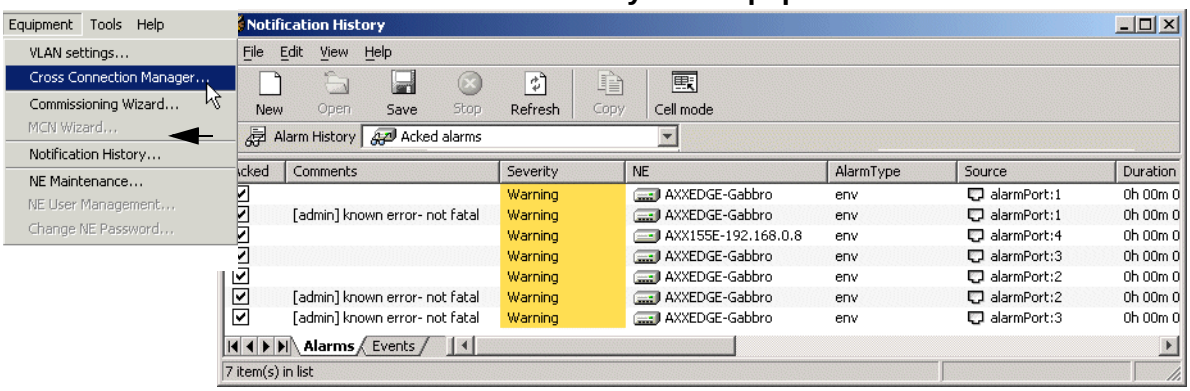


Figure 101 Notification history- Alarms

2. Click **Refresh.**

AXX 9840 INSITE collects the notification history logs.

3. Select **Alarm Tab** to view alarm history.

4. **Scope and/ or filter list**.

The Notification History application is able to retrieve the alarm log directly from the equipment, or it can perform a query in the database.

By clicking on the icon on the left side in the toolbar a filter-dialog will appear. This filter will be used against the database.

In the drop-down list, filters and the Network Elements will appear.

- If a filter is selected the alarms in the database will be presented.
- If a Network Element is selected all alarms from the Network Element will be retrieved.

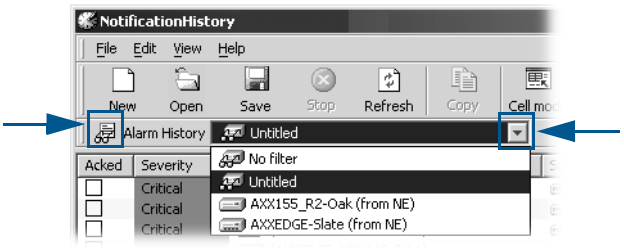


Figure 102 Notification History

Procedure: **VIEW EVENT HISTORY**

For attribute details, see “Event notification” on page 132

1. Select **Notification History** from **Equipment** menu.
2. Select **Event Tab** to view event history.
3. **Scope and/ or filter** list (Network Element and/ or History Database)

.

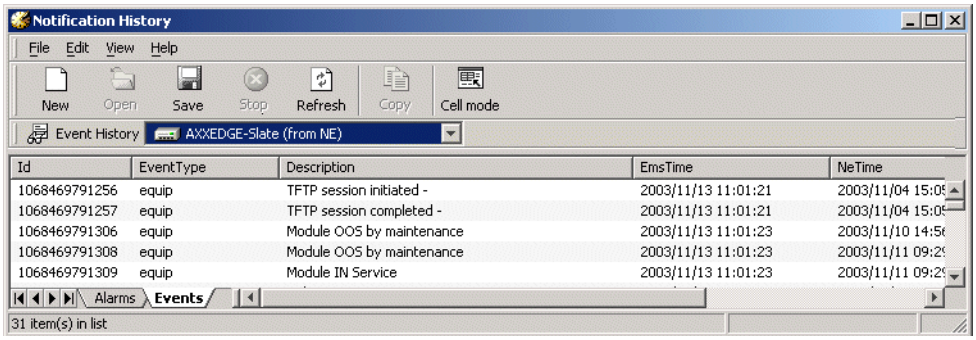


Figure 103 Event History

Procedure: **SAVE HISTORY LOG(S)**

1. Select history log (alarm or event tab).
2. Press **Save** from the toolbar.

The file browser is opened.

3. Browse directory and enter file name.
4. Press **Save** in file browser.

The selected history log (alarm or event) is saved as an xml-file to local or remote directory. You can see the destination in the window title field:

5. The next time you press **Save**, you will not be prompted for a filename. The log you saved will be updated. Use **File>Save As** if you want to save under a new name.

Procedure: **OPEN HISTORY LOG(S)**

1. Press **Open** from the toolbar
   The file browser is opened.
2. Browse the directory and find the previously saved alarm or event log file.
   Example: alarmlog.data.xml
3. Double click the file to display the saved alarms or events in the viewer.
   A new tab with the name of the opened file will appear:

4. You can now view the list, copy from it or print a report.

3.6.9 Rearrange views

Procedure: **PRESENT COLUMNS IN VIEW**

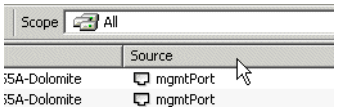
You can choose which columns to be visible in the Notification List. See Table 28 and Table 29

1. Select desired **Tab** in Notification List.
2. Right-click the column heading and select **Columns.**

Available columns for given Notification List are listed (checked in default view)

3. **Uncheck** undesired column(s) and they are no longer visible in the Notification List..

Right click column heading



Select columns

Figure 104 Visible columns

Procedure: **CHANGE COLUMN ORDER**

1. Click and hold the column heading.

2. **Drag** and **drop** the column to **new position**.
   The columns switch places in view.

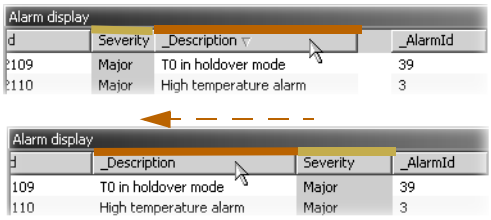


Figure 105 Column order

Procedure: **RESIZE COLUMN(S)**

1. **Rest** the mouse pointer **to the right** of **desired column header**.

The mouse pointer turns into a double-arrow.

2. **Click** and **drag** to s**uitable column-size.**

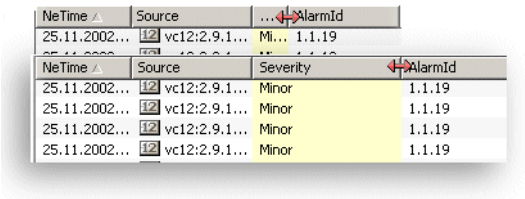


Figure 106 Column size

Procedure: **SORT COLUMNS**

1. **Click** on **desired column** to **sort ascending.**

The columns set an arrow to indicate sorting

2. **Click again** to sort **descending.**

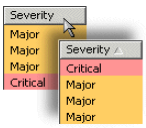


Figure 107 Column sorting

3.7 Map Viewer

The purpose of this chapter is to describe how AXX 9840 INSITE presents a graphical view of the network element, i.e., the internal managed objects in one network element.

The graphical objects representing the managed object instances and attributes reflect changes in alarm status, attribute value changes, state changes on the managed object instance and show managed object instances creation and deletion.

A view is in the context of this chapter; a view that presents graphical objects representing managed objects and attributes, also called a map view. Has nothing to do with geographical maps.

AXX 9840 INSITE presents a default map view in the desktop. Other views are available from a popup menu on the managed objects and attributes. Which type of view to present as default for an object or an attribute, is by your choice.

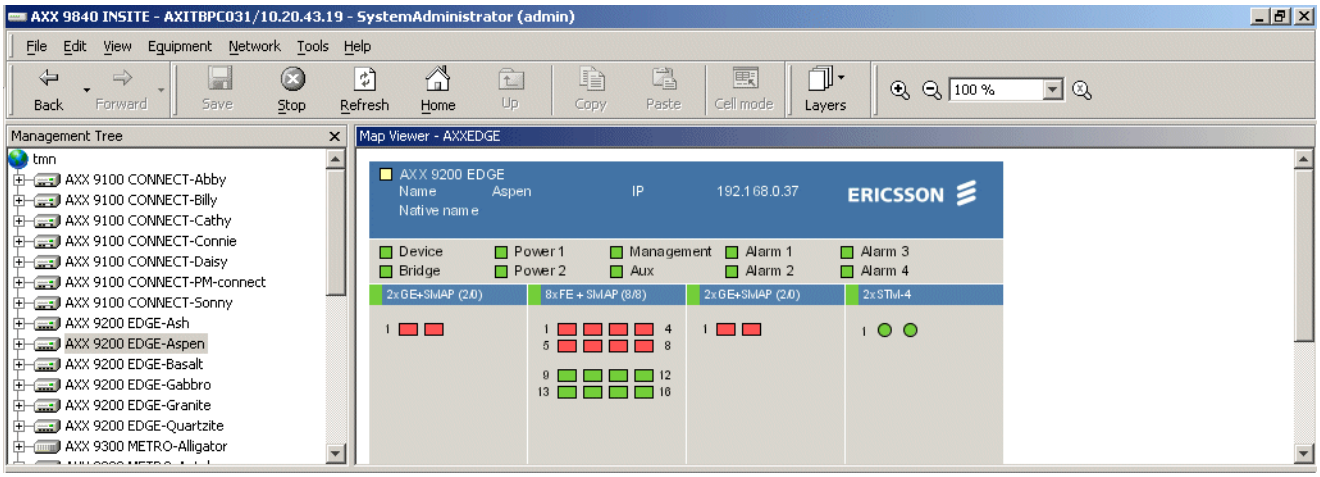


Figure 108 Example of map view

NOTE! For Zoom options, see page 3-80

Inconsistent numbering of physical and logical ports

In previous versions of the standard NE maps, the GUI labels have been following the port numbering on the physical modules. (E.g., in an AXX10, the LAN ports are numbered 1 - 4 on the HW unit. In the management tree, however, they are identified as lan:3.3.6 - lan:3.3.9. In the old maps, they were numbered 1 - 4.) This inconsistency has been confusing , and we have chosen to

harmonize between the two applications in the management system: Management Tree and the MapViewer. Consequently, The ports are now numbered 6 - 9 in the maps as well.

Numbering on the HW units may deviate from what is shown on screen.

3.7.1 Open Map Viewer

1. **Select** a network element in Management Tree
2. **Right-click** and select **View Graphics** or **View Graphics in New Window** if you want to monitor several maps at the same time.

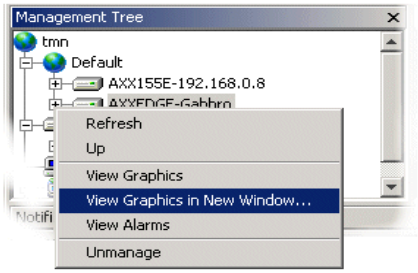
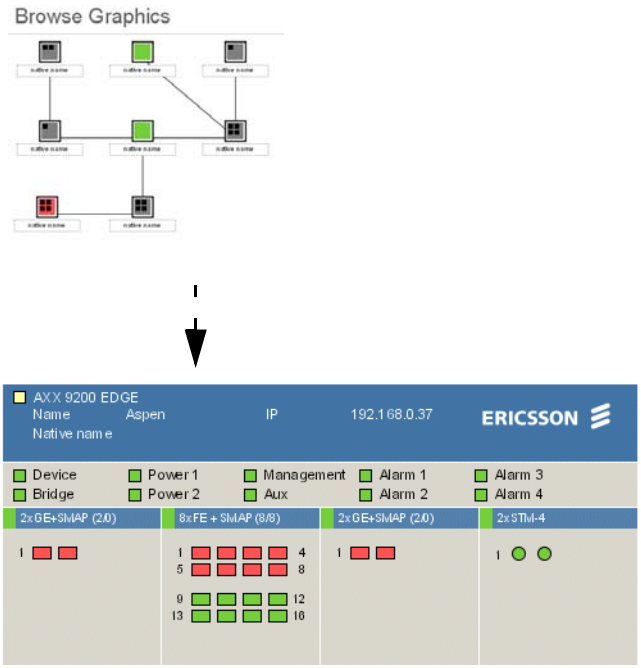


Figure 109 View Graphics

or,

1. C**lick** on desired network element **in overview map**.



To navigate: 

Figure 110 Graphic view- example of AXX155E

AXX 9840 INSITE presents a graphical view with a defined set of managed objects within the element represented by graphical objects.

1. Or, select **Map Viewer** from the **Tools** menu.

AXX 9840 INSITE opens the Map Viewer in a new window

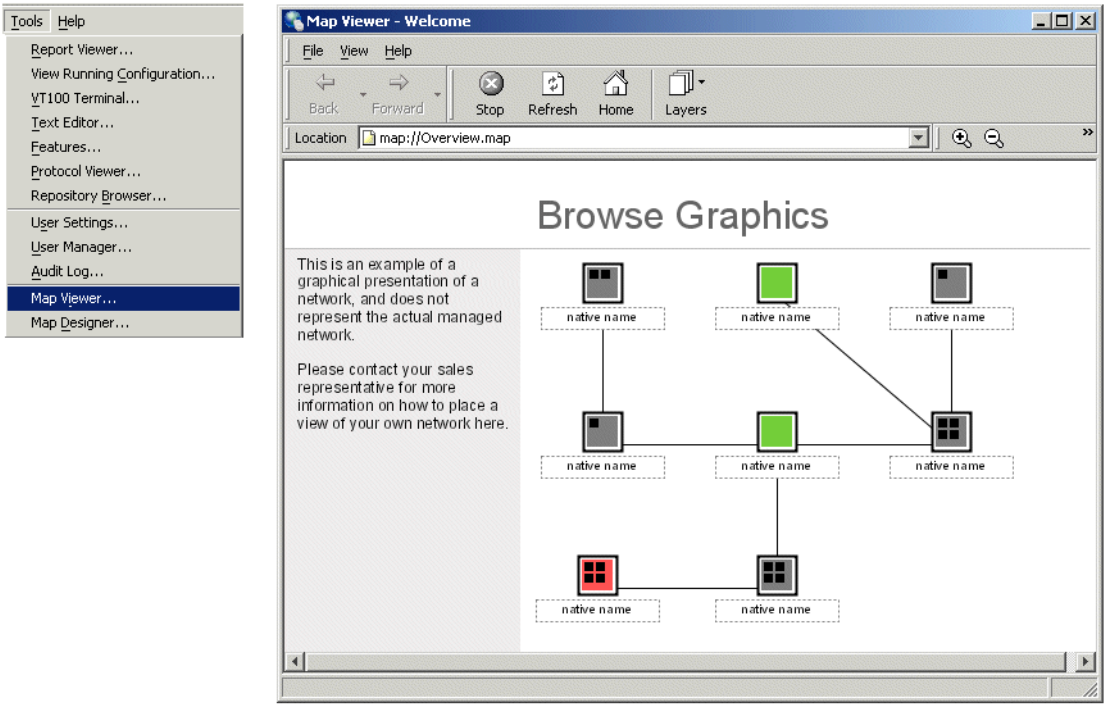


Figure 111 Map Viewer in dedicated window

3.7.2 Current alarm status

The graphical objects for managed objects reflect the current alarm status of the managed objects. The alarm with the highest severity currently reported on the managed object determine the color of the object.

If an alarm is generated on a managed object on the network element you are currently looking at, AXX 9840 INSITE might change the color of the managed object in the graphical view. The color is determined by the alarm with the highest severity reported on the managed object at the time.

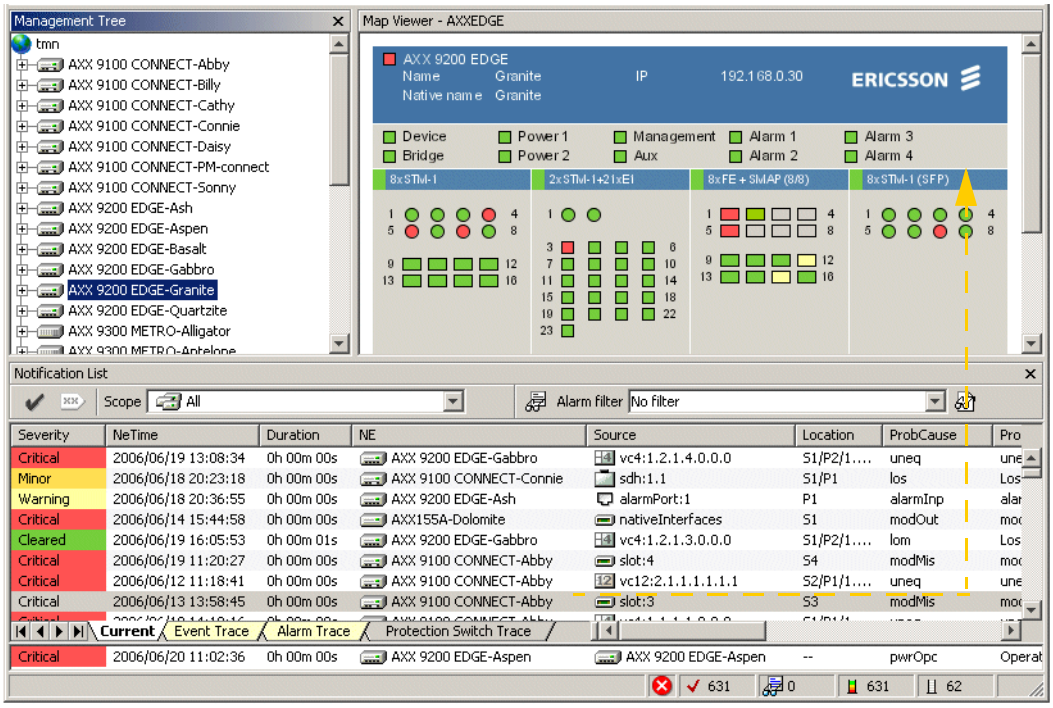


Figure 112 Example of graphical objects for MO reflecting alarm status

TIP! Zoom to make size of view as desired

3.7.3 Visualization of object create/delete

AXX 9840 INSITE supports visualization of object create and object delete operations.

If you e.g. remove an installed module in an AXX 9200 EDGE slot and replace it with another type, this will be reflected in the graphical objects.

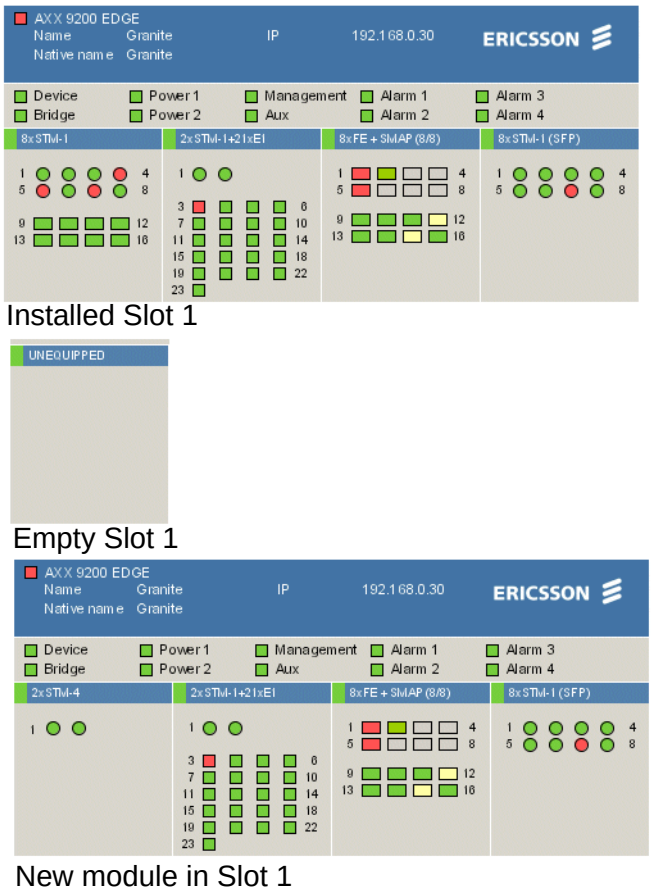


Figure 113 Visualization of object create/delete

3.8 Topology Editor

3.8.1 Introduction

The topology editor's main task is to identify and store physical port-to-port interconnections between NEs in a network of managed Ericsson AXXESSIT NEs. The ports can be connected through electrical, optical or radio media, and the traffic can be of different nature, such as Ethernet/IP or SDH.

The topology information is stored in a persistent repository as *.xml files.

The repository information is crucial for:

- Map presentations of physical connectivity between NEs.
- Basis End to End routing with information about available physical routes through the network.

3.8.2 Start the Topology Editor

1. From the **Network** menu select **Topology Editor**.

Figure 114 Network menu

2. The application will now display user defined links that are already stored in the repository.

NOTE! See the "Topology Discovery Wizard" on page 165 to perform a search on existing topological links based on OSPF data stored in the managed NEs.

3.8.3 Overview

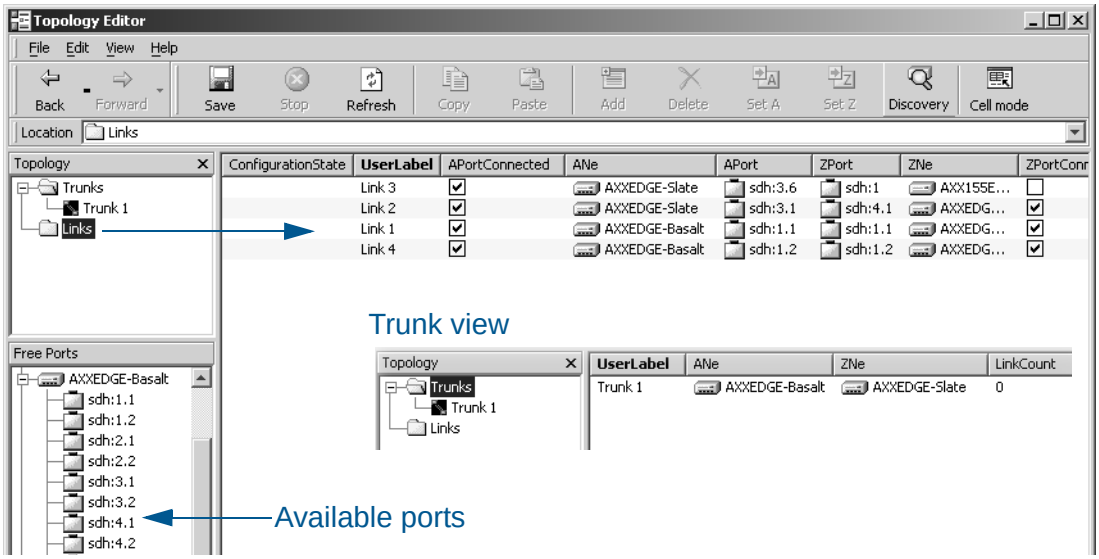


Figure 115 Topology Editor - Overview

3.8.4 Menu Items

File menu

Menu item	Description	Toolbar Icon	Hot Key
Save	Saves contents		Ctrl + S
Close	Close Topology Editor		Alt + F4

Table 31 File menu

Edit menu

Menu item	Description	Toolbar Icon	Hot Key
Copy	Copy selected items		Ctrl + C
Paste	Paste content on clipboard		Ctrl + V
Add	Add new link		Ctrl + N
Delete	Deletes the selected items		Delete

Menu item	Description	Toolbar Icon	Hot Key
Set A	Set selected port to A-port in link		
Set Z	Set selected port to Z-port in link		
Select All	Select all items		Ctrl + A
Clear Selection	Clears current selection		
Invert Selection	Inverts the current selection		
Cell Mode	Toggle between row and cell selection		

Table 32 Edit menu

View menu

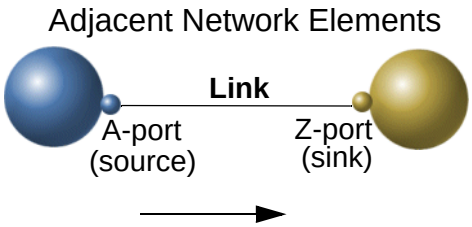
Menu item	Description	Toolbar Icon	Hot Key
Stop	Stops loading of items		
Content pane	Toggle the content pane		
Refresh			F5

Table 33 View menu

3.8.5 Links

Introduction

This section shows how to create links between adjacent network elements. Please see “Trunks” on page 164 and note that “View the network topology” on page 166 explains how trunks and links are displayed in topological maps.



Procedure: **CREATE A LINK**

The procedure below assumes that the involved NEs have physical connections between the ports used in the example.

1. Double-click desired **A-port** in the Content pane.

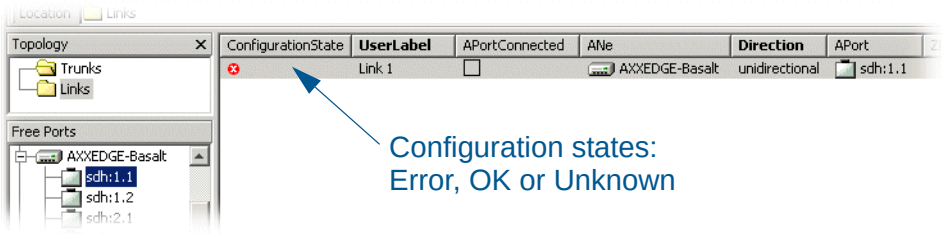


Figure 116 A-port selected

2. Double-click desired **Z-port**
3. Edit the following Link attributes:
   - **User label**: default Link n +1
   - **Additional information**: Free text field.
4. Click **Save.**

Remove Link

1. **Select** desired Link and **right-click**.

2. Select **Delete** from the menu.

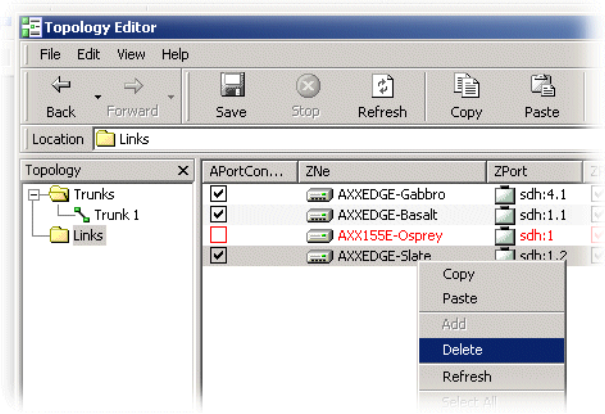


Figure 117 Link - Delete

3. Click **Save**.

3.8.6 Trunks

Introduction

A trunk is a grouping of topological links between two NEs, and is intended to provide a common presentation alternative for several parallel topological links in a graphical map view.

When two or more links have been created, a trunk is automatically created between the actual NEs and given the name of the NEs in the connection. See the figure below.

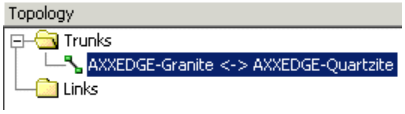


Figure 118 Trunk Identification

NOTE! The Trunks are automatically generated, and cannot be modified.

“View the network topology” on page 166 explains how trunks and links are displayed in topological maps.

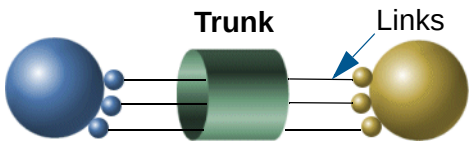


Figure 119 Links grouped as trunk

3.8.7 Topology Discovery Wizard

The Topology Discovery Wizard will help you to discover links that are not discovered during the automatic search of the Topology Browser application. You can scope the search by selecting specific NEs, and then choose which discovered links to add to the topology repository.

1. Open th ard with the discovery icon on the icon toolbar. 

2. Read the Welcome introduction window. Press next.

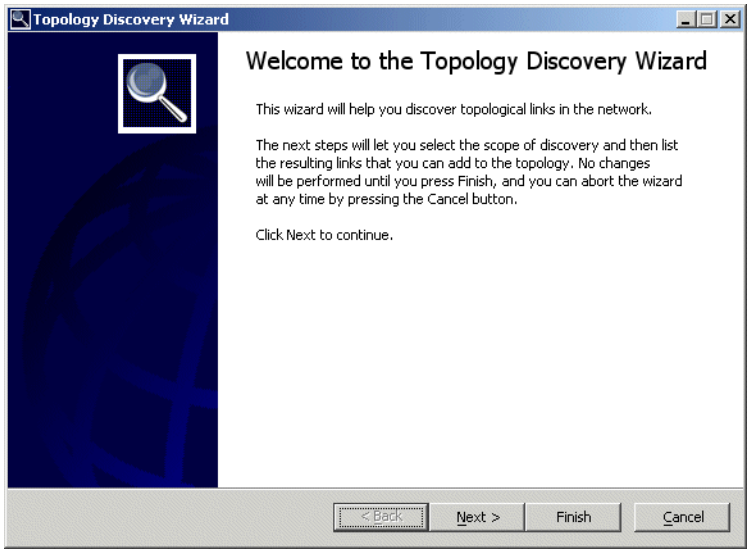


Figure 120 Welcome to the topology Discovery Wizard

3. Decide the scope of the discovery. Only links to the selected NEs will be shown.

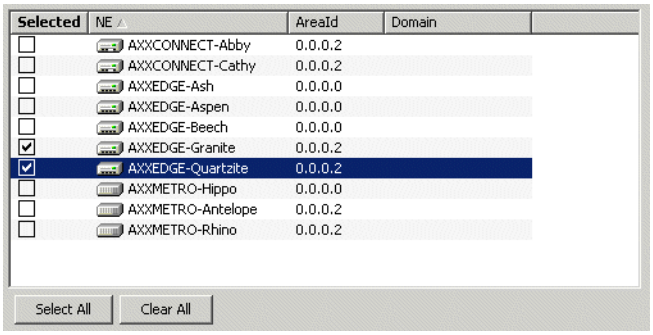
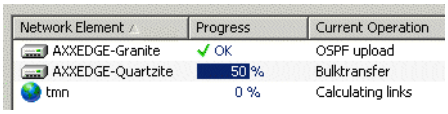
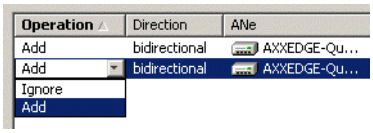


Figure 121 Select NEs for link discovery

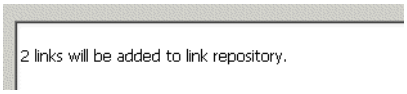
4. Discovering links. This step shows the status of the search.



5. The wizard lists the discovered links, and you can select the ones you want to add to the topology database.



Press Next, and see a summary of the operations:



Press Finish, and see the result of the operations:

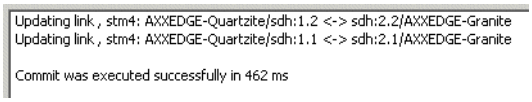


Figure 122 Add discovered link to the topology database

6. Press Close to exit the wizard.

3.8.8 View the network topology

3.8.8.1 Introduction

Physical topology maps can be created manually or automatically.

3.8.8.2 Manual Topology View building

Please see the Map Designer User Guide for further information on manual Topology View building.

3.8.9 Topological Links in the Map View

Topology View building - automatic

AXX 9840 INSITE has a set of template views for building physical topology views. If the topological links are already present in the topology repository, they will appear automatically on the map when both the terminating network elements exist within the current map view instance.

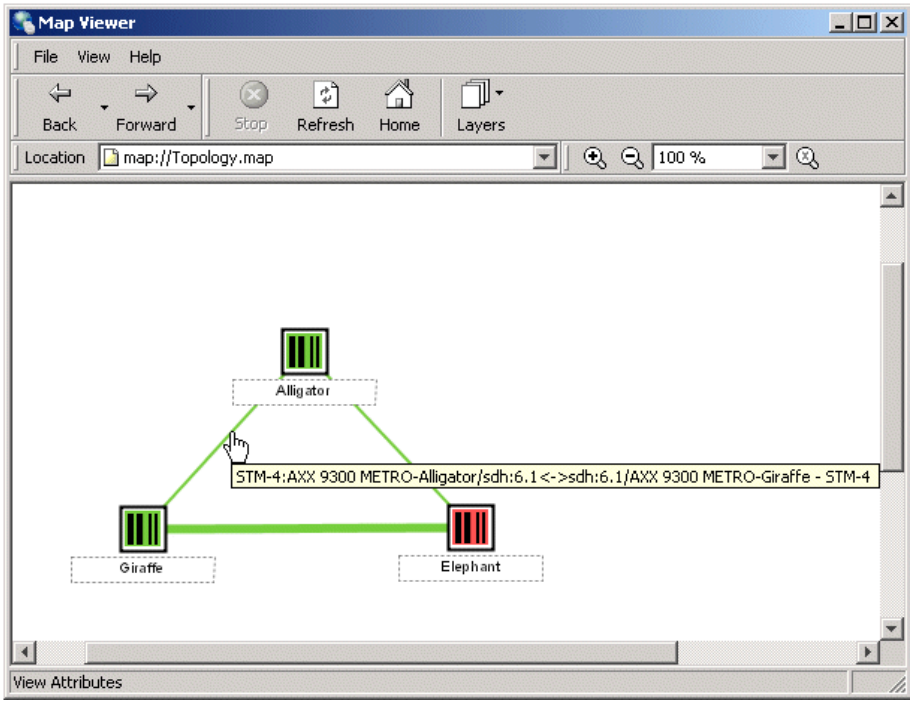


Figure 123 Topology View building

3.8.10 Dynamic Alarm Presentation in Map View

A topological link has an alarm state and a connection state (connected, unconnected, online, off-line). The alarm and connection state are deducted from the status of the links associated network element ports, and is mapped to the topological links.

If an alarm affects the link, AXX 9840 INSITE generates a new notification with the topological link as source managed objects.

The link-alarm with the highest severity decides the graphical presentation of the alarm situation. In case of trunks, link alarms are propagated from the link objects to the trunk object.

3.8.11 Mapped network element alarms

The link alarms are mapped from the **sdhPort**, **MS** and **RS** managed objects, and are presented graphically through coloring of the link object. The mappable alarms are:

- LOS (loss of signal)
- LOF (loss of frame)
- LOM (loss of multiframe alignment)
- Degraded Signal Defect
- Remote Defect Indication
- Trace Identifier Mismatch
- Excessive Error Defect
- Communication Subsystem Failure
- MSP Signalling Failure
- Out of Frame

4 MCN setup

4.1 The MCN Wizard

MCN - Management Communication Network

4.1.1 NE Management Introduction

The main purpose of an Ericsson AXXESSIT NE is to transport Ethernet and PDH (E1/E3/T3) data over an SDH network. The transmitted data is referred to as customer traffic. Independently, the NEs must be monitored and configured from one or more AXX 9800 TMN management stations. The data sent between the NEs and management stations is referred to as management traffic, and the network over which it flows is the MCN.

It may be surprising to learn, but the effort to design the MCN for management traffic often exceeds the effort to design the customer traffic network. This is not specific to Ericsson AXXESSIT, but a common trait of most network types, including telecommunication networks and company data networks. Although designing the MCN can be challenging, after the design is complete, Ericsson AXXESSIT has assured that configuring the NEs is not.

4.1.2 MCN Wizard Introduction

This chapter describes how to configure an NE for management using the MCN Wizard. The wizard is a pop-up window that makes management configuration simple. Management can alternatively be configured from a management station’s Desktop. The wizard offers no additional or hidden features that can’t be configured from the Desktop. Some management configuration can only be done from the Desktop.

NOTE! This chapter explains the use of the MCN Wizard. Although descriptions explain what each setup step does, this chapter does not provide an in-depth discussion of management.
This chapter does not cover every management related attribute or every attribute value, nor does it address access right limitations based on roles.
Design of an MCN network, which involves the consideration of

multiple NEs and the SDH network itself, is beyond the scope of the chapter.
A more in-depth description of management is can be found in chapter the “General management”.

NOTE! The MCN Wizard supports many network element types, but this chapter focuses solely on the AXX 9300 METRO, AXX 9200 EDGE and AXX 9100 CONNECT.

NOTE! The chapter assumes that the user has successfully connected to the NE through a management station.

NOTE! The MCN Wizard makes no changes to an NE until the entire configuration has been completed and the user confirms the changes. It is therefore safe to “play” with the wizard as long as the changes are not saved.

4.1.3 IP Numbered, IP Unnumbered, and System Mode

NOTE! Although the goal of this chapter is to avoid advanced technical information, a simple description of IP Numbered, IP Unnumbered and System Mode is required.

All NE types are managed using protocols transmitted in IP (Internet Protocol) packets. Multiple protocols are used for management, and the AXX 9300 METRO uses different protocols then other Ericsson AXXESSIT NE types, but all management relies on IP.

Typically in IP networks, every network interface is assigned a unique IP address. A special technique, IP Unnumbered, allows an interface to share an address of another interface from the same computer. Any interface with its own IP address is numbered. Any interface sharing another’s IP address is unnumbered.

Some of the Ericsson AXXESSIT management techniques use IP Unnumbered interfaces. IP Unnumbered offers greater flexibility, simpler MCN design, and is recommend for the majority of MCNs.

An AXX 9300 METRO can use a combination of IP Numbered and unnumbered interfaces. On an AXX 9200 EDGE or AXX 9100 CONNECT, the entire NE must be set up for IP Numbered or IP Unnumbered. The choice is known as the System Mode. Setting the

System Mode is a fundamental strategic choice that is done from the AXXCLI on an unconfigured NE.

For the AXX 9200 EDGE and AXX 9100 CONNECT, the MCN Wizard support is limited to IP Numbered System Mode. The MCN Wizard will start on an NE in IP Unnumbered mode, but before any configuration can be assigned, the user will be informed that the mode is unsupported.

NOTE! The remainder of this chapter is only applicable to AXX 9200 EDGEs and AXX 9100 CONNECTs in IP Numbered mode, as well as to all AXX 9300 METROs.

4.1.4 Starting the MCN Wizard

The MCN Wizard is a pop-up window started from the management station's Desktop.

Select **Equipment > MCN Wizard...** from the Desktop's menu bar.

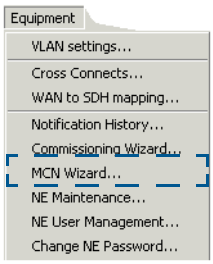


Figure 124 Equipment menu

4.1.5 Setup Step - Welcome to the MCN Wizard

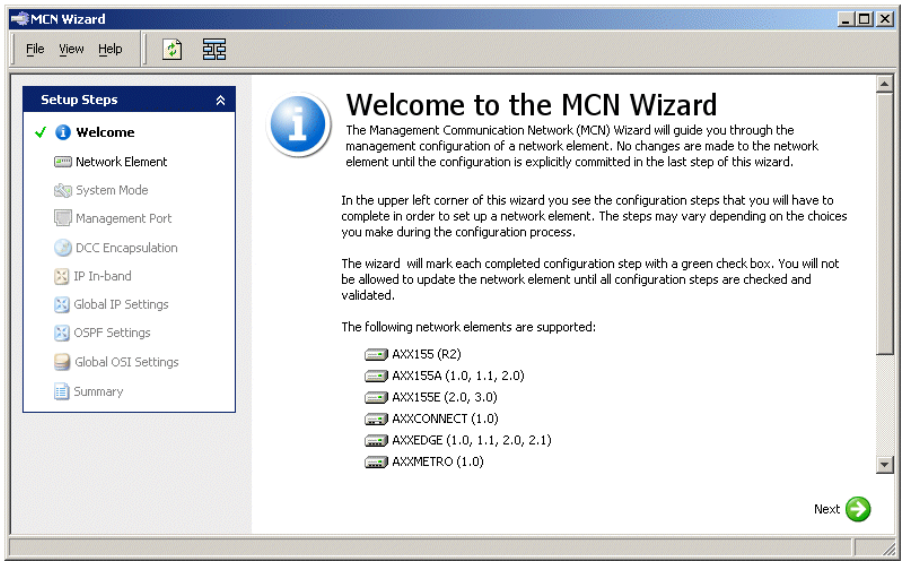


Figure 125 Welcome to the MCN Wizard

The MCN Wizard is split into two panes, one left and one right.The wizard begins by introducing itself with a welcome message on the right side pane.

The left side pane is a list of the setup steps. The user is prompted for information at each step. To move from step to step, click “Next” in the lower right of the window.

There are differences in the left side pane depending on the NE type. When the wizard starts and is showing the welcome message, the setup steps are generic and not yet NE type specific. See the figure below, the AXX 9300 METRO (left) and the AXX 9100 CONNECT and the AXX 9200 EDGE (right)

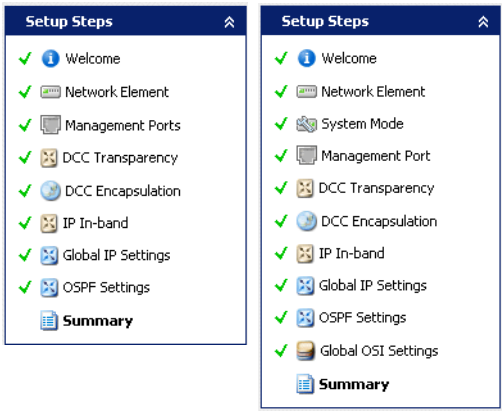


Figure 126 Setup Steps

4.1.6 Setup Step - Network Element

The Network Element setup step allows the user to select the NE to be configured. After an NE is selected, management information about the NE is listed. The exact information shown, varies with the NE type. Nothing on the NE is configured in this setup step.

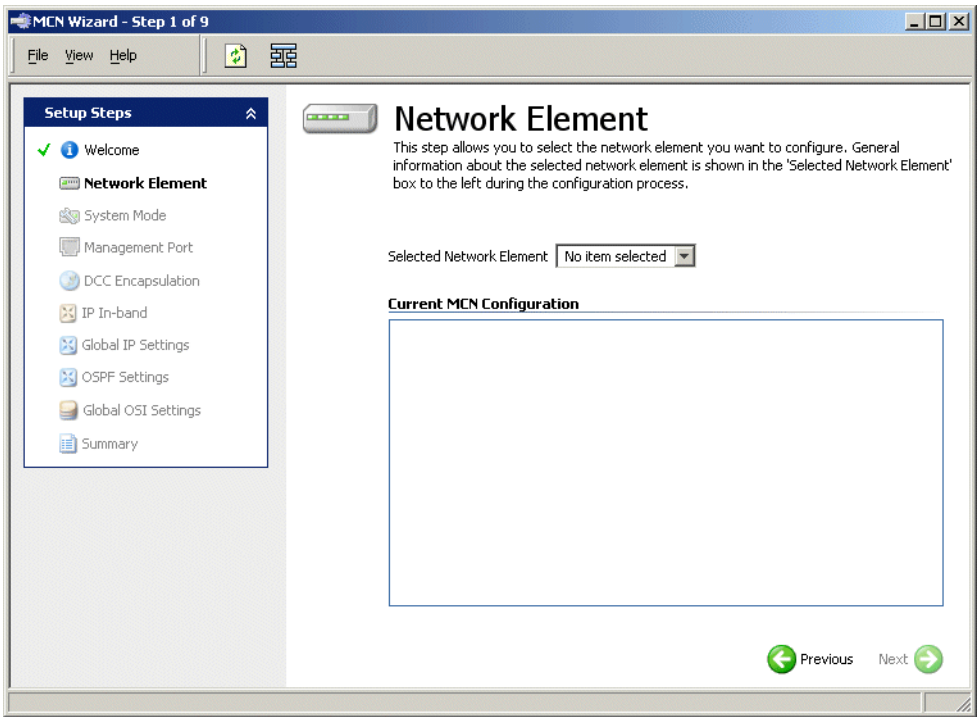


Figure 127 Network Element

4.1.7 Setup Step - System Mode (AXX 9200 EDGE and AXX 9100 CONNECT)

The AXX 9200 EDGE and AXX 9100 CONNECT are configured for either IP Numbered or IP Unnumbered system mode from the AXXCLI.

Nothing is configured from the wizard's System Mode setup step, but the user is shown in which mode the NE is configured. Because the MCN Wizard does not support IP Unnumbered, configuration with the wizard is only possible if IP Numbered mode is in use.

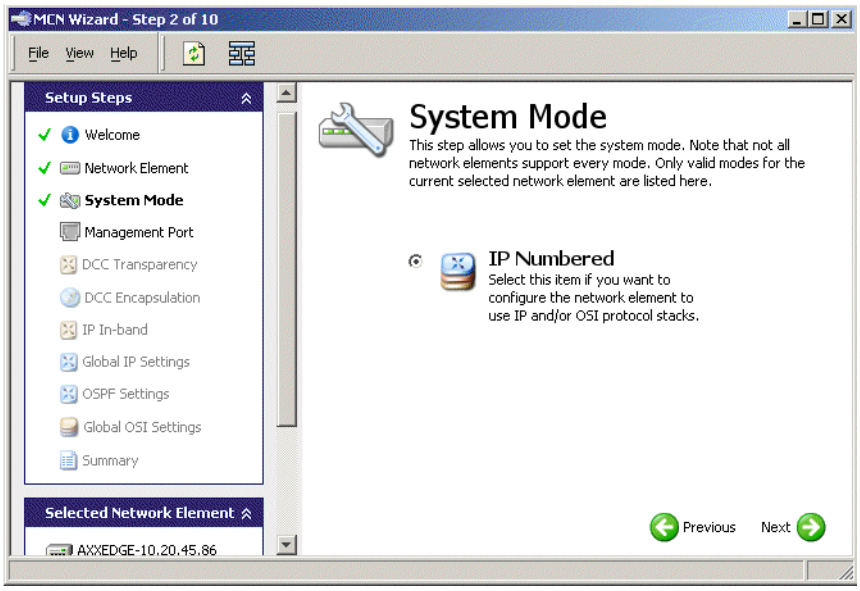


Figure 128 System Mode

4.1.8 Setup Step - Management Port (AXX 9200 EDGE and AXX 9100 CONNECT)

NOTE! This section is AXX 9200 EDGE and AXX 9100 CONNECT specific. For Management Port configuration on an AXX 9300

METRO see the section “Setup Step - Management Ports (AXX 9300 METRO)” on page 176.

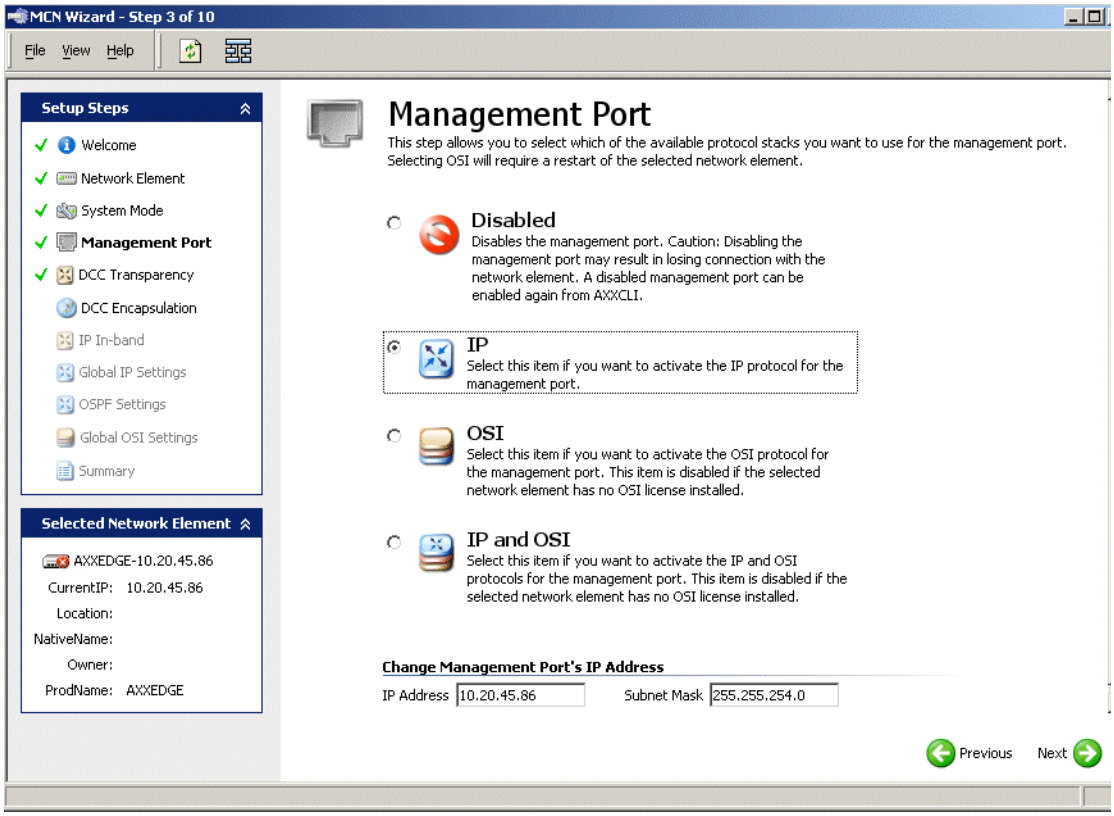


Figure 129 Management Port

The Management Port setup step configures accessability to the port. Most commonly, IP is selected, and an IP address and subnet mask are assigned. It is likely that IP is already in use and an address and a mask have been assigned. This step is commonly passed after reviewing, but not altering the configuration.

If the Management Port will be unused, it can be disabled. This can be desirable for security reasons. However, most commonly, it is left in the default state of IP, even when unused.

Finally, if an OSI license is installed, the two OSI options are available. These are needed in the extremely rare case where the host running the management station is using OSI protocols to communicate with the NE. Further discussion of OSI over the Management Port is beyond the scope of this chapter.

Caution!

If the user is currently accessing the NE over its Management Port and change the IP address or disable IP, the connectivity will most likely be lost when the configuration is saved.

4.1.9 Setup Step - Management Ports (AXX 9300 METRO)

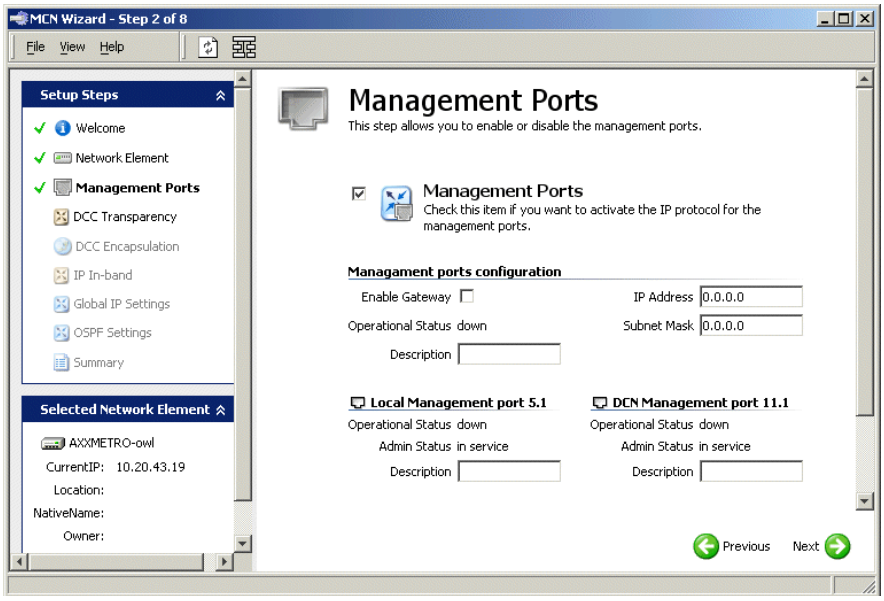


Figure 130 Management Ports

Like all NEs, an AXX 9300 METRO logically has one Management Port with one IP address. However, physically it has between two and four Management Ports. The ports are found on the Aggregate Modules (AMs) and Miscellaneous Modules (MMs). The AM ports are 5.1 and 6.1. The MM ports are 11.1 and 20.1. Only Management Ports on installed AMs and MMs appear in the wizard.

The Management Ports setup step allows both the logical and physical ports to be configured. However, in the majority of cases, the configuration is correct before the wizard is started, and the step is commonly passed after reviewing, but not altering the configuration.

If the Management Port will be unused, it can be disabled. This can be desirable for security reasons. However, most commonly, it is left in the default state of enabled, even when unused.

An IP address and subnet mask can be assigned to the logical Management Port. It is like that they are already assigned, and the user will probably not need to change them.

The “Enable Gateway” option can be turned on or off. Details about the gateway feature are beyond the scope of this chapter, but it is required in IP Unnumbered networks (not necessarily on every NE). In most cases, the gateway is left in its default state, enabled.

Finally, a description can be assigned globally and to each physical port.

4.1.10 Setup Step - DCC Transparency

SDH has 12 bytes, the DCC (Data Communication Channel) bytes, that are reserved for management. The bytes are divided unequally between the two SDH header sections. The Multiplexer Section header has nine bytes (D4-D12), and the Regeneration Section header has three (D1-D3). The two sections are independent. With Ericsson AXXESSIT NEs, when management is done over the DCC bytes, it is over one header or the other. All else being equal, D4-D12 are preferred, because they provider greater bandwidth.

According to SDH standards, the DCC bytes should carry OSI formatted data. Most commonly, Ericsson AXXESSIT NEs are deployed to not use OSI over the DCC bytes. Instead, the bytes are used with a different formatting to carry management traffic, or they are ignored and management traffic is transported through other means.

In SDH networks where third party devices follow the OSI over DCC standard, problems can arise. In these situations, the Ericsson AXXESSIT NEs can ignore the DCC bytes, but this is not enough to avoid a communications problem for the third party devices.

DCC transparency allows an NE to receive DCC bytes on one SDH port, and resend them on another. In this way, the bytes are tunnelled through the NE, and it is transparent to the nodes which are sending and receiving the bytes. The NE ignores the content of the tunnelled bytes.

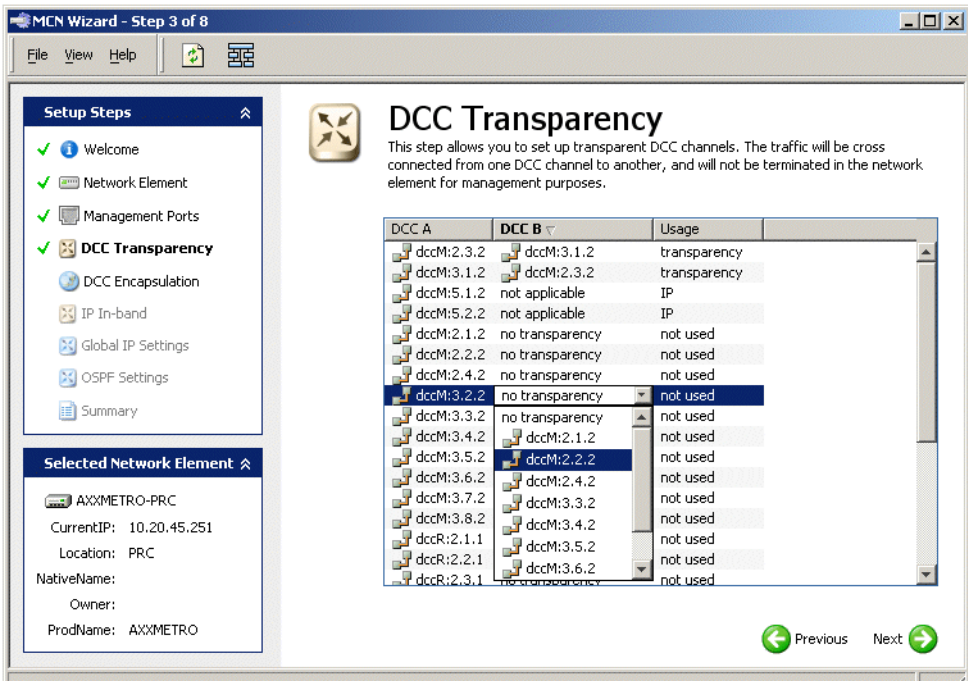


Figure 131 DCC Transparency - AXX 9300 METRO

NOTE! This setup step does not configure an NE for management over its DCC bytes, but to tunnel the bytes from one SDH port to another.

NOTE! It is rare that SDH ports are configured to be unidirectional on Ericsson AXXESSIT NEs. It is so rare, that the possibility is ignored here. Ports are assumed to be bidirectional.

The DCC Transparency setup step varies slightly between the AXX 9300 METRO, AXX 9200 EDGE, and AXX 9100 CONNECT. However, the basics of the configuration is the same for the three NE types. The description that follows is based on the setup step for an AXX 9300 METRO.

The DCC A column lists every SDH port on an expected module twice. (i.e. It lists every SDH port known to the NE twice.) Each port is listed once as dccM (D4-D12) and once as dccR (D1-D3).

The Usage column shows the current status of the DCC bytes. Usage is “not used” when the bytes are ignored, “transparency” when the bytes are tunnelled, and otherwise indicates that the bytes are used for management along with the formatting, “IP” for example.

The final column, DCC B, has a pull-down menu listing all the ports where DCC A can be tunnelled. Because the number of Muliplexer Section DCC and Regeneration Section DCC bytes differ, they cannot be tunnelled. Therefore the DCC B pull-down menu lists each known port only once. Ports where the bytes are in use for management or transparency, aren't listed in the menu.

To configure transparency between two ports, a user can locate either port in the DCC A column. The other port is selected in the DCC B pull-down menu, and the configuration is complete. The transparency will be bidirectional.

NOTE! The biggest difference between using the wizard to configure an AXX 9300 METRO or an AXX 9200 EDGE or an AXX 9100 CONNECT is that an AXX 9200 EDGE or an AXX 9100 CONNECT must have both ports of a tunnel separately configured to be bidirectional.

NOTE! When tunnelling for both D4-D12 and D1-D3 is required, they are configured independently.

4.1.11 Setup Step - DCC Encapsulation (AXX 9300 METRO)

NOTE! The section "Setup Step - DCC Transparency" on page 177 provides an overview of the DCC bytes in the SDH headers. It should be read as an introduction to this section.

Sending data over the DCC bytes of an SDH header is one of several options available for transporting management traffic between an management station and an NE. When the DCC bytes are used, there are a variety of encapsulation techniques to choose from. The choices vary with NE type.

The DCC Encapsulation setup step configures SDH ports to transport management traffic over DCC bytes.

NOTE! This section is AXX 9300 METRO specific. For DCC Encapsulation on an AXX 9200 EDGE or AXX 9100 CONNECT see the section "Setup Step - DCC Encapsulation - (AXX 9200 EDGE and AXX 9100 CONNECT)" on page 181.

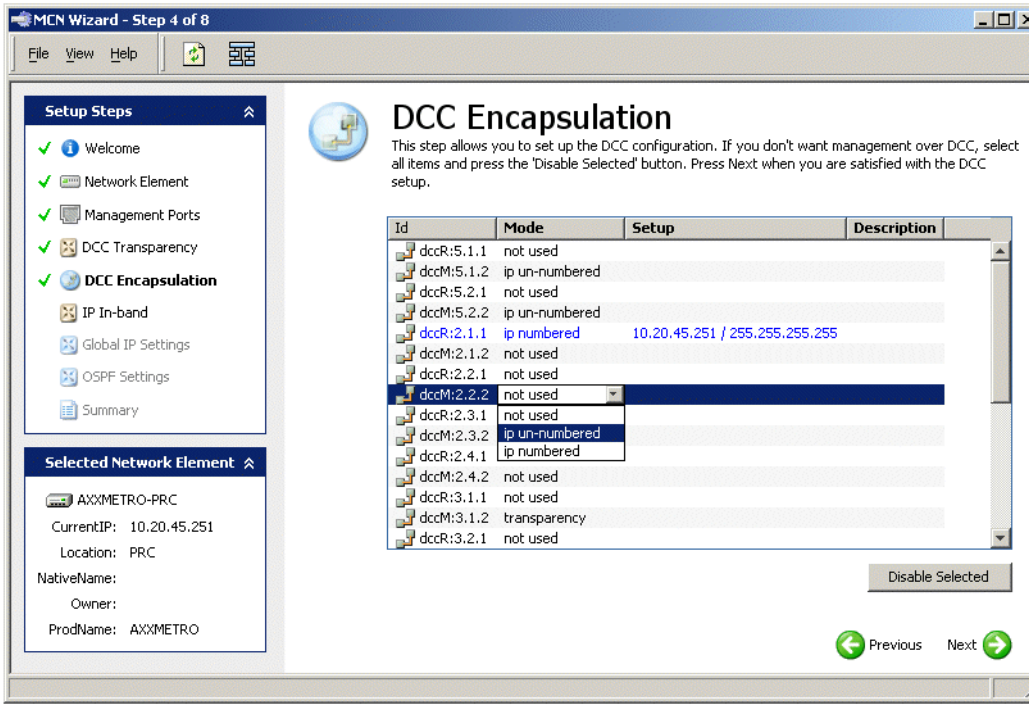


Figure 132 DCC Encapsulation - AXX 9300 METRO

For the AXX 9300 METRO, one DCC encapsulation technique available, It has a variety of names, but is most commonly referred to as IP/PPP or IP over PPP. The IP management traffic is encapsulated in PPP (Point to Point Protocol) which is encapsulated in DCC. This is both the most widely used DCC encapsulation technique on Ericsson AXXESSIT NEs, and the one preferred by Ericsson AXXESSIT.

From the perspective of IP, the DCC bytes function as a standard networking interface. On an AXX 9300 METRO, each DCC networking interface used for management can be configured as either IP Numbered or IP Unnumbered.

TIP! The section “IP Numbered, IP Unnumbered, and System Mode” on page 170 provides an overview of IP Numbered and IP Unnumbered interfaces.

The Id column lists every SDH port on an expected module twice. (i.e. It lists every SDH port known to the NE twice.) Each port is listed once as dccM (D4-D12) and once as dccR (D1-D3). In other words, there is an entry for each potential DCC networking interface.

The Mode column shows the current status of the DCC networking interface. The Mode is “not used” when the DCC bytes are ignored, “transparency” when the bytes are tunnelled to another SDH port, and if the bytes are already used for management, the Mode is “ip numbered” or “ip un-numbered”.

If the bytes are currently set for “transparency”, and the user wants to change the configuration so that they transport management traffic, transparency must first be disabled (see “Setup Step - DCC Transparency” on page 177).

After the Mode is set to “ip numbered”, the Setup column will change to show an IP address and a subnet mask. The address is the Management Port address, and is there to show the user the format of the data to enter. The user should assign the planned IP address and mask.

If IP Unnumbered is being implement, nothing beyond setting the Mode is required. IP Unnumbered interfaces share the IP address of the Management Port.

As with so many Ericsson AXXESSIT features, a Description can also be added.

Finally, a button “Disable Selection” appears below and to the right of the table. If multiple DCC interfaces are currently set for DCC management (i.e. multiple interfaces are set to “ip numbered” or “ip un-numbered”) the “Disable Selection” button can be used to quickly disable more then one at a time. Select (highlight) multiple interfaces and then click the button. All selected interfaces except those in “transparency” mode will be set to “unused”. This of course can also be done interface by interface without the button.

NOTE! The PPP encapsulation uses CRC-32 for a frame checksum. Although CRC-32 is more widely used and provides greater reliability then CRC-16, that later may be required for interoperability with third party devices. CRC-16 can be selected from the Desktop.

4.1.12 Setup Step - DCC Encapsulation - (AXX 9200 EDGE and AXX 9100 CONNECT)

NOTE! This section is AXX 9200 EDGE and AXX 9100 CONNECT specific. For DCC Encapsulation on an AXX 9300 METRO see the section “Setup Step - DCC Encapsulation (AXX 9300 METRO)” on

page 179.
That section provides an introduction to management over DCC which should be read as an introduction to this section.

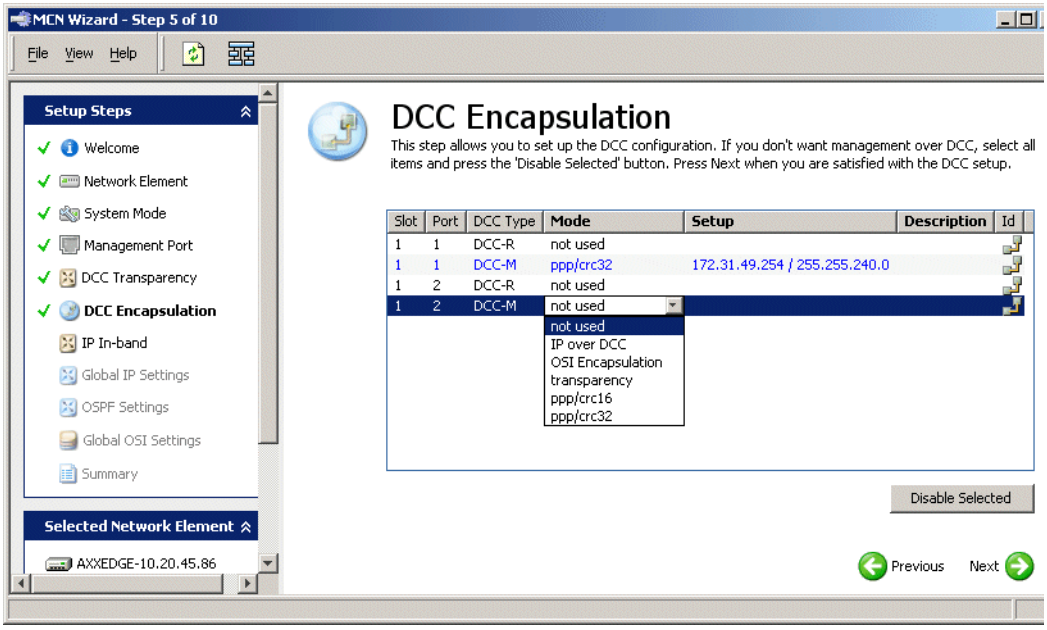


Figure 133 DCC Encapsulation - AXX 9200 EDGE

For the AXX 9200 EDGE and AXX 9100 CONNECT, multiple DCC encapsulation techniques are available including the Ericsson AXXESSIT preferred IP/PPP. Regardless of the encapsulation technique used, a unique IP address must be assigned to the DCC networking interface. As a reminder, the MCN Wizard only configures AXX 9200 EDGEs and AXX 9100 CONNECTs in IP Numbered mode, where all networking interfaces require a unique IP addresses.

TIP! The section “IP Numbered, IP Unnumbered, and System Mode” on page 170 provides an overview of the IP Numbered and IP Unnumbered interfaces.

The Slot, Port and DCC Type columns combine to list every SDH port on an expected module twice, (i.e. They list every SDH port known to the NE twice.) Each port is listed once as dccM (D4-D12) and once as dccR (D1-D3). In other words, there is an entry for each potential DCC networking interface.

The Mode column shows the current status of the DCC networking interface. The Mode is “not used” when the DCC bytes are ignored, “transparency” when the bytes are tunnelled to another SDH port, and if the bytes are already used for management “IP over DCC”,

“OSI Encapsulation”, “ppp/crc16” or “ppp/crc32” depending on the encapsulation in use.

“ppp/crc32” is IP/PPP. This is the Ericsson AXXESSIT preferred encapsulation, and by far the most widely used.

”ppp/crc16” is also IP/PPP but with a 16 bit CRC (Cyclical Redundancy Check). It is used for inter operability with third party SDH nodes that have implement IP/PPP but not a 32 bit CRC. The encapsulation is not widely used.

“OSI Encapsulation” follows the SDH standard of OSI protocols over the DCC bytes. “OSI Encapsulation” is only available if an OSI license is installed. The encapsulation is not widely used.

“IP over DCC” is a proprietary solution that should only be used for compatibility with the older AXX155 NE type. The AXX155 does not support IP/PPP.

Only for an AXX 9200 EDGE, an extra Mode option exists over DCC-R. “remote module” provides support for the AXX10 and AXX11 NE types. Information about the AXX10 and AXX11 is beyond the scope of this chapter.

As soon as the Mode is set to “ppp/crc32”, “ppp/16”, “OSI Encapsulation” or “IP over DCC” the Setup column will change to “<ip address / subnet mask>”. The user should assign the planned IP address and mask. The format requires a “/” (slash) between the address and the mask. For example: 172.31.2.254 / 255.255.248.0

The final setting “transparency” is another method for configuring tunnelling as described in the section “Setup Step - DCC Transparency” on page 177.

Each line has a Description field which can be set even for ports that are “unused”.

Finally, a button “Disable Selection” appears below and to the right of the table. If multiple interfaces are currently set for DCC management, the “Disable Selection” button can be used to quickly disable more then one at a time. Select (highlight) multiple interfaces and then click the button. All selected interfaces except those in “transparency” mode will be set to “unused”. This of course can also be done interface by interface without the button.

4.1.13 Setup Step - IP In-band (AXX 9300 METRO)

When management traffic travels in the same channel as customer traffic, it is described as in-band. When a dedicated channel with independent bandwidth is used for management traffic, it is described as out-of-band (OOB). The Management Port and DCC networking interfaces, which were covered earlier in this chapter, are both OOB.

Two independent in-band options are available for management.

The first in-band option is a management VLAN. Most commonly, the VLAN is carried over one or more WAN ports to exchange management traffic between NEs. For security reasons, the VLAN should carry only management traffic. A VLAN is by nature a broadcast medium making it incompatible with IP-Unnumbered which requires a point-to-point interface. So a management VLAN is limited to IP-Numbered interfaces.

The second in-band option is L1CC (Layer 1 Communication Channel). It is a proprietary solution that takes bandwidth from the L1 (Layer 1) Ethernet port where it is configured. This reduces the L1 ports bandwidth. L1CC IP traffic is encapsulated in PPP and multiplexed with the customer traffic from the L1 port. Bandwidth is only taken when management traffic is transmitted. Otherwise the full bandwidth is available to the L1 port.

Both the management VLAN and L1CCs are configured from the IP In-band setup step.

NOTE! This section is AXX 9300 METRO specific. For IP In -band on an AXX 9200 EDGE or AXX 9100 CONNECT see the section

“Setup Step - IP In-band (AXX 9200 EDGE and AXX 9100 CONNECT)” on page 187.

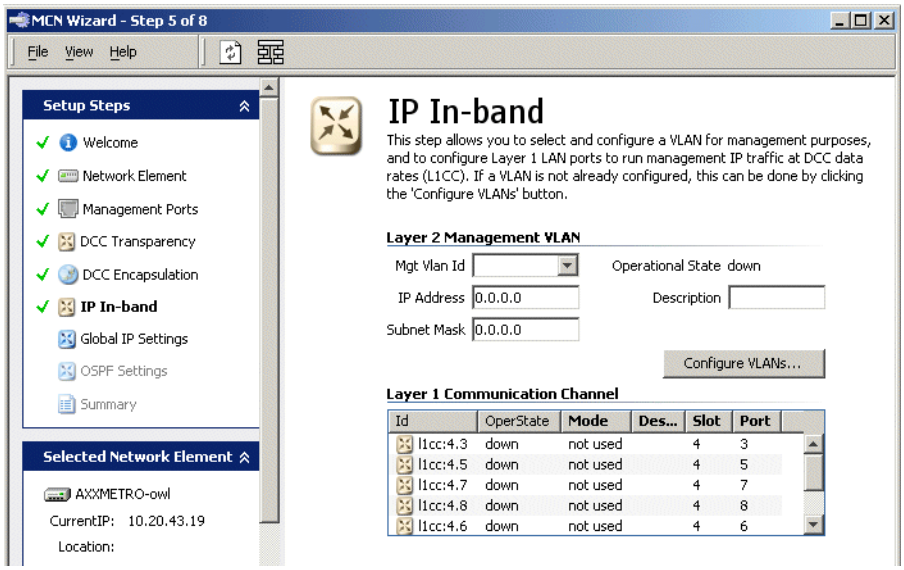


Figure 134 IP In-band - AXX 9300 METRO

Management VLAN

The AXX 9300 METRO can have one management VLAN. The VLAN must exist before the wizard can configure it for management. If a VLAN for management wasn't prepared in advance, the "Configure VLANs..." button will start the VLAN Settings GUI, which is used to create VLANs.

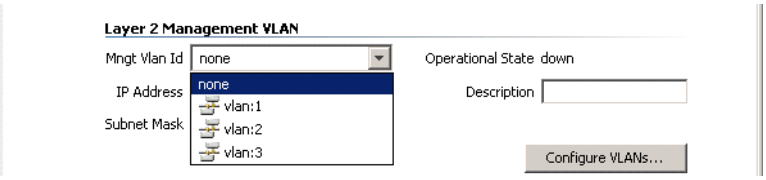


Figure 135 Management VLAN - AXX 9300 METRO

The "Mngt Vlan Id" field is a pull-down menu that lists all VLANs on the NE. The user selects the VLAN planed for management, and assign the planned IP address and subnet mask. The IP address is applied to all ports in the VLAN. As with so many Ericsson AXXESSIT features, a Description can also be added.

Layer 1 Communication Channel

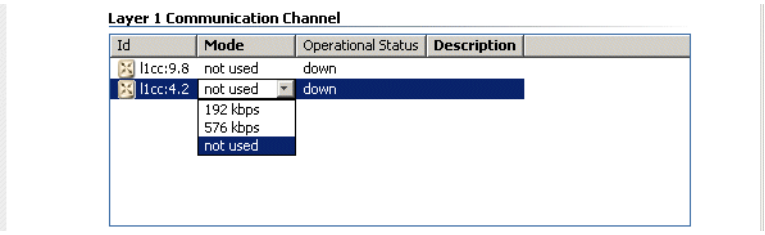


Figure 136 Layer 1 Communication Channel - AXX 9300 METRO

An Ethernet port must be in L1 mode before the MCN Wizard can configure it for L1CC management. The Id column lists each L1 port. To enable L1CC, the Mode column is set to 192 kbps or 576 kbps. The difference between the two settings is the bandwidth for management.

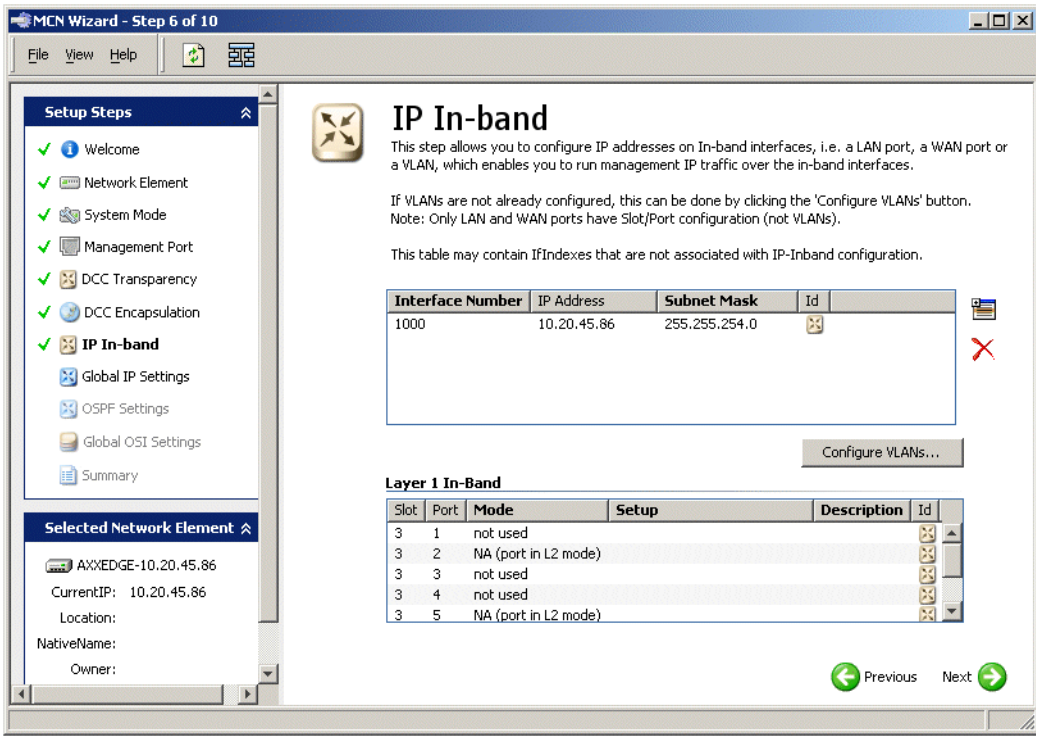
The choose of bandwidth is a trade-off. Higher management traffic throughput comes at the cost of taking more bandwidth from the L1 port. Additionally, when the far end NE is an AXX 9100 CONNECT, 192 kbps must be used. An SDH expert may notice that the L1CC bandwidths are the same as for DCC channels. While this is true, L1CC is an in-band solution and does not travel in the DCC bytes. The bandwidths match because of NE internal handling.

An AXX 9300 METRO's L1CC ports are always unnumbered so no additional configuration, such as the assignment of an IP address, is required.

As with so many Ericsson AXXESSIT features, a Description can optionally be added to each L1CC interface.

4.1.14 Setup Step - IP In-band (AXX 9200 EDGE and AXX 9100 CONNECT)

NOTE! This section is AXX 9200 EDGE and AXX 9100 CONNECT specific. For IP In-band on an AXX 9300 METRO, see the section "Setup Step - IP In-band (AXX 9300 METRO)" on page 184. That section provides an introduction to in-band management which should be read as an introduction to this section.



Management VLAN

NOTE! The interface for configuring a Management VLAN on an AXX 9200 EDGE and AXX 9100 CONNECT is different then for an AXX 9300 METRO. This should not confuse the user. Only the

configuration interfaces are different, the management VLANs created are compatible.

The AXX 9200 EDGE and AXX 9100 CONNECT allow for multiple management VLANs. A VLAN must exist before the wizard can configure it for management. If a VLAN for management wasn't prepared in advance, the "Configure VLANs..." button will start the VLAN Settings GUI, which is used to create VLANs.

Management VLANs are configured from the upper table in the IP In-band setup step. The table is not a list of VLANs used for management, but a list of all IP interfaces. All networking interfaces with IP addresses are IP interfaces. When a VLAN is assigned an IP address, as is required for a Management VLAN, it becomes an IP interface.

Every interface that can be assigned an IP address in an NE has a fixed Interface Number. This includes all VLANs, the Management Port, DCC headers, and all Ethernet ports. All interfaces that have already been assigned an IP address are IP interfaces and appear in the table.

The table's Interface Number column identifies each IP interface. Non-VLAN IP interfaces are unimportant while configuring Management VLANs, and their presence in the table can be ignored by the user.

The Interface Numbers for VLANs range from 100000 to 103999. The number is assigned when the VLAN is created. To make a VLAN available for Management, the user must know the Interface Number which can be found in the VLAN Settings GUI as well as on the Desktop.

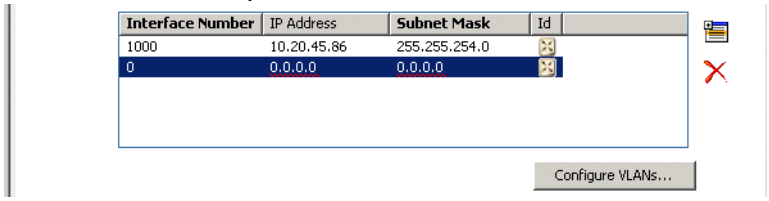


Figure 137 IP Interfaces Table - AXX 9200 EDGE and AXX 9100 CONNECT

Click the **Add** button to put an additional entry in the table. Enter the Interface Number, planned IP address and planned subnet mask for the management VLAN, and the configuration is complete.

Note that the **Delete** button can be used to remove highlighted entries from the table. The table exists to add and delete management VLANs, and removing other entries is not recommended.

Layer 1 In-Band (L1CC)

An Ethernet port must be in L1 mode before the wizard can configure it for L1CC management. The Slot and Port columns identifies each LAN port. The Mode column identifies if the port is configured in Layer 2 and therefore not available for L1CC, “NA (port in L2 mode)”.

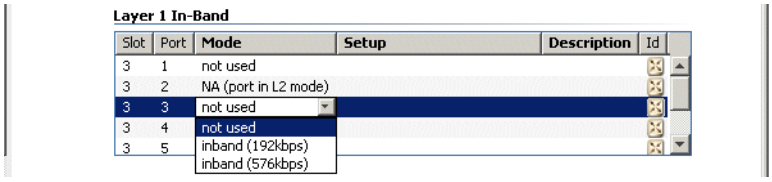


Figure 138 Layer 1 In-Band - AXX 9200 EDGE and AXX 9100 CONNECT

To enable L1CC, the Mode column is set to 192 kbps or 576 kbps. As explained in the section “Layer 1 In-Band (L1CC)” on page 189, the only difference in the two settings, is the bandwidth provided for management. The AXX 9100 CONNECT only supports 192 kbps.

As soon as the Mode is set to “inband (192kbps)” or “inband (576 kbps)” the Setup column will change to “<ip address / subnet mask>”. The user should assign the planned IP address and mask.

As with so many Ericsson AXXESSIT features, a Description can optionally be added.

NOTE! The AXX 9200 EDGE and AXX 9100 CONNECT also support L1CC for IP-Unnumbered mode, but it must be configured from the Desktop.
L1CC unnumbered is required for compatibility with the AXX 9300 METRO which doesn’t support L1CC in IP-Numbered mode.

4.1.15 Setup Step - Global IP Settings

The previous setup steps, Management Port, DCC Encapsulation, and IP In-band, configure IP networking interfaces for management. In a well designed MCN, those interfaces interconnect all NEs and management stations. However, the interconnections are not sufficient. Each management station needs to know the routes to reach the NEs, and the NEs require routes back to the management stations. IP routing tables on each NE and management station are required.

NOTE! An explanation of IP routing is beyond the scope of this manual. It is assumed that the user is familiar with common IP routing terminology, concepts, configuration, and design.

An NE's routing table is configured from two setup steps, Global IP Settings and OSPF settings.

Global IP Settings, the current setup step, manually manages the NE's routing table allowing static entries to be added and deleted. Additionally, on an AXX 9200 EDGE or AXX 9100 CONNECT, RIP (Routing Information Protocol) can be enabled. The AXX 9300 METRO does not support RIP, and the protocol use is not recommended by Ericsson AXXESSIT. OSPF is preferred for dynamic routing.

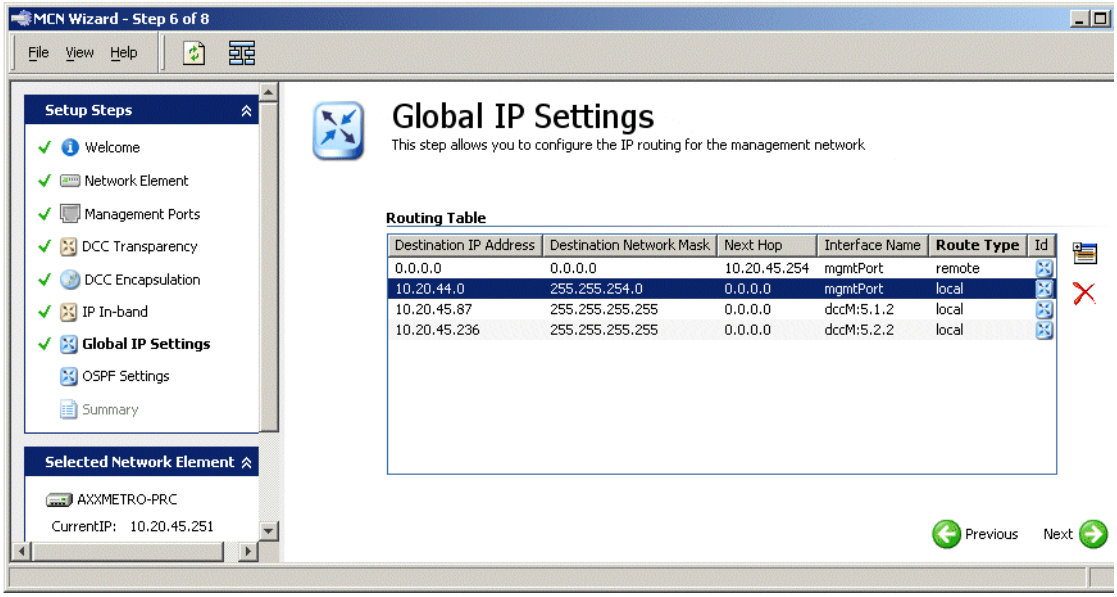


Figure 139 Global IP Settings - AXX 9300 METRO

AXX 9300 METRO

Use the **Add** button to create a new static route. Enter the Destination IP Address, Destination Network Mask, and Next Hop. The Interface Name will automatically be determined when the entry is saved. Route Type provides information about the route, and cannot be changed. Statically added routes have the Route Type remote.

The **Delete** button can be used to remove highlighted entries from the table. The table exists to add and delete static routes, and removing entries with the Route Type local is not recommended.

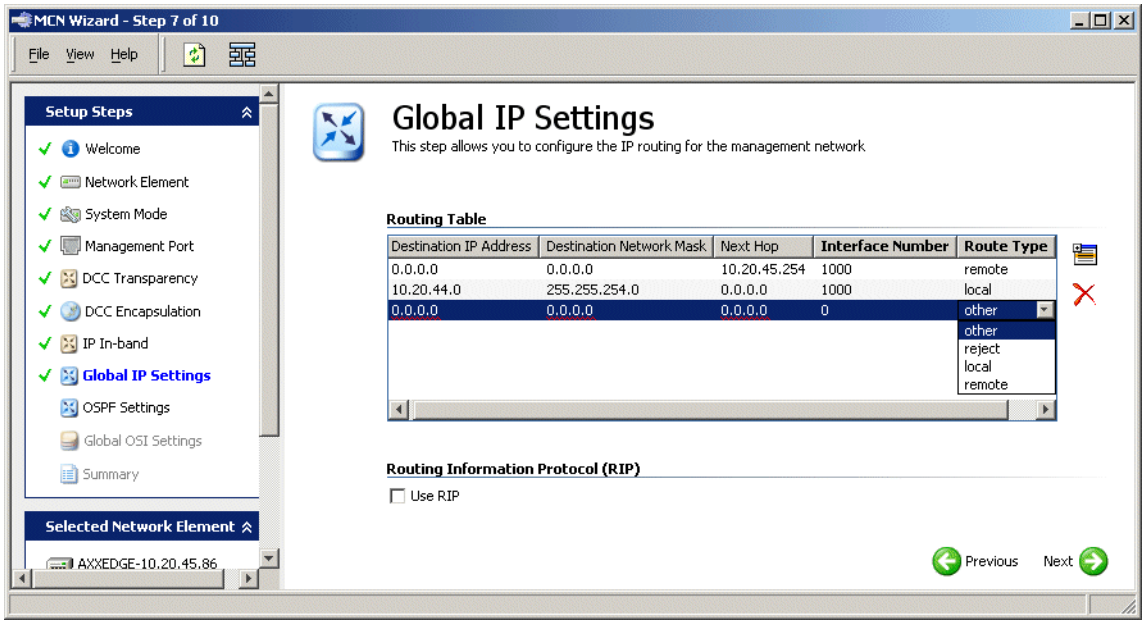


Figure 140 Global IP Settings - AXX 9200 EDGE and AXX 9100 CONNECT

AXX 9200 EDGE and AXX 9100 CONNECT

Use the **Add** button to create a new static route. Enter the Destination IP Address, Destination Network Mask, and Next Hop. Unlike the AXX 9300 METRO's Interface Name, The Interface Number must also be set. Route Type provides information about the route, and should be set to "remote". Assignment of other Route Type values is rare and beyond the scope of this chapter.

The **Delete** button can be used to remove highlighted entries from the table. The table exists to add and delete static routes, and removing entries with Route Types other then remote is not recommended.

4.1.16 Setup Step - OSPF Settings

NOTE! The section "Setup Step - Global IP Settings" on page 189 provided an explanation of the need for routing in an MCN. It should be read as an introduction to this section.

The OSPF (Open Shortest Path First) routing protocol dynamically builds routing tables. Although OSPF networks are normally maintained by a team of experts, a simple OSPF configuration for

an MCN is generally easier to configure then a network using static routes.

OSPF works in both IP Numbered and IP Unnumbered modes.

NOTE! Understanding OSPF and OSPF configuration options are beyond the scope of this chapter. This section offers a cookbook list of steps for a basic OSPF configuration that will support the majority of MCNs. Explanations of what each configuration step does, is not provided.

READ MORE: “Open Shortest Path First” on page 9.

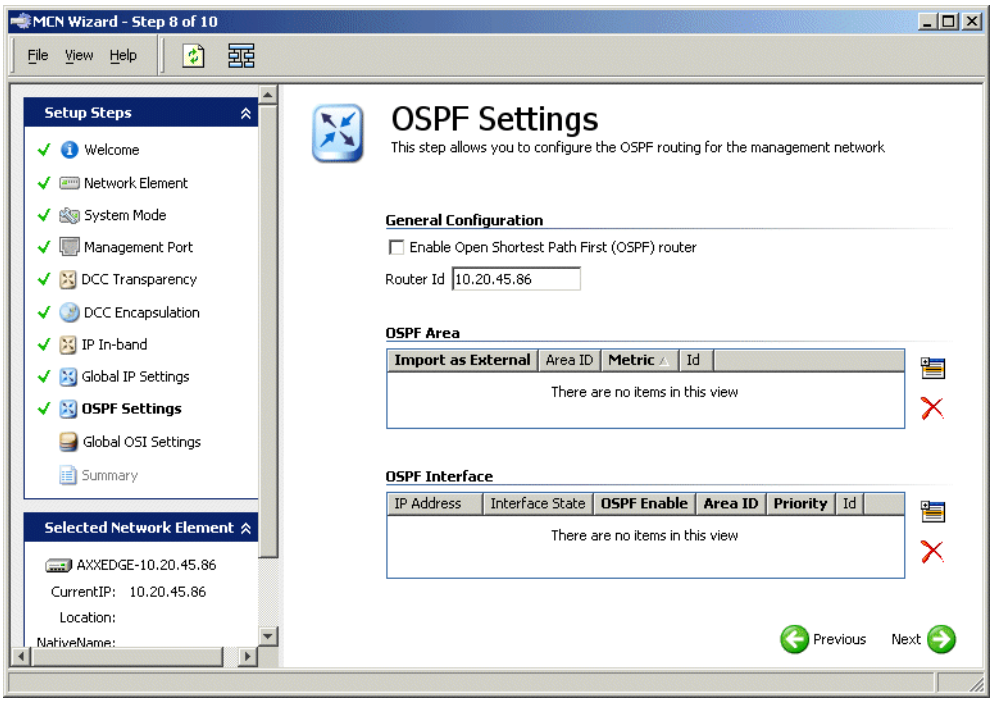


Figure 141 OSPF Settings - AXX 9200 EDGE and AXX 9100 CONNECT

To enable OSPF select “Enable Open Shortest Path First (OSPF) router”.

NOTE! When OSPF is enabled, the NE must be rebooted before the protocol will work properly, and before it can be completely configured.
The user can jump ahead to the Summary setup step to save the configuration before rebooting the NE.

The remainder of this section assumes that OSPF was enabled, and that the NE has since been rebooted.Every OSPF node requires a unique 32 bit identifier (Router Id). On an NE, it defaults to the match the IP address of the NE's Management Port.

Every IP interface where OSPF is running must be in an OSPF area. Required areas must first be added to the OSPF Area table.

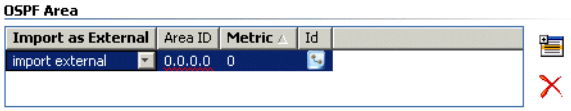


Figure 142 OSPF Area - AXX 9200 EDGE and AXX 9100 CONNECT

Use the **Add** button to put a new entry in the OSPF Area table. The defaults created by clicking Add include the Area ID 0.0.0.0. The defaults are correct for the cookbook solution, which works with only one area.The wizard's OSPF Area table for an AXX 9300 METRO is identical to that of an AXX 9200 EDGE or AXX 9100 CONNECT except that it lacks the Metric column.

The **Delete** button can be used to remove highlighted entries from the table. Note that the last area in the table cannot be removed, even if OSPF is disabled.

Since the NE has been rebooted with OSPF enabled, the OSPF Interfaces table lists all IP interfaces. By default, on an AXX 9200 EDGE and AXX 9100 CONNECT, all the interfaces are enabled for OSPF. That is acceptable for the cookbook solution. On an AXX 9300 METRO, interfaces where OSPF must run, have to be explicitly enabled. All other default values in the OSPF Interfaces table are correct for the cookbook solution, and no changes are required.

The wizard's OSPF Interface table for an AXX 9300 METRO is identical to that of an AXX 9200 EDGE or AXX 9100 CONNECT with two excepts. First, the Metro lacks the Priority column. Second, the Metro has an extra column, Interface Name. Because the AXX 9300 METRO's interfaces can be in IP Unnumbered mode while using the wizard, the IP Address is not enough to uniquely identify an interface. The Interface Name provides for unique identification.

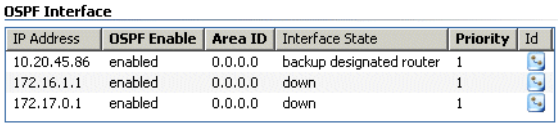


Figure 143 OSPF Interface - AXX 9200 EDGE and AXX 9100 CONNECT

4.1.17 Setup Step - Global OSI Settings (AXX 9200 EDGE and AXX 9100 CONNECT)

NOTE! The section “Setup Step - DCC Transparency” on page 177 provides an overview of the DCC bytes in the SDH headers, and explains that the standard encapsulation for those bytes is OSI.

NOTE! When OSI is implemented on Ericsson AXXESSIT NEs, it is used in existing SDH networks with third party devices.
The organizations using OSI have previous SDH experience, and the skills to properly configure OSI. Because of that, and because OSI is not widely used on Ericsson AXXESSIT NEs, a discussion of OSI is not covered in this chapter.

As with DCC/OSI itself, the Global OSI Settings setup step is limited to NEs with an OSI license installed.

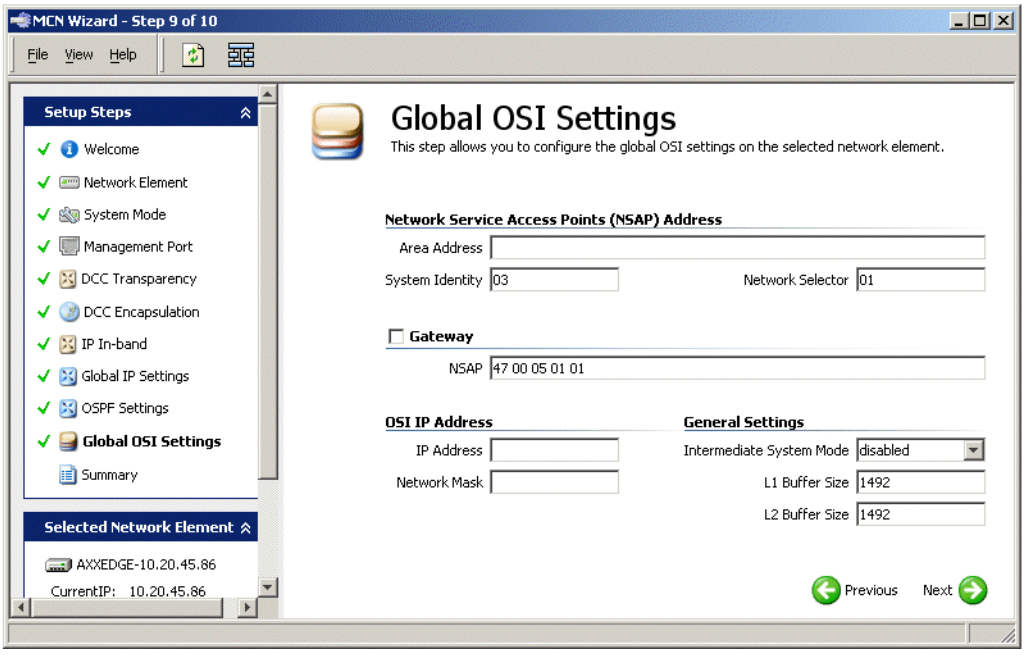


Figure 144 Global OSI Settings

4.1.18 Setup Step - Summary

Summary, the final setup step, allows the user to review the configuration before committing changes to the NE.

NOTE! If any configuration needs to be changed, the user can revisit the appropriate setup step by selecting it in the left hand pane.

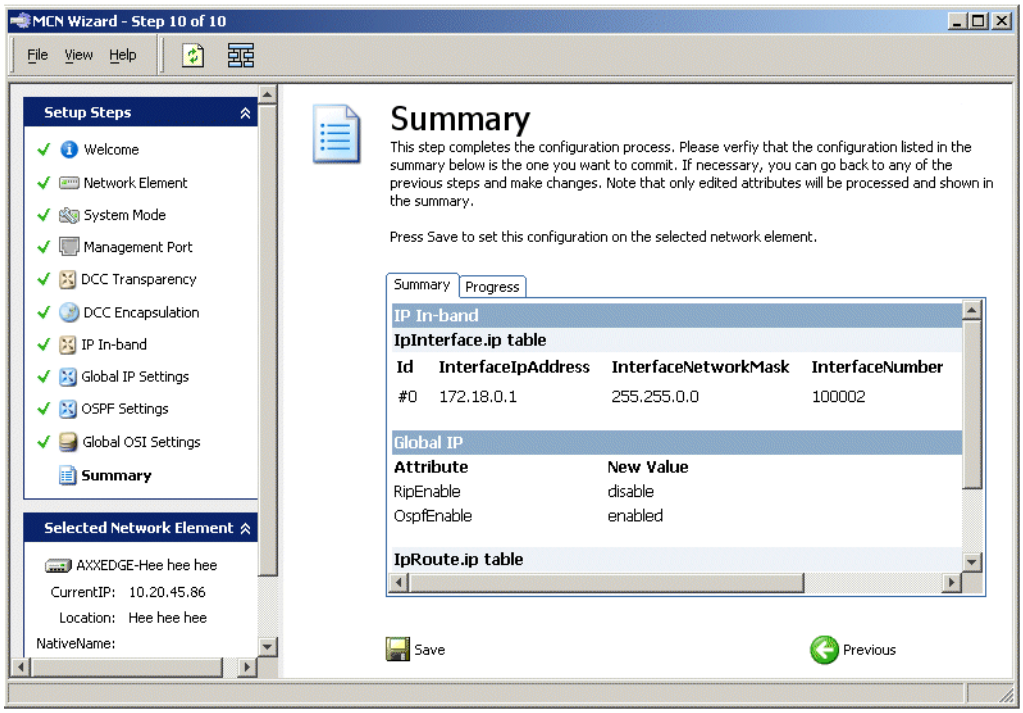


Figure 145 Summary - AXX 9200 EDGE

Click 

"**Save"** to commit the configuration to the NE. Upon saving, the view switches from the "Summary to the "Progress" tab, which documents each change as it's made.

The Progress tab shows a "FAILED" message if any setup step fails. The user can click on any setup step in the left hand pane to correct the configuration.

After the configuration is successfully saved to the NE, the MCN Wizard can be closed.

5 Ethernet Services Management

5.1 Introduction

This section describes management of Ethernet services on the Ericsson AXXESSIT network elements; AXX 9100 CONNECT (R1.2) and AXX 9200 EDGE (R2.3). The section does not cover a network level view of the Ethernet service aspect.

Same Ethernet Virtual Connection (EVC) attributes must be set locally on network elements. In this implementation the term EVC is used to denote the set of these local attributes for the end-to-end EVC.

Click desired topic below :

Learn more >>> **“About the Ethernet Services”**

Create >>> **“Ethernet Service Wizard”**.

Maintenance >>> **“Ethernet Services - Maintenance”**

NOTE! In the following section the assumption is made that creation of UNI's, Ethernet services and of some profiles are done in the Ethernet Services wizard, while maintenance is performed from the Management Tree application.

5.1.1 Recommended reading

As this section only focus on implemented Ethernet services for AXX 9100 CONNECT (R1.2) and AXX 9200 EDGE (R2.3), the following documents are recommended (http://www.metroethernetforum.org) for both basic- and in-depth studies:

- Metro Ethernet Forum, Technical Specification
  Ethernet Services Attributes - Phase 2 - Approved Draft 4
- Metro Ethernet Forum, Technical Specification
  MEF 10, Ethernet Services Attributes Phase 1, November 2004.

5.2 About the Ethernet Services

5.2.0.1 Ethernet services as defined by MEF and ITU-T

The technical definition of an Ethernet service is in terms of what is seen by each customer edge (CE) including the user network interface (UNI.) The UNI is the physical demarcation point between the responsibility of the service provider and the responsibility of the subscriber/customer.

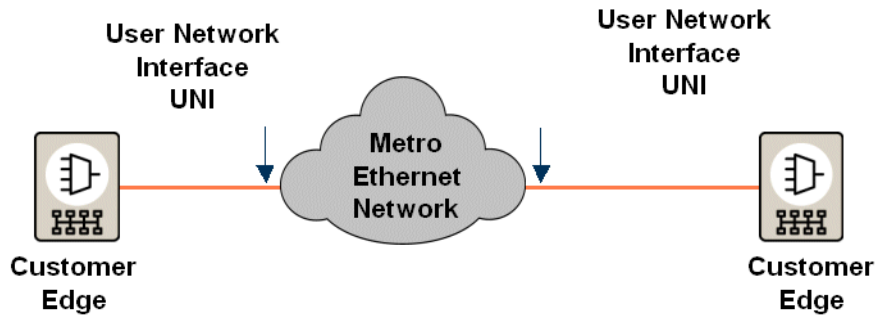


Figure 1 Ethernet service definition

The CE and Metro Ethernet network (MEN) exchange service frames across the UNI. A service frame is an Ethernet frame transmitted across the UNI toward the service provider or an Ethernet frame transmitted across the UNI toward the subscriber.

There are no assumptions about the details of the MEN. It could consist of a single switch or an agglomeration of networks based on many different technologies, e.g. SDH, ATM, MPLS, WDM, or Ethernet.

The Ethernet virtual connection (EVC) specifies the connectivity between UNI's. There are a number of service attributes that an EVC can have. There are also a number of different service attributes for a UNI.

5.2.1 Bandwidth profile

The bandwidth profile defines the set of traffic parameters applicable to a sequence of service frames. Associated with the bandwidth profile is a rate-limiting algorithm (policing) to determine

service frame compliance with the specified parameters. In this implementation there is currently one type of bandwidth profile; ingress bandwidth profile.

A bandwidth profile is enforced by the provider's network and is part of a service level specification between the subscriber and the service provider. The outcome of any rate-limiting algorithm within the service provider network is a set of service frames that are labeled as Green, Yellow, or Red based on their level of conformance to the used bandwidth profile. Frames marked Red are always dropped.

The parameters forming a bandwidth profile are

- Committed Information Rate (CIR) expressed as bits per second. CIR >=0.
- Committed Burst Size (CBS) expressed as bytes. When CIR > 0, CBS is greater than or equal to the maximum service frame size.
- Excess Information Rate (EIR) expressed as bits per second. EIR >=0.
- Excess Burst Size (EBS) expressed as bytes. When EIR > 0, EBS is greater than or equal to the maximum service frame size.
- Colour Mode (CM) has only one of two possible values, "colour-blind" and "colour-aware."

Please note that Egress bandwith profile is not implemented.

For more details, please see Technical Specification MEF 10, Ethernet Services Attributes Phase 1, November 2004.

Table 1 An example of a bandwidth profile

Unique identifier	Business
CIR	50M
CBS	16 Kb
EIR	-
EBS	-
Color mode	"Color blind"

5.2.2 Colour to Priority (C2P) profile

The Colour to Priority profiles determines the "service level" of the Ethernet service. The service level is determined by the PRI field, as defined by IEEE 802.1p, in the Ethernet service frame. PRI is used to give different priority to different kinds of traffic. The priorities influence the way switches treat traffic coming in on their ports

The network elements are delivered with a predefined set of these profiles (as factory settings) and in most cases these profiles will be used. They are denoted GOLD, SILVER, and BRONZE . Customisable profiles are also supported.

A colour to priority profile is associated with one or more sequences of service frames. The mapping from colour to priority is necessary to be able to place the service frames in one of four queues at each Ethernet port. Each network element has a priority to queue mapping table that applies to all Ethernet ports on the element.

The IEEE 802.1p priority mechanism uses eight priority levels, numbered 0 - 7, inclusive. The relative ranking between these levels is not fixed by the standard. There is however a recommended relative ranking and priority assignment to traffic types, in the standard. This recommendation is found in the table below.

Table 2 Relative ranking of priority levels/assignment to traffic types

Priority Level	**Traffic Type**
7 (highest priority)	network management
6	voice
5	video
4	controlled load
3	excellent effort
0	best effort
2	undefined
1 (lowest priority)	background

In the table, the priority levels are given in the order of descending relative priorities, from top to bottom. Note that the recommendation is to let priority level 0 (zero) have higher priority than 2 and 1."

For instruction on creating a colour-to-priority profiles please see “Colour-to-Priority (C2P)” on page 232.

5.2.3 User Network Interface - UNI

a UNI is the physical demarcation point between the responsibility of a service provider and the responsibility of the subscriber to Ethernet services, see “Ethernet services as defined by MEF and ITU-T” on page 199.

On a network element this is represented as a characteristic of the physical Ethernet port (i.e., LANx port.) The LANx ports are not always associated with a UNI instance e.g. if used for transport inside the MEN.

5.2.4 Rate limiting application configuration

Bandwidth profiles can be applied to ingress traffic flows. A flow identifies a sequence of service frames with a common characteristic. Up to 16 rate-limiting functions can be active on an FE LANx port and up to 64 functions on a GE LANx port.

Possible choices are:

- Rate-limiting per UNI
- Rate-limiting per UNI & EVC combination (i.e. per EVC in the UNI)

A service frame must never be subject to more than one rate-limiting function.

5.2.5 Service frame sequences

This section describes how a service frame is handled and modified from entering a network element (ingress traffic) and until it is sent out of the element as egress traffic.

Table 3 Service frame handling - walkthrough

Action
A frame enters as an ingress service frame and the VLAN ID from the customer network is used to identify which EVC this frame belongs to.
Disposition of service frames according to the configuration of the layer 2 control protocols service frames.
The layer 2 control protocols service frames for each EVC is applied.
Depending on the rate limiting function service frame sequence target (i.e., UNI, UNI&EVC,) a bandwidth profile is applied to service frame.
The rate limiting function maps the service frames to a colour. The priority used is the Ethernet service frame priority assigned by the rate limiting function (802.1p.)
The service frame is inserted into a queue according to the priority to queue mapping that is universal to the network element. The priority is the Ethernet service frame priority assigned by the rate limiting function (802.1p.)

5.2.6 Bandwidth capacity on one UNI

A bandwidth profile is always associated to a UNI, i.e., either directly when associated with UNI or indirectly when associated with UNI&EVC. The UNI has a total possible bandwidth capacity that can be supported.

5.2.7 CIR and EIR

If only one bandwidth profile applies to all service frames on a UNI, CIR + EIR <= port capacity.

If more than one flow (or sequence of service frames) are defined for the UNI, the sum of all CIR's in the used bandwidth profiles must not exceed the port capacity. It is in this situation not correct to limit according to CIR + EIR since for multiple flows over-subscription using statistical multiplexing can be used.

If the user selects a bandwidth profile to be associated with e.g. a UNI&EVC, the user is informed if capacity is not available and bandwidth profiles that can be used are presented. The system informs about the available capacity and presents those bandwidth profile instances that can be used.

5.2.8 Definitions

5.2.8.1 From Metro Ethernet Forum

AVC	Attribute Value Change
Bandwidth Profile	A characterization of ingress Service Frame arrival times and lengths at a reference point and a specification of the disposition of each Service Frame based on its level of compliance with the Bandwidth Profile. In this document the reference point is the UNI.
CE-VLAN ID	Customer Edge VLAN ID
Committed Burst Size	CBS is a Bandwidth Profile parameter. It limits the maximum number of bytes available for a burst of ingress Service Frames sent at the UNI speed to remain CIR-conformant.
Committed Information Rate	CIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of ingress Service Frames up to which the network delivers Service Frames and meets the performance objectives defined by the CoS Service Attribute.
CoS[1]	Class of Service
Coupling Flag[2]	CF is a Bandwidth Profile parameter. The Coupling Flag allows the choice between two modes of operations of the rate enforcement algorithm. It takes a value of 0 or 1 only.
Egress Service Frame	A Service Frame sent from the Service Provider network to the CE.
E-LAN Service	Ethernet LAN Service
E-Line Service	Ethernet Line Service
Ethernet LAN Service	An Ethernet Service Type distinguished by its use of a Multipoint-to-Multipoint EVC.
Ethernet Line Service	An Ethernet Service Type distinguished by its use of a Point-to-Point EVC.
Ethernet Virtual Connection	An association of two or more UNIs that limits the exchange of Service Frames to UNIs in the Ethernet Virtual Connection.
EVC	Ethernet Virtual Connection
Excess Burst Size	EBS is a Bandwidth Profile parameter. It limits the maximum number of bytes available for a burst of ingress Service Frames sent at the UNI speed to remain EIR-conformant.

Excess Information Rate	EIR is a Bandwidth Profile parameter. It defines the average rate in bits/s of ingress Service Frames up to which the network may deliver Service Frames without any performance objectives.
Ingress Service Frame	A Service Frame sent from the CE into the Service Provider network.
Service Frame	An Ethernet frame transmitted across the UNI toward the Service Provider or an Ethernet frame transmitted across the UNI toward the Subscriber.
Service Level Agreement	The contract between the Subscriber and Service Provider specifying the agreed to service level commitments and related business agreements.
Service Provider	The organization providing Ethernet Service(s).
Subscriber	The organization purchasing and/or using Ethernet Services.
UNI	User Network Interface
User Network Interface	The physical demarcation point between the responsibility of the Service Provider and the responsibility of the Subscriber.

1.Not implemented in this release

2.Not implemented in this release

5.2.8.2 Other definitions

Policing	Used as name for the functional block on NE performing rate limiting. Also used as a synonym for rate limiting.
Rate limiting	A function that uses the data from the bandwidth profile to limit the rate of the traffic in a defined flow of service frames.
MEN	Metro Ethernet Network.

5.3 Ethernet Service Wizard

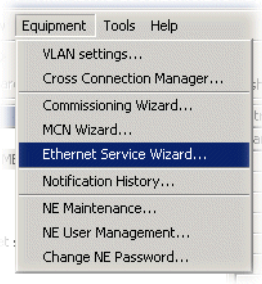
Before continuing with the described management tasks, make sure that:

- the network elements are physically installed in the field.
- modules are provisioned.
- the physical topology of the network is known.
- the management communication network has been configured and the user has management connection to AXX network elements in the network.
- the network elements have been configured and are ready for setup of user traffic.

NOTE! Make sure that the end points of a service have the same configuration if required, since the wizard is not end-to-end aware.

5.3.1 Start the Ethernet Service Wizard

1. From the **Equipment** menu select **Ethernet Service Wizard**.



READ MORE: “Configuration examples” on page 239.

5.3.2 Welcome page

With the wizard you can configure UNI's and provision Ethernet services on the following network elements:

- AXX 9100 CONNECT (R1.2)
- AXX 9200 EDGE (R2.3).

The wizard helps you configure UNIs and Ethernet Services on one NE.

NOTE! The wizard is only used for creation. General management of existing Ethernet services and UNI's is done from the Management Tree application. See “Ethernet Services - Maintenance” on page 226.

NOTE! **After completing a wizard flow you need to re-open the wizard to start a new flow.** This is due to limitations in the framework of the first wizard release.

Click Next when you are ready to begin the provisioning process.

5.3.3 NE and Task Selection

The task selection page allows you to choose between Ethernet Service or UNI Definitions.

Using AXX 9840 INSITE you will also select network element on this page.

Using AXX 9820 CRAFT this page is called Task Selection since the you are already connected to the NE.

Ethernet Service

Provision a new Ethernet service on the target network element. The wizard will not let you provision any Ethernet service unless there exist UNI's and bandwidth profiles instances on the network element.

NOTE! The wizard is only provisioning the service on one network element at a time and must be re-run on all elements containing UNI's in the service to provision the Ethernet service network wide.

UNI Definitions

Configure UNI's (User Network Interface) on the network element. All LANx ports on the network element can be configured as UNI's.

NOTE! At least one UNI on the network element is a pre-requisite for Ethernet service provisioning.

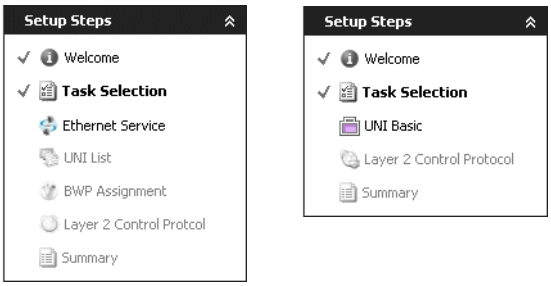


Figure 2 Setup steps - Overview

5.3.3.1 Dispositions

The table below displays the dispositions set creating a UNI and what dispositions that are editable or already set, when creating a Service on this UNI.

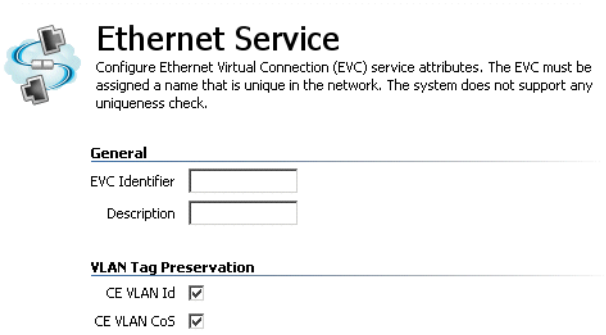
Table 4 Dispositions - overview

		Dispositions						
		Set per UNI			**Set per Service**			
		Pass to EVC	Discard	Peer	Tunnel (default)/ Discard (opt)	Discard by UNI	Peer by UNI	Forward Unchanged/ Discard
Layers	L1	X						X
	L1		X			X		
	L1			N/A				
	L2	X			X			
	L2		X			X		
	L2			X			X	

5.4 Create Ethernet Service

In this page configure the EVC service attributes. The Ethernet Service must be assigned a name that is unique in the network. The system does not support any uniqueness check.

1. Assign an Ethernet service name (there is a one-to-one relation between Ethernet service and EVC) that must be unique in the MEN.

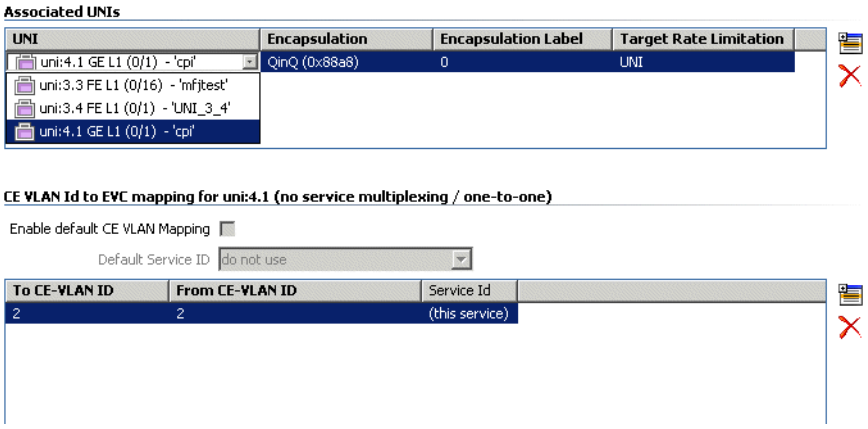


2. Configure the preservations attributes .

Attributes	Description
EVC Identifier	Unique name of the Ethernet Virtual Connection (EVC).
Description	Administrative description
VLAN Tag Preservation	Ensures that the CE VLAN tag is preserved when transported in MEN.
CE VLAN Id	Uncheck to disable. See “Dispositions” on page 210.
CE VLAN CoS	Uncheck to disable.See “Dispositions” on page 210.

5.4.1 UNI List

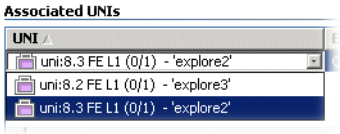
The UNI List page consist of two tables, the first one is where you add UNI's to the Ethernet Service and the second is where you view and add CE VLAN entries to the selected UNI.



The system verifies that the necessary building blocks (bandwidth profiles and UNI's) exist. If a building block is missing, the system informs you and does not start the Create Ethernet service wizard flow.

When you want to add a UNI to the list you will only be presented the UNIs that are not already added to the list, so this combo box will diminish until you cannot add any more (in which case the Add button is disabled).

3. Click **Add** and select one or more UNI's.



For the CE VLAN list (for each UNI), the table lists the CE VLANs that are already part of that UNI and allow you to add more. The ones that are already in the list will be disabled and cannot be edited or deleted (The Delete icon to the right will be disabled when you select one of these rows). But you can add new ones that will be fully editable and deletable.

Note that ranges of CE VLAN ID's are mapped. A range can contain one or more ID's, and that maximum 129 ranges are allowed.

For the CE VLAN list (for each UNI), the table lists the CE VLANs that are already associated with services on that UNI. You can add new CE VLAN's for this service

4. In the CE VLAN ID list click **Add**.

For each associated UNI, you must configure which CE VLAN ID('s) that are mapped to this the EVC (Ethernet service.). The CE VLAN ID, i.e. the VLAN ID of a VLAN in the customer network, identifies an EVC on a UNI. If more than one CE VLAN ID is mapped to an EVC, the UNI must have the bundling attribute enabled and if the all-to-one-bundling attribute is set, all CE VLAN ID's are mapped to one EVC.

5. Determine if a provider VLAN should carry the service, and if so, configure the encapsulation type to be used and the provider VLAN tag.

Associated UNIs

Attributes	Descriptions
UNI	Available User Network Interfaces
Encapsulation See “Encapsulation” on page 214	QinQ 0x88a8 QinQ 0x8100 QinQ 0xFFFF
Encapsulation label	VLAN tag used by the provider VLAN
Target Rate Limitation	UNI or UNI-EVC

Selected UNI CE VLAN Id to EVC Mapping

Attributes	Description
Use default CE VLAN Mapping	Check to enable
Default Service Id	Select Do not use or a defined Service Id
From CE VLAN Id	Customer Edge VLAN Id
To CE VLAN Id	Customer Edge VLAN Id
ServiceId	System generated service identification

5.4.1.1 Encapsulation

Rule 1:
Ports cannot run 802.1q if CE-VLAN CoS preservation is enabled.

Rule 2:
Ports cannot run 802.1q if CE-VLAN Id preservation and bundling is enabled.

Table 5 Legend for the next two tables

UNI	Def
NSM-121	No Service Multiplexing/One-to-one
NSM-B	No Service Multiplexing/Bundling
NSM-A21	No Service Multiplexing/All-to-one
SM-121	Service Multiplexing/One-to-one
SM-B	Service Multiplexing/Bundling

Layer 1

For services EVPL, EPLAN and EVPLAN.

Table 6 Encapsulation - Layer 1

UNI	CE VLAN ID	CE VLAN COS	Encapsulation
NSM-121	X	X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
NSM-121			None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
NSM-121	X		None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
NSM-121		X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
NSM-B	X	X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
NSM-B			None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
NSM-B	X		None/.QinQ(0x8100)/QinQ(0xFFFF).
NSM-B		X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
NSM-A21	X	X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
NSM-A21			None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
NSM-A21	X		None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
NSM-A21		X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
SM-121	X	X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
SM-121			None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
SM-121	X		None/802.1q/QinQ(0x8100)/QinQ(0xFFFF).
SM-121		X	QinQ(0x88a8)/QinQ(0x8100)/QinQ(0xFFFF).
SM-B	X	X	QinQ(0x88a8).
SM-B			Not allowed. CE VLAN ID must be enabled.
SM-B	X		QinQ(0x88a8).
SM-B		X	Not allowed. CE VLAN ID must be enabled.

Layer 2

For services EVPL, EPLAN and EVPLAN.

Table 7 Encapsulation - Layer 2

UNI	CE VLAN ID	CE VLAN COS	Encapsulation
NSM-121	X	X	QinQ.
NSM-121			802.1q/QinQ.
NSM-121	X		802.1q/QinQ.
NSM-121		X	QinQ.
NSM-B	X	X	QinQ.
NSM-B			Not allowed. CE VLAN ID must be enabled.
NSM-B	X		QinQ.
NSM-B		X	Not allowed. CE VLAN ID must be enabled.
NSM-A21	X	X	QinQ.
NSM-A21			Not allowed. CE VLAN ID must be enabled.
NSM-A21	X		802.1q/QinQ.
NSM-A21		X	Not allowed. CE VLAN ID must be enabled.
SM-121	X	X	QinQ.
SM-121			802.1q/QinQ.
SM-121	X		802.1q/QinQ.
SM-121		X	QinQ.
SM-B	X	X	QinQ.
SM-B			Not allowed. CE VLAN ID must be enabled.
SM-B	X		QinQ.
SM-B		X	Not allowed. CE VLAN ID must be enabled.

5.4.2 Bandwidth Profile Assignment

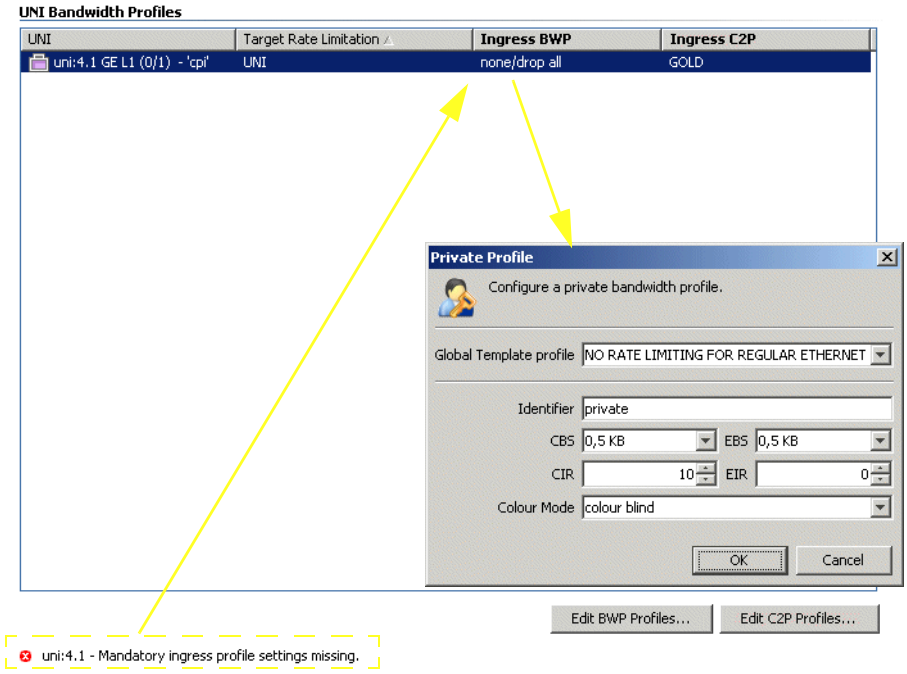
In this page a bandwidth profile is assigned to each specified flow of ingress service frames.

The **TargetRateLimitation** defines the flow that the IngressBWP is assigned to; either all service frames on UNI or all service frames on UNI for a specific EVC.

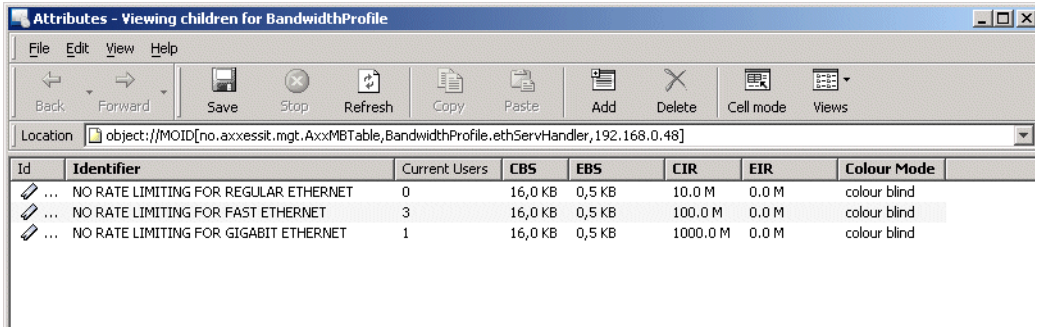
The conformance to the IngressBWP gives a service frame a colour.

The **IngressC2P** defines the mapping of the frame colour to a priority value (802.1p PRI.) The priority determines the traffic class on the output port (see Bridge Traffic Control configuration.)

The topmost table will list all the globally defined bandwidth profiles as well as an option called "private profile". If you select this private profile, a dialog box will open, allowing you to configure a bandwidth profile specifically for this service or UNI.



Press **Edit BWP Profiles** in lower left corner of the wizard page to open the Global Bandwidth profiles in a generic attribute window.



This window shows the table as you would have seen it from the Management Tree. When new profiles are added here, they will show up in each dropdown list in the wizard page tables.

6. Select a bandwidth profile target type for the service.

7. Attach Bandwidth profiles to the specific target instances (specific flow of service frames.) The target instance is determined by the bandwidth profile target value:

Target: UNI
Associate ingress bandwidth profiles to each UNI.

Target: EVC
Associate ingress bandwidth profiles to each combination of UNI and EVC.

8. You can tell the system to use selected Bandwidth profile as a **template** for creating a new bandwidth profile instance. The system will create a new bandwidth profile instance with filled in values from the "template" except the profile name. You can edit all attributes.

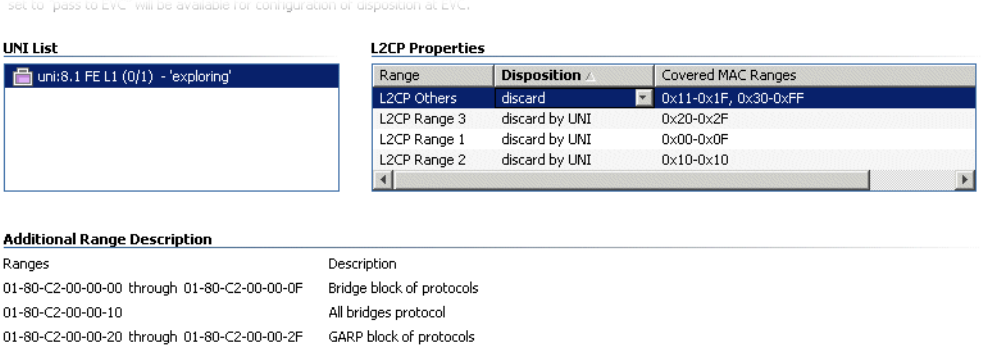
UNI Bandwith Profiles

Attributes	**Description**
UNI	
Target Rate Limitation	
Ingress BWP	none/drop all or private; NO RATE LIMITING FOR REGULAR ETHERNET, NO RATE LIMITING FOR FAST ETHERNET , NO RATE LIMITING FOR GIGABIT ETHERNET
Ingress C2P	GOLD, SILVER or BRONZE

5.4.3 Layer 2 Control Protocol

The last wizard page of the Ethernet flow is the Layer 2 Control Protocol service frame handling. Here you set the disposition for each range for each UNI that is configured to use EVC.

The left list contains all UNI's that are associated with the service/EVC. Selecting one UNI in the list, the L2CP Properties table displays L2CP setting for one UNI/EVC combination.



9. Configure the handling of the Ethernet service frames falling within one the L2CP ranges for each UNI. Legal values:

Discard: Discard all ingress service frames within the L2CP range and not generate any egress service frames carrying the L2CP range. Only allowed if UNI has L2CP range handling set to "Pass to EVC."

Tunnel: Carry L2CP service frames across the service provider network without being processed. Only allowed if UNI has L2CP range handling set to "Pass to EVC."

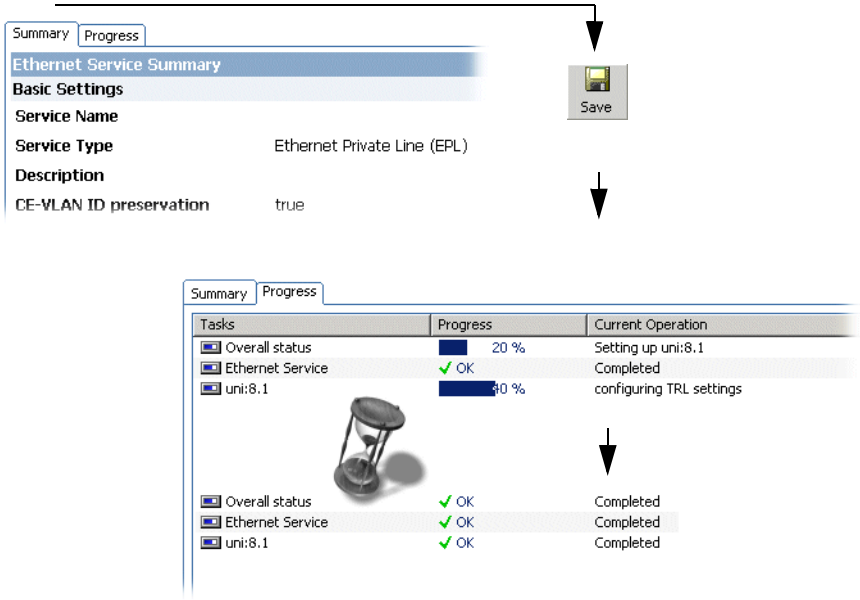
Forward unchanged:Only ports in L1. Only allowed if UNI has L2CP range handling set to "Pass to EVC."

L2CP Properties

Attributes	Description
Protocol	Name of
Disposition	Discard, tunnel or forward unchanged

5.4.4 Summary

The view will automatically switch to the Progress tab and show the progress of the Save operation.



10. Press **Save** to commit the changes.

The system updates the number of currently active EVC's on the UNI. The network element generates an object create notification to inform other connected management systems about the newly created Ethernet service instance.

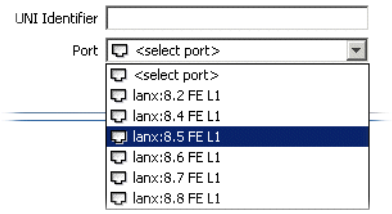
5.5 Create a UNI

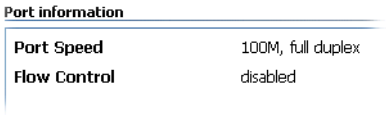
1. In the **Task Selction** select **UNI definitions** and click **Next**.

5.5.1 UNI Basic

In the first page you configure a LANx port as a UNI. A UNI must be assigned a name that is unique in the network. The system does not support any uniqueness check.

The UNI's properties are assigned default values when possible.





2. Enter a **name** for the UNI that is **unique** in the network.
3. Select **Port** .The system presents available LANx ports to be defined as UNI. The system differentiates between FE ports and GE ports.

NOTE! If a LANx port is a member of a VLAN where one or more other member ports are un-tagged and configured as UNI, all services on this UNI will be non-functional. The wizard does not stop you from doing this type of configuration and no error messages are reported from the element.

NOTE! You cannot change speed and duplex setting on a LANx port defined as UNI. Changes to port settings can only be done after removing services and disable UNI associated .

NOTE! In order to define a 10 Mb FE LANx as UNI, the port settings must be; full duplex fast and disabled autoneg.

4. Edit desired **UNI Properties**.

5. Enable **Storm Protection** if desired. Enter a value for Max packets per second if selected.

General/ Port selection

Attributes	Description
UNI Identifier	Assign a name to the UNI instance that is unique in the MEN.
Port	Select a LANx port. Physical port parameters for the LANx port, port speed and flow control are presented.

UNI Properties

Attributes	Description
Untagged VLAN ID	All traffic at the CE is untagged, will be assigned this VLAN ID. It is used for CE VLAN ID to EVC mapping.
Service multiplexing/bundling	no service multiplexing/one-to-one, no service multiplexing/bundling, no service multiplexing/all-to-one, service multiplexing/one-to-one or service multiplexing/bundling ling. The system handles the mutual dependencies between Dynamic behaviour between values Service multiplexing (SM,) all to one bundling (ATO,) and bundling (B) attributes: SM = Y => ATO =N ATO = Y => B = N B = Y => ATO = N
Default Port Priority	0-7

Storm protection

Attributes	Description
Broadcast	If enabled, Set Max packets per second
Multicast	If enabled, Set Max packets per second

Service multiplexing/bundling

Service multiplexing:
If service multiplexing is enabled on an UNI, the NI can be associated withe more than one service/EVC.

Bundling:
Ranges of CE VLAN ID’s can be mapped to service/EVC.

On to One bundling:
Only one CE VLAN ID for each service/EVC.

All to One bundling:
All CE VLAN ID’s at UNI will be mapped to one service/EVC

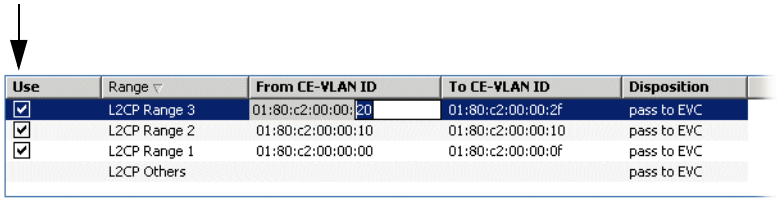
Table 8 Combinations of Service Multiplexing/ Bundling

	Combination 1	Combination 2	Combination 3	Combination 4	Combination 5
Service Multiplexing		x			x
Bundling		x	x		
All to One Bundling				x	
One to One Bundling	x				x

5.5.2 Layer 2 Control Protocol

The next page of UNI creation is to set the ranges and their disposition.

If the Use column is checked, you are able to edit the cells in that row. The From and To cells consist of an editor that always displays the "01:80:c2:00:00:" first and only the last octet is editable. The row with range "Others" does not have a Use, From or To cell.



You can specify from zero and up to three MAC address ranges and each range has its individual disposition value. All MAC addresses not included in a range fall into the "Others" range that is always present. The disposition of "Others" is configurable.

The disposition value tells the element how to treat a frame within the range.

6. Edit UNI ranges and their disposition.

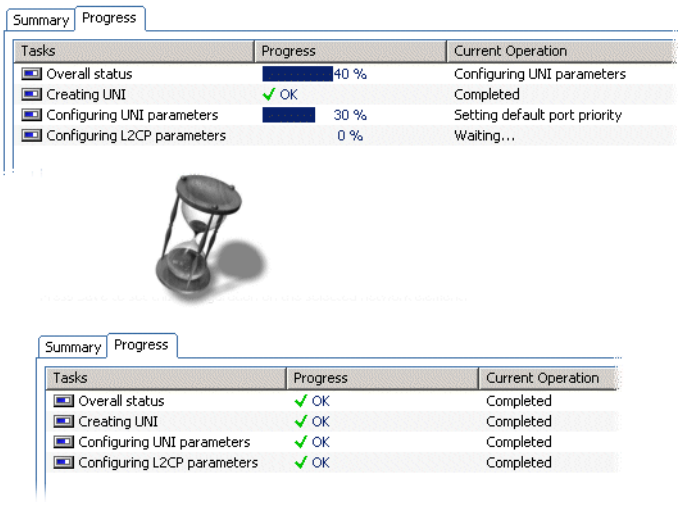
Attributes	**Description**
Use	Check to use selected Range
Range	L2CP Range 1 L2CP Range 2 L2CP Range 3 L2CP Range others
From CE-VLAN-ID	Mac adress. Only the last byte of the MAC address is configurable.

Attributes	Description
To CE-VLAN-ID	Mac adress. Only the last octet of the MAC address is configurable.
Disposition	Discard. Discard all ingress service frames within the L2CP range and not generate any egress service frames carrying the L2CP range. Note; with this choice the L2CP cannot be processed by an EVC.). Peer (only ports in L2). Acts as a peer of the CE in the operation of the service frames in the L2CP ranges. Note: with this choice the L2CP cannot be processed by an EVC. Pass to EVC . Handling determined by the L2CP handling attribute of the EVC's associated with the UNI.)

5.5.3 Summary

The Summary page shows the UNI you are about to create. Pressing Save will commit the changes.

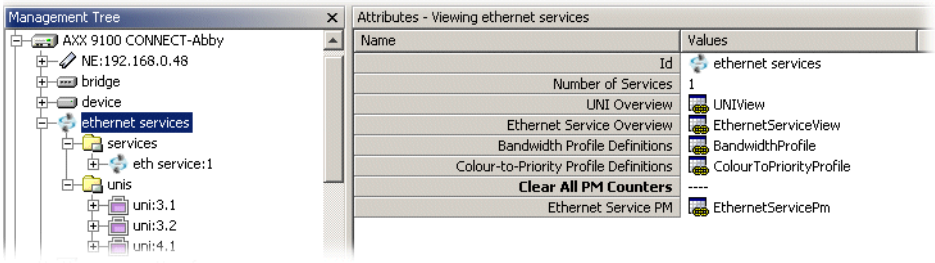
The view switch to the Progress tab and show the progress of this operation.



5.6 Ethernet Services - Maintenance

After using the Ethernet Services wizard you can use the Management tree for maintenance purposes on the active Ethernet services.

1. In the Management Tree select **ethernet services**.

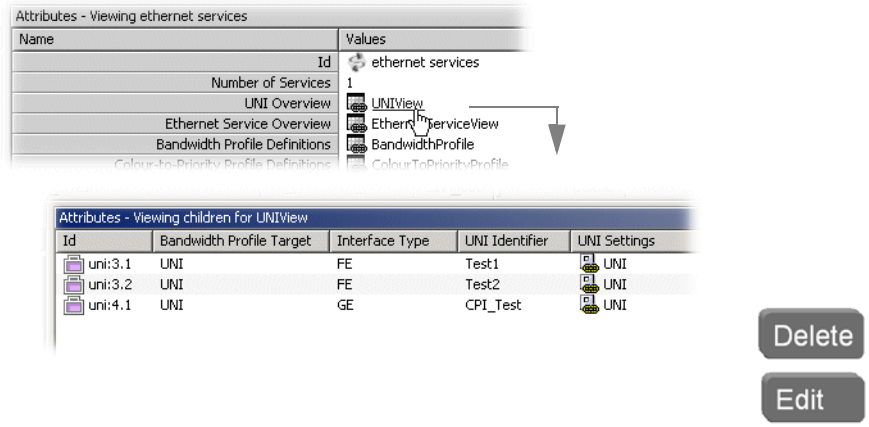


The following subsections describes the different maintenance tasks available.

Available management tasks are visualized as follow:

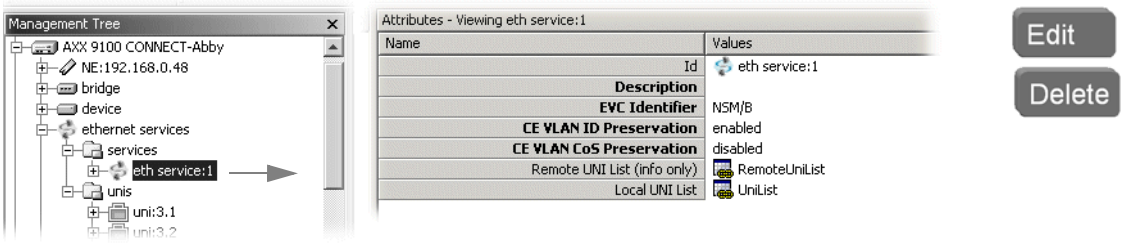
5.6.1 UNI Overview

Select UNIView to display attributes for currently defined UNIs.



For details on UNI settings see “Edit UNI's” on page 236.

5.6.2 Ethernet Service view



5.6.2.1 Edit Ethernet service

1. Select desired **Ethernet service** for editing.
2. Service related objects available for editing are displayed with bold text. If other changes are to be made, the service instance must be replaced by a new service.
3. Commit the updates.

Attribute value change notifications are generated to inform other connected management systems about the updated instance.

Id: System generated service identification

Description:Free text service description

EVC Identifier: Unique name of the Ethernet Virtual Connection

CE VLAN ID Preservation: enabled or disabled

CE VLAN CoS Preservation:enabled or disabled

Remote UNI List :
info only

Local UNI List:
info only

5.6.2.2 Delete Ethernet service

1. Select the **Ethernet Services** node in the **Management tree**.

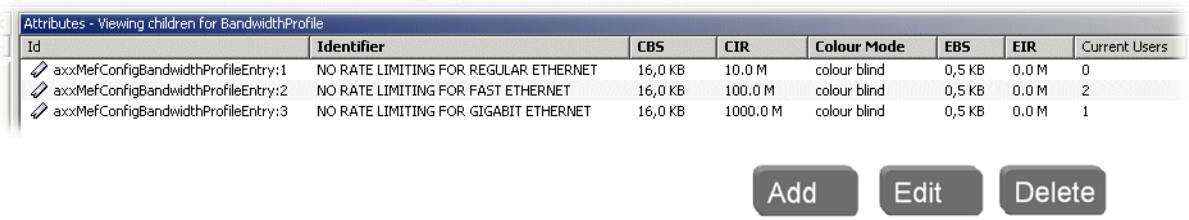
Select the **EthernetServiceView** . The system presents a list of all configured Ethernet services on the network element.

2. Select the **service to be deleted** and click **Delete**.

The system releases all associations to profiles and updates number of users for the profiles.

The system removes the Ethernet service CE VLAN ID(s) from the CE VLAN ID to EVC mapping contained by UNI's of the service. The system updates the number of currently active EVC's on UNI's. The system deletes PM data for this service. The system warns the user about the PM data deletion since this can have consequences for the e.g. billing data. An object delete notification is generated to inform other connected management systems about the newly deleted Ethernet service and related instances.

5.6.3 Bandwith Profile



The system presents a list of all bandwidth profiles. Each profile is presented with a flag indicating if the profile is currently associated with an Ethernet service

The CIR and EIR parameters can be set from 0 Mbps to 100 Mbps in steps of 500 Kbps for a FE port and from 0 Mbps to 1 Gbps in steps of 1 Mbps for a GE port. The CBS and EBS can be set up to 16 K for a FE port and for a GE port in steps of 512 bytes.

NOTE! Avoid setting CIR/EIR to x.5 values, when editing BW profiles used on GE ports.

Id: System generated entry identification

Identifier: Unique BW identifier

CBS:
Committed Burst Size (CBS) expressed as bytes.
Legal Values 0,5 KB - 16KB

CIR:
Committed Information Rate (CIR) expressed as bits per second.

Colour Mode: colour blind

EBS:
Excess Burst Size. Legal Values 0,5 KB- 16KB

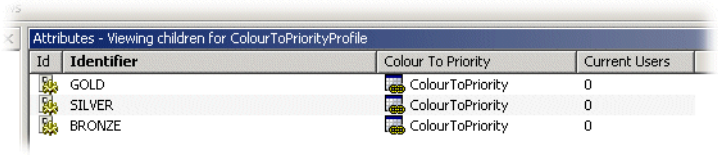
EIR:
Excess Information Rate expressed as bits per second. The total traffic limited by one instance of a profile is given by CIR+EIR.The CIR part will get a green mark and the EIR part will get a yellow mark.

Current Users:
Number of services currently using this profile.

5.6.3.1 Delete bandwidth profile

1. Select a bandwidth profile for deletion.
2. The system verifies that the bandwidth profile is not in use by any Ethernet service on the network element. If not in use, profile is deleted and an object delete notification is generated to inform other connected management systems about the newly deleted profile. If in use, the system warns and denies the deletion.

5.6.4 Colour-to-Priority (C2P)



Add Edit Delete

5.6.4.1 Edit Colour to priority profiles

The system presents a list of all Colour to priority profile instances. Each instance is presented with a flag indicating if the profile is currently associated with one or more Ethernet services.

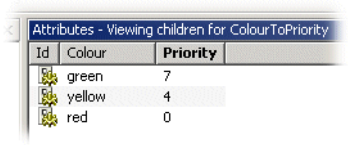
1. Select a Colour to priority profile instance to be updated. A profile instance in use cannot be edited.
2. Update the mappings.
3. Click **Save**.

Attribute value change notifications are generated to inform other connected management systems about the updated instance.

Id: System generated entry identification

Identifier: Unique name of profile entry

Colour To Priority



Add Edit Delete

Current Users: Display number of users using the profile.

5.6.4.2 Delete Colour to priority profiles

1. Select a priority to mapping instance for deletion.
2. Click **Delete** and the **Save**.

The system verifies that the selected profile instance is not in use by any Ethernet service on the network element.

3. If not in use, profile instance is deleted and an object delete notification is generated to inform other connected management systems about the newly deleted profile.

5.6.5 Ethernet Service PM

The network elements support performance monitoring per flow. It is reported data about the number of ingress and egress green, yellow, and red frames and green, yellow, and red octets. Green frames are the frames that conform to the CIR/CBS part of the bandwidth profile and are the traffic that can be guaranteed. The yellow frames are the frames that meet the EIR/EBS part of the profile.

The red frames are the frames that violate both the CIR/CBS and EIR/EBS parameters and are remarked or dropped.

Performance data is available for all flows.

The available time periods are

- 15 minutes (MEF requirement)
- 24 hours

The network element holds current data and historical data, the number of historical time periods are

- 32x15 minutes (MEF requirement)
- 1x24 hours

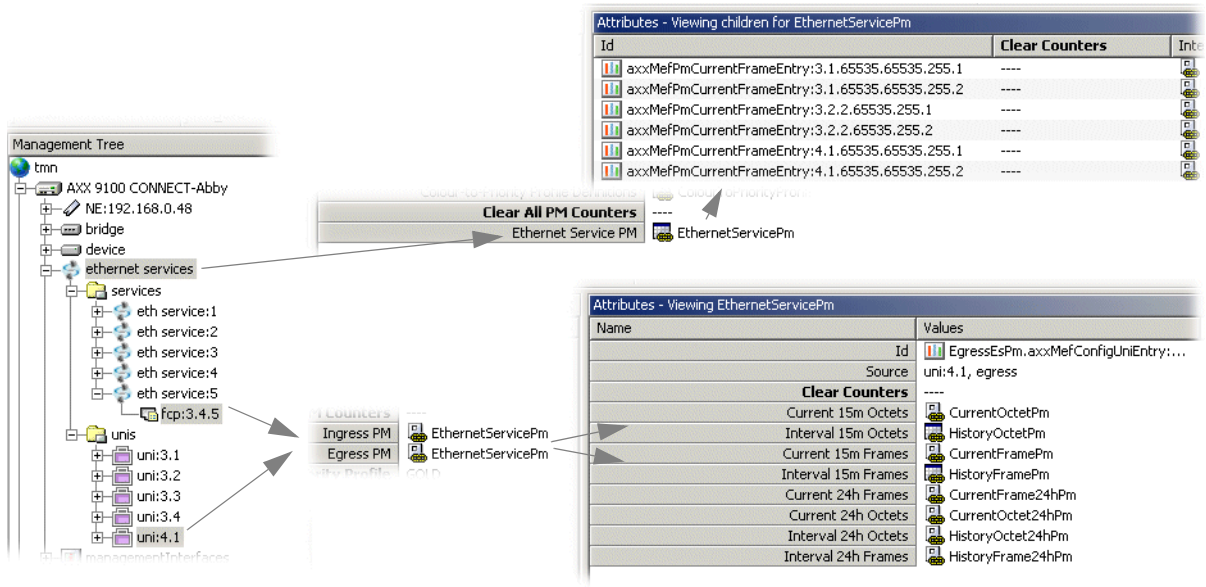


Figure 3 Performance monitoring - overview

5.6.5.1 Clear PM Counters

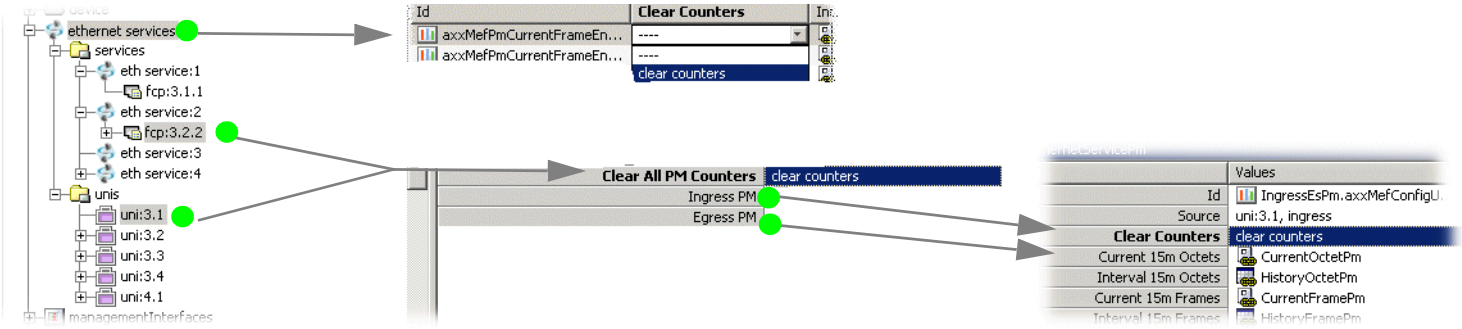
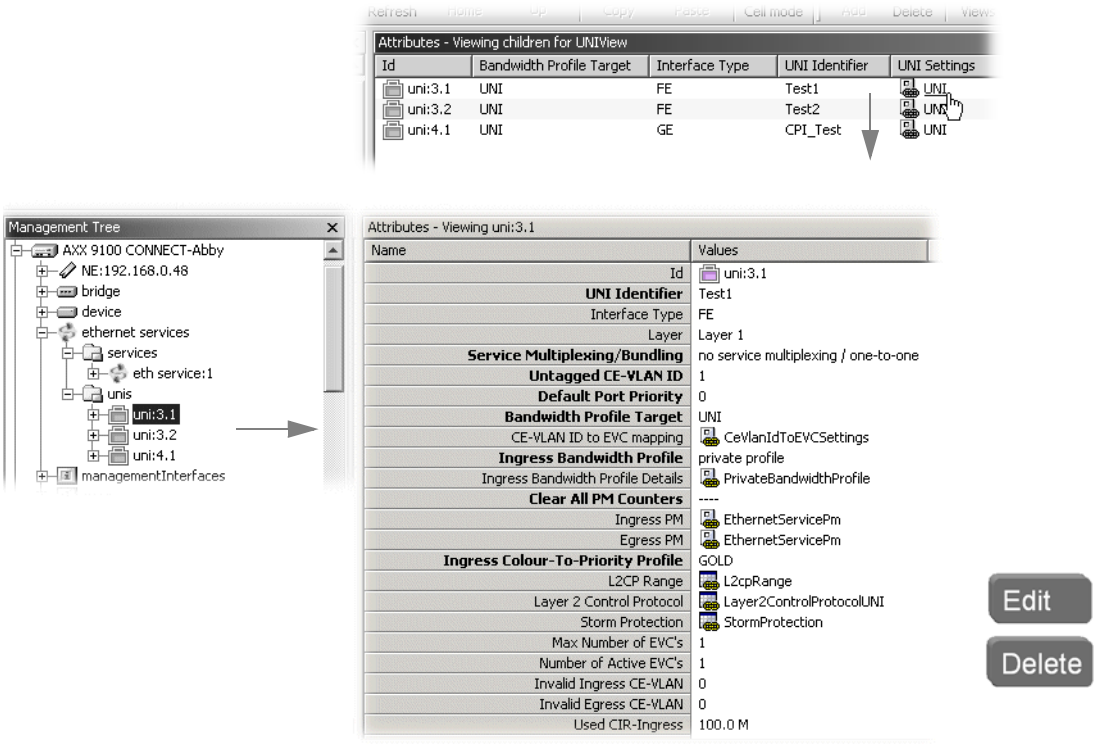


Figure 4 Clearing PM counters - overview

5.6.6 UNI



5.6.6.1 Edit UNI's

1. Select a UNI object for editing. Click UNI Settings

The system presents those attributes that can be edited based on the knowledge about the usage of the UNI object.

Attribute value change notifications are generated to inform other connected management systems about the updated UNI attributes.

Id: System generated entry identification

UNI Identifier: Name of the UNI instance that is unique in the MEN.

Interface Type:FE or GE

Layer: Layer 1 or Layer 2

Service Multiplexing/Bundling:
no service multiplexing/ one-to-one , no service multiplexing/bundling, no service multiplexing/all-to-one, service multiplexing/ one-to-one or service multiplexing/bundling

Untagged CE-VLAN ID:
Untagged Customer Edge VLAN ID

DefaultPortPriorty: 0-7

Bandwith Profile Target: UNI or UNI-EVC

CE-VLAN ID to EVC mapping:
Click to display; Id, From CE-VLAN ID, To CE-VLAN ID and Service Id

Ingress Bandwith Profile:
none/ drop-all or private

Ingress Bandwith Profile Details:
Id, Identifier, CIR, CBS , EIR, CBS , Colour Mode and number of Current Users.

Clear All PM Counters:
clears counters

Ingress PM:
Click EthernetServicePm to display PM data

Ingress Colour-to-Priority Profile:
Gold, silver ,bronze and user defined profiles

L2CP Range:
Id, Range , From -To (MAC address range)

Layer 2 Control Protocol:
Id, Range and Disposition

Storm Protection
Id; Storm Protection (type), Maximum Number of Packets, enable/disable and Number of Dropped Packets

Max number of EVCs:
Maximum number of EVCs that the UNI can support

Number of Active EVCs:

Invalid Ingress CE-VLAN:

Invalid Egress CE-VLAN:

Used CIR-Ingress:
Committed Burst Size expressed as bits per second

Used EIR-Ingress:
Excess Information Rate expressed as bits per second

Used CBS-Ingress:
Committed Burst Size expressed as bytes

Used EBS-Ingress:
Excess Burst Size (EBS) expressed as bytes

5.6.6.2 Delete UNI's

1. Select a UNI instance for deletion.

The system verifies that the selected UNI instance is not associated with any Ethernet service on the network element.

2. If no associations exist, the UNI instance is deleted and an object delete notification is generated to inform other connected management systems about the newly deleted UNI.

5.7 Configuration examples

5.7.1 Application of services

Metro Ethernet Forum (MEF) specifies two generic types of services: E-Line (point-to-point) and E-LAN (multipoint-to multipoint.)

These two generic service types can be used to build more specific Ethernet service applications in the network.

Guidelines for four specific Ethernet service applications are described in the following sections. You must yourself make sure that the configuration is applied according to this specification on all involved UNI's and EVCs in service.

All values are legal for those service attributes that are not explicitly listed here.

5.7.2 Ethernet Private Line (EPL)

This is a point-to-point service on layer 1, i.e., it is a service between two LANx ports operating on layer 1. Ethernet service frames are not processed. Multiple EPL services can be active in one network element. The total number of this service type on an element is limited by the total aggregate capacity, the number of EoS mappers, and the number of physical Ethernet interfaces. A UNI can only support one EPL service instance.

The service is supported on both FE and GE ports. Since it is a layer 1 service the EoS mapper capacity sets the upper limit to the bandwidth profile settings, i.e., CIR, CBS, EIR, and EBS.

The rate limiting function can be applied on UNI and EVC service frames flows. Rate limiting can reduce the traffic capacity of the EPL below the EoS capacity.

The Ethernet service traffic is subject to the priority to queue mapping defined for the involved LANx port.

Non-conforming traffic can be treated in two different ways; either using flow control to prevent buffer overflow or by dropping packets when the buffer is full.

Performance management data related to this service is available as RMON data on LANx port, as G.826 data on involved SDH objects, and as performance data counters for Ethernet service.

Tunnelling of user traffic and layer 2 control protocols may be used on network element to make it possible to create layer 2 services in another element.

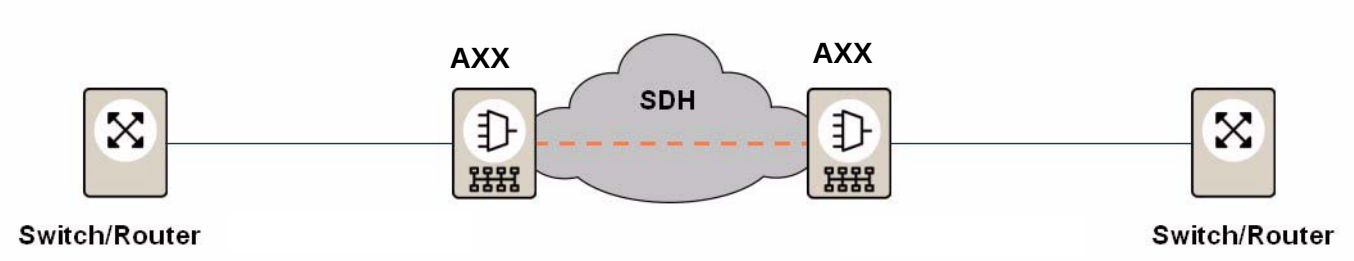


Figure 5 Ethernet Private Line service - - a layer 1 service

UNI service attributes	**Values**
LANx port mode	Full Duplex
Service Multiplexing	No
Bundling	No
All to One Bundling	Yes
CE-VLAN ID to EVC Mapping	All service frames to single EVC
Maximum number of EVC's	1
Bandwidth Profile Per Ingress	
UNI	
CIR	<= UNI Speed
CBS	> largest service frame size
EIR	0
EBS	0
CM	color-blind
CF	Not Specified

EVC service attributes	Values
EVC Type	Point-to-Point
UNI List (local and remote)	Two UNI's associated with the EVC
CE-VLAN ID Preservation	Yes
CE-VLAN CoS Preservation	Yes

Layer 2 Control Protocol	Values
Spanning Tree Protocols (STP, RSTP and MSTP)	Tunnel
Link Aggregation Control Protocol (LACP)	Tunnel
Link OAM (802.3ah)	Tunnel
IEEE 802.1x Port Authentication protocol	Tunnel
Generic Attribute Registration Protocol (GARP)	Tunnel
GARP VLAN Registration Protocol (GVRP)	Tunnel
GARP Multicast Registration Protocol (GMRP)	Tunnel
Multicast to all bridges in a bridged LAN on standard address	Tunnel

5.7.3 Ethernet Virtual Private Line (EVPL)

The EVPL service is essentially an EPL service where the data streams from multiple subscribers, share a common transport network resource (an EoS connection between WAN/WANx interfaces.) It is a L1 service, but the L2 switching capability is used for the grooming of the traffic from the different subscribers. The total number of this service type on an element is limited by the total aggregate capacity, the number of EoS mappers, and the number of physical Ethernet interfaces. The different EVPL services can be routed in different directions in the network.

The service is supported on both FE and GE ports. Since it is a layer 1 service the EoS mapper capacity sets the upper limit to the bandwidth profile settings and the sum of e.g. CIR for all EVPL services cannot be higher than the EoS capacity.

The rate limiting function can be applied on UNI and EVC service frames flows. Non-conforming traffic is remarked with lower priority. The non-conforming traffic is dropped if there is congestion in the network. It is also possible to drop non-conforming traffic without remarking the packets.

The Ethernet service traffic is subject to the priority to queue mapping defined for the involved LANx port.

Provider bridging is used to transport the traffic from the different subscribers transparently through the network. The service provider is inserting an additional VLAN tag that is unique for the subscriber. The VLAN tag is used to separate the traffic from the different subscribers.

Performance management data related to this service is available as RMON data on LANx port, as G.826 data on involved SDH objects, and as performance data counters for Ethernet service.

Tunnelling of user traffic and layer 2 control protocols may be used on network element to make it possible to create layer 2 services in another element.

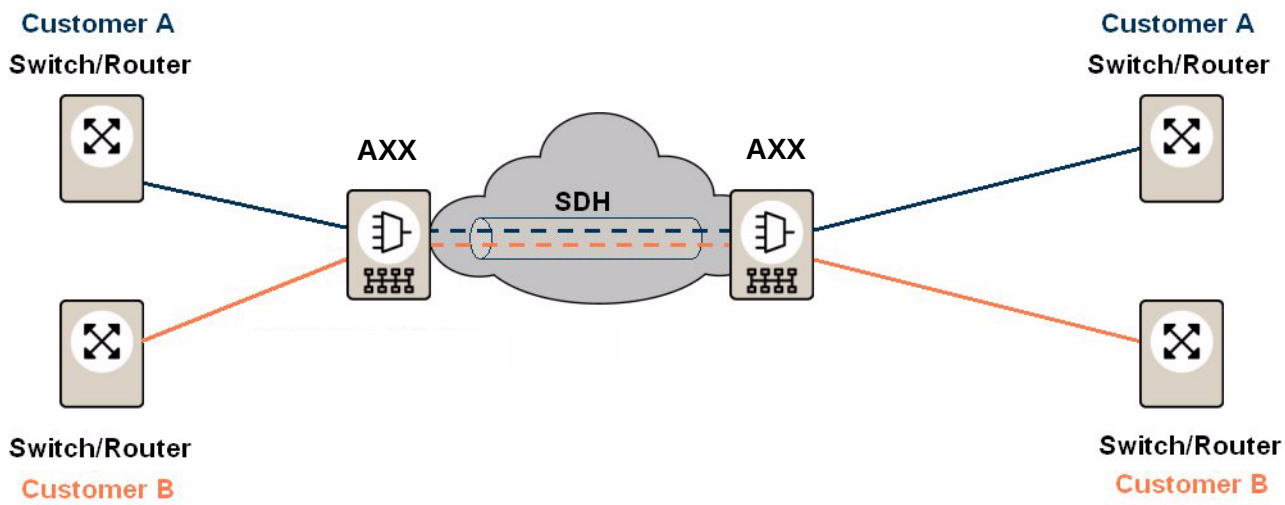


Figure 6 EVPL service

UNI service attributes	Values
Mode	Full Duplex
Service Multiplexing	Yes => All-to-one -> No
Bundling	If Yes, then CE-VLAN ID Preservation -> Yes No if All to One Bundling =Yes
All to One Bundling	If Yes, then CE-VLAN ID Preservation -> Yes No if Bundling or Service Multiplexing = Yes
Maximum number of EVCs	>= 1

EVC service attributes	Values
EVC Type	Point-to-Point
UNI List (local and remote)	Two UNI's associated with the EVC
CE-VLAN ID Preservation	Yes/No
CE-VLAN CoS Preservation	Yes/No

Layer 2 Control Protocol	Values
Spanning Tree Protocols (STP, RSTP and MSTP)	Discard
Link Aggregation Control Protocol (LACP)	Discard
Link OAM (802.3ah)	Discard
IEEE 802.1x Port Authentication protocol	Discard
Generic Attribute Registration Protocol (GARP)	Discard
GARP VLAN Registration Protocol (GVRP)	Discard
GARP Multicast Registration Protocol (GMRP)	Discard
Multicast to all bridges in a bridged LAN on standard address	Discard

5.7.4 Ethernet Private LAN (EPLAN)

The EPLAN service provides LAN-type connectivity between multiple subscriber sites through dedicated connections. It is a L2 service and the Ethernet frame is fully processed. Multiple EPLAN services can be active in the network element. The number is limited by the total aggregate capacity, the number of EoS mappers, and the number of physical Ethernet interfaces. The different Ethernet services can be routed in different directions in the network.

The service is supported on both FE and GE ports.

The rate limiting function can be applied on UNI, future (UNI&CoS), EVC, and future (EVC&CoS) service frames flows. Non-conforming traffic is remarked with lower priority. The non-conforming traffic is

dropped if there is congestion in the network. It is also possible to drop non-conforming traffic without remarking the packets.

The Ethernet service traffic is subject to the priority to queue mapping defined for the involved LANx port.

Provider bridging is used to transport the traffic from the different subscribers transparently through the network. The service provider is inserting an additional VLAN tag that is unique for the subscriber. The VLAN tag is used to separate the traffic from the different subscribers.

Performance management data related to this service is available as RMON data on LANx port, as G.826 data on involved SDH objects, and as performance data counters for Ethernet service.

Tunnelling of user traffic and layer 2 control protocols may be used on network element to make it possible to create layer 2 services in another element.

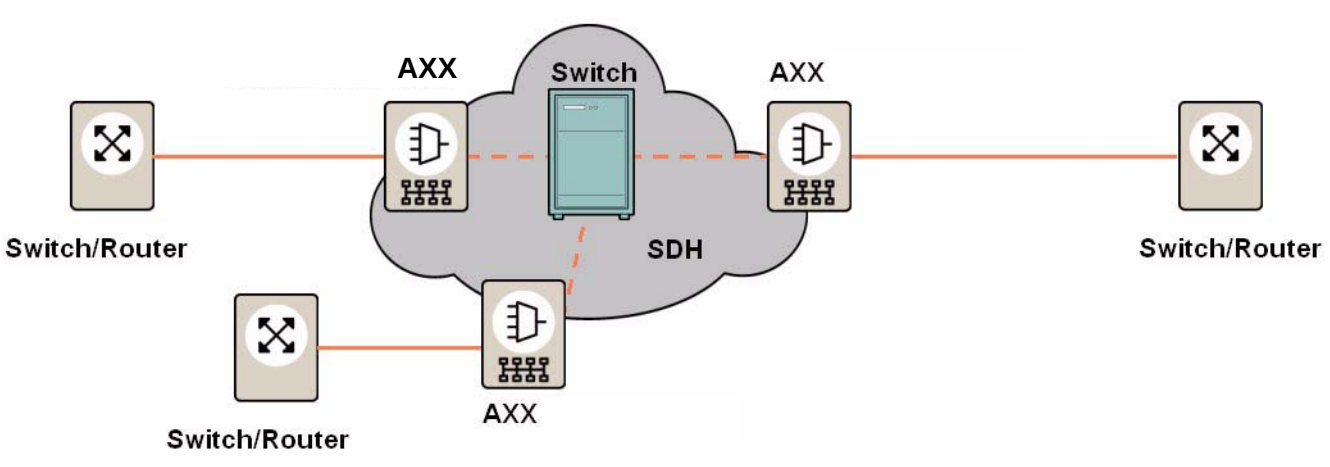


Figure 7 EPLAN based on a network topology with a centralised switch

UNI service attributes	Values
	No specific requirements

EVC service attributes	Values
EVC Type	Multipoint-to-multipoint
UNI List	Two or more UNI's associated with the EVC
CE-VLAN ID Preservation	Yes/No
CE-VLAN CoS Preservation	Yes/No

5.7.5 Ethernet Virtual Private LAN (EVPLAN)

This service is a combination of EVPL and EPLAN. The bandwidth is shared among different subscribers, as are switches and/or routers in the carrier network. Ultimately, the sharing of bandwidth in the transmission channels and switches gives EVPLAN the potential for very cost-effective carrier network resource use.

The EoS mapper capacity must be higher than the sum of guaranteed traffic from all subscribers. Multiple EVPLAN services can be active in the network element. The number is limited by the total aggregate capacity, the number of EoS mappers, and the number of physical Ethernet interfaces. The different Ethernet services can be routed in different directions in the network.

The service is supported on both FE and GE ports.

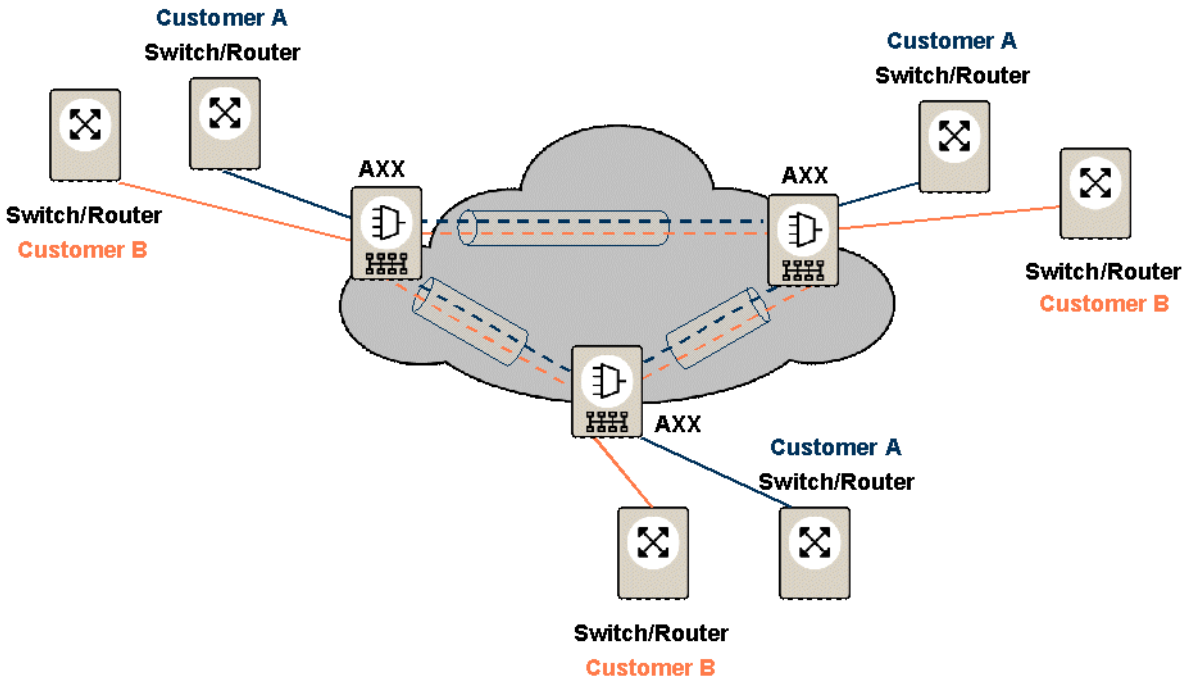
The rate limiting function can be applied on UNI and EVC and service frames flows. Non-conforming traffic is remarked with lower priority. The non-conforming traffic is dropped if there is congestion in the network. It is also possible to drop non-conforming traffic without remarking the packets.

The Ethernet service traffic is subject to the priority to queue mapping defined for the involved LANx port.

Provider bridging is used to transport the traffic from the different subscribers transparently through the network. The service provider is inserting an additional VLAN tag that is unique for the subscriber. The VLAN tag is used to separate the traffic from the different subscribers.

Performance management data related to this service is available as RMON data on LANx port and as G.826 data on involved SDH objects.

Tunnelling of user traffic and layer 2 control protocols may be used on network element to make it possible to create layer 2 services in another element.



UNI service attributes	Values
	No specific requirements

EVC service attributes	Values
EVC Type	Multipoint-to-multipoint
UNI List	Two or more UNI's associated with the EVC
CE-VLAN ID Preservation	Yes/No
CE-VLAN CoS Preservation	Yes/No

6 NE updates and upgrades

6.1 NE Maintenance

This section describes how to update and upgrade an NE with download files through the NE Maintenance GUI.

- Update:
  Maintenance release of an NE. Contains bug fixes and improvements, but no new functionality.
- Upgrade:
  Main version release of an NE. Contains new functionality.
- Configuration backup and restore is also described.

NOTE! AXX 9200 EDGE is used as an example in the presented procedures.
Where AXX 9300 METRO diverges, special sections and procedures indicate this.

NOTE! When a firewall is used, the TFPP port (port #69) on the target PC must be enabled when performing db backup.

READ MORE: The features presented are also available from the Management Tree, see “Software Download and Configuration Management Tree” on page 288.

6.1.1 Introduction

The NE contains device software and firmware, module software and firmware, license(s) and configuration data. See “NE support” on page 251.

Contact your assigned distribution channel to obtain software release available for updates and upgrades of the NE.

6.1.2 Software download process

The management system supplies the selected NE with the necessary information to start downloading new files. The download process is controlled by the element itself.

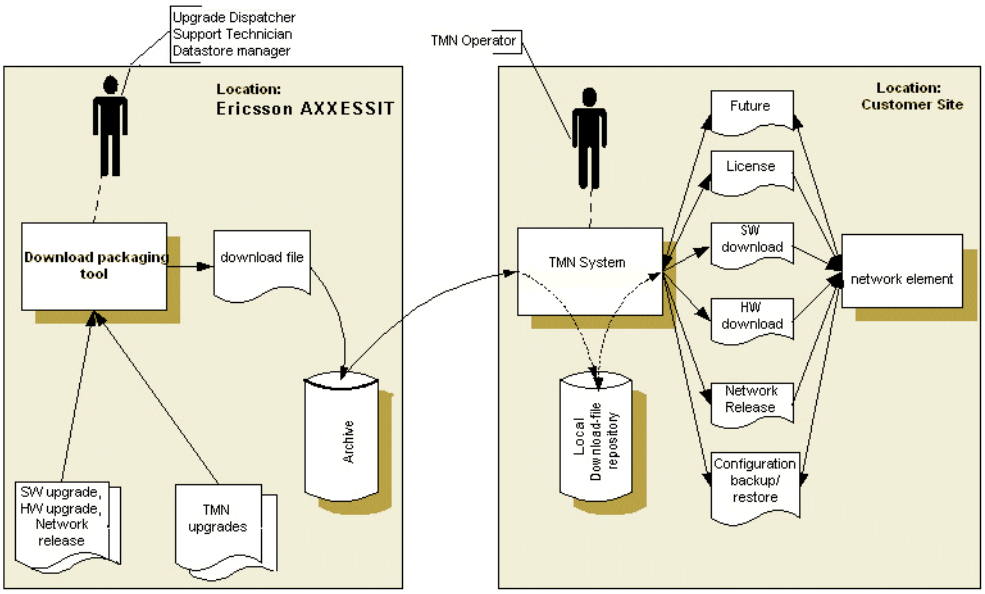


Figure 8 Software download process overview[1]

NOTE! A download file can contain AXX 9840 INSITE upgrades and patches for the management system itself. Handling of such tasks is not a part of this section.

An NE or NE plug-in module can be upgraded in the following ways:

6.1.2.1 Software upgrade

Software upgrade is performed as file downloads to the NE device or to selected modules.

6.1.2.2 Firmware upgrade

Some NE types have programmable hardware functionality through the use of FPGAs [2]. The hardware is upgraded by downloading files with new FPGA code.

1. Firmware is mentioned as hardware (HW) in figure above
2. FPGA: Field Programmable Gate Array

6.1.2.3 License upgrade

The license keys of the NE control the availability of NE features. License files contain information that activates or de-activates feature licenses in the NE.

6.1.2.4 Configuration backup and restore

Enables efficient backup and restore of the configuration of NEs. Configuration files are stored on local or remote file systems.

6.1.2.5 NE support

The NE Maintenance GUI support NEs as follows:

AXX 9300 METRO

- Network release and embedded software control file.
- Module software and firmware releases as part of a network release
- Scheduled and automatic restart of equipment after download completion.

AXX 9200 EDGE and AXX155A:

- Network release and embedded software control file.
- Plug- in module upgrade (remote module included: AXX10 for AXX 9200 EDGE).
- Software upgrade.
- License upgrade.
- Configuration backup and restore.
- Firmware (FPGAs) upgrade.
- Scheduled and automatic restart of equipment after download completion.

AXX155E and AXX155R2:

- Software upgrade.
- License upgrade.
- Configuration backup and restore.
- Manual restart of equipment after download completion.

NOTE! A network release supports a given set of traffic modules. If a new module is introduced, the NE needs a new network release.

NOTE! AXX 9300 METRO uses Network Releases only, so one single file is needed every time an update or upgrade is needed, regardless of the software or firmware type.

6.1.2.6 Download Files

There are two classes of download files: “Single download file” and “Network release download file”.
The download files have administrative information that tells the NE whether it is a SW, HW, license or configuration file. The files appear as *.package.zip, sorted in file browser as file type ‘Packages and Network Releases’.

Single download file

It consists of one file per download: Software file, firmware file, license file, and configuration file.

Network release download file

It is a collection of single download files which are combined and packed into one file. This download file contains one or more independent upgrade components:

- Device software
- Device firmware
- Device licenses
- Plug-in module software and firmware

This upgrade will be controlled by the embedded software on the NE which checks which components are included in the release and asks for upgrade of those components that are newer.

Location of shared download files

A prerequisite for software download is that the files are located in a directory where the TFTP download server can locate them. This is the `"./res/software" directory` of the installed AXX 9840

INSITE. The files may be placed in the download directory manually, or by use of the Package Installer, see page 6-263.

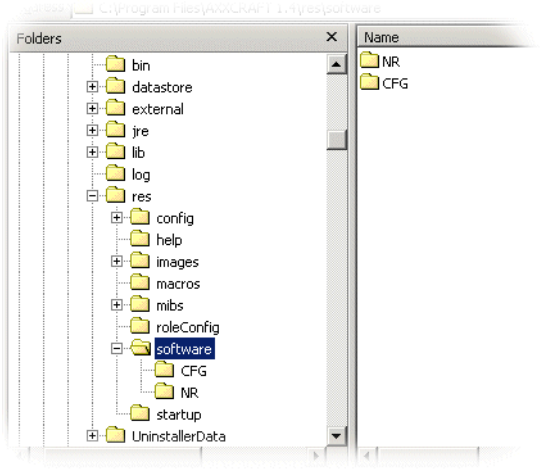


Figure 9 Central software directory - shared location of download files

6.1.3 TFTP server settings

The embedded FTP (File Transfer Protocol) host of the management system has a default interface setup. This is the first network host located on the computer.

AXX 9300 METRO uses SCP over SSH l to provide secure file transfer over a non-secure network (such as a TCP/IP network).

NOTE! External FTP host is not supported by the custom GUI. See “Software Download and Configuration Management Tree” on page 288 for details.

Procedure: **EDIT TFTP SERVER SETTINGS**

This procedure is for advanced users only, and applies to those environments with several IP interfaces.

1. Select **TFTP Server** in the GUI Information pane.

2. **Edit the address** to the desired host interface IP.

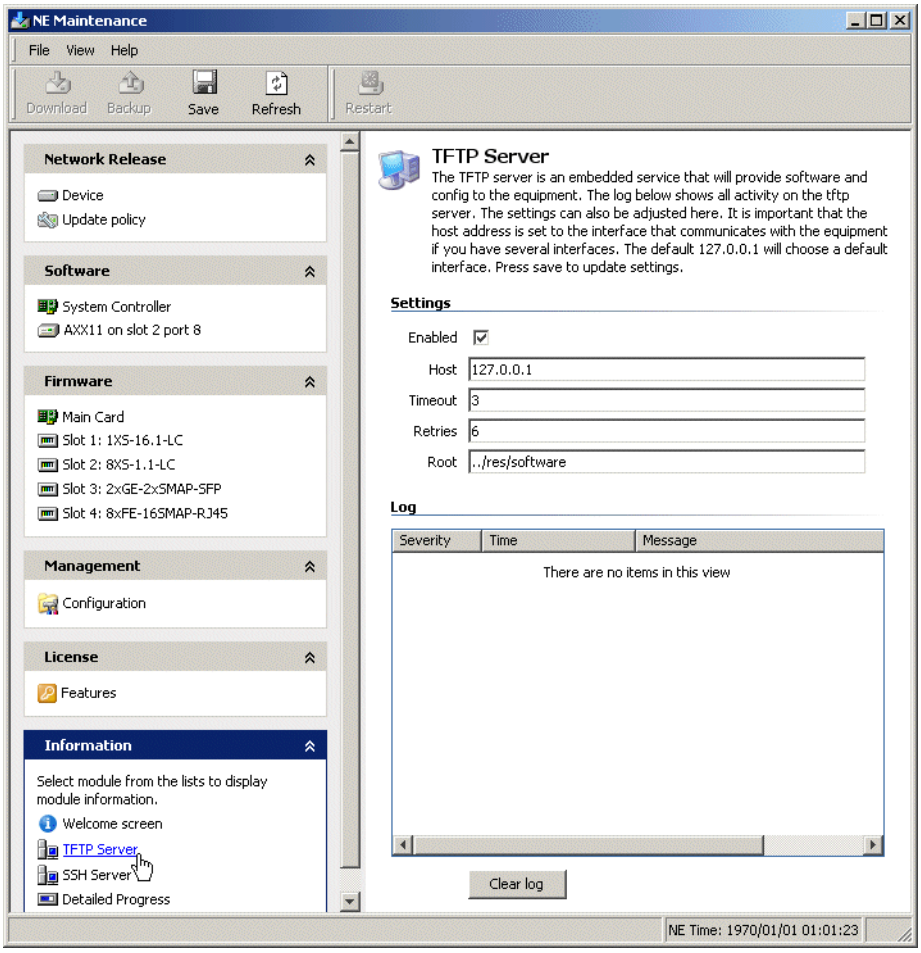


Figure 10 TFTP server settings - Interface IP example

Host: Host interface IP number to run the embedded TFTP server

Timeout: Number on TFTP server time-out in seconds

Retries: Number on package transmission in seconds

Root: Location of the TFTP data repository

NOTE! If the TFTP port is occupied by an other program this will be reported in the Error log.

6.1.3.1 Detailed Progress

Procedure: **VIEW DETAILED TFTP PROGRESS**

1. Click the **Detailed Progress link** in the **Information** pane to get a detailed overview of the download progress in a separate window:

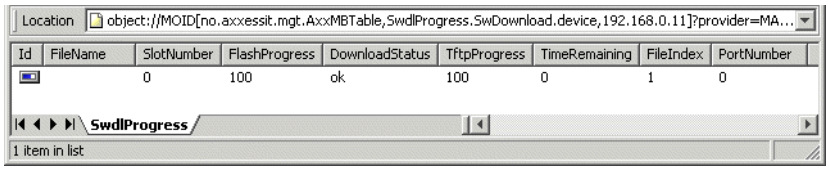


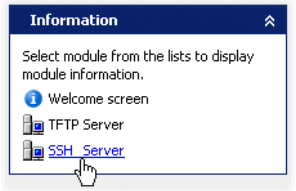
Figure 11 TFTP download progress

6.1.4 SSH settings

AXX 9300 METRO uses SCP/SHH for file transfers in association with network release download and configuration backup/restore. You can configure the AXX 9840 INSITE to use its embedded SCP/SSH software, or use an external SSH server.

Procedure: **EDIT SSH SERVER SETTINGS**

1. Click **SSH Server** in the Information pane



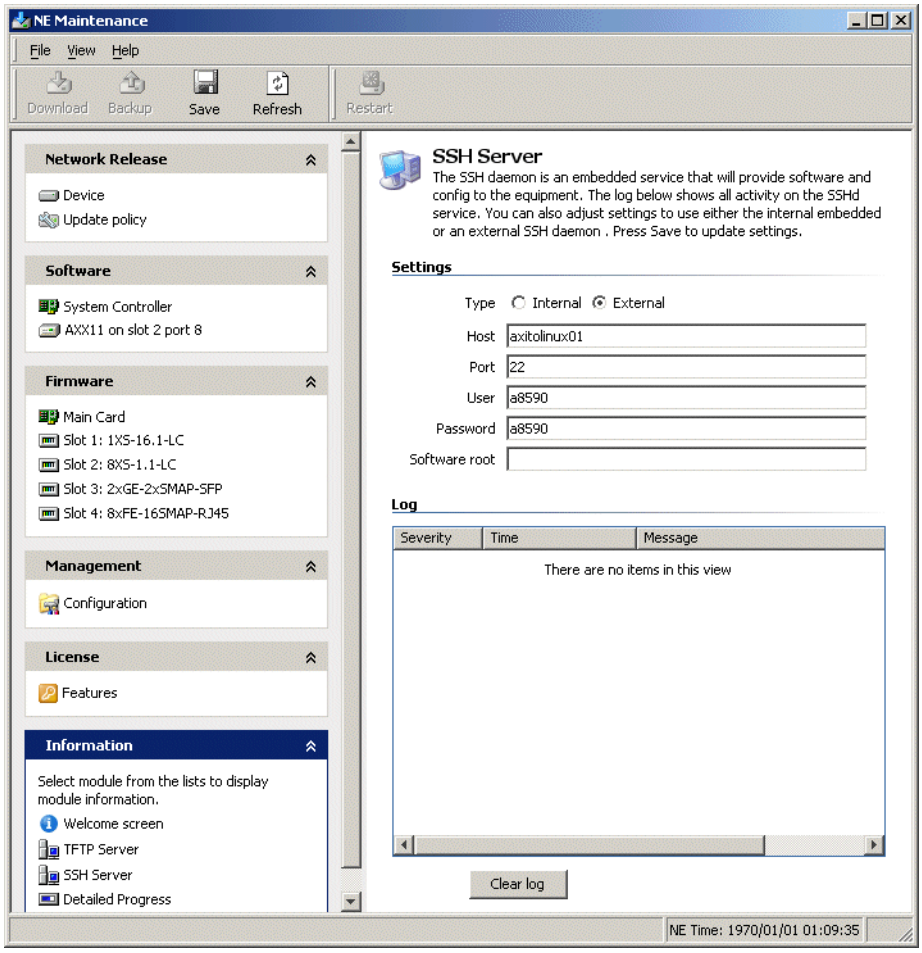
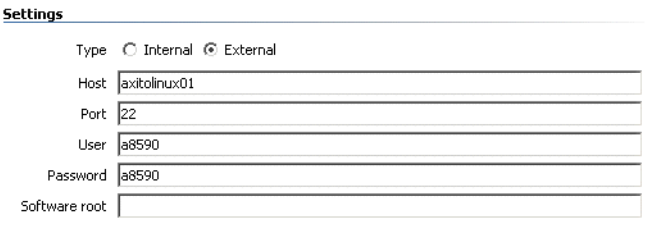


Figure 12 SSH Server settings

2. Select **SSHd type**; external or internal



3. Enter **Host** in IP format and **Port**.

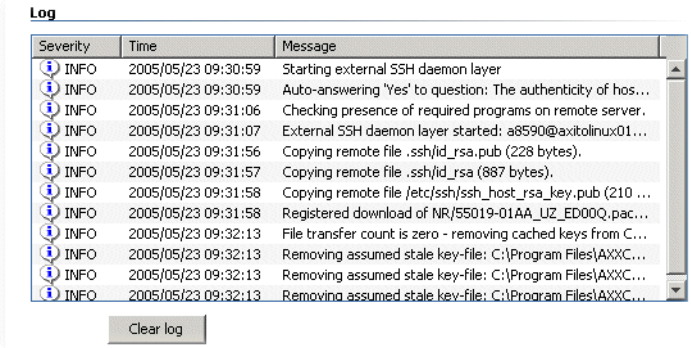
4. Enter **User** and **Password**

5. Optionally enter **path** to location of Software **root**.

NOTE! If you enter a character string for the host name, you will receive a not valid IP address

Log

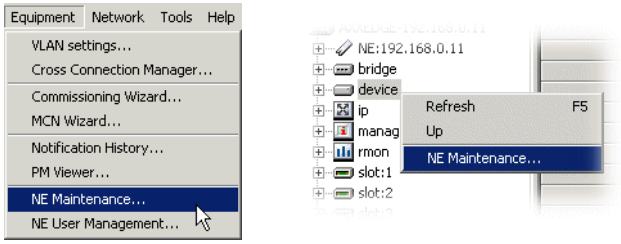
The log shows file transfer events.



6.1.5 Presentation of the NE Maintenance GUI

Procedure: **OPEN THE NE MAINTENANCE GUI**

The NE Maintenance GUI is available from both the Management Tree and the Equipment menu.



1. From the **Equipment menu** select NE Maintenance or right-click device in the Management Tree.

The NE is presented with panes to the left. Data available on the equipment sw banks and data available in the management system repository are listed in the window to the right.

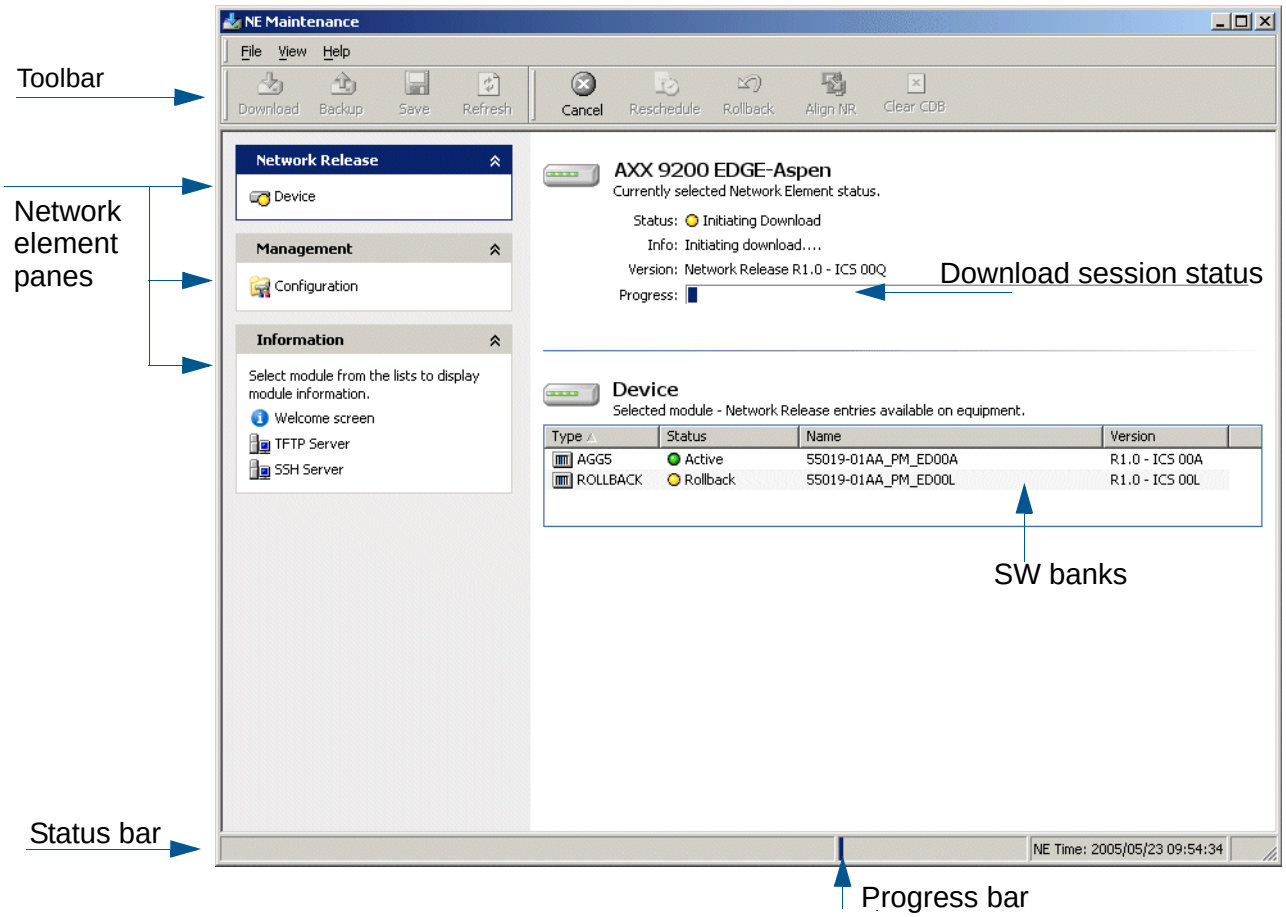


Figure 13 NE Maintenance GUI - overview

The Figure 13 presents an AXX 9300 METRO. If connected to an AXX 9200 EDGE the GUI will show service modules available on the NE, listing the network release download files available for the equipment.You may navigate in the NE Maintenance GUI when activated session runs in the background.

NOTE! In order to view, navigate and operate on the AXX 9200 EDGE service modules, they must have the following settings in the Management Tree and
Attributes Viewer:
ServiceState: ‘inservice’
InstallState:‘InstalledAndExpected’

Please see “Modify Slot” on page 379 for further details.

NOTE! It is not possible to run several sessions at the same time.

6.1.5.1 Operational and Administrative SW bank of NEs

The NE stores its software and firmware in banks. Some NEs have two banks, numbered as bank 1 and bank 2. At any time, only one bank is operational.

NOTE! Both firmware and software downloads are located in two banks, where one is active and the other is passive.

In the example below, bank 1 initially is both the administrative and the operational. After a SW download to bank 2, a switch (bank) command is performed and bank 2 becomes the administrative bank. When a restart is done, bank 2 also becomes the operational bank and the new software is active.

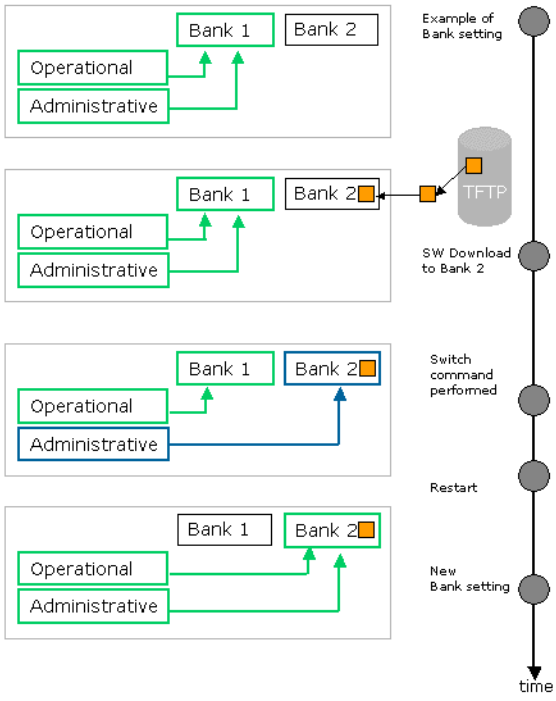


Figure 14 General illustration of switching SW banks

NOTE! AXX 9200 EDGE and AXX155A: You modify the parameters related to the administrative bank. This is the bank that becomes active after restart.

You can switch between the software banks, displayed as active or inactive. Bank switch is supported with progress status such as switching, restarting, and finished.

The inactive bank will be replaced in case of a network release upgrade. However, you can select which bank to be active after a restart of the NE: The current installation state or the downloaded firmware/ software.

NOTE! AXX 9300 METRO does not support user controlled bank switching.

Procedure: **MANUALLY SWITCH BANKS**

1. Select **Inactive bank**.

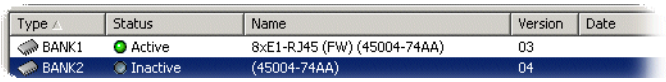


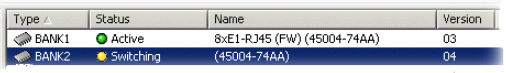
Figure 15 Select inactive bank- example

2. Press **Switch bank** 

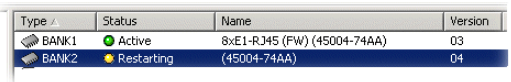
from toolbar or from right- click menu.

The system switches bank and restarts the NE.

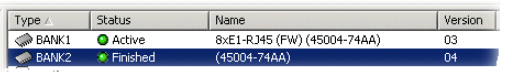
...switching



...restarting



...completed



...after “Refresh”

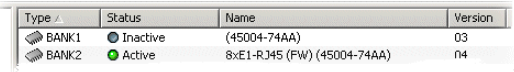


Figure 16 Bank switch- example

3. Press **Refresh** 

.

The system is updated and presents the equipment with new software bank.

6.1.5.2 Confirmation dialogue

A confirmation dialogue box will appear according to the command you have chosen, prior to the session start. Only the relevant options will be available[1].

1. Press **OK** to confirm download session.

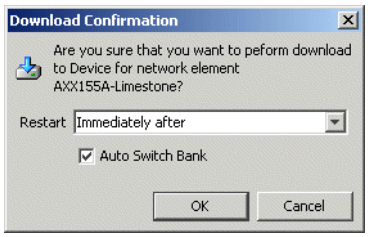


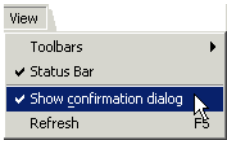
Figure 17 Confirmation dialog box - example device

You may change the restart option and switch bank setting.

Procedure: **DEACTIVATE CONFIRMATION DIALOG**

You can turn off this function from View menu.

1. Select **View** menu from toolbar.
2. Uncheck **Show confirmation dialog**.



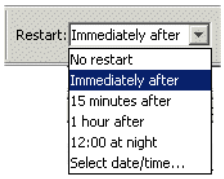
1. It is not possible to reselect switch bank for sessions concerning license and configuration.

6.1.5.3 Restart options

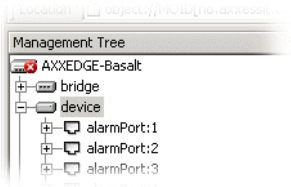
An NE must be restarted after a download session in order to be upgraded with the selected download file.

Procedure: **RESTART AUTOMATICALLY AFTER DOWNLOAD:**

1. In the Download wizard select **“Immediately after”**.



In case of an immediate restart, the NE will be without contact for a while, represented as **connection lost** in the Management Tree.



To see the new installation state of a restarted equipment:

2. Press 

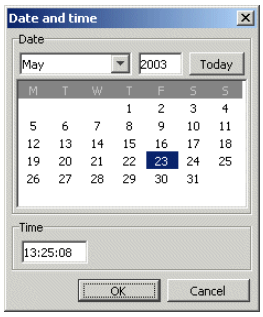
in the NE Maintenance GUI.

NOTE! An automatic restart is recommended. Some NEs need a manual restart.

Procedure: **SCHEDULE RESTART AFTER DOWNLOAD:**

1. In the Download wizard select **‘Select date/ time...’** from Restart pull- down menu.

2. Set **date/ time** in calender.



3. Press **OK**.

6.1.6 How to install download file into the management system

The Package Installer will help you install software into the management system. You will select a download file you already have or that is downloaded from the suppliers site and add this to the central software repository. New software for the equipment will then be available from the NE Maintenance GUI.

For overview see “Software download process” on page 250 and “Location of shared download files” on page 252.

1. Select **targeted NE** from menu.

2. Select **Package Installer** from **File menu**.

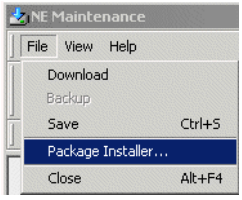


Figure 18 Start package installer

3. Read the information in the introduction window, and press **Next**.

4. **Browse** and **select** download file from the software- folder, and press **open.**

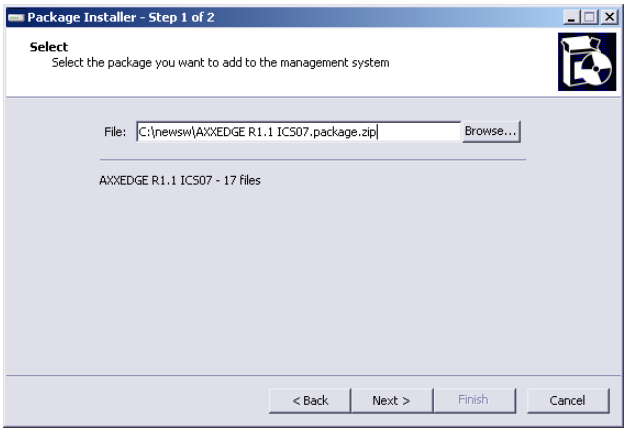


Figure 19 Package Browser - example (Network release of AXX 9200 EDGE)

5. Press **Next** for summary.

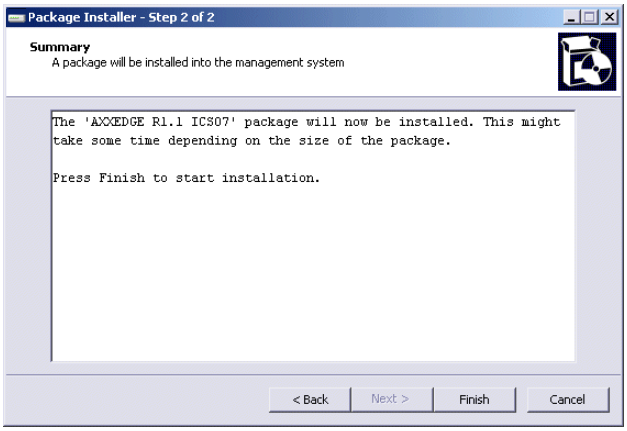


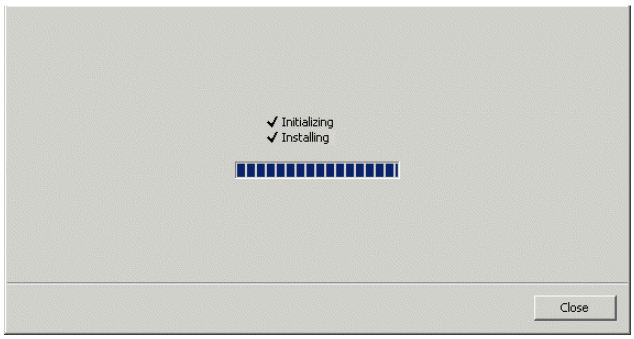
Figure 20 Summary of file transfer

6. Verify the compatibility of the selected download file for the NE and compare the version and ICS numbers of the download file to what is already installed on the equipment.

NOTE! Press Back if you want to reject the current download file and reselect in step 1. To exit the wizard at any time, you can press Cancel.

7. Press **Finish** to activate file transfer.

The selected file is unpacked and transferred to the management system software repository.



8. Press **Close** to exit wizard.

The download file (network release or single file) is available in the repository list(s) in the Download wizard, and saved to the “.res/software” directory. of the installed management system.

6.1.7 How to download network release to an AXX 9300 METRO

The following procedure explains necessary steps needed to download a network release to an AXX 9300 METRO.

To save management DCN bandwidth, only files that have changed between currently running and targeted downloaded network release are download. The def-file contains information on the contents of the network release (hardware/software file references, module type associations, version/ICS information, HW compatibility information and traffic affecting status for the different modules).

AXX 9840 INSITE reads def-file properties and calculates download volume prior to downloading the network release to the network element.

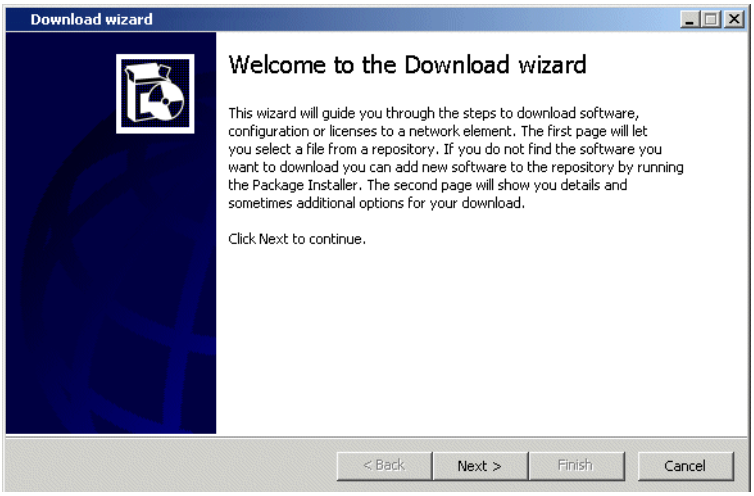
NOTE! Module software and firmware releases are downloaded as part of a network release.

Procedure: DOWNLOAD NETWORK RELEASE TO AN AXX 9300 METRO

1. Click 

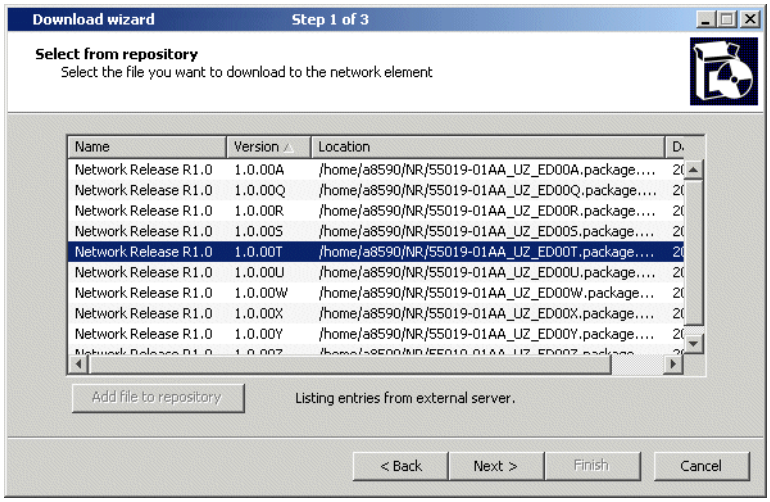
in the toolbar.

2. The Download wizard launches.**Read** the wizard **summary** and press **Next** to continue.



3. **Select** the **NR file** you want to download and click **Next**.

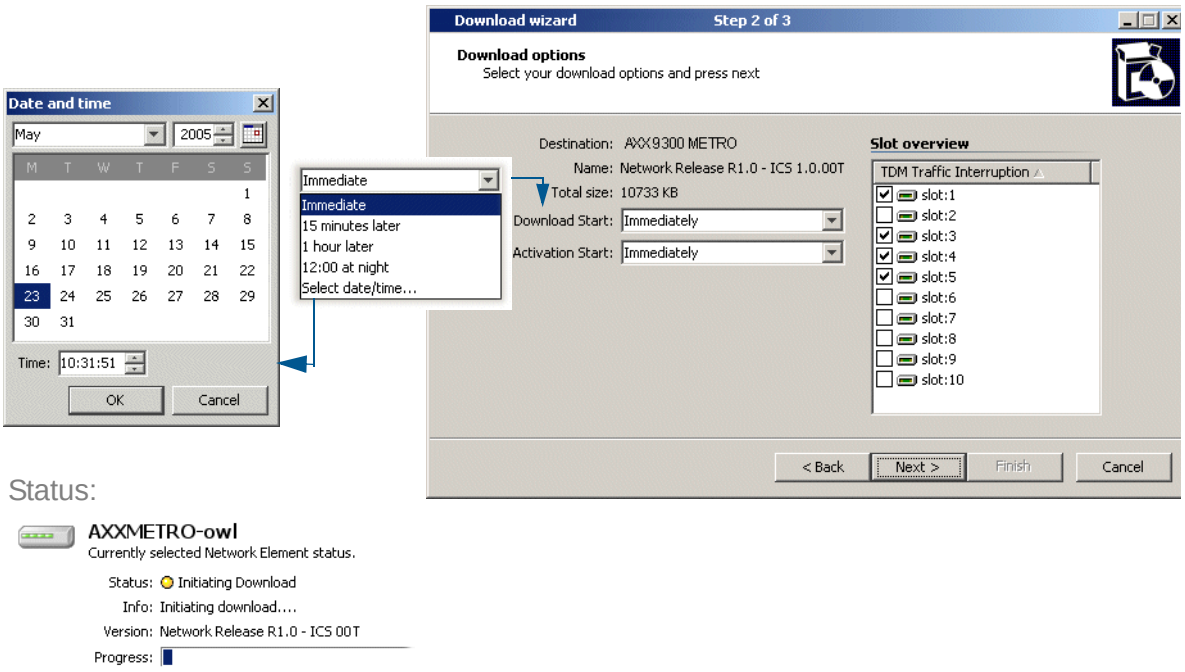
NOTE! In this example the “Add to repository” button is not available because an external server is used, thus only entries in the external server is listed.



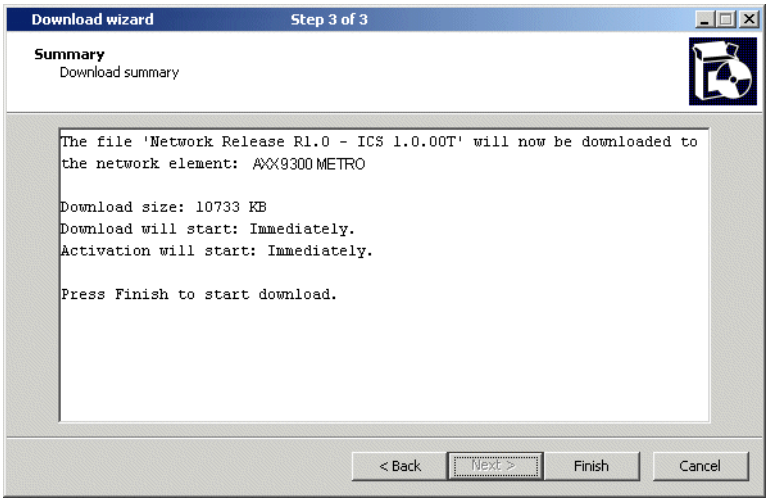
You choose visible columns in the Repository list from the column’s right- click menu.

4. The wizard now initialises the download.

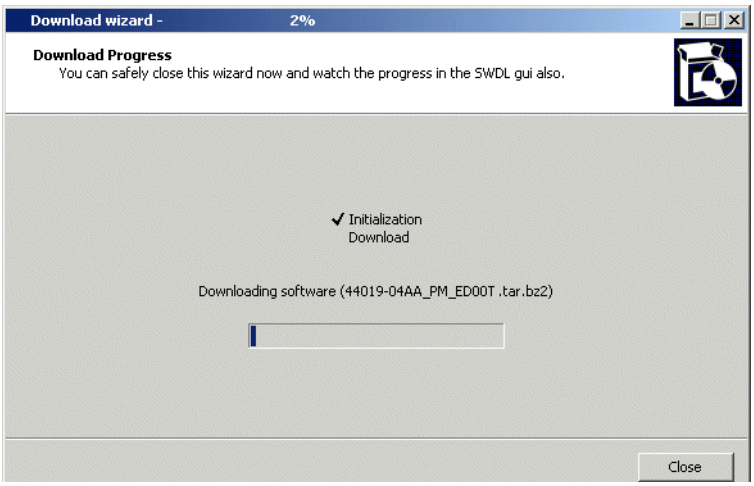
5. Select **Download NE Time** and **Activation NE Time**. Please note slots that are subject for TDM traffic interruption.



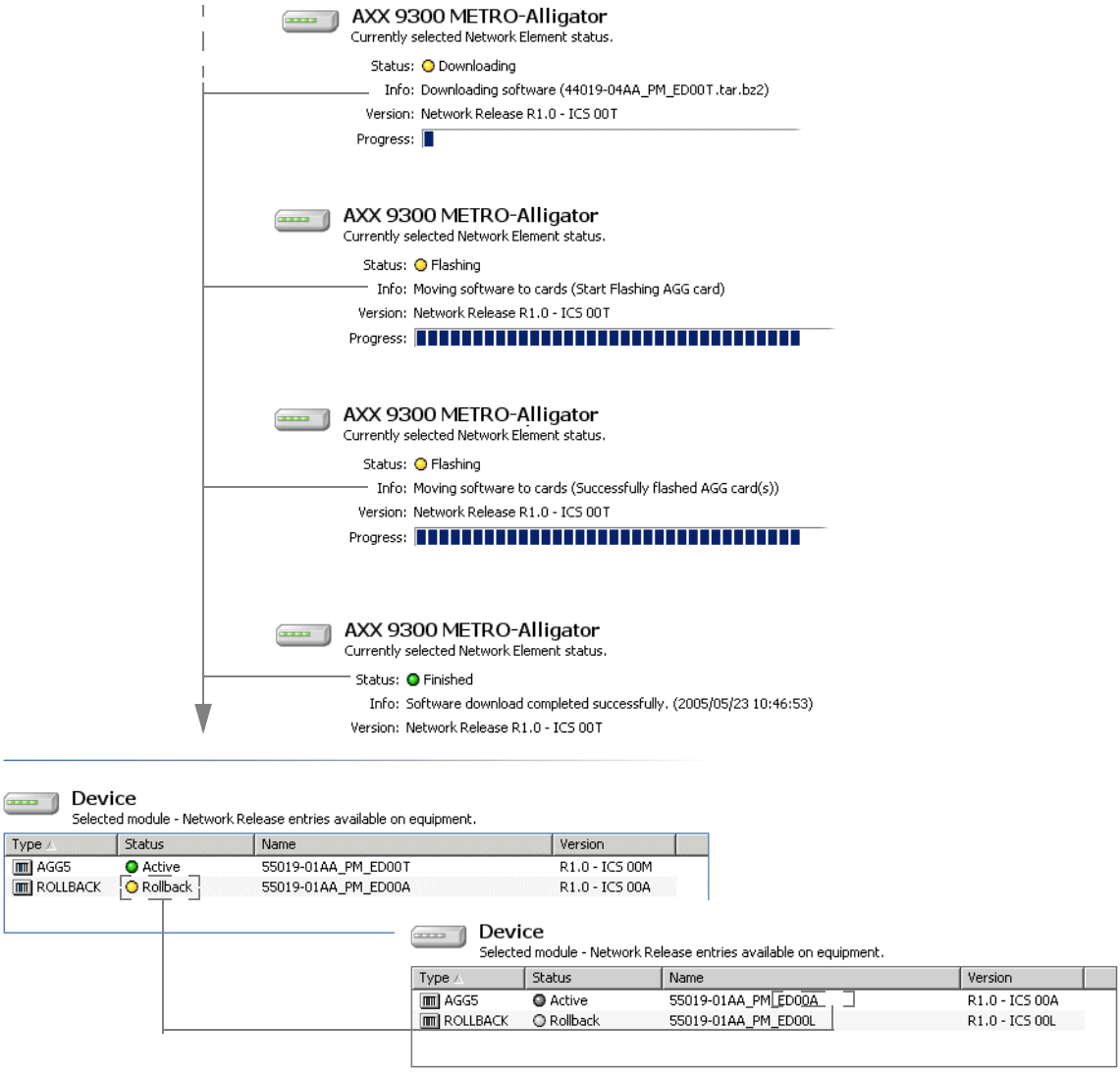
6. Click **Next** to start download according to your time-settings.



7. Read the summary and click **Finish** to start the installation.



8. You can safely close the wizard and watch the progress in the NE Maintenance GUI.



6.1.8 Rollback of AXX 9300 METRO Network Release.

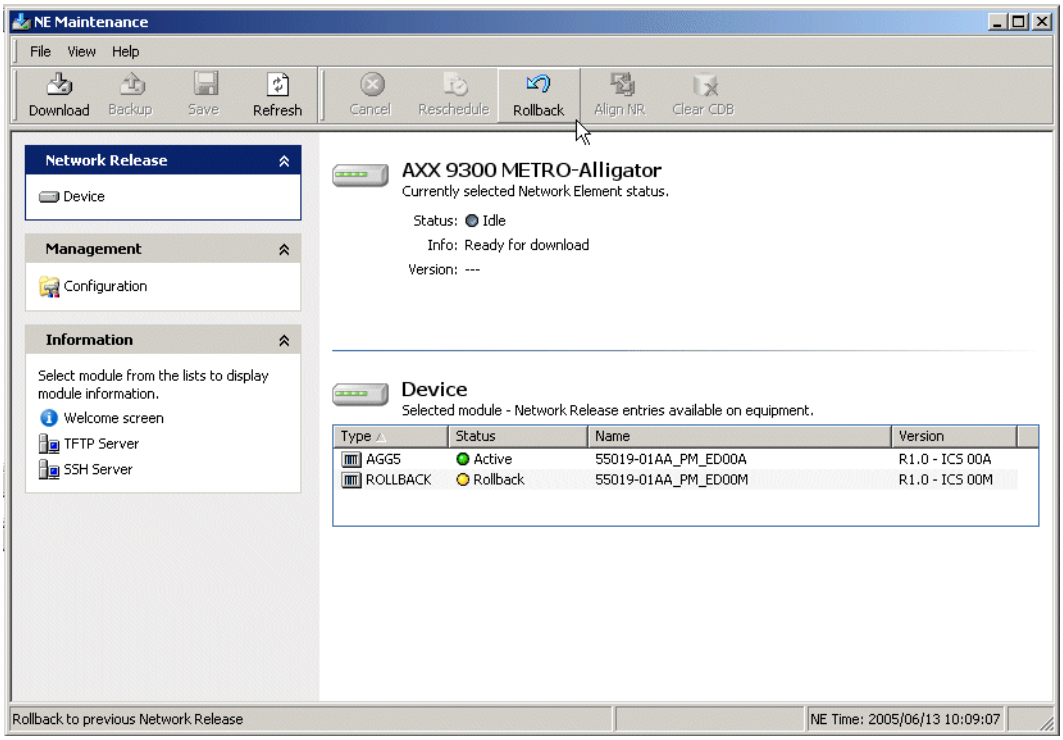
Roll-backs can be performed to recover from non-successful network release downloads. The rollback reverts the network element running configuration to the original state.

Depending on the situation, a rollback may be initiated in two situations:

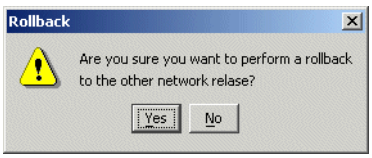
- A download session is partially completed due to an error sequence. The system automatically rolls back to a "previously known good" situation.
- The user manually forces a rollback based on error information from the network element.

Procedure: **ROLLBACK TO PREVIOUS NETWORK RELEASE**

1. Click **Device** in the Network Release Pane.
2. In the toolbar click **Rollback**.

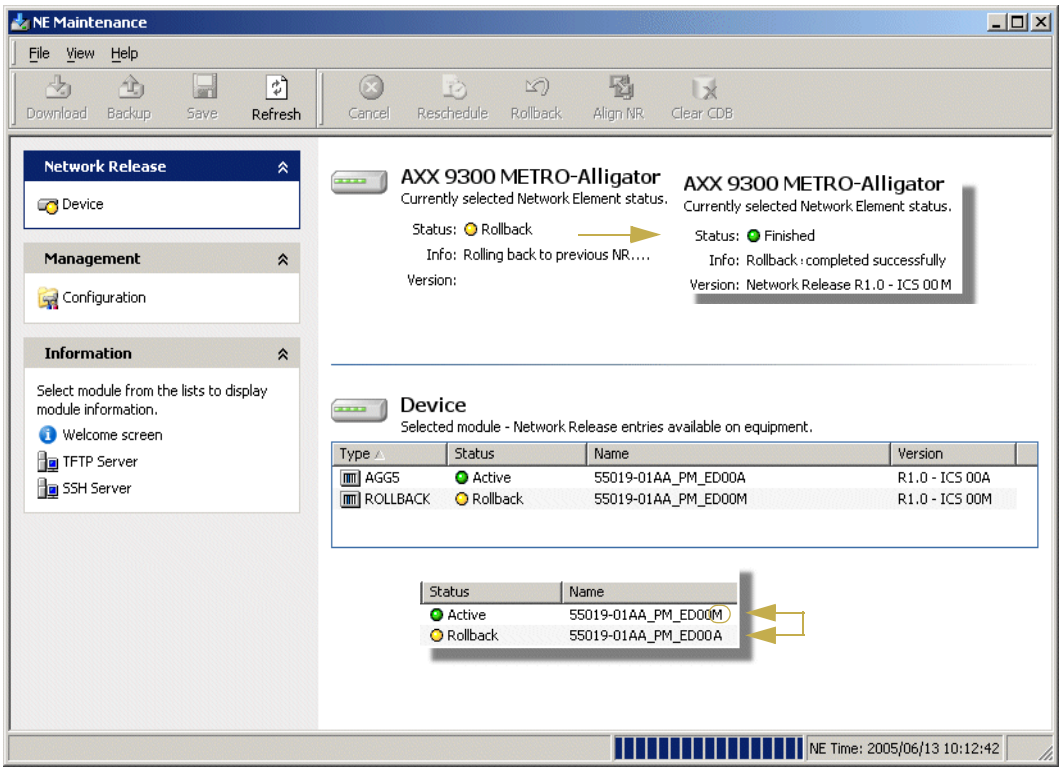


3. Press **Yes** to start the rollback operation.



4. **Select** the **NR file** you want to download to the NE

5. View the Rollback progress and the Status becoming Finished.



NOTE! Only one rollback is allowed. That is, if "*ED00M*" is the "rollback NR" and "*ED00A*" is the "active NR" and a roolback is performed, you cannot afterwards rollback to "*ED00A*" (now the rollback NR).

6.1.9 Align AXX 9300 METRO Network Release

This operation is only available when the AXX 9300 METRO has two AG modules with different Network Releases (Duplex mode). To align the Network Releases of the modules and set the modules to redundant mode, you can follow the procedure below.

Procedure: **ALIGN NETWORK RELEASE**

1. Open the NE Maintenance GUI
2. Select “Device”.
3. The table lists the software entries for the AG modules; one will be indicated as active, and the other as inactive.
4. Press the “Align NR” button and the mode changes to redundant mode. This may take 1-2 minutes.

6.1.10 Rollback of AXX155A and AXX 9200 EDGE Network Release

The AXX 9200 EDGE/AXX155A does not support the sophisticated rollback option for the whole Network Release level. In order to perform rollback to previous release level, the procedure is to run a Network Release download (def-file) for the desired rollback release.

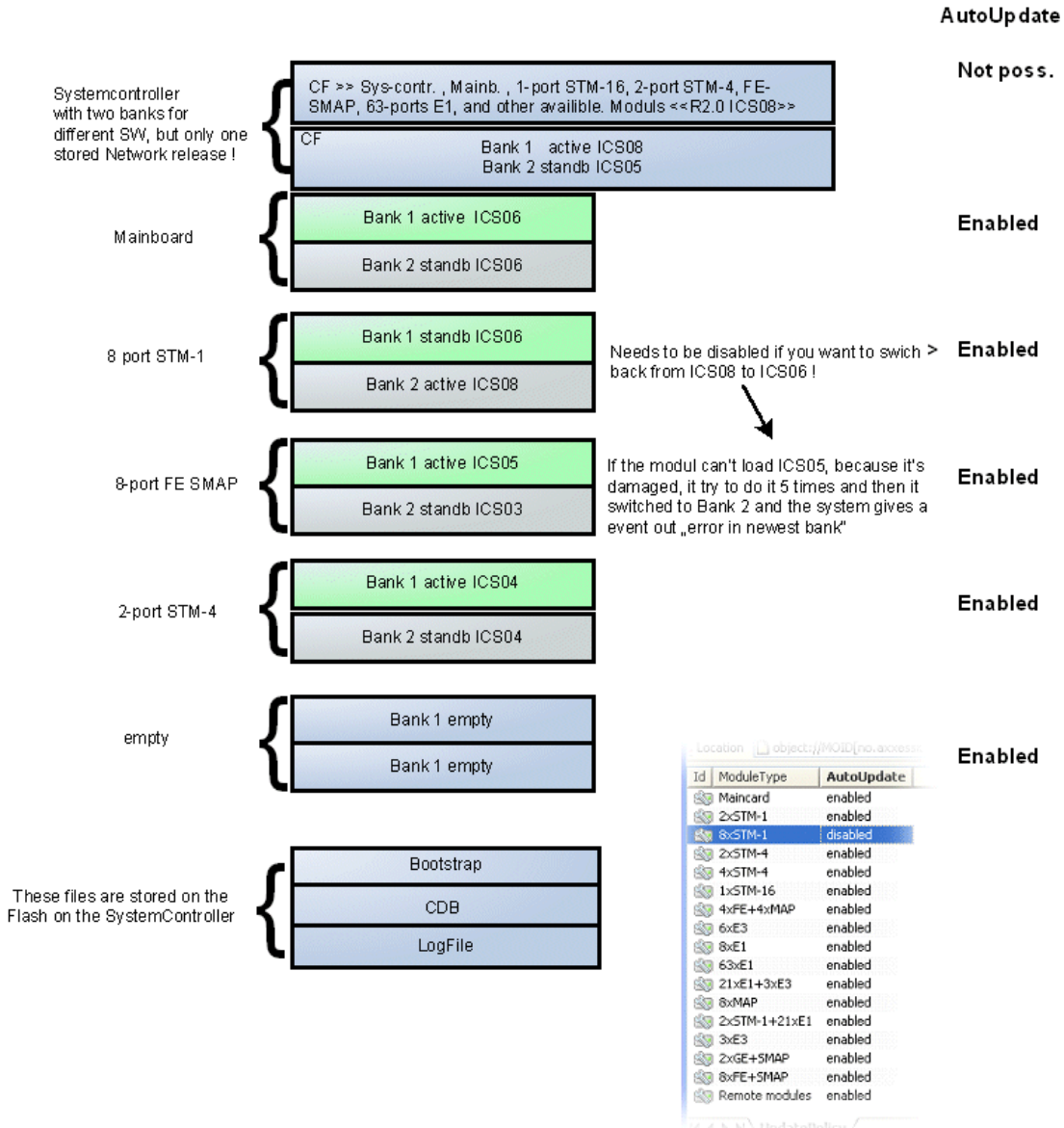
This procedure cannot be performed using the NE maintenance GUI. External TFTP server and menu options from the "Management Tree" can be used instead.

NOTE! This procedure will only be successful if the configuration file on NE does not include settings introduced by features for the upgraded release.

Manual rollback per module AXX 9200 EDGE introduced in release 2.0 an "Update Policy" manager, which is mainly intended as an option to disable upgrade of traffic modules prior to issue a Network Release Upgrade.This feature makes it necessary to include one more step before the manual switch can be performed for a specific module. Any attempt to manually switch back to previous firmware level will be declined until the Update Policy entry for this module type is disabled.

The firmware is stored individually in two banks on separate flashes. The inactive bank contains the version aligned with the previous NR release level and the new release level has been loaded in active

bank. In the example below we provide a guideline for how you can switch the firmware to the release as it was before the upgrade.



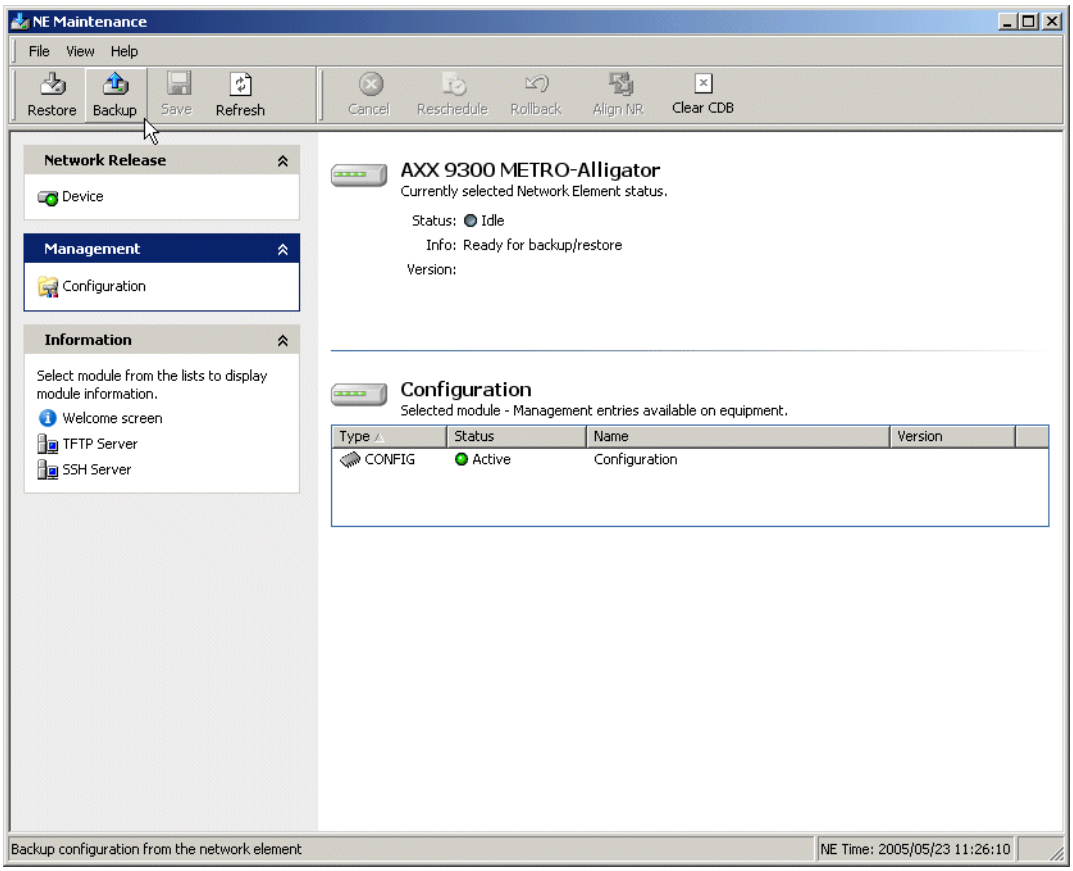
6.1.11 AXX 9300 METRO - Configuration backup and restore

This section shows necessary tasks to backup and restore configuration for an AXX 9300 METRO.

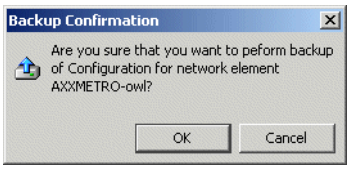
Procedure: **BACKUP CONFIGURATION**

1. Select Configuration in the Management pane

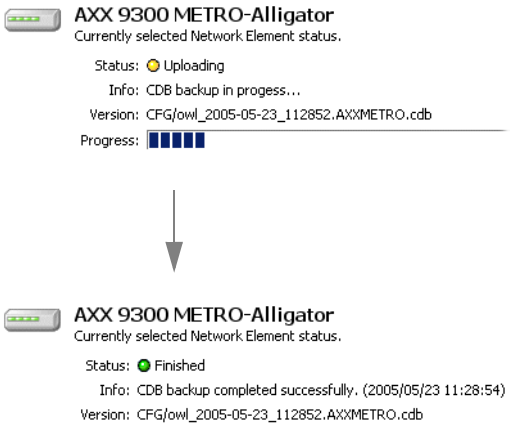
2. In the toolbar press **Backup**



3. Click **OK** to confirm the backup operation.

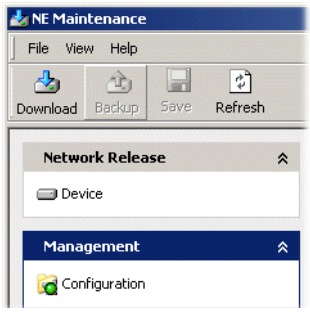


4. View the backup progress in the NE Maintenance GUI.



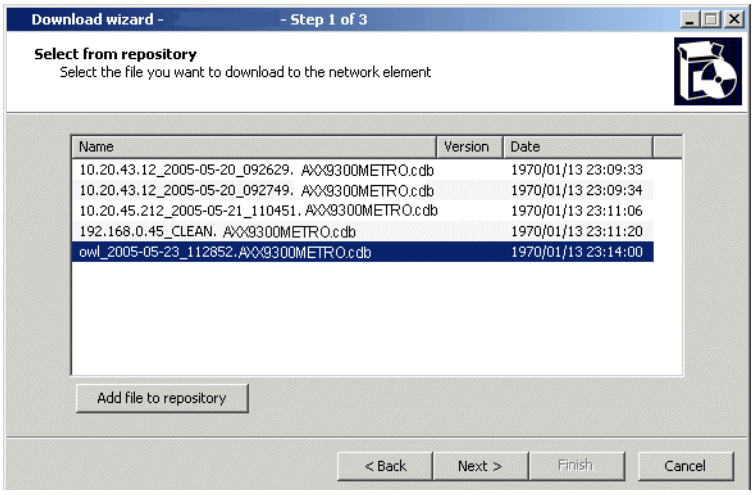
Procedure: RESTORE CONFIGURATION

1. Select **Restore** in the toolbar.



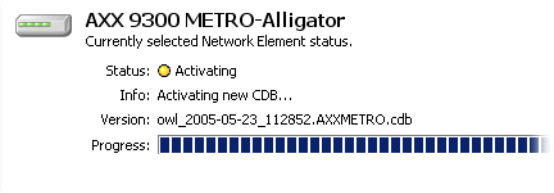
2. The Download wizard launches. **Read instructions** and click **Next**.

3. **Select** desired **cdb-file** to restore and click **Next**.



4. Read summary and click **Next**.

5. View progress in the NE Maintenance GUI.



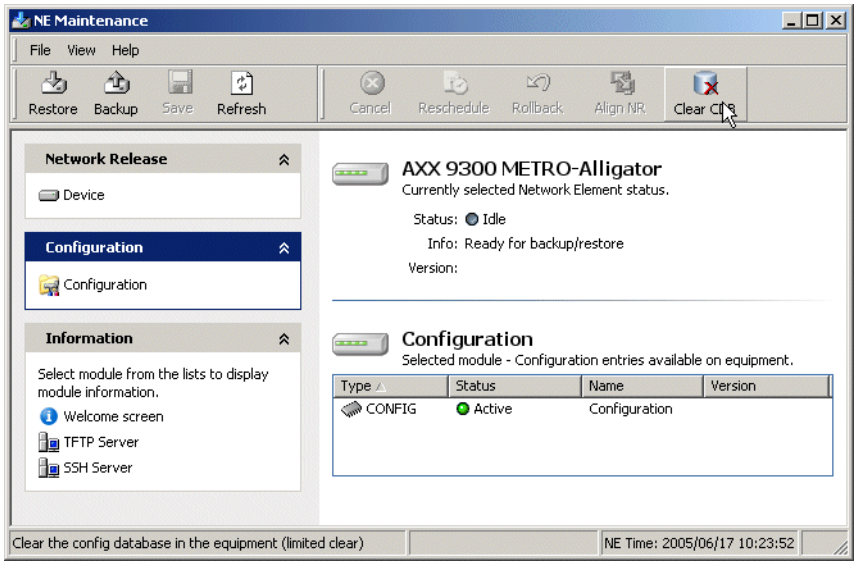
Procedure: CLEAR CONFIGURATION DATA BASE (CDB)

This procedure explains how to perform a limited clear DCB. All configuration except Ip-address and default gateway is cleared.

Warning!

Perform Backup CDB prior to the following procedure. See “” on page 273.

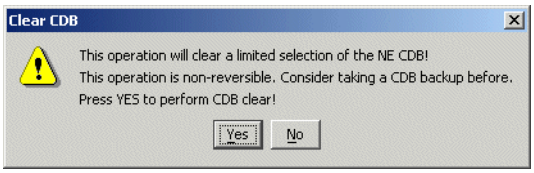
1. Select the **Configuration** pane



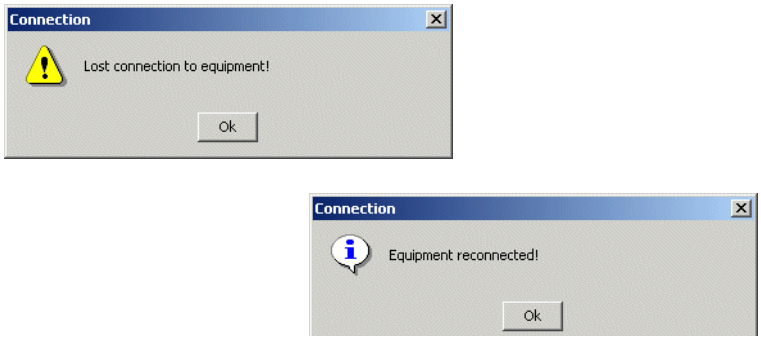
2. **Click** 

to perform a limited clear of the configuration database in the equipment.

3. Click Yes to perform a limited CDB clear.



Connection lost/ Equipment reconnected will be reported during the clear-operation.



View progress in the NE Maintenance GUI. Also click the Event Trace in the Notification List.

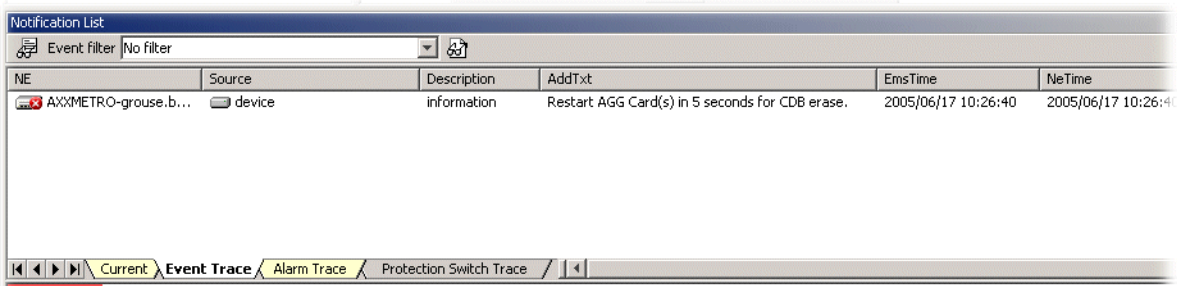


Figure 21 Event trace during Clear CDB

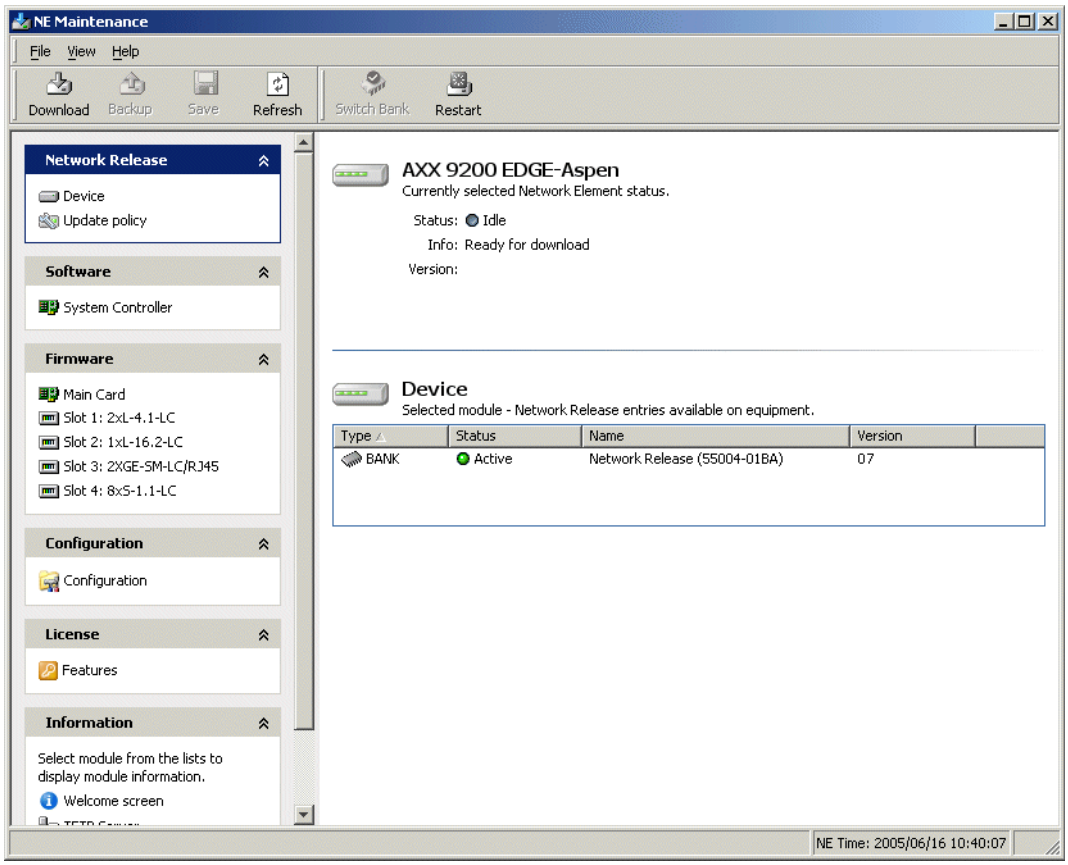
6.1.12 How to upgrade a NE with a new network release

NOTE! If a scheduled restart is set before a new download session is started; the scheduling parameters will be overwritten.

Procedure: **HOW TO UPGRADE AN AXX 9200 EDGE WITH A NEW NR**

This procedure illustrates a network release upgrade to AXX 9200 EDGE with automatic restart of the NE and automatically switch of banks. It also apply to firmware and software download sessions.

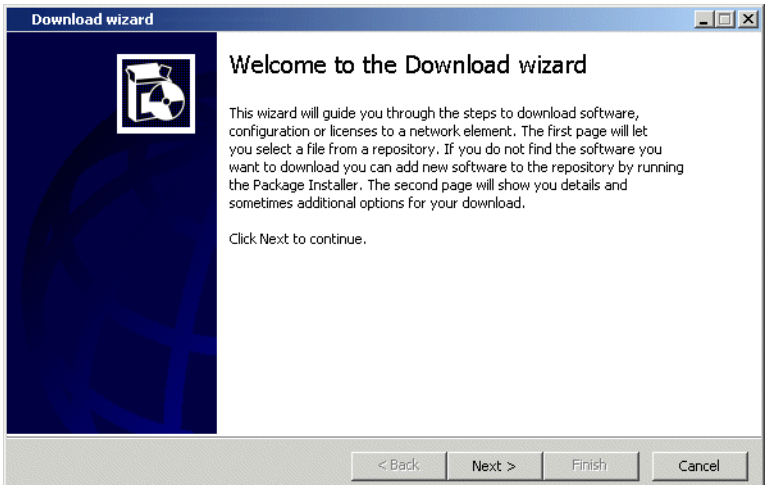
1. In the **Network Release pane** press **Device.**



2. From the toolbar select 

.

3. The **Download wizard** starts. Read instructions and press **Next**.



4. Select desired **Network Release** from the Repository list.

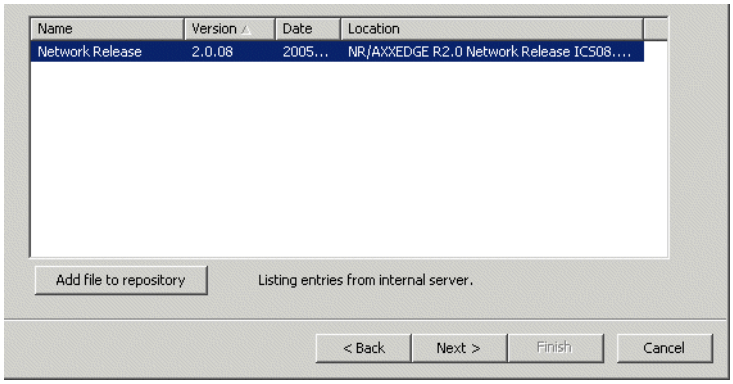
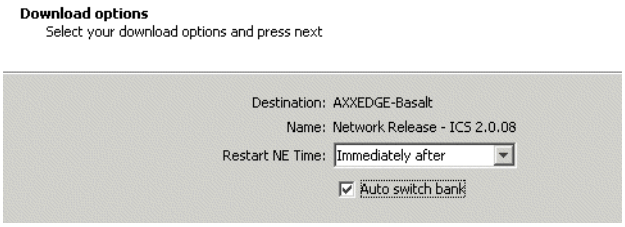
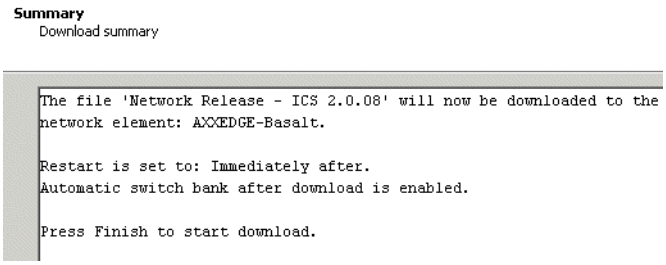


Figure 22 Select download file- example R2.0 network release ICS08

5. Choose **Immediately restart** (optional), see page 6-262 for other options and tick the **Auto switch bank** checkbox.



6. Press **Next** and read the Download summary.



7. Press **Finish** to initate download.

8. You may close the Download wizard and view the download progress in the NE Maintenance GUI (see Figure 23) and in the Notification List see

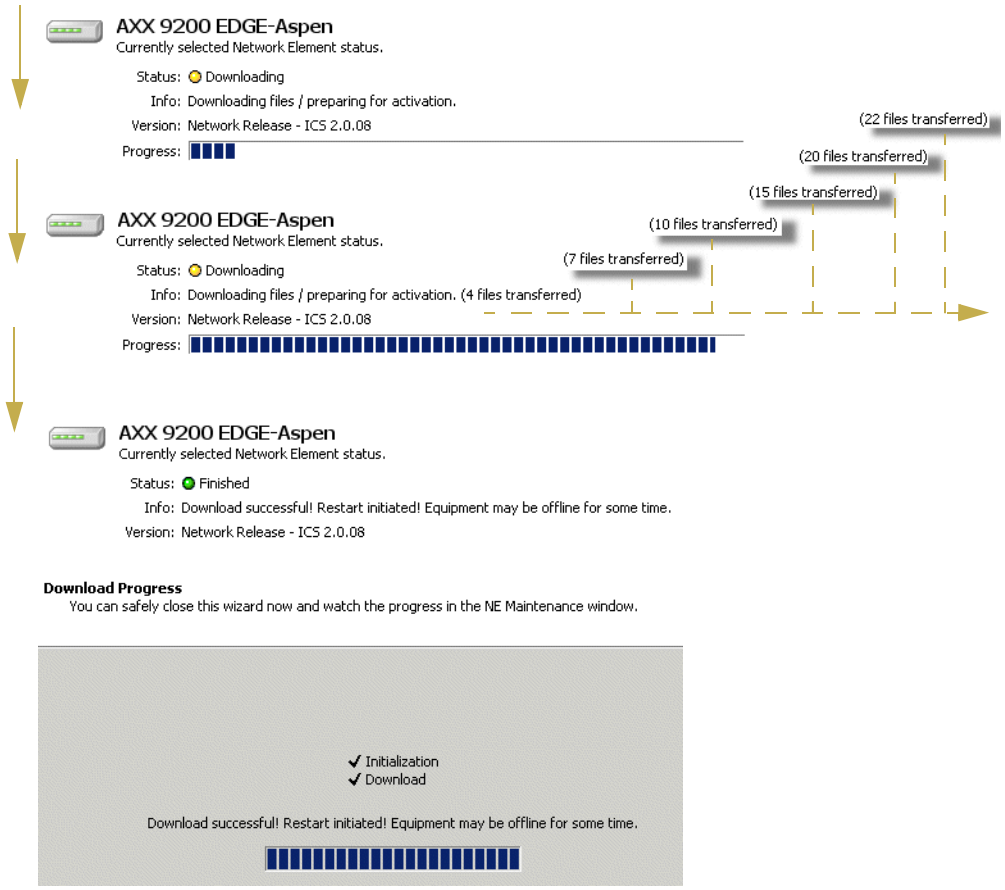


Figure 23 Downloading Network Release - progress

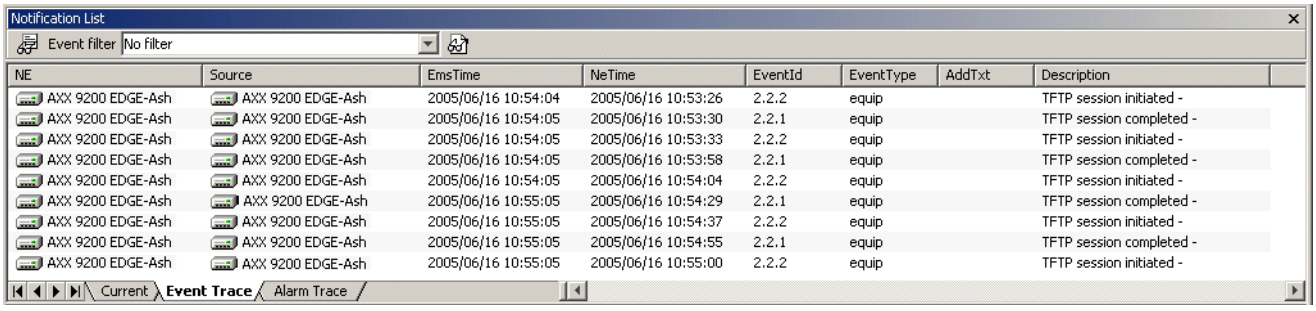
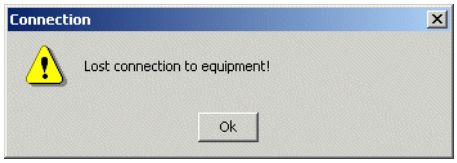


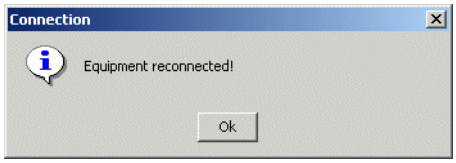
Figure 24 Event Trace tab in Notification List.

9. **When** the download is **completed** a **restart is initiated** and "Connection Lost" is reported. Click **OK**.



NOTE! If a scheduled restart is selected, the status bar will displays restart time when the download is complete. This information is kept until the restart of the NE is completed.

10. After a while the equipment is reconnected. Click **OK**.



11. The new network release is now downloaded and running on the network element.

6.1.13 License handling

Procedure: **HOW TO UPGRADE NE WITH FEATURE LICENSE**

This procedure shows how a license upgrade on an AXX 9200 EDGE.

1. In **the License pane** press **Features.**

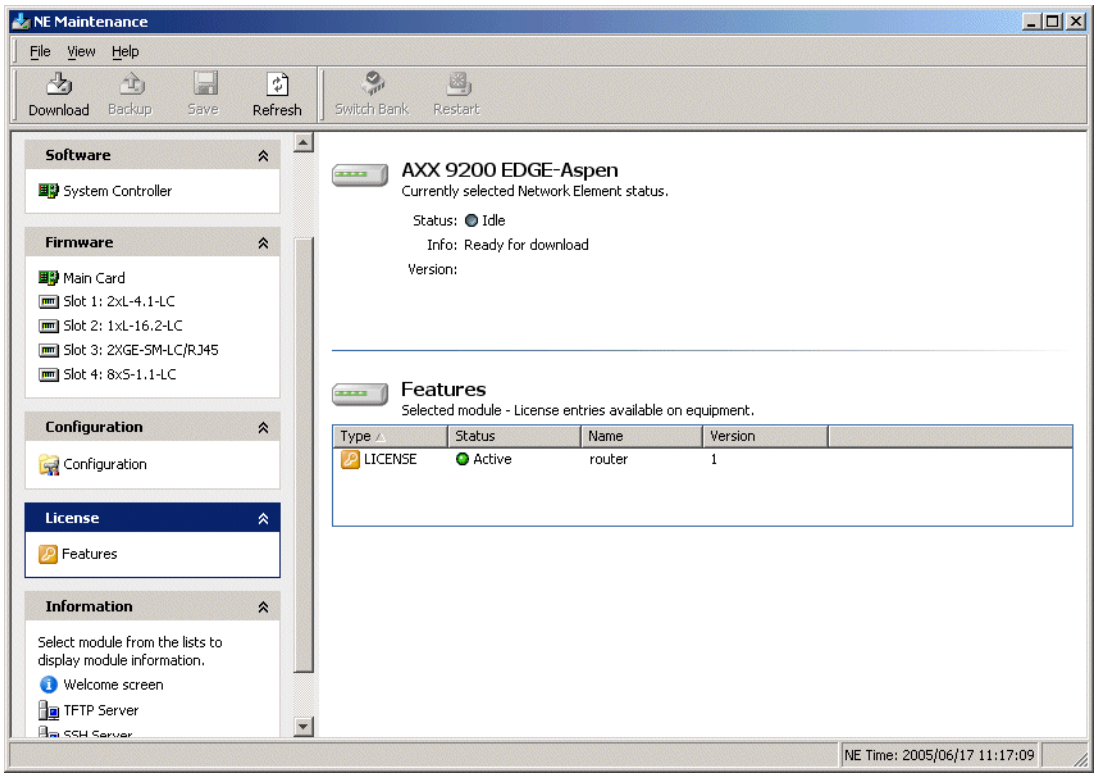
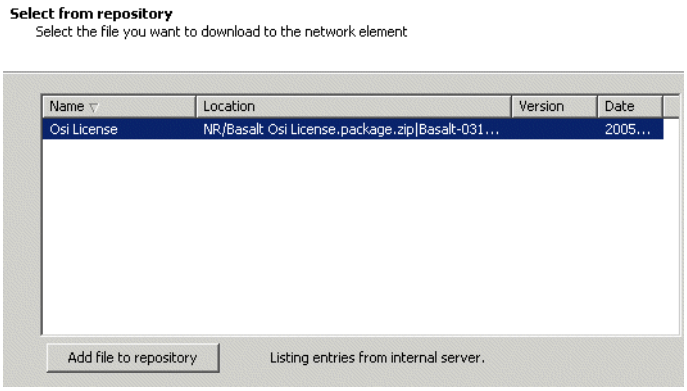


Figure 25 Install feature license on the equipment- example adding OSI

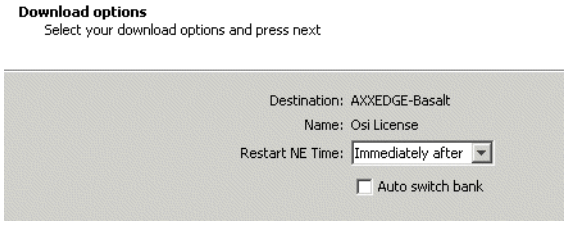
2. Press **Download**  . and the **Download wizard** launches.

3. Read instructions and click **Next**.

4. Select desired **license** to download.

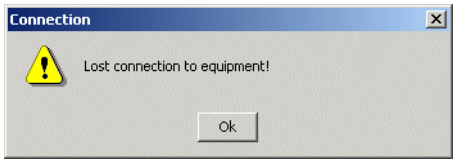


5. Select **restart NE Time** after download completion and click Next.

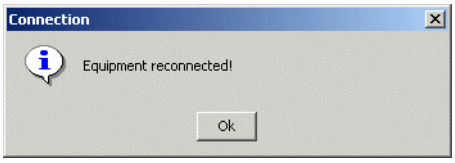


6. Read summary and click **Finish** to start download.
   View progress in the NE Maintenance GUI.

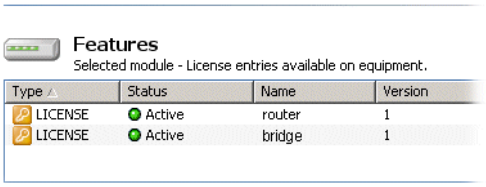
7. **When** the download is **completed** a **restart is initiated** and "Connection Lost" is reported. Click **OK**.



8. After a while the equipment is reconnected. Click **OK**.



9. The new feature license is now downloaded and available on the network element.



10. Press **Refresh** to update the management system.

The list of available features on the equipment is updated.

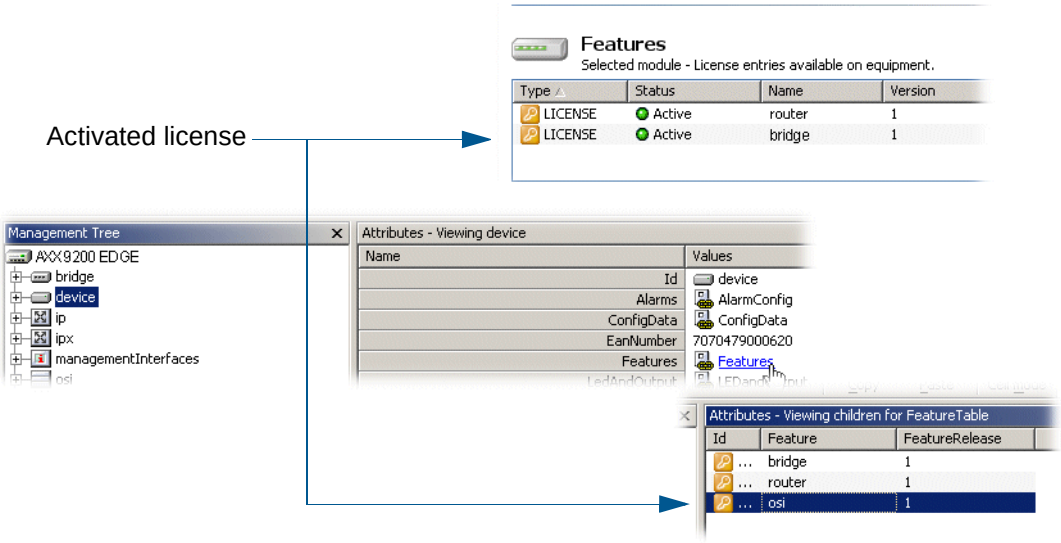
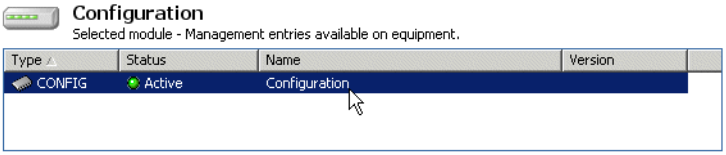


Figure 26 Updated feature list - example osi license

6.1.14 How to backup and restore configuration data

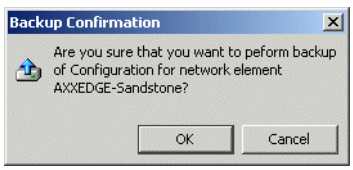
Procedure: **CREATE BACKUP FILE OF DATA CONFIGURATION**

1. Open Management **pane** and press **Configuration.**
2. Select the **Active** configuration on the NE.



3. Click **Backup**  .

The **Backup Confirmation** dialogue box appears.



4. Press **OK** to confirm.

The system creates a configuration file and saves the active configuration data from the NE.

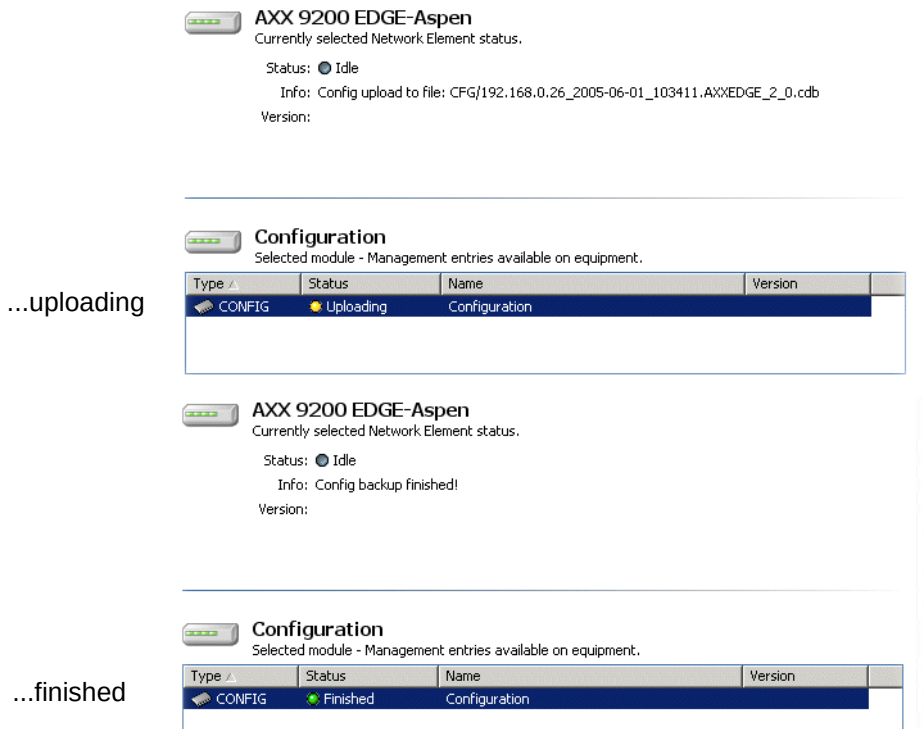


Figure 27 Upload session- example configuration back- up progress

The configuration file is available in the Repository list in case a restore is needed.

Location of backup file

For first time backup, the management system will create a CFG-folder under "`.res/ software" directory and` save the backup file(s) to this folder, as shown in Figure 28

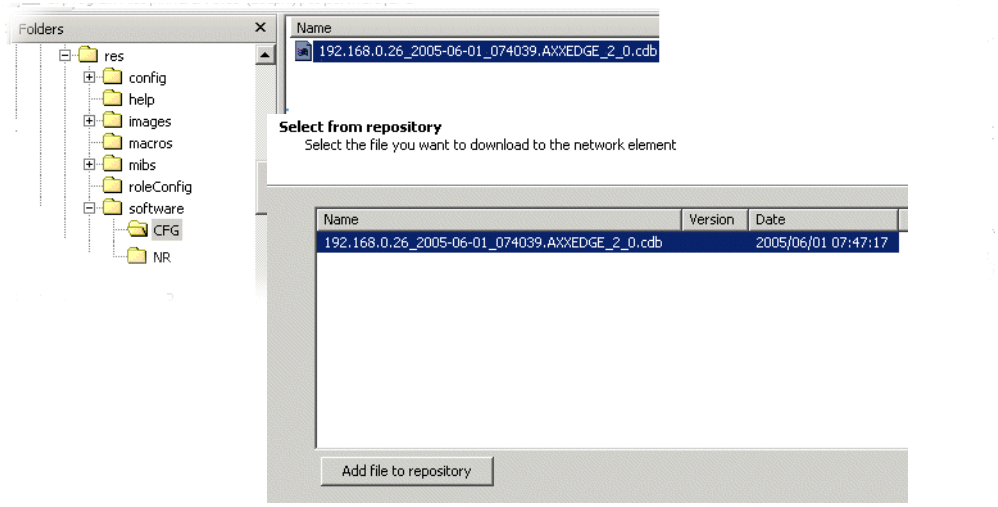
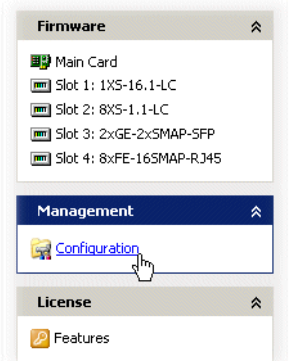


Figure 28 Configuration folder and file- locations

Procedure: **RESTORE DATA CONFIGURATION FROM A BACKUP FILE**

1. Open **the Management pane** and click **Configuration**.

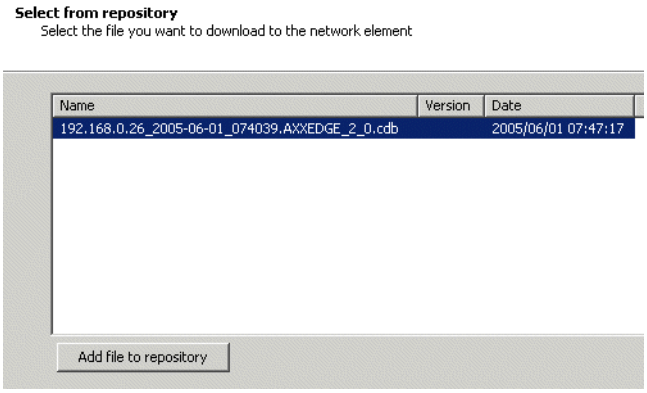


2. In the toolbar click **Restore**. 

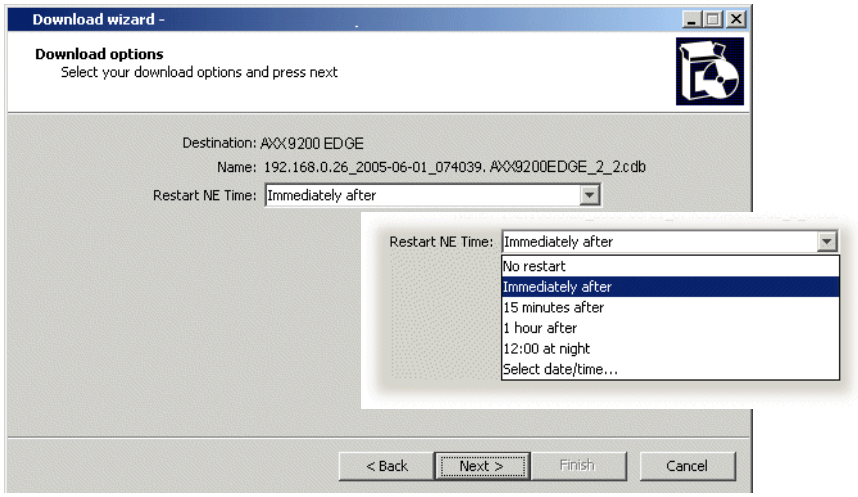
3. The Download wizard launches.

4. Select **Next** after reading the instructions.

5. **Select** desired **cdb-file** from the repository.



6. Click **Next**.



7. Select **Restart NE time** and click **Next**.

8. **Read Summary** before clicking **Finish**.

9. View progress in the NE Maintenance GUI.

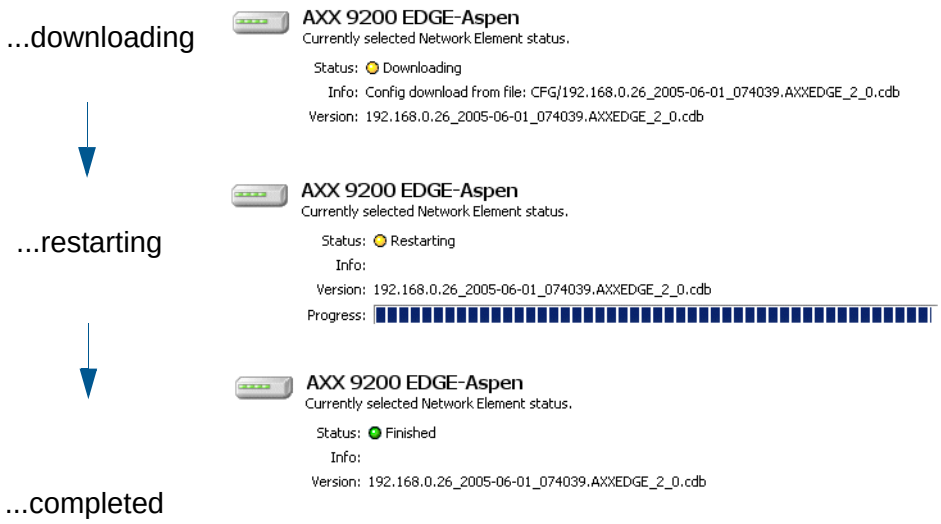


Figure 29 Restore data configuration- progress

The configuration data of the NE is restored.

6.2 Software Download and Configuration Management Tree

The following descriptions and procedures present Software Download through the Management Tree and Attribute viewer, supporting manual file transfer to external TFTP server and supplementary procedures for some NEs.

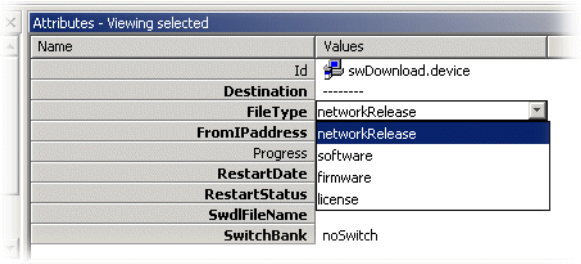
The overall information is also available in a custom GUI, see “NE Maintenance” on page 249.

Please see Release Notes for a link to an example of an FTP server that has been verified to work in cooperation with AXX 9840 INSITE.

NOTE! Secure server ignores requests outside the TFTP root. This applies for NEs with license keys especially.

6.2.1 Download Network Release - AXX 9200 EDGE

1. **Unzip** the Network Release File.
2. **Copy** the **contents** to the TFTP - server.
3. In the Management Tree select **device** > **SWdownload**.
4. Set **destination** to **device**
5. Set **Filetype** to **networkRelease**



6. Enter **FromIPaddress** (TFTP server Ip address).
7. Set **restartstatus** to **immediateRestart**.
8. Enter **SwdlFileName** attribute values (File path and name).
9. Click **Save**.

NOTE! The status of the SwitchBank attribute (switch/noSwitch) is overruled when Filetype is set to networkRelease.

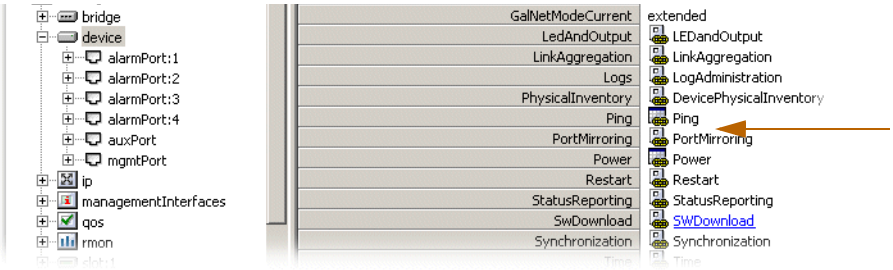
6.2.2 License download

AXX155E

1. Select **device > SWdownload.**
2. Enter **FromIPaddress** (TFTP server Ip address).
3. Enter **SwdlFileName** attribute values (File path and name).
4. Click **Save.**
5. **Perform a restart (See “AXX155E” on page 289).**

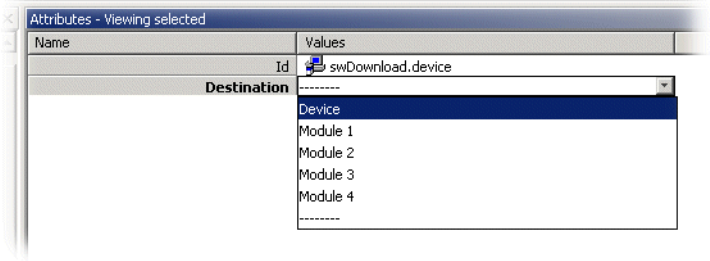
AXX 9200 EDGE

1. Select **device** and then **SWDownload.**

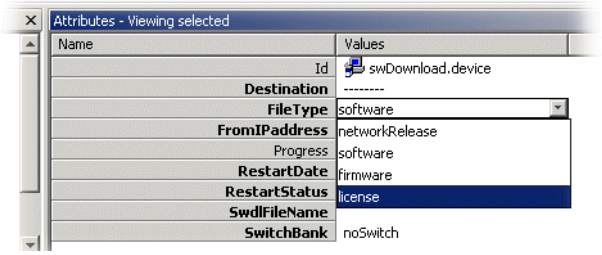


The following attributes are modifiable:

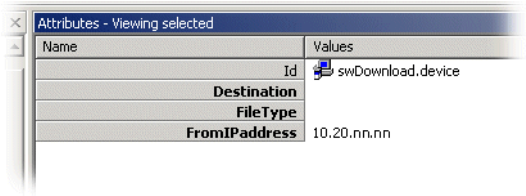
2. Set **destination** to **device**.



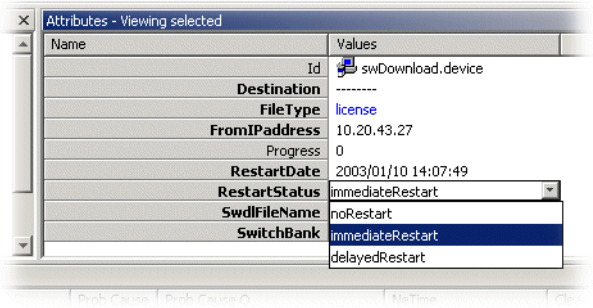
3. Set **Filetype** to **license**.



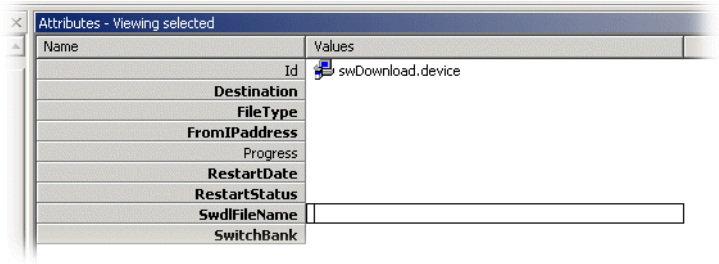
4. Enter **FromIPAdress** (TFTP server Ip address).



5. Set **RestartStatus** to **immedateRestart**.



6. Enter **SwdlFileName** attribute values (File path and name)



7. Click **Save.**

6.2.3 Software Download to the NE

6.2.3.1 Use of Filetype in Attributes

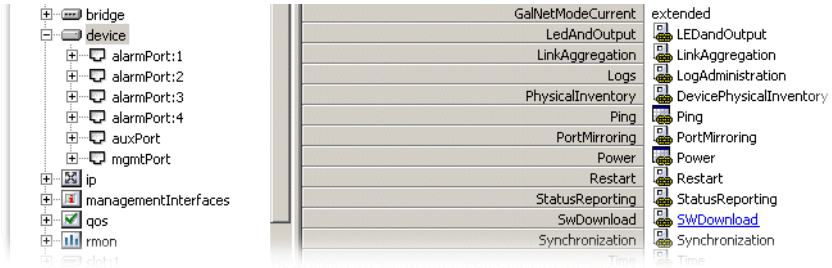
This applies to AXX 9200 EDGE and AXX155A.

Set FileType to Software: The system controller will be restarted.

Set FileType to Firmware: The main card will be restarted.

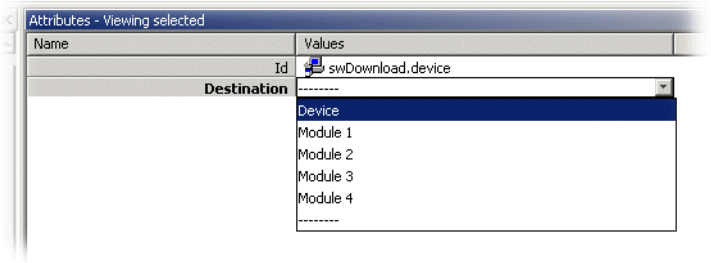
This will also lead to a restart of the system controller and all the modules, i.e. a complete restart of the whole device.

1. Select **device** and then **SWDownload.**

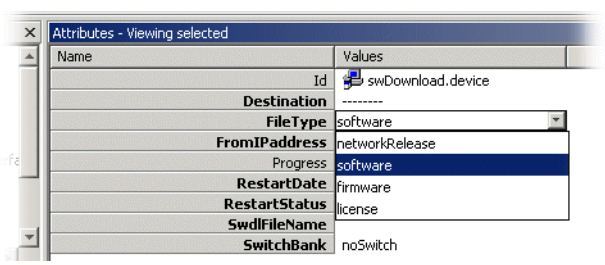


The following attributes are modifiable:

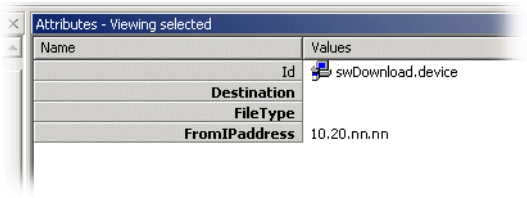
2. Select desired **destination**.



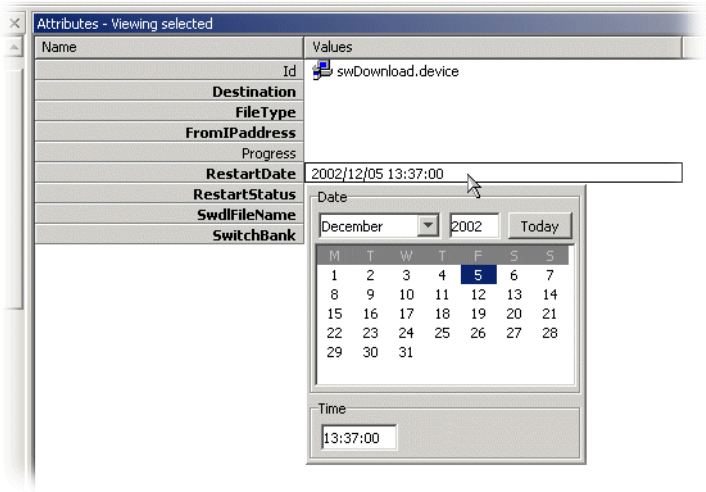
3. Set **Filetype** to software.
The system restarts the System Controller.



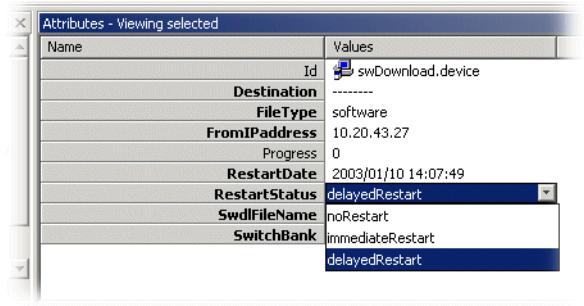
4. Enter **FromIPAdress** (TFTP server Ip address).



5. Set **RestartDate** if you want **delayed restart**. See step 6 below.

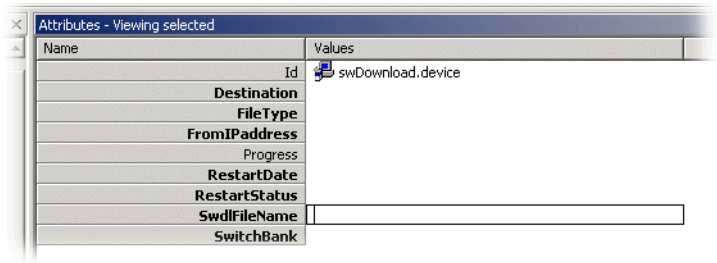


6. Select **RestartStatus**.

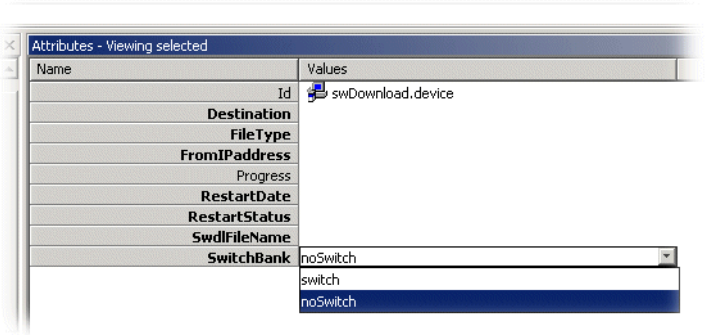


Whether the NE should restart immediately or at a specific date/time after the download process.

7. Enter **SwdlFileName** attribute values (File path and name)



8. Set **SwitchBank** attribute.



Switch:

After the restart the Operational bank will be switched and the new (downloaded) SW will be active.

noSwitch:

The Operational bank will not be switched after the restart, hence a manual switch must be performed in order to activate the new software. Please see description of steps in “Manual switch of banks” on page 293.

9. Click **Save**.

Manual switch of banks

1. Select **device** > **DevicePhysicalInventory** > **Software**
2. Select **Administrativebank** and switch to **opposite** bank number.
3. Click **Save.**
4. Perform a **restart**.

6.2.4 SW download to AXX155E

1. Select **device > SWdownload.**
2. Enter **FromIPaddress** (TFTP server Ip address).
3. Enter **SwdlFileName** attribute values (File path and name).

4. Click **Save.**

5. **Perform a restart.**

6.2.5 Backup and Restore of NE configuration data

Introduction

The purpose of this section is to guide you through management of the configuration data in the NE.

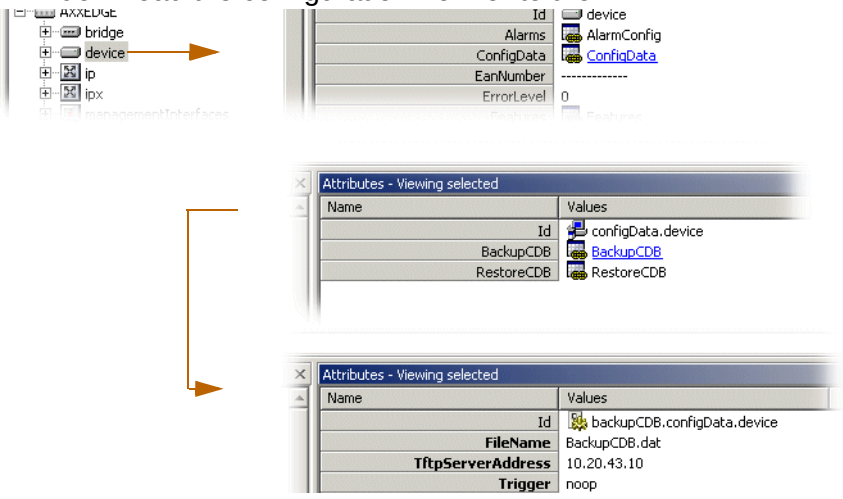
The section involves backup, presentation of an ongoing backup process and starting a restore of configuration data between a host and a NE. The configuration data is BER coded and can not be edited on the host.

Backup Configuration Data

Backup CDB will perform an back-up of the configuration data of selected NE and place it on the TFTP-server.

1. Select **device** in the selected network topology

2. Click on **ConfigData**. Here you selects whether to upload or download the configuration from or to the NE



3. Select **BackupCDB**.

The following attributes values are modifiable:

TftpServerAddress:

Destination IP address if configuration data should be uploaded on a remote host.

FileName:

File name and path for the configuration data storage

Trigger

If set to *noop* only parameters are saved.

If set to *backup*, the backup operation is started when clicking Save.

4. Enter values for the parameters and set **trigger** to **backup**
5. Click **Save** to commit the changes.
6. The TFTP upload process starts on the NE and the configuration data is stored on the selected host in the specified location (path and file name.)

NOTE! It is recommended to monitor the TFTP console during the upload process.

NOTE! Some TFTP servers require that the file exist on the TFTP server before an upload can be performed.

Restore Configuration Data

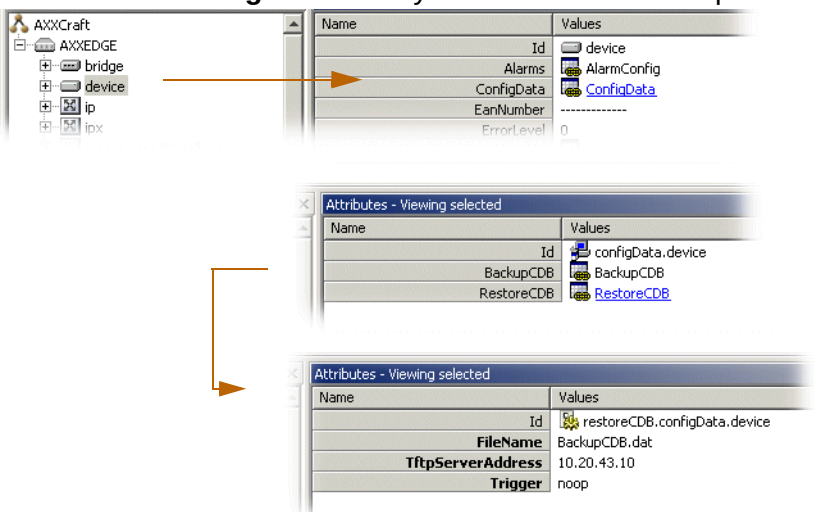
6.2.5.1 Prerequisites

The previous configuration data restore session has finished. If a scheduled restart is set before a new configuration data restore process is started, the scheduling parameters will be overwritten.

In order for AXX 9840 INSITE to restart the NE after the TFTP download session is terminated, the AXX 9840 INSITE needs to be able to capture the **endTftpSession** trap sent from the NE. This is the trigger needed by AXX 9840 INSITE to restart the NE.

1. Select **device** in the Management Tree.

2. Click on **ConfigData**. Here you select whether to upload or



download the configuration from or to the NE.

3. Select **RestoreCDB.**

The following attribute values are modifiable:

FileName:

File name and path for the configuration data storage

TftpServerAddress:

Source IP address of configuration data to be downloaded

Trigger

If set to *noop* only parameters are saved.

If set to *restore*, the restore operation is started when clicking Save

4. Set the parameters for the configuration data restore and set **trigger** to **restore**.

5. Click **Save** to commit the changes.

The TFTP download process starts in the NE and the configuration data is stored in the NE. AXX 9840 INSITE will restart the NE after a restore is completed.

NOTE! It is recommended to monitor the TFTP console during the download process.

7 General management

7.1 Manage the management interfaces

7.1.1 Introduction

NOTE! Management traffic and configuration is also described in the “MCN setup” chapter. We recommend the MCN wizard for MCN setup operations.

This chapter describes the configuration operations supported by the “Management Interfaces”managed object (M.O.). It is organized by the following sections:

7.1.1.1 Management modes and configurations.

This section describes the management modes supported by the management interfaces, and how they can be configured using the management tree.

7.1.1.2 “AXX 9200 EDGE Scenarios”

A repository of simple, but yet typical configuration scenarios that can be applied in combination to specific networks.

7.1.1.3 “OSI Stack”

Manage common parameters

- Download SW to Network Element
- Up/download of NE configuration data

7.1.1.4 “Alarm and Event configuration”

The purpose of this section is to guide you through the configuration of alarm and event reporting, and to be able to suppress and configure specific alarms.

7.1.1.5 “Manage common parameters”

The purpose of this section is guide you through management of the attributes that are related to the NE sub-rack and the NE common hardware and software.

7.1.1.6 “Manage synchronization”

The purpose of this section is to select the synchronization source for the internal SDH timing (T0) and the external synchronization output (T4).

7.1.1.7 “Alarm and Event configuration”

The purpose of this section is to guide you through the configuration of alarm and event reporting, and to be able to suppress and configure specific alarms.

7.1.1.8 “AXX 9300 METRO Shelf Management”

AXX 9300 METRO differs from the other Ericsson AXXESSIT network elements with plug-in modules. AXX 9300 METRO requires configuration of expected module modes, not expected module types. This is because the same module type can support different communication modes.

7.1.1.9 “Alternative procedures”

Operating on equipment protection groups, Aggregate Module Equipment Protection, Pre-provisioned modules/modes are installed and automatically configured.

7.1.1.10 “More about AXX 9300 METRO modules”

7.1.1.11 “Manage slots on AXX 9200 EDGE”

The purpose of this section is to describe the tasks and dynamic involved in inserting modules into and removing modules from a slot.

7.1.2 Configuration of AXX155A

Configuration of AXX155A is not described in details in this manual. Features are aligned with AXX 9200 EDGE with the following exceptions:

- Limited to STM-1 aggregation

- GE Ethernet modules and ports are not supported
- 1 service slot (named slot in Tree)
- 1 fixed slot (native interfaces in Tree)

The attributes under the Management Interfaces managed object are not unique in the information model. Each attribute mirrors a similar attribute located under another managed object. The attributes under the Management Interfaces managed object have been put together to allow the user to set-up basic configuration of the management interfaces without having to browse through many managed objects in the Management Tree. For advanced configuration operations, additional managed objects must still be used.

7.2 Management modes and configuration

NOTE! The following sections describe how to configure the Management Port and the DCCs by using the Management Interfaces managed object present in the Management Tree.

The management traffic is IP based (SNMP and TFTP messages), and therefore configuring a management path comes to deciding which encapsulation shall be used to send the IP datagrams carrying the management traffic over the network. For the management interfaces, two main encapsulation types exist:

- IP directly carried over a layer 2 protocol (Ethernet, PPP, or proprietary).
- IP encapsulated within CLNP carried over a layer 2 protocol (IEEE 802.x or LAP-D).

In addition, each management interface can be turned off[1]. Actual encapsulation support varies depending on the management interface type (Management Port or DCC). An overview of the different management modes versus the Management Interfaces is given in Table 9

1. This is an important feature for security purposes, especially for the Management Port which is physically accessible on the network element (main card).

Table 9 Management Modes versus Management Interfaces

Management Interface	Not Used	IP			OSI Encapsulation	
		IP / Ethernet	IP / proprietary encapsulation	IP / PPP	CLNP / IEEE 802.x	CLNP / LAP-D
Management Port	X	X*			X*	
DCC	X		X	X		X

NOTE! The Management Port is able to run both IP over Ethernet and CLNP over IEEE 802.x at the same time. On the contrary, a DCC can run only one mode at a time. In addition, a maximum of 8 DCCs can be used for management purposes, i.e. only up to 8 DCCs can have their management mode not set to "Not Used".

7.2.1 Management Port Configuration - AXX 9300 METRO

The Management Port on the AXX 9300 METRO can run two types of encapsulation, referred to as modes. A particular mode is selected by setting the variable mode (Management Interfaces >Management Port > mode). Required configuration for one of the four possible modes is further detailed in the next sections:

- not used
- IP

Procedure: **CONFIGURE THE MANAGEMENT PORT WITH MODE SET TO NOT USED:**

1. Click the **management Interfaces** managed object in the Management Tree, and then on **ManagementPort** link in the attributes window.

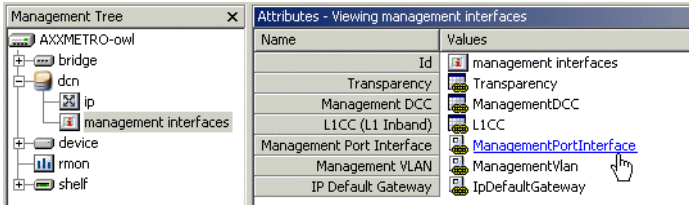


Figure 30 Management Interfaces - managed object

2. In the attributes window, select wanted **Mode**.

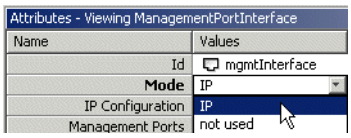


Figure 31 ManagementPort - mode selector

3. **Save**.

Procedure: **CONFIGURE THE MANAGEMENT PORT WITH MODE SET TO IP**

1. In the attributes window, set mode to **IP** and Sa**ve**.

2. Click on **ipAddress** in the attributes window.

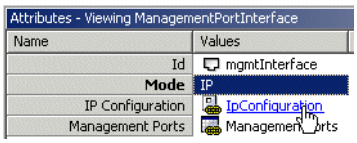


Figure 32 ManagementPort - ipConfiguration

3. Set **protocol** to **IP**, and set **ipAddress** and **subnetMask** for the management port according to your IP addressing scheme/plan.

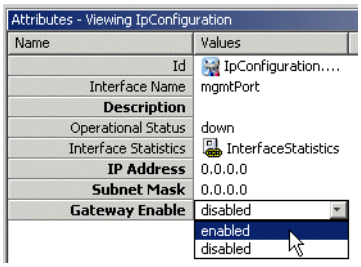


Figure 33 ManagementPort - add ipAdress

4. Set the **Gateway Enable** attribute

5. Save.

Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object.

7.2.2 Management Port Configuration - AXX 9200 EDGE

The Management Port can run four types of encapsulation, referred to as mode. A particular mode is selected by setting the variable mode (Management Interfaces >Management Port > mode). Required configuration for one of the four possible modes is further detailed in the next sections:

- not used
- IP
- osiEncapsulation
- ipAndOsiEncapsulation

Procedure: **SELECT MODE**

To configure the Management Port with mode set to Not Used:

1. Click the **management Interfaces** managed object in the Management Tree, and then on **ManagementPort** link in the attributes window.

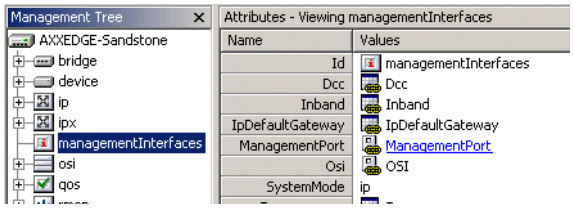


Figure 34 Management Interfaces - managed object

2. In the attributes window, select wanted **Mode**.

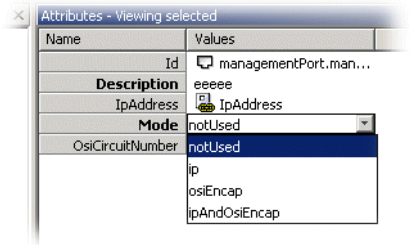


Figure 35 Management Port - mode selector

3. **Save**.

Procedure: **MODE: IP**

To configure the Management Port with mode set to IP:

1. In the attributes window, set mode to **IP** and Sa**ve**.
2. Click on **ipAddress** in the attributes window.

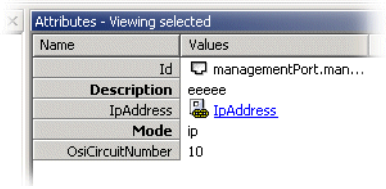


Figure 36 managementPort - ipAddress attribute

3. Click **Add**. Set **protocol** to **IP**, and set **ipAddress** and **subnetMask** for the management port according to your IP addressing scheme/plan.

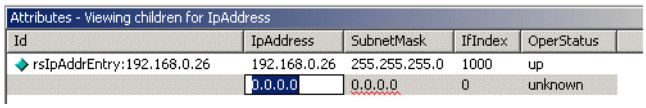


Figure 37 managementPort - add ipAdress

4. Save.

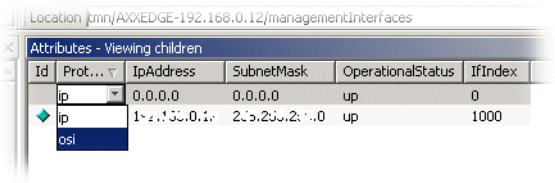
Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object as explained in section “IP Default Gateway Configuration” on page 308.

Procedure: **MODE: OSI ENCAPSULATION**

To configure the Management Port with mode set to OSI Encapsulation:

1. In the attributes window, set **mode** to **osiEncapsulation**.

2. **Save**.



3. Set **IP address.** Please see “OSI Configuration” on page 309.

4. Click **Add** on the toolbar. Set **protocol** to **OSI**, and set **ipAddress** and s**ubnetMask** according to your IP addressing scheme/plan.

5. **Save**.

Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object as explained in “IP Default Gateway Configuration” on page 308.

To define the parameters related to the OSI encapsulation and to the OSI stack, see “OSI Configuration” on page 309

Procedure: **MODE: IP AND OSI ENCAPSULATION**

To configure the Management Port with mode set to IP and OSI Encapsulation

1. In the attributes window, set **mode** to **ipAndOsiEncapsulation**.

2. **Save**.

3. Click on **IpAddress** in the attributes window. Be aware that two IP addresses must be defined, one for the IP interface and one for the OSI interface

4. To add an **IP address** to the **IP interface**

   - Click **Add** on the toolbar.
   - Set **protocol** to **IP**, and **set ipAddress** and **subnetMask** according to your IP addressing scheme/plan.

5. To **add** an **IP address** to the **IP interfaceOSI interface**[1]

- Click **Add** on the toolbar.
- Set **protocol** to **OSI**, and set **ipAddress** and **subnetMask** according to your IP addressing scheme/plan.

6. **Save**.

Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object as explained in “IP Default Gateway Configuration” on page 308.

To define parameters related to the OSI encapsulation, and to the OSI stack, see “OSI Configuration” on page 309.

7.2.3 DCC Configuration - AXX 9200 EDGE

A DCC can run four types of encapsulation modes. A particular mode is selected by setting the variable mode (Management Interfaces >DCC >mode). Required configuration for one of the three possible modes is further detailed in the next sections.

- not used
- IPOverDcc
- osiEncapsulation
- Transparency

Procedure: **SELECT MODE**

To configure a DCC with mode:

1. Click on the **AXX 9200 EDGE** managed object and then on the **management Interfaces** managed object in the Management Tree.

2. Click on **dcc** in the attributes window.

1. Since only one ifIndex for the OSI interface exists, an IP address for the OSI interface might already be present in the IP address table. Such an address might have been defined via another management interface, e.g. a DCC channel.

3. In the attributes window, each row represents a DCC interface. Set the **mode** for the selected DCC interface.

4. **Save**.

Procedure: **MODE: IP**

To configure a DCC with mode set to IP:

1. Select the **management Interfaces** object in the Management Tree.

2. Click on **dcc** in the attributes window.

3. In the attributes window each row represents a DCC interface. Set the **mode** to **IP over DCC** for the **desired DCC interface.**

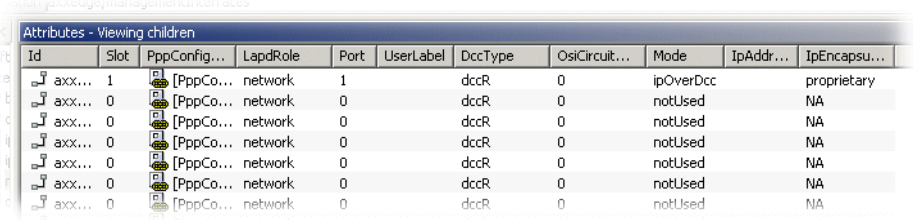


Figure 38 Management Interfaces - dcc attribute

4. In addition, when the mode is set to IP, the **layer 2 encapsulation** for the IP datagrams must be configured. This is done by setting the **ipEncapsulation** variable to the desired encapsulation (**proprietary**, **ppp/crc32 or ppp/crc16**).

Figure 39 ipEcapsulation - encapsulation selector

5. Save.

6. Click on **ipAddress** in the attributes window.

7. Click **Add** and **set ipAddress** and **subnetMask** according to your IP addressing scheme/plan.

8. Save.

If mode is set to IP, and ipEncapsulation is set to PPP, additional configuration for PPP can be performed via the pppConfiguration variable (Management Interfaces > DCC > pppConfiguration).

Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object as explained in “IP Default Gateway Configuration” on page 308.

Procedure: **MODE: OSI ENCAPSULATION**

To configure a DCC with mode set to OSI Encapsulation:

1. Click on the **AXX 9200 EDGE** managed object and then on the **management Interfaces** managed object in the Management Tree.
2. Click on **dcc** in the attributes window.
3. In the attributes window, each row represents a DCC interface. Set **mode** to **OSI Encapsulation** for the **desired DCC interface**.
4. In addition, when the mode is set to OSI Encapsulation, the **LAP-D role** for the DCC must be configured. This done by setting the **lapdRole** variable to the desired role (network or user).

Figure 40 lapdRole - role selector

5. Save.
6. Click on **ipAddress** in the attributes window.
7. Click **Add** on the toolbar. Set **protocol** to **OSI**, and **set ipAddress** and **subnetMask** according to your IP addressing scheme/plan[1].
8. Save.

1. Since it exists only one ifIndex for the OSI interface, an IP address for the OSI interface might already be present in the IP address table. Such an address might have been defined via another management interface, e.g. another DCC channel or the Management Port.

Depending on your topology, additional routing information might have to be configured. You can define static routes, and/or control dynamic protocols (RIP, OSPF) by using the IP managed object in the Management Tree. Defining a default gateway can be done directly from the Management Interfaces managed object as explained in “IP Default Gateway Configuration” on page 308.

To define parameters related to the OSI encapsulation, and to the OSI stack, see “OSI Configuration” on page 309.

7.2.4 IP Default Gateway Configuration

Procedure: **CONFIGURE AN IP DEFAULT GATEWAY ON THE NE**

1. Click on the **AXX 9200 EDGE** managed object, then on the **management Interfaces** managed object in the Management Tree.
2. Click on **ipDefaultGateway** in the attributes window.
3. Set the **defaultGatewayIpAddress** and **defaultGatewayInterface** according to your IP addressing plan.
4. Save.

NOTE! The default gateway must be directly reachable from the network element, i.e. the default gateway must belong to a subnet defined on the interface identified by defaultGatewayInterface.

Modifying the default gateway results in removing the previous default gateway from the network element's routing table, and adding the new (modified) gateway to the routing table.

Warning!

Secure routing before removal of default gateway.

7.2.5 OSI Configuration

Procedure: **OSI ENCAPSULATION AND STACK**

1. Click on the **AXX 9200 EDGE** managed object and then on the **management Interfaces** managed object in the Management Tree.
2. Click on **osi** in the attributes window.
3. Set the **network element NSAP address**. The NSAP address is entered as **area address** (areaAddress1 variable), **system ID** (systemId variable), and **network selector** (nsel variable).
4. Set the **ipaddress** and **subnet mask**.
5. Up to **three area addresses** can be allocated to the same area. Use areaAddress2 and areaAddress3 to define multiple area addresses.
6. Set **isMode** to configure the intermediate system mode (none, IS, L1 IS or L2 IS).
7. Set **gatewayEnable** to configure whether the device shall act as a gateway or a network element.
8. **If** the device is **configured as network element**, set the **gatewayNsap** to the **NSAP address of the gateway**.
9. Save.

Please see “OSI Stack” on page 316 for more details about the OSI encapsulation feature.

7.3 AXX 9200 EDGE Scenarios

This section presents 4 typical network topologies and describes how the management interfaces can be configured through the Management Interfaces managed object in AXX 9840 INSITE in order to carry management traffic.

7.3.1 Important note

In the following scenarios, it is assumed that both RIP and OSPF are disabled. That is, either the router license has not been downloaded to the network element (RIP is then disabled per default), or the router license has been downloaded but RIP has been manually disabled over the Management Interfaces. In the following scenarios, it is assumed that both RIP and OSPF are disabled.

Although each IP network is unique, the topologies and configurations presented in this chapter can be thought of basic building blocks, which can be combined together in order to be applied to a specific network.

In a real network, with a larger number of network elements, additional managed objects can be required to perform the configurations. In particular, configuration of IP and/or OSI static routes, activation and configuration of dynamic routing protocols (RIP, OSPF, IS-IS) require the use of additional managed objects. Configuration of some these features (e.g OSI static routes, IS-IS) are dependent of the license downloaded to the network element.

IP over DCC (with proprietary or PPP encapsulation) requires configuring a subnet per link (per DCC). Any network element configured with IP over DCC, and located more than 2 DCC links away from AXX 9840 INSITE must either have a static route to AXX 9840 INSITE, or run a dynamic routing protocol. As the number of static routes grows with the number of interfaces configured to run IP over DCC, running a dynamic routing protocol can be advantageous. Note that depending on the network topology, care must be taken when enabling IP routing protocol over DCC to prevent the DCC network from being advertised as a path for the user traffic (as opposed to only the management traffic).

Each of the next sections (“Scenario 1: AXX 9840 INSITE and AXX 9200 EDGEs on the same subnet” on page 312 to “Scenario 4: OSI Encapsulation” on page 315) presents a figure of a typical IP topology, together with the required parameters to be configured in the Management interfaces M.O.

7.3.2 Notations used

The following notations are used throughout the rest of this section:

The **"/<prefix-length>**[1]**"** notation is used to denote the {IP address, subnet mask} pairs. As an example, the notation 192.168.0.1 / 24 refers to the following pair {IP address 192. 168.0.1, subnet mask 255.255.255.0}.

"N/A" (non-applicable) is used to denote that an attribute is not relevant for a particular configuration, i.e. the value of the attribute will not influence the configuration.

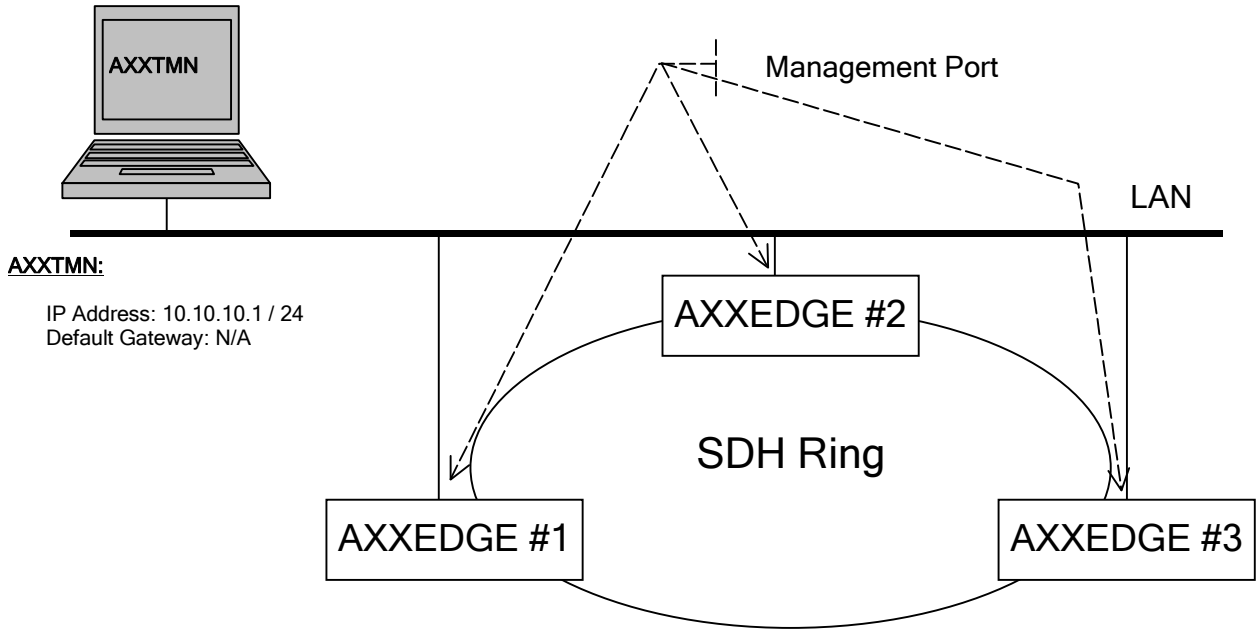
The notation **"Interface (OSI)"** used for defining the interface of the default gateway indicates that the ifIndex of the OSI interface should be used. Possible values are (OSI), (MGMT Port), or (DCC #n) to indicate the ifIndex of the OSI interface, the ifIndex of the Management Port, or the ifIndex of DCC channel n respectively. The values of the ifIndex can be found under the respective M.O.s, i.e. OSI, Management Port, and DCCs.

The notation "**Interface: (XXX)**" used for defining the interface of the default gateway (see scenarios 2 to 4) indicates that the ifIndex of the XXX interface should be used. Possible values for XXX are (OSI), (MGMT Port), or (DCC #n) to indicate the ifIndex of the OSI interface, the ifIndex of the Management Port, or the ifIndex of DCC channel n respectively. The values of the ifIndex can be found under the respective M.O.s, i.e. OSI, Management Port, and DCCs

1. The prefix-length is equal to the total number of contiguous 1-bits in the traditional subnet mask.

7.3.3 Scenario 1: AXX 9840 INSITE and AXX 9200 EDGEs on the same subnet

(System mode IP (default))



AXXEDGE #1:

Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.10 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: N/A
  - interface: N/A
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

AXXEDGE #2:

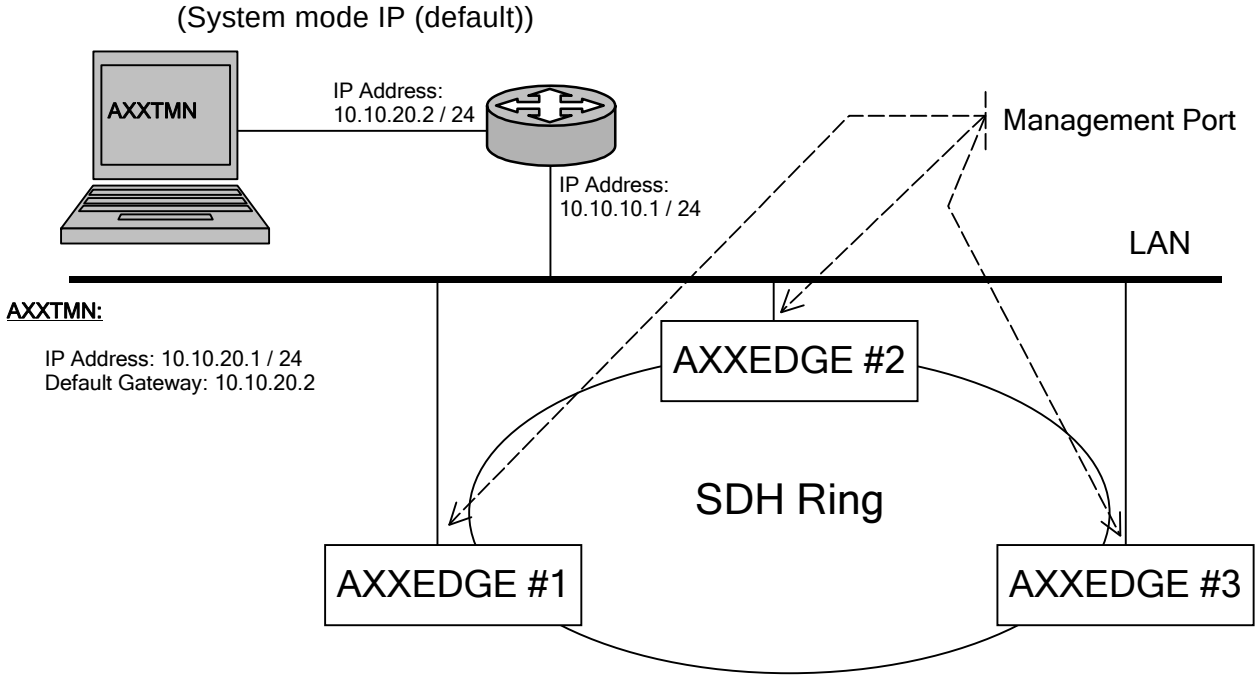
Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.20 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: N/A
  - interface: N/A
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

AXXEDGE #3:

Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.30 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: N/A
  - interface: N/A
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

Figure 41 AXX 9840 INSITE and AXX 9200 EDGEs on the same subnet

7.3.4 Scenario 2: AXX 9840 INSITE and AXX 9200 EDGEs on different subnets



AXXEDGE #1:

Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.10 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - **ipAddress: 10.10.10.1**
  - **interface: (Mgmt Port)**
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

AXXEDGE #2:

Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.20 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - **ipAddress: 10.10.10.1**
  - **interface: (Mgmt Port)**
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

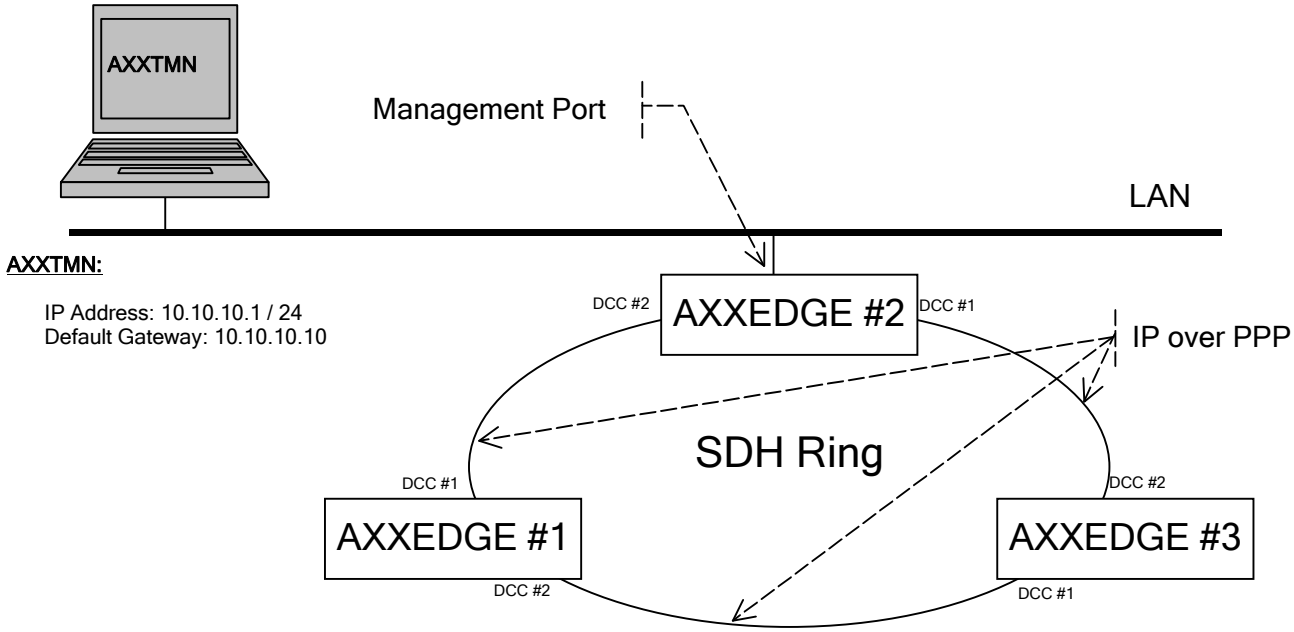
AXXEDGE #3:

Management Interfaces
- Management Port
  - **mode: IP**
  - **ipAddress: IP, 10.10.10.30 / 24**
- DCC#1
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - pppConfiguration
    - initialMRU: N/A
    - pppIpAdminStatus: N/A
    - compression: N/A
  - ipAddress: N/A
- DCC#2
  - mode: notUsed
  - ipEncapsulation: N/A
  - lapdRole: N/A
  - ipAddress: N/A
- IP default Gateway
  - **ipAddress: 10.10.10.1**
  - **interface: (Mgmt Port)**
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

Figure 42 AXX 9840 INSITE and AXX 9200 EDGEs on the different subnets

7.3.5 Scenario 3: IP over PPP

(System mode IP (default))



AXXEDGE #1:

Management Interfaces
- Management Port (local access)
  - mode: IP
  - ipAddress: 20.20.20.20. / 24
- DCC#1
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.10.1
- DCC#2
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.30.2
- IP default Gateway
  - ipAddress: N/A (Dynamic routing obtained via OSPF / RIP)
  - interface: (DCC #1)
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

AXXEDGE #2:

Management Interfaces
- Management Port
  - mode: IP
  - ipAddress: IP, 10.10.10.10 / 24
- DCC#1
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.20.1
- DCC#2
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.10.2
- IP default Gateway
  - ipAddress: N/A
  - interface: N/A
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

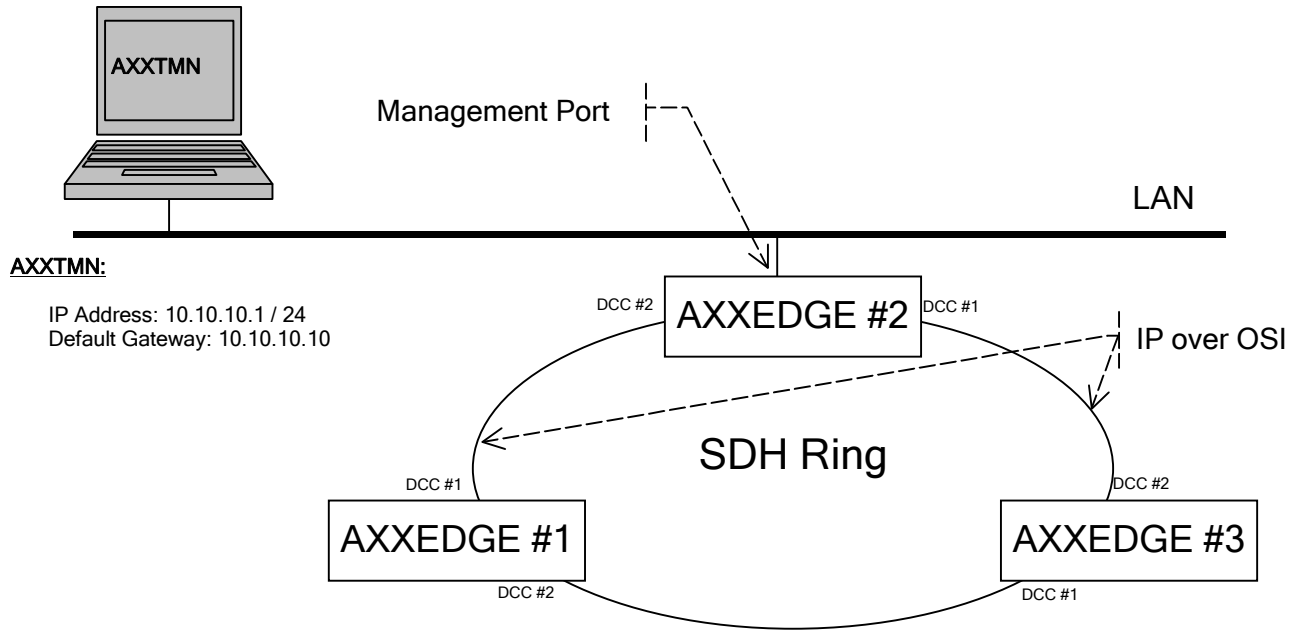
AXXEDGE #3:

Management Interfaces
- Management Port (local access)
  - mode: IP
  - ipAddress: 30.30.30.30. / 24
- DCC#1
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.30.1
- DCC#2
  - mode: IPoverDCC
  - ipEncapsulation: PPP/CRC-32
  - lapdRole: N/A
  - ipAddress: 192.168.20.2
- IP default Gateway
  - ipAddress: N/A (Dynamic routing obtained via OSPF / RIP)
  - interface: (DCC #1)
- OSI
  - areaAddress1: N/A
  - systemId: N/A
  - nsel: N/A
  - isMode: N/A
  - gatewayEnable: N/A
  - gatewayNsap: N/A

Figure 43 IP over PPP

7.3.6 Scenario 4: OSI Encapsulation

(System mode IP (default))



AXXEDGE #1:

Management Interfaces
- Management Port (local access)
  - mode: IP
  - ipAddress: 20.20.20.20 / 24
- DCC#1
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: user
  - ipAddress: N/A
- DCC#2
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: network
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: 192.168. 0.2
  - interface: (OSI)
- OSI
  - areaAddress1: 490000
  - systemId: 102030405060
  - nsel: 01
  - isMode: L1Is
  - gatewayEnable: disabled
  - gatewayNsap: 49000000011122334401
  - OSI IP: 192.168.0.1 / 24

AXXEDGE #2:

Management Interfaces
- Management Port
  - mode: IP
  - ipAddress: IP, 10.10.10.10 / 24
- DCC#1
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: user
  - ipAddress: N/A
- DCC#2
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: network
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: N/A
  - interface: N/A
- OSI
  - areaAddress1: 490000
  - systemId: 102030405070
  - nsel: 01
  - isMode: L1Is
  - gatewayEnable: enabled
  - gatewayNsap: N/A
  - OSI IP: 192.168.0.2 / 24

AXXEDGE #3:

Management Interfaces
- Management Port (Local access)
  - mode: IP
  - ipAddress: 30.30.30.30 / 24
- DCC#1
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: user
  - ipAddress: N/A
- DCC#2
  - mode: OSI Encapsulation
  - ipEncapsulation: N/A
  - lapdRole: network
  - ipAddress: N/A
- IP default Gateway
  - ipAddress: 192.168.0.2
  - interface: (OSI)
- OSI
  - areaAddress1: 490000
  - systemId: 102030405080
  - nsel: 01
  - isMode: L1Is
  - gatewayEnable: disabled
  - gatewayNsap: 49000000011122334401
  - OSI, 192.168.0.3 / 24

Figure 44 OSI Encapsulation

7.4 OSI Stack

7.4.1 Introduction

This chapter explains the basic concepts behind the OSI encapsulation feature.

Note that the OSI M.O. exists only if the OSI license has been downloaded to the network element.

The OSI stack is managed via the OSI managed object. Additionally, basic OSI configuration, e.g. NSAP address, IS mode, can also be performed via the Management Interfaces managed object (see “OSI Configuration” on page 309).

NOTE! The network element must be restarted before any change to the OSI stack parameters is effective.

OSI interface versus OSI circuits

The network element supports OSI encapsulation of IP traffic to allow two network elements to communicate transparently over CLNP-based networks, e.g. CLNP-based LAN or CLNP-based SDH networks.

The OSI encapsulation feature requires using the embedded OSI stack (refer to “OSI Encapsulation” on page 317 for more detailed information). As shown in Figure 45 , only the Management Port and the Data Communication Channels (DCCs) are capable of

carrying OSI traffic. The interface between the Management Port or a DCC and the OSI stack is referred to as an OSI circuit.

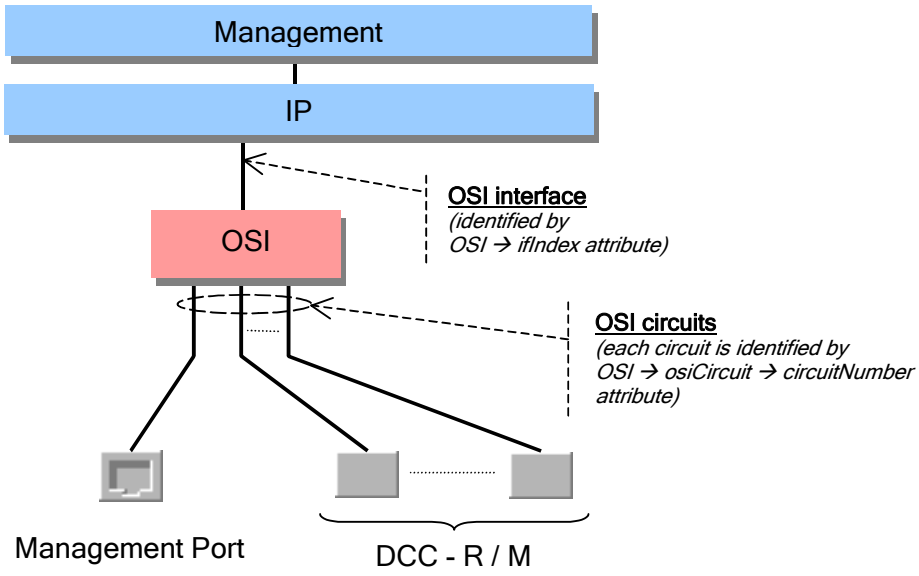


Figure 45 OSI interface versus OSI circuits

The OSI stack communicates with the IP layer through a single logical IP interface, referred to as the OSI interface. The OSI interface is identified (as any other IP interface) by an ifIndex. The value of this ifIndex is indicated by the OSI > ifIndex attribute.

7.4.2 OSI Encapsulation

The network element supports OSI encapsulation of IP traffic to allow two network elements to communicate transparently over CLNP-based networks. Typically the OSI Encapsulation feature is used to communicate over the DCC channels in an SDH networks with foreign equipment. The feature requires that the SDH network supports OSI on the DCC as specified by ITU-T G.784.

Physical versus logical IP models

A typical configuration using the OSI Encapsulation feature is shown in Figure 46

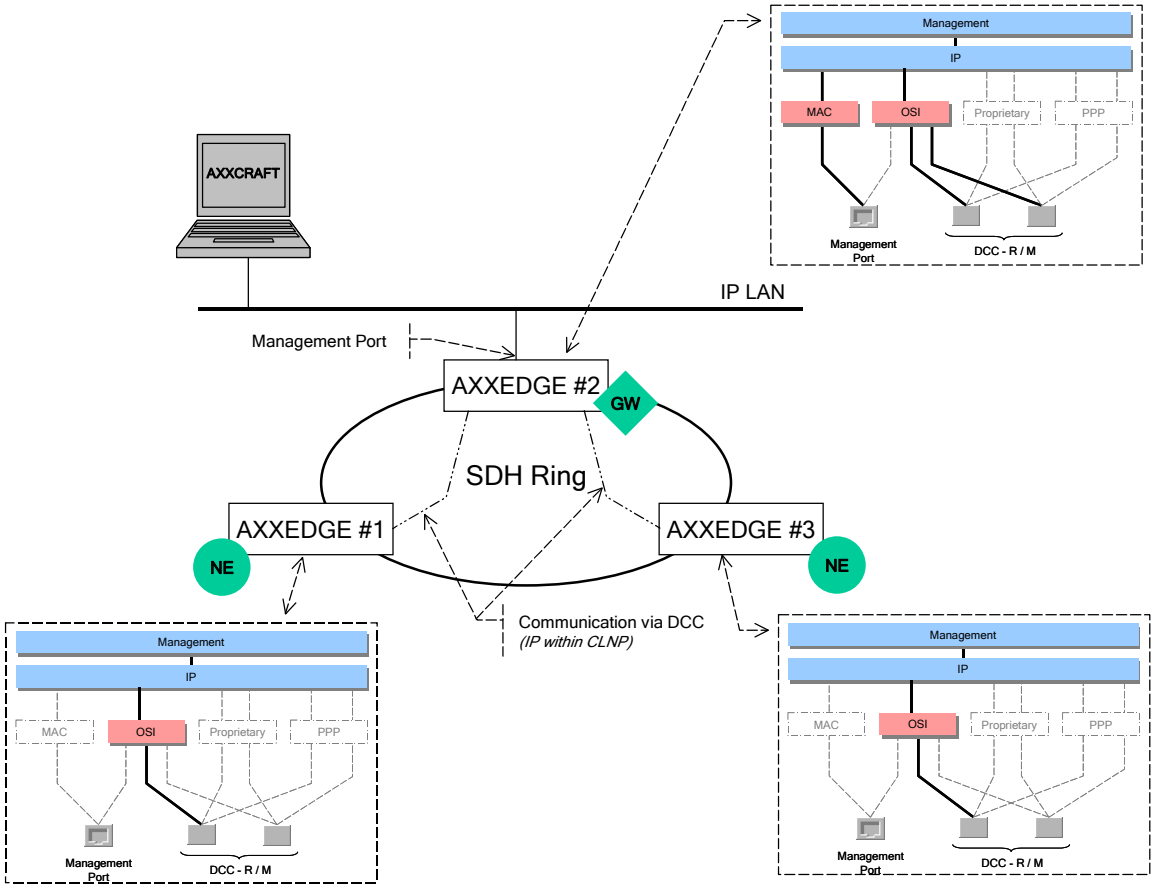


Figure 46 Typical configuration for OSI Encapsulation

The figure shows that AXX 9200 EDGE#2 is used as gateway between the IP LAN where the management PC running AXX 9840 INSITE is located and the other AXX 9200 EDGE network elements (AXX 9200 EDGE#1 and AXX 9200 EDGE#3). The network elements communicate by encapsulating their IP traffic within CLNP[1] traffic. From the AXX 9840 INSITE point of view, AXX 9200 EDGE#2 is an IP router providing access to an IP subnet where AXX 9200 EDGE#1 and AXX 9200 EDGE#3 are located. Figure 47 ,shows the logical model of the physical topology shown in Figure 46

1. CLNP is the network layer (layer 3) protocol used to implement OSI networks.

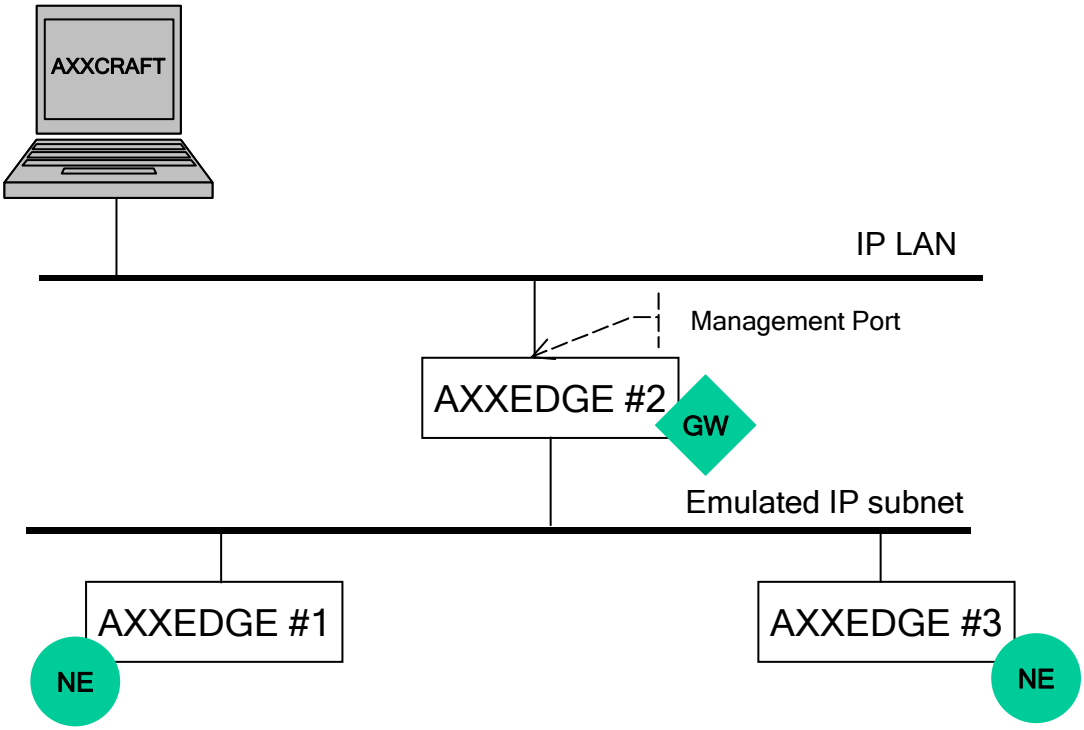


Figure 47 IP logical model

In order to enable communication over the CLNP-based network, the network elements must be allocated an NSAP address[1]. In addition, the network elements must also know where, i.e. the destination NSAP address, to send CNLP traffic.

To simplify the configuration, two concepts have been defined: NE and GW.

- NE a network element (NE) always sends CLNP traffic to its gateway (GW). Therefore, a NE must be configured only with its own NSAP address, and the NSAP address of its GW.
- GW a gateway must be able to decide where to forward IP traffic coming from AXX 9840 INSITE. To simplify the configuration, the GW is able to dynamically build an Address Mapper table. The table has one entry per NE present in the topology, and contains for each NE its IP address and its NSAP address. When the GW receives an IP data gram to be forwarded further to a remote AXX 9200 EDGE, it extracts the destination IP address, and gets

1. A Network Service Access Point (NSAP) address is one of two types of hierarchical addresses (the other type is the network entity title, or NET) used to implement OSI addressing at the network layer (CLNP).

the corresponding destination NSAP address by looking up at the Address Mapper table. The GW is then able to build the required CLNP data gram with the appropriate destination NSAP address.

To enable the gateway to dynamically build the Address Mapper table, each NE sends periodically Hello messages to its configured GW. The message contains IP and NSAP addresses for the NE. The GW uses this information to build and keep updated the Address Mapper table. The GW does not send any Hello messages.

Configuring an AXX 9200 EDGE running OSI Encapsulation as a GW (by setting the attribute OSI > osiIpAdaptation >gatewayEnable to 'Enabled') means the AXX 9200 EDGE will automatically build an Address Mapper table for all the NEs configured to be served by this AXX 9200 EDGE.

Protocols

The OSI Encapsulation feature encompasses both proprietary and standard protocols. The OSI block shown in Figure 45 to identify the use of the OSI Encapsulation feature is detailed further in Figure 48 .

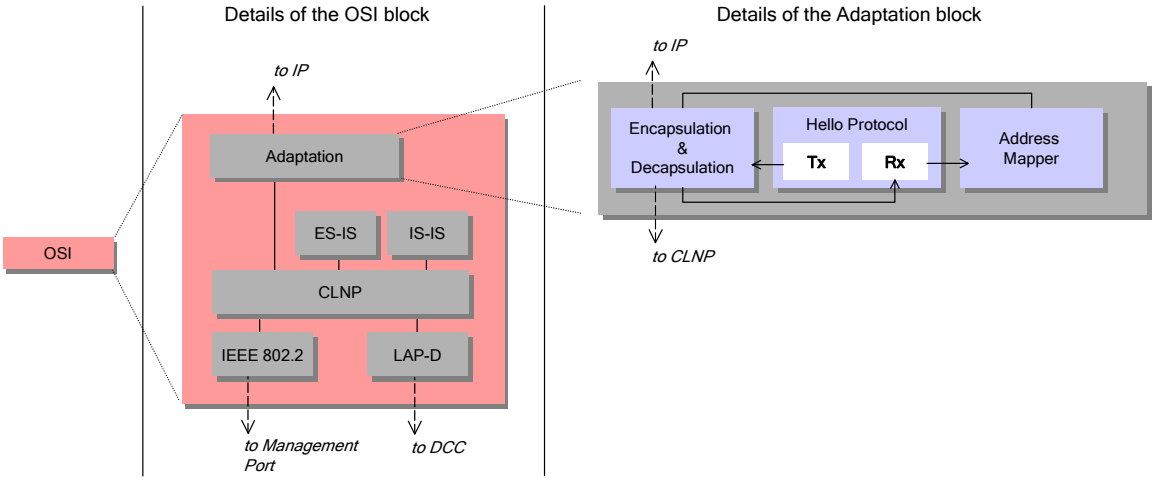


Figure 48 OSI Encapsulation Protocols

Within the OSI block, the IEEE 802.2, LAP-D, CLNP, ES-IS, and IS-IS refer to standard protocols in the OSI protocol suite. The adaptation block is the Ericsson AXXESSIT proprietary solution to encapsulate (and decapsulate) IP traffic within CLNP.

The Adaptation block is made up of three sub-blocks:

1. Encapsulation & Decapsulation this entity represents the actual encapsulation/decapsulation of IP datagrams in/from CLNP datagrams.

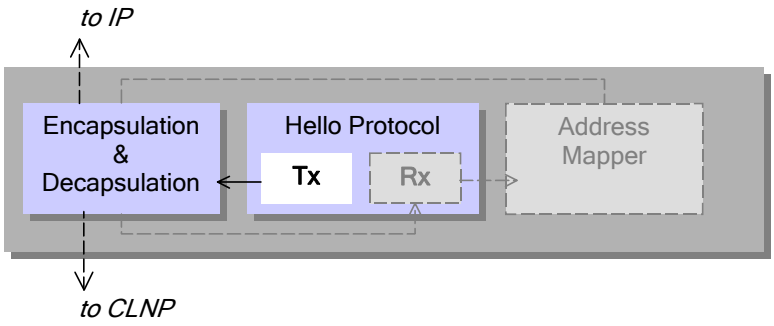
2. Hello Protocol this process is used by:

   - The NE to send periodic Hello messages to the GW.
   - The GW to receive Hello Message and update the Address Mapper Table

3. Address Mapper table implemented in a GW to keep the mapping between the IP and NSAP addresses of the NEs.

Depending on the configuration of the AXX 9200 EDGE as a NE or a GW, a different set of processes is enabled in the Adaptation block as shown in Figure 49 , where the disabled (inactive) processes are represented as boxes with dotted lines.

a) NE configuration



b) GW configuration

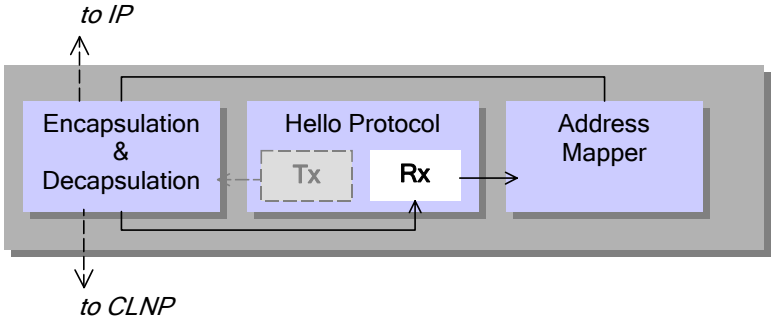


Figure 49 Active (enabled) processes in a) NE configuration, and b) GW configuration

Resilience

No resilience solution is implemented in the first release of the product, i.e. each NE can only be configured with one gateway.

7.4.3 Frequently Asked Questions

Why does OSPF not operate correctly over the OSI interface?

Network elements running OSI encapsulation over DCC create a hub-and-spoke partially meshed topology over the SDH network. Such a topology requires that the network elements be configured to run OSPF broadcast network type (see NOTE! below) over their OSI interface. In addition, it is necessary that the hub network element, i.e. the network element running as a gateway (GW), be elected the Designated Router (DR) to ensure that adjacency can be formed with every spoke.

NOTE! The network element currently only supports broadcast and point-to-point network types for OSPF.

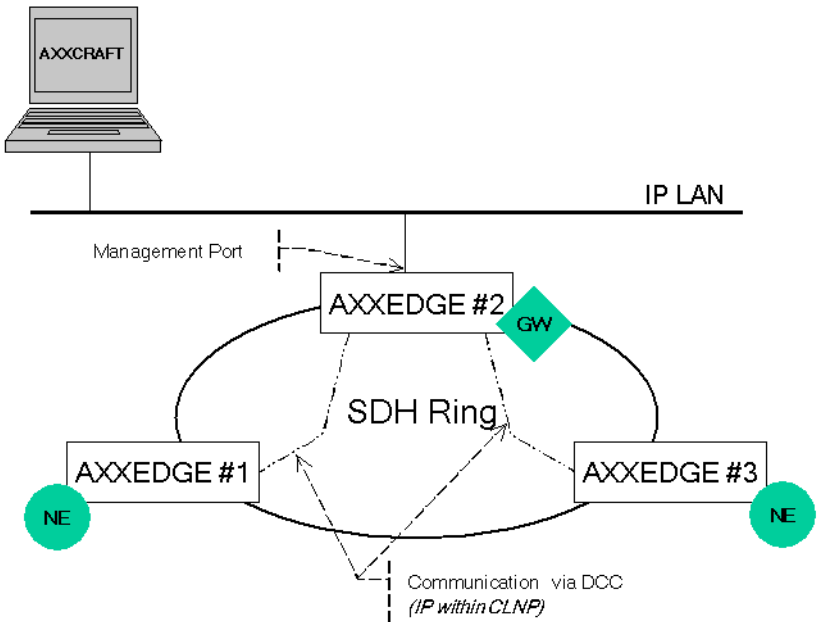


Figure 50 OSPF over OSI interface

Figure 50 displays an example of such a topology, where AXX 9200 EDGE#2 (configured as GW) must be elected as Designated Router by OSPF for the routing protocol to operate correctly. This is because AXX 9200 EDGE#2 is the only network element with full connectivity to other network elements.

Ensuring that the spokes (NEs - AXX 9200 EDGE#1 and #3 in the previous example) never initialize as Designated Router or Backup Designated Router during the election process is achieved by setting their OSPF priority on the OSI interface to zero (IP -> ospf -> ospfInterface -> priority = 0). Also see “Configure an OSPF interface” on page 593.

7.5 Manage common parameters

7.5.1 Introduction

The purpose of this section is guide you through management of the attributes that are related to the NE sub-rack and the NE common hardware and software.

The section involves presentation and modification of the NE identification, time settings, users, available features, the physical inventory, restart issues, LEDs and alarm output, and ping mechanism.

Synchronization, download of software, upload and download of configuration data, and management of NEs are described in separate sections.

7.5.2 View Common Parameters

1. Select the **device** in the Management Tree.

The system presents the common attributes (parameters):

- Identification of the network element
- Time settings
- Users
- Available features (licenses)
- Physical inventory
- Restart of network element
- Logs (alarm logs, performance data logs)
- LEDs and alarm output

- Ping mechanism

7.5.3 Modify Common Parameters

Procedure: **IDENTIFICATION OF THE NETWORK ELEMENT**

1. Select Network Element in the Management Tree

2. The following attributes can be modified:

Location

When entering value for Location, avoid special characters such as apostrophes and quotation marks. Only use letters.

NativeName

Owner

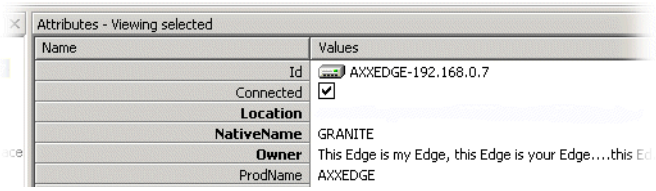


Figure 51 Identification of network element

Label

The attribute Label is based on the Location attribute and generated, based on the following rules:

Rule 1: Label =Location

Rule 2: Label = Location + "_" + <seq_no>
(if Location not have an unique value.). See example below.

Rule 3: Label = Ip address, if no contact with NE first time in management.

Rule 4: If Location is blank, Label = Ip address

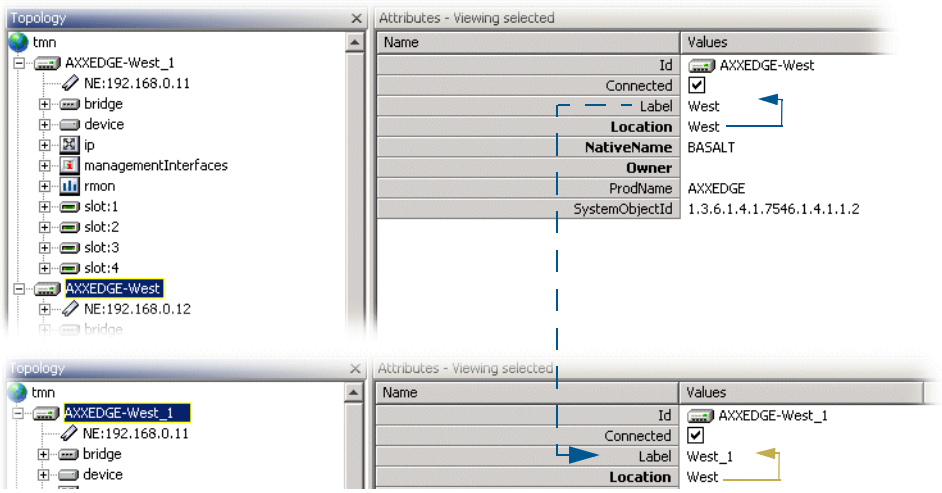


Figure 52 Attribute label

3. Click **save** to commit changes.

Procedure: TIME SETTINGS

The example below shows AXX 9200 EDGE.

1. Select **AXX 9200 EDGE** and then the **device** managed object

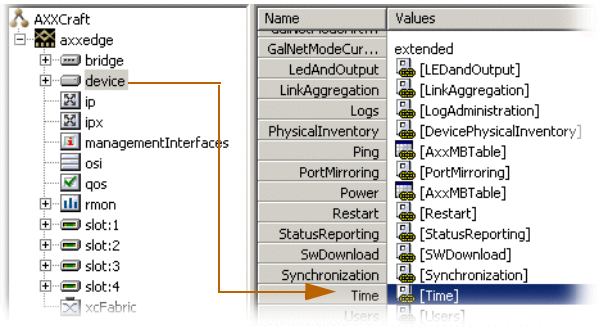


Figure 53 Time settings - time attribute

2. Click **Time.**

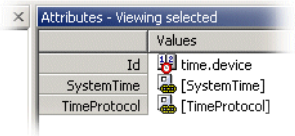


Figure 54 Time attribute - values

3. Click **SystemTime>Time** to view or modify.

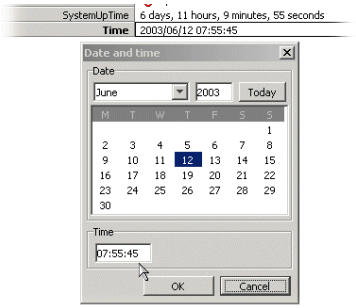


Figure 55 Time attributes - System Time

4. Click **TimeProtocol** to view or modify the following objects:

TimeServerIpAddress

TimeSyncInterval

TimeZone

Users

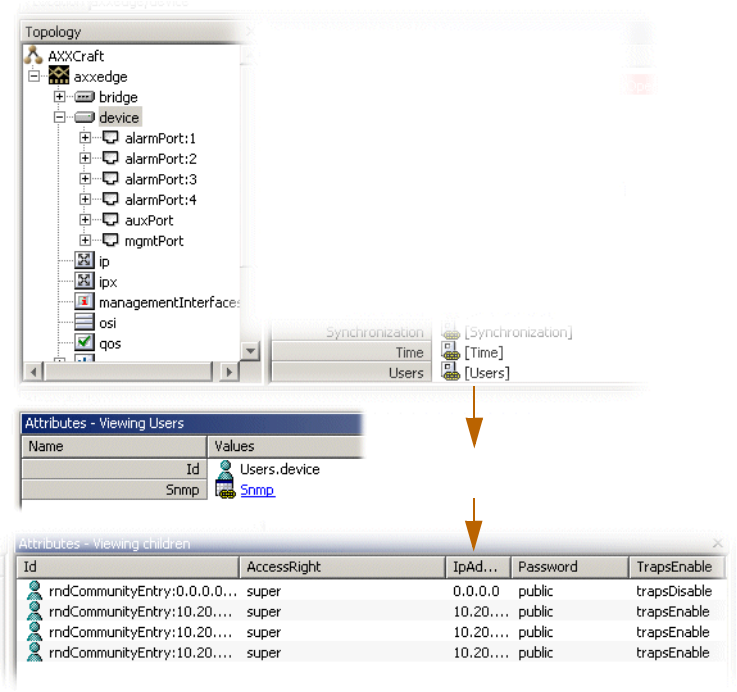


Figure 56 Add a new user - overview

Add a new user

1. **Navigate** as described above.
2. Click **Add**.
3. **Enter**
   - password
   - IpAddress
4. **Select** desired **AccessRight** from pull-down menu.
5. **Select** desired **TrapsEnable** state from the pulldown menu.
6. Click **Save**.

VT 100 password (AXX155E only)

1. Select **device**>**time**>**VT100**
2. Edit **Vt100Password** to desired value
3. Click **Save**

Available features (licenses)

1. Select device > Features > FeatureTable to view available licences
   .

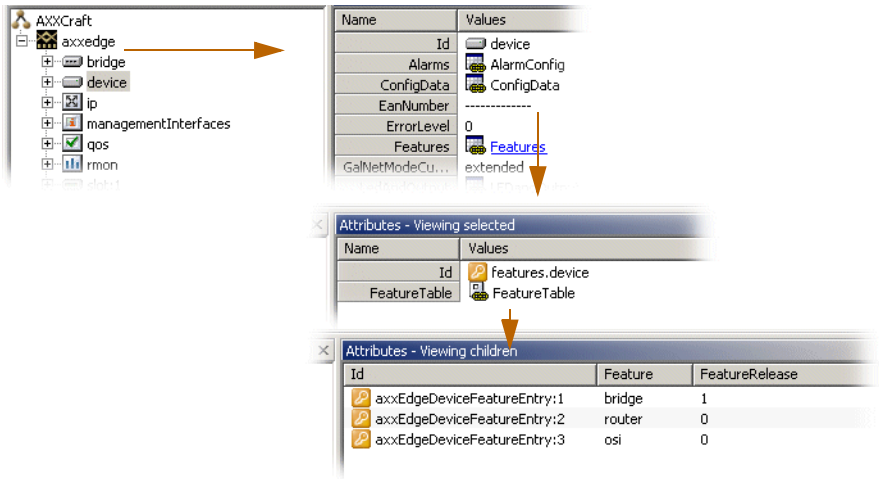


Figure 57 Available features

7.5.3.1 Feature selection

You can make the system present the features per NE with a filter applied to the managed objects.

Feature table attributes

- Key
- Description
- Enabled
- Locked
- Version
- Licensed
- License Key
- License Installed
- Authorized

Procedure: **CREATE A SELECTION IN FEATURE TABLE**

1. Select Tools menu and open Features
2. The Features list appears. Select NE from pulldown menu

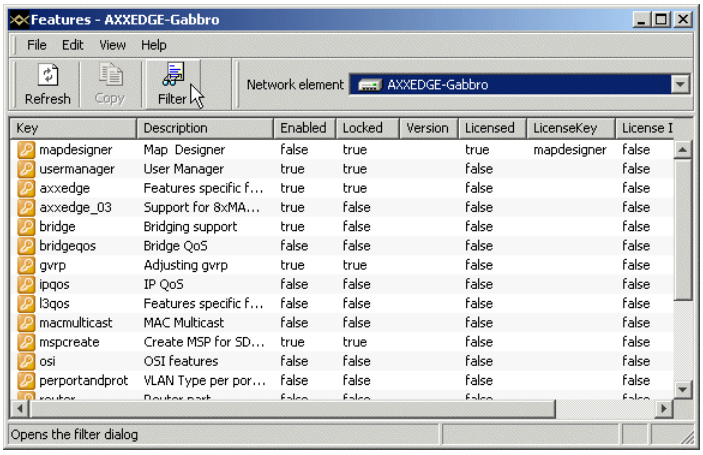


Figure 58 NE Features

3. Click Filter icon 

Feature Filter table appears on screen

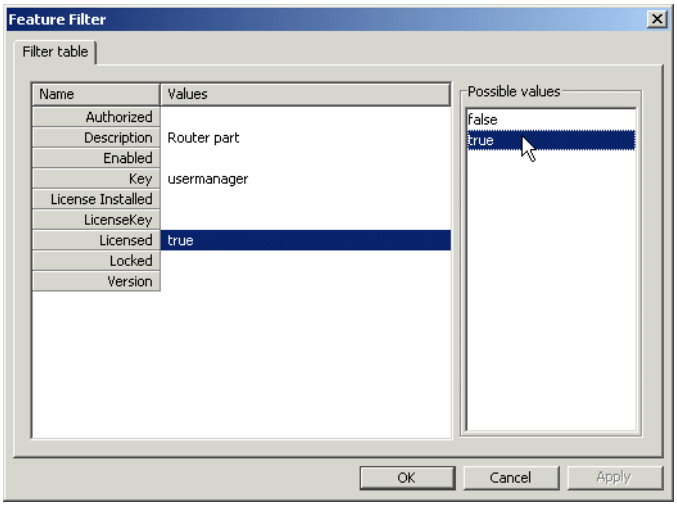


Figure 59 Feature filter table

4. Select filter attribute name in Filter table

Possible values appear in window to the right

5. Double- click values

6. Click OK

Feature filter closes down and NE Features appear as filtered.

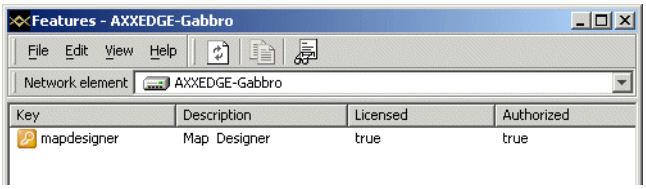


Figure 60 Filtered NE features

NOTE! The list is confirmed with Filter Enabled- icon in Status bar 

Procedure: **PHYSICAL INVENTORY - AXX 9200 EDGE**

1. Select **device** > **DevicePhysicalInventory**.

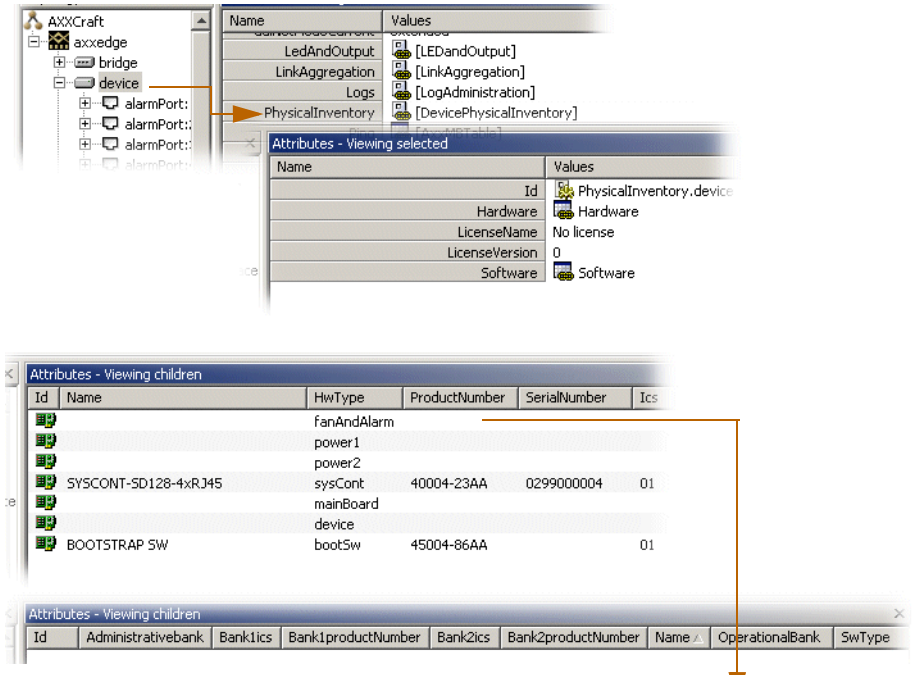


Figure 61 Physical inventory - overview

2. Select Hardware hyper link to list hardware inventory.

3. Select **Software** hyper link to list software inventory.

Procedure: **RESTART OF AXX 9200 EDGE**

1. Click **device**>**Restart**

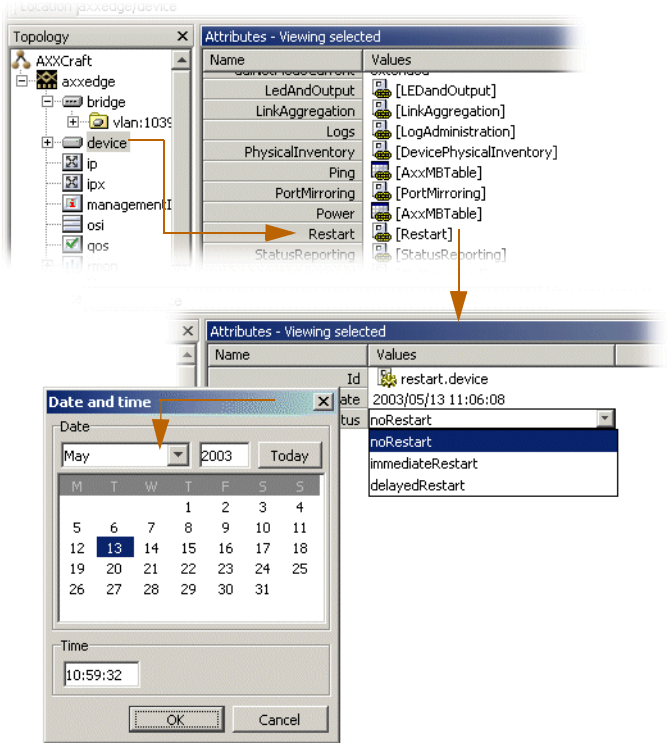


Figure 62 Restart of network element - overview

2. If selecting **delayedRestart**, **set time** and **date**.
3. Select desired **RestartStatus.**
4. Click **Save**.

Procedure: **RESTART OF AXX155E**

1. Click **device**>**Restart.**
2. Select **restart**.
3. Click **Save.**

Logs (alarm logs, performance data logs)

Clear Alarm History

1. Select device > LogAdministration.
2. Set **ClearAlarmHistory** to **clear.**
3. Click **Save**.
4. Refresh Notification History in the Notification List.

Clear PM Data

1. Select device > LogAdministration.
2. Set **ClearPMData** to **clear.**
3. Click **Save**.

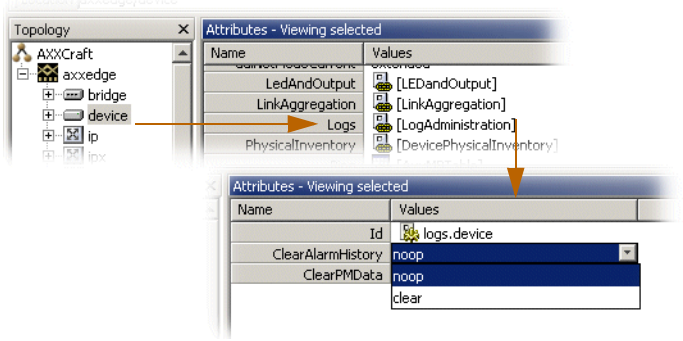


Figure 63 Clear alarm- and performance data log

LEDs and alarm output

1. Click **device** > **LEDandOutput**
2. Select **severity** to light the NE LEDs.

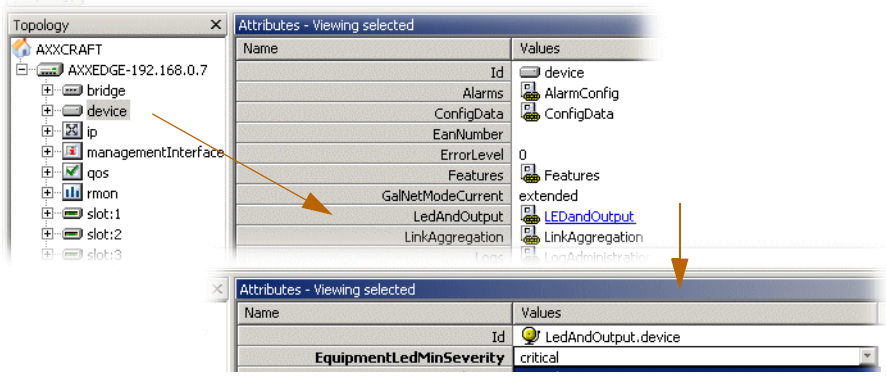


Figure 64 LEDs - severity selector

Status Reporting

Status reporting is a kind of "alive" reporting from the device to all trap-receivers defined in the community-table.

This function can be "enabled/disabled" and the status-trap-reporting frequency (time out) can be specified/altered.

The system currently reports the following in this status-trap:

- EquipmentLedStatus,
- AlarmTrafficLedStatus,
- DeviceStatusReporting,
- DeviceStatusReportingFrequency,
- sysDescr,
- sysObjectID,
- sysUpTime,
- sysContact,
- sysName,
- **sysLocation**

One of the NE/ network discovery criteria in Ericsson AXXESSIT's management solutions is Trap Discovery. The status trap sent by NE default every 10 minutes completes this solution.

Ping mechanism

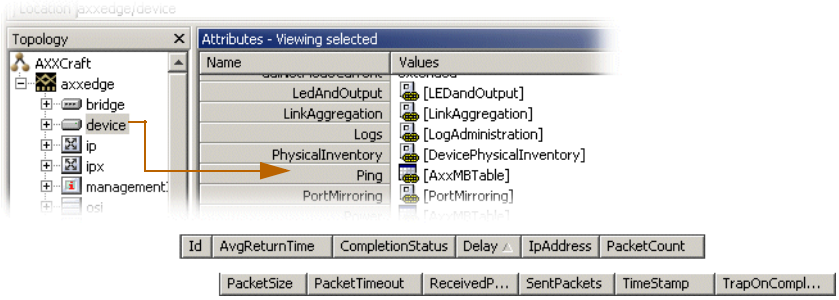


Figure 65 Ping mechanism

1. Select **device** > **Ping** hyper link
2. The following attributes are modifiable:

Delay

PacketCount

TrapOnCompletion (true/false)

PacketSize

PacketTimeout

Alarm Ports

1. Select **device** > **alarmPort** in the Management Tree.
2. The following attributes are modifiable:

Description: Free text description

Mode: enabled or disabled

TriggeredWhen: opens or closes (when an alarm is to be triggered)

3. Click **Save**.

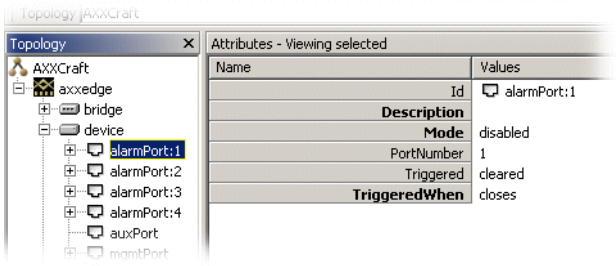


Figure 66 Alarm ports

AUX Port - AXX 9200 EDGE

1. Select **device** > **auxPort**

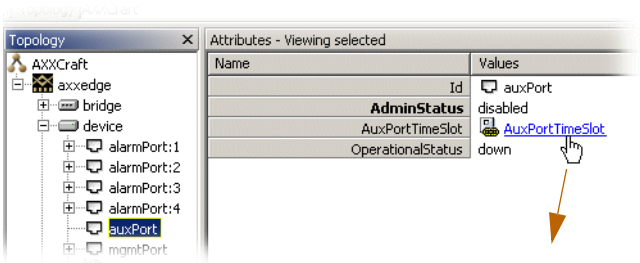


Figure 67 AUX port

2. The following attributes are modifiable:

AdminStatus : enabled or disabled

AuxPortTimeSlot:see below.

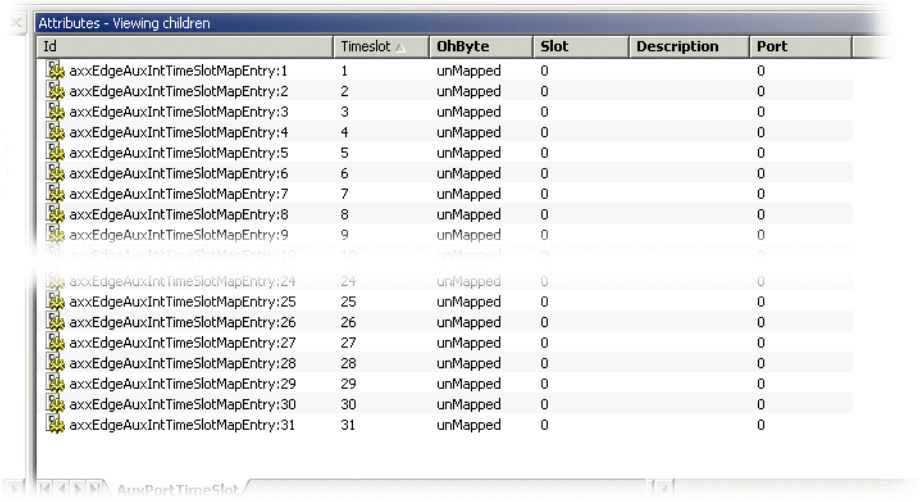


Figure 68 AUX port - Timeslots

The following attributes can be modified for **AuxPortTimeSlot:**

OhByte: e1, e2, f1 or unmapped

Slot:

Description:

Port:

Power module - AXX 9200 EDGE

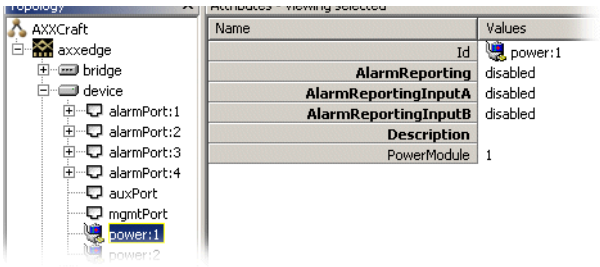


Figure 69 Power module - attributes

1. Select device > power
2. The following attributes are modifiable:

AlarmReporting: disabled or enabled

AlarmReportingInputA: disabled or enabled

AlarmReportingInputB: disabled or enabled

Description: free text description

7.6 Manage synchronization

7.6.1 Introduction

The purpose of this section is to select the synchronization source for the internal SDH timing (T0) and the external synchronization output (T4).

The AXX 9200 EDGE T0 and T4 automatic selection processes can select the source from a short-list of available inputs. This selection is based on quality and priority.

You can override the automatic selection process by manual commands.

The first part of this section gives a short introduction to SDH synchronization which is meant to help you in understanding the requirements specified in this document.

READ MORE: The synchronization is G.781 compliant. For further reading on SDH synchronization, please see ETSI ETS 300 417-6-1, ITU-T Recommendation G.781, G.812 ("Timing requirements of slave clocks suitable for use as node clocks in synchronization networks") and G.813 ("Timing characteristics of SDH equipment slave clocks (SEC)").

7.6.2 SDH synchronization

Synchronization networks

A synchronization network is a set of clock nodes that are maintained in synchronization with one another. To achieve this it is necessary to accurately transfer synchronization reference information between nodes so that their relative synchronization may be monitored and maintained.

Since it is difficult to synchronize all international nodes from the same master clock, each network operator typically have a Primary Reference Clock (PRC) as defined in ITU-T Recommendation G.811.

From the PRC the synchronization reference information is distributed to all nodes in the SDH network in a tree-type network topology as shown in Figure 70

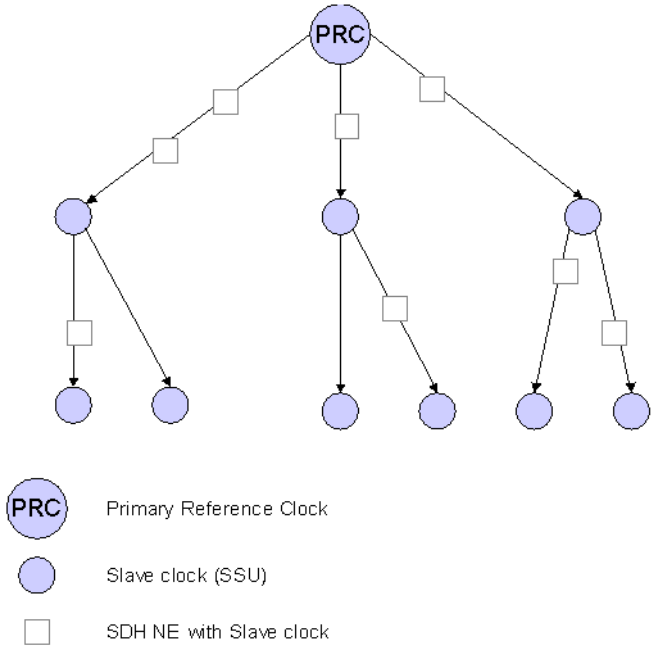


Figure 70 Figure 1 Example synchronization network

Intermediate slave clocks can enter holdover conditions if their connection to the master clock is lost. Slave clocks called Synchronization Supply Units (SSU's) will continue to serve their branch of the network until the connection with the PRC is re-established. There may be several SSU's concatenated in a large network.

Intermediate SDH NEs will also contain slave clocks, the SDH Equipment Clock (SEC). Their quality are not sufficient for providing synchronization reference information to other parts of the network, but they can serve the SDH NE itself in holdover mode if all high quality incoming references are lost.

As can be seen from the figure, the SDH NEs have a dual role since they need a synchronization reference to operate properly in a network and they are important for distribution of synchronization reference information to other networks.

Selecting the best synchronization reference

To reinforce the reliability of the synchronization network, alternative routes are often used between the clocks. The slave clock can then be switched to another synchronization reference manually, or automatically by monitoring the signal at the physical interface.

An improvement to simple signal monitoring is to send the Synchronization Status Message (SSM) along with the synchronization signal to indicate the Quality Level (clock type) of the source clock. The next clock in the chain can now select the best clock based on this Quality Level.

Not all connections used for synchronization can send the SSM along with its synchronization reference. In this case it is possible to manually indicate the Quality Level for this interface in AXX 9200 EDGE. This ensures that also references without SSM can be part of the automatic selection process that is based on Quality Level.

To avoid timing loops in the network it is sometimes necessary to indicate in SSM that this synchronization reference should not be used. This is done by sending the Do Not Use (DNU) message.

Synchronizing the SDH equipment

All SDH equipment contains a clock for the SDH pointer adjustments, cross connection matrix operations and the outgoing line signal (STM-N). It is normally operating as a slave clock and locked to a high quality incoming reference, but can run in holdover mode if the reference is lost.

This section describes how the Internal Timing (T0) is derived from the available synchronization references in AXX 9200 EDGE.

Synchronization reference information can be extracted from any of the incoming STM-N SDH interfaces (T1), 2 Mbit/s PDH interfaces (T2) or the external 2MHz synchronization input (T3) as indicated in Figure 71

The figure shows that only one at the time of the available synchronization references will be used as a reference for the SDH

equipment Clock (SEC). SEC is the clock used for Internal Timing (T0). When no reference is available it will run in Hold-Over mode.

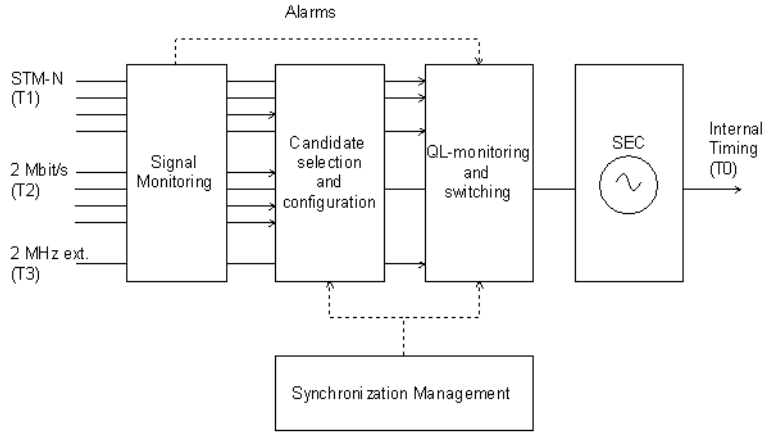


Figure 71 T0 selection

7.6.3 AXX 9200 EDGE

Signal Monitoring

All interfaces are monitored for signal level and framing errors. The failure will be reported to the candidate selection and QL-monitoring and switching processes.

Candidate selection and configuration

In AXX 9200 EDGE up to five synchronization reference candidates can be selected to participate in the selection process.

For each synchronization source candidate the following parameters can be read/configured:

- Type (T1, T2 or T3 where T2 must be a 2Mbit/s PDH Port in PRA mode).
- Identification of the synchronization source candidate (via its slot number, port number etc.)
- Whether SSM usage is enabled (T1 only).
- Assigned Quality Level (QL). If SSM usage is disabled, the operator is free to assign a fixed QL.
- Current Quality Level. If SSM usage is enabled (T1) the Quality Level of the incoming signal is seen here. If an alarm is detected on the synchronization source interface, the Current Quality Level indicates "Failed" (Independent on SSM usage).

- The priority of the synchronization source candidate. This priority will apply only when there are multiple candidates all having the highest QL among all possible source candidates.
- Hold-Off time and Wait To Restore time. (See QL monitoring and selection process).

For each synchronization source candidate the following methods are available:

- Set/Clear Lockout. This is used to temporarily exclude a specified synchronization source.
- Clear WTR.

QL-monitoring and switching

The QL-monitoring and selection process will continuously monitor the Quality Level (QL) of the candidate synchronization references and select the reference with the best QL. Only error free references are included in the selection process. (Alarms are detected in the Signal Monitoring functional block). If there is more than one candidate with the highest available QL, the priority parameter will be used for selection.

The following parameters can be read/configured for the selection process:

- Selected synchronization reference and its QL.
- Switch mode. This indicates whether the selection process is running in the Automatic, Forced or Manual switch mode (See methods below).

The following methods are available for the selection process:

- Manual switch command. A manual switch can be performed only to a source with the highest available QL. This means that manual switching can only be used to override the synchronization source priorities.
- Forced switch command. This command overrides the currently selected synchronization source.
- Clear command. Clears any of the Manual or Forced switch commands.

SEC

The AXX 9200 EDGE slave clock.

SEC will enter holdover mode for the specified Hold-Off time if an alarm is detected on the selected synchronization reference. After

the Hold-Off time the selection process will switch to the error free reference with the highest QL.

When a candidate synchronization reference recovers from an alarm condition, the signal shall be free for faults for the wait to restore time before taken into consideration by the selection process.

The selected T0 reference is also used on all output STM-N signals.

Synchronizing external equipment

AXX 9200 EDGE also provides an external synchronization output (T4). This is a separate 2 MHz signal that can be used directly as a synchronization reference for other equipment or as a synchronization reference to a separate Stand Alone Synchronization Equipment (SASE).

Synchronization reference information can be extracted from any of the incoming STM-N SDH interfaces (T1) or the internal timing (T0) as indicated in Figure 72

The figure shows that only one at the time of the available synchronization references will be used for External Timing (T4).

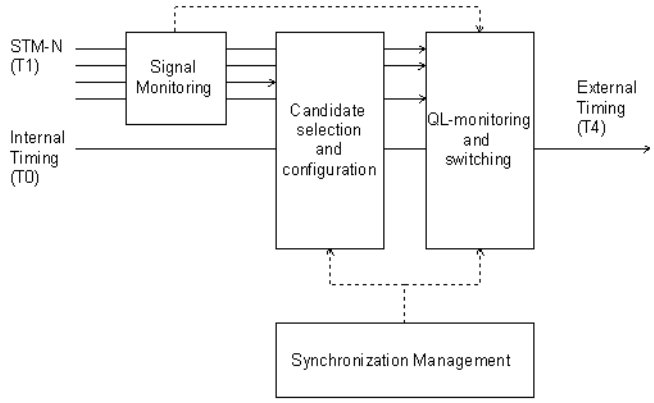


Figure 72 T4 selection

Here is a short description of the functional blocks for T4 selection:

7.6.3.1 Signal Monitoring:

- See “SDH synchronization”on page 7-336.

7.6.3.2 Candidate selection and configuration:

- See “SDH synchronization”in page 7-336.
  T0 can be one of the candidates.

7.6.3.3 QL-monitoring and switching:

See “SDH synchronization”in page 7-336.

Additional parameter for T4:

- QL Minimum Level (QLM).

Rules

- When referring to a T1 or T2 synchronization reference slot and port numbering is used.
- When referring to the T0 or T3 synchronization reference no further identification is required.
- SSM is always disabled for T2 and T3 references
- A 2 Mbit/s PDH Port should be treated as a T2 Source only when it is operating in PRA mode
- In principle a user can add the same source twice, but you should be advised not to do this.
- More than one reference can have the same priority.
- You should receive a warning before deleting the active synchronization source. However, no further restrictions apply.
- The Automatic selection process will find the best source based on the Current QL. If more than one source have the highest QL, the source with the highest QL and Priority will be selected. If priority is also the same, AXX 9200 EDGE will choose the first source in the list with highest QL and Priority.
- A Manual switch can be performed only to a source with the highest available QL.
- A Forced switch overrides the currently selected synchronization source.
- The new source selected by the Manual and Forced switching cannot have a Current Quality level of "Failed" or "SEC".
- WTR Clear does not exist as a method in the MIB. Must set WTR = 0 and then back to original value if method is implemented in Manager.
- T0 is the default candidate for T4
- If no candidates are available for the T4 selection process, no synchronization source is selected and the external synchronization output is squelched
- When QL of the selected T4 reference falls below the QLM level, the T4 output signal shall be squelched (muted) to let the slaved oscillator go into holdover or select another reference.

- T4 is only used for external synchronization output (not for output STM-N signals).

Synchronization Alarms

Synchronization alarms are treated as any other AXX 9200 EDGE alarms as described in a separate section.

The following table identifies the alarms related to SDH synchronization events:

Table 10 Alarms related to SDH synchronization events

AlarmId	**Description**	**Comment**	**Clearable**	**Default Severity**
T0_HOLDOVER	SETG enters holdover	No sync. sources available (applies to T0 sync. only)	Yes	MAJOR
T0_SWITCH	Change of sync. source	Applies to automatic, manual or forced switchover (T0 only).	No	INFO
SYNCSRC_QL	QL_FAILED or QL_DNU for any sync. candidate	Applies to T1/T2/T3 sources member of the T0 sync. table	No	INFO
T4_SQUELCH	T4 output squelched (on "permanent" basis)	No T4 sync. candidate with QL equal to or above QL_{min}	Yes	MAJOR
T0_DEFECT	SETG failure	Caused by defective hardware impacting the internal T0 clock	Yes	CRITICAL

NOTE! By a synchronization candidate is meant a synchronization source contained in either of the T0 or T4 sync. source tables (5 entries each).

7.6.4 View the Synchronization Data (T0 or T4)

T0 and T4 Synchronization are treated in common in the description of the flows due to their common behaviour. The user is considered to be an experienced SDH user since synchronization management is not directly related to the services offered by AXX 9200 EDGE.

- You access the synchronization attributes from the Management Tree.

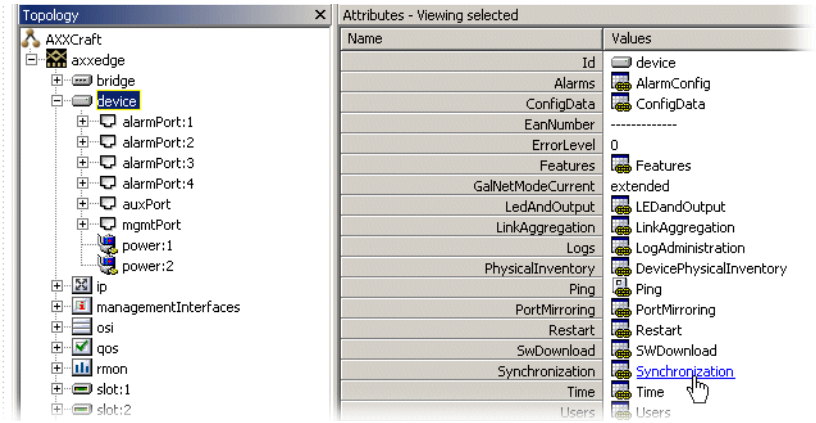


Figure 73 Synchronization - selecting managed object

The system presents a list of all Synchronization Source candidates.

All attributes of the Synchronization Source candidate are presented as defined in the information model.

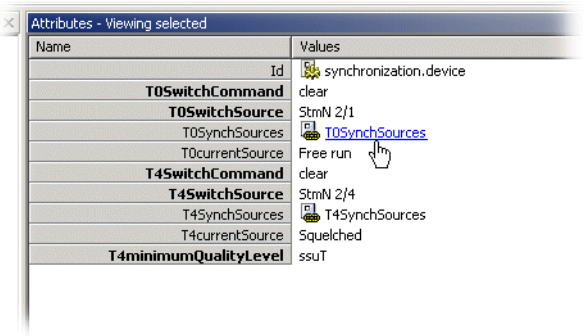


Figure 74 Synchronization - T0SynchSources attribute

If the source experiences a signal error the SSM attribute shows "Failure" instead of the SSM value.

The system presents the synchronization attributes with the relevant data.

7.6.5 Add Synchronization Source candidate (T0 or T4)

Procedure: **ADD SYNCHRONIZATION SOURCE CANDIDATE (T0 OR T4)**

1. Select **TOSynchSources** or **T4 SynchSources**

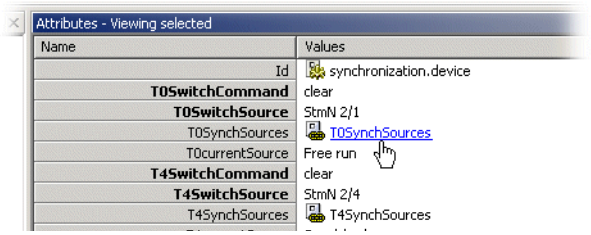


Figure 75 Add Synchronization Source - attribute selection

2. Click **Add** on the toolbar

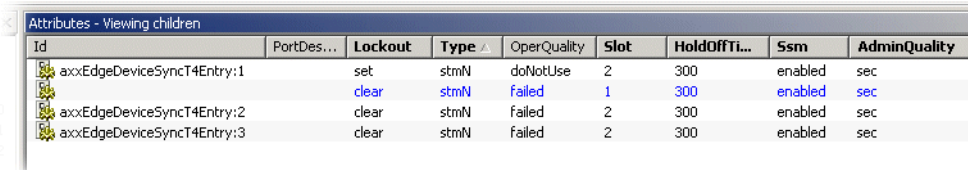


Figure 76 Add Synchronization Source

3. Enter the synchronization parameters in the Management Tree for the new candidate. The list of existing Synchronization source candidates must be less than five.

Type: STM-n, e1, external

Slot/ Port: number

SSM: enabled/disabled

Admin Quality/Assigned Quality Level
(N/A when SSM is enabled): sec, ssuL[1], ssuT, prc

Priority: 1..5 (where 1 is highest priority)

Lockout: clear/set

Hold-Off Time: 300..1800 ms

Wait To Restore Time: 0..12 min

4. Click **Save** to commit the new synchronization source candidate.

If you attempt to add a new synchronization source candidate when the candidate list is fully populated (five entries), you will be informed that a candidate must be deleted before adding a new.

The system verifies that the candidate is legal before performing the actual add. If any errors are found, the candidate is not added and you is informed and given the opportunity to correct the problem.

You can add more than one candidate before committing and a failure on one candidate has no consequence for the addition of the other candidates.

1. Synchronization Supply Unit (SSU):
- High quality
- Two types: SSU Transit (ssuT) better quality than SSU Local (ssuL)
- Between PRC and SEC
- Can sync. a part of a network if connection to PRC is lost

7.6.6 Modify Synchronization Source candidate (T0 or T4)

1. Access the synchronization attributes from the Management Tree.

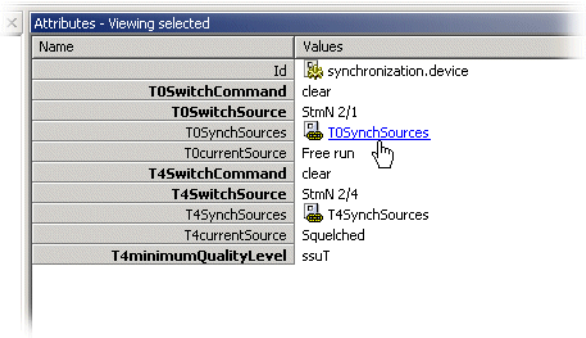


Figure 77 Modify Synchronization Source - attribute selection

2. Modify the modifiable Synchronization Source candidate attributes.

   - SSM Enabled can be True only for T1.
   - QL can only be modified if SSM Enabled is False.

3. Click **Save** to commit the changes.

7.6.7 Delete Synchronization Source candidate (T0 or T4)

You have two possible alternatives for deleting a Synchronization Source candidate:

Procedure: **DELETE SYNCHRONIZATION SOURCE CANDIDATE ALT. 1**

1. Access the **synchronization attributes** from the Management Tree.

2. Select the **synchronization source candidate(s)** to delete and click **Delete** in the toolbar menu.

3. Click **Save** to commit.

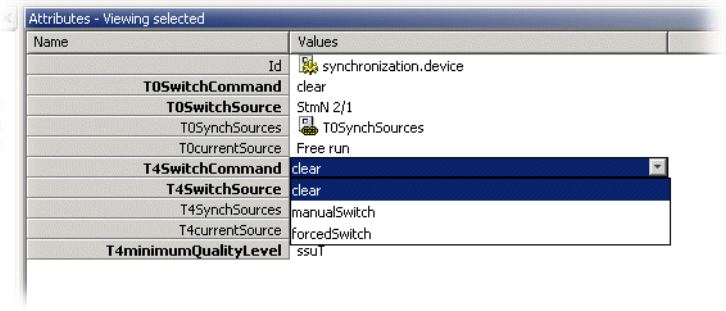
Procedure: **DELETE SYNCHRONIZATION SOURCE CANDIDATE ALT. 2**

1. Select the **Port** (synchronization source) in the Management Tree
2. Select **Do not use for T0 Synchronization** from the drop down menu.
3. Select **Delete**. If you selected synchronization source candidate is the active synchronization source, you receives a warning from the system.
4. Click **Save** to commit the final delete.

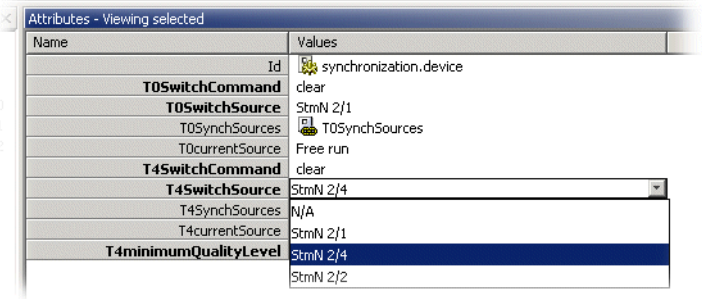
7.6.8 Operate Synchronization Switch (T0 or T4)

Procedure: **OPERATE SYNCHRONIZATION SWITCH (T0 OR T4)**

1. Select **T0** or **T4SwitchCommand** and set to desired value



2. Click T0 or T4SwitchSource and select new synchronization source.
   (One of the synchronization source candidates).



3. Click **Save** to commit the changes.

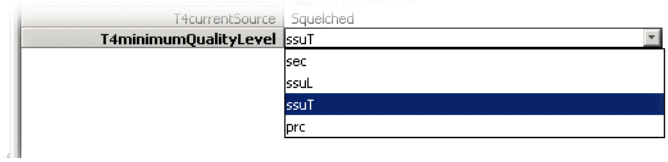
If the switch parameters are valid, the switch is performed. If a Manual or Forced switch is performed, the selected source will remain selected until a new Forced, Manual or Clear command is sent.

7.6.9 View Synchronization Switch (T0 or T4))

Access the synchronization attributes from the Management Tree.

The attributes for the synchronization switch are presented:

Quality Level Minimum (T4 Only)

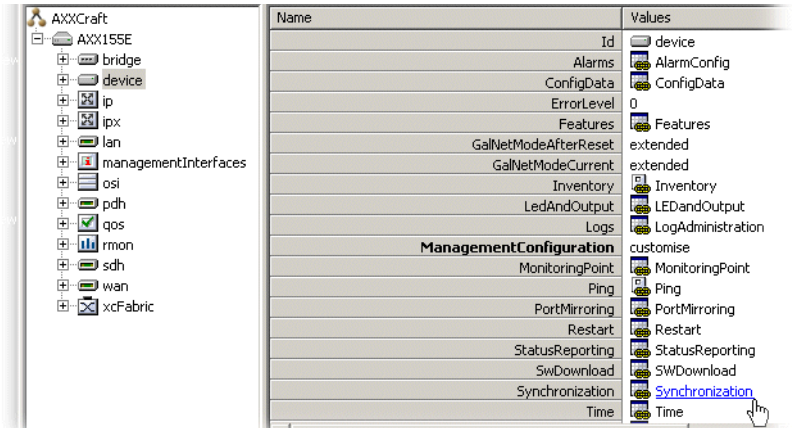


·Manual, Forced or Automatic selection Mode

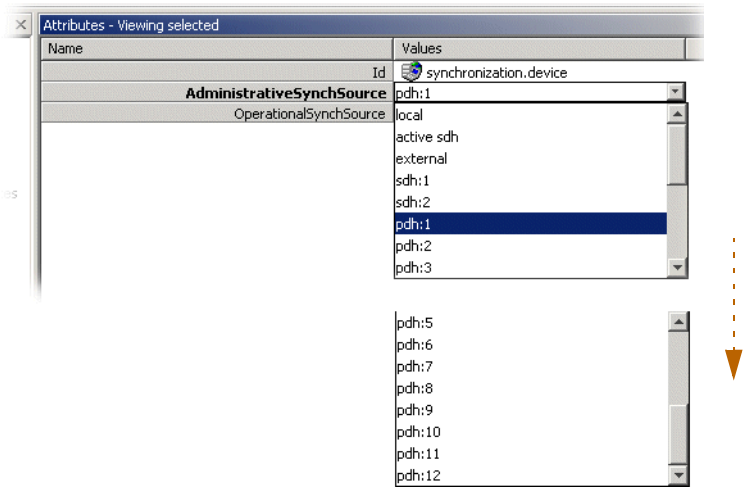
7.6.10 Operate Synchronization on AXX155E

Procedure: **AXX155E SYNCHRONIZATION.**

1. Select **device** > **Synchronization**.



2. Select **AdministrativeSynchSource** from pulldown menu.



3. Click **Save** to activate the selected synchronization source.

7.7 Alarm and Event configuration

7.7.1 Introduction

The purpose of this section is to guide you through the configuration of alarm and event reporting, and to be able to suppress and configure specific alarms.

The network element has a predefined set of combinations of managed objects and alarm types, i.e., alarm points. These combinations can not be changed by you but the severity level and a description can be defined.

Suppression of specific alarms is important to avoid alarm floods in the network and to focus on the root cause. AXX 9200 EDGE let you suppress a number of different alarm types, e.g. AIS.

In some situation you might want to suppress alarms that are kind of oscillating between being active and not active. A time interval, a persistency filter, indicates the time period an alarm must have been on or off before being reported. The persistency filters are defined for a group of alarms of a specific type.

There are three possible persistency group categories:

- High order level alarms
- Low order level alarms
- Unfiltered alarms

For some managed objects you can enable or disable the alarm reporting.

7.7.2 Event Forwarding

No alarms or events can be reported before the identity of the receiver of alarms and events has been configured. It is possible to forward alarms and events to more than one receiver.

Event forwarding is enabled when a new user is added with the TrapsEnable attribute set to TrapsEnable as described in 5.3.3.

7.7.3 Configure General Alarm Reporting

In AXX 9200 EDGE there are several levels where alarm reporting can be disabled or enabled. Alarms will be reported to a manager only when alarm reporting is enabled on all levels (See Figure 78) In addition the Event forwarding must be configured for the Managers IP address as described above.

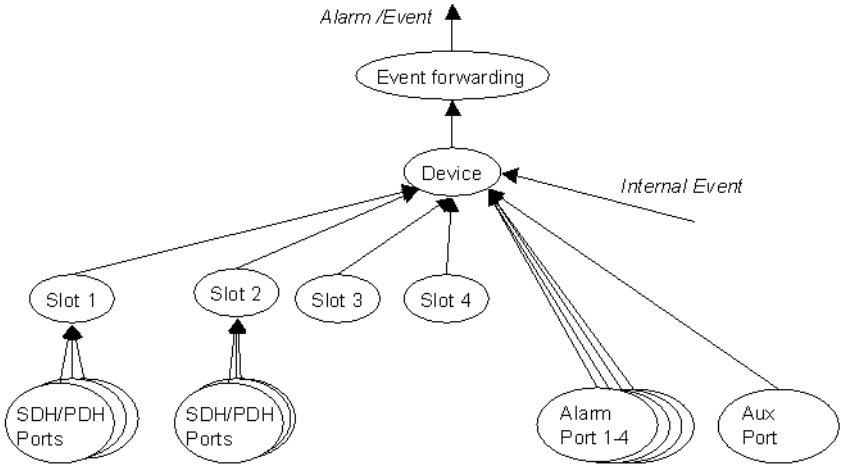


Figure 78 General Alarm Reporting filters.

Note that all alarms from objects below, including itself have to pass through the filter.

In addition to general alarm reporting, it is possible to filter specific alarm types on specific object instances.

Device Alarm Enabling

It is possible to enable or disable alarm and event reporting from AXX 9200 EDGE. In the disabled state, no alarms or events are reported (Some generic events, like cold start, etc. are still reported).

1. Select device > AlarmConfig > **AlarmReporting**.
2. Set **AlarmReporting** to **enabled** or **disabled**.

Slot Alarm Enabling

1. Select the **slot** that should report alarms
2. Set **AlarmReporting** to **enabled**.

Traffic Port Alarm Enabling

1. Select the **SDH** or **PDH** port that should report alarms.
2. Set A**dminStatus** to **enabled**.

Alarm Port Alarm Enabling

1. Select the **Alarm port** that should report alarms.
2. Set **AdminStatus** to **enabled** or **disabled**.

Aux Port Alarm Enabling

1. Select the **Aux port** that should report alarms.
2. Set **AdminStatus** to **enabled**.

NOTE! Slot and port alarm reporting is by default disabled when the slot is configured for a new expected module.

7.7.4 Suppress Specific Alarms

In addition to configuration of the general alarm filters described above, it is possible to suppress specific alarm types to avoid alarm floods in the network. Other alarms from the same objects will be reported independently of these settings.

Suppress RDI, EXC, DEG, SSF alarms

RDI, EXC, DEG, SSF alarm reporting can be suppressed from the VC-12, VC-3 or VC-4 layers.

1. Select device > AlarmConfig > **AlarmReportingVc**.
2. Set **suppress** for the **attributes** corresponding to the **Alarms** that should be suppressed:
   - RdiAlarms

- ExcAlarms
- DegAlarms
- SsfAlarms

Suppress AIS alarms from SDH ports

AIS alarm reporting can be suppressed from the TU12, TU3 or AU-4 layers.

1. Select device > AlarmConfig > **AlarmReportingVc**.
2. Set **suppress** for the **AisAlarms** attribute.

Suppress AIS alarms from E1 and E3 ports

1. Select device > AlarmConfig > **AlarmReportingE1E3**.
2. Set **AisAlarms** to **suppress**.

Suppress AIS alarms from AUX port

1. Select device > AlarmConfig > **AlarmReportingAux**.
2. Set **AisAlarms** to **suppress**.

7.7.5 Modify Alarm severity and description

It is possible to modify the severity of the reported alarms from AXX 9200 EDGE.

1. Select device > AlarmConfig > **AlarmPointConfig**.

2. Set the **Severity level** and **Description** for the combination of alarm type and object type of your choice. The next time the alarm is reported from this object type it will come up with the configured Severity and Description in the Notification List.

7.7.6 Set Signal Degrade Threshold

The threshold for a DEG alarm to be reported (and used for MSP switching) can be set for the VC-12, VC-3, VC-4, MS and RS layers.

1. Select device > AlarmConfig > **SdTreshold**.
2. Set **SdThreshold** to a value between **-6 and -9** (BER= 10E-6 to 10E-9).

7.7.7 Modify Alarm Persistency

Alarm reporting on and off can be delayed by setting the Alarm Persistency filters in AXX 9200 EDGE.

The alarms are divided into groups according to their importance for fault management.

Persistency Group 1 (highOrderLevel)

Table 11 Persistency Group1

Associated alarm types	**Object classes associated with each alarm type**
LOS	SdhPort, pdhPort
LOF	rs
AIS	ms
EXC	rs, ms
DEG	rs, ms
TIM	rs
RDI	ms
CDF	rs, ms
AUX	auxPort

Persistency Group 2 (unfiltered)

Table 12 Persistency Group 2

Associated alarm types	Object classes associated with each alarm type
LOP	tu4, TU3, TU12
LOM	vc4
LOF-RX, LOF-TX	e1

Persistency Group 3 (lowOrderLevel)

Table 13 Persistency Group 3

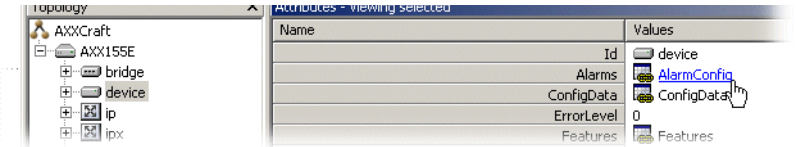
Associated alarm types	Object classes associated with each alarm type
AIS	tu4, tu3, TU12, e1, e3
EXC	vc4, vc3, vc12
DEG	vc4, vc3, vc12
SSF	vc3, vc12
TIM	vc4, vc3, vc12
RDI	vc4, vc3, vc12
UNEQ	vc4, vc3, vc12
PLM	vc4, vc3, vc12

1. Select device > AlarmConfig > **AlarmPersistency**.
2. Set **onFilter** or **offFilter** to a value between **0 and 30 seconds**.

7.7.8 Modify AXX155E Alarm Configuration attributes

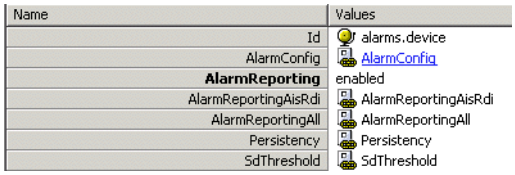
Location of Alarm Configuration attributes

1. Select device > **AlarmConfig**



Modify Alarm severity and description

1. Select device > AlarmConfig > **AlarmConfig**.

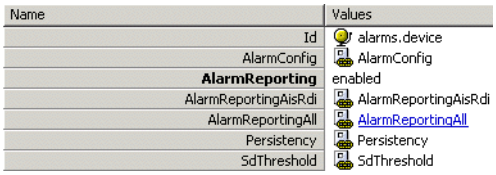


2. Set the **Severity level** and **Description** for the combination of alarm type and object type of your choice.

3. Click **Save**. The next time the alarm is reported from this object type it will come up with the configured Severity and Description in the Notification List.

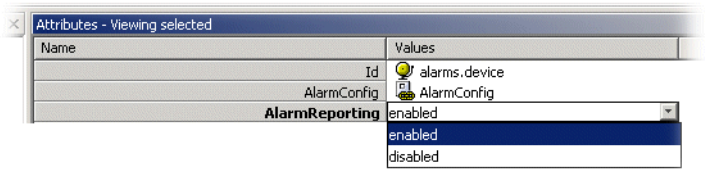
View all alarm reporting instances

1. Select **AlarmReportingAll** to view all alarm reporting instances.



Enable Alarm reporting

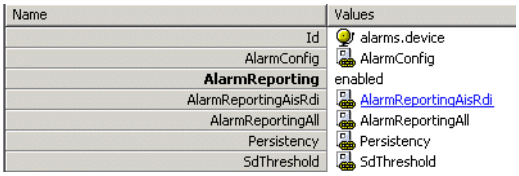
1. Set **AlarmReporting** to **enable** using the available pull-down menu.



2. Click **Save**.

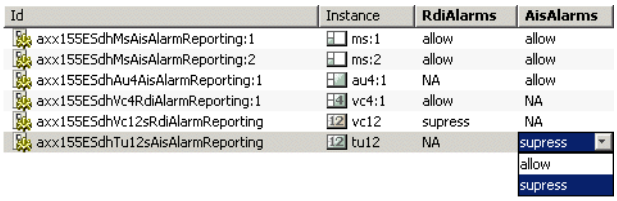
Procedure: **MODIFY AIS RDI ALARM REPORTING**

1. Select **AlarmreportingAisRdi**.



2. Select desired **instance.**

3. Select **allow** or **supress** for **Ais** alarm.

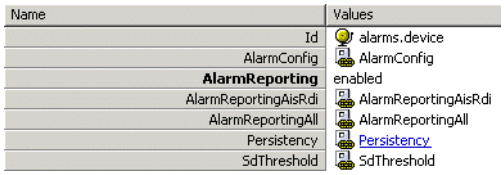


4. Repeat for **Rdi** alarm.

5. Click **Save**.

Procedure: **MODIFY ALARM PERSISTENCY**

Alarm reporting on and off can be delayed by setting the Alarm Persistency filters in AXX155E.



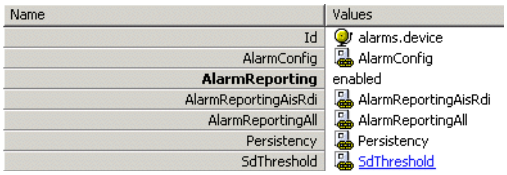
1. Select device > AlarmConfig > **AlarmPersistency**.

2. Set **onFilter** or **offFilter** to a value between **0 and 255 seconds**.

3. Click **Save** when desired value settings are completed.

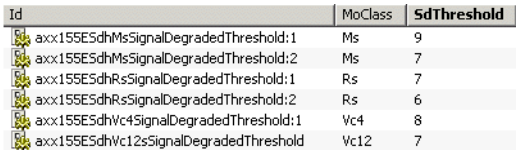
Procedure: **MODIFY SIGNAL DEGRADED (SD) THRESHOLD**

1. Select SdTreshold



2. Select desired MO class

3. Set **SdTreshold** to a value between 6 and 9.



4. Click Save.

7.8 AXX 9300 METRO Shelf Management

7.8.1 Overview

NOTE! AXX 9300 METRO differs from the other Ericsson AXXESSIT network elements with plug-in modules. AXX 9300 METRO requires configuration of expected module modes, not expected module types. This is because the same module type can support different communication modes.

7.8.2 View the current shelf configuration

Select an AXX 9300 METRO network element in the AXX 9840 INSITE GUI

The AXX 9840 INSITE reads the current slot configuration from the targeted network element and presents it in the Management Tree as you can see in the figure below.

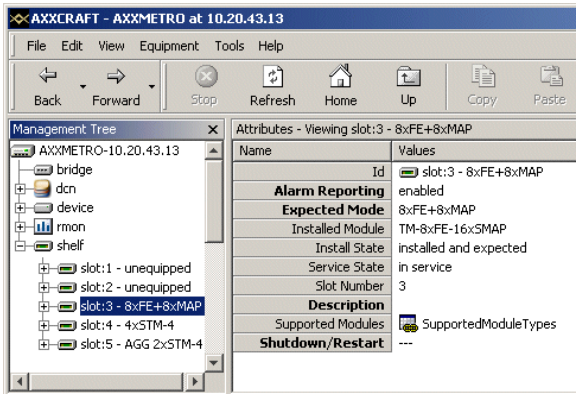


Figure 79 Shelf configuration

The AXX 9840 INSITE presents

- The expected module modes and install status per slot
- The current module types
- The current expected interface modules and install status per slot
- Equipment protection configuration

7.8.3 Configure the shelf slots

The AXX 9840 INSITE system describes the slot configuration by two attributes: the expected module mode and the current install state. The range of modes supported by a slot is dependant of the number of module types supported by the slot, and this varies from slot to slot, as illustrated below.

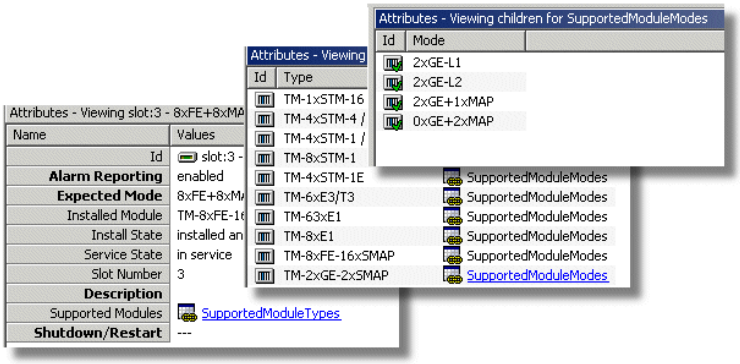


Figure 80 Supported modules and their modes per slot

One module type may support several modes, as shown in the examples below:

- SDH example: A TM-4STM4/1xSTM16-SFP tributary module supports two modes: 4xSTM4 and 1xSTM16.
- Fast Ethernet example: A TM-8xFE+16xSMAP-SFP module support three modes: 8xFE+8xMAP, 2xFE+14xMAP, 0xFE+16xMAP.

One module mode can be supported by several module types, as shown in the example below:

- STM-16 modes are supported by both the TM-1xSTM16-SFP module and the TM-4xSTM4/1xSTM16-SFP module.

Procedure: **CONFIGURE SHELF SLOTS**

1. Specify the mode of the expected or present module.
   You can do this even if the module isn't yet physically present in the slot.
   If the current module type does not support the selected mode, it will be reflected in the InstallState attribute (mode not installedAndExpected).
2. Select Expected modes from a list of available modes presented by the AXX 9840 INSITE. The list varies per slot, depending on the module types supported by the slot.
3. If equipment protection is defined for a module, the list of allowed modes in the protecting slot automatically follows the working slot. No user selections are allowed.
4. If a tributary mode selection implies that a connector module is required (electrical interface ports), the AXX 9840 INSITE / AXX 9820 CRAFT automatically specifies the valid connector module Expected Mode.

NOTE! The 8xFE module can be provisioned by both electrical ports and optical port interface modules. There is no automatic provisioning of FE connector module expected type until port provisioning is performed, see “Configure ports” on page 362

READ MORE: “Restrictions on equipping modules with interface modules” on page 372.

READ MORE: “Connector module assignment” on page 374 for details about tributary module and their required connectors.

7.8.4 Configure ports

Some AXX 9300 METRO traffic modules are equipped with exchangeable port interface modules. (SFP) These modules will change the optical properties of the port.

Procedure: **CONFIGURE PORTS**

1. Select slot/module
2. If the slot has defined an expected module, the AXX 9840 INSITE presents the configuration of each port. If the module supports interface modules, the AXX 9840 INSITE displays the current install port interface settings (installed module, installed vs. actual status) of each port.
3. Set the expected interface module type (expected port interface) for each port, and the network element reverts with updated port interface settings.
4. **8xFE module only** - the module supports selectable electrical or optical interface per port. If an electrical interface is selected, the interface module install state properties are irrelevant, and the port requires a connector module to be installed:
   - If one or more electrical interface ports are provisioned, the AXX 9840 INSITE automatically defines an expected connector module in the corresponding connector slot.
   - If no electrical interface ports are provisioned, and there exists an existing connector module, the AXX 9840 INSITE changes the corresponding module connector slot expected module to 'none'.
5. If required, define interface port attributes:

- CWDM/DWDM type interface modules

- Wavelength (nanometer)

- Range (kilometers)

7.8.5 Manage tributary module equipment protection

To configure equipment protection, you use the "EquipmentProtectionGroup" object in the AXX 9300 METRO.

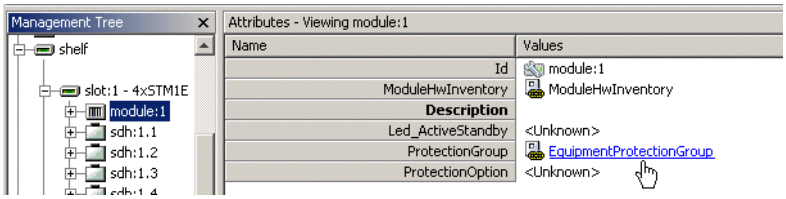


Figure 81 EquipmentProtectionGroup

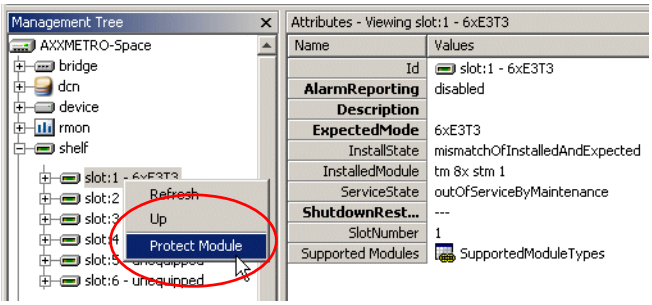
All relevant protection statistics and configuration attributes are associated to that object.

NOTE! This procedure is only relevant for E1, E3 and STM-1E tributary modules. Equipment protection on aggregate modules is handled separately.

Procedure: **CONFIGURE EQUIPMENT PROTECTION MODULE PAIR**

When you establish a new equipment protection group, all configuration operations are performed on the working slot/module and the protecting slot/module becomes unavailable for editing. The odd numbered slot is the working slot, and the even numbered is the protecting slot.

1. Right-click the working tributary slot and select “**Protect Module**” to establish equipment protection.



2. The AXX 9840 INSITE validates the request and responds according to the mutually exclusive alternatives below:

- If the expected mode can be supported by equipment protection, the AXX 9840 INSITE allows this as a legal choice.
- If the slot targeted as protecting contains another module type/mode, the AXX 9840 INSITE performs additional validation:
- The AXX 9840 INSITE does not allow protection configuration if the targeted protecting slot contains a module where the ports are carrying user traffic (the ports are carrying cross connected traffic).

You are requested to remove all cross connections, and the flow terminates.

- If the module is not used for existing traffic, the AXX 9840 INSITE requests a confirmation before continuing the flow.
- The AXX 9840 INSITE automatically configures the protecting slot expected mode. The protecting module attributes become unavailable for modification.

3. The AXX 9840 INSITE presents the protection group attributes with default configuration attributes, and you can do one of the following:

- If expected and installed module type match, you accept the default values, and the AXX 9840 INSITE configures the network element.
- If expected and installed module type don’t match, you can accept the default values and the AXX 9840 INSITE stores the configuration values until compatible modules are installed in the network element.
- Continue to the "Edit Equipment Protection" sub-flow to configure the protection group.

7.8.5.1 Edit Equipment Protection

Equipment protection is non-revertive, and no attributes are available for modification.

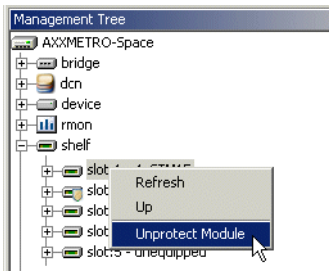
This means that if a fault occurs and the system switches the protecting module to working, it will stay in that state until you manually switch it back or AXX 9840 INSITE performs a new protection switch.

The AXX 9840 INSITE presents the current protection attributes:

- Which module (working or protecting) is currently active
- Status parameters of the protection group (ref. information model).

7.8.5.2 Remove Equipment Protection

1. Right click the working slot and select Unprotect Module.



2. The AXX 9840 INSITE de-commissions equipment protection and the protecting slot/module becomes available for configuration

3. The AXX 9840 INSITE performs the following "clean-up" activities, if required.

- Automatically change the corresponding "expected connector module" attributes, if required.
- Issue warnings to the user in the following cases:

  - If the module in the previously protecting slot becomes illegal in its current location (e.g. E1 module in an even-numbered slot).

  - If a new connector module is required (e.g. E3 modules that uses different connector modules for protected and un-protected set-ups)

7.8.6 Automatic configuration of connector modules

Whenever a tributary module is modified or equipment protection established or removed, the AXX 9840 INSITE checks if it is required to modify the associated connector module expected type. This may be the case when:

- The new module type requires another connector module type or no connector modules
- For E3 modules, which use different connector modules in un-protected and protected modes
- For E1 modules, which use no connector modules in even-numbered slots in an equipment configuration mode.
- For the 8xFE module, configuration of expected connector modules depends on whether electrical interfaces was defined for the module during port configuration. One or more electrical FE interface requires a connector module.

7.9 Alternative procedures

7.9.1 Operating on equipment protection groups

You may select a protection group and perform the following operations on the group:

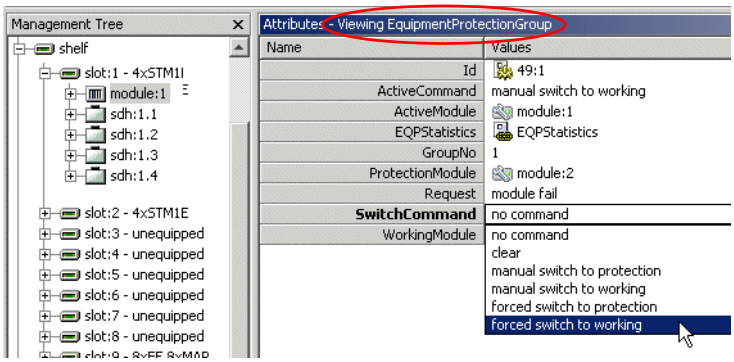


Figure 82 Protection Switch Command

- Manual protection switch to working or protecting.
  The switch is performed if the targeted module is operative, and prohibited if the targeted module is not

- Forced protection switch to working or protecting.
  The switch is performed regardless of the operative state of the targeted working/protecting module
- Lockout protection enabled/cleared: When enabled, automatic protection switching is disabled, and the currently active module stays active regardless of fulfilled switching criteria. When cleared, automatic switching is enabled. reviewthis

The AXX 9840 INSITE notifies you in the following cases:

- When a manual protection switch command is issued, and the targeted module is not operative, a warning is issued.
- When a forced switch command is issued, and the targeted module is not operative, the AXX 9840 INSITE requests a confirmation.

7.9.2 Aggregate Module Equipment Protection

An aggregate module has equipment protection on the System controller, SDH cross connection and Ethernet crossbar. The management port on AM is the Craft management port. Only the CRAFT Management Port on ACTIVE can be used to manage the AXX 9300 METRO. The SDH port is like an other SDH port. MSP protection group with the other AM. SNCP with any port.

The network element does not associate "working" and "protecting" with any specific slot, but implements equipment protection in a "warm standby" configuration:

- When two compatible aggregate modules are installed, the network element automatically configures them in a protection group.
- The first of the aggregate modules that reach normal state will be the ACTIVE module. The second will be in state WARM STANDBY.
- You may at any time attempt to force the state of an active aggregate module to standby, and a switchover will take place if the other module is operative after a switchover (due to an error or command) the AM module will not automatically switch back.
- The network element will automatically perform a switchover when the switching criteria are fulfilled.

7.9.3 Pre-provisioned modules/modes are installed and automatically configured.

Pre-provisioning occurs when slot modes are pre-configured, and the physical modules are not installed in the network element slots.

Flow:

1. The network element registers that a new module is installed in the slot, and validates it according to the expected mode:

- If the installed module supports the expected mode, the module is configured according to the expected mode.
- If the module mode of the module is not according to the current network release, the network element automatically updates the module firmware to suit the new module mode. A notification is sent to the AXX 9840 INSITE.
- If the installed module does not support the expected mode, the network element issues a warning to the AXX 9840 INSITE.
- If the installed and expected interface module deviates for any port, the network element issues a notification to the AXX 9840 INSITE. Link state of the non-confirming port is "down".

2. The AXX 9840 INSITE updates the status in all presented views (Management Tree, NE maps, notification lists etc.).

3. If a protecting module is inserted, and supports the expected mode, the network element automatically configures the protecting module according to the predefined parameters. A slot may be used as a protected group or as a new module.

4. The AXX 9840 INSITE evaluates the network element, and notifies the user:

- As an event,
  if the configuration is performed successfully.
- As a warning,
  if the configuration of the tributary modules are performed successfully, but there is a connector mismatch.
- As an error,
  if the configuration fails.

7.10 More about AXX 9300 METRO modules

7.10.1 Module ports and interface modules

AXX 9300 METRO uses plug-in interface modules on many traffic module ports to implement the physical properties of optical port interfaces. The interface modules are installed per port, and supports the SFP (small form-factor pluggable) standard. Electrical interfaces are located on connector modules.

Interface module types are specific for optical properties and port bit rate. The different types are defined by the Port Interface data type:

- Short-haul SDH interface modules (LED based)
- Long-haul SDH interface modules (laser based)
- DWDM (dense wavelength division multiplexing)
- CWDM (coarse wavelength division multiplexing)

The type of module port interface is decided during module provisioning by specifying the "Expected Port Interface" attribute. For modules supporting mixed electrical and optical port configurations, this attributes value range will include both electrical and optical settings.

Each traffic module type has a specific range of legal interface module types, which will be a sub-set of the Information Model "Port_Interface" data type.

7.10.2 Equipment Protection switching strategies

Equipment protection switching occurs in two situations:

1. When a module fails, the system automatically switches to the backup module in accordance with the strategies defined for the working/protecting module combo.
2. In case a module shall be removed, replaced or upgraded, you can force a protection switch to the other module to avoid a disruption of the functions/services supported by the module pair.

7.10.2.1 Tributary modules

The tributary module contains traffic interfaces - SDH, LAN or PDH. An AXX 9300 METRO unit may or may not be equipped with tributary modules.

Tributary modules with optical interfaces have the connector located at the front of the module. Tributary modules with electrical interfaces have their associated connectors located in connector module slots.

The tributary module variants are:

- TM-1xSTM-16 SFP: One SDH STM-16 interface. Plug-in SFP modules control the optical properties of the interface.
- TM-4xSTM4/1xSTM16-SFP: Four STM-4 optical interfaces or one STM-16 optical interface. Plug-in SFP modules decide the optical properties of the interface.
- TM-4xSTM1/1xSTM4-SFP: Four STM-1 optical interfaces or one STM-4 optical interface. Plug-in SFP modules decide the optical properties of the interface.
- TM-8xSTM1-SFP: Eight optical STM-1 optical interfaces. Plug-in SFP modules decide the optical properties of the interface
- TM-4xSTM1E. Four electrical STM-1 interfaces. This module requires a complementary connector module.
- TM-6xE3/T3: Six PDH interfaces of type E3 or T3 (34,368 Mbps or 44,736 Mbps). The module contains electrical interfaces and must be supported by a complementary connector module.
- TM-63xE1: 63 PDH interfaces of type E1 (2.048 Mbps). The module contains electrical interfaces and must be supported by a complementary connector module. This module may use an additional remote unit to connect to other equipment.
- TM-8xE1: Eight PDH interfaces of type E1 (2.048 Mbps). The module contains electrical interfaces and must be supported by a complementary connector module.
- TM-8xFE-16xMAP-SFP: Eight Fast Ethernet interfaces - electrical or optical - and 16 WAN-to-SDH mappers. Plug-in SFP modules control the optical properties. If electrical interfaces are used, a complementary connector module must support the module.
- TM-2xGE-2xMAP-SFP: Two Gigabit Ethernet interfaces - optical or electrical - and two WAN-to-SDH mappers. Plug-in SFP modules control the optical properties.

7.10.2.2 Miscellaneous module MM-1

The miscellaneous module contains "device" interfaces such as Management Port, AUX ports, Alarm Inputs etc. An operative AXX 9300 METRO unit must be equipped with at least one miscellaneous module.

The miscellaneous module type of AXX 9300 METRO is:

- MM-3xRJ45+DSUB25+DSUB3. The module supports the following interfaces: SDH synchronization interface, Auxiliary interface, Management interface and alarm interface, as well as LED indicators for system status display

7.10.2.3 Connector modules

Contains connectors for tributary modules with electrical interfaces. The AXX 9300 METRO backpane connects the tributary modules and the connector modules

The AXX 9300 METRO supports the following connector modules:

- CM-FEx8xRJ45: Contains electrical interfaces for up to eight Fast Ethernet ports, and supports one un-protected tributary module.
- CM-6x1.0/2.3: Contains electrical interfaces for up to six E3, T3 interfaces. Supports one un-protected tributary module
- CM-PROT-6x1.0/2.3: Contains electrical interfaces for up to twelve E3, T3 interfaces. The module supports tributary modules in an equipment protection configuration, and interfaces up to six E3/T3 ports.
- CM-2xLFH: Contains two LFH connectors for up to 63 E1 electrical interfaces (1x32 + 1x31)
- CM-4x1.0/2.3: Contains four 1.0/2.3 Coaxial connectors for STM-1e interfaces
- CM-PROT-4x1.0/2.3 - Coaxial connectors for STM-1e interfaces and Protection switch

7.10.2.4 Fan Module:

Fan modules provide forced ventilation for the AXX 9300 METRO. Each fan module contains 6 fans.

7.10.2.5 Remote Units:

The remote units are passive patch panels for electrical interfaces. The module variants are:

- 32xE1-LFH-RJ45: 120 ohm patch panel for up to 32 electrical E1 interfaces.
- 32xE1-LFH-1.0/2.3: 75 ohm patch panel for up to 32 electrical E1 interfaces.

There are no TMN requirements for management of passive remote units.

7.10.3 Restrictions on equipping slots with modules

There are some restrictions to slot equipping in the AXX 9300 METRO:

- If the AXX 9300 METRO is configured for equipment protection, adjacent slots must be used, with the odd-numbered slot for the working module and the even-numbered for the protecting module.
- If two modules of the same type are located in adjacent slots it is not implicit that they are in an equipment protection configuration. Adjacent equal type/mode slots may be operating in un-protected mode.
- There are no restrictions on which of the aggregate module slots an un-protected aggregate module is inserted (even or odd slot).

NOTE! Connector modules supporting E3/T3/STM-1E equipment protection consume two slots.

7.10.4 Restrictions on equipping modules with interface modules

The following table describes which module types use interface modules, and what types are allowed per module and/or module mode.

Module type	Interface Mode	SFP	Comment
AM-1xSTM16-SFP	S-16.1 Short haul L-16.1 Medium haul L-16.2 Long haul "L-16.2C"CWDM None	x x x x	- Optical - Optical - Optical - Optical
TM-1xSTM16-SFP	S-16.1 Short haul L-16.1 Medium haul L-16.2 Long haul "L-16.2C" CWDM None	x x x x	- Optical - Optical - Optical - Optical
TM-4xSTM1/1xSTM4-SFP			**STM-1 mode**
	S-1.1 Short haul L-1.1 Medium haul L-1.2 Long haul "L-1.2C" CWDM STM-1e electrical None	x x x x x	- Optical - Optical - Optical - Optical - Electrical
			STM-4 mode
	S-4.1 Short haul L-4.1 Medium haul L-4.2 Long haul "L-4.2C" CWDM None	x x x x	- Optical - Optical - Optical - Optical
TM-4xSTM4/1xSTM16-SFP			**STM-4 mode**
	S-4.1 Short haul L-4.1 Medium haul L-4.2 Long haul "L-4.2C" CWDM None	x x x x	- Optical - Optical - Optical - Optical
			STM-16 mode
	S-16.1 Short haul L-16.1 Medium haul L-16.2 Long haul "L-16.2C" CWDM None	x x x x	- Optical - Optical - Optical - Optical -
TM-8xSTM1-SFP	S-1.1 Short haul L-1.1 Medium haul L-1.2 Long haul "L-1.2C" CWDM STM-1e electrical None	x x x x x	- Optical - Optical - Optical - Optical - Optical

Module type	Interface Mode	SFP	Comment
TM-4xSTM1E	NA	-	Connector module, electrical IF
TM-6xE3/T3	NA	-	Connector module, electrical IF
TM-63xE1	NA	-	Connector module, electrical IF
TM-8xE1	NA	-	Connector module, electrical IF
TM-8xFE-16xMAP-SFP	100 Base TX 100 Base FX 100 Base LX10" 100 Base ZX" None	x x x - 	Selectable optical interface Module or connector module Electrical interface.
TM-2xGE-2xMAP-SFP	1000 Base TX 1000 Base SX 1000 Base LX10" 1000 Base ZX" GE-CWDM None	x x x x x 	-Electrical -Optical -Optical -Optical long distance -Optical
MM-1		-	Connector module, electrical IF

Note:

- "L-1.2C" = Optical, brackets indicate similar performance to an L1.2C, but not fully according to standard
- "Base ZX" = Optical, brackets indicate similar performance a Base ZX, but not fully according to standard

7.10.5 Connector module assignment

There is a fixed relationship between traffic module slot number and connector module slot number, with some exception due to equipment protection configurations:

7.10.5.1 Un-protected modules

Connector slots have a one-to-one relationship with corresponding traffic slot modules, as described in the table below:

Traffic slot no	Connector slot no
1	12
2	13
3	14
4	15
7	16
8	17
9	18
10	19

7.10.5.2 Protected modules

E1, E3 and Stm-1E modules in an equipment protection configuration have a complex relationship depending on the type of module. The table below shows the relationship:

Protected module	Traffic slot no	Connector slot no
E1 modules	1 and 2	12 (slot 13 un-equipped)
	3 and 4	14 (slot 15 un-equipped)
	7 and 8	16 (slot 17 un-equipped)
	9 and 10	18 (slot 19 un-equipped)
E3, T3 and STM-1E	1 and 2	Slot 12/13 combined
	3 and 4	Slot 14/15 combined
	7 and 8	Slot 16/17 combined
	9 and 10	Slot 18/19 combined

Combined slots means that a double-width connector module is used.

7.10.6 Equipment protection in AXX 9300 METRO

AXX 9300 METRO offers optional 1:1 equipment protection on selected tributary modules, warm standby functionality on parts of the aggregate module functionality to ensure resilience against equipment failure.

Connector modules are not equipment protected.

The AXX 9300 METRO back pane is not equipment protected.

It is not possible to equipment protect tributary modules with optical interfaces. Protection similar to equipment protection for modules with optical interfaces is done by using MSP protection. Note that in this case it is the SDH links that are protected, not the equipment.

The aggregate module controls the switching between main and protecting modules. In a protected aggregate module configuration, the switching is controlled by the active (main or protecting) module.

The user can override the automatic switching and force a manual switch from the AXX 9840 INSITE.The protected modules are constantly monitoring their status, and automated switching is performed, based on a pre-defined set of rules.

7.11 Manage slots on AXX 9200 EDGE

7.11.1 Introduction

A slot represents a physical position on the network element where different HW modules can be located, seeFigure 83 The purpose of this section is to describe the tasks and dynamic involved in inserting modules into and removing modules from a slot.

This section also involves presentation and modification of slots. Slots are static and cannot be created or deleted.

Please see the AXXEGDE Technical Reference for details on the different traffic modules available.

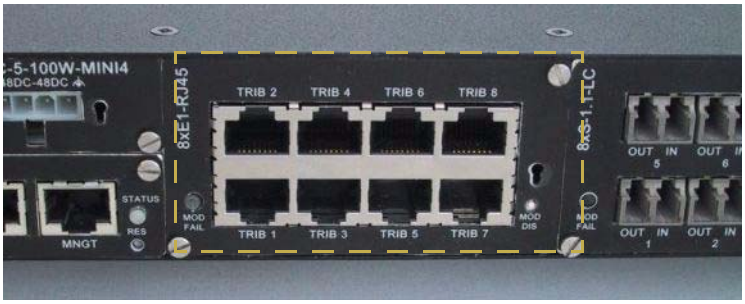
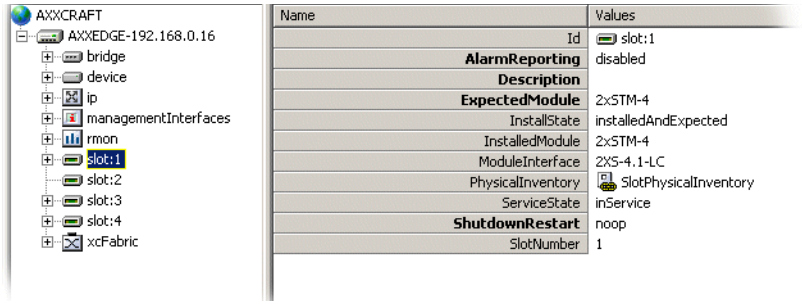


Figure 83 Slot on the network element

7.11.2 View Slot

1. Select a slot in the Management Tree.
2. The browser presents four slots numbered from 1 to 4. The slot attributes as defined in the information model are available in the attribute window. Each slot can be equipped with one HW module. By default the slot is unequipped.



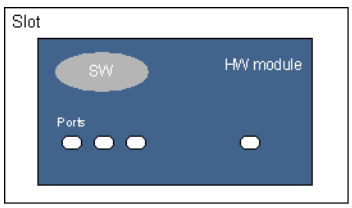


Figure 84 Slot - module - port concept

A slot can be empty or have a HW module with a given number of ports and SW version installed as illustrated in Figure 84 . The physical inventory data for the module, if module present in slot, is also presented in the attribute window.

You can configure the slot and set the expected module type for the slot. The module does not have to be physically inserted. The slot has therefore an attribute that reflects the relation between the expected module and the installed module, i.e. the **slot state**:

- Empty
- Installed and expected
- Expected and not installed
- Installed and not expected
- Mismatch of installed and expected
- Unavailable
- Unknown

A state diagram for the possible transitions of a slot is shown in Figure 85 . This is the suggested state machine from *TMF 814 supporting documentation, equipmentStates.pdf.*

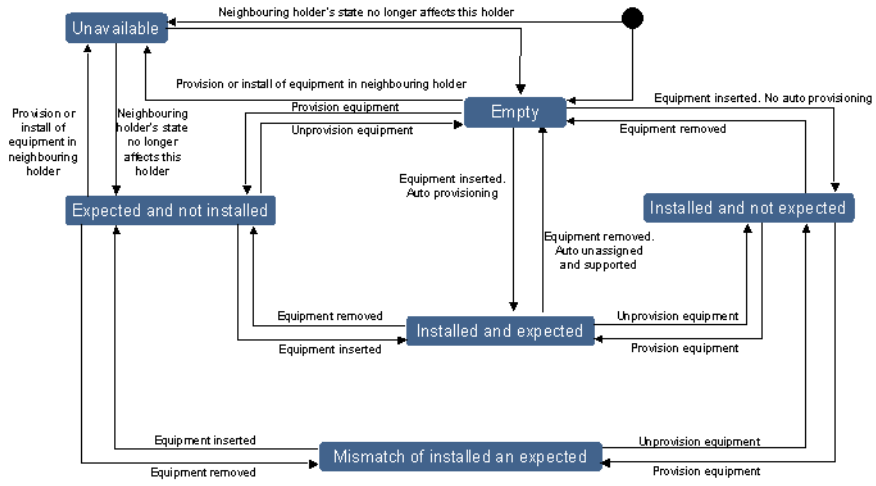


Figure 85 Relation between installed and expected module in a slot.

A State machine for the values of the attribute describing the relation between installed and expected module in a slot is shown in Figure 85

If a mismatch between the two modules occurs an alarm will be generated. The alarm is cleared if the module is replaced or the expected module is changed, i.e., a match between expected and installed.

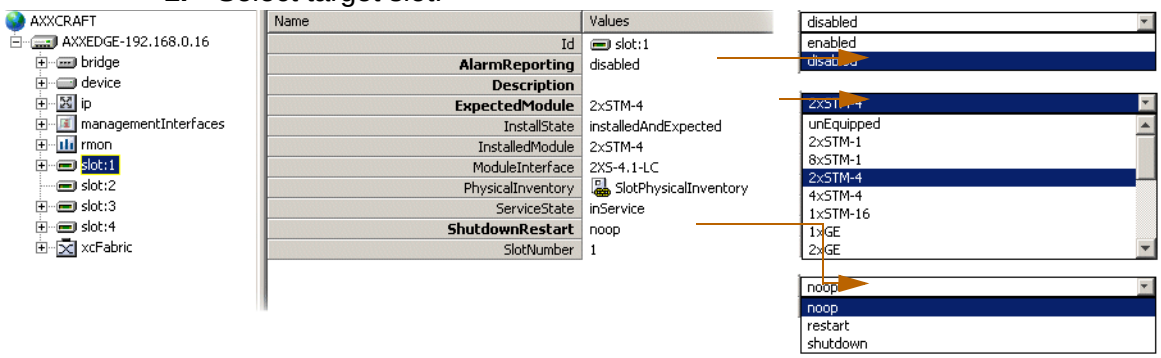
You can configure an expected module and assign it to a slot without any physical module present. The system populates the Management Tree according to the specified expected module. Before replacing a module, i.e., selecting a new expected module type, the expected module of the slot must be set to unequipped.

For management of different ports, see “Traffic Port management”.

7.11.3 Modify Slot

To modify the expected module attribute the ports of the previous expected module must be unused and unstructured.

1. Select target slot.



2. The following attributes are modifiable:

AlarmReporting: enable or disable.

ExpectedModule: select module of current interest.

ShutdownRestart: noop, restart or shutdown.

NOTE! Module Interface shows physical interface on selected module. Thus this attribute value indicates LongHaul(ex. 2xL-4.2-LC), ShortHaul(ex. 2xS-4.1-LC) for STM only. Connector is also indicated.

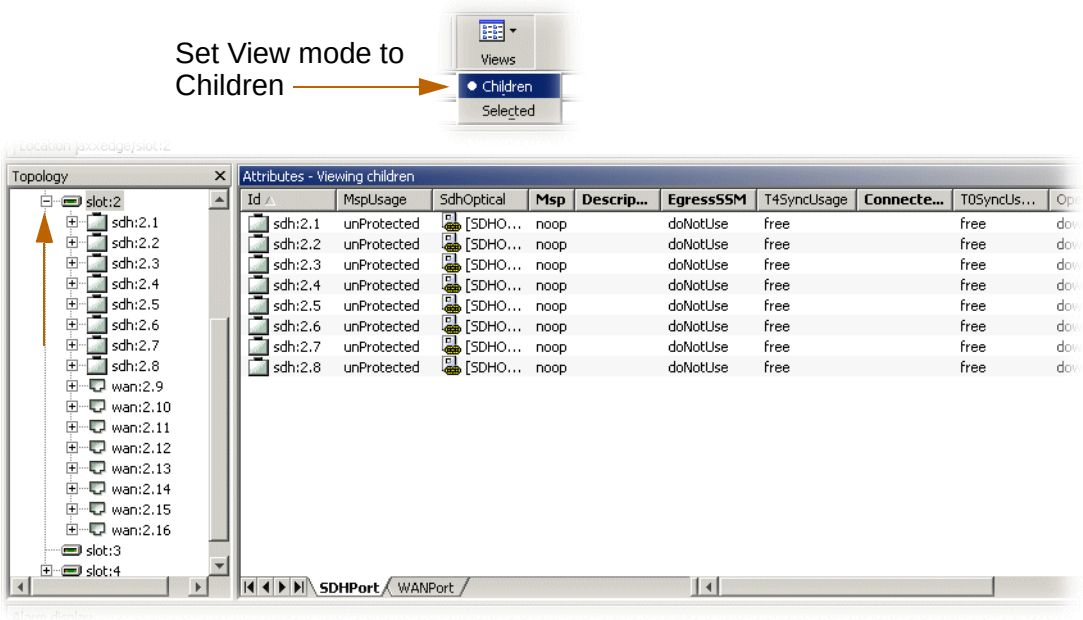
3. Modify the modifiable slot attributes.

4. Click **Save** to activate the modifications.

For some of the changes to take effect a restart of the module is required. In these cases you are prompted to restart. See “” on page 331.

5. When a slot has been configured to contain a specific module, the ports of the module are automatically created in the network element. The type of ports created depends on the module type configured for the slot.

Set View mode to Children



The ports of an installed module were not created if the slot was configured to contain another module type or being empty.

7.11.4 Troubleshooting and FAQ

7.11.4.1 Troubleshooting

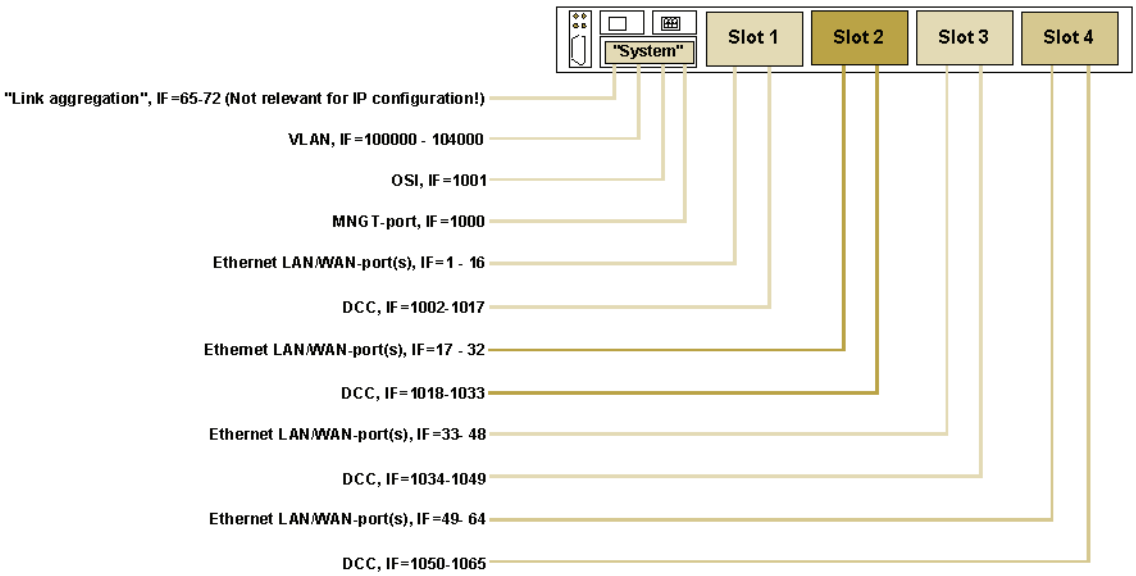
I cannot configure the Slot for another module type.

When the Slot Expected Module attribute is set to a specific module type, the Managed Objects for the expected module type are created in AXX 9200 EDGE. Likewise, when the Expected Module is already set to a module type and we want to configure the Slot for a different module type, the Managed Objects for the configured module will be deleted before the Managed Objects for the new module type can be created.

In order to avoid unintentional traffic breaks, AXX 9200 EDGE checks whether the existing configured module is involved in cross-connections, carrying management traffic or is used for synchronization purposes.

7.11.4.2 AXX 9200 EDGE Physical Interface Indices

The IF-indices for physical/logical ports on the AXX 9200 EDGE are as follows:



8 Traffic Port management

8.1 Introduction

This chapter describes traffic port configuration, organized as follows:

- Traffic port types (SDH, PDH, LAN, WAN).
- Cross Connection Manager
- “Ethernet mapping with VCAT/LCAS”.
- “FAQ”. - A few troubleshooting tips, and frequently asked questions.

8.1.1 About port types

One of the differentiators of AXX 9300 METRO, AXX 9100 CONNECT and AXX 9200 EDGE compared to other products is the possibility to equip it with a number of different port types. Some ports are part of the base unit and always present. (Management Port, AUX Ports, Alarm input and output ports).The alarm ports and auxiliary port cannot be created or deleted.

Traffic ports are available on replacable traffic modules. When a slot is configured to support a specific traffic module the ports of the traffic module is automatically created as described in “Manage slots on AXX 9200 EDGE” on page 376.

In this chapter we concentrate on the configuration of the traffic ports. The chapter is organized according to the following structure:

- SDH ports
- PDH ports
- LAN ports
- WAN ports and mapping

Troubleshooting and FAQ: this chapter contains a few troubleshooting tips, and gives answers to a number of Frequently Asked Questions.

8.1.2 Definitions

SNC - Sub Network Connection
General term for connecting termination points across a network.

There are 3 main classes:

- SNC internally implemented within a network element cross connection matrix between two Connection Termination Points (CTPs).
- Point to point connection between two Network Element CTPs
- End to end SNC: An ordered set of class 1 and 2 CTPs across an interconnected network of several NEs

8.1.3 Selecting a traffic port

Traffic ports are always located on a traffic module in slot 1 to 4. In managed objects for modules and ports are available when the slot is configured for a specific module type. This section describes how to select a traffic port independent of the traffic it carries.

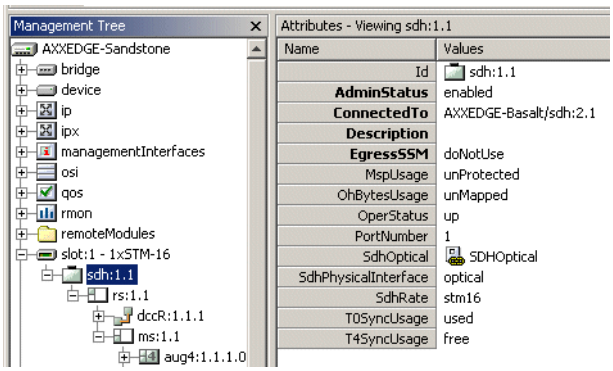


Figure 86 Selecting a traffic port

Procedure: **SELECT TRAFFIC PORT**

1. Click on the managed object and then the **slot** managed object (where the port is) in the Management Tree.
2. When the slot is expanded, click on the **port** managed object with the desired **port number**.

3. The port is selected and the attributes related to the physical and electrical **characteristics** of the port are **displayed** in the Attributes View.

4. The physical port usually carries a set of protocols (e.g. SDH) and the protocols are available from the Management Tree.

8.2 SDH ports

8.2.1 Configuring SDH port structure (channelization)

By default the SDH ports are unstructured (or not-channelised) when created. Only the *sdh Port*, *rs*, *ms* and *aug1* managed objects are available. In this state the paths inside the STM-N frame cannot be terminated nor cross-connected, but the port can be used as a protection port in an MSP protection scheme and a synchronization source candidate. It can also carry DCN traffic in the DCC channels.

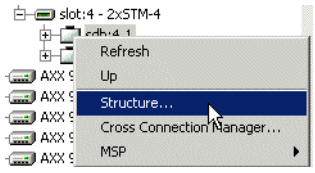
The motivation for structuring an SDH port is to identify the paths in the STM-N frame and making them available for cross-connection. As you structure the port it will fan out in the Management Tree, showing termination points that are now available for cross-connection.

NOTE! STM-4 and STM16 ports on AXX 9200 EDGE release 2.0 and later are not unstructured but automatically structured to the AUG-1 level.

8.2.2 SDH Structuring Wizard

Procedure: **CHANGE THE STRUCTURE OF AN SDH OBJECT.**

1. Select desired **sdh port.**



2. Right-click and select **Structure**.

No changes will be performed until you press Finish, and you can abort the wizard at any time with the Cancel button.

Structure Information displays the current SDH structure. The decisions you make in subsequent steps will affect this structure

Structure Type; Select the type of SDH structure you want.

Completing the Structure SDH Wizard; This step lists all the changes that will be performed when you press Finish.

The following sections show how to perform structuring, using the Management Tree.

8.2.3 SDH Structuring - with the Management Tree

Procedure: **MAKE AU-4 TERMINATION POINTS OF AN SDH PORT AVAILABLE FOR XC**

1. Select an **sdh port** as described in “Selecting a traffic port” on page 384.
2. Select the **rs** and then the **ms** managed objects as the port expands.
3. Select the **aug1** managed object that should be structured. (STM-N ports have N aug1 objects)

Figure 87 Select the aug1 managed object

4. Set the **Structure** attribute to AU-4

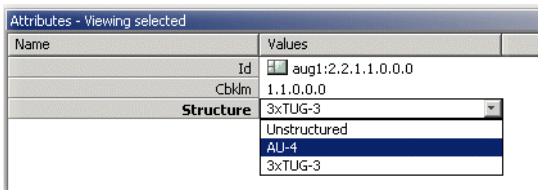


Figure 88 Set the Structure attribute

5. **Save**
6. Repeat for the other **aug1** objects on the port if you want to structure them as AU-4.

Procedure: **MAKE TU3 TERMINATION POINTS OF AN SDH PORT AVAILABLE FOR XC**

1. Perform **steps 1-3 in “” on page 387**
2. Set the **Structure** attribute to **3xTUG-3**.
3. Select the AU-4, **vc4** and then the TUG-3 managed object that should be structured.
4. Set the Structure attribute to **TU3**.
5. Save.
6. **Repeat** for the **other TUG-3** objects on the port if you want to structure them as TU3.

Procedure: **MAKE TU12 MANAGED OBJECTS OF AN SDH PORT AVAILABLE FOR XC**

1. Perform steps 1-3 in “” on page 387.
2. Set the **Structure** attribute of the TUG-3 managed object to **TU12**.
3. Click **Save** on toolbar.
4. Repeat for the other TUG-3 objects on the port if you want to structure them as TU12.

8.2.4 Modify or remov AXX 9200 EDGE SDH port structure

It is also possible to modify or remove the structure of an SDH port when the involved termination points are not cross-connected.

Procedure: MODIFY BETWEEN TU12 AND TU3OBJECTS

1. Remove all cross-connections that are terminated in the TU12 or TU3 termination points belonging to the TUG-3 object that you want to modify.
2. Follow the guidelines in “Configuring SDH port structure (channelization)” on page 385, to make TU3or TU12 termination points of an SDH port available for cross-connection.

Procedure: MODIFY BETWEEN AU-4 AND TU3/TU12 OBJECTS

1. Remove all cross-connections that are terminated in the AU-4, TU12 or TU3 termination points belonging to the aug1 object that you want to modify.
2. Set the TUG-3 Structure to "**none**" for all TUG-3 objects contained by the aug1 object that should be modified (see above).
3. Follow the guidelines in “Configuring SDH port structure (channelization)” on page 385, to make AU-4, TU3or TU12 termination points of an SDH port available for cross-connection.

NOTE! Modification of the structure involves deletion of existing Termination Points and creation of new Termination Points (if new structure is not "none"). To avoid unintentional traffic loss, AXX 9200 EDGE will not allow modification of the structure before all cross-connections belonging to a structure object have been deleted.

NOTE! Set the structure of all contained TUG-3 objects to "none" before you modify the aug1.

8.2.5 Setting and reading Path Trace Identifiers

Path Trace are available at two levels in the SDH port:

- RS Path Trace that will be terminated in the STM-N port on the opposite side of the link.
- VC-4 Path Trace that will be terminated in the SDH node terminating the VC-4 path.

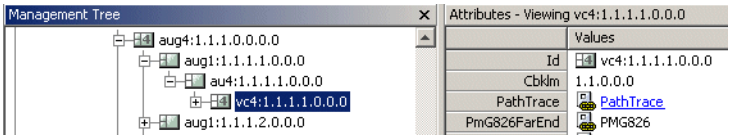
Procedure: **SET OR READ RS PATH TRACE IDENTIFIERS**

1. Expand an **sdh port**.
2. Click the **rs** object.
3. Click on **PathTrace** link in the attribute view.
4. The following attributes can be set:
   - **PathTrace**:
     Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
   - **PathTraceExpected**:
     Enter a value for the Path Trace Identifier that you expect to receive from the other side of the path.
   - **PathTraceTransmitted**:
     Enter a value for the Path Trace Identifier that you want to transmit to the other side of the path.
5. The following attributes can be read:
   - **PathTraceReceived**:
     The actual received Path Trace Identifier from the other side of the link
6. Save.

Procedure: **SET OR READ VC-4 PATH TRACE IDENTIFIERS**

NOTE! VC4 Path Trace is available only when the SDH port is structured with a VC-4 object, i.e. aug1 Structure is 3xTUG-3. See “Configuring SDH port structure (channelization)” on page 385.

1. Expand an **sdh port** to the desired vc4.



2. Click on **PathTrace** and set the path trace parameters. The attributes are the same as for RS Path Trace.

3. Save.

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.

8.2.6 Monitoring SDH Port Performance

PM - Performance Monitoring is available at **three levels** in the SDH port:

- RS PM, monitoring the near end of the Regenerator Section
- MS PM, monitoring the near and far end of the Multiplexer Section
- VC-4 PM, monitoring the near and far end of the VC-4 path

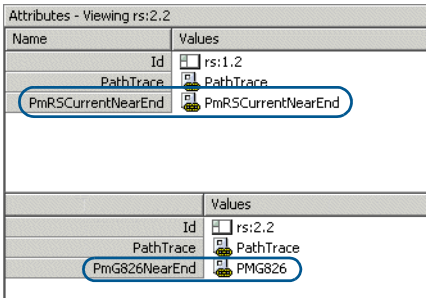
NOTE! The attribute names differ slightly between AXX 9300 METRO and AXX 9200 EDGE

Procedure: **READ RS PM COUNTERS**

1. Expand an **sdh** port.

2. Select the **rs** managed object.

3. Click on **PmG826NearEnd** to read near end PM data **or** **PmG826FarEnd** to read far end PM data.



AXX 9300 METRO view

AXX 9200 EDGE view

Figure 89 PM on RS - AXX 9200 EDGE and AXX 9300 METRO views.

4. The following attributes are available

   - **Current15Min ES**,**SES**, **BBE** and **UAS**
   - **Current24Hour ES**, **SES**, **BBE** and **UAS**

5. To see the Performance history of the previous 16x15 minute counters click on **Interval15Min**, or click on **Interval24Hour** to see the **previous 24 hour** counter.

6. The following attributes are available

   - **Interval15Min ES**,**SES**, **BBE** and **UAS**
   - **Interval24Hour ES**, **SES**, **BBE** and **UAS**

Procedure: **READ MS PM COUNTERS**

1. Expand an **sdh** port.

2. Select the **ms** managed objects.

3. Click on **PmG826NearEnd** to read near end PM data **or** **PmG826FarEnd** to read far end PM data.

4. The **attributes** are the **same as for RS PM**.

Procedure: **READ VC-4 PM COUNTERS**

1. Expand an **sdh** port.

2. Select the **rs** and then the **ms** managed objects as the port expands.

3. Select the **aug1** managed object that contains the **vc4** to measure.

4. Select the AU-4 and then the **vc4** managed objects as the port expands.

5. Click on **PmG826NearEnd** to read near end PM data or **PmG826FarEnd** to read far end PM data.

6. The **attributes** are the same as for **RS PM** in “” on page 391.

8.2.7 Enable the SDH port to carry traffic and report alarms

By default the Administrative Status of the SDH port is set to disabled when the port is created. No traffic will pass through the port and no alarms are reported before it is enabled.

Procedure: **ENABLE ADMINSTATUS**

1. Select an **sdh** port and set the Administrative status.

2. The AXX 9300 METRO has four service states:

State	Description
in service (IS)	This is the normal operation state: -The port is able to carry traffic - Alarm reporting is enabled - Loops are not allowed to be activated
out of service (OOS)	This state is equivalent to a port shutdown: - The port is not able to carry traffic - Alarm reporting is disabled for the port (includes alarms related to configurable Physical Interface module) - Loops are not allowed to be activated - For optical SDH ports the laser is shut down - For electrical STM-1 ports AIS is transmitted in the payload

State	Description
out of service - maintenance (OOS-MT)	This state is intended for testing, faultfinding and maintenance activities: - The port is able to carry traffic - Alarm reporting is disabled - Loops are allowed to be activated
out of service - auto in service (OOS-AINS)	The OOS-AINS state is a temporary state intended for provisioning purposes. This means that a port configured to OOS-AINS automatically goes into IS state if a valid signal is applied to the port. A valid signal is a signal that is clearing a LOS (Los of signal) alarm or a Link Down alarm (LANX and WANX Ethernet ports). For a state change to occur the signal must be valid for a certain time, which is a configurable parameter from 0 to 48 hours in steps of 15 minutes. The parameter is a global parameter for the NE. In this state the port operates in the following manner: - The port is able to carry traffic - Alarm reporting is disabled - Loops are not allowed to be activated

3. AXX 9200 EDGE:
   Set **AdminStatus** to **enabled**.

4. Save.

NOTE! When disabled, the SDH port inserts VC4-UNEQ out of the port and AU-4-AIS towards the cross-connection matrix

NOTE! Even if the SDH port is enabled it will only report alarms if the AlarmReporting attribute of the slot is set to enabled.

8.2.8 Port synchronisation quality output signaling

STM-N signals are often used to carry synchronization information. A dedicated protocol is used to indicate the quality of the signal that is output from one SDH node to the next SDH node:

Procedure: **SYNCHRONISATION QUALITY**

1. Select an **sdh** port.

2. Set **EgressSSM** to **t0** or **doNotUse**. t0 will always indicate the quality status of the internal clock.

3. Save.

NOTE! When an SDH port is used as a synchronization source candidate, the S1 byte will be automatically set to "Do not use".

8.2.9 Use the SDH Port as a synchronization source input

See“Add Synchronization Source candidate (T0 or T4)” on page 345

8.2.10 DCC channels to carry management traffic

See “DCC Configuration - AXX 9200 EDGE” on page 305.

8.3 PDH ports

AXX 9300 METRO and AXX 9200 EDGE can be equipped with two different PDH port types:

- **E1** (2 Mbit/s) supporting transparent data and NT functionality of ISDN PRA. E1 Ports are available when the slot is configured for the 8xE1 module or the 63xE1 module.
- **E3** (34/45 Mbit/s) supporting transparent data. E3 Ports are available when the slot is configured for the 6xE3 module.

AXX155E is equipped with **E1** ports.

8.3.1 Setting the Port mode

1. Select a **pdh** port.
2. When the pdh port managed object is expanded, select the **e1** or **e3** managed object.

3. For **e1** ports set the **E1Mode** attribute to **tra** (2 Mbit/s transparent G.703), or **pra** (ISDN PRA), or **prafixed** (Primary rate access with fixed timing).

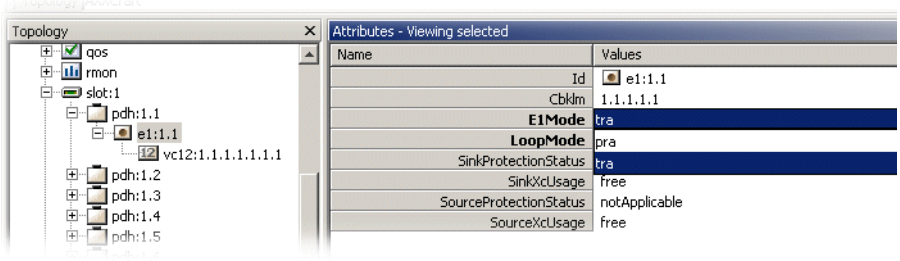


Figure 90 Set the E1Mode attribute

4. For **e3** ports set the **E3Mode** attribute to **e3** (34 Mbit/s transparent G.703) or **t3** (45 Mbit/s transparent G.703).

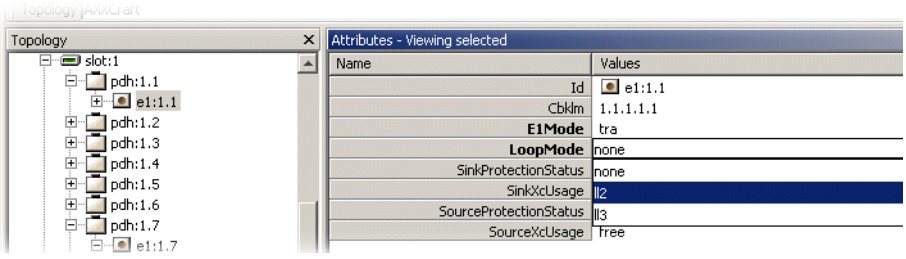
5. Save.

8.3.2 Setting a loop in a PDH Port

1. Select a **pdh** port as described in “Selecting a traffic port” on page 384.

2. When the pdh port managed object is expanded, select the **e1** or **e3** managed object.

3. Set the **loopMode** attribute to **ll2** (loop back to network) or **ll3** (loop back to customer).



4. Save.

NOTE! There are restrictions for setting the loops of PDH Ports:

- AXX 9840 INSITE cannot set and release loops when the E1Mode is set to pra. (in this mode loops can only be managed from an NT1 or similar).

- A loop cannot be set when pdh Port AdminStatus is set to disabled.

8.3.3 Setting a loop in an AXX155E PDH port

1. Select desired **pdh** port
2. When the pdh port managed object is expanded, select the **e1** managed object.
3. Set the **loopMode** attribute to **ll2** (loop back to network) or **ll3** (loop back to customer)
4. Save.

8.3.4 Releasing a loop in a PDH Port

1. Select a **pdh** port.
2. When the **pdh** port managed object is expanded, select the e1 or e3 managed object.
3. Set the **loopMode** attribute to **none**.
4. Save.

NOTE! Alternatively, any loop will be released if pdh Port AdminStatus is set from enabled to disabled.

8.3.5 Assign VC12s in AXX155E

This section use VC12 as example in assigning VCs in a network element.

1. Expand desired **PDH port** in the Management Tree, to view VC12 managed object attributes.
2. Set **AssignedCbklm** to desired value.

You may use the **Cross Connection Manager** window to view available VC12s with cbklm values.

3. Click **Save**.

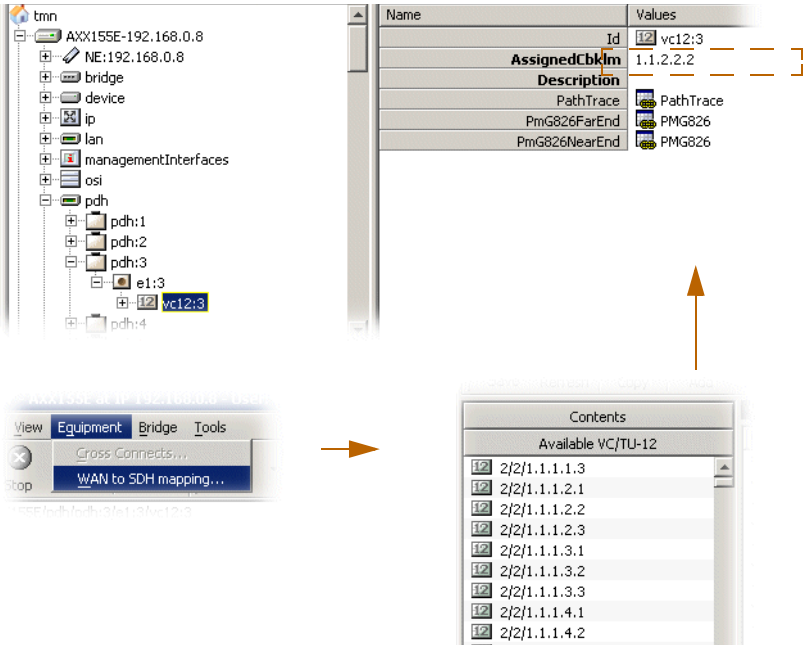


Figure 91 Assigning VCs - VC12 Example

8.3.6 Setting and reading Path Trace Identifiers

1. Expand a **pdh** port.
2. Click on the **e1** or **e3** managed object.
3. Click on the **vc12** (E1) or **vc3** (E3) managed object
4. Click on **PathTraceVC12**.

The following attributes can be set:

- **PathTrace**:
  Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.
- **PathTraceExpected**:
  Enter a value for the Path Trace Identifier that you expect to receive from the other side of the path.
- **PathTraceTransmitted**:
  Enter a value for the Path Trace Identifier that you want to transmit to the other side of the path.

5. The following attributes can be read:

- **PathTraceReceived**:
  The actual received Path Trace Identifier from the other side of the link

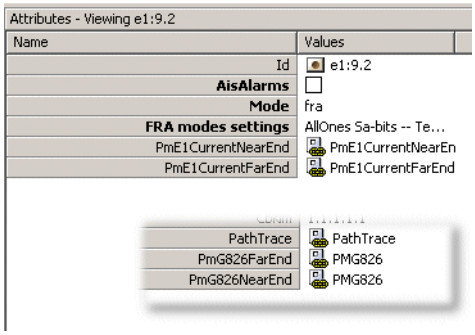
6. Save.

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.

8.3.7 Monitoring PDH Port Performance

1. Expand a **pdh** port.
2. Select the **e1** or **e3** managed object.
3. Click on the **vc12** (for e1 ports) or **vc3** (for e3 ports). (NA for AXX 9300 METRO)

4. Click on **PmG826NearEnd** to read near end PM data or **PmG826FarEnd** to read far end PM data. AXX 9300 METRO differs as shown in the figure below:



AXX 9300 METRO view

Figure 92 PM data links differences

5. The following attributes are available:

- **Current15Min ES**,**SES**, **BBE** and **UAS**
- **Current24Hour ES**, **SES**, **BBE** and **UAS**

6. To see the **Performance history** of the previous **16x15 minute** counters click on **Interval15Min**, or click on **Interval24Hour** to see the previous **24 hour** counter.

7. The following attributes are available

- **Interval15Min ES**,**SES**, **BBE** and **UAS**
- **Interval24Hour ES**, **SES**, **BBE** and **UAS**

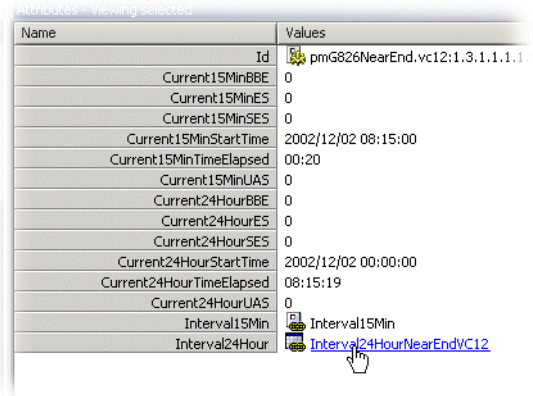


Figure 93 PmG826NearEnd - Interval24Hour attribute

8.3.8 Monitoring PDH E1 Port Performance

The E1 counters are based on CRC-4 counters for near end and E-bit counters for far end monitoring. Defect criteria for near end is

LOS-TX(Loss Of Signal), LOF-TX(Loss Of Frame) and module/slot alarms. For far end there are no alarms present to indicate any defects.

The valid flag for previous intervals and past 24 hours is set only when the port has been in PRA-mode during the whole period. For ports in TRA-mode, the PM counters can only be used to indicate SES/UAS due to LOS-TX or module/slot alarms.

1. Select a pdh E1 port.
2. When the pdh port managed object is expanded, select the e1 managed object.
3. Click on the PMG826 link for PmG826NearEnd to read near end PM data or PmG826FarEnd to read far end PM data.
4. To see the Performance history of the previous 16x15 minute counters click on **Interval15Min**, or click on **Interval24Hour** to see the previous 24 hour counter.
5. The following attributes are available
   - Interval15Min ES, SES, BBE and UAS
   - Interval24Hour ES, SES, BBE and UAS

8.3.9 Enabling the PDH port to carry traffic and report alarms

By default the Administrative Status of the PDH port is set to disabled when the port is created. No traffic will pass through the port and no alarms are reported before it is enabled.

1. Select a **pdh** port as described in “Selecting a traffic port” on page 384.
2. Set **AdminStatus** to **enabled**.
3. Save.

NOTE! When disabled the PDH port generates AIS upstream and downstream.

8.4 LAN Ports

This section is organized as follows:

- “AXX 9200 EDGE - LAN port attributes”
- “AXX155E LAN port attributes”
- “LANx port”

8.4.1 AXX 9200 EDGE - LAN port attributes

An AXX 9200 EDGE slot can be configured to carry a Fast Ethernet (FE) 8xFeRJ45 module. Please see “Manage slots on AXX 9200 EDGE” on page 376 for details.

1. When the module is installed in desired slot, click desired LAN port to view modifiable attributes.

2. Attributes marked as bold are modifiable:

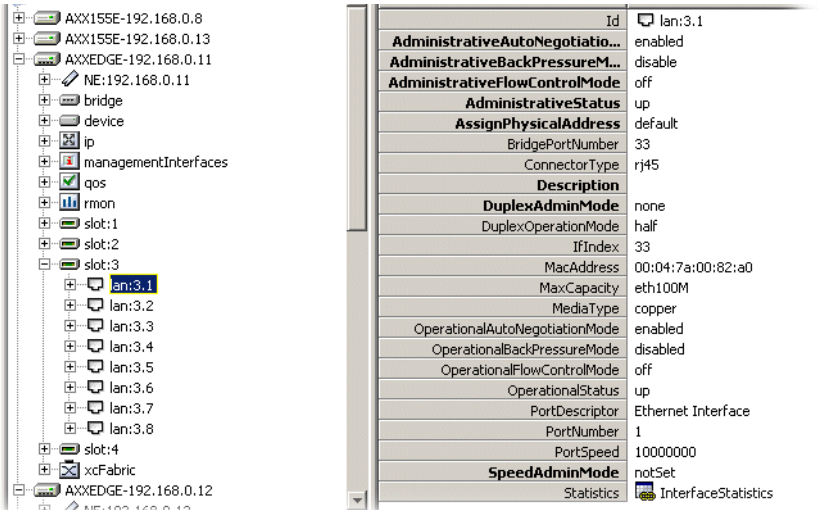


Figure 94 LAN port attributes - AXX 9200 EDGE example

Modifiable attributes and their possible values:

AdminAutoNegotiationMode:	disabled or enabled
AdminBackPressureMode:	disabled or enabled
AdminFlowControlMode:	on, off or auto negotiation
AdminStatus:	disabled or enabled
AssignPhysicalAddress:	reserve or default
Description:	string

DuplexAdminMode:	none, half or full
SpeedAdmin mode:	not set, 10M or 100M

3. Click **Save** if you have modified any attributes.

8.4.2 AXX155E LAN port attributes

The AXX155E is equipped with 4 LAN ports. For configuration of LAN ports see “AXX 9200 EDGE - LAN port attributes” on page 402

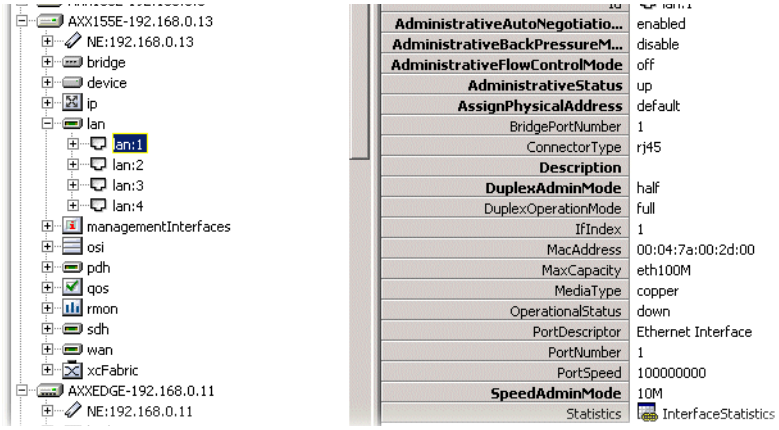


Figure 95 LAN port attributes - AXX155E example

For LAN ports attributes, see “AXX 9200 EDGE - LAN port attributes” on page 402.

For “Force LAN Down”, Also see page 8-477“Force LAN Down” on page 477.

8.4.3 LANx port

LANx is the expression of an Ethernet (LAN) port with two layers and extended functionality supporting VLAN provisioning, and advanced mapper modules(Layer 1).

See “VCAT and GFP mappers” on page 465 or “VLAN provisioning” on page 547.

8.4.3.1 LANx settings

This is a presentation of dedicated attributes for LANx ports. For common attributes, see “LAN Ports” on page 402.

Jumboframes; enabled or disabled.

FlowControl_BackPressure; on, off or autoneg.

OperFlowControl; on or off (read only).

Priority(802.1p); disabled or 802.1p (enabled).

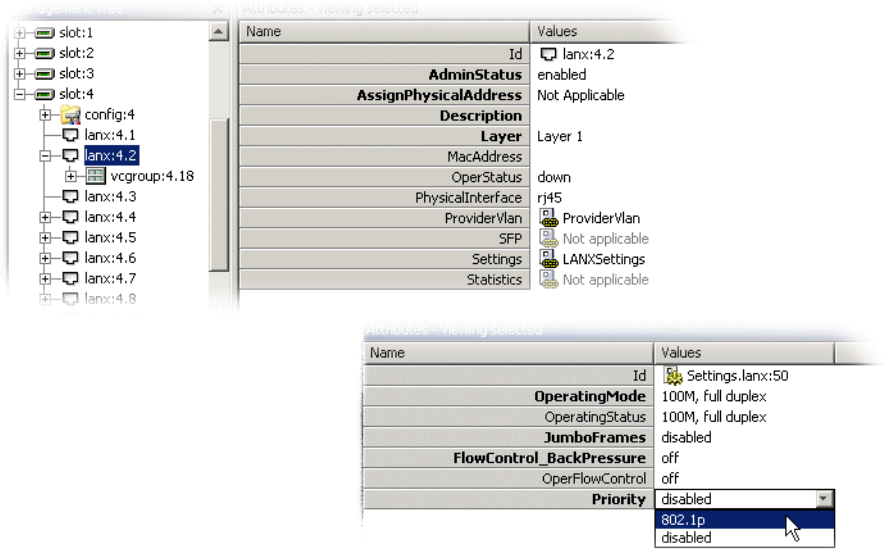


Figure 96 LANx port attributes- example Layer 1

Layer 1

When FlowControl_BackPressure is set to **off**, you enable Priority by selecting **802.1p** (enabled mode).

Priority (802.1p) and FlowControl_BackPressure may both be **disabled/ off** at the same time.

When JumboFrames is set to **disabled**, the package size is 1536 byte frames.

Set JumboFrames to **enabled** to increase the package to 9216 (9k) byte frames.

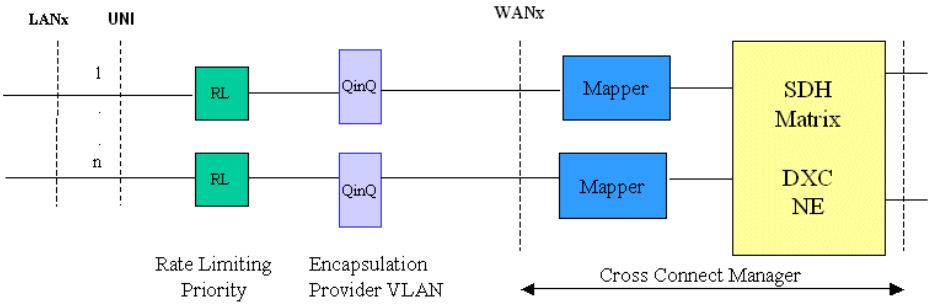
Layer 2

When FlowControl_BackPressure is set to **on** or **autoneg**., you can set Priority (802.1p) in **disabled** mode. When FlowControl_BackPressure is set to **off**, you can enable Priority (**802.1p**).

JumboFrames; set to **disabled** for 1536 byte frames, or **enabled** for 6144 (6k) byte frames.

8.5 WAN ports

A WAN[1] can be established by mapping Ethernet ports to the SDH Frame Structure. The Ethernet packets are transported end-to-end on a path through an SDH network. In layer 2 mode the WAN port is a port at the internal L2 switch. See figure..



Functional diagram of LAN and WAN ports in layer 1 mode.

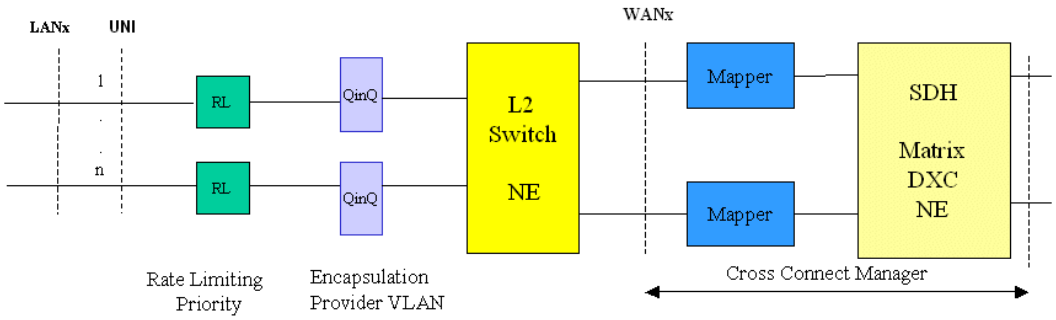


Figure 97 Functional diagram of LAN and WAN ports in layer 2 mode.

In layer 1 mode the WAN port is a point before the mapping function. In both cases the Cross Connect Manager is used to set up a connection from WAN to the other side of the SDH matrix.

See “Configuring SDH port structure (channelization)” on page 385, “WANx ports” on page 485, and “Ethernet mapping with VCAT/LCAS” on page 460.

1. Wide Area Network

8.5.1 Introduction

The purpose of this section is to describe the tasks involved in assigning capacity from the SDH server layer to a WAN port. The total assigned WAN capacity is made up of SDH channels.

Each SDH channel is equivalent to a VC-12 (2 Mbit/s). This section describes the VC-12/TU12 layer rate only. The SDH channels can be from different SDH ports.

Each SDH channel is equivalent to a VC-12, VC-3 or VC-4. The WAN channels can be sub-network connection (SNC) protected, supported with protection scheme SNC/I (inherent monitoring).

SDH channel mapped to a VC-12 (2 Mbit/s) is described in this section to exemplify a SDH layer rate. See “Ethernet mapping with VCAT/LCAS” on page 460.

WAN ports and the mapping

The AXX 9200 EDGE network element in this example has eight WAN ports. These are located on the 8xSTM-1 module. They are connected to a Layer 2 switch, see Figure 98 A WAN port has a maximum capacity of 100Mbits/s.

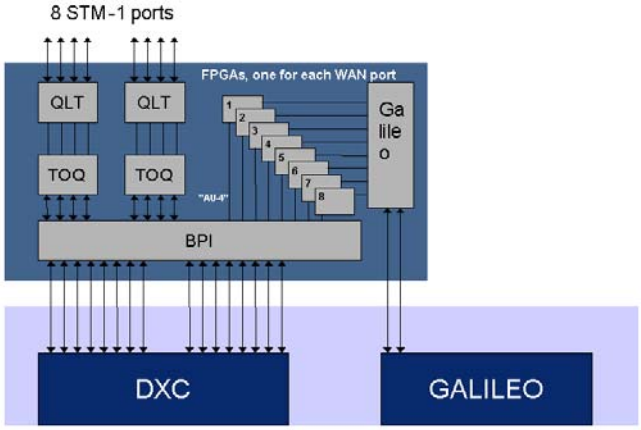


Figure 98 The 8xSTM-1 module with WAN ports (AXX 9200 EDGE)

Figure 99 shows that the potential capacity of 100Mbit/s is realized through 50 channels each able to carry 2.160 Mbit/s. The capacity of the WAN port is therefore decided by how many channels that are used for traffic. See “WAN port - 50 channels/47 channels?” on page 486.

A WAN port can be mapped to one STM-1 port, i.e., there are potentially 63 available VC-12s. Only the 50 first of these are used. These 50 channels have hard coded mapping to 50 VC-12 containers.

The D.C.B.K.L.M numbering is described in “D.C.B.K.L.M value usage” on page 453.

The WAN VC-12s are cross connected to the available TU12s on the SDH ports. All 50 WAN VC-12s are always available for cross connection. A WAN VC-12 always represents the termination point ‘A’ in the Cross Connection Manager and the connection is always bi-directional. The cross connection can be protected. If there exists a VC-12 (or channel) inside the WAN capacity that is not cross connected, the network element issues an alarm on the WAN VC-12 (unequipped alarm.)

For uni- directional, see “Uni- directional VCAT with LCAS” on page 470.

The order of the channels is essential and must be the same on both sides of a WAN over SDH connection, e.g., containers sent from channel 1 must be received on channel 1. A sequence number is used to indicate the correct order of the VC-12 on the receiving side of a WAN connection between two AXX 9200 EDGEs. If the connection is not between two AXX 9200 EDGE, the sequence number will be zero. A scenario where the cross connection between two TU12s and two VC-12s in one AXX 9200 EDGE are wrong, are illustrated in Figure 100

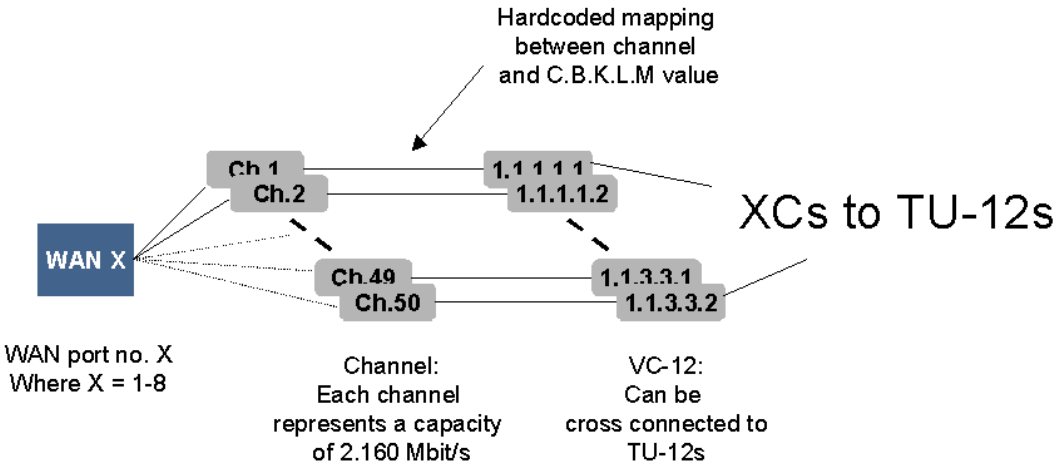


Figure 99 View of one WAN port and its logical view

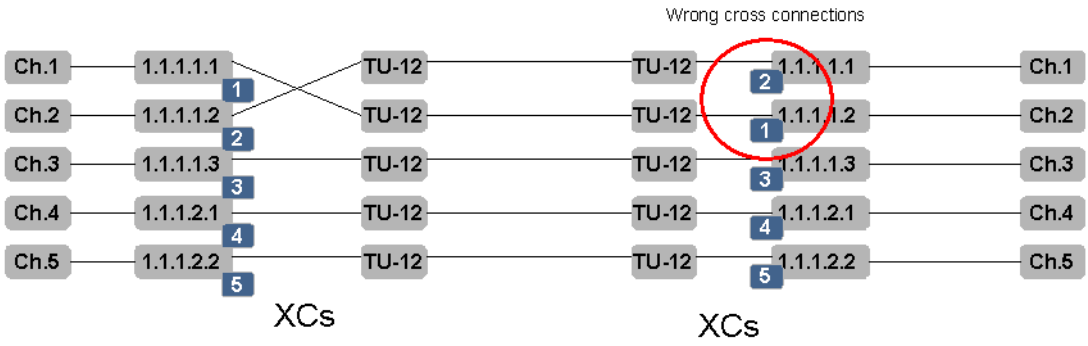


Figure 100 Sequence numbers for correct order of TU12 to VC-12 cross connections.

Alarms and performance monitoring data is collected and reported for those VC-12s that are within the WAN capacity.

8.6 Cross Connection Manager

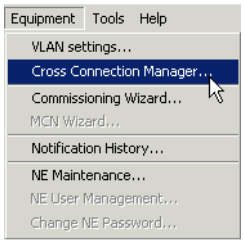
Use the Cross Connection Manager to create and manage:

- Ethernet over SDH mapping
- Cross connections

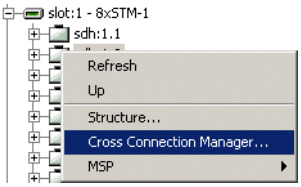
8.6.0.1 Open the Cross Connection Manager

1. You can open the Cross Connection Manager in two ways:

The equipment menu on the desktop



Right click a port in the Management tree



8.6.0.2 GUI - Overview

The system presents the GUI with the search pane open. This is where you decide what type of cross connect you want to work with. When you have selected the type, the system will present the actual ports for the selected cross connection(XC) type.

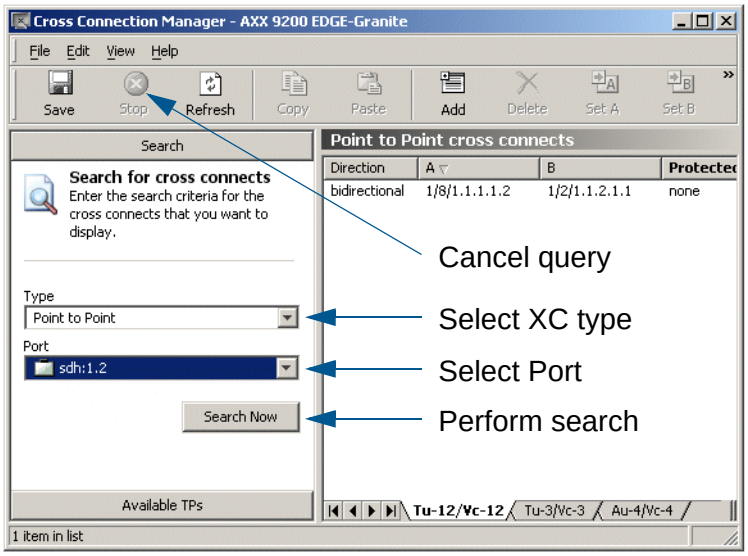


Figure 101 Cross Connection Manager GUI - Search

NOTE! When you have started the search with the “Search Now” button, the selection panel will turn gray and you will not be able to change parameters until you cancel the search or the search is finished.

When you have selected XC type and the port you want to establish an XC on, AXX 9840 INSITE presents the available TPs, the existing XCs and a preview of the selected XC as shown in the example below:

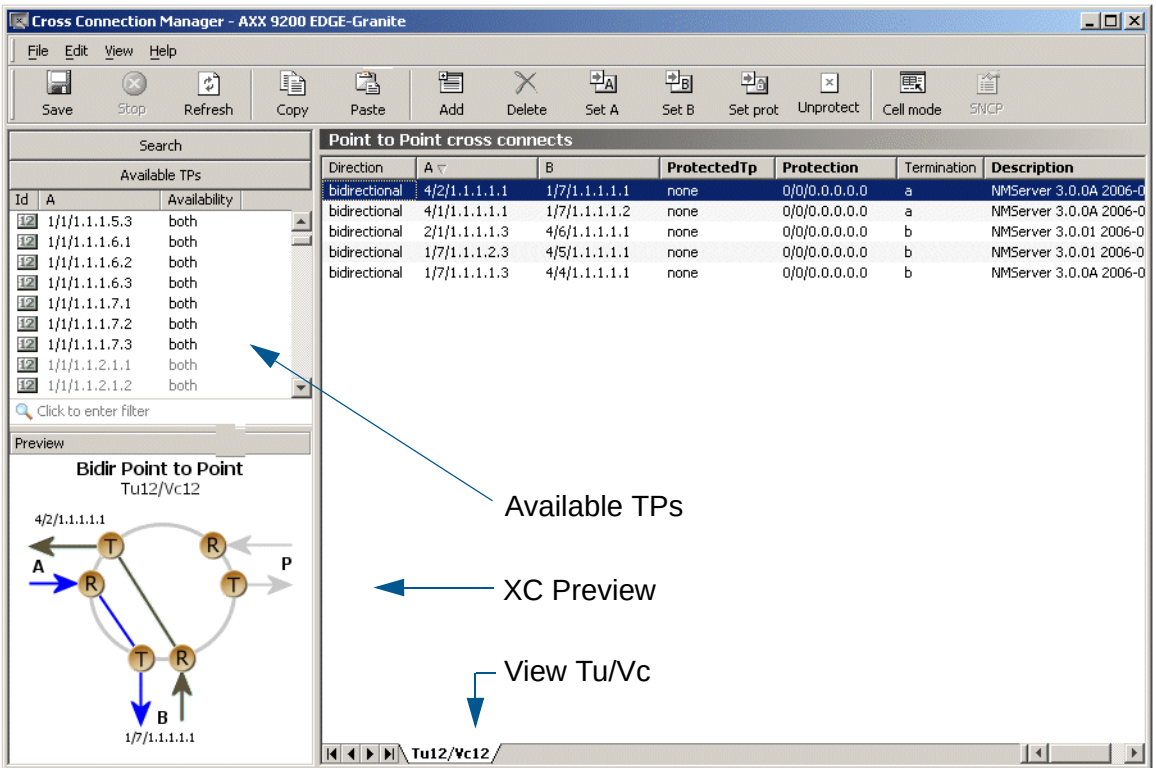


Figure 102 Cross connection GUI - Overview

Actual and Potential TPs (AXX 9300 METRO)

In the Available TPs pane, the Actual and Potential TPs are differentiated with the font colour as illustrated below:

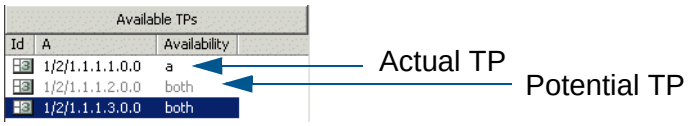


Figure 103 Actual and Potential TPs

TP type	Font	Description
Actual TP	Black	Available, structured capacity
Potential TP	Light grey	Available, unstructured capacity - These TPs will be automatically structured when the XC is performed.

Refresh the presentation

Refresh the Available TP list and cross-connection list based on the last operations performed and saved.

Floating termination points indication on AXX 9300 METRO

When connected to an AXX 9300 METRO NE, you can monitor the number of floating termination points as shown in the figure below:

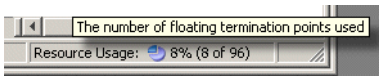
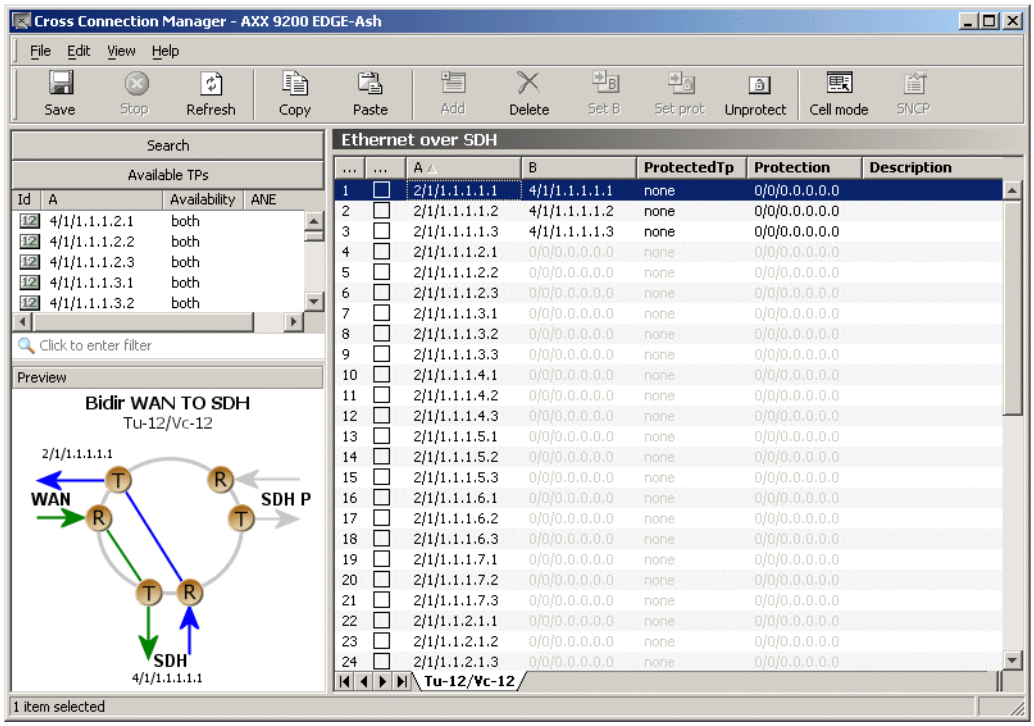


Figure 104 Resource indicator

A list of available STM- n ports is presented in accordance to VC-level.



Available columns:

The visible choices depend on the installed module and its configuration.

Figure 105 WAN channels list- example VC/ TU 12

Cancel a query

Queries in progress can be cancelled with the 

Stop operation button.

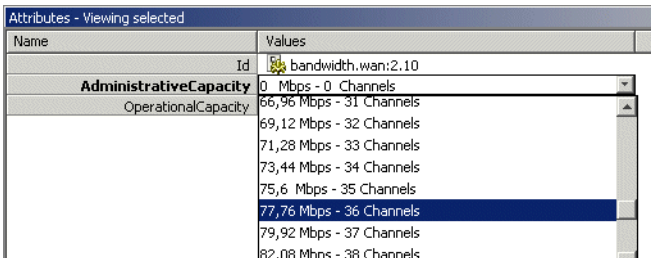
8.6.1 Add initial WAN Port capacity

The addition of WAN port capacity is performed in a **two step process**.

This is illustrated for Ericsson AXXESSIT proprietary and VC12. The **first step** is to set the administrative capacity of the WAN port. This will tell AXX 9200 EDGE how many of the 50 possible WAN channels to use for mapping into the SDH server layer.

1. Select a **wan port**.

2. When the wan port managed object is expanded, select **Bandwith**.



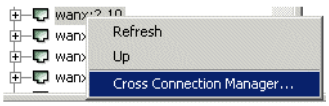
3. Set the **AdminCapacity** to a **value between 0 and 100 Mbit/s**.

4. Save.

The **next step** is to cross-connect the WAN channels that are in use after setting the administrative capacity:

5. Select the **wan port** again, right click and select **Cross Connection Manager**.

.



A list of all the WAN channels of the WAN port is shown. The list shows the **static relation** between **each channel number** and a **VC12 object** in the WAN port. The **WithinCapacity** attribute

indicates if the channel is in use by the WAN channel (i.e. if it was included when setting administrative capacity above).

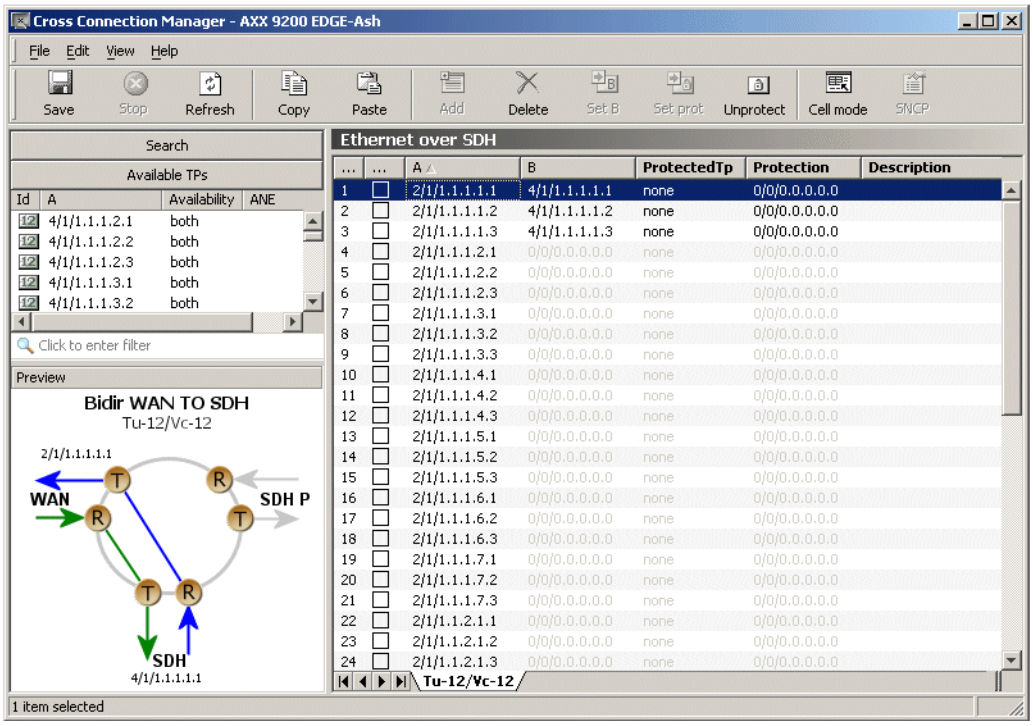


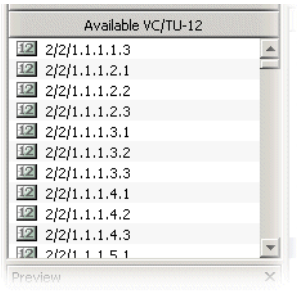
Figure 106 WAN channels list- example VC12 on AXX 9200 EDGE

6. Make sure the **Content panel** is available in the left part of the window.

   If it is not available select the 

   Content button in the toolbar.

7. Select the **Available VC/TU12 List** in the Content panel.
   The list contains the **free TU12 termination points** in AXX 9200 EDGE.



   SHIFT and CTRL buttons can be used for multiple selection

NOTE! If the Available VC/TU12 List in the Content panel does not show the TU12 termination points that you want to map your WAN port to, you have to make sure they are made available for cross-connection. See “Configuring SDH port structure (channelization)” on page 385.

8. Double-click the **TU12 termination point** that you want to use to map to your **WAN channel number 1**. The selected TU12 is inserted as the B termination Point for channel 1.
9. Double-click the **termination point** that you want to use to map to your **WAN channel number 2**.
10. Continue **until all channels** that are within capacity has a B termination point.
11. Save.

NOTE! Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate nodes. The WAN channel will only work if it is connected to the WAN channel with the same channel number on the opposite end of the SDH network.

NOTE! The WAN port will not report alarms on channels that are not part of the administrative capacity.

8.6.2 Modify WAN Port capacity

You can modify the WAN port capacity in the same way as you added the initial WAN capacity (as shown in “Add initial WAN Port capacity” on page 413):

1. Select a **wan port** as described in “Selecting a traffic port” on page 384.
2. When the wan port managed object is expanded, select **Bandwith**.
3. Set the **Bandwith** to a new value **between 0 and 100 Mbit/s**.

4. Save.

5. Select the **wan port again**, right click and select **Cross Connection Manager**.

A list of all the WAN channels of the WAN port is shown. The list shows the static relation between each channel number and a VC12 object in the WAN port. The WithinCapacity attribute indicates if the channel is in use by the WAN channel (i.e. if it was included when setting administrative capacity above).

6. If you increased the administrative capacity in step 3, more channels have the WithinCapacity attribute set and they need a B termination point to be mapped to the SDH server layer. Follow steps 5-10.

7. If you decreased the administrative capacity in step 3, less channels have the WithinCapacity attribute set and the B termination points can be released for other purposes. Follow steps 12-15.

Increasing capacity in the SDH server layer:

Make sure the Content panel is available in the left part of the window. If it is not available select the Content button in the toolbar

1. Select the **Available VC/TU12 List** in the Content panel.
   The list contains the free TU12 termination points in AXX 9200 EDGE.

NOTE! If the Available VC/TU12 List in the Content panel does not show the TU12 termination points that you want to map your WAN port to, you have to make sure they are made available for cross-connection. See “Configuring SDH port structure (channelization)” on page 385.

2. Double-click the **TU12 termination point** that you want to use to map to your **first new WAN channel**. The selected TU12 is inserted as the B termination Point for this channel.

3. Double-click the **termination point** that you want to use to map to your **next new WAN channel**.

4. Continue **until all new channels** that are within capacity has a B termination point.

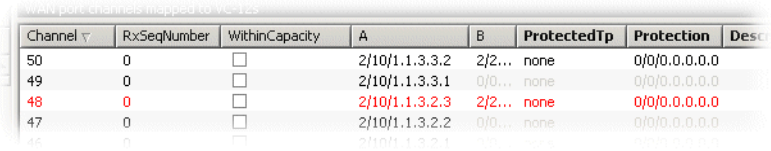
5. Save.

6. Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate SDH nodes.

8.6.2.1 Decreasing capacity in the SDH server layer

1. Select the **WAN channels** that are **not used any more** by the WAN port mapping (channels with B termination points, but not WithinCapacity). Multiple selection is possible with SHIFT or CTRL buttons.

2. Click **Delete** on the toolbar. The selected channels becomes red.



Channel	RxSeqNumber	WithinCapacity	A	B	ProtectedTp	Protection
50	0	☐	2/10/1.1.3.3.2	2/2...	none	0/0/0.0.0.0.0
49	0	☐	2/10/1.1.3.3.1	0/0...	none	0/0/0.0.0.0.0
48	0	☐	2/10/1.1.3.2.3	2/2...	none	0/0/0.0.0.0.0
47	0	☐	2/10/1.1.3.2.2	0/0...	none	0/0/0.0.0.0.0

3. Click **Save** on toolbar.
   The SDH TU12 termination points are released from WAN port mapping.

4. Remember to perform the same operation on the WAN port on the other side of the SDH network and deleting cross-connections in intermediate SDH nodes.

NOTE! It is not possible to modify the B termination point after it has been saved. If you want to modify the B termination point the channel must first be deleted, and then a new Termination Point can be added.

8.6.3 Protect a WAN port

WAN ports can be protected by the SNC protection scheme in the VC12/TU12 SDH layer. That means that the WAN channels (not necessarily all WAN channels of a WAN port) can have two different routes through the SDH server network, and that the receiving WAN channel selects the route with the best signal.

1. **Add initial** WAN port **capacity** as described in “Add initial WAN Port capacity” on page 413.
2. Set the **ProtectedTP** attribute to **a** for the WAN channels you want to protect
3. Select the **first WAN channel** you want to protect.
4. Make sure the **Content panel** is available in the left part of the window.
   If it is not available select the Content button in the toolbar
5. Select the **Available VC/TU12 List** in the Content panel.
   The list contains the free TU12 termination points in AXX 9200 EDGE.

NOTE! If the Available VC/TU12 List in the Content panel does not show the TU12 termination points that you want to protect your WAN channel with, you have to make sure they are made available for cross-connection. See “Configuring SDH port structure (channelization)” on page 385.

6. Select the **TU12 termination point** that you want to protect your WAN channel with.
7. Click on the **Set Prot** button 

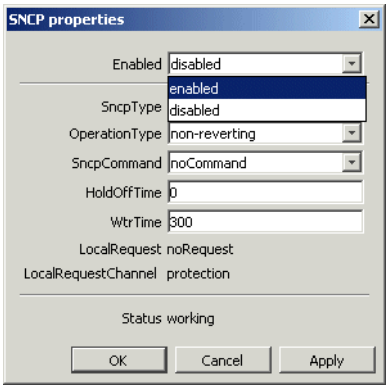
in the toolbar. The **protection TP** is filled in for the selected WAN channels.
8. Select the **next WAN channel** to protect and insert the **protection TU12**. Proceed **until all WAN channels** are protected (channels that have the Protected TP attribute set to **a**).
9. Click **Save** on toolbar. Remember to perform the **same operation** on the WAN port on **the other side** of the SDH network and adding cross-connections in intermediate nodes.

NOTE! By default the protection is enabled.

10. Select the **WAN channels** where you want to enable protection (SHIFT and CTRL buttons can be used for multiple selection).
11. Click the **SNCP** 

button in the toolbar

12. Set the **Enabled** attribute to **enabled** and click **OK**.



NOTE! Remember to perform the same operation on the WAN port on the other side of the SDH network. (However SNC protection is not bidirectional and does not have to be enabled in both ends simultaneously for the SNC protection scheme to work on the side that is enabled).

NOTE! It is not possible to modify the Protection termination point after it has been saved. If you want to modify the Protection termination point the ProtectedTP must first be saved as none. Then the Protection TP can be modified. Remember to set the ProtectedTP back to a.

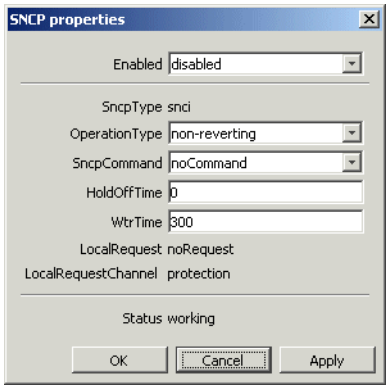
8.6.4 Modifying protection parameters of the WAN port

WAN ports are protected as described in “Protect a WAN port” on page 418. The SNC is then set up with a set of default parameters. The parameters can easily be modified:

1. Select a wan port as described in “Selecting a traffic port” on page 384.
2. Right click and select **Cross Connection Manager**.
3. Select the **WAN channels** where you want to modify protection parameters (SHIFT and CTRL buttons can be used for multiple selection).

4. Click the **SNCP**  button in the toolbar

5. Modify the **SNC protection** parameters and click OK.

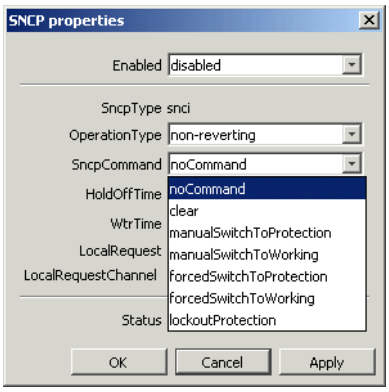


6. Click **Save** on toolbar.

8.6.5 Commanding WAN port protection switch

You can control the SNC protection switch by sending a command.

1. Select a **wan port** as described in Selecting a traffic port.
2. Right click and select **Cross Connection Manager**.
3. Select the **WAN channels** where you want to modify protection parameters (SHIFT and CTRL buttons can be used for multiple selection).
4. Click the **SNCP** button in the toolbar
5. Select the **SncpCommand** and click **OK**.



6. Click **Save** on toolbar. Depending on the priority of the command and current status of each channel, a switch may now take place for some or all selected WAN channels.

8.6.6 Setting Path Trace Identifiers for WAN port

Path Trace parameters can be read for each channel (VC12) in the WAN port.

1. Select a **wan port**.
2. Click on the **PathTraceWAN** parameter group
3. The following **attributes** can be set for all channels of the WAN port:

PathTrace:
Set to enable if TIM alarms should be reported for the WAN port when there is a mismatch between PathTraceReceived and PathTraceExpected.

PathTraceExpected:
Enter a value for the Path Trace Identifier that you expect to receive from the other side of the WAN channels.

PathTraceTransmitted:
Enter a value for the Path Trace Identifier that you want to transmit to the other side of the WAN channels.

4. Click Save on toolbar

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.

8.6.7 Reading Path Trace Identifiers for WAN port

Path Trace parameters can be read for each channel (VC12) in the WAN port.

1. Select a **wan port**.

2. When the wan port managed object is expanded, click on the **channel** (**vc12**) where you want to see the **Received Path Trace**.

3. Click on **PathTraceVC12**

4. The following attributes can be read:

PathTrace:
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.

PathTraceExpected:
Enter a value for the Path Trace Identifier that you expect to receive from the other side of the path.

PathTraceTransmitted:
Enter a value for the Path Trace Identifier that you want to transmit to the other side of the path.

PathTraceReceived:
The actual received Path Trace Identifier from the other side of the link

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received PathTrace.

8.6.8 Monitoring WAN Port Performance

1. Select a **wan port**.

2. When the wan port managed object is expanded, click on the **channel** (**vc12**) where you want to see the **Performance data**.

3. Click on **PmG826NearEndVc12** to read **near end PM data** or **PmG826FarEndVC12** to read **far end PM data**.

4. The following attributes are available

Current15Min ES,**SES**, **BBE** and **UAS**

Current24Hour ES, **SES**, **BBE** and **UAS**

5. To see the Performance **history** of the previous 16x15 minute counters click on **Interval15Min**, or click on **Interval24Hour** to see the previous 24 hour counter.

6. The following attributes are available

I**nterval15Min ES**,**SES**, **BBE** and **UAS**

Interval24Hour ES, **SES**, **BBE** and **UAS**

8.6.9 Advanced WAN Port operations

For frequent users of AXX 9840 INSITE, it is possible to make use of the enhanced editing facilities to speed up the configuration work.

Procedure: **SELECT AND INSERT MULTIPLE TERMINATION POINTS**

1. Select the **channels** where you want to **add termination points as B-end** or **Protection**.
   Use SHIFT or CTRL buttons to select more than one channel, or simply drag the mouse down the list while pressing the left mouse button.

2. Select the **TU12 termination points** that you want to add to the B-ends of the channels in the same way.

3. Click the **Set B** 

button in the toolbar.

4. Select the **TU12 termination points** that you want to add to the **Protection TPs** of the channels.

5. Click the **Set Prot** 

button in the toolbar.

6. Save.

NOTE! You are only allowed to set the B or Protection termination points of channels where B or P are not in use.

If you want to modify the B termination point the relation with the existing B termination point must first be deleted. Then a new Termination Point can be added.

If you want to modify the Protection termination point the

ProtectedTP must first be saved as none. Then the Protection TP can be modified. Remember to set the ProtectedTP back to a.

NOTE! If you do not select the same number of instances of WAN channels and termination points, the channels will be filled in with as many TPs as available, starting from the top of the selected channel list. If more TPs are selected than channels, the last TPs will not be used.

Procedure: **ENTER TERMINATION POINTS MANUALLY**

1. Select an **unconfigured WAN channel.**
2. Click on the **B termination point**. A list of slots appears.
3. Select **a slot**. A list of ports appears.
4. Select **a port**.
5. Continue selecting each of the **CBKLM** values.
6. Enter the **Protection termination point** the same way if used (and set **ProtectedTP to a**).
7. Save.

NOTE! The information can also be entered directly without selecting the numbers from the drop down list. Remember to use the following format: <slot/port/C.B.K.L.M>

8.6.10 Set up cross-connections

8.6.10.1 Select and search

In the XC GUI, start by Selecting an XC type and the port you want to establish the XC on. This step is similar for all XC types:

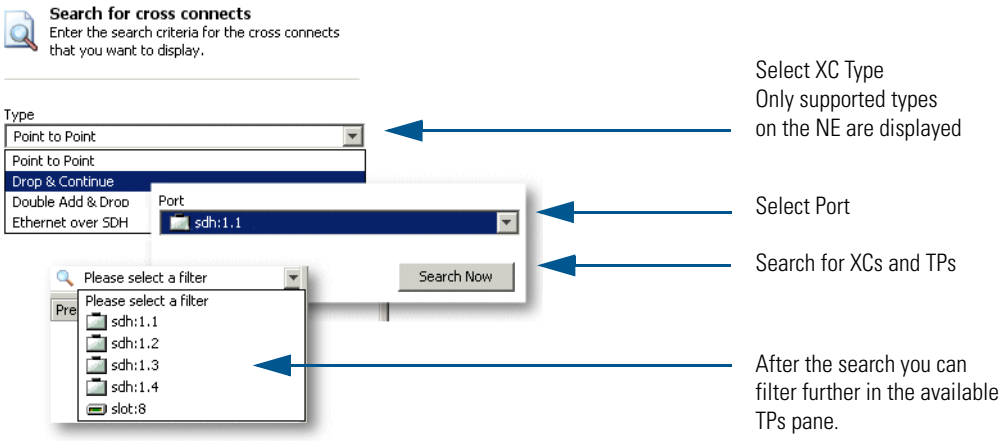
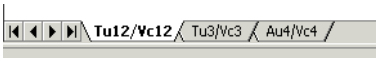


Figure 107 Select type and Port

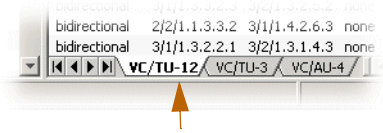
Select the layer you want to establish the XC on:



8.6.10.2 From a 2Mbit/s E1 port to a timeslot in an SDH port

Create a cross-connection from a 2Mbit/s E1 port to a timeslot in an SDH port (TU12 termination point):

1. Open the Cross-Connection Manager from the Equipment menu.
2. Perform a search on the port you want.
3. Select the **VC/TU12 tab** in the bottom of the window.



4. See the **Available TP List** in the Content panel. The list contains the free E1 ports and TU12 termination points in AXX 9200 EDGE.

NOTE! If the Available TP List in the Content panel does not show the E1 termination points that you want to cross-connect from, you have to make sure the slot is configured for E1 ports. See “Setting the Port mode” on page 395.

NOTE! If the Available TP List in the Content panel does not show the TU12 termination points that you want to cross-connect to, you have to make sure they are made available for cross-connection. See “Configuring SDH port structure (channelization)” on page 385.

NOTE! You can create bidirectional or unidirectional cross-connections. In the Available TP list you will see whether the termination point is available in both directions or as A-end or B-end.

5. Double click the **E1 port** in the Available TP list. A new cross-connection is created with the E1 port as the A-end.
6. Double click the **TU12** (timeslot) that you want to connect to. The TU12 is moved to the B-end of the cross-connection.
7. Select **Direction** (unidirectional or bi-directional).
8. Save.

NOTE! Remember that both the E1 port and the SDH port must be enabled before traffic can flow between the ports. See “Enable the SDH port to carry traffic and report alarms” on page 393 and “Port synchronisation quality output signaling” on page 394.

8.6.10.3 From a 45 Mbit/s E3 (T3) port to a timeslot in an SDH port

Create a cross-connection from a 45 Mbit/s E3 (T3) port to a timeslot in an SDH port (TU3 termination point):

1. Follow the description in 8.6.10.2 but select the **VC/TU3 tab** in step 2.

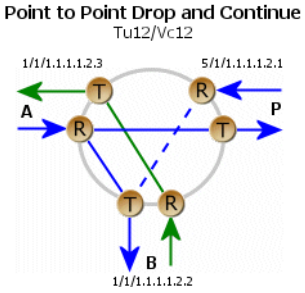
Create a pass-through cross-connection

From one SDH port to another SDH port:

1. Follow the example in 8.6.10.3 but select **TU12** or **TU3** or **AU-4** termination points for **both A and B ends**.

8.6.11 AXX 9300 METRO Cross connection examples

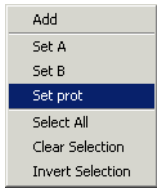
8.6.11.1 Drop and Continue



1. Add an XC:
   - Doubleclick an available TP, and an XC is added and the A- end is set.
   - Doubleclick the TP you want to be the B-end, and the B- end is set.

NOTE! The protected TP is always B for this XC type

2. Set protection:
   - Select the TP you want to protect the XC with and right click



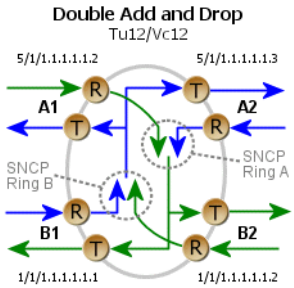
or press 

   Select Set Prot, and the Selected TP will protect the XC.

3. Enter a description.

4. Save.

8.6.11.2 Double Add and Drop



Here, you have two TPs on each side A1,A2 and B1,B2.

1. Select A1,A2,B1 and B2 by double clicking on the TPs respectively, and the values are filled in.
2. Enter Description
3. Save

8.6.11.3 Broadcast -Unprotected

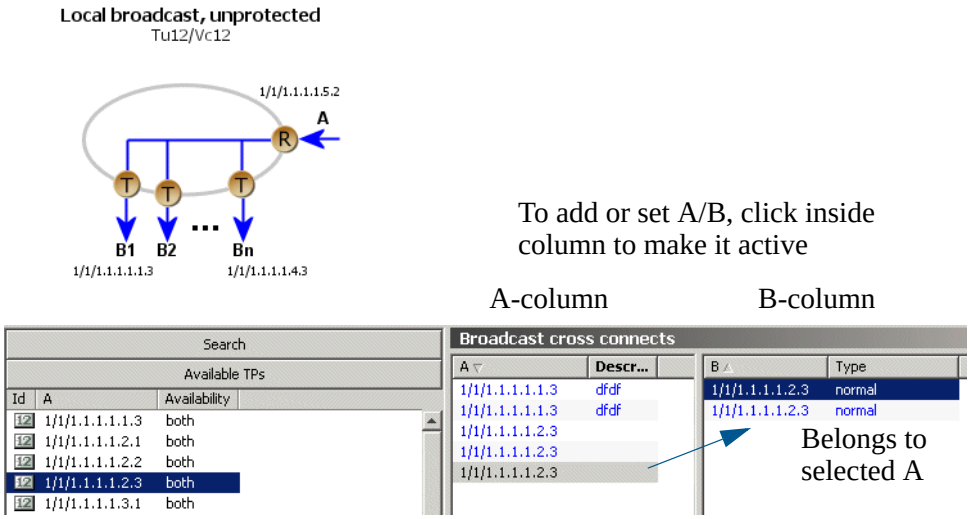


Figure 108 Broadcast columns

Add A and B TPs

1. Add A: doubleclick the available TP you want to be the A-end
2. Add B1-Bn: doubleclick the available TPs you want to broadcast to.

3. Add new A: Click inside the A-column to activate. Then doubleclick to add, or select an available TP and click the Add button.

4. After A is selected, further Doubleclick adds B-ends in the B-column.

TIP! First doubleclick selects A-end, and further selects B-ends under this A-end.

Edit A and B TPs

- Edit an A-end:

1. Select the A TP you want to change in the A-column.

2. Select the available TP you want to change to

3. Press the Set A button and save

- Edit a B-end:

1. Select the B TP you want to change in the B-column.

2. Select the available TP you want to change to

3. Press the Set B button and save

8.6.12 Modify cross connections

A cross-connection is a relationship between termination points and the relationship cannot be modified after it has been created.

It is not possible to modify the Direction (bi-directional or unidirectional) of a cross-connection in the supported release of AXX 9200 EDGE. The only parameter that can be modified is the description of the cross-connection.

Cross-connections can be protected after they have been created. See 8.6.13.

8.6.13 Protect PtoP cross connections

The A-end or B-end of a cross-connection can be protected by the SNC protection scheme when a cross-connection is being set up or after the cross-connection has been set up.

NOTE! When the cross-connection is uni-directional and protectedTp is “a”, a static bridge will be created from the A-end to the B and Protection termination points. (SNCP parameters are not used).

NOTE! When the cross-connection is uni-directional and protected TP is” b”, an SNC protection switch is created where the signal from A is working connection and the signal from Protection is protection connection. In this case the SNCP parameters are available after the cross-connection has been saved.

1. Open the **Cross-connection Manager** from the **Equipment** menu.
2. Set the **ProtectedTP** attribute to **a** or **b** for **one** or **more** cross-connections. This is the termination point you want to protect.
3. Select the **cross-connection** you want to protect.
4. Select the **Available TP List** in the Content panel.
   The list contains the free TU12/VC12 or TU3/VC3 or AU-4 termination points in AXX 9200 EDGE.

NOTE! If the Available TP List in the Content panel does not show the termination points that you want to protect your WAN channel with, you have to make sure they are made available for cross-connection. See “Configuring SDH port structure (channelization)” on page 385.

NOTE! You can protect bidirectional or unidirectional cross-connections. In the Available TP list you will see whether the termination point is available in both directions or as A-end or B-end.

5. Select the **termination point** that you want to protect your **a or b-end** with.
6. Click on the **Set Prot** button 

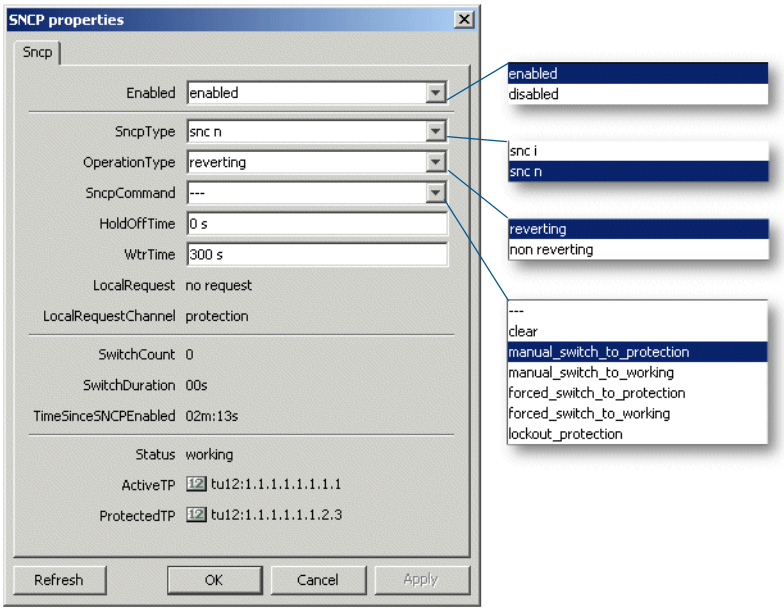
in the toolbar. The protection TP is filled in for the selected cross-connection.
7. Click **Save** on toolbar.

NOTE! By default the protection is disabled and will not work before it is enabled. Follow instructions below to enable SNC protection.

SNC protection

8. Select the **cross-connections** where **you want to enable** protection. (SHIFT and CTRL buttons can be used for multiple selection).
9. Click the **SNCP** button 

in the toolbar
10. Set the **Enabled attribute** to enabled and click **OK**.



NOTE! It is not possible to modify the Protection termination point after it has been saved. If you want to modify, the ProtectedTP must first be saved as “none”. Then the Protection TP can be modified. Remember to set the ProtectedTP back to a or b.

Modify protection parameters of a cross-connection

A-end or B-end of cross-connections are protected as described in “Protect PtoP cross connections” on page 431. The SNC is then set

up with a number of default parameters. The parameters can easily be modified:

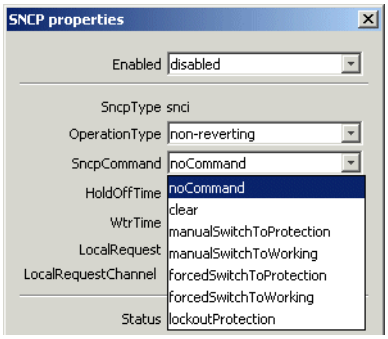
1. Open the **Cross Connection Manager** from the **Equipment menu**.
2. Select a **cross-connection** in the Cross Connection Manager.
3. Select the **cross-connections** where **you want to modify protection** parameters (SHIFT and CTRL buttons can be used for multiple selection).
4. Click the **SNCP** button 

in the toolbar
5. Modify the **SNC protection parameters** and click OK.
6. Click **Save** on toolbar.

8.6.14 Command cross-connection protection switch

You can control the SNC protection switch by sending a command.

1. Open the **Cross Connection Manager** from the **Equipment menu**.
2. Select the **cross-connections** where **you want to modify protection parameters** (SHIFT and CTRL buttons can be used for multiple selection).
3. Click the **SNCP** button in the toolbar
4. Select the **SncpCommand** and click **OK**.



Depending on the priority of the command and current status of each channel, a switch may now take place for some or all selected cross-connections.

8.6.15 Delete cross connections

1. Open the cross-connection GUI by selecting **Cross connection Manager** from **Equipment menu**.
2. Select **the panel for the type** of cross-connection(s) you want **to delete** (VC/TU12, VC/TU3 or VC/AU-4).
3. Select the **cross-connections** that you want **to delete**.
4. Click **Delete** on the toolbar
5. Click **Save** on toolbar.

8.6.16 Advanced cross-connection operations

For frequent users of AXX 9840 INSITE, it is possible to make use of the enhanced editing facilities to speed up the configuration work.

8.6.16.1 Set up multiple cross-connections by multiple selection

1. Select the **Termination points** that you want **to use as A-ends**. Use SHIFT or CTRL buttons to select more than one termination point.
2. Click **Add** on toolbar. The same number of cross-connections as the selected TPs are created with the A-end filled in.
3. Select the **TU12 termination points** that you want **to add to the B-ends** of the cross-connections in the same way.
4. Click the **Set B** button on the toolbar.
5. If you want **to protect** the connections, select the **TU12 termination points** that you want to **add to the cross-connections**.
6. Click the **Set Prot** button on the toolbar. Remember to **set ProtectedTP** to **a** or **b**.
7. Save.

NOTE! You are only allowed to set the B or Protection termination points of cross-connections where B or P are not in use.
If you want to modify the A or B termination point the cross-connection must be deleted and created again.
If you want to modify the Protection termination point the ProtectedTP must first be saved as none. Then the Protection TP can be modified. Remember to set the ProtectedTP back to a.

NOTE! If you do not select the same number of instances of cross-connections and termination points, the A or B end will be filled in with as many TPs as available, starting from the top of the selected cross-connection list. If more TPs are selected than cross-connections, the last TPs will not be used.

8.6.16.2 Set up multiple cross-connections by repeated operations

1. Double click the **termination point** you want **to use as A-end**. A new cross-connection is created.
2. Double click the **termination point** you want **to use as B-end**. B-end is filled in.
3. Repeat **1** and **2** for as many cross-connections as you want.
4. Click **Save** on toolbar.

8.6.16.3 Enter termination points manually:

1. Add a **new cross-connection**.
2. Click on the **A**, **B** or **Protection termination points**. A list of slots appears.
3. Select **a slot**. A list of ports appears.
4. Select **a port**.
5. Continue selecting each of the **CBKLM values**.
6. Enter the information the same way (or select from list of free TPs) for the other termination points.
7. Save.

NOTE! The information can also be entered directly without selecting the numbers from the drop down list. Remember to use the following format: <slot/port/C.B.K.L.M>

8.7 AXX 9300 METRO Cross Connection Management

8.7.1 Introduction

This section describes the management of a cross connection between two SDH/PDH ports. Parts of the flow are automated to improve user friendliness.

Cross connecting between the high-order and low-order matrix is a part of the automatic structuring feature of the AXX 9300 METRO, and is not a manual operation to be done by a user.

When cross connecting, you select between actual and potential termination points in the cross connection matrix.

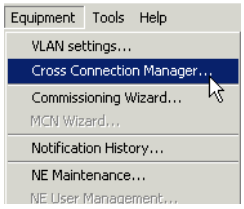
- Potential termination points represent unstructured capacity.
- Available termination points represent structured, but not cross connected capacity in the cross connect.

Procedure: **CREATE A CROSS CONNECTION BETWEEN SDH PORTS**

Creating one cross connection may imply the creation of additional physical cross connections between the high-order cross connection and VC4 floating termination points during automatic structuring.

AUs or TUs are cross connected between SDH ports. The number of SDH ports involved depends on the selected protection scheme. The number of physical cross connections depends on the configuration state of the cross connect.

1. Open the Cross Connection Manager. The GUI may be scoped to a targeted network element, depending on the context it was opened in.



2. Select type of cross connection:

- Point-to-point
- Drop & continue (p-t-p)
- Double add and drop)
- Broadcast

3. Select the AU or TU layer in which the cross connection shall be performed, and the AXX 9840 INSITE presents the actual and potential termination points available for cross connection.

4. Select the non-protecting branches of the cross connection from a selection of free actual and potential termination points. You cross connect the protecting branches from a selection of un-used actual and potential termination points:

- AXX 9840 INSITE presents the AU/TU termination points available for cross connections
- Select the 'A', 'B' termination points for cross connection.

5. The user selects the circuit protection scheme (if any) and protecting termination point. The default is no protection. The available choices are:

8.7.1.1 Point-to-point XC:

- No protection
- Protection on floating VC4 (if cross connecting below floating VC4)
- Protection on TU or AU point-to-point cross connect
- Combinations of the above

8.7.1.2 Broadcast XC:

- Broadcast or continue broadcast, no protection
- Protection, combinations (one or both) of:
  - Broadcast protection
  - Continue protection

8.7.1.3 Point-to-point drop & continue

- Protection is a mandatory feature of this cross connection structure, and not selectable.

8.7.1.4 Ring-to-ring XC (double add and drop, double drop and continue)

- Protection is a mandatory feature of this cross connection structure, and not selectable.

6. Define the cross connection configuration parameters:

- Common parameters such as directionality.

NOTE! Broadcast cross connections are always uni-directional, and
complex ring-to-ring cross connections are always bi-directional.

- Optional protection parameters (revertive, non-revertive, timing parameters etc.)

7. Commit the cross connection to the network element and the AXX 9840 INSITE controls the required sequence of actions:

- Automatic structuring to convert a potential termination point to an actual termination point:
  - Structuring the parent SDH port AU area, if required
  - Cross connection to a floating VC4 termination point, if required.
  - Structuring the parent SDH port TU area, if required.
- AXX 9840 INSITE performs the actual protected or un-protected cross connection.

8. AXX 9840 INSITE reverts with completion status and terminates the workflow:

- If OK, the workflow is completed.
- If not OK, the system presents a "probable cause" diagnostic, and performs an automatic rollback to the original state:
  - Termination points are freed up.
  - Cross connection branches are removed.
  - Any automatically generated structuring is un-structured, including floating VC4 cross connections.

8.7.2 Create a PDH port termination

This procedure terminates an SDH port AU or TU in a PDH E1 or E3/T3 port. E1 ports are terminated in VC12s, and E3/T3 ports are terminated in VC3s.

NOTE! The PDH ports are grouped into PDH groups where the PDH ports under the group shares a common structuring configuration.

The PDH group may be:

- **Un-structured:**
  All the PDH ports under the group is unstructured, and their VC4, VC3 or VC12's does not appear as actual termination points in the XC GUI.
- **Structured down to the designated VC/TU layer:**
  All the PDH ports under the group are structured down to the designated TU layer, and is cross connected from the high-order to the low-order VC4 floating termination points through the same floating VC4.
- **VC4-tunnelled:**
  All PDH ports under the port group is terminated in a VC4, that is available for cross-connection to an SDH port AU-4.

When the port group is un-structured, all VC3 or VC12 termination points appear as potential in the XC GUI, and the system is required to define the structuring mode for the port group. If the port group is structured, all VC3 or VC12 termination points (and VC4 for E3 tunnelling) will appear as actual termination points in the XC GUI.

Procedure: **CREATE A PDH PORT TERMINATION**

1. Open the XC GUI.
2. Select the AU or TU layer in which the termination shall be performed.
3. Select the PDH port and the SDH port timeslot to terminate:

- If a PDH port group is un-structured, all the PDH port group ports will appear as potential in the GUI
- If a PDH port group is structured, all the PDH port group ports will appear as actual in the XC GUI.
- If a PDH port group is structured in another layer (for instance VC4 tunneling mode when attempting termination in the VC3/TU3 layer), no PDH ports belonging to the group will appear as actual or potential.

4. Define the termination common parameters (ID, directionality, description etc.)

5. Commit the termination, and the AXX 9840 INSITE performs the required sequence of actions:

- If the port group is unstructured, the following actions is performed by AXX 9840 INSITE:
  - Structuring to the designated layer (VC3 or VC4 tunnel for E3, VC12 for E1).
  - Unless an E1/E3 VC4 tunnel is created: create a path from the PDH port group to the low-order cross connection through a floating VC4 termination point.
  - Structuring the port group from the cross connected floating VC4 to the targeted TU/VC layer
- AXX 9840 INSITE cross connections the targeted PDH port VC to the selected AU (VC4 tunneling) or TU in the SDH port.

6. The system reverts with completion status:

- If OK, the workflow is terminated.
- If not OK, the system presents a 'probable cause' diagnostic to the user and awaits a response with the following choices:
  - Modify the termination parameters and retry
  - Cancel the termination. When canceling the termination, AXX 9840 INSITE performs an automatic rollback to free up any reserved resources.

Any automatically generated SDH structuring is un-structured. Any automatic PortGroup configuration associated with the current workflow is reversed (including un-structuring of PDH port group ports).

8.7.3 Edit a cross connection or PDH termination

Editing an SNC implies:

- Changing the cross connection path properties (directionality etc.)
- Changing the protection scheme

- Modifying the protection attributes
- Adding or removing protection branches

The flow is identical to the “” on page 436, and omitting the steps for properties you don’t want to change.

If an SDH protecting branch is reassigned, the TMN system performs re-structuring as required. If automatic un-structuring is enabled, the original protecting branch is un-structured automatically.

NOTE! The type of cross connection (point-to-point, broadcast, add and drop, drop and continue) is not available for editing. In such cases the cross connection must be deleted and re-created.

8.7.4 Delete a cross connection or PDH termination

This procedure deletes a cross connection, including all physical cross connections and TP reservations

1. Select the cross connection and activates deletion

2. The AXX 9840 INSITE performs the following tasks:

- Requesting the user if cross connections to floating VC4 terminations with SNCP shall be removed or not.
- The physical cross connections are removed
- If the automatic un-structuring is enabled, AXX 9840 INSITE un-structures the parts of the SDH port(s) that were used in the context of the deleted cross connection instance:
  - Un-structuring the low-order cross connection as far as possible without impacting exiting cross connections in the low order matrix
  - If yes to removing SNCP floating VC4 terminations, un-structure the high-order cross connection as far as possible without impacting existing cross connections in the high order matrix.

3. The system reverts with a completion status.

- If OK, the workflow terminates.
- If not OK, the system presents diagnostics with details on the cause and location of the failure(s), and the workflow terminates.

The cross connection is still available in the TMN system for you to perform corrective operations.

8.8 Alternative procedures

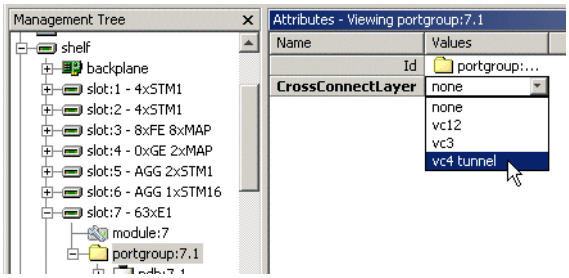
8.8.1 Setting the PDH port group layer rate

If required, you can manually pre-provision the PDH port with a layer rate different from the default "un-structured". This is done in the Management Tree on the PortGroup object, and is implemented on all PDH ports belonging to the port group.

Pre-provisioned layer rates creates actual VC4(tunneled), VC3(E3/T3) or VC12 PDH termination points under a PDH port group. If un-provisioned, all PDH termination points belonging to the port group will be potential.

Structuring:

1. Select the PDH port group>CrossConnectLayer as shown in the figure below:.



2. Select the PDH port group configuration with the desired layer rate:

   - E1 port:
     - Un-structured
     - Structured down to VC12/TU12
     - VC4-tunneling of the up to 63 PDH ports belonging to the port group.
   - E3/T3 port:
     - Un-structured
     - Structured down to VC3
     - VC4- tunneling of the 3 PDH port group

3. Save to commit the selection to the NE, and AXX 9840 INSITE implements the PDH port group configuration:

   - Structuring the PDH port group to the designated layer rate (AU-4, TU3 or TU12), and performing any necessary floating VC4 cross connection.

- Un-structuring the PDH port group, and removing any associated floating VC4 cross connections.

8.9 Actual and potential cross connection capacity

The cross connection or termination capacity available depends on the structuring of the SDH ports and PDH port groups of the network element. Structured, un-used capacity is actual capacity and un-structured un-used capacity is potential capacity.

Potential capacity represents the ports unstructured capacity, and is calculated for each AU/TU layer as the capacity available when structuring all of the remaining payload capacity for that layer only.

- A fully structured SDH port offers a fixed pre-defined the set of AU and TU containers available to the XC for cross connection.
- An un-structured SDH port offers potential AU and TU capacity only. The capacity will not be available until the port is structured (manually or automatically, see chapter 4.2) down to the designated targeted level.
- A partially structured SDH port will offer a mix of pre-defined and potential capacity to the XC. The selection of structured or unstructured capacity when cross connecting is done automatically according to a pre-defined set of rules, or manually by the user.
- PDH capacity is structured per PDH port group, and is common for all ports within a port group.

The TMN XC special GUI presents both actual and potential capacity during the workflow.

The TMN XC special GUI presents the usage (or availability) of cross connected VC4 termination points.

8.10 SDH Protection Management

8.10.1 Introduction

The purpose of this section is to guide you through management of the 1+1 linear Multiplex Section Protection (MSP) between two SDH Ports.

The section involves management of the complete life cycle of an MSP, including creation, presentation, modification, deletion and manual operation the MSP switch.

8.10.1.1 Multiplex Section Protection

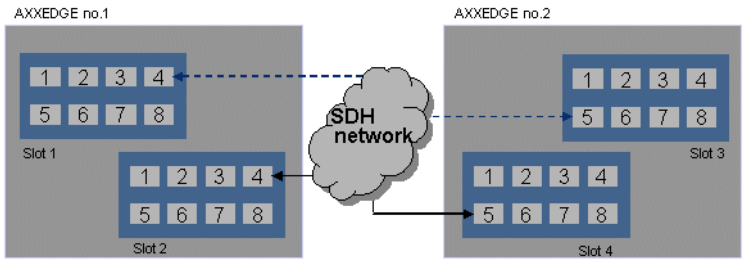


Figure 109 1+1 MSP between two AXX 9200 EDGE

The 1+1 MSP provides protection of the SDH ports by replacing the supporting trail when it fails as illustrated in Figure 109 This is a 100% redundant protection scheme.

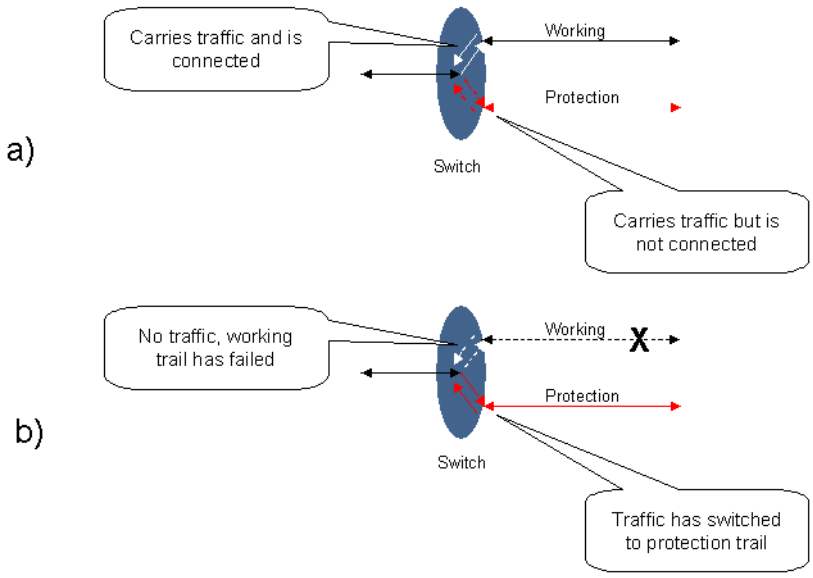


Figure 110 Protection switching scenarios

Both working and protection trails are enabled and the signal is bridged to both, see Figure 110 - a). The received signal from the working trail is forwarded to the receiving client while the protection is not. If the working trail fails and a switch is performed, the traffic on the protection trail is received by the client, see Figure 110 - b). Traffic from working trail is ignored. The network element uses a bi-directional switching protocol, i.e., both ends of the trails switches simultaneously. To synchronize this simultaneously switching, the network elements signal to each other in the K1&K2 bytes in the MS overhead of the SDH traffic. A bi-directional switching protocol gives a better control of the traffic in the network but uses a little more time to perform the switching than a uni-directional switching protocol does.

The switching has two different modes:

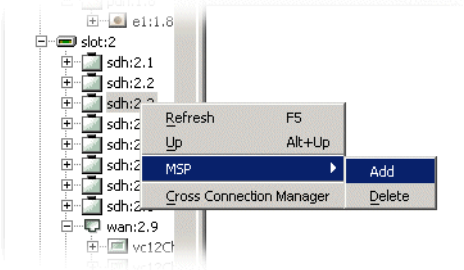
- **Revertive**- traffic returns to the working trail when recovered
- **Non-revertive**-traffic stays on protection trail indefinitely or until told otherwise

The time to wait before restoring the trail can be defined.

When switching either from or to protection, an event notification will be emitted.

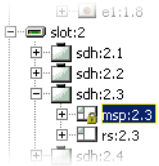
8.10.2 Protect section by MSP

1. In the Management Tree right click the **sdh port** that should be the Working port.



2. Select **Add** in the pop-up menu. An **msp object is created** below the port.

3. Select the **msp** object in the Management Tree.



4. Select **Protection Slot and Port.**
   The list will only contain ports when the conditions below are fulfilled:

   - Working and Protection port must be selected from slot 1 and 2 or 3 and 4. E.g. it is not possible to set up MSP protection with Working port from slot 1 and Protection port from slot 3. Working and Protection ports can be selected from the same slot.
   - A Protection port must be unstructured on the highest structurable level:

     AXX 9200 EDGE Release 1.1 / 1.0:
     - aug1.

     AXX 9200 EDGE Release 2.0:
     - aug4 for STM-4 and STM-16,
     - aug1 for STM-1.

NOTE! STM-4 and STM16 ports on AXX 9200 EDGE release 2.0 and later are automatically structured to the AUG-1 level and must manually be
un-structured to the AUG-1 level.

(See “Modifying or removing AXX 9200 EDGE SDH port structure” on page 5 -5).

   - The port must not be connected to a remote module.
   - Working and Protection port must both have the same STM-N rate.
     E.g: both STM-1.

5. Select **Protection Slot and Protection**.

6. Use **default** or **fill in new values** for the other attributes.

7. Save.

The MSP scheme is created in AXX 9200 EDGE and starts working immediately. You will also see that the same msp object is now

available under the protection port. You will also see that if the msp has the same Object identifier (e.g. 1.2.) as the parent sdh port, the port is a Working port. If it has a number that is different from the parent sdh port (e.g. sdh port is 1.4 and msp is 1.2) it is a Protection port for the sdh port with the same Object Identifier as the msp object.

NOTE! Working and Protection port must be selected from slot 1 and 2 or 3 and 4. E.g. it is not possible to set up MSP protection with Working port from slot 1 and Protection port from slot 3. Working and Protection ports can be selected from the same slot.

NOTE! A Protection port must be unstructured (See “Modify or remov AXX 9200 EDGE SDH port structure” on page 389).

NOTE! Working and Protection port must both have the same STM-N rate. E.g: both STM-1.

8.10.2.1 Modify MSP

1. In the Management Tree right click the **sdh port** that is the Working port.
2. Select **msp object** below the sdh port.
3. Modify the **attributes** of the MSP scheme.
4. Click **Save** on toolbar.

NOTE! If the link is operating on the Protection section in bidirectional mode, you may brake traffic if you set the MspEnabled to disabled or OperatingMode to unidirectional in one of the nodes This is due to the behavior of the APS protocol).

NOTE! To avoid problems always make sure the link is operating on the Working section and to command it to lockout of protection before making the modifications.

8.10.2.2 Delete MSP

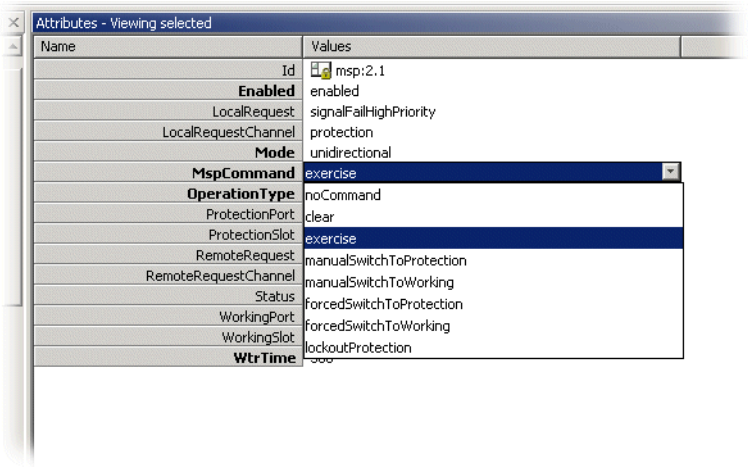
1. In the Management Tree right click the **sdh port** that is the Working port.
2. Select **MSP** and **Delete** in the pop-up menu. The msp object disappears both from the Working port and the Protection port in the Management Tree.
3. Save.

NOTE! Be aware that it is possible to delete an MSP when traffic is on Protection Section. This will cause a short break during switchover time. (If Working section is available).

NOTE! To avoid problems always make sure the link is operating on the Working section and to command it to lockout of protection before deleting the MSP.

8.10.2.3 Command MSP switch

1. In the Management Tree right click the **sdh port** that is the Working port.
2. Select **msp** object below the sdh port.
3. Select one of the commands under **MspCommand**.



4. Save.

NOTE! Commands will only take place if there are no higher priority requests in the system.

NOTE! A new command will clear the current command before executing the new command. In this case the new command may not be executed when the new command has lower priority than the old command because the MSP will search for the request with highest priority present. E.g. sending a Manual Switch to protection command instead of a Forced Switch to protection command will not work if there is a Signal Degrade request on the Protection section.

NOTE! All commands can be cleared by the clear command.

8.10.2.4 Legal combinations of SNCP and MSP

It is possible to use both SNCP and MSP in an AXX 9200 EDGE simultaneously, as long as the following is satisfied:

- The PROTECTED SNCP entity can be part of an MSP protected port, but the WORKING or PROTECTION entity can not.

Consider the example; an STM-4 ring where some TU12s are dropped off the ring and sent to an AXX155E via an STM-1 link. In this case, SNCP can be used in the ring, protecting the TU12s to be dropped from the ring towards the AXX155E. MSP can then be used for the STM-1 link to protect the traffic between the AXX 9200 EDGE and the AXX155E. This is because the TU12s that are dropped from the ring are the “Protected” TU12s, while the TU12s in the ring are the “Working” and “Protection” TU12s. Consequently, it is not possible to use MSP on the “East” or “West” links of the ring, since the TU12s that are carried here are the “Working” or “Protection” part of the SNCP protected paths.

8.10.3 SubNetwork Connection Protection

SNCP is strongly related to the cross-connection that is protected in the network element. In AXX 9840 INSITE SNCP related issues are handled from the cross-connections GUI.

NOTE! The maximum number of SNCP instances that can be used with guaranteed switching time below 50 ms, is 252. This corresponds to one full STM-4 (or four STM-1s) structured into TU12s. These 252 SNCP instances can be a mixture of AU-4, TU3 and TU12 in any combination, and taken from any C.B.K.L.M address within an STM-1/4/16. A larger number of instances than 252 may be used, but in this case we cannot guarantee switching times below 50 ms.

The resolution of the Hold-off timer is N x 100ms +/- 60 ms. I.e. for a 500 ms Hold-off timer, the real timer value may be any value between 440 ms and 560 ms.

The Working, Protection and Protected parts of an SNCP protected path can be carried over different link rates. E.g. for an SNCP protected TU12, the Working TU12 could be carried over an STM-16 link, while the Protection TU12 could be carried over an STM-4 link.

8.10.3.1 Protect connection by SNCP

See “SNC protection” on page 432

Modify SNCP

See“Modify protection parameters of a cross-connection” on page 432

Command SNCP switch

See“Command cross-connection protection switch” on page 433.

SNC Protected Uni-directional Cross-connection Limitations

NOTE! When one direction of a path forms part of an SNC protected uni-directional cross-connection, the other direction can not form part of a different SNC protected uni-directional cross-connection. But the two directions can form part of two different uni-directional un-protected cross-connections. This applies to uni-directional cross-connections on all path layers. Suppose the uni-directional VC-12 cross-connection from 1/1/1.1.1.1.1 (input) to 1/2/1.1.1.1.1 (output) is SNC protected by 1/3/1.1.1.1.1 (input). In this case, the output direction of 1/1/1.1.1.1.1 and 1/3/1.1.1.1.1, and the input direction of 1/2/1.1.1.1.1 are un-used. However, due to the above mentioned limitation, they can not be part of a new SNC protected uni- directional cross-connection, e.g. from 1/2/1.1.1.1.1 (input) to 1/1/1.1.1.1.1 (output) protected by 1/14/1.1.1.1.1. They may however form part of un-protected uni-directional cross-connections.

See “Circuit protection for uni-directional VCAT” on page 468.

8.11 SDH Cross Connection Management

8.11.1 Introduction

The purpose of this section is to describe the tasks involved when managing cross connections between termination points on the network element.

The section involves management of the complete life cycle of a cross connection, including creation, presentation, modification, deletion and manual operation of the sub-network connection protection switch.

A cross connection is defined by its termination points. Only termination points with the same characteristic information can be cross-connected. The characteristic information of a termination point defines the format of the signal that can be transferred by this termination point. Format defines the capacity of the signal, e.g. TU12 and VC-12 have the same characteristic information since they both have a 2 MBits traffic capacity.

For the different NE types Unidirectional and bi-directional XCs with or without protection are supported with XC types according to the table below.

XC type	AXX 9300 METRO	AXX 9200 EDGE	AXX 9100 CONNECT
Point to Point	**X**	**X**	**X**
Drop & Continue	**X**	**-**	**-**
Double Add & Drop	**X**	**-**	**-**
Broadcast	**X**	**-**	**-**

Table 14 XC type support for the different NEs

The first part of this section gives a short introduction to SDH layers and cross connections which is meant to help the reader in understanding the requirements specified in this document. For further reading on SDH and cross connections, please see ITU-T Recommendations G-Series.

8.11.1.1 SDH layer network and cross connections

An SDH network has a layered structure as depicted in Figure 111 The layers operate in a client/server based scenario. The

service layer generates the bit streams that are to be carried across the SDH network. This layer is not part of SDH. The path layer is a virtual layer and can only be observed through a management system. It is in this layer the cross connection management and structuring of the SDH ports are performed. The path layer works on containers.

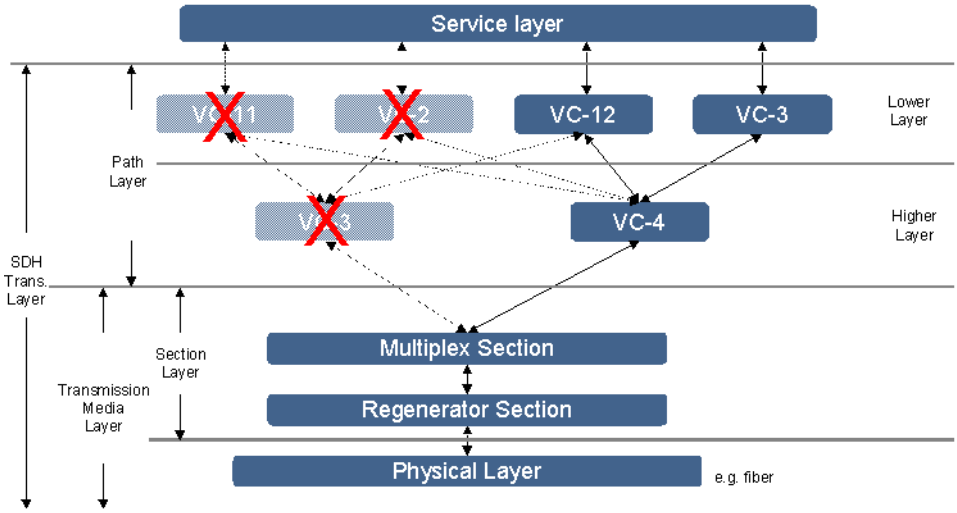


Figure 111 SDH layer network

8.11.1.2 SDH port structuring

The multiplexing structure of the SDH ports determine which layers and their termination points that are available to be cross connected. The multiplexing structure for SDH in all layers are shown in Figure 112 (taken from ITU-T Recommendation G.707.) The C.B.K.L.M value determines the path trough the structure. The usage of the C.B.K.L.M value follows the rules defined in Table 1.

Only traffic on non-terminated containers called connection termination points can be cross connected, i.e. AU-4, TU3, and

TU12. The other containers, VC-4, VC-3, and VC-12, represent trail termination points where the traffic can be "read."

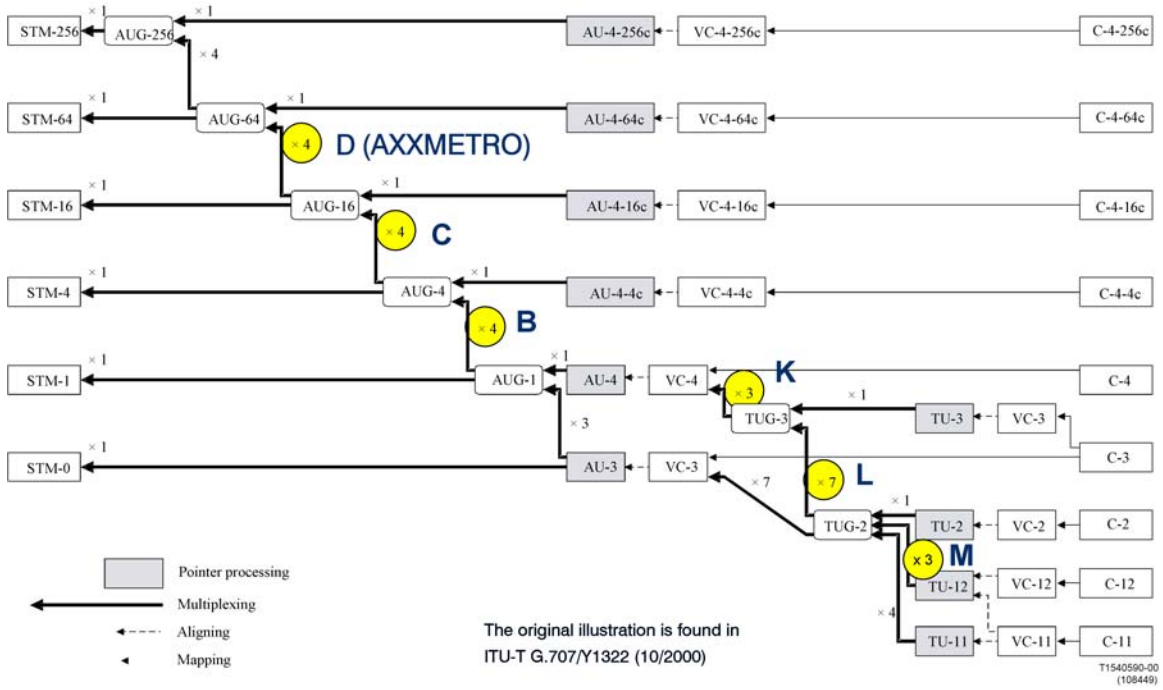


Figure 112 SDH multiplexing structure

8.11.1.3 D.C.B.K.L.M value usage

Rule	**Example**
When referring to SDH objects the complete D.C.B.K.L.M value is used even if some fields are in-significant.	
Not significant fields in D.C.B.K.L.M are set to 0.	AU-4 in STM-16: C.B.**0**.**0**.**0** TU3 in STM-16: C.B.K.**0**.**0**
C identifies which AUG-4. If no AUG4 exists, its is set to 1, like a phantom AUG4.B identifies which AUG-1. If no AUG-1 exists, its is set to 1, like a phantom AUG-1.	STM-1: C = **1**, B = **1** There is **one** AUG-1 in STM-1 and a phantom AUG4 STM-4: C = **1**, B = **1** - **4** There is one AUG4 in STM-4 STM-16: C = **1** - **4**, B = **1** - **4** Example: AU-4 in STM-1: **1**.**1**.0.0.0 TU3 in STM-4: **1**.**3**.3.0.0 TU12 in STM-16:**2**.**4**.2.7.2

Rule	Example
The C.B.K.L.M value is used for VC objects associated with E1, E3, and E4 modules but the C and B values are always 0.	VC-12 on E1 module: **1.1.1.1.1** Protecting: **1.1.1.1.2** VC-3 on E3 module: **1.1.1.0.0** Protecting: **1.1.2.0.0** VC-4 on E4 module: **1.1.0.0.0** (not release1) Protecting: **1.2.0.0.0**
For VC objects for WAN	VC-12 on E1 module: **1.1.x.y.z** VC-3 on E3 module: **x.y.z**.0.0 (not release 1) VC-4 on E4 module: **x.y**.0.0.0 (not release 1)
Combination 0.0.0.0.0 is not a legal value and can be used as en error code.	

Table 15 D.C.B.K.L.M value usage

NOTE! The D value in D.C.B.K.L.M is only supported by the AXX 9300 METRO NE, see Figure 112

8.11.1.4 Cross connection management

Cross connection management is the management of connectivity within the NE itself. Cross connections (XC) are set up between connection termination points with the same characteristic information, e.g., cross connections between AU-4s, or between TU3s, between VC-12 and TU12, or between two VC-12s.

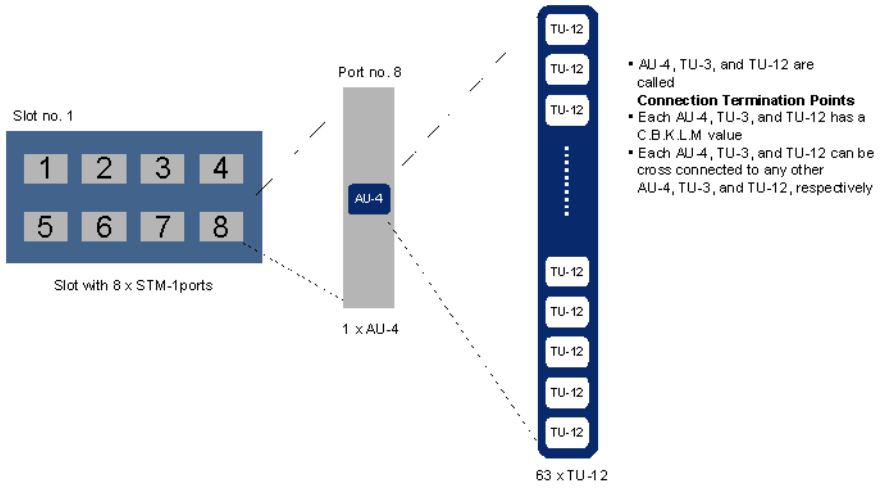


Figure 113 Slot - port - CTP relations

In AXX 9200 EDGE there are four slots that can hold an SDH module. The module can be of different types, i.e., STM-1, STM-4, or STM-16. In this document the STM-1 module with 8 ports is used as an example.

In addition the AXX 9200 EDGE can have PDH modules with a number of E1 or E3 ports. The E1 and E3 ports have a corresponding VC-12 or VC-3, respectively. These VCs can be cross connected to termination points on the SDH modules or with each other.

Example

A slot with an 8 x STM-1 module has eight ports. Available CTPs on Port no.8 in Slot no. 1 are shown in Figure 113 . There is one AU-4 on the port and depending on the structuring of the AU-4 container, there are 63 TU12s, 3 TU3s, or a combination of TU12s and TU3s since the TUG-3s can be structured independently, which can be cross connected. This means that in this single slot there are 8 x 63 = 504 CTPs (maximum) in the lower layer and 8 x 1 = 8 CTPs in the higher layer.

What are the possible CTPs to be cross connected to?

If we assume that all four slots in this AXX 9200 EDGE are equipped with 8 x STM-1 modules there are 3 x 504 = 1512 possible choices for the connecting CTP in the lower layer and 8 x 3 = 24 in the higher layer. If an AXX 9200 EDGE is equipped with four STM-16 modules, each of these modules has 4 x 4 x 63 = 1008 TU12 CTPs. This means that the cross connection matrix in the fabric has the dimension 4032 x 4032.

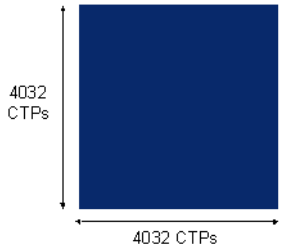


Figure 114 Largest possible cross connection matrix

This is a very large number of choices and impossible for a user to keep track of. In addition there are several different types of cross connections:

- Point-to-point

- WAN XCs (special type of point-to-point)
- Drop and continue (AXX 9300 METRO R1)
- Broadcast (AXX 9300 METRO R1)

These types can be with or without protection and uni-directional or bi-directional, see Figure 115 to Figure 120

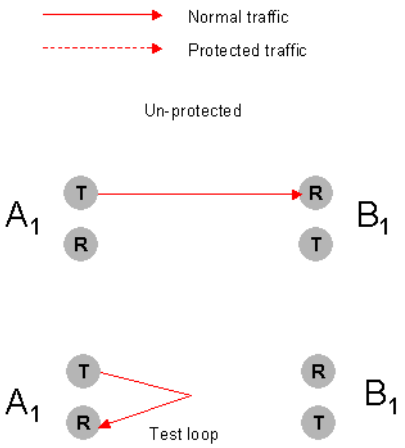


Figure 115 Unidirectional XC, un-protected

Un-protected, uni-directional cross connections can be used for test loops, as illustrated in Figure 115 A1

In Figure 116 protection has been set up for the termination point A1 and B2. The protected termination point A1 has no switching possibility since the cross connection is uni-directional, but termination point B2 has switching.

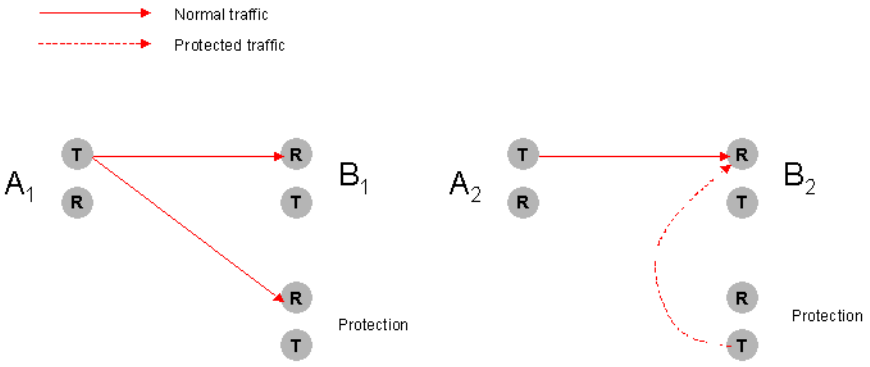


Figure 116 Uni-directional XC, protected

The bi-directional, un-protected cross connection is depicted in Figure 117 . For bi-directional cross connections all termination points have switching possibilities when protected. In Figure 118 the termination points A1 and B2 are protected, i.e. A1 can choose to receive from either B1 or the protection and B2 can switch between A2 or the protection.

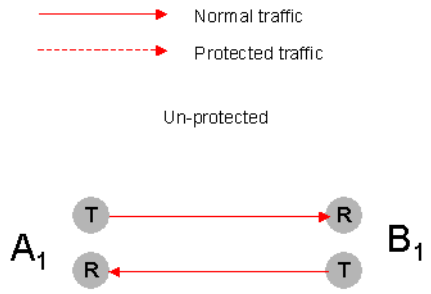


Figure 117 Bi-directional XC, un-protected

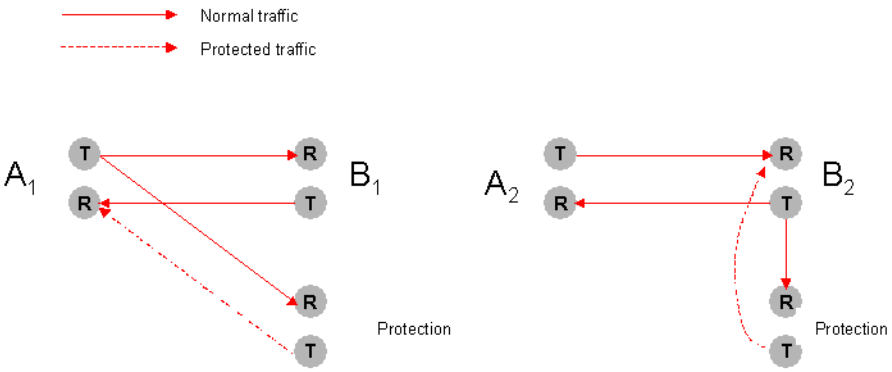


Figure 118 Bi-directional, protected

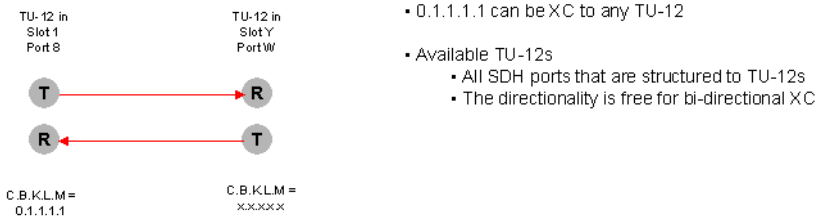


Figure 119 Example of bi-directional, un-protected, point-to-point XC

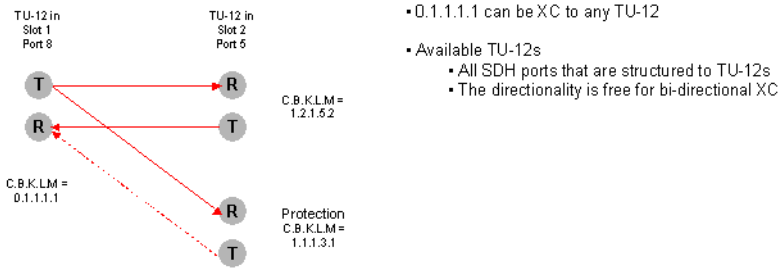


Figure 120 Example of bi-directional, protected, point-to-point XC

Examples of an un-protected, bi-directional, point-to-point cross connection and a protected, bi-directional, point-to-point cross connection are given in Figure 119 and Figure 120 respectively.

8.11.1.5 AXXMTRO Specific XCs

Point to Point Drop and Continue

This bidirectional XC can connect traffic between two SDH rings. Set up A towards the source, B towards the other ring, and P is the alternative protecting route.

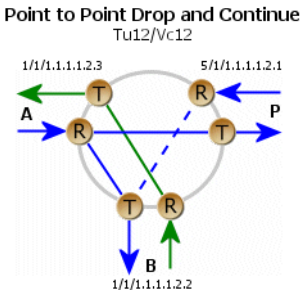


Figure 121 Example of Point to Point Drop and Continue

Broadcast

A broadcast cross connection is a uni-directional point-to-multipoint cross connection, built from one basic frame and several broadcast legs.

A broadcast cross connection can be viewed as a complex attribute, consisting of several basic PtP XCs that shares the same A termination point.

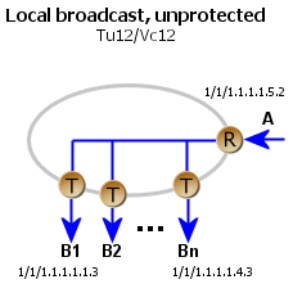


Figure 122 Example of Broadcast XC

The two types of Broadcast XC

- Local broadcast - unprotected:
  One broadcast input termination point (A) with several drop-off legs to termination points B<n>. "A" TP is mandatory, "B" TP's can be added or deleted. At least one "B" TP is mandatory.
- Continue broadcast - unprotected:
  One pass-through broadcast input/output termination point "A" and "C" with several drop-off legs to termination points "B<n>". "A" TP is mandatory, "B" and "C" TPs can be added or deleted, but at least one "B" or "C" TP is mandatory.

Double Add and Drop

Protected ring interconnection with protection where two rings enters the network element. Includes two SNCP instances. This cross connection scheme assumes that fully protected ring-to-ring interconnection is implemented by one network element.

Pro: Less costly, requires only one network element.

Con: Complex construct, single point-of-failure

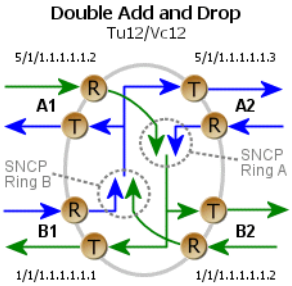


Figure 123 Example of Double Add and Drop XC

8.12 Ethernet mapping with VCAT/LCAS

8.12.1 Introduction

The Ericsson AXXESSIT network elements[1] support different types of Ethernet over SDH (EoS) mapping, as shown in Table 16

This section describes Generic Framed EOS mapping. This mapping type is module dependent, see “VCAT and GFP mappers”. Generic Framed (GFP-F) mapping can be combined with VCAT[2], at VC-12, VC-3 and VC-4 level, and LCAS[3].

Presentation and initial configuration of other WAN port parameters are described in “Configuring SDH port structure (channelization)” on page 385. For Ericsson AXXESSIT proprietary, see examples given in previous sections, such as “Modify WAN Port capacity” on page 416.

Table 16 Ethernet mapping types and properties

Ethernet mapping types	**Properties**				**Comments**
	Packet encapsulation[a]	**Bandwidth control[b]**	**Directionality[c]**	**Standard[d]**	
Ericsson AXXESSIT proprietary[e]	Proprietary	VC channels	Bi-directional	Proprietary	WAN mapping not compatible with 3.rd party equipment WAN connection recovery from VC channel faults (proprietary).
VCAT without LCAS	GFP-F	VC channels	Uni-directional	ITU-T G.707.	WAN mapping compatible with 3.rd party equipment.

1. AXX 9300 METRO 1.0, AXX 9100 CONNECT 1.0,AXX 9200 EDGE 2.0, AXX155A 2.0 and AXX155E 3.0.
2. Virtual Concatenation.
3. Link Capacity Adjustment Scheme.

Ethernet mapping types	Properties				Comments
	Packet encapsulation[a]	Bandwidth control[b]	Directionality[c]	Standard[d]	
VCAT with LCAS	GFP-F	VC channels plus LCAS selective VC enabling	Uni-directional	ITU-T G.707.	WAN mapping compatible with 3.rd party equipment. WAN connection recovery from VC channel faults (LCAS).
Soft-LCAS	GFP-F	VC channels	Bi-directional	Proprietary	WAN mapping compatible with 3.rd party equipment. WAN connection recovery from VC channel faults (proprietary).

a. Method of encapsulating Ethernet packets prior to across the SDH mapped WAN.

b. Method of assigning SDH capacity to the WAN port.

c. Decides if uni- or bi-directional virtual containers (VC) are assigned to the WAN port when allocating SDH bandwidth.

d. Specifies according to which standard, if any, WAN-to-SDH mapping is performed.

e. The ethernet traffic is mapped into a number of VC-12 containers in a roundrobin fashion with an inverse multiplexer function. The IP traffic is mapped into one or a number of VC-12 containers. See previous sections.

8.12.2 About GFP, VCAT and LCAS

Generic Framing Procedure

The GFP, VCAT and LCAS standards provide a standardised way of allocating bandwidth for packet services through circuit switched networks such as SDH (and SONET[1]).

This standard ensure inter-operability between mixed vendor transport networks, providing the required support for establishing packet (Ethernet) services over a circuit switched transport network. This is required properties when extending packet switched networks in metro or national wide environments, and competes with today's emerging Metro Ethernet standards.

A main benefit of these standards compared to pure Ethernet/MPLS metro and national wide networks is that all the SDH benefits of network resilience provided by protection schemes (MSP, SNC) are maintained while still providing full Ethernet service interfaces at the endpoints of the transport network.

1. SONET is the American National Standards Institute standard for synchronous data transmission on optical media.

This also enables owners of existing SDH network infrastructure to adapt their existing networks to the mixed packet- and circuit switched client environments of today.

GFP is a generic format for encapsulating client-side data and control packets in order to enable controlled transport through a SDH network.

GFP is a method used to encapsulate and map packet traffic in a way that is optimal for transport through circuit switched (line switched) networks such as SDH networks. The packaging conserves both client-side data and control information transparently through the switched network.

The packaging process performs the following:

- Adding and removing GFP overhead at the entry/exit points of the transport network, providing administrative information to the SDH network to allow it to transport the packages through the network according to the client side quality requirements.
- Allow better bandwidth utilization through the SDH network when mapping packets to SDH transport channels by transforming client side line character stream coding (Layer 1 coding) to a more bandwidth efficient scheme.
- Providing generic support for transport network services such as VCAT and LCAS
- Adding packet (Ethernet) service information, allowing the SDH network the possibility to differentiate between client side service requirements at the same port (for example pint-to-point Ethernet services and multipoint-to-multipoint (LAN) services).
- Providing an end-to-end (near-end to far-end) management channel to be used by the VCAT/LCAS (or other) methods

GFP Performance Monitoring

The following performance parameters apply:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received

- Number of bad GFP frames received, based upon payload CRC calculation
- Number of HEC uncorrected errors

A degrade alarm is available for the error type PMs, which are:

- Number of bad GFP frames received, based upon payload CRC calculation
- Number of HEC uncorrected errors

The error type PMs is handled in a similar way as the SDH performance parameters. The non error type PMs is handled in the same way as the RMON counters, the non error type PMs are:

- Total number GFP frames transmitted and received
- Total number Client management frames transmitted and received

VCAT - Virtual Concatenation

VCAT provides efficient bandwidth allocation for mapped packet traffic in the SDH network. Bandwidth is provided by assigning a group of SDH VC's to transport the GFP packet belonging to a client interface.

VCAT is a standardized end-to-end method for better bandwidth utilization of the SDH channels by allocating SDH bandwidth in increments in steps corresponding to increments of the SDH specific VC bandwidth (nxVC12, nxVC3, nxVC4 etc.).

This is a non-proprietary method similar to, but exceeding the Ericsson AXXESSIT proprietary Ethernet port bandwidth allocation by using several VC12s to provide the required bandwidth.

VCAT allows using VC12s, VC3s, VC4s into VC Groups, routing it through selectable AUs/TUs on different ports. Further, it compensates for delays caused by different routes through the network, and assures that end-pint traffic is assembled in the same sequence as it was disassembled at the entry-points.

VCAT works similar to Ericsson AXXESSIT proprietary mapping, but has more features, and is ITU-T standardized.

LCAS- Link Capacity Adjustment Scheme

LCAS provides on-the-fly bandwidth adjustments within a VCAT VC Group by allocating or de-allocating VC's from the VC Group. This is normally done to remove failing VC's from a VCAT VC Group, and provides both failure resilience and rapid restoration of traffic capacity.

LCAS is a feature added to VCAT VC Groups, allowing for dynamic allocation and re-allocation of bandwidth in an operative Ethernet port.

LCAS is a standardized method to adjust the bandwidth of the packet transport channel through the SDH network on the fly. This bandwidth adjustment will typically be caused by the LCAS operative status of the different VC's used in a VCAT virtual circuit group.

GFP- F, VCAT and LCAS Alarms and Events

The following alarms and events apply to GFP, VCAT and LCAS:

Table 17 GFP, VCAT and LCAS alarms

Id	GFP	VCAT	LCAS	Defect ref.	Short description
exm	Xa			ITU-T G.806.	GFP ex-header ident mismatch
pfm	Xa			ITU-T G.806.	GFP payload FCS ident mismatch
lfd	X			ITU-T G.806.	GFP loss of frame delin.
plm	Xa			ITU-T G.806.	GFP payload mismatch
upm	Xa			ITU-T G.806.	GFP user payload mismatch
lom		Xb		ITU-T G.806.	loss of multiframe
sqm		Xb		ITU-T G.806.	sequence indicator mismatch
loa		Xb		ITU-T G.806.	loss of alignment for ch’s with traffic
gidErr			Xb		Group Id different for active ch’s
lcasCrc			Xb		CRC error detected
nonLcas			Xb		non-Lcas source detected
plcr			Xb		partial loss of capacity receive (rx)
tlcr			Xb		total loss of capacity receive (rx)
plct			Xb		partial loss of capacity transmit (tx)

Id	GFP	VCAT	LCAS	Defect ref.	Short description
tlct			Xb		total loss of capacity transmit (tx)
fopr			Xb		failure of protocol
sqnc		-		ITU-T G.806.	SQ numbers not consistent
acMstTimeout			Xc		ack Mst timeout
rsAckTimeout			Xc		RS-ack timeout
eosMultiple			Xa	ITU-T G.806.	two or more ch's have EOS
eosMissing			Xa		No channel has EOS
sqNonCont			Xa		missing SQ detected in set of channels
sqMultiple			Xa		equal SQ for two or more channels
sqOor			Xa		SQ outside of range
mnd			Xa		member not deskewable
ctrlOor			Xa		undefined for one or more ch's

Legend:

Xa: Alarms to be enabled.

Xb: Alarms are default.

Xc: Event notifications.

8.12.3 VCAT and GFP mappers

The following mapper modules[1] apply:

- Octal LAN 10/ 100Base- TX module with standard mapper circuits (8XFE-SMAP)
- Dual optical LAN 1000Base- TX module with standard mapper circuits (2XGE-SMAP)

8.12.3.1 VC level for VCAT

The VC available VCAT VC levels depends on the Ethernet port:

1. Reference: Check product documentation for further technical description.

Fast Ethernet

- VC-12-nv (n=1..50)
- VC-3-nv (n=1,2,3)
- VC-4-nv (n=1)[1]

Gigabit Ethernet[2]

- VC-3-nv (n=1..12)
- VC-4-nv (n=1..7)

The VC- level can be configured individually per mapper port. A mix of different VC- levels in one VC Group is not allowed.

NOTE! The number of available Ethernet ports varies between the different network elements. Mapping type is defined per Ethernet port, and will apply to all VCs in the VC Group assigned to the port.

The mapping is flexible, and can be done to several SDH ports per Ethernet port within the mapping layer[3]:

- VC12 channels to TU12
- VC3 channels to TU3
- VC4 channels to AU-4

8.12.4 VCAT and LCAS configuration modes

8.12.4.1 Uni- directional VCAT with LCAS

VCAT with standardised LCAS functionality is always uni-directional, which enables the possibility to have different capacity in each direction, but requires a separate capacity setup in each direction. For procedure, see “Uni- directional VCAT with LCAS” on page 470.

1. Apply to AXX 9200 EDGE.
2. See note 1.
3. Ethernet port mapping and layers: LAN-Layer 1 and WAN (Layer 2).

8.12.4.2 Uni- directional VCAT without LCAS

When VCAT is used without LCAS functionality, there is no mechanism for removing of a faulty VC container in a VC Group.

8.12.4.3 Bi- directional VCAT with soft-lcas

Bi-directional VCAT with soft-LCAS is a proprietary mapping mode. This mode has bi-directional symmetric capacity with proprietary functionality similar to standardised LCAS.

Faulty containers in a VC Group will be removed based upon the VC alarm condition or based upon RDI signalling (similar to Ericsson AXXESSIT proprietary mapping). This allows a VC Group to continue operation even if the VC Group has a failed member.

8.12.5 VCAT administrative bandwidth

Network elements use the administrative bandwidth[1] as a separate defined parameter, independent on the actual assignment of TP's[2].

Bandwidth (BW) control

The operative traffic capacity for VCAT enabled ethernet port is controlled by the administrative bandwidth for VC channels in a VC Group. **Within Capacity** is a BW control parameter[3] for the upstream traffic. This attribute is available in the Cross connection Manager and Management Tree, and will be ticked for VC channels running traffic. If a VC channel should fail and the capacity for VCG is reduced, the attribute will appear as not ticked.

Bandwidth for uni- directional VCAT

In uni- directional VCAT, the upstream (traffic flow towards the SDH ports) and downstream (traffic flow towards the Ethernet port) is routed in separate, uni-directional VC Groups. The bandwidth is provided by mapping STM-n port(s) as termination points to the Ethernet port. The TP's will carry VCs in a VC Group assigned to the Ethernet port.

The administrative bandwidth can be:

1. The administrative bandwidth is used as a notification.
2. In AXX155E, the administrative bandwidth is implicit when selecting the TPs to be mapped to the Ethernet port.
3. Apply to AXX 9200 EDGE.

- Symmetric capacity: Same bandwidth downstream and upstream.
- Asymmetric capacity: Different bandwidth for the two directions.

NOTE! The directionality is manually set for upstream and downstream.

8.12.5.1 Bandwidth for bi-directional VCAT

The administrative bandwidth for bi- directional VCAT[1] is identical for both directions (transmit and receive), as the same TUs and AUs are used to provide the bandwidth.

NOTE! The bandwidth must also be implemented through cross-connecting the Ethernet port channels[2] to the designated AUs or TUs.

8.12.6 VCAT circuit protection

If the network element contains a SDH cross connect, SNC/N or SNC/I is allowed when supported by the network element.

For bi- directional VCAT[3] and general procedure, please see “Protect a WAN port” on page 418 and “Protect PtoP cross connections” on page 431.

8.12.6.1 Circuit protection for uni-directional VCAT[4]

You define circuit protection when cross connecting Ethernet port channels to the SDH ports. Since the VC's are unidirectional, the

1. Equivalent to Ericsson AXXESSIT proprietary mapping.
2. Apply to AXX 9200 EDGE.
3. See note 1.
4. See note 2.

VC termination can be both A-side (transmit) and B-side (receive), as illustrated in the figure below:

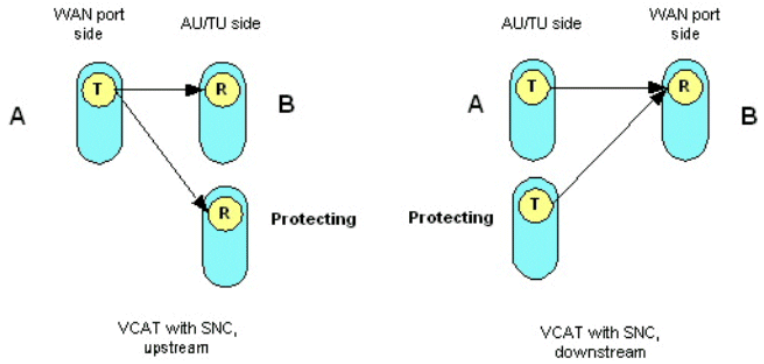


Figure 124 VCAT with SNC- Illustration

See “Legal combinations of SNCP and MSP” on page 449.

8.12.7 Establish Ethernet mapping with VCAT

You establish, modify and delete an ethernet mapping at the endpoints of a Ethernet path through the network. For procedure illustration, see “Uni- directional VCAT with LCAS” on page 470.

8.12.7.1 Before you start

- The STM-n port(s) are structured to the required level.
  See “SDH Cross Connection Management” on page 451.
- The slot expects an ethernet port (LAN/ WAN) with a mapper module.

8.12.7.2 Overview

An ethernet port is mapped to the SDH network with the following parameters settings:

- The ethernet mapping type is selected for the ethernet port.
- The bandwidth is provided for the ethernet port channels.
- Cross connections of ethernet port channels to the target SDH port(s) TP's is established with the intended directionality and circuit protection schemes.

You can perform the standardised mapping in Management Tree and in the WAN mapping GUI. Mapping operation from Management Tree results in an attribute correspondence in the WAN mapping GUI, see Figure 125

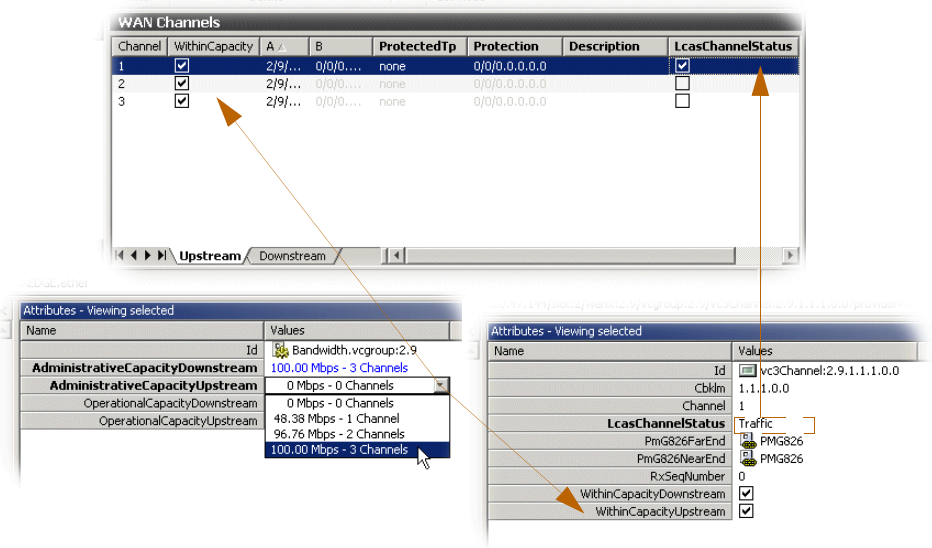


Figure 125 Ethernet mapping- GUI overview

8.12.7.3 Uni- directional VCAT with LCAS

You have selected the ethernet mapping to be uni- directional VCAT VC3 level with LCAS. AXX 9200 EDGE with mapper module 8xFE-16xSMAP as the installed ethernet port (here: WANx) is used as an example.

NOTE! This procedure is generic, and the example can easily be used for Uni- directional VCAT without LCAS by disabling the LCAS attribute(s), or for Bidirectional by selecting softlcas. See mapping properties in Table 16

1. Select the **VC Group** from desired ethernet port (here: WANx).

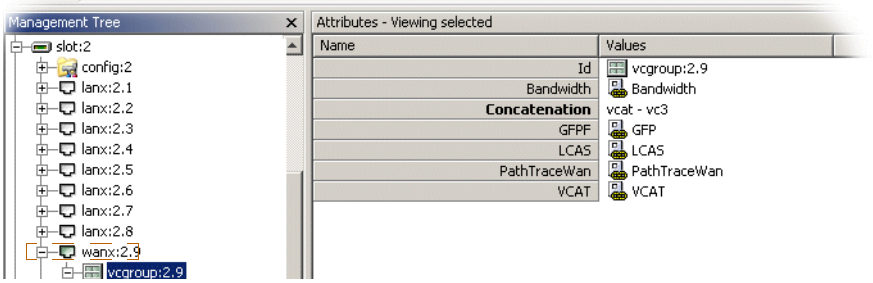


Figure 126 Ethernet port - VC Group view

2. Select **VC level** from **Concatenation**.
   The appropriate structuring level is set to VCAT enabled port.

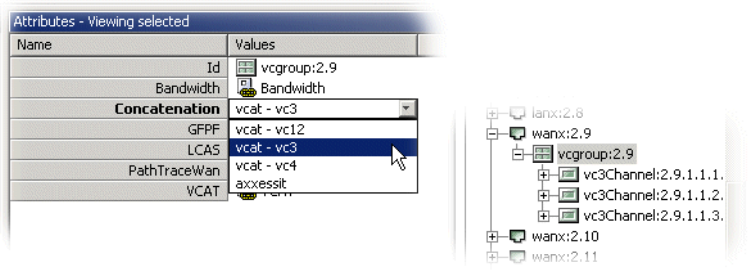
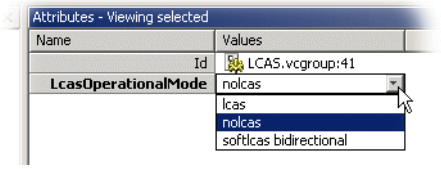


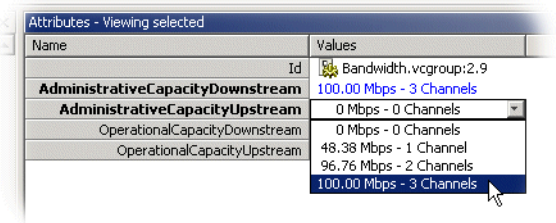
Figure 127 VC Group concatenation and VC- level structure

3. Select LCAS to **VC Group** from **LCAS Operational Mode**.
   LCAS is enabled for the VCAT enabled port, independent traffic direction.

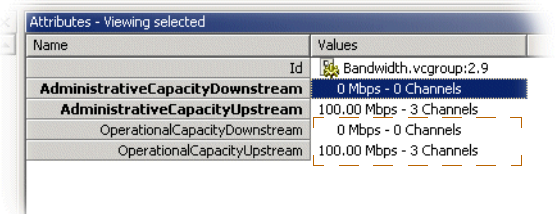


4. Select **VC Group** and press **Bandwidth.**

5. Set the **Administrative Capacity** for downstream and upstream.

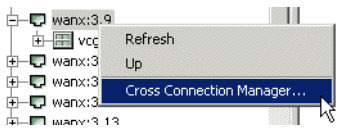


6. Verify **Operational capacity** for traffic directions (optional.)



Example of asymmetric capacity

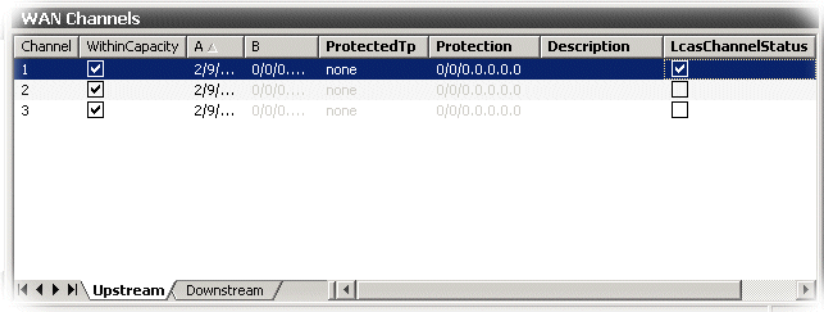
7. Right- click VCAT enabled port to open **WAN- to- SDH mapping**.



The WAN Mapping GUI is opened for the selected port, displaying upstream direction with list of available VC termination points (TPs).

NOTE! If the list of TPs is empty, you should see “Before you start” on page 469.

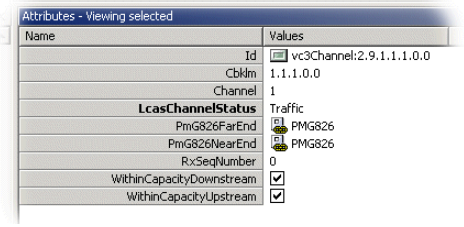
8. Tick **LCAS Channel Status** for the VC channels to be activated upstream.



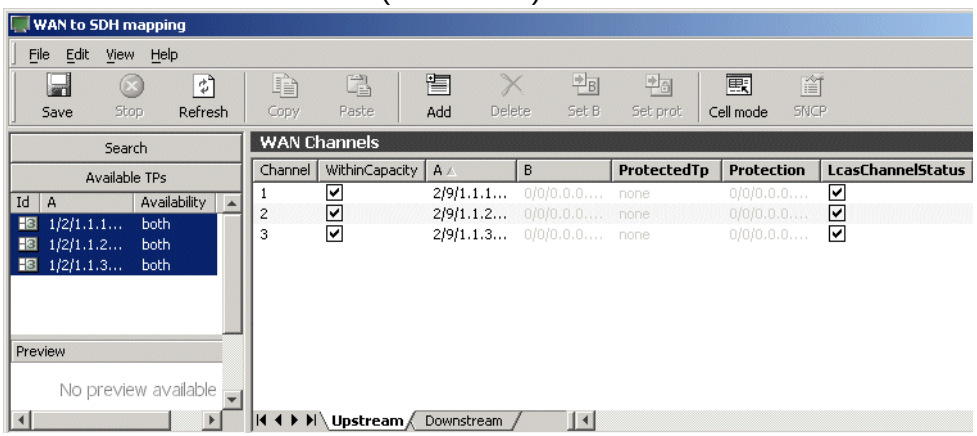
Alternative procedure:

Select one **VC channel** from VC group in Management Tree, and choose Traffic as **LCAS Channel Status**.

Repeat the operation for selected VCs (optional).

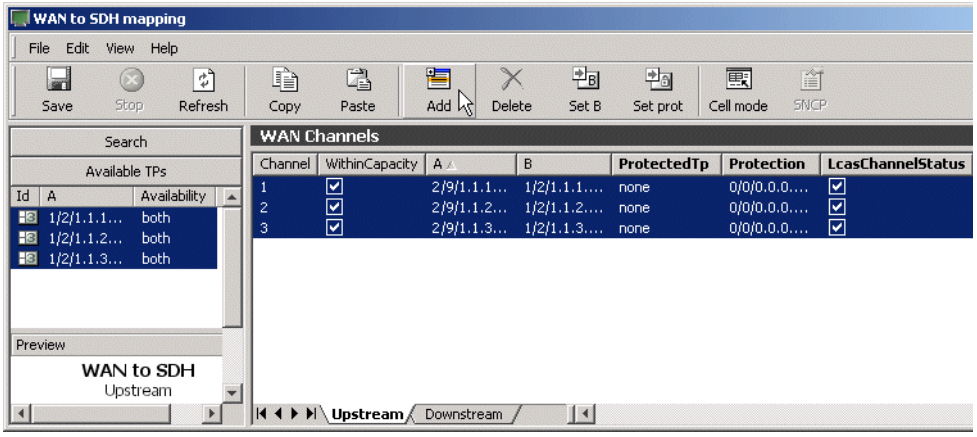


9. Select the **desired TPs** (here: three).



10. Select **VC channels** (here: three) to connect to SDH frame.

11. Press **Add**. See “Advanced WAN Port operations” on page 424. The VCAT enabled port traffic (here: upstream) is distributed through the STM ports.



NOTE! Repeat the mapping steps for traffic distribution in downstream direction.

Define VC XC- point for **SNC protection** to traffic direction(s) (optional.)

See “Protect a WAN port” on page 418, “Protect PtoP cross connections” on page 431, and “Legal combinations of SNCP and MSP” on page 449.

8.13 AXX155E SDH Protection Management

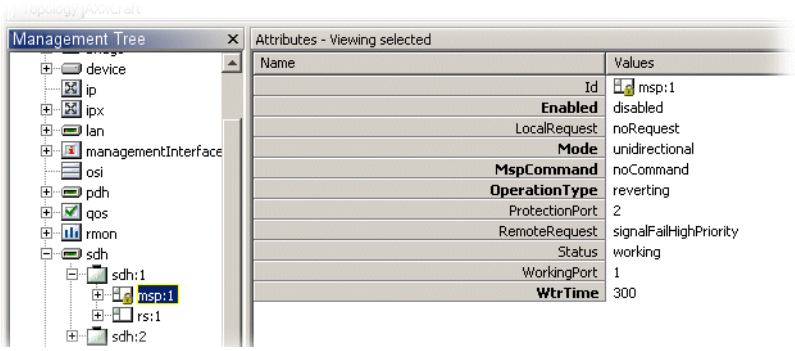
8.13.1 Multiplex Section Protection

The AXX155E offers 1+1 linear Multiplex Section Protection (MSP). The protocol used for K1 and K2 (b1-b5) is defined in ITU-T G.841, clause 7.1.4.5.1. The protocol used is 1+1 bi-directional switching compatible with 1:n bi-directional switching.

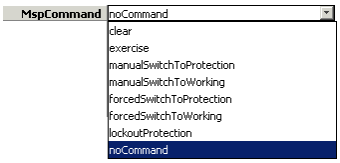
The operation of the protection switch is configurable as described in below:

Modify MSP parameters

1. Select **sdh1** port (working) and click on the **msp** object



Modifiable parameters:

Enabled	Set to enabled or disabled
Mode	Set to unidirectional or bidirectional
MspCommand	Set one of the following: 
OperatingType	Set to reverting or non-reverting
WtrTime	Wait to restore time; number of seconds to wait before switching back to the preferred link after it has been restored (0,1, ...,12 minutes, default 5 min (300 seconds))

2. Click **Save**.

8.14 WAN Ports - AXX155E

A WAN can be established by mapping WAN ports to the SDH Frame Structure at the end- points of a path through a SDH network.

See “SDH port structuring” on page 452, “WANx ports” on page 485, and “Ethernet mapping with VCAT/LCAS” on page 460.

8.14.1 Brief Description

One of the special features of AXX155E is the possibility to concentrate IP traffic over the SDH network. The purpose of this chapter is to describe the tasks involved in assigning capacity from the SDH server layer to WAN ports.

Each SDH channel is equivalent to a VC-12 (2.160 Mbit/s)). AXX155E has one or four WAN ports depending on the hardware configuration.

See “Ethernet mapping with VCAT/LCAS” on page 460.

8.14.2 WAN ports and mapping

The network element has one or four WAN ports. A WAN port has a maximum capacity of 100Mbits/s.

The WAN ports are logical ports and not physical ports. The potential capacity of 100Mbit/s is realized and guaranteed through 47-50 VC12s each able to carry 2.160 Mbit/s. The overhead, i.e., extra bits, are used to handle escaped characters. The capacity of the WAN port is therefore decided by how many VC12s that are assigned to the port.

AXX155E has one STM-1 port and potentially 63 VC12s are available fro a WAN port. Each WAN port has 50 channels that are dynamically mapped to VC12s. See “WAN port - 50 channels/47 channels?” on page 486.

The VC-12s have static cross connections to the available TU12s on the SDH ports.

The order of the 0-50 channels are essential and must be the same on both sides of a WAN connection, e.g., containers sent from channel 1 must be received on channel 1.

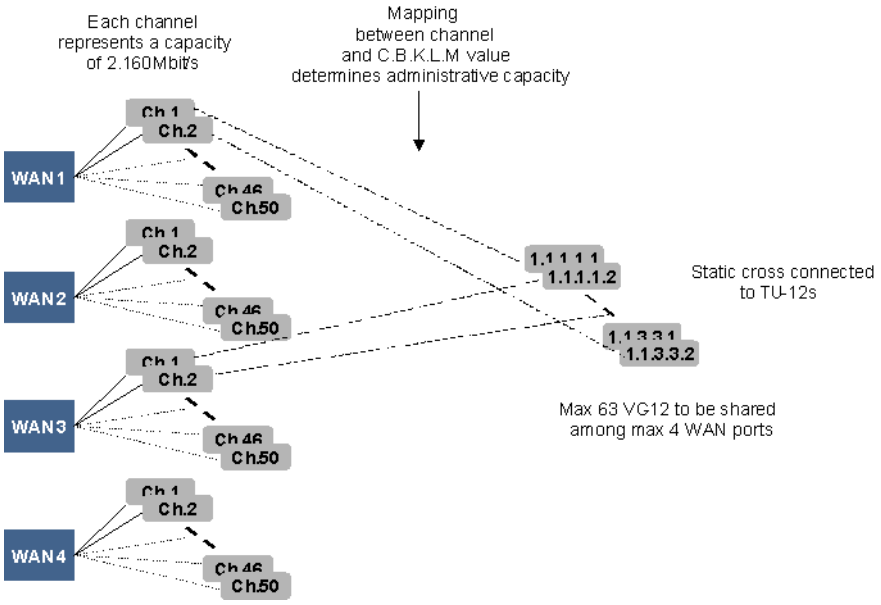


Figure 128 View of the WAN ports and their logical view

Alarms and performance monitoring data is collected and reported for the VC-12s.

8.14.3 Differences between AXX 9200 EDGE and AXX155E

8.14.3.1 AXX 9200 EDGE

In AXX 9200 EDGE each WAN port has always a potential capacity of 100 Mbits/s realized through 50 channels. The available capacity is not dependent on the capacity used by the other WAN ports. When you set the capacity, the system selects the first X channels corresponding to this capacity. The channels have a static mapping to VC-12s. You must cross connect the VC-12s to TU12s to activate the capacity.

8.14.3.2 AXX155E

In AXX155E each WAN port also has a potential capacity of 100Mbits/s, but the available capacity is dependent on the capacity used by the other WAN ports. You set and activate the capacity indirectly by selecting a set of channels and map them to VC-12s. The VC-12s are statically cross connected to TU12s.

The administrative bandwidth is implicit to AXX155E when selecting the TPs to be mapped to the Ethernet port. Also see “VCAT and GFP mappers” on page 465.

8.14.4 Force LAN Down

This feature requires alternate routes for the IP traffic.

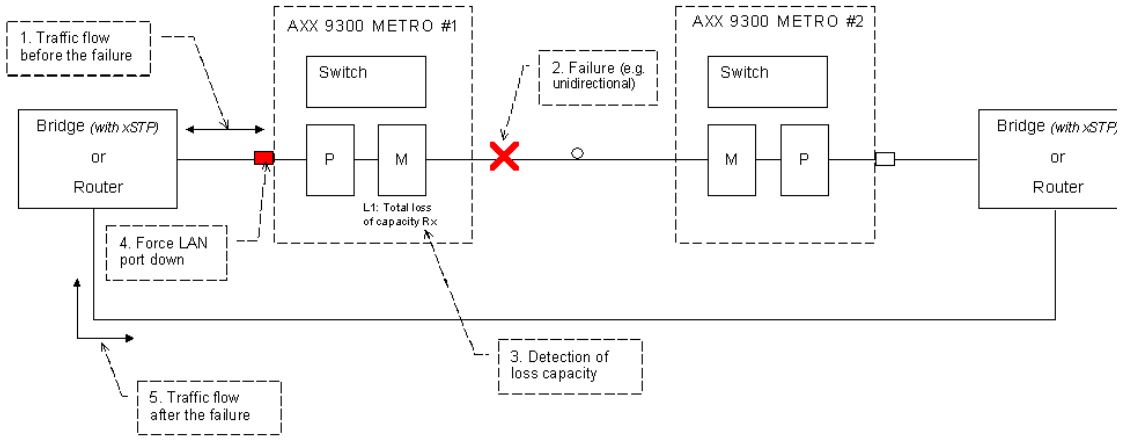


Figure 129 Force LAN down

Rationale for this feature:

Networking devices such as bridges or routers can usually recover quickly from a link failure on a direct link (a link to which they are directly attached). On the other hand, indirect link failure recovery often relies on keep-alive mechanisms that must time-out before the failure can be detected. The "Force LAN down" feature will cause a failure on the "SDH side" to force the associated LAN port (in L1 mode) down, and therefore allowing (in the example above) the networking device to be quickly informed of the failure, and initiate quick recovery, i.e. by switching the traffic onto the other link.

Criteria to be used to force a LAN port down is the same as in the implementation for AXX 9300 METRO, i.e. a LAN port (in mode L1) is forced down when the associated WAN port (mapper) reports some specific alarms.

The attribute called forceLanDown, is located under the LANx port class to control this feature. The attribute is relevant only for LANx ports in L1 mode. The default value for forceLanDown is: **disabled**.

8.14.4.1 Force LAN down on WAN down alarm

In cases of mode transitions, you are recommended to follow this procedure:

1. Delete all **VLAN** entries in VLAN-tables for desired network element.

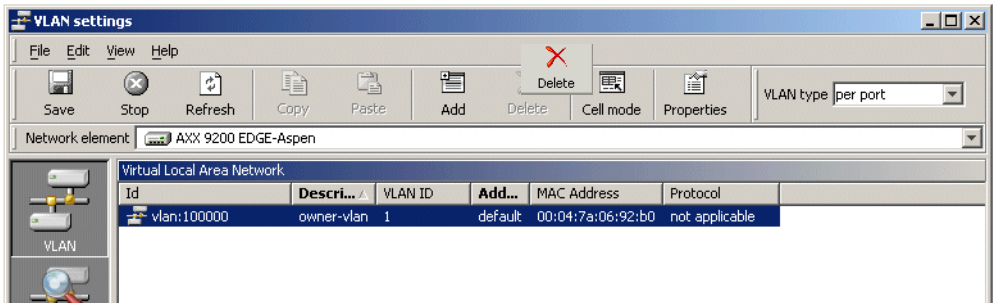


Figure 130 VLAN entry- example

2. Click **WAN** in Management Tree.

The WAN mode is **normal** (default) in Attributes.

3. Change **WANmode** to **LAN down on WAN down**.

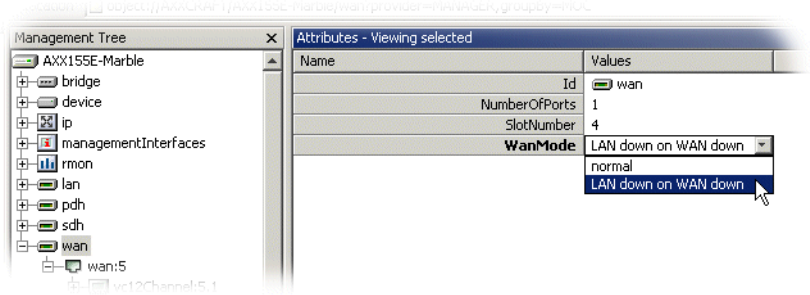


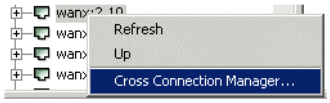
Figure 131 Force LAN down on WAN down

4. Press **Save.**

5. Restart the device.

8.14.4.2 Cross-connect the WAN channels

1. Select the **wan port**, right click and select **Cross Connection Manager**. A list of all the WAN channels of the WAN port is



shown. The list shows the **static relation** between **each channel number** and a **VC12 object** in the WAN port.

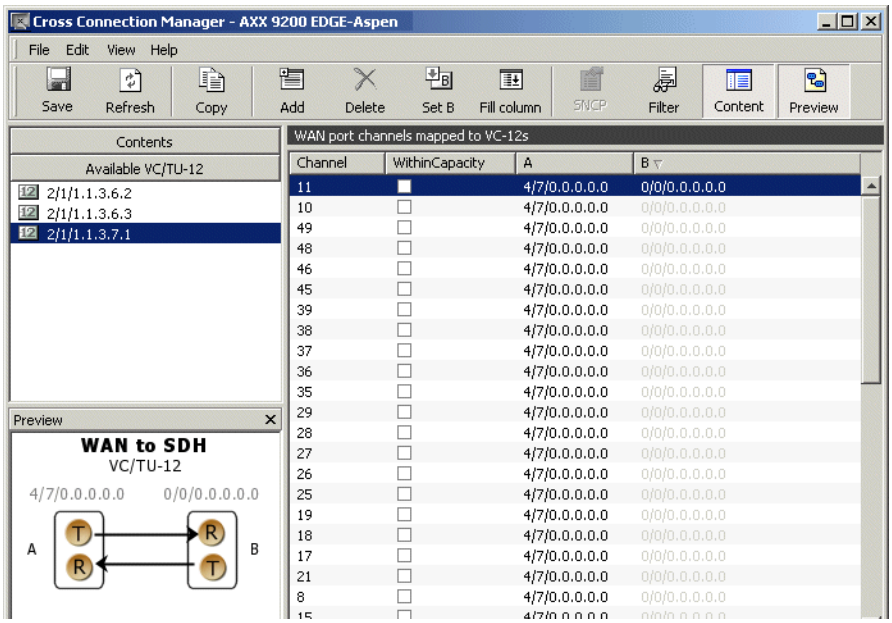
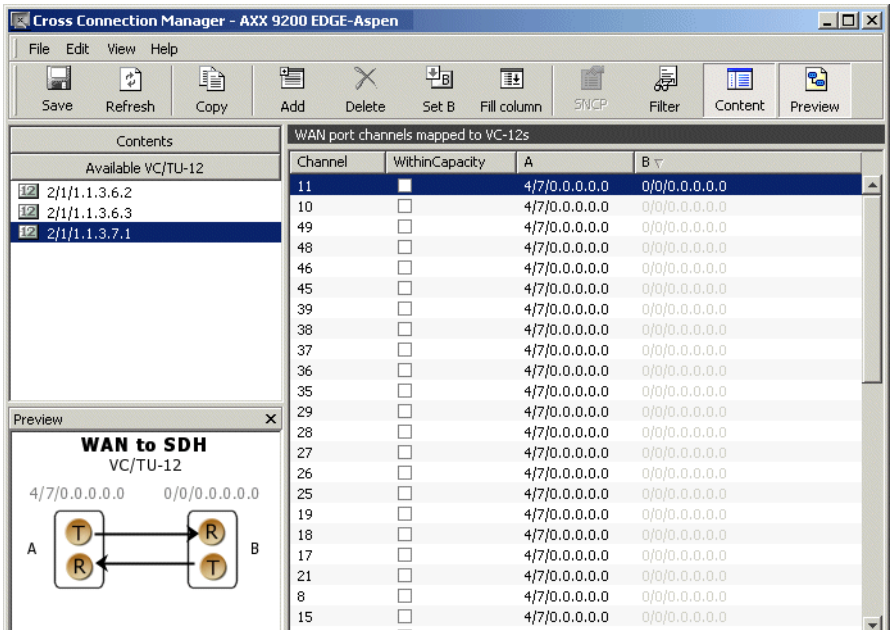


Figure 132 WAN channels list- example VC12 on AXX155E

8.14.4.3 Cancelling a query

Queries in progress can be cancelled by selecting the Stop 

operation from the tool bar or the menu.

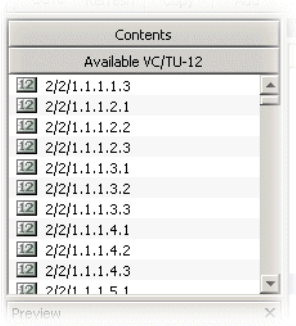


2. Make sure the **Content panel** is available in the left part of the window.

   If it is not available select the 

   Content button in the toolbar.

3. Select the **Available VC/TU12 List** in the Content panel.
   The list contains the **free TU12 termination points** in AXX155E.



4. Double-click the **TU12 termination point** that you want to use to map to your **WAN channel number 1**. The selected TU12 is inserted as the B terminationPoint for channel 1.

5. Double-click the **termination point** that you want to use to map to your **WAN channel number 2**.

6. Continue **until all desired channels** have a B termination point.

7. Save.

NOTE! Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate nodes. The WAN channel will only work if it is connected to the WAN channel with the same channel number on the opposite end of the SDH network.

NOTE! The WAN port will not report alarms on channels that are not part of the administrative capacity.

8.14.5 Increasing capacity in the SDH server layer:

Make sure the Content panel is available in the left part of the window. If it is not available select the Content button in the toolbar.

1. Select the **Available VC/TU12 List** in the Content panel.
   The list contains the free TU12 termination points in AXX155E.

NOTE! **2.**Double-click the **TU12 termination point** that you want to use to map to your **first available WAN channel**.
The selected TU12 is inserted as the B termination Point for this channel.

NOTE! For the AXX155E, mapping must be performed in a continuous range.

3. Double-click the **termination point** that you want to use to map to your **next new WAN channel**.
4. Continue **until all desired channels** have a B termination point.
5. Save.
6. Remember to perform the same operation on the WAN port on the other side of the SDH network and adding cross-connections in intermediate SDH nodes.

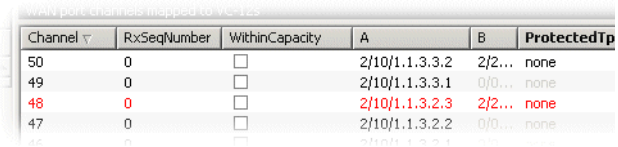
8.14.6 Decreasing capacity in the SDH server layer:

1. Select the **WAN channels** that are **not used any more** by the WAN port mapping (channels with B termination points, but not

WithinCapacity). Multiple selection is possible with SHIFT or CTRL buttons.

NOTE! For the AXX155E, deleting mappings must be performed in a continuous range.

2. Click **Delete** on the toolbar. The selected channels becomes red.



3. Click **Save** on toolbar. The SDH TU12 termination points are released from WAN port mapping.

4. Remember to perform the same operation on the WAN port on the other side of the SDH network and deleting cross-connections in intermediate SDH nodes.

NOTE! It is not possible to modify the B termination point after it has been saved. If you want to modify the B termination point the mapping must first be deleted, and then a new Termination Point can be added.

8.14.7 Setting Path Trace Identifiers for WAN port

Path Trace parameters can be read for each channel (VC12) in the WAN port.

1. Select a **wan port**.

2. Click on the **PathTraceWAN** parameter group

3. The following **attributes** can be set for all channels of the WAN port:

PathTrace:
Set to enable if TIM alarms should be reported for the WAN port when there is a mismatch between PathTraceReceived and PathTraceExpected.

PathTraceExpected:
Enter a value for the Path Trace Identifier that you expect to receive from the other side of the WAN channels.

PathTraceTransmitted:
Enter a value for the Path Trace Identifier that you want to transmit to the other side of the WAN channels.

4. Click Save on toolbar

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received Path Trace.

8.14.8 Reading Path Trace Identifiers for WAN port

Path Trace parameters can be read for each channel (VC12) in the WAN port.

1. Select a **wan port**.

2. When the wan port managed object is expanded, click on the **channel** (**vc12**) where you want to see the **Received Path Trace**.

3. Click on **PathTraceVC12**.

4. The following attributes can be read:

PathTrace:
Set to enable if TIM alarms should be reported when there is a mismatch between PathTraceReceived and PathTraceExpected.

PathTraceExpected:
Enter a value for the Path Trace Identifier that you expect to receive from the other side of the path.

PathTraceTransmitted:
Enter a value for the Path Trace Identifier that you want to transmit to the other side of the path.

PathTraceReceived:
The actual received Path Trace Identifier from the other side of the link.

NOTE! When Path Trace is set to enabled, AIS is inserted downstream instead of the original signal when there is a mismatch between expected and received PathTrace.

8.14.9 Monitor WAN Port Performance

1. Select a **wan port**.
2. When the wan port managed object is expanded, click on the **channel** (**vc12**) where you want to see the **Performance data**.
3. Click on **PmG826NearEndVc12** to read **near end PM data** or **PmG826FarEndVC12** to read **far end PM data**.
4. The following attributes are available

Current15Min ES,**SES**, **BBE** and **UAS**

5. To see the Performance **history** of the previous 16x15 minute counters click on **Interval15Min**.
   The following attributes are available

I**nterval15Min ES**,**SES**, **BBE** and **UAS**

8.14.10 Advanced WAN Port operations

For frequent users of AXX 9840 INSITE it is possible to make use of the enhanced editing facilities to speed up the configuration work.

Selection and insertion of multiple termination points

1. Select the **channels** where you want to **add termination points as B-end**. Use SHIFT or CTRL buttons to select more than one channel, or simply drag the mouse down the list while pressing the left mouse button.
2. Select the **TU12 termination points** that you want to add to the B-ends of the channels in the same way.
3. Click the **Set B** 

button in the toolbar.
4. Save.

NOTE! You are only allowed to set the B termination points of channels where B is not in use.
If you want to modify the B termination point the relation with the existing B termination point must first be deleted. Then a new Termination Point can be added.

NOTE! If you do not select the same number of instances of WAN channels and termination points, the channels will be filled in with as many TPs as available, starting from the top of the selected channel list. If more TPs are selected than channels, the last TPs will not be used.

8.14.11 WANx ports

WANx is the expression of an ethernet (WAN) port with extended functionality supporting an advanced mapper module, see “VCAT and GFP mappers” on page 465.

WANx settings

FlowControl; off or on.

Priority(802.1p); disable or 802.1p. (read- only)

Manage Priority through FlowControl by setting the opposite values.

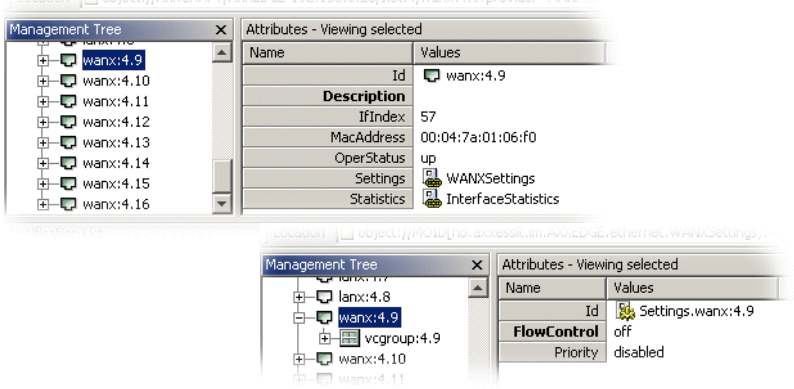


Figure 133 WANx port- attributes view

8.14.12 FAQ

8.14.12.1 Why should I set the Path Trace Identifier attributes?

You do not have to set the Path Trace Identifier attributes, but it is a very useful tool for checking the connectivity of complex networks. Basically a Path Trace Identifier is inserted at the beginning of a path and extracted at the end of a path. By setting Path Trace

Transmitted to a logical value, e.g. "BONN-3-21" you can easily see if this value is received on the other side of the network.

If you enter a value for the Path Trace Expected value and enable Path Trace, a TIM alarm will be triggered if the received value is different from the transmitted value.

8.14.12.2 What is a WAN port?

WAN ports perform the mapping between a traditional Lan Port and the SDH network. The WAN port is an internal interface in AXX 9200 EDGE.

8.14.12.3 WAN port - 50 channels/47 channels?

Why does a WAN port have 50 channels when I can achieve the maximum capacity of 100 Mbit/s using 47 channels?

The WAN port is mapping the ethernet packets into VC12 containers. Each VC12 container always carry 2.16 Mbit/s. However, the mapping process requires some overhead. The overhead will vary with the actual PDU type mapped into the VC12 channels. This means that the bit rate at the Ethernet interface is a bit less than the bit rate of the VC-12 channel. With a certain type of PDUs, 100Mbit/s is achieved using only 47 channels, while some PDUs may require 50.

9 Performance Management

9.1 Introduction

This chapter describes the presentation of Performance Management (PM) data as they occur on the network element. The PM data available on the network element is:

- G.826 performance data for the SDH paths and section termination points.
  - G.826 on Multiplex Section (MS), Regeneration Section (RS), Virtual Containers (VC).
  - Non-intrusive monitors on AUs and TUs cross- connected through the network element.
- Values of the various counters.
- RMON.

PM data can be monitored from Management Tree. You can read the registered PM data on the network element, get it presented in performance management data tables. The file can be read, copied and/or edited in any tool, for instance MS Excel. It is possible to clear all PM data on the network element, see “Logs (alarm logs, performance data logs)” on page 332.

Definitions

According to G.826 PM data, the following definitions are used:

Errored second (ES)

A one second period with one or more errored blocks or at least one defect.

Severely errored second (SES)

A one second period which contains >= 30% errored blocks or at least one defect

Background block error (BBE)

An errored block not occurring as a part of a SES

Unavailable seconds (UAS)

A period of unavailable time begins at the onset of ten consecutive SES events. These ten seconds are considered to be part of unavailable time. A new period of available time begins at the onset of 10 consecutive non-SES events. These ten seconds are considered to be part of available time. UAS is the number of second of unavailable time.

9.2 PM Tools

9.2.1 Introduction

This chapter describes the performance management and how you can view current and historical performance data.

The description and presentation of performance data is divided into:

- Reporting selected historical performance data, such as G.826 reports, time series information etc. with the PM Viewer.
- Present or report on the quality of the communication services (WAN / TDM circuits)

The chapter mainly describes viewing historical G.826 performance management data as stored persistently in the TMN system. Historical PM data is presented in the PM Viewer. See “Using the PM Viewer” on page 496.

Background

G.826 data is available in the TMN system database and in the network elements under management.

The network elements have limited memory for historical data storage, and the oldest data will be removed in favour of new, current data registered to the network element. Historical data is collected from the network element in the managed network by the TMN system, which has a greater storage capacity.

This feature is valid for all Ericsson AXXESSIT network elements that support G.826 monitoring.

9.3 View historical PM data

Performance Management involves the following activities:

1. Setting up the TMN system to collect performance data from network elements for storage and presentation.
2. Presenting historical performance data for each of the network elements or for a group of network elements (managed objects).

Two types of PM data is collected for the network elements from Ericsson AXXESSIT: G.826 and counters + RMON.

The intention of the historical G.826 presentation is to:

- Present the quality of the SDH topological links (MS and/or RS measurements).
- Present the quality of the communication services (WAN and/ or TDM circuits) implemented by the network as SDH Virtual Containers (VCs).

9.3.1 Presentation of G.826 data

The purpose of viewing G.826 data is to:

- Provide a display of the quality on selected links/ circuits or groups of selected links/ circuits over time for documentation of quality.
- Allow sorting and filtering to identify and highlight ***time periods*** that comply with your specified quality criteria.
- Support problem identification and resolution.

The following sections present the steps for selecting and limiting available PM data for report presentations.

9.3.1.1 Selecting filtering data classes

The first main step in limiting the available selections of G.826 data allows you to distinguish between two main areas of G.826 performance data presentation:

- The need for documenting the quality of the SDH infrastructure.

- The need for documenting the transmission quality of the communication services provided by LAN/WAN and TDM (PDH) circuits.

  The alternatives are:
  a. G.826 data associated with topological links (NE link endpoints).
  b. G.826 data associated with TDM (PDH) or LAN/ WAN circuits.

SDH link domain

The SDH link domain covers MS near/ far G.826 measurements and RS near G.826 measurements.

Selection choices are:

- Topological link (selected by one of the network elements that are link endpoints).
  This choice is also available as a "quick selection" from the Management Tree, Topology Editor or Topological Map.
- Network element or group of network elements.
  This selection will include all the SDH port of the selected network elements.
- Network element slot.
  This selection will include all SDH ports within the selected slot.
- Network element slot/port.
  This choice is also available as a "quick selection" from the Management Tree.
- Slot/Port MS/RS object

PDH/ WAN port domain

G.826 performance measurement data of PDH and WAN ports are carried by the VCs assigned to the ports.

Selection choices are:

- Network Element instance.
  This choice will present all G.826 data associated with PDH and WAN ports within the selected network element
- Network element slot instance.
  This selection will present all PDH and/or WAN port G.826 data associated with the selected slot.
- Network element VC- 4 instance.

- WAN or PDH port instance.
  This selection will present all G.826 data associated with the selected port. For the PDH port, this choice is also available as a "quick selection" from the Management Tree, Topology Editor or Topological Map.

9.3.1.2 Filtering data sources

The second main step allows you to limit the amount of presented data within the selected domain. This step has two paths, depending on the domain (link or WAN/PDH port):

A WAN port selection will result in 1 to 50 VCs being presented, depending on the bandwidth configured for the WAN port

9.3.1.3 Selecting data presentations

Selecting data ranges

A PM Viewer and reports present a tabular view of G.826 data stored in the management system, allowing filtering, copying and sorting to limit the amount of data available in the simple query.

- Time/ date interval
- Type of measurement (15 min. / 24 hour)
- G.826 near end and/ or far end measurements
- G.826 record fields (BBE[1], ES[2], SES[3], UAS[4])
- Calculations on G.826 record fields (AND, NOT, <, >, <= or >=)
  SDH specific:
- MS and/or RS

The tabular views of G.826 PM data is based on your scoping parameters.

Filtering features are provided to you in the standard query in order to present PM data for the managed network.

1. Background Block Error
2. Errored Seconds
3. Severely Errored Seconds
4. Unavailable Seconds

Performance measurement parameters

- Network element instances.
- Managed object instances.
- G.826 attributes (BBE, SES, ES, UAS) within given limits.
- Near end data or Far end data, or both.
- Time interval - collected performance data from time 1 to time 2.
- Period - 15 minutes, hour, 24 hours, week, month, year.

Time interval

A calendar is available to set the time interval.

TIP! Set time interval: Select larger then <, set date and time from calendar, and press Add date/ time. Press AND, select less then >, set date and time from calender and press Add date/ time).

9.4 PM Monitoring Configuration

In the opening page of the PM Configuration you add and edit performance management monitors for your network elements. The collected data can then be viewed in the PM viewer, and reports can be created from the Report viewer.

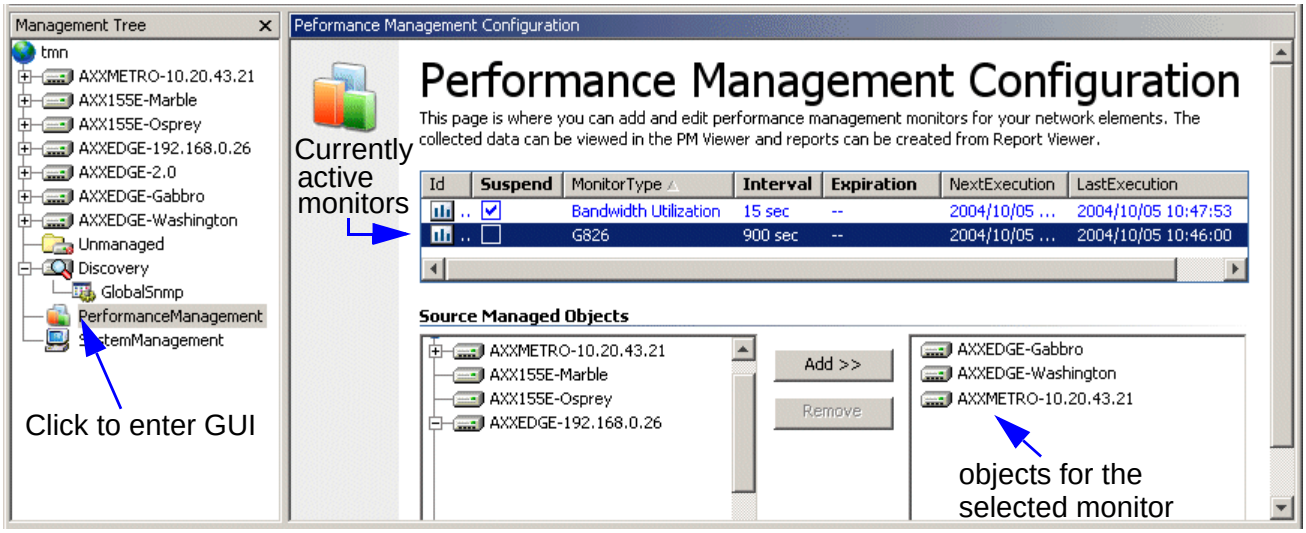


Figure 134 PM Configuration overview

NOTE! PM data is stored persistently in the TMN system, not in the Network Elements.

Brief introduction about the configuration with typical steps:

1. **Add Monitor**:  on the toolbar
   Monitor => Group of measurement points sharing timing data

2. Choose **monitor type**:
   - G.826
   - Bandwidth Utilization

3. **Configure** the monitors you have created

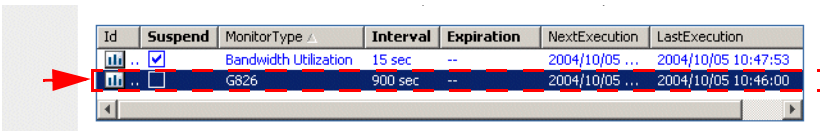
4. Select the **data source objects** you want to monitor and click Add>>
   - Whole NE (all possible measurement points within the NE)
   - Whole Module(= slot)
   - Single points (LAN/WAN/MS/RS/VC)

5. **Press Save** () on the toolbar) to execute your selections
   Some settings may be edited (shown by bold in the column heading)

Details about the possible selections and their configurations are described on the following pages.

9.4.0.1 Delete Monitor

1. Select **desired monitor** in the list of active monitors.



2. In the toolbar press **Delete**.  .

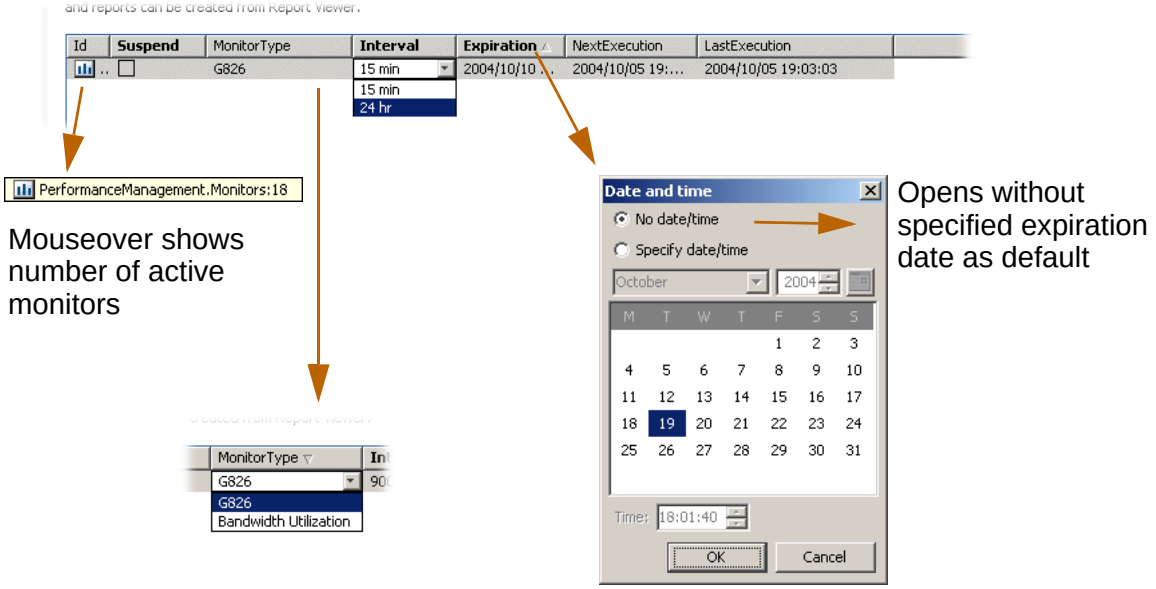
3. In the toolbar press **Save**. 

9.4.1 G.826 Monitor Setup

9.4.1.1 Overview of selections

1. Click Add on the toolbar, and a new monitor will appear ready for you to configure as shown in Figure 135

Figure 135 G.826 Monitor Setup



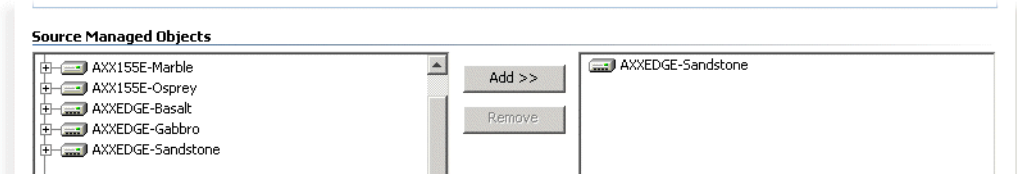
The list below describes the different columns in the PM Config window:

Id	Mouseover shows the number of active monitors
Suspend	**Tick to hold the registration of data temporarily**
MonitorType	Indicates the selected monitor type
Interval	**Possible values: 15min or 24hr intervals**
Expiration	**Choose the last date and time for data collection**
NextExecution	Indicates the next scheduled data collection
LastExecution	Indicates the last scheduled data collection

9.4.1.2 Select objects to monitor

2. In the Source Managed Objects window you select the objects you want to monitor for G.826 data. Source Managed Objects.

3. Click Add>>



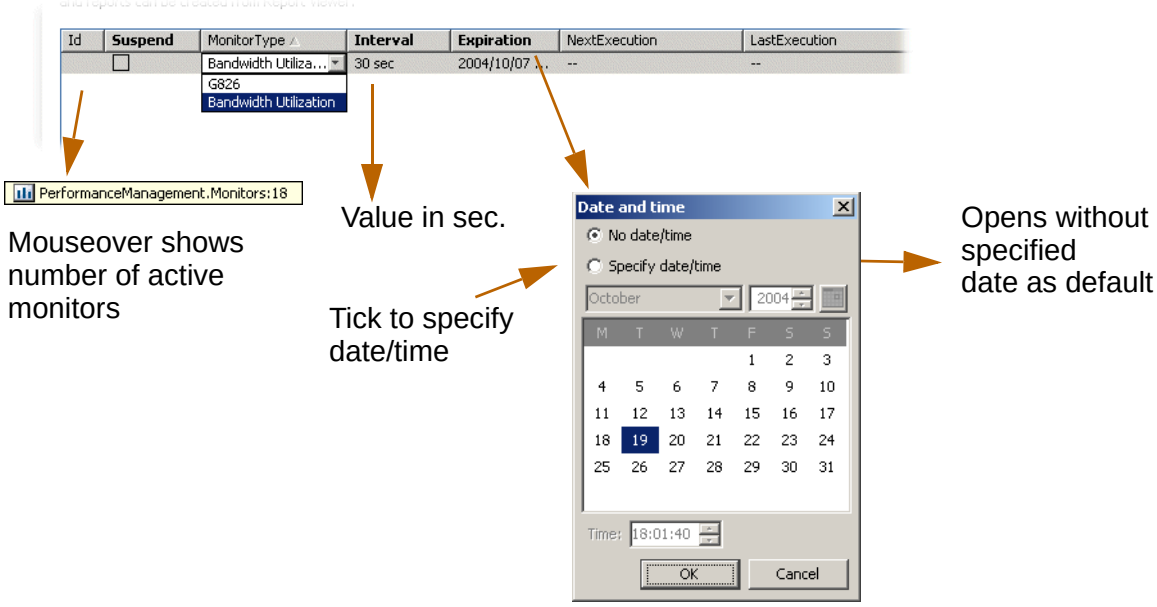
You will only be allowed to select Network Elements, and the objects can't be expanded.

4. Click save to activate the monitor for the selected objects

9.4.2 Configuration of Bandwidth Utilization Monitor

When activated, this monitor will initiate an RMON testing probe on the selected Network Element

Figure 136 Configuration of Bandwidth Utilization Monitor



The list below describes the different columns in the PM Config window:

Id	Mouseover shows the number of active monitors
Suspend	**Tick to hold the registration of data temporarily**
MonitorType	Indicates the selected monitor type
Interval	**Possible values: from 3 to 3600 seconds**

Expiration	Choose the last date and time for data collection
NextExecution	Indicates the next scheduled data collection
LastExecution	Indicates the last scheduled data collection

9.4.2.1 Select objects to monitor

1. In the Source Managed Objects window, select the objects you want to monitor for Bandwidth Utilization data. In this monitor you can only select ports (WAN, LAN, WANx and LANx)

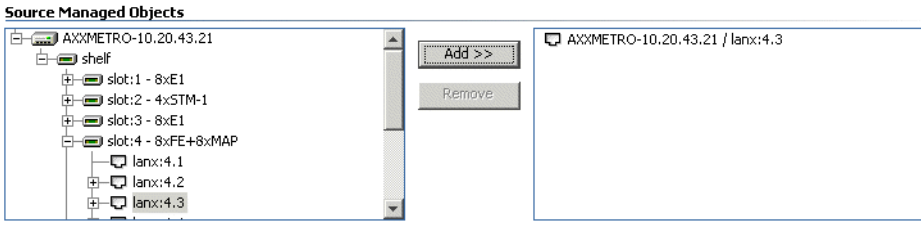


Figure 137 Source Managed Objects

2. The objects can be expanded, and the Add>> button becomes active when you select legal ports.

3. Click save to activate the monitor.

9.5 Using the PM Viewer

The PM Viewer presents the PM data in tabular views.

Qeries shown in the PM viewer can be copied, pasted or imported as xml files to a 3 rd party application, such as MS Excel.

1. Open the **PM Viewer** from the Equipment menu.

The PM Viewer presents a simple query (default), see Figure 138

2. Select the type of **query** you want from the View menu.

   With the **simple query,** you can create, view and save custom PM reports for a single network element.

   From the **standard query** you can, in addition, scope, sort and filter the PM data for a single managed object or a group of network elements reported for the managed network**.**

Scoping:

To select the information you want to read from the TMN PM database. Small scopes are presented more quick than big scopes.

Filtering:

How you organize, sort and display the information from the scope you read.

NOTE! The PM-data reading will stop after 5000 lines.
If this happens, adjust your parameters to reduce the amount of data.

9.5.1 Overview

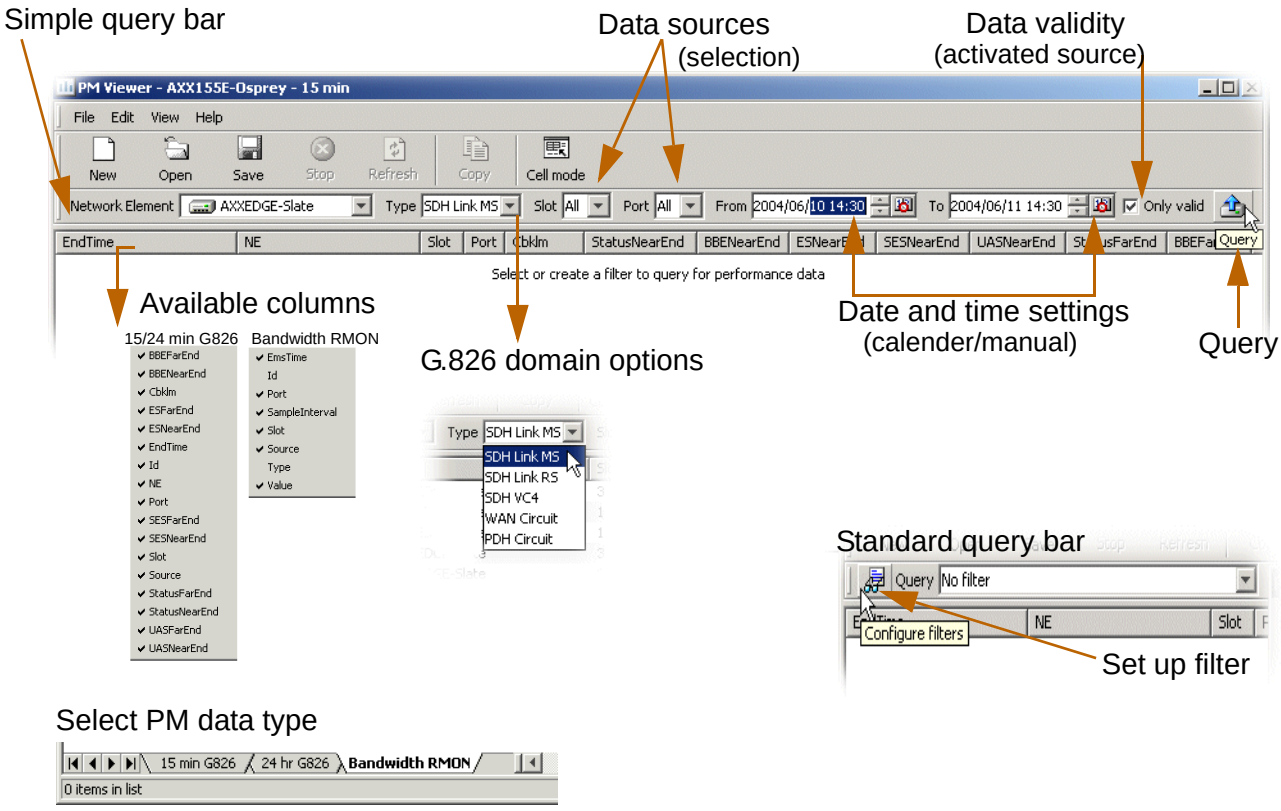
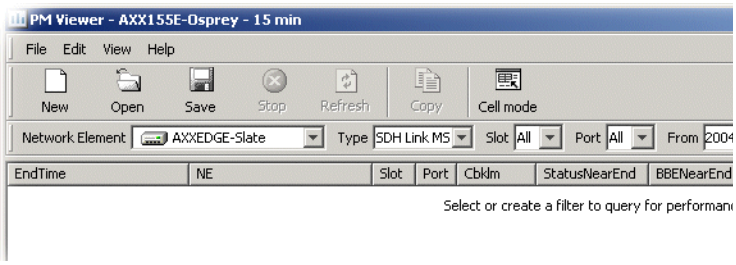


Figure 138 The PM Viewer- overview

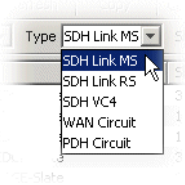
NOTE! The different operations to be described assume you have necessary access rights and knowledge of the network topology, including intermediate VC4 terminations.

9.5.2 Select PM data whith Standard query

1. Open the **PM Viewer** from the Equipment menu.
2. Navigate to the **Standard query bar,** as shown in Figure 141 -The list is empty. If not, choose File >**'new'** to clear the list.
3. Select desired **Network Element**.



4. Select **domain** from **Type**.



5. Select **data source** selection; slot(s) and port(s).
6. Set **date and time** for historical PM data.
7. Uncheck **'Only valid'** (optional) to include managed, unactive objects.
8. Click the **Query** button**.**

The PM Viewer presents a PM report based on your data source selection.

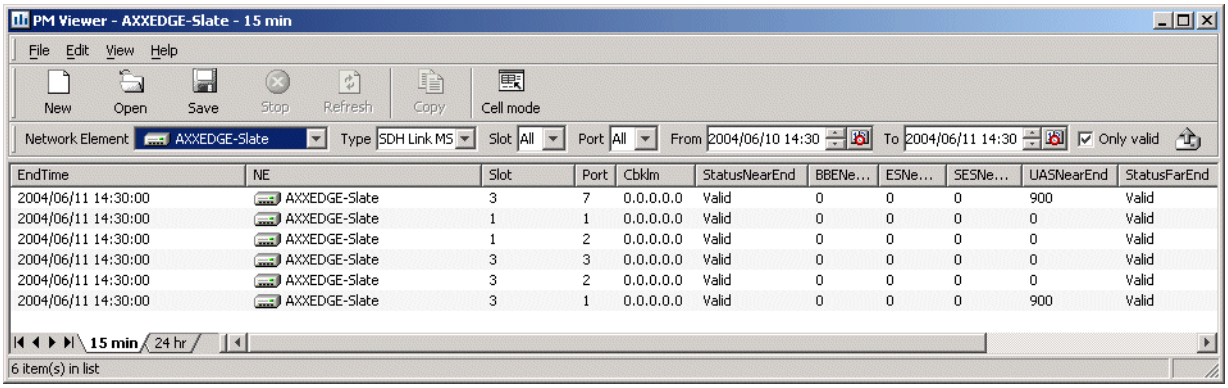


Figure 139 G.826 PM report- example 15 minutes PM data for SDH link MS

NOTE! You will receive a warning if the query is large or will cause heavy load on the system in a way that the query can take time to carry out.

9. Toggle the **PM data interval**.

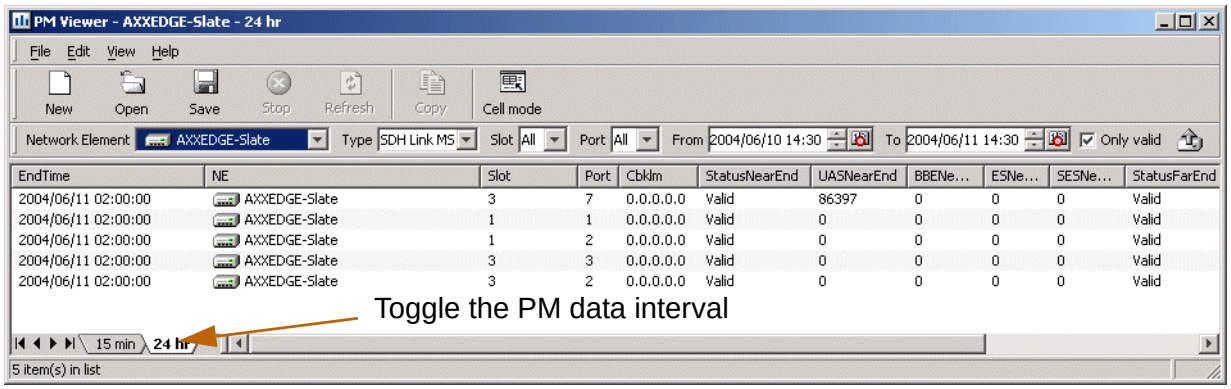


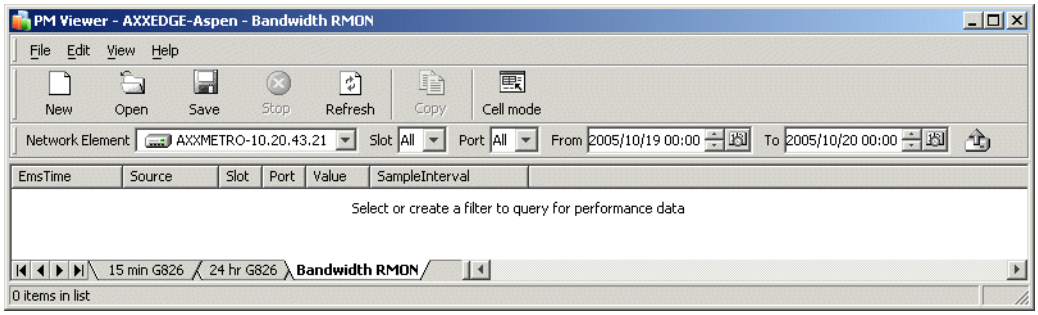
Figure 140 G.826 PM query- example 24 hours PM data for SDH link MS

9.5.3 Select Bandwidth RMON PM data whith simple query

1. Open the **PM Viewer** from the Equipment menu.
2. Navigate to the **Simple query bar,** as shown in Figure 141

The list is empty. If not, choose File >**'new'** to clear the list.

3. Select desired **Network Element**.



4. Select **data source** selection; slot(s) and port(s).
5. Set **date and time** for historical PM data.
6. Click the **Query** button**.**

The PM Viewer presents a PM report based on your data source selection.

NOTE! You will receive a warning if the query is large or will cause heavy load on the system in a way that the query can take time to carry out.

9.5.4 Select PM data whith standard query

The tabular views of G.826 PM data is based on your scoping parameters. Filtering features are provided to you in the standard query in order to present PM data for the managed network.

9.5.4.1 Query parameters

- Network element instances.
- Managed object instances.
- G.826 attributes (BBE, SES, ES, UAS) within given limits.
- Near end data or Far end data, or both.
- Time interval - collected performance data from time 1 to time 2.
- Period - 15 minutes, hour, 24 hours, week, month, year.

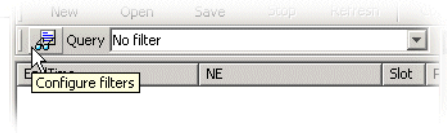
9.5.4.2 Time interval

A calendar is available to set the time interval.

TIP! Set time interval: Select larger than < , set date and time from calendar, and press Add date/ time. Press AND, select less than >, set date and time from calender and press Add date/ time).

9.5.4.3 Create filtered PM query for multiple network elements.

1. Check **Standard query** from the View menu.
   The Standard query bar appears in a filter mode.



2. Press **Configure filter** to open filter menu.

3. Specify a **Filter name** for the PM query.

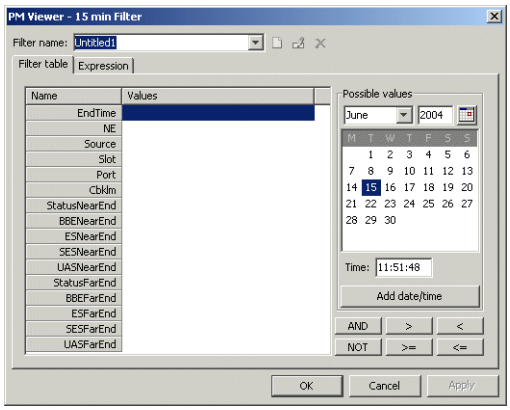


Figure 141 Filter menu from the PM Viewer

4. Select the desired filter **parameters** from the menu.

5. Press **OK**.
   The new filter is available from the Query pull-down menu.

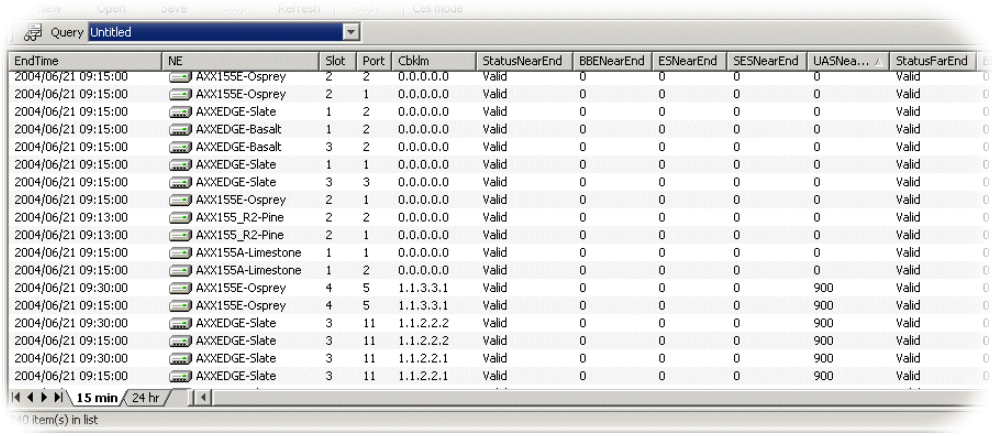


Figure 142 G.826 PM report- example 15 minutes for managed network

9.5.4.4 Present PM query for managed object

For SDH ports and topological link (select one of the network elements that are link endpoints), you can create a ‘quick selection’ by right- clicking this managed object in the Management Tree.

1. Right- click desired **managed object instance** in the Management Tree.

2. Select **View Performance Data**.

3. Select desired **PM data interval**.

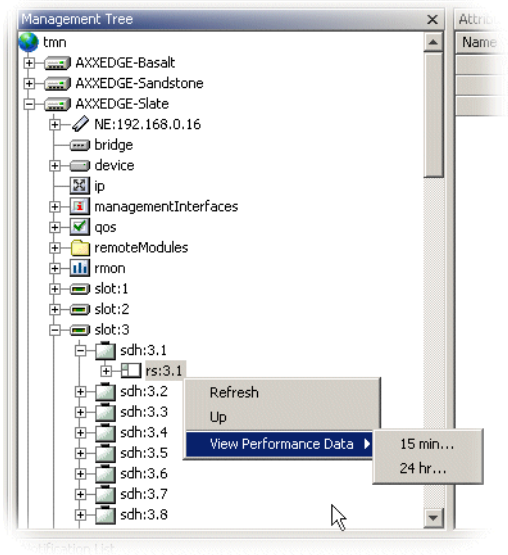


Figure 143 Launch PM report from the Management Tree- example

The PM Viewer opens and reports available G.826 PM data in a standard query

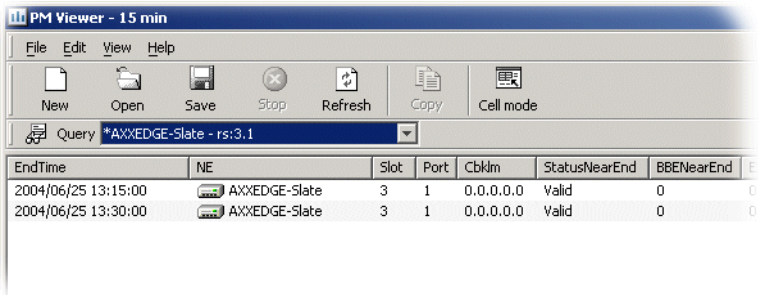


Figure 144 PM report - example of a 'quick selection'

NOTE! The Filter name displayed in the Query pull-down menu is a temporary filter for the selected scope, and will not be saved.

9.5.5 Save the PM data to file

You can save the PM query to create PM reports for statistics and manually trend analysis. You can at any time save the specific presentation (includes instance related information) independent of the query type.

1. Press **Save** from the toolbar in the PM Viewer.
2. In the file browser, **browse** to desired location and **create** a folder.
3. **Save** the PM report to this folder.

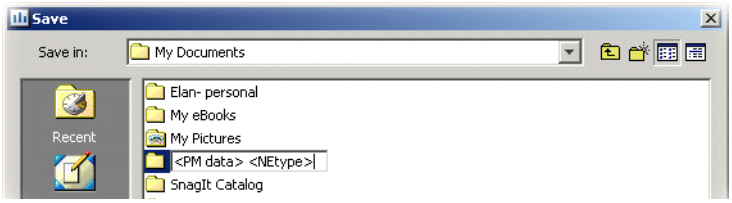


Figure 145 Save query as PM report

9.5.6 Restore PM data from file

1. Press **Open** from the toolbar in the PM Viewer (or import xml- file from 3rd. party application[1]).
   -The system opens the file browser.

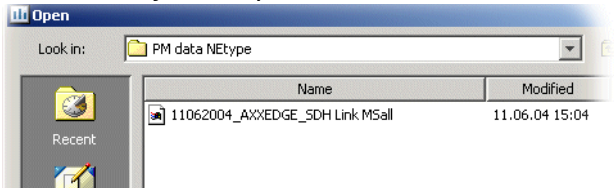
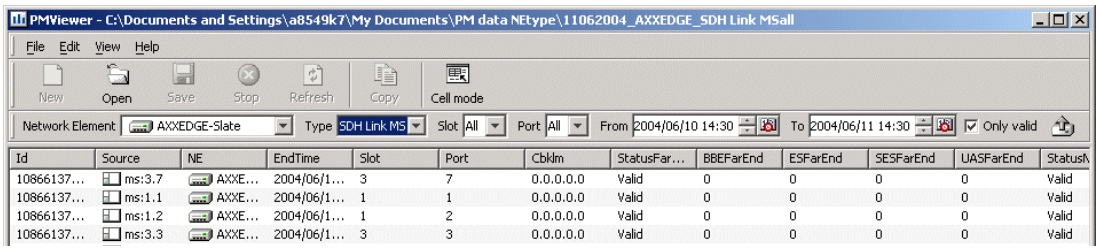


Figure 146 Open PM report

2. Select desired PM report file.

The historical PM report is presented to you in the PM Viewer.



1. The presented data can be saved to an XML file for import to other tools.

Figure 147 PM report file opened in the PM Viewer- example.

9.6 View performance management data

This section describes:

- “View G.826 performance data”
- “View counters”

9.6.1 View G.826 performance data

Background

G.826 PM data is available in the network elements under management. The network elements have limited memory for historical data storage, and the oldest data will be removed in favour of new, current data registered to the network element[1].

G.826 specifies the accumulated performance data for 15 minutes and 24 hours periods. The incomplete data for the current 15 minutes period is also available. This is updated continuously on the network element. PM data is stored in time series measurement periods (for instance such as the last 15 minutes and the last 24 hours period) on the network element.

From Management Tree, you can select G.826 PM data for the following managed objects:

- RS Near End
- MS Near End and Far End
- VC-3 Near End and Far End
- VC-4-4c Near End and Far End
- VC-4 Near End and Far End
- VC-12 Near End and Far End
- None- intrusive monitors on AUs and TUs

Near End and Far End data apply to all managed object, except for the RS.

1. Time periods and interval may vary between the different network element types.

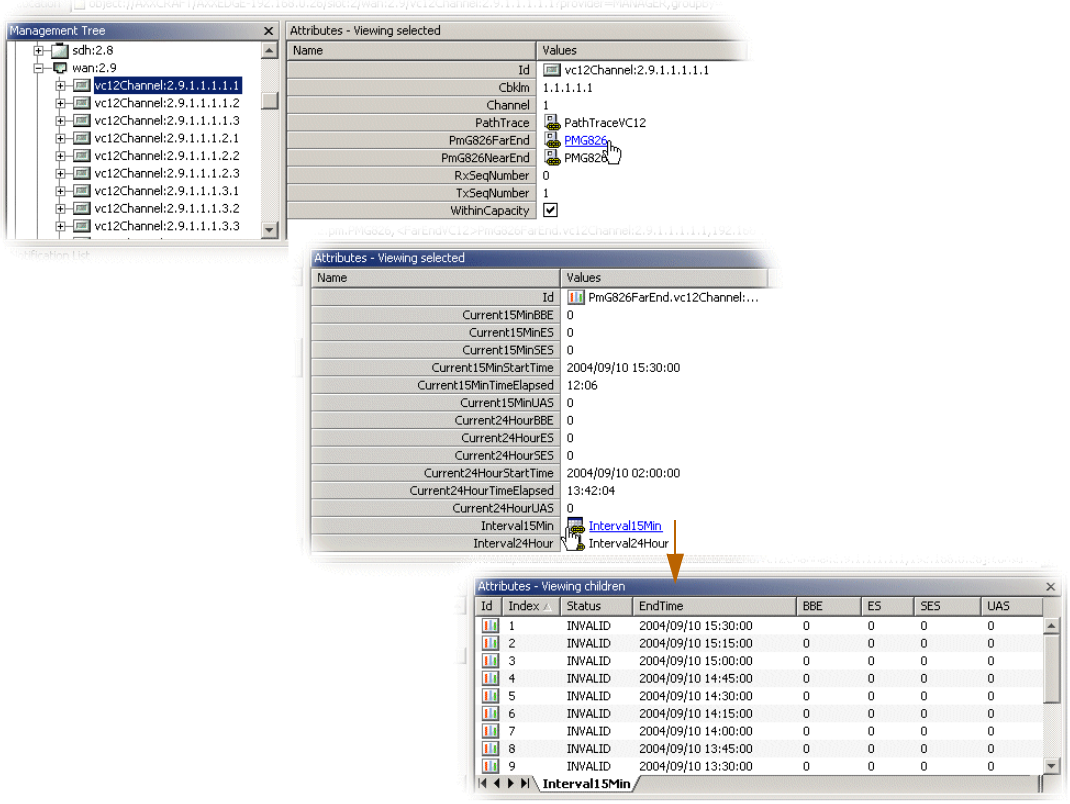


Figure 148 View PM data- Example

9.6.2 View counters

From the Management Tree you can view all managed objects that are monitored objects, for instance:

- LAN ports
- WAN ports
- Bridge
- IP
- IPM
- IPX

Criteria for counting/ Valid-data

Data is set as valid if PM counting criteria is fulfilled, see example “”Corrupted and incomplete measurements in the PM buffers will be

tagged as ‘invalid’. For disabled ports, there is no PM counting: BBE, ES, SES, UAS have value 0, and Valid-flag will not be affected.

Procedure: **G.826 PM COUNTING AND VALID- FLAG:**

When PM counting is performed, the Valid-flag will not be set if one of the following rules apply:

1. The flag will not be set for any 15-min. period (for any levels) if 600 seconds (10 minutes) or less are counted (since counter-reset or device-reset).
2. The flag will not be set for any 24-hour period (for any levels) if 20 hours or less are counted (since counter-reset or device-reset).
3. For RS/MS/VC-4 levels the flag will not be set for any 15-min. if the STM-n port was not defined at the beginning of the period (defined meaning that STM-n port was expected in that slot/port position).
4. For RS/MS/VC-4 levels the flag will not be set for any 24-hour period if rule 3) was true for 80 15-min. intervals (20 hours) or less.
5. For VC-4 level the flag will not be set for any 15-min. period if the AUG-1 is not structured as AU-4 or 3xTUG-3 at the beginning of the period.
6. For VC-4 level the flag will not be set for any 24-hour period if rule 5) was true for 80 15-min. intervals (20 hours) or less.

9.6.2.1 Application of rules to managed objects:

- RS-level valid- data: rules 1,2,3,4
- MS-level valid- data: rules 1,2,3,4
- VC-4-level valid- data: rules 1,2,3,4,5,6
- E3-(/VC-3-) valid- data: rules 1,2
- E1(/VC-12-) valid- data: rules 1,2

- WAN (/VC-12-) valid- data: rules 1,2

9.7 Manage RMON

This section describes management of RMON (Remote Network Monitoring) within a network of Ericsson AXXESSIT network elements.

RMON is an IETF standard (RFC 2819) for monitoring the status of a network by activating probes/monitors at targeted ports in the network, and using RMON clients to collect and present the status information.

About RMON measurements in Ericsson AXXESSIT network elements

With Ericsson AXXESSIT RMON Management, the user can set up local monitoring devices (probes) at selected locations in the managed network. The RMON monitors perform data acquisition and local storage.

An RMON monitor can be set up to accumulate information (perform diagnostics and collect statistics) in local PM buffer, and to log PM associated events or to generate RMON traps to the management system. To collect information, the management system can either poll the monitors regularly or be notified by monitor notifications (SNMP traps), triggered by exception conditions.

9.7.1 RMON overview

Manage time series measurements on local area networks (LANs) and interconnecting E1/E3 lines from a central site with RMON. RMON uses monitoring probes to acquire and store measurements. Remote monitoring according to RMON needs management, and has to be set up specifically.

With RMON management you create RMON monitors, configuring measurement sessions, alarm conditions, logging and alarm generation, and acquire RMON data views.

- **Events** is used to define event types generated from the device.
- **Alarms** is used to set up alarm thresholds for RMON monitoring.

- **History Control** is used to set up the periodic sampling of information from the network element ports, and to configure RMON probes/ monitors.
- **Logs** is used to log selected events from RMON Events.
- **Statistics** contains statistics on each monitored ethernet interface on the network element.

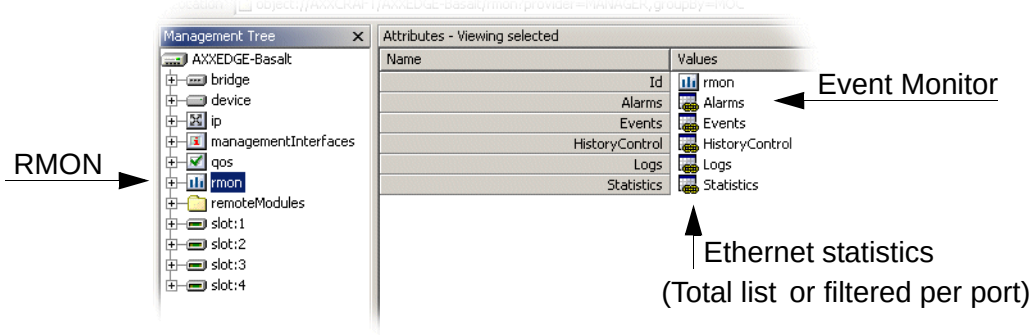


Figure 149 RMON - GUI overview

The following sub- sections explain how to create, configure and inspect RMON monitor(s):

- “Create RMON History Monitor(s)”.
- “Create RMON Event Monitor”.
- “View RMON Data”.

9.7.2 Create RMON Event Monitor

NOTE! Not applicable for AXX 9300 METRO in this release

This section describes how to create a RMON Event Monitor as follows:

a “Define RMON event types”.

b “Configure a RMON Event Monitor”

- “Define a monitor source”
- “Define detection criteria”

Procedure: **DEFINE RMON EVENT TYPES**

Set RMON event types prior to configuring RMON Event Monitors. Events are defined as entries in the **RMON Event Table**. You can choose between the following alternatives:

- Generate log entries (to **RMON Logs**)
- Generate RMON traps (to **Event Trace**, Notification List)
- A **combination** of Log entry and RMON traps (as illustrated in the following sections)

1. **Add** a new event to **RMON Event Table**.
2. Select event **Type** (here: Log entry and SNMP trap).
3. Enter **Community** string for communication with intended trap recipient.

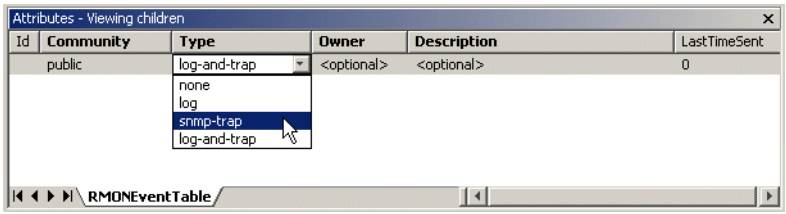


Figure 150 RMON Events-GUI example

4. Enter an **Owner** (optional).
5. Enter a **Description** (optional).
6. Repeat the procedure for as many event definitions as desired.
7. **Save** event definition.

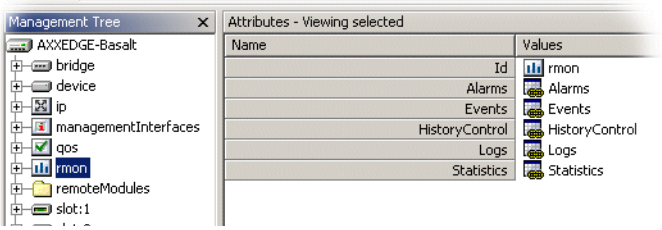
NOTE! **T** The event Id is used in configuring RMON event monitors.

9.0.0.1 Configure a RMON Event Monitor

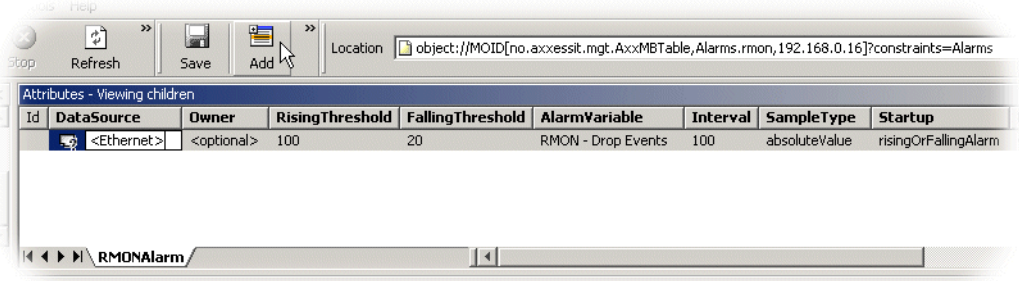
You configure RMON Event Monitor by defining the conditions for event generation from RMON Alarms. If editing an existing monitor, you select the desired table entry.

Procedure: DEFINE A MONITOR SOURCE

1. Select **Alarms** from RMON attributes.



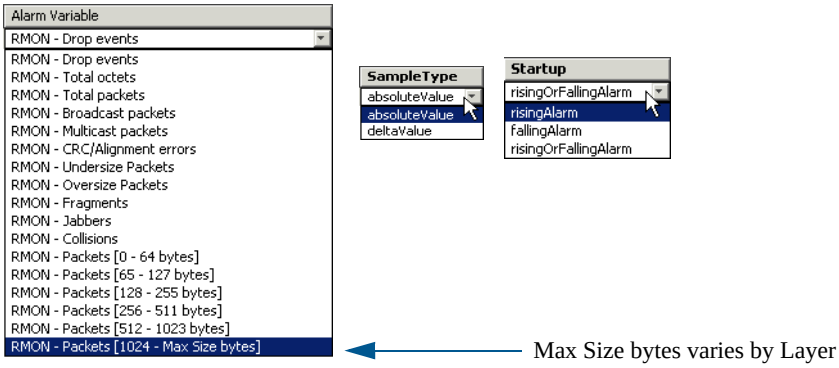
2. **Add** a new monitor entry to RMON Alarm table.



3. Specify a LAN/ WAN port as **DataSource** for desired ethernet interface instance (Port if-index or BridgePortNumber.)

4. Enter an **Owner** for monitor administration (optional).

5. Select the port status to be used in detecting the alarm situation from **AlarmVariable** pull- down list.



Define detection criteria

6. Set **Interval** for the periodic check for alarm conditions.

7. Choose absolute values or delta values from **Sample Type** if the monitor checks alarm conditions (difference between last and current sample).

8. Set the desired alarm **Startup** conditions:

This attribute defines the initial behaviour of the monitor:
Alarms are generated if the monitor is in an alarm situation (below falling threshold or above rising threshold) at startup.

Alarm Rising Threshold (integer - number of occurrences).
The monitor triggers an event when the counter value rises above this level.

Alarm Falling Threshold (integer - number of occurrences).
The monitor triggers an event when the counter value sinks below this level.

Rising Event cross-reference.
A cross reference to the Event Table that identifies the event that is triggered when the monitor registers a rising threshold violation.

Falling Event cross-reference.
A cross reference to the Event Table that identifies the event that is triggered when the monitor registers a falling threshold violation.

9. **Save** RMON event monitor configuration.

The network elements RMON monitor can start generating alarm events for selected ethernet interface.

9.0.1 Create RMON History Monitor(s)

Sampling interval is as defined by the user. Sampling duration is as granted by the network element. Each sample contains the full set of RMON counter data associated with the data source.

An RMON historical monitor maintains both a 'current' and a 'historical' list of statistical data. History Statistics contains the periodical samples from one specific Ethernet interface instance.

1. **Add** a monitor for time series measurements in RMON History Control.

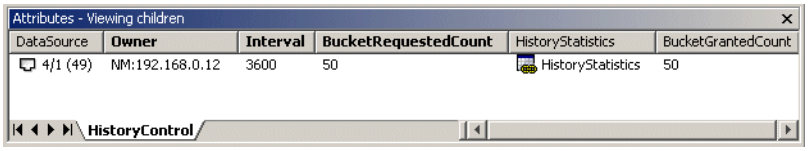


Figure 151 RMON History Monitor- example

2. Specify a LAN/ WAN port as **DataSource** for the desired ethernet interface instance (Port if-index or BridgePortNumber.)
3. Enter an **Owner** (optional).
4. Set polling parameters for each data sampling:
   Poll **interval** in seconds, or poll duration as number of polls in **BucketRequestedCount**.
5. **Save** RMON monitor configuration.
   The network element starts monitoring historical data.
6. Inspect the poll duration of the RMON monitor from **BucketGrantedCount**.

NOTE! The monitored data is based on free-running sets of counters. RMON has no support for detecting counter overflow.

9.1 View RMON Data

RMON data is available for inspection in several RMON tables within the network element:

- **RMON Statistics** present statistics for each monitored ethernet interface. See “Inspection of current statistical data” on page 515.
- **RMON History Statistics** present time series of statistics measurements. See “Inspection of History statistics per port” on page 516.
- **RMON Logs** contain logged events from each monitored interface.
  See “View logged events” on page 517.

- **RMON Traps** are presented in **AXX 9840 INSITE Event Trace** view. This information is not stored on the network element. See “Notification Trace List” on page 135.

You can manage several RMON Monitors in the network element at any time.

For RMON data views, see “Other desktop features” on page 88.

9.1.1 View statistical data

This section describes the following:

- “Inspection of current statistical data”.
- “Inspection of History statistics per port”.

Presented RMON data can be printed to file.

Inspection of current statistical data

1. Press **RMON** in Management Tree.
2. Select **Statistics** from RMON attributes.

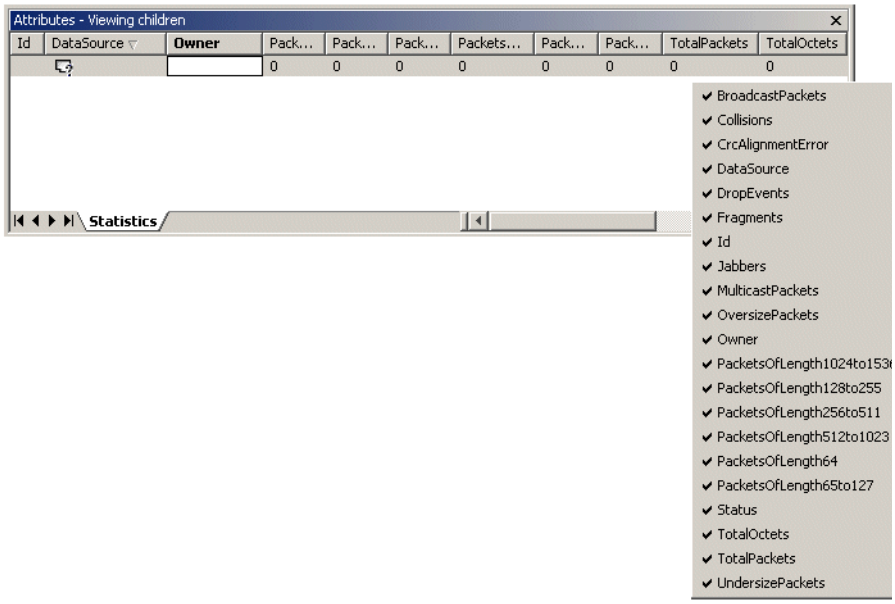


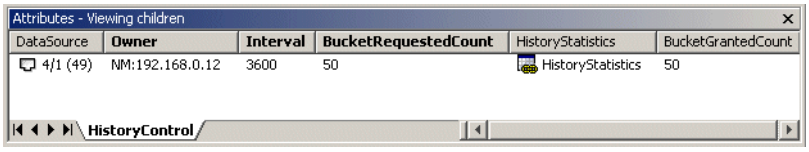
Figure 152 RMON Statistics- GUI overview

The current statistical information of all monitored interfaces for all monitored ports will be presented.

3. Customize visible columns from right- click menu (optional).

9.1.1.1 Inspection of History statistics per port

1. Select **History Control** from RMON attributes.
RMON statistical time series table view for all history monitors and to all the ports is presented.



2. Select the **RMON history monitor** for LAN/ WAN interface you want to inspect.

3. Press **History Statistics** link to view the RMON statistical time series for that specific port.

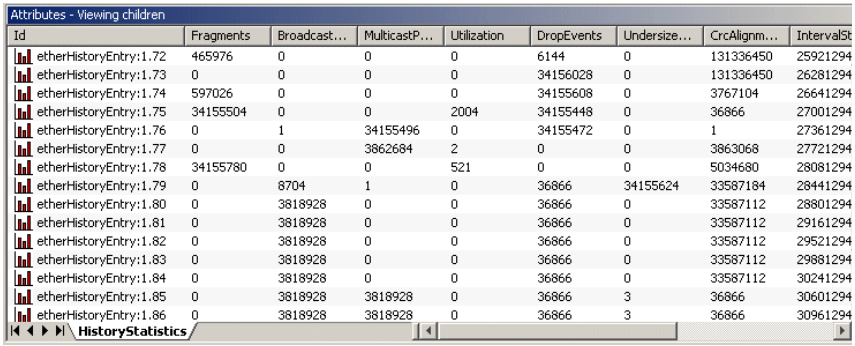


Figure 153 RMON History statistics - example

9.1.2 View logged events

NOTE! Not supported for AXX 9300 METRO in this release

9.1.2.1 Inspection of the Event Log

If the event monitor is configured to log events locally, you can inspect this in the RMON Logs.

1. Select **Logs** from RMON attributes.

All events logged by all monitors within the selected network node will be presented.

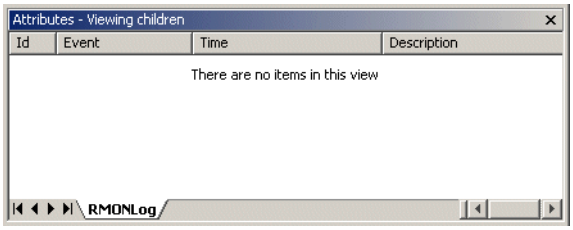


Figure 154 RMON Logs-view

9.1.2.2 Inspection of a filtered Event Log

Inspect events filtered for a specific LAN/ WAN port.

1. Select desired RMON monitor from **RMON Alarms**.
2. Open **RMON Event** logs from **Rising Event** and/ or **Falling events**.

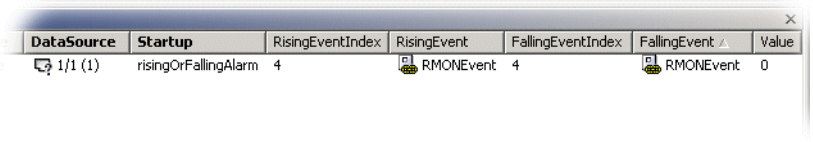


Figure 155 Alarm monitor- example

A filtered table view of the Event Log will be presented, containing all events associated by the selected monitor. All logged events are presented with timestamp and description fields.

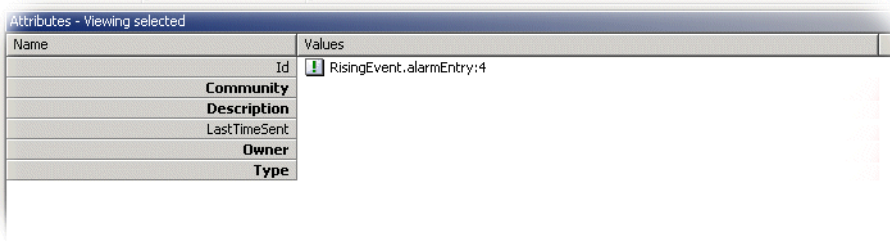


Figure 156 RMON Event log to alarm monitor-view

9.1.3 Delete RMON Monitor

1. Select desired **monitor** (Alarms or History) in the relevant RMON table.
2. Press **Delete**.

RMON monitor (and any RMON event definitions) is removed in from the network element.

RMON data presentation is closed on your desktop. When deleting RMON monitors, the associated log table entries (History Statistics, Event Log entries) are removed automatically.

10 Report tool

10.1 The Report Viewer

The Report Viewer application presents embedded reports with content based on selected parameters. This feature helps you to get an overview of what configuration data are currently implemented in the managed network.

The reports may be used for general analysis of the state of the management system and managed network, or to provide an overview on configured services in the network. To achieve this, the application uses data from the management tree or the management database.

10.1.1 Reports from the Management Tree

Reports may use information presented in the management tree as an input data source:

Network element configuration reports:

- Inventory report
- Commissioning report
- MCN report
- VLAN Settings

Network and communication services reports

- Network topology reports (NE/link/trunk connectivity)

Network element provisioning reports:

- WAN to SDH mapping report

10.1.2 Reports with database as a source

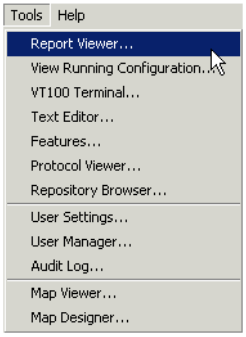
Some management information is stored in data structures not directly associated with structures in the management tree, for instance time series measurements of performance data.

- Bandwidth Utilization
- Link Performance
- VC Performance

In order to see data, the data collection must be turned on.
See the ““PM Tools” on page 488”.

10.1.3 Use the Report Viewer

The application can be accessed from the Tools menu:



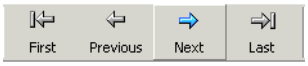
The application opens with the Welcome view which contains initial instructions. Please read the introduction before you carry on.

10.1.4 The toolbar buttons

The toolbar has these buttons, described respectively below:

Open	Opens a dialog where you can browse and open previously stored reports of the format JasperReports(*.jrprint)
Save	Saves your report to the formats pdf and xml
Print	Opens a standard system print dialog
Refresh	Regenerates the current report. This works for the report you just created, without changing the view, only.
Run	Generates a report according to your choices in the “New Report” view

Report viewing options:



First	Jumps to the first page
Previous	Shows the previous page
Next	Shows the next page
Last	Jumps to the last page

Actual	Scales the page to actual size
Fit	Scales the page to fit inside the active window
Width	Scales the page to fit the width in the active window
Zoom in	Enlarges the text
Zoom out	Reducers the text

10.1.5 Create and view reports

Click “New Report” and you will see this page:

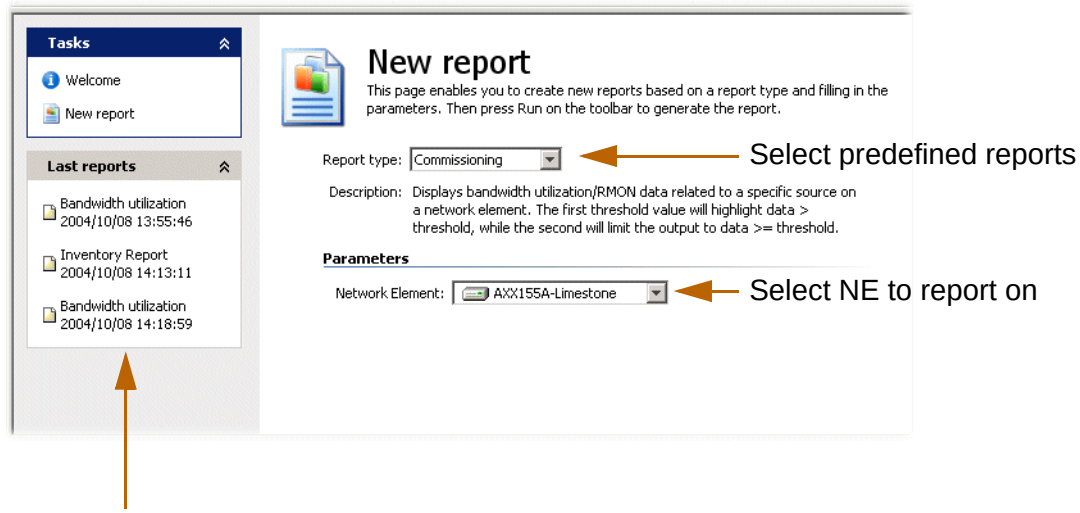


Figure 157 New report interface

The combo box contains a set of predefined reports. These reports collect data from the system in two ways, either through a metadata sql system or with a direct link to the database.

Predefined reports:

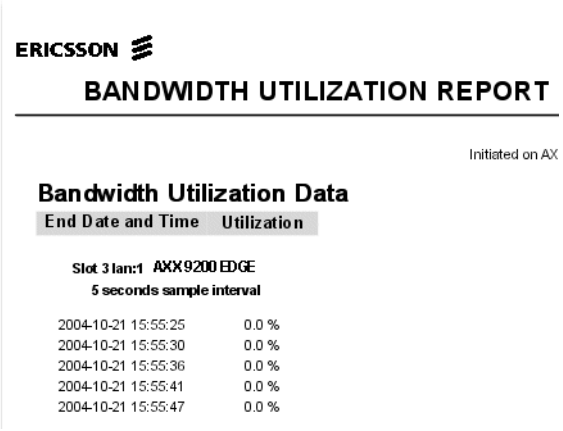
Report type
Bandwidth utilization
Commissioning
Inventory Report
MCN
Link Performance
VC Performance
VLAN
WAN to SDH
Cross Connects
Topology

10.1.5.1 Description of the different reports

Bandwidth utilization

Displays bandwidth utilization/RMON data related to a specific source on a network element. The first threshold value will highlight data > threshold, while the second will limit the output to data >= threshold.

In order to see data, the data collection must be turned on.
See the “PM Tools” user guide available with the licence.


ERICSSON

BANDWIDTH UTILIZATION REPORT

Initiated on AX

Bandwidth Utilization Data

End Date and Time	Utilization
Slot 3 lan:1 AXX9200 EDGE	
5 seconds sample interval	
2004-10-21 15:55:25	0.0 %
2004-10-21 15:55:30	0.0 %
2004-10-21 15:55:36	0.0 %
2004-10-21 15:55:41	0.0 %
2004-10-21 15:55:47	0.0 %

Figure 158 Bandwidth utilization report example

Commissioning

Displays commissioning information for the chosen element.

Figure 159 Commissioning Report example

ERICSSON

Commissioning Report for AXX 9200 EDGE-Basalt

Generated by admin on 2006-06-20 at 17:36:33

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.2.37

Network Element

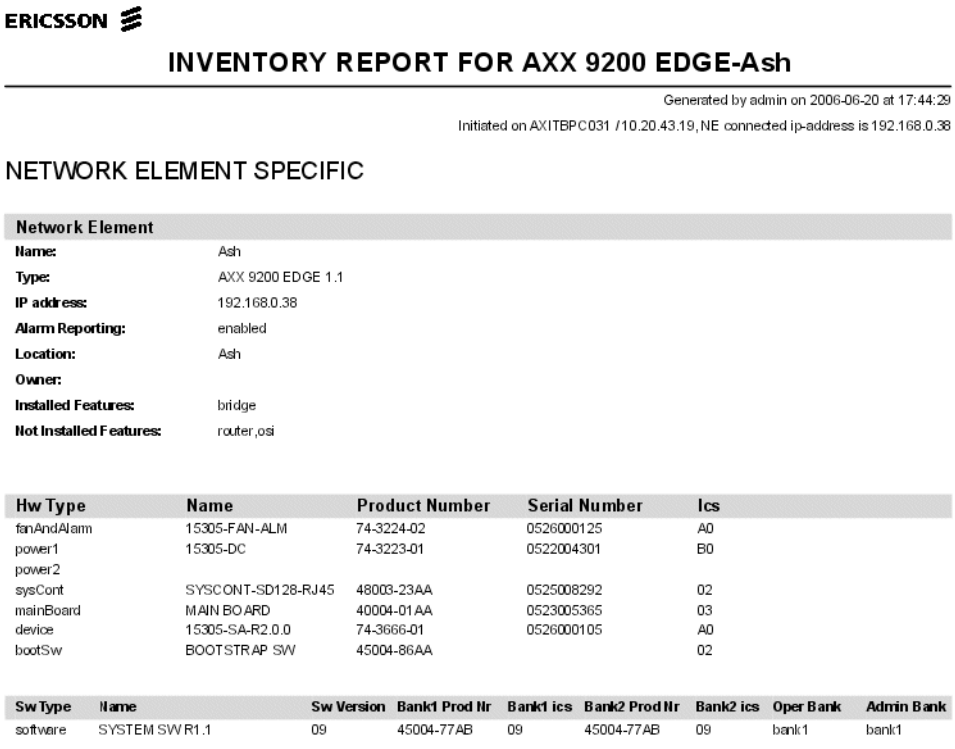
Name:	Basalt
Type:	AXX 9200 EDGE 2.1
IP address:	192.168.2.37
Alarm Reporting:	enabled
Location:	Basalt
Owner:	
Installed Features:	bridge,router,osi
Not Installed Features:	

Hw Type	Name	Product Number	Serial Number	Ics
fanAndAlarm	4XFAN-ALARM-DESUB9	50004-24AA	0310001231	01
power1	-48DCDC-5-100/W-MINI4	50004-06AA	0310001213	02
power2				
sysCont	SYSCONT-SD128-4xRJ45	40004-23AA	0299000004	01
mainBoard	MAIN BOARD	40004-01AA	0303005419	01
device	ONS15305 64x64/20G	74-3103-01	0311001966	02
bootSw	BOOTSTRAP SW	45004-86AA		02

Sw Type	Name	Sw Version	Bank1 Prod Nr	Bank1 ics	Bank2 Prod Nr	Bank2 ics	Oper Bank	Admin Bank
software	SYSTEM SW	06	45004-77BA	12	45004-77BB	06	bank2	bank2
firmware	MAIN CARD FW	06	45004-70AA	06	45004-70AA	06	bank1	bank1
network	Network Release		55004-01BB	06			not applicable	not applicable

Inventory report

Displays the Network Element inventory.
- Device info
- Power info
- Slot and module info



ERICSSON

INVENTORY REPORT FOR AXX 9200 EDGE-Ash

Generated by admin on 2006-06-20 at 17:44:29

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.0.38

NETWORK ELEMENT SPECIFIC

Network Element	
Name:	Ash
Type:	AXX 9200 EDGE 1.1
IP address:	192.168.0.38
Alarm Reporting:	enabled
Location:	Ash
Owner:	
Installed Features:	bridge
Not Installed Features:	router,osi

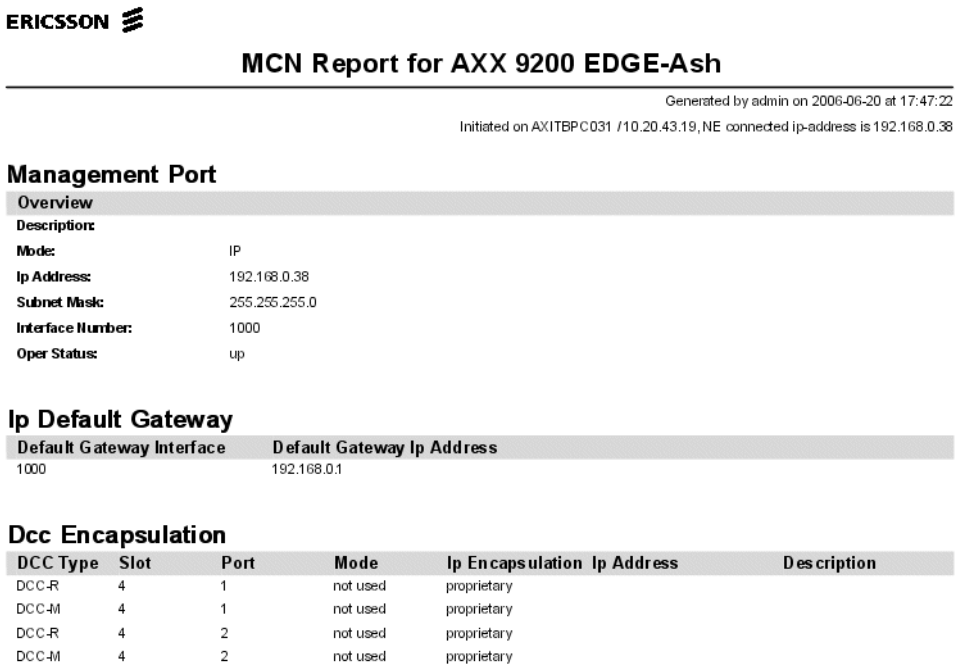
Hw Type	Name	Product Number	Serial Number	Ics
fanAndAlarm	15305-FAN-ALM	74-3224-02	0526000125	A0
power1	15305-DC	74-3223-01	0522004301	B0
power2				
sysCont	SYSCONT-SD128-RJ45	48003-23AA	0525008292	02
mainBoard	MAIN BOARD	40004-01AA	0523005365	03
device	15305-SA-R2.0.0	74-3666-01	0526000105	A0
bootSw	BOOTSTRAP SW	45004-86AA		02

Sw Type	Name	Sw Version	Bank1 Prod Nr	Bank1 ics	Bank2 Prod Nr	Bank2 ics	Oper Bank	Admin Bank
software	SYSTEM SW R1.1	09	45004-77AB	09	45004-77AB	09	bank1	bank1

Figure 160 Inventory Report example

MCN

Displays the MCN data on the chosen network element.



ERICSSON

MCN Report for AXX 9200 EDGE-Ash

Generated by admin on 2006-06-20 at 17:47:22

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.0.38

Management Port

Overview	
Description:	
Mode:	IP
Ip Address:	192.168.0.38
Subnet Mask:	255.255.255.0
Interface Number:	1000
Oper Status:	up

Ip Default Gateway

Default Gateway Interface	Default Gateway Ip Address
1000	192.168.0.1

Dcc Encapsulation

DCC Type	Slot	Port	Mode	Ip Encapsulation	Ip Address	Description
DCC-R	4	1	not used	proprietary		
DCC-M	4	1	not used	proprietary		
DCC-R	4	2	not used	proprietary		
DCC-M	4	2	not used	proprietary		

Figure 161 MCN Report example

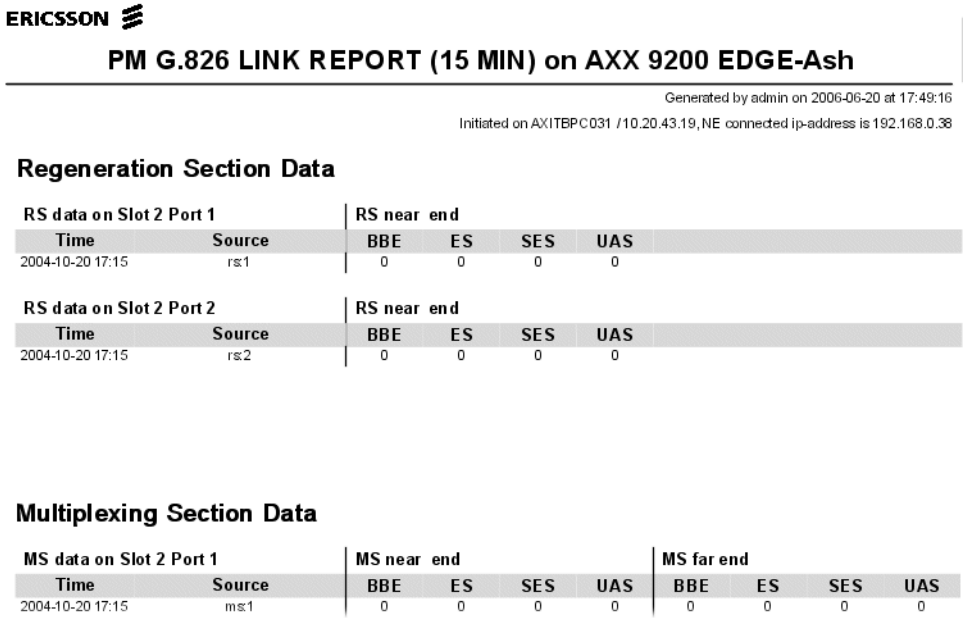
Link performance

Displays G826 performance data related to MS and RS objects. The data selection is based on the decided time interval and selected network element. Data values above the first set of threshold values will be colored in red. The second set of threshold values delimits the output to data >= threshold values.

ES	Errored Seconds
SES	Severely Errored Seconds
BBE	Block Background Errors
UAS	Unavailable Seconds

See the ““PM Tools” on page 488” for detailed information about the parameters

The report requires that a monitor is starter in order to display any data.



ERICSSON

PM G.826 LINK REPORT (15 MIN) on AXX 9200 EDGE-Ash

Generated by admin on 2006-06-20 at 17:49:16

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.0.38

Regeneration Section Data

RS data on Slot 2 Port 1		RS near end			
Time	Source	BBE	ES	SES	UAS
2004-10-20 17:15	rs:1	0	0	0	0

RS data on Slot 2 Port 2		RS near end			
Time	Source	BBE	ES	SES	UAS
2004-10-20 17:15	rs:2	0	0	0	0

Multiplexing Section Data

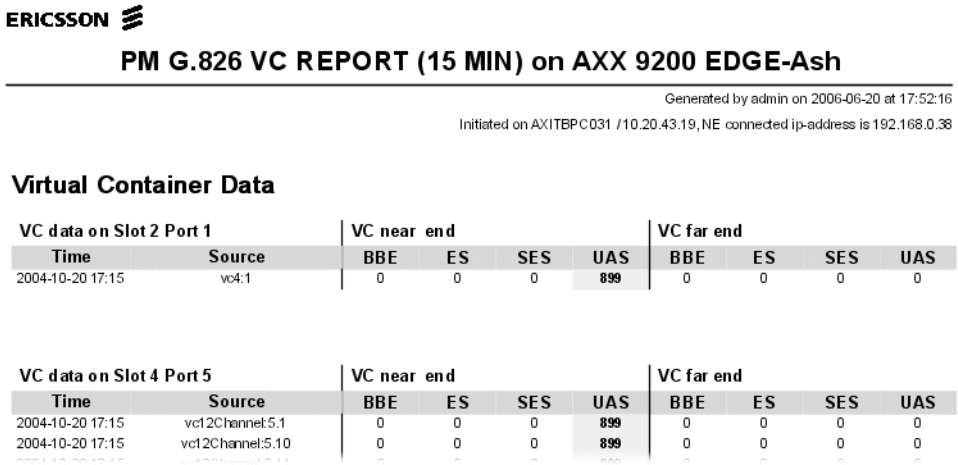
MS data on Slot 2 Port 1		MS near end				MS far end			
Time	Source	BBE	ES	SES	UAS	BBE	ES	SES	UAS
2004-10-20 17:15	ms:1	0	0	0	0	0	0	0	0

Figure 162 Link Performance Report example

VC performance

Displays G826 performance data related to VC objects. The data selection is based on the decided time interval and selected network element. Data values above the first set of threshold values will be colored in red. The second set of threshold values delimits the output to data >= threshold values.

The report requires that a monitor is starter in order to display any data.



ERICSSON

PM G.826 VC REPORT (15 MIN) on AXX 9200 EDGE-Ash

Generated by admin on 2006-06-20 at 17:52:16

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.0.38

Virtual Container Data

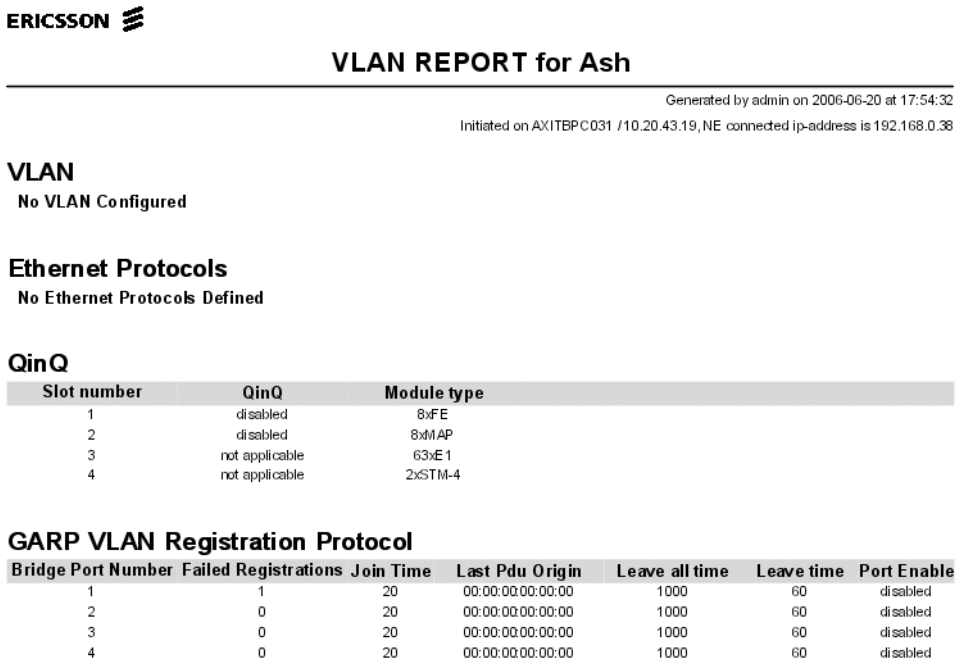
VC data on Slot 2 Port 1		VC near end				VC far end			
Time	Source	BBE	ES	SES	UAS	BBE	ES	SES	UAS
2004-10-20 17:15	vc4:1	0	0	0	899	0	0	0	0

VC data on Slot 4 Port 5		VC near end				VC far end			
Time	Source	BBE	ES	SES	UAS	BBE	ES	SES	UAS
2004-10-20 17:15	vc12Channel:5.1	0	0	0	899	0	0	0	0
2004-10-20 17:15	vc12Channel:5.10	0	0	0	899	0	0	0	0

Figure 163 VC Performance report

VLAN

Displays the VLAN settings for the chosen network element.



ERICSSON

VLAN REPORT for Ash

Generated by admin on 2006-06-20 at 17:54:32

Initiated on AXITBPC031 /10.20.43.19, NE connected ip-address is 192.168.0.38

VLAN

No VLAN Configured

Ethernet Protocols

No Ethernet Protocols Defined

QinQ

Slot number	QinQ	Module type
1	disabled	8xFE
2	disabled	8xMAP
3	not applicable	63xE1
4	not applicable	2xSTM-4

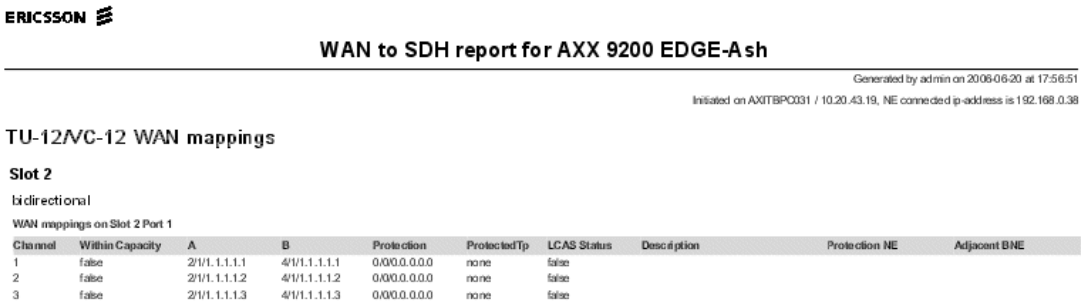
GARP VLAN Registration Protocol

Bridge Port Number	Failed Registrations	Join Time	Last Pdu Origin	Leave all time	Leave time	Port Enable
1	1	20	00:00:00:00:00:00	1000	60	disabled
2	0	20	00:00:00:00:00:00	1000	60	disabled
3	0	20	00:00:00:00:00:00	1000	60	disabled
4	0	20	00:00:00:00:00:00	1000	60	disabled

Figure 164 VLAN report example

WAN to SDH

Displays all WAN mappings configured on the chosen network element.



ERICSSON

WAN to SDH report for AXX 9200 EDGE-Ash

Generated by admin on 2006-06-20 at 17:56:51

Initiated on AXITBPC031 / 10.20.43.19, NE connected ip-address is 192.168.0.38

TU-12/VC-12 WAN mappings

Slot 2

bidirectional

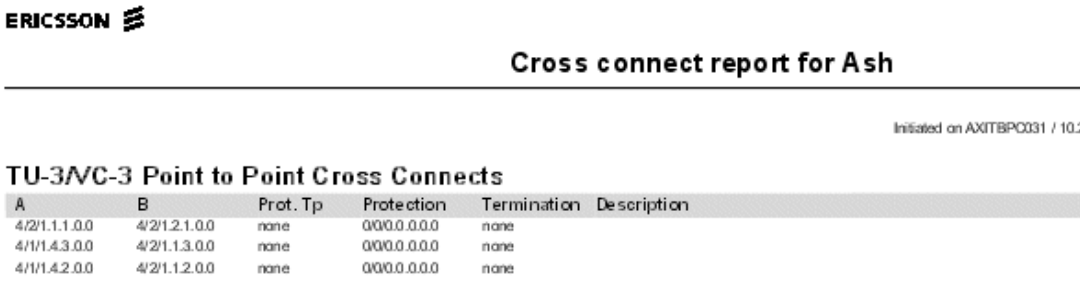
WAN mappings on Slot 2 Port 1

Channel	Within Capacity	A	B	Protection	ProtectedTp	LCAS Status	Description	Protection NE	Adjacent BNE
1	false	2/1/1.1.1.1.1	4/1/1.1.1.1.1	0/0/0.0.0.0.0	none	false			
2	false	2/1/1.1.1.1.2	4/1/1.1.1.1.2	0/0/0.0.0.0.0	none	false			
3	false	2/1/1.1.1.1.3	4/1/1.1.1.1.3	0/0/0.0.0.0.0	none	false			

Figure 165 Wan to SDH report example

Cross connects

Displays all cross connects configured on the chosen network element.



ERICSSON

Cross connect report for Ash

Initiated on AXITBPC031 / 10.

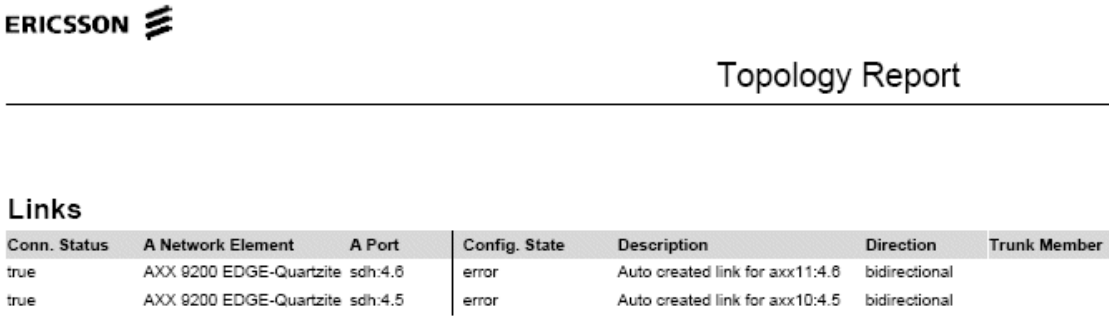
TU-3/VC-3 Point to Point Cross Connects

A	B	Prot. Tp	Protection	Termination	Description
4/2/1.1.1.0.0	4/2/1.2.1.0.0	none	0/0/0.0.0.0.0	none	
4/1/1.4.3.0.0	4/2/1.1.3.0.0	none	0/0/0.0.0.0.0	none	
4/1/1.4.2.0.0	4/2/1.1.2.0.0	none	0/0/0.0.0.0.0	none	

Figure 166 Cross connects report example

Topology report

Displays topology information about the chosen network element..



ERICSSON

Topology Report

Links

Conn. Status	A Network Element	A Port	Config. State	Description	Direction	Trunk Member
true	AXX 9200 EDGE-Quartzite	sdh:4.6	error	Auto created link for axx11:4.6	bidirectional	
true	AXX 9200 EDGE-Quartzite	sdh:4.5	error	Auto created link for axx10:4.5	bidirectional	

Figure 167 Topology Report example

11 Layer 2 Configuration

11.1 Introduction

11.1.1 Brief description

The purpose of this chapter is to guide you through management of the bridging service (L2 forwarding) on the network element.

This includes:

- Presentation and modification of the bridge,
- Presentation and modification of MAC Multicast and IGMP Snooping,
- Presentation and modification of spanning tree protocol (STP) and Rapid STP (RSTP),
- Presentation and modification of traffic control.
- Presentation and modification of VLAN

NOTE! The following examples focus on AXX 9200 EDGE, but the features described also apply for AXX 9300 METRO 1.0 , AXX 9100 CONNECT and AXX155E.

11.2 Bridge

11.2.1 Introduction

This chapter describes the configuration operations supported by the Bridge managed object (M.O.). It is organized in 3 sections:

- Introduction
- Examples: this chapter is a repository of simple, but yet typical configuration scenarios.

- Troubleshooting and FAQ: this chapter contains a few troubleshooting tips, and gives answers to a number of Frequently Asked Questions.

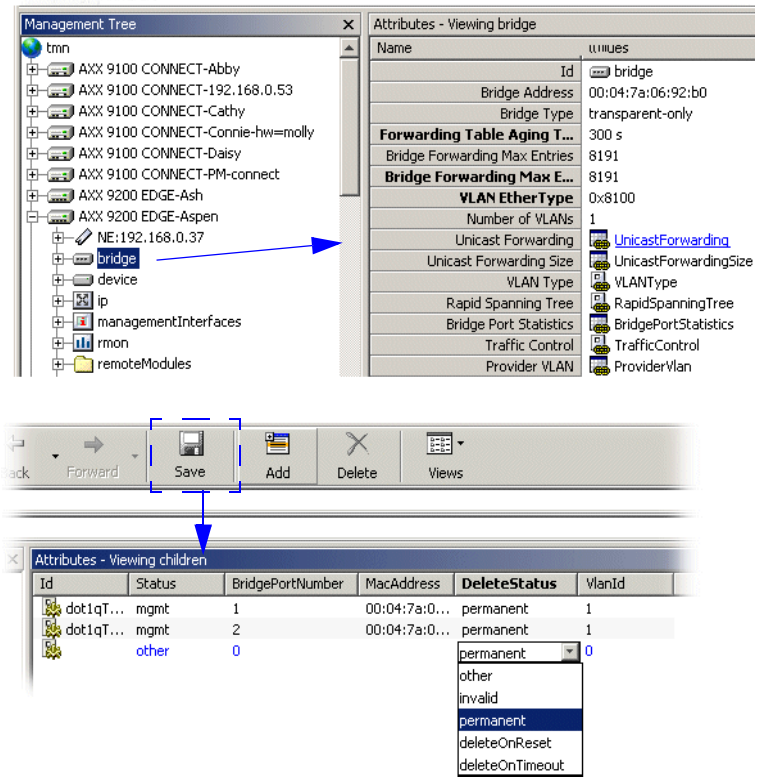
11.3 Examples

11.3.1 Configuration of static unicast forwarding information

11.3.1.1 AXX 9100 CONNECT and AXX 9200 EDGE

To configure an entry in the MAC unicast forwarding table:

1. In the Management Tree, click the **NE** managed object, and then the **Bridge** managed object.
2. Click on **UnicastForwarding** in the attributes window.



3. Click **Add** on the toolbar.
4. The following attributes have no default values, and must be defined:

bridgePortNumber: Set the bridge port number of the port through which the MAC address can be reached.

macAddress: Set the MAC address. The MAC address must be a unicast address.

vlanId: Set the VLAN ID for which this entry applies.

deleteStatus: Set '**permanent**' **if** the entry should not be removed dynamically from the table (such an entry will stay over a reset of the bridge).Set '**deleteOnReset**' **if** the entry should be removed dynamically from the table after the next reset of the bridge.Set '**deleteOnTimeout**' if the entry should be dynamically aged out by the bridge.

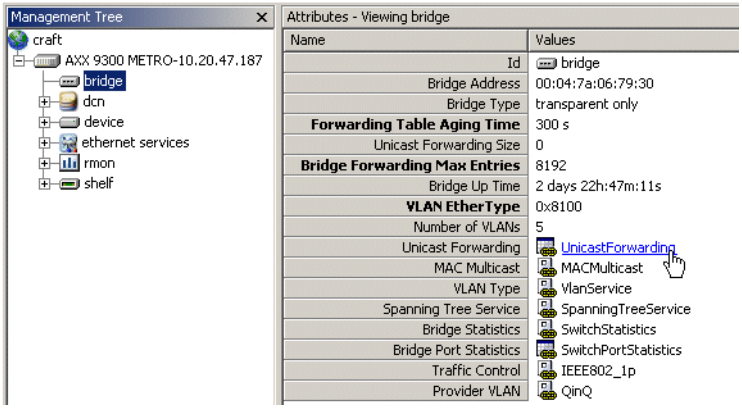
5. Save.

11.3.1.2 AXX 9300 METRO

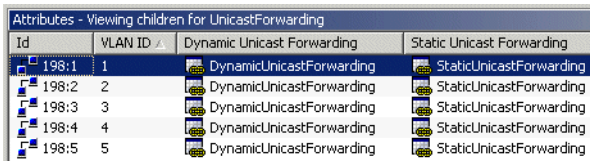
To configure an entry in the MAC unicast forwarding table:

1. In the Management Tree, click the **NE** managed object, and then the **Bridge** managed object.

2. Click on **UnicastForwarding** in the attributes window.



3. Select Static Unicast Forewarding



4. Click **Add** on the toolbar.

5. The following attributes have no default values, and must be defined:

Port: Select the port through which the MAC address can be reached.

MAC Address: Set the MAC address. The MAC address must be a unicast address.

VLAN ID: Set the VLAN ID for which this entry applies.

StaticStatus:
Set '**permanent**' if the entry should not be removed dynamically from the table (such an entry will stay over a reset of the bridge).Set '**deleteOnReset**' if the entry should be removed dynamically from the table after the next reset of the bridge.

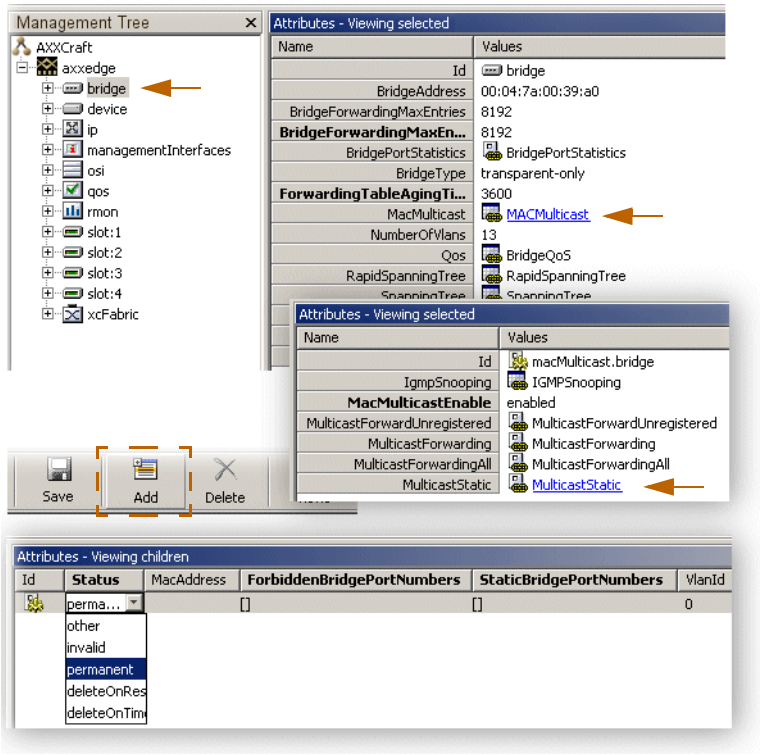
6. Save.

11.3.2 Configuration of static multicast forwarding information

To configure an entry in the MAC multicast forwarding table:

1. Click on the AXX 9200 EDGE managed object, and then the Bridge managed object in the Management Tree.

2. Click on **MACMulticast**, then on **MulticastStatic** in the attributes window.



3. Click **Add** on the toolbar.

4. The following attributes have no default values, and must therefore be defined:
   vlanId: Set the VLAN ID for which this entry applies.

   MacAddress: Set the MAC address. The MAC address must be a multicast or broadcast address.

   StaticBridgePortNumbers: Set the set of ports through which the multicast/broadcast frame must be forwarded regardless of any dynamic information. The set of ports is entered as an octet string where each bit represents one port (see 5.2.3 in the FAQ section for additional information).

   ForbiddenBridgePortNumbers: Set the set of ports through which the frames must not be forwarded regardless of any dynamic information. The set of ports is entered as an octet string where each bit represents one port (see 5.2.3 in the FAQ section for additional information).

   Status: Set 'permanent' if the entry should not be removed dynamically from the table (such an entry will stay over a reset of the bridge).Set 'deleteOnReset' if the entry should be removed dynamically from the table after the next reset of the bridge.Set 'deleteOnTimeout' if the entry should be dynamically aged out by the bridge.

5. Save.

NOTE! When a multicast forwarding information is added to the table, the same entry is automatically added to the Bridge > macMulticast >multicastForwarding attribute. The multicastForwarding attribute contains both static, i.e. user-defined, and learned entries related to group (multicast) addresses.

11.3.3 IGMP Snooping

When a host wants to receive multicast traffic, it must inform the routers on its LAN. The Internet Group Management Protocol (IGMP) is the protocol used to communicate group membership information between hosts and routers on a LAN. Based on the information received through IGMP, a router forwards multicast traffic only via interfaces known to lead to interested receivers (hosts).

On the contrary, bridges flood multicast traffic out all ports per default, and therefore waste valuable network resources. IGMP snooping on a bridge can eliminate this inefficiency. IGMP snooping looks at IGMP messages to determine which hosts are actually interested in receiving multicast traffic. Based on this information, the bridge will forward multicast traffic only to ports where multicast receivers are attached.

Enabling IGMP snooping

To enable IGMP snooping on the network element:

1. Click on the **Bridge** managed object in the Management Tree.
2. Click on the **MACMulticast** attribute in the attribute window.
3. Set the **MAC Multicast Enable** attribute to "**enabled**".
4. Click on the **igmpSnooping** attribute in the attribute window.
5. Set the **IGMP SnoopingEnable** attribute to "**enabled**".
6. **Save**.

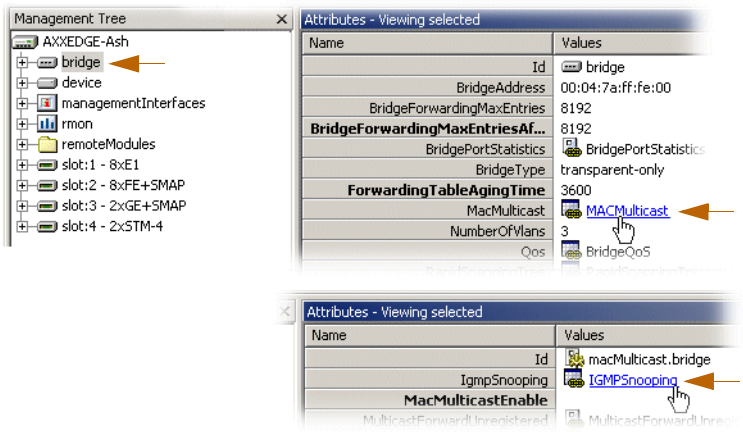


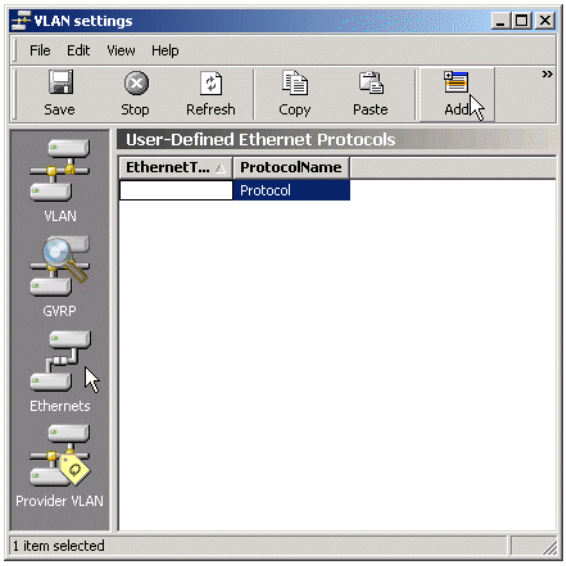
Figure 168 Enabling IGMP Snooping

11.3.4 Configuration of an Ethernet user defined protocol

The ethernetDefinedProtocol attribute allows you to define a non-predefined protocol based on the etherType field of Ethernet frames. This user-defined protocol is further used to create protocol-based VLANs.

To configure an Ethernet user defined protocol:

1. Select **VLAN Settings** from the **Brigde** menu
2. Click **Ethernets** in the Content pane.



3. Click **Add** (if no protocol is already defined). If a protocol is already defined, both fields described in step 4 can be directly edited.).
4. Set the **EthernetType** attribute to the value of the **EtherType**[1] indicating the required protocol. The **ProtocolName** attribute can optionally be used to give **a user-friendly name** to the protocol.
5. Save.

Example

Assuming that a user wants to define a VLAN based on the Address Resolution Protocol (ARP), the ethernetType must be set to 0806 (in hex), and the protocolName attribute could be, for example, set to "ARP" to identify the protocol.

NOTE! The Ethernet user defined protocol is relevant only when the network element runs VLAN per protocol and port.

Maximum one Ethernet user defined protocol can be currently defined on the network element.

1. The EtherType numbers are maintained by the Internet Assigned Numbers Authority (IANA), and can be accessed on the Web at the following address: http://www.iana.org/assignments/ethernet-numbers

To use the Ethernet user defined protocol as a VLAN protocol for a particular VLAN, set the protocolType attribute under Bridge > VLAN to ethUserDefined. The protocol attribute under Bridge > VLAN, which is used to identify a specific protocol, must then always be set to 1, since there is maximum one Ethernet user defined protocol.

11.4 Miscellaneous

11.4.1 Spanning Tree Protocol Configuration

The Spanning Tree Protocol (STP/RSTP) allows layer 2 devices to discover a subset of the topology that is loop-free, but still with a path between every pairs of LANs.

Previous versions of the product supported common STP according to IEEE 802.1D 1998. This versions supports Rapid Spanning Tree Protocol (RSTP) according to 802.1D 2004, which is compatible with STP.

By default (when enabled) the device is setup to run RSTP, but when inserted in a topology which runs STP, the algorithm will adapt to run this version instead.Configuring the STP algorithm per device

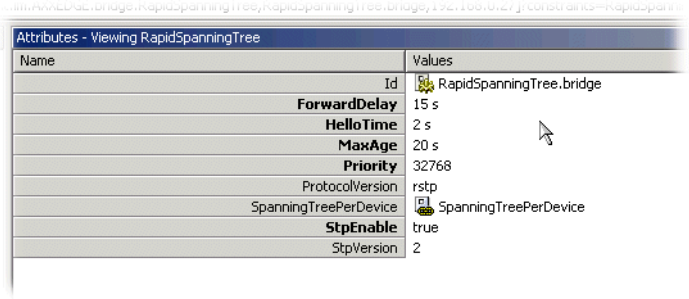
11.4.2 Rapid Spanning Tree Protocol configuration

The AXX 9200 EDGE 2.0 and AXX155E 3.0 network elements support RSTP (Rapid Spanning Tree) according to IEEE 802.1w.

To configure RSTP on a port:

In the example below AXX 9200 EDGE is used.

1. Click on the **AXX 9200 EDGE** managed object, and then on the **Bridge** managed object in the Management Tree.



2. Click on the **RapidSpanningTree** attribute in the attribute window.
3. Set **stpEnable** to '**true**'.
4. Edit the **forwardDelay**, **helloTime**, **maxAge**, and **priority** attributes if required.
5. Click **Save**.
6. Click on the **SpanningTreePerDevice** attribute in the attribute window.
7. Edit the **BelongToVLAN** attribute as required (if this attribute is set to '**true**', only ports members of a VLAN will participate in the RSTP algorithm).
8. Click **Save**.
9. Optionally, the **Priority**, **Cost**, and **PortEnable, AdminEdgePortStatus, AdminPointToPointStatus** attributes can be edited per port. To do so, click on the **SpanningTreePort attribute**, and modify the attributes as required.
10. Click **Save**.

11.4.3 MAC Multicast

Multicast is a method of sending one packet to multiple destinations. Multicasting is used for applications such as video conferencing, and for distribution of certain information like some routing protocols. A standard IEEE 802.1D bridge will forward multicast frames on all ports that are members of the same VLAN as the port receiving such frames. This might not be desirable if the there is a lot of multicast traffic being transported through a multi-port bridge

where the recipients are connected on only one (or a few) of the bridge ports. To alleviate unnecessary bandwidth consumption, the AXX155E and AXX 9200 EDGE supports specific tables to control the forwarding of Multicast traffic if desired. Both devices also supports IGMP (Internet Group Management Protocol) snooping which is used to update the multicast tables based on the IGMP messaging between end nodes and IP multicast routers.

Note that multicast traffic will be forwarded as usual if this feature is not enabled, and that the use of these tables are only necessary for performance tuning.

11.4.3.1 Enabling MAC Multicast Control Tables

The internal resources of the AXX155E /AXX 9200 EDGE used for the multicast tables are shared with the VLAN tables. The total of VLAN entries and multicast groups registered are 4000, and both types of entries occupy the same amount of resources. Hence, to enable the Multicast feature, ensure that the maximum amount of VLANs is less than 4000 according to how many multicast groups anticipated. For most applications 4000 VLAN are well above what will be used, and in these cases one can safely reserve a good chunk of entries for multicast traffic.

11.4.3.2 Configuring MAC Multicast

Multicast menu has the following menu options:

- IGMPSnooping
- MacMulticastEnable
- MulticastForwardUnregistered.
- MulticastForwarding.
- MulticastForwardingAll.
- MulticastStatic

The parameter MacMulticastEnable is for enabling/disabling of the MAC Multicast control tables.

11.4.3.3 MulticastForwarding

The Forwarding-Table contains multicast filtering information configured into the bridge, or information learned through IGMP Snooping. The Forwarding-Table information specifies the allowed

egress ports for a given multicast group address on a specific VLAN, and indicates for which ports (if any) this information has been learnt from IGMP snooping.

VLAN-TAG-ID: Identifies the VLAN to which the filtering information applies.

MULTICAST-ADDRESS: Identifies the destination group MAC address to which the filtering information applies.

EGRESS-PORTS: Indicates the configured egress ports for the specified multicast group address. This does not include ports listed in the Forward All Ports list for this address.

LEARNT: Indicates a subset of ports from the Egress Ports list which were identified by IGMP Snooping and added to the multicast filtering database.

11.4.3.4 MulticastForwardingAll

The Forward-All-Table allows ports in a VLAN to forward all multicast packets.

VLAN-TAG_ID: Identifies the VLAN to which the filtering information applies.

EGRESS-PORTS: Specifies which ports on a VLAN can participate in a Forward Unregistered group. The default setting is all ports.

FORBIDDEN-PORTS: Specifies which ports on a VLAN are restricted from participating in a Forward All group.

STATIC PORTS: Indicates if the egress ports are static or dynamic configured.

11.4.3.5 MulticastForwardUnregistered

The Multicast-Forward-Unregistered-Table defines the behaviour of ports regarding forwarding of packets that is not covered by any of the other tables.

VLAN-TAG_ID: Identifies the VLAN to which the filtering information applies.

EGRESS-PORTS: Specifies which ports on a VLAN can participate in a Forward Unregistered group. The default setting is all ports.

FORBIDDEN-PORTS: Specifies which ports on a VLAN are restricted from participating in a Forward Unregistered group.

STATIC PORTS: Indicates if the egress ports are static or dynamic configured.

11.4.3.6 MulticastStatic

The Static-Table contains manually configured filtering information for specific multicast group addresses. This includes information about allowed and forbidden egress ports, and is also reflected in the Forwarding-Table.

VLAN-TAG_ID: Identifies the VLAN to which the filtering information applies.

MULTICAST-ADDRESS: Identifies the destination group MAC address of a frame to which the filtering information applies.

STATIC-EGRESS-PORTS: Indicates a set of ports to which packets received from, and destined to, are always forwarded. This is regardless of the IGMP Snooping setting.

FORBIDDEN-PORTS: Indicates the set of ports to which packets received from and destined to a specific port must not be forwarded. This is regardless of the IGMP Snooping setting.

STATUS: The possible values are:

Permanent—The table entry is currently in use. When the bridging status is reset this table entry remains in use.

Delete on Reset—This table entry is currently in use. However, when the bridging status is reset the entry is deleted

Delete on Timeout—This table entry is currently in use. However when the bridge times out the entry is deleted.

Modification of the Multicast Forward All Table and Multicast Forward Unregistered Table involves edition of the "Forbidden Ports" and/or "Static Ports" lists. The user edits the "Forbidden Ports" list and the "Static Ports" list on both the Multicast Forward All Table and the Multicast Forward Unregistered Table.

Ports already present in a "Forbidden Ports" list cannot be added to a "Static Ports" list.

11.4.4 Traffic Control

11.4.4.1 View Traffic Control

The user selects the Traffic Control object in the Management Tree. The system presents all attributes related to Traffic Control as specified by the information model.

11.4.4.2 Modify Traffic Control

The Traffic Control menu has the following menu options:

- PortPriority
- PriorityGroup
- TrafficClass.

11.4.4.3 PortPriority

BridgePortNumber: a port number identifying one of the on the device. For each row, the information in the row applies to the port identified in this column.

DefaultPriority: this is the priority value assigned to frames arriving at this port, when implicit priority determination is used. Any frames arriving at this port, not carrying a priority value in a tag, will get the DefaultPriority value as priority. The value is an IEEE 802.1p priority level. Range is 0 – 7, inclusive.

NumberOfTrafficClasses: gives the number of classes of service – that is, the number of output queues, for the port. All ports on the device will always use 4 queues.

11.4.4.4 PriorityGroup

BridgePortNumber: a port number identifying one of the on the device. For each row, the information in the row applies to the port identified in this column.

PriorityGroup: indicates which ports are located on the same module, and are thus using the same priority configuration. The AXX 9200 EDGE has a theoretical maximum of 65 ports, which are all listed in this table whether or not they are present. PriorityGroup 32 indicates that the port is not present (i.e. the corresponding slot holds a STM-n module which has no Ethernet interfaces).

11.4.4.5 TrafficClass

Classification of ethernet frames are done according to the information in the TrafficClass table. The device use four queues for differentiating traffic, and as 802.1p defines eight different priorities, the priorities must be mapped into those four queues. The default mapping scheme is as recommended by IEEE, but this is configurable by the operator.

Priority Level	Class of Service
6, 7	**3**
4, 5	2
0, 3	1
1, 2	0

Recommended mapping when using four queues.

BridgePortNumber: a port number identifying one of the on the device. For each row, the information in the row applies to the port identified in this column.

Priority: priority value according to 802.1p. Legal values 0-7.

TrafficClass: indicates which service queue the selected priority value is to be mapped to. Legal values 0-4 (4 is highest priority).

11.5 Manage VLAN

11.5.1 Introduction

The purpose of this section is to guide you through management of a VLAN (virtual local area network) on the network element.

A network element can be configured to run either VLAN per port or VLAN per port and per protocol.

The section also involves management of the complete life cycle of a VLAN, including:

- Creation, presentation, modification, and deletion of a VLAN
- Creation, presentation, modification, and deletion of an Ethernet User Defined Protocol
- Presentation and modification of GVRP (Generic Attribute Registration Protocol VLAN Registration Protocol)

11.5.2 Virtual Local Area Networks

A LAN consists of a number of computers that share a common communication line within a small geographical area. A Virtual LAN is a LAN where the grouping of computers are based on logical connections, e.g. by type of users, by department etc. It is easier than for a physical LAN to add and delete computers to/from a VLAN and to manage load balancing. The management system relates the virtual picture and the physical picture of the network.

The network element supports two types of VLAN

- Per port
- Per port and protocol

Both types of VLANs cannot be run simultaneously on the network element, i.e., either all VLANs per port or all per port and per protocol. The protocol can either be one from a set of predefined protocols or from Ethernet protocols defined by you. Different Ethernet protocol types can be IP, IPX, Appletalk, etc. The network element supports GVRP, i.e., automatic set up of VLAN in non edge nodes in a VLAN.

The number of Ethernet-ports in AXX 9200 EDGE which can be assigned to a VLAN, is limited to 64. The maximum number of Ethernet-ports per slot is 16. Also see “How many VLANs does the network element support?” on page 579.

There are three steps involved in the definition of VLAN on the network element.

- A common VLAN type is defined for the Bridge
- A set of common parameters for a new VLAN is defined
- New ports can be added to a VLAN

It is assumed you have the appropriate rights to perform management operations.

11.6 VLAN provisioning

AXX 9840 INSITE has a custom graphical user interface (GUI) for VLAN provisioning, see Figure 169 The VLAN Setting GUI makes VLAN related configuration easier for the user by grouping together a number of managed objects and attributes under a unique GUI.

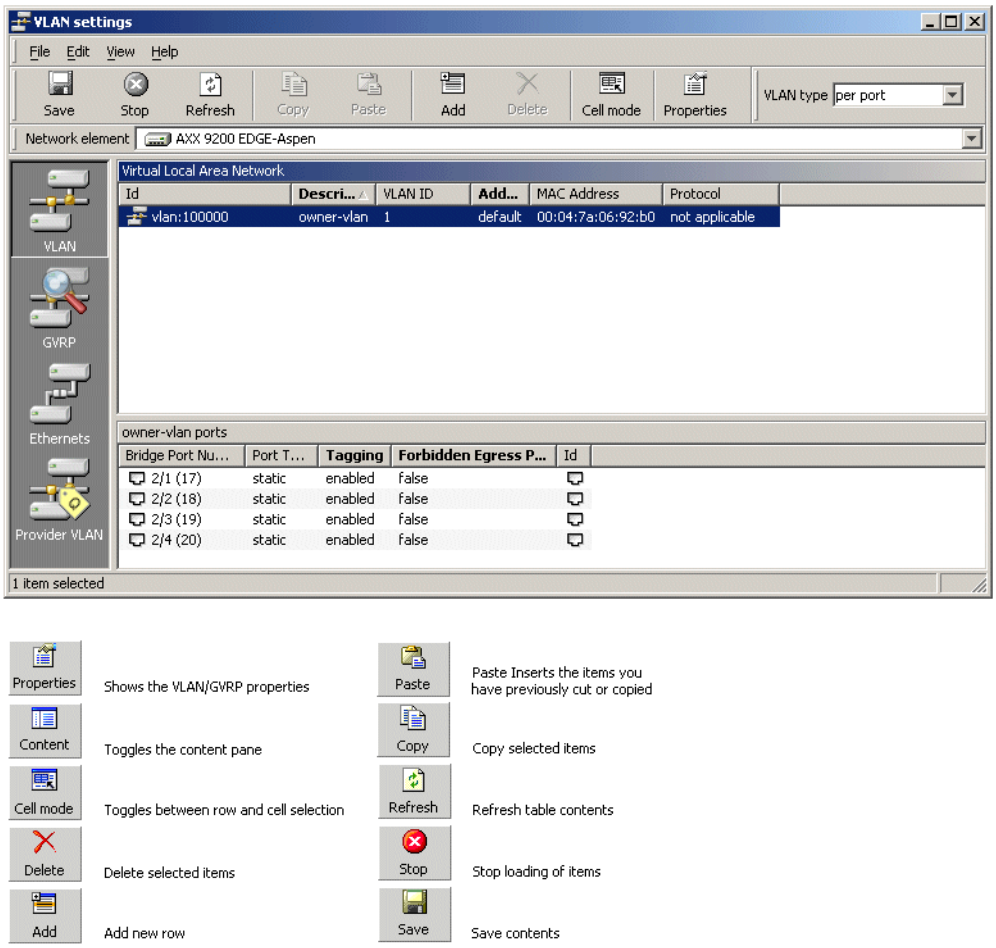


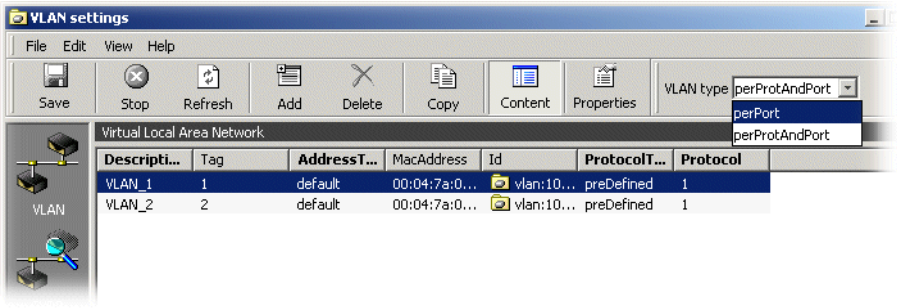
Figure 169 VLAN Settings - Overview

The following examples show how a VLAN per port, and a VLAN per port and protocol can be created and provisioned by using the custom GUI. The VLAN custom GUI can be opened either by clicking on VLAN Setting under the Bridge menu on the AXX 9840 INSITE desktop, or by right-clicking on Bridge M.O. in the Management Tree, and then selecting VLAN Setting.

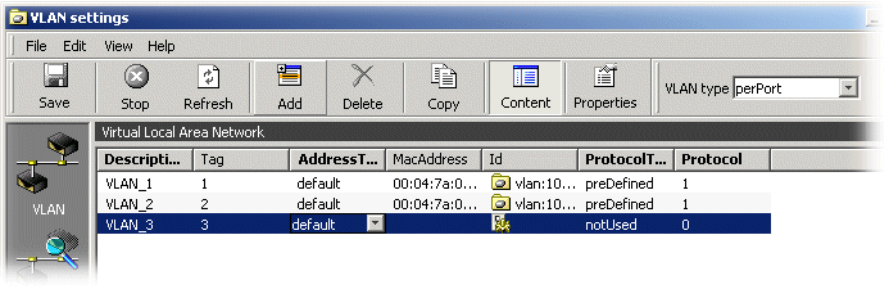
11.6.1 Configuration of a new VLAN per port

Procedure: **CREATE A NEW VLAN PER PORT**

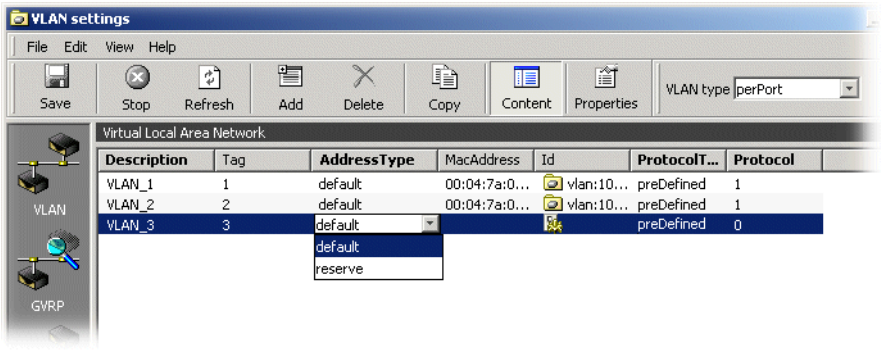
1. Verify that the VLAN type on the top right corner of the GUI is set to "**perPort**". If not, set VLAN type to "perPort", and click "Yes" when asked if the network element should be rebooted.



2. Click **Add**  in the GUI.



3. The GUI suggests default values for all the attributes. **Edit** the description, tag, and/or addressType attributes **if required**.

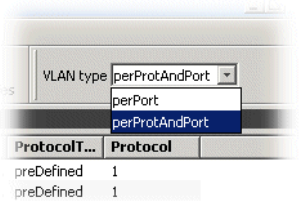


4. Click **Save**. 

11.6.2 Configuration of a new VLAN per protocol and per port

Procedure: **CREATE A NEW VLAN "PER PROTOCOL AND PER PORT"**

1. Verify that the VLAN type on the top right corner of the GUI is set to "**perProtAndPort**". If not, set VLAN type to "perProtAndPort", and click Save. The network element must be restarted before the change is effective.



2. Click **Add** on the GUI.

3. Edit the **Protocol** to indicate which protocol will be used to determine the VLAN membership of a packet. You can choose between 8 **pre-defined protocols**, and **one Ethernet user defined protocol**.

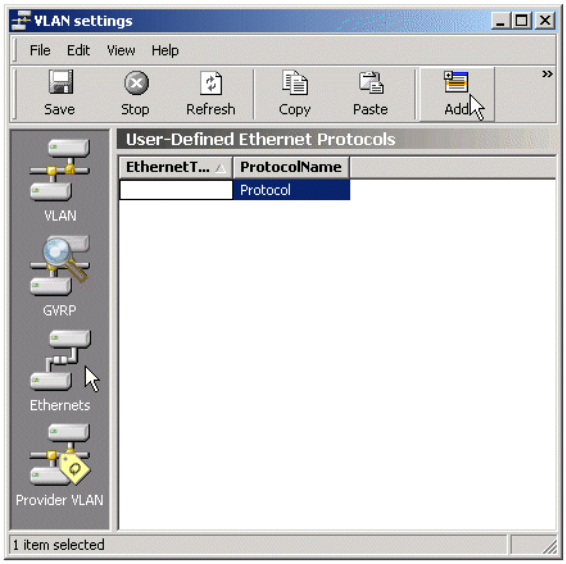
11.6.3 Configuration of an Ethernet user defined protocol

11.6.3.1 To use the Ethernet user defined protocol, set:

The ethernetDefinedProtocol attribute allows you to define a non-predefined protocol based on the etherType field of Ethernet frames. This user-defined protocol is further used to create protocol-based VLANs.

Procedure: **CONFIGURE AN ETHERNET USER DEFINED PROTOCOL**

1. Select VLAN Settings from the Brigde menu
2. Click **Ethernets** in the Content pane.



3. Click **Add** (if no protocol is already defined). If a protocol is already defined, both fields described in step 4 can be directly edited.).
4. Set the **EthernetType** attribute to the value of the **EtherType**[1] indicating the required protocol. The **ProtocolName** attribute can optionally be used to give **a user-friendly name** to the protocol.
5. Save.

1. The EtherType numbers are maintained by the Internet Assigned Numbers Authority (IANA), and can be accessed on the Web at the following address: http://www.iana.org/assignments/ethernet-numbers

Example

Assuming that a user wants to define a VLAN based on the Address Resolution Protocol (ARP), the ethernetType must be set to 0806 (in hex), and the protocolName attribute could be, for example, set to "ARP" to identify the protocol.

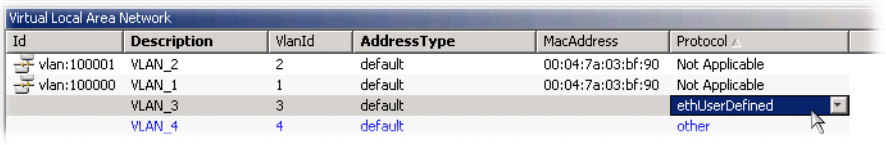
NOTE! The Ethernet user defined protocol is relevant only when the network element runs VLAN per protocol and port.

Maximum one Ethernet user defined protocol can be currently defined on the network element.

To use the Ethernet user defined protocol as a VLAN protocol for a particular VLAN, set the protocolType attribute under Bridge > VLAN to ethUserDefined. The protocol attribute under Bridge > VLAN, which is used to identify a specific protocol, must then always be set to 1, since there is maximum one Ethernet user defined protocol.

Procedure: **USE A PRE-DEFINED PROTOCOL**

1. Select **ethUserDefined** in the Protocol pulldown menu**.**



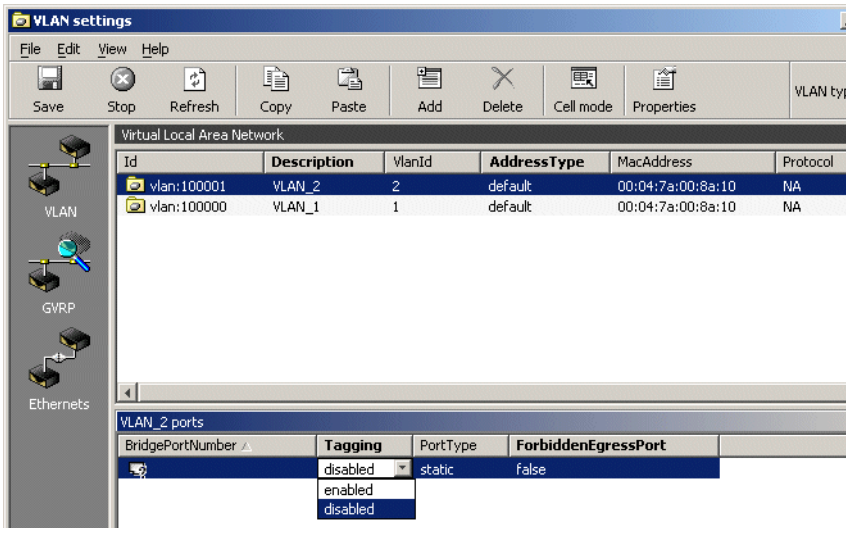
2. **Edit** the description, tag, and/or addressType attributes if required.

3. Click **Save**.

11.6.4 Configuration of a VLAN port member

Procedure: **ADD PORT MEMBERS TO AN EXISTING VLAN**

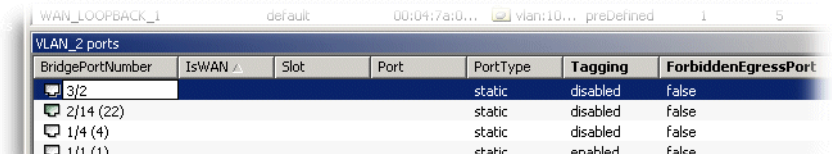
1. Select the **VLAN** to which ports will be added. The VLAN is highlighted in the "Virtual Local Area Network" window (top window). The **list of ports** already members of the VLAN is displayed in the "VLAN ports" window (bottom window).



2. **Activate** the "VLAN ports" window by clicking anywhere in the window. The color of the title bar for the VLAN ports window changes to blue to indicate that the window is selected.

3. Click **Add**.

4. Edit the **BridgePortNumber** attribute. The attribute is displayed as slot/port(bridgePortNumber) and can be entered by the user as "slot/port" or bridgePortNumber[1] (the system will update the display automatically)."



5. Edit the **Tagging** and **ForbiddenEgressPort** attributes if required.

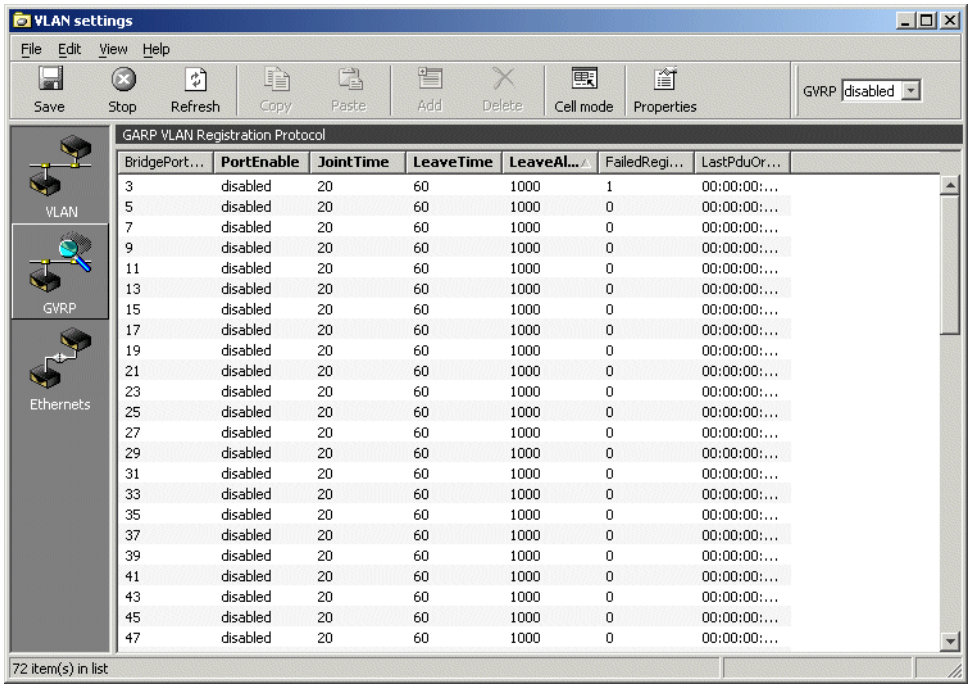
6. Click **Save**.

1. The value of bridgePortNumber for LAN and WAN ports can be found under the LAN and WAN managed objects respectively.

11.6.5 GVRP

GARP VLAN registration protocol (GVRP)

1. Click **GVRP** in the Content pane.

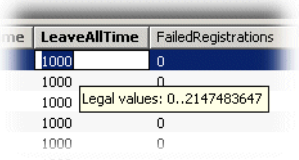


The following attributes are modifiable:

PortEnable	Set to enabled or disabled
JointTime	Set value in centiseconds.
LeaveTime	Set value in centiseconds.
LeaveAllTime	Set value in centiseconds.

Legal time values

Click in desired attribute cell and focus the mouse pointer over the cell.
A tooltip will display legal value range for the selected attribute.



11.6.6 Provider VLAN (IEEE 802.1Q,Q in Q)

11.6.6.1 Overview

The 802.1Q Tunnelling is part of the Layer 2 switching capabilities of the AXX product line. The desired functionality enables the operator to tunnel separate customer traffic, containing 802.1Q tagged (VLAN tagged) Ethernet frames, through a second layer of VLANs. This allows the operator to be oblivious to the customers VLAN schemes, and focus on managing only one VLAN per customer through the network. At the same time, the different customers on a shared device can use whatever VLAN IDs they choose without the risk of interfering with each others VLAN schemes.

11.6.6.2 Definitions

Tunnel Port

By tunnel port we mean a LAN port that is configured to offer 802.1Q-tunnelling support. A tunnel port is always connected to the end customer, and the input traffic to a tunnel port is always 802.1Q tagged traffic. The different customer VLANs existing in the traffic to a tunnel port will be preserved when the traffic is carried across the network.

Trunk Port

By trunk port we mean a LAN port that is configured to operate as an interswitch link/port, able of carrying double-tagged traffic. A trunk port is always connected to another trunk port on a different switch. Switching shall be performed between trunk ports and tunnels ports and between different trunk ports.

11.6.6.3 Applications - examples

Application 1

Application 1 is two AXX155E connected back to back over an SDH network as shown in Figure 170 , carrying Ethernet traffic from different customers using double tagging (802.1q tunnelling).

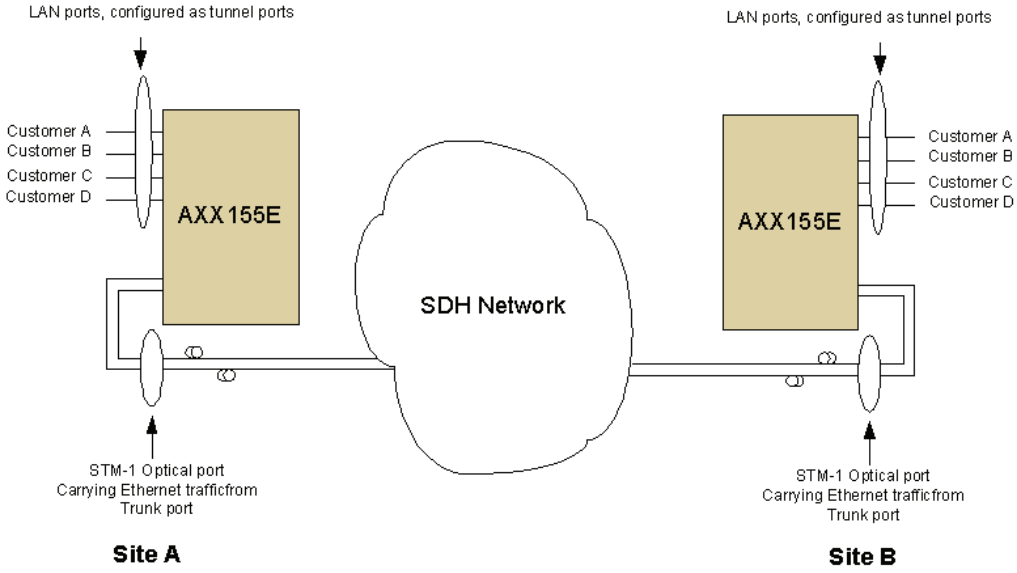


Figure 170 Application 1

In this application both the tunnel ports and the trunk port are on the same switch.

Application 2

Application 2 is two AXX 9200 EDGE connected back to back over an SDH network as shown in Figure 171 , carrying Ethernet traffic from different customers using double tagging (802.1q tunnelling). This application is equal to application 1 except that the number of tunnel ports is increased and the trunk port is a GE port, which requires an STM-4 or STM-16 optical interface (and would also need a GE mapper module).

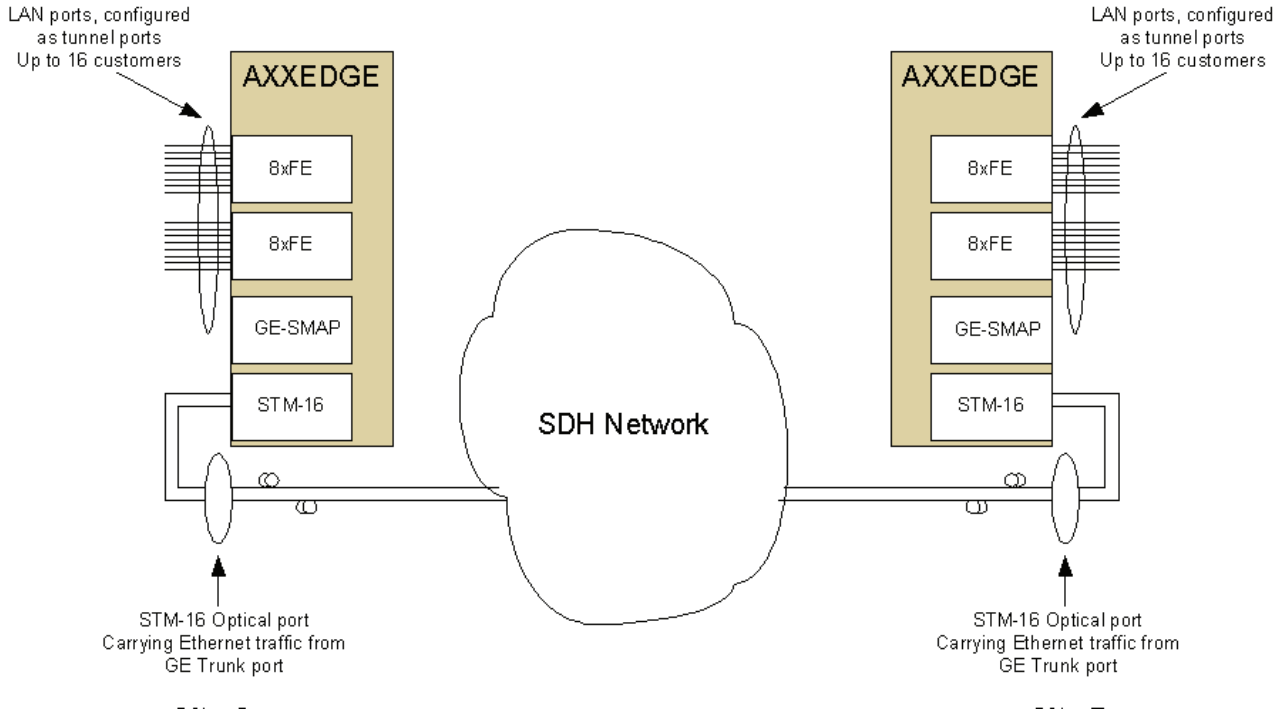


Figure 171 Application 2

The customer tunnel ports are FE ports, while the trunk port mapped into the SDH traffic is a GE port. In this application the tunnel ports and the trunk ports resides on different switches.

Application 3

In application 3, shown in Figure 172 below, the AXX 9200 EDGE has the same trunk port towards the network as in application 2, but 8 of the tunnel ports towards the customers are removed and replaced of 8 STM-1 ports connected to AXX155E devices (for simplicity only two ports and two AXX155E devices are shown). Each of the 8 STM-1 ports is connected to a LAN port on a GT48510A switch via a mapper circuit. The LAN ports on the GT48510A are configured as trunk ports, making them able to talk to the trunk ports on the AXX155Es. This application also includes switching between trunk ports. The ability to connect to third party equipment assume FPGAs translating from proprietary set of tags to a standardized set. Until these FPGAs are introduced, the other end of the optical link would terminate in another Ericsson AXXESSIT device.

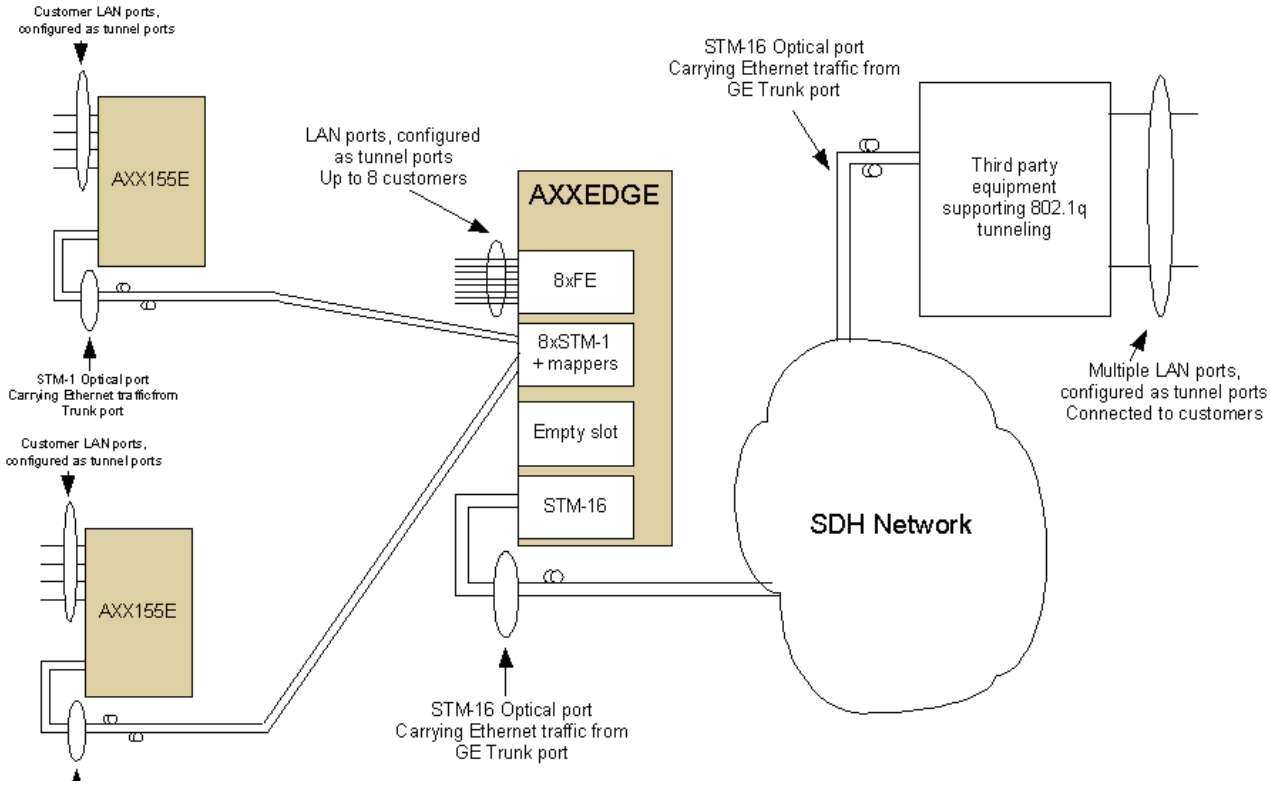


Figure 172 Application 3

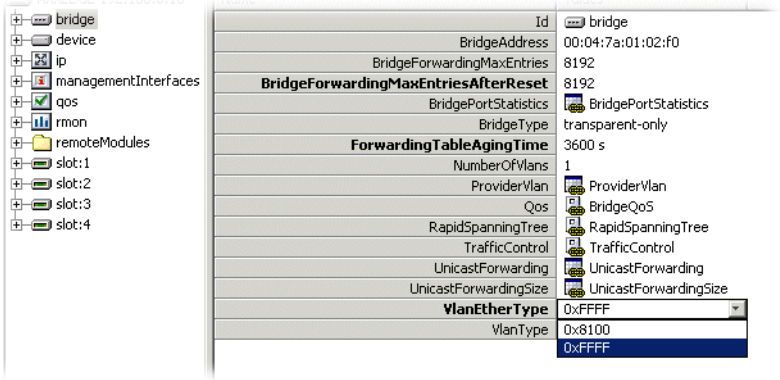
11.6.7 Provider VLAN

Procedure: **SET UP PROVIDER VLAN - AXX 9200 EDGE**

Depending on network element and module version, the Provider VLAN features is implemented on two different levels:

- Switch/Bridge or
- Module/Port policer (new in AXX 9200 EDGE R2.0 and AXX155E R3.0) The new LAN/WAn modules implements QinQ in Policers allowing for individual setup pr. port. The older modules require a common QinQ setup on the switch.

1. Select **bridge** > **VLanEtherType** in the Management Tree.



2. Using the pulldown menu set **VLanEtherType**
   Set **0xFFFF** for configuration in Switch. This setting completes the QinQ configuration for old modules
   Set **0x8100** for configuration through Policer (new modules only).Continue configuration as described in “” on page 559.

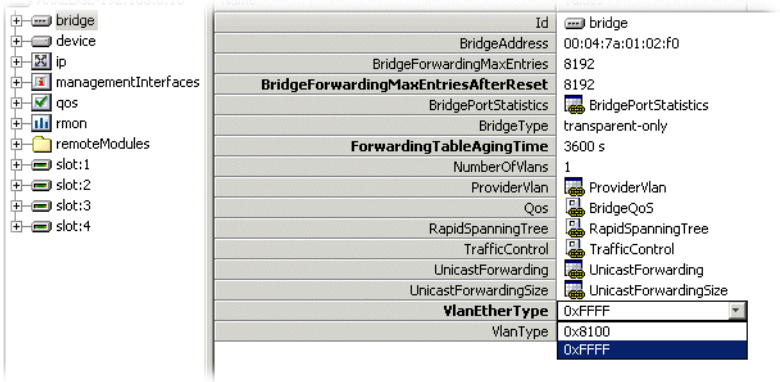
3. Click **Save**.

NOTE! VlanEtherType set to 0x8100, is only applicable to the new FE/GE+SMAP modules introduced for AXX 9200 EDGE R2.0 and AXX155E R3.0. These modules support QinQ configuration on per port basis.

Procedure: SET UP PROVIDER VLAN - AXX 9200 EDGE WITH FE/GE+SMAP MODULES

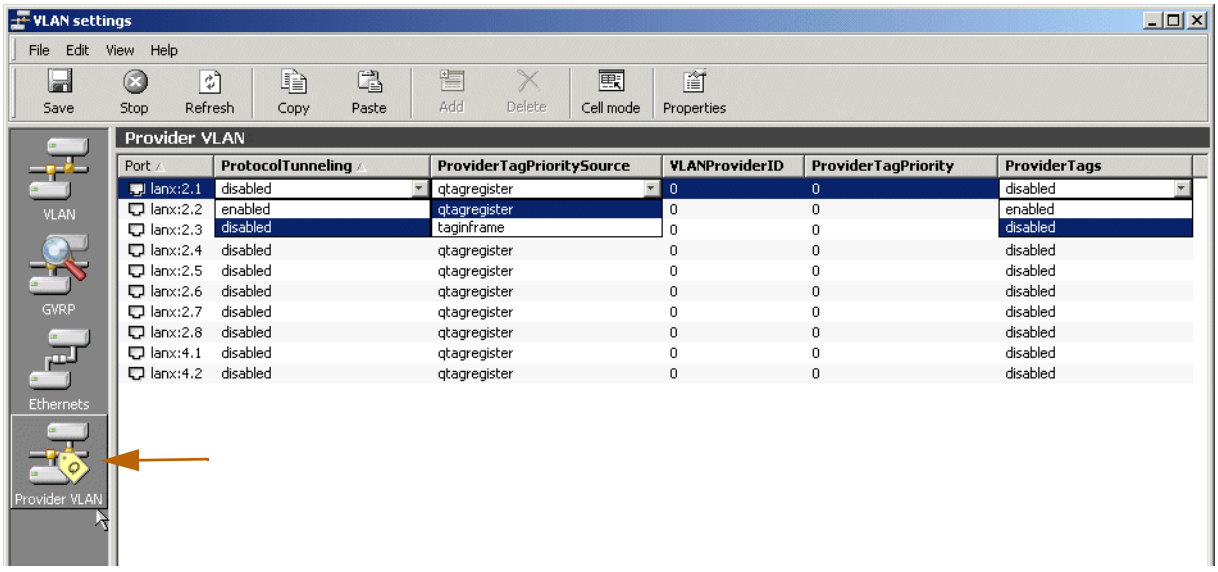
NOTE! The following description is only applicable for the following modules introduced in AXX 9200 EDGE R2.0; 2xGE-SM-LC/RJ45, 2xGE-2xSMAP-SFP and the 8xFE-16xSMAP-RJ45

1. Select **bridge** > **VLanEtherType** in the Management Tree.



2. Using the pulldown menu verify that **VLanEtherType** is set to **0x8100.**

3. Click the **Provider VLAN** button in the **Content pane** in VLAN settings window. Available ports with Provider VLAN available, are displayed:



11.6.7.1 ProtocolTunneling

Enabling the ProtocolTunneling attribute makes the port transparent to other Layer 2 protocols, such as RSTP.

As an example, If a Service Provider VLAN manages his own Spanning Tree, the Network Owner may need to exempt the port used by the Service Provider from the Network Owners own spanning trees to prohibit the two spanning tree protocols from interfering with each other.

11.6.7.2 ProviderTagPrioritySource

Ethernet packages in a VLAN is allocated a priority that controls the packets flow through the network switches. When entering Service Provider VLAN traffic into a Network Owner VLAN, this attribute controls if the Network Owner VLAN shall inherit the Service Provider VLAN priority settings, or assigns his own priority settings.

taginframe forces the Network Owner VLAN to inherit the Service Provider priority.

qtagregister assigns a Network Owner custom priority to his VLAN traffic. The priority is read from a local data register.

11.6.7.3 VLANProviderID

This attribute identifies the Service Provider VLAN that uses the highlighted LAN/WAN port.

11.6.7.4 ProviderTagPriority

This attribute sets the custom priority value (0..7) that is used when the ProviderTagPrioritySource is set to "qtagregister".

11.6.7.5 ProviderTags

This attribute enables or disables QinQ (Provider VLAN) support on the selected port.

4. Set Provider VLAN attributes for desired ports and click 

.
5. Repeat for other network elements that are part of the desired application. (Select **File**>**Reconnect** to access the other NE's)

Procedure: SET UP PROVIDER VLAN - AXX155E

NOTE! This procedure is only applicable to AXX155E R 3.0 equipped with the new WAN module, supported in this release.

1. Select Bridge>**Bridgemode** in the Management Tree.

2. Set Bridgemode = **provider**

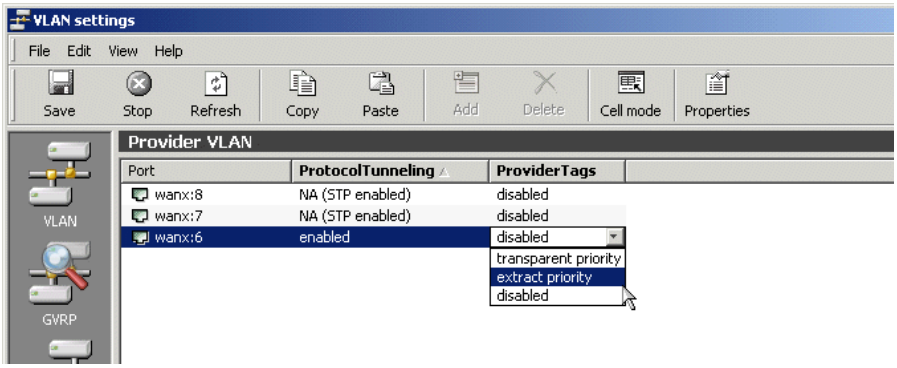
The switch will now operate with a proprietary VLAN Ethertype; 0xFFFF.

Using a VLAN with one LAN port and one WAN port, where the LAN port is untagged and the WAn Port is tagged, the switch will enter an additional VLAN tag. This tag is identified by the type 0xFFFF and has priority as set in Bridge>TrafficControl>PortPriority (default priority for this port). The tag has VLAN ID as indicated in the VLAN Table.

The Provider Tag configuration allows the Mapper in the FPGA to switch the proprietary 0xFFFF to 0x8100, enabling these frames to switched by other 3rd party switches.

1. Click the **Provider VLAN** button in the **Content pane** in VLAN setting window.

2. Select **ProviderTags** setting;
   disabled,
   transparent priority: use the default port priority
   or **extract priority:** inherit priority from the customer traffic.

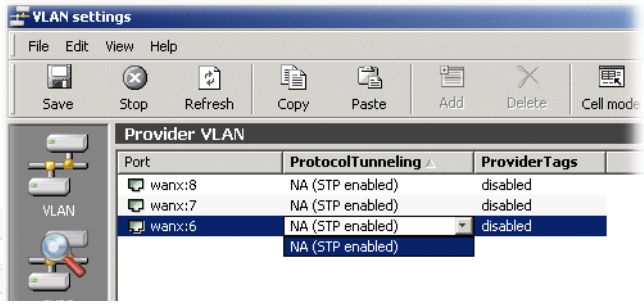


3. Click **Save**.

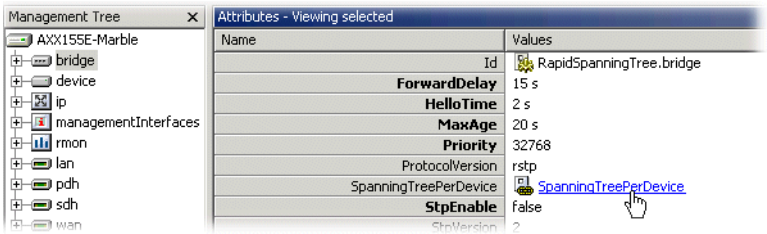
4. Repeat for other network elements that are part of the desired application. (Select **File**>**Reconnect** to access the other NEs)

11.6.7.6 Enabling ProtocolTunneling.

ProtocolTunneling is default set to NA (due to STP enabled).

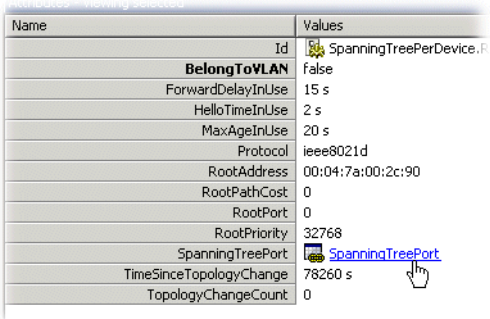


Procedure: **ENABLE PROTOCOL TUNNELING**

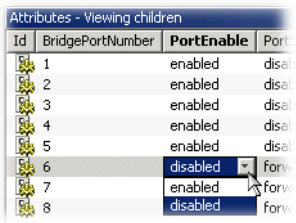


1. In the Management Tree select **bridge** > **SpanningTreePerDevice.**

2. Select **SpanningTreePort**.

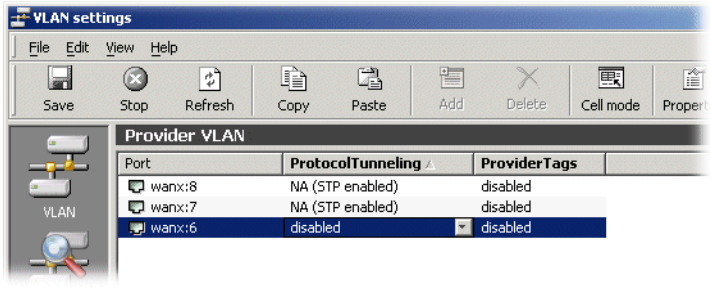


3. Select desired Port and set **PortEnable** attribute to **disabled**.

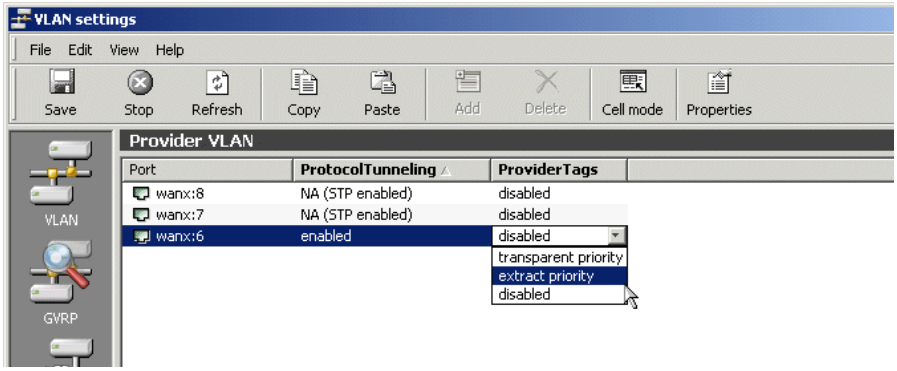


4. Return to VLAN Settings and continue the Provider VLAN settings.

5. Set **ProtocolTunneling** to **enabled**



6. Set **ProviderTags** to desired **value: disabled,transparent priority** or **extract priority**



11.6.8 L1 Ethernet Service over SDH

For point-to-point connections from site A to site B, layer 1(L1) Ethernet transport may be the preferred solution. Ethernet L1 bridging provides high security and fits well requirements for e.g. Ethernet Private Line (EPL) services.

In this chapter we provide examples for how to configure this kind of service through a SDH network using Ericsson AXXESSIT products. Typically this will be a matter of configuring a LANx-port in L1 mode, configure LCAS (optional for VCAT/ not applicable for proprietary mapping), assign bandwidth by means of VC's and finally cross-connect the references for Ethernet over SDH transport.

For most point-to-point network scenarios this would be sufficient, but some network topologies have special requirements and the L1 bridging concept supported by our products makes it possible to cover also more advanced applications.

Descriptions in subsequent chapters provide examples for basic and advanced Ethernet L1 configuration using Ericsson AXXESSIT products.

Prerequisites:

HW (Ethernet modules) must support L1 configuration. This can be recognised by the object identification "LANx-port" in management solutions.

11.6.8.1 Network scenario for L1 service through SDH

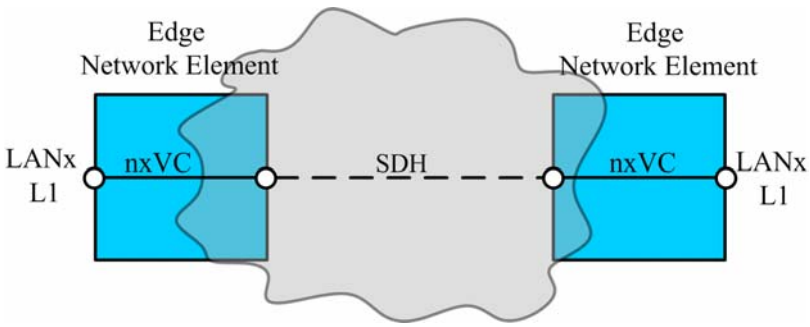


Figure 173 Basic L1 service (LAN to LAN)

Procedure: **CONFIGURATION FOR A L1 CONNECTION THROUGH SDH:**

The order and required configuration for a L1 connection through SDH is equal in both ends of the connection.

1. Select desired LANx-port and configure L1 mode. Press **Save**

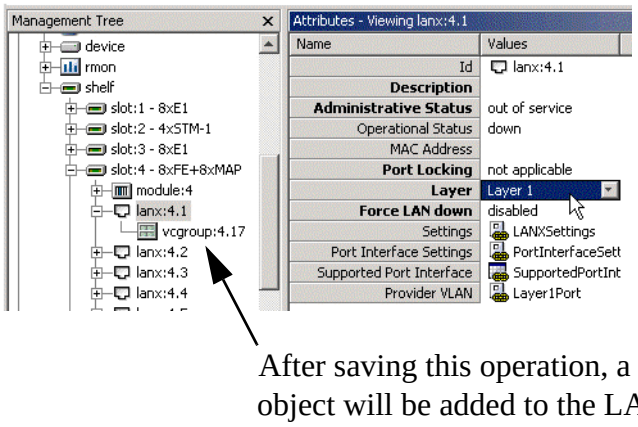


Figure 174 Configure a LANx port to L1

NOTE! For AXX 9300 METRO you can configure all ports for L1 bridging globally per module. This configuration is performed when configuring "ExpectedMode" during commissioning/activation of the module. Refer to relevant chapter, which addresses module configuration for more information.

2. Configure desired concatenation. I.e. select VCAT VC-12, VCAT VC-3, VCAT VC-4 or Ericsson AXXESSIT proprietary mapping.

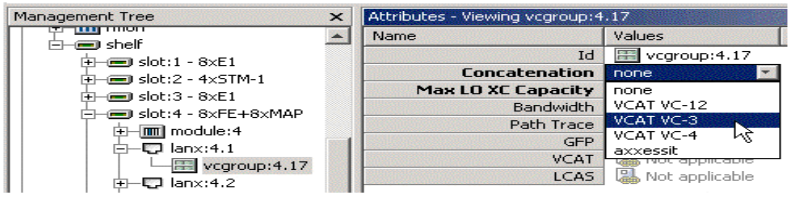


Figure 175 Configure concatenation

NOTE! For GE-ports in AXX 9300 METRO, an additional step is required for
VCAT VC-3: It is necessary to decide what amount of VCs to occupy in the LO DXC.

It is wise to reserve a number which fits potential future requirements for the customer connection.

3. (Optional) If the VCs in the vcgroup travel through different routes in the SDH network, or if there are requirements for hitless increase of bandwidth, LCAS should be configured.
Optionally the proprietary solution "SoftLCAS" can be used for bidirectional cross-connections, but for this mode hitless increase of bandwidth cannot be obtained.

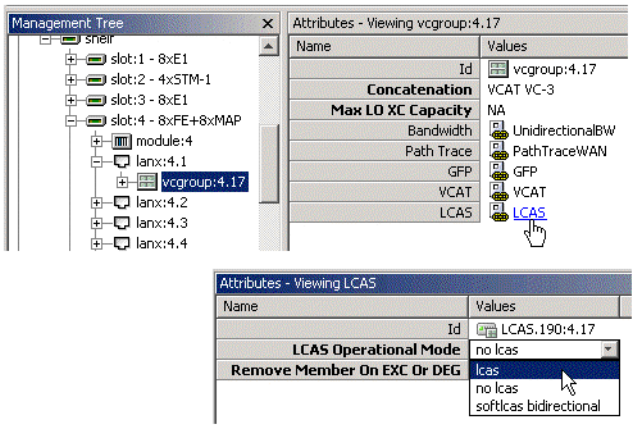


Figure 176 L1 LANx LACS

4. Assign desired bandwidth by means of number of VCs.

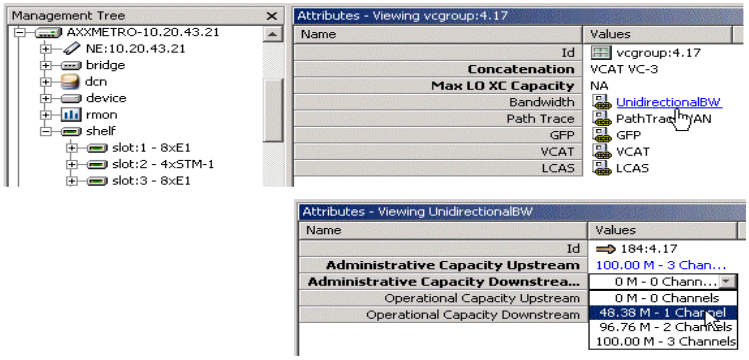


Figure 177 Assign bandwidth

5. Cross-connect the VC referenc(es) for the LANx-port with VC references for the desired SDH-aggregate port.

6. Right-click on top of the LANx-port object and start the WAN-to-SDH mapper GUI.

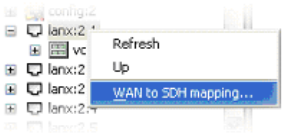


Figure 178 Start the Cross Connection Manager GUI

7. Refer chapter to “Cross Connection Manager” on page 410 for detailed descriptions of how to perform the WAN-to-SDH mapping.

   Notice that your selection for LCAS mode will influence how the cross-connections will be set up. If you selected softLCAS in step 3, you will be able to cross-connect bidirectionally. Otherwise you will need to cross-connect upstream and downstream individually.
   Also notice the requirement for enabling per channel.

11.6.8.2 Advanced L1 Ethernet configuration

For some applications LANx-port(s) in L1 mode need more advanced configuration in order to meet special requirements for transporting the customer traffic through the Provider Network.

The Ericsson AXXESSIT products have the option to assign a Provider VLAN tag and/or enable Protocol tunnelling for a LANx-port in L1 mode.

These parameter settings make it possible to send L1 traffic through a L2 switch in intermediate node(s) without caring for customer

VLAN tag(s) in use and/or e.g. to tunnel customer BDPU packets. The figure below shows a typical network scenario.

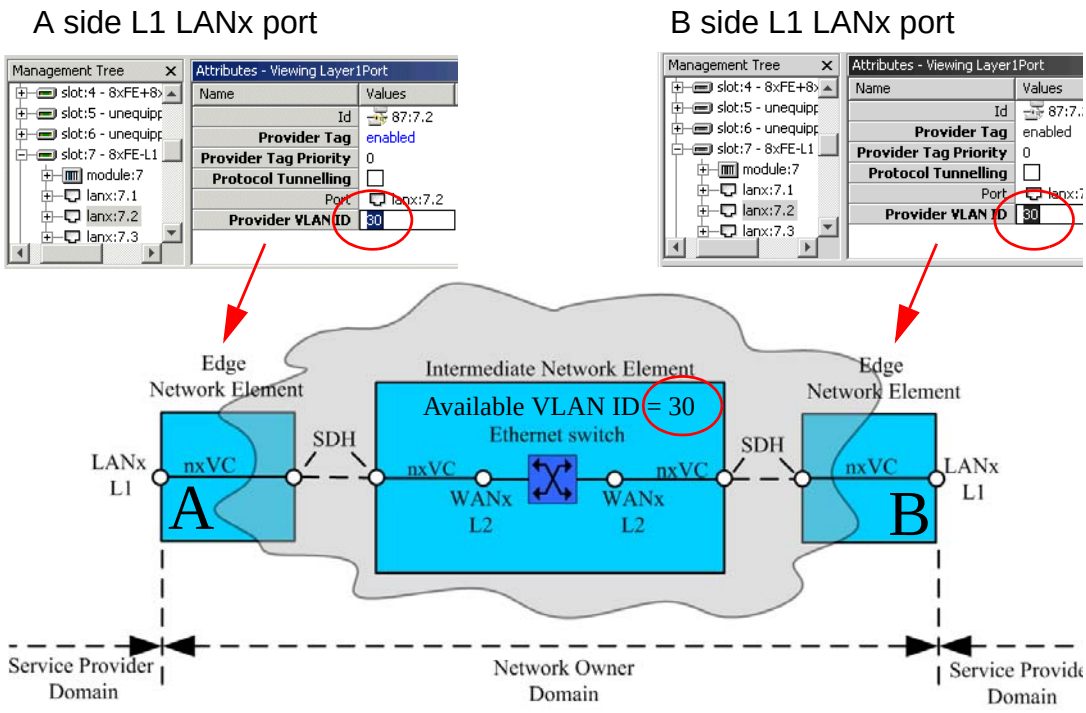


Figure 179 Provider VLAN (QinQ) for Layer 1 ports

Procedure: **EXAMPLE FOR QINQ TAGGING OF L1 PORTS:**

The customer may send Ethernet traffic as multiple VLANs by means of a IEEE802.1Q trunk. In order to switch this trunk as a Provider VLAN in the intermediate L2 switch, the WANx-ports on both sides of the switch must have matching configuration. In the network in Figure 179 we want to send the traffic through the available VLAN ID = 30 in the intermediate node:

1. Select the A-end LANx port.
2. On the ProviderVLAN attribute, click on the Layer1Port link.
3. In that view, set the Provider Tag attribute to enabled.
4. Set the Provider VLAN ID to 30 (example).
5. Repeat the procedure for the B-side LANx port.

Procedure: **EXAMPLE FOR "PROTOCOL TUNNELLING" ENABLING L1 PORTS:**

When this feature is enabled on a L1 LANX port, you can tunnel external protocols such as "Spanning Tree" through the network.

In order to pass through the L2 WANx-ports on the intermediate node(s), Protocol Tunnelling must be enabled on LANx-ports on both A and B side.

1. Select the A-end LANx port.
2. On the ProviderVLAN attribute, click on the Layer1 Port link.
3. In that view, tick the Protocol Tunnelling checkbox to enabled.
4. Repeat the procedure for the B-side LANx port.

NOTE! “Protocol Tunnelling" is a proprietary feature and is only supported for LANx-ports.

11.7 Link aggregation

11.7.1 Introduction

The purpose of this section is to describe the tasks involved when managing the link aggregation functionality of the network element. Link aggregation is also called Trunking.

Link aggregation is used to optimise port (link) usage by grouping ports together to form a single aggregate. Link aggregation multiplies the bandwidth between the devices, increases port flexibility and provides link redundancy.

The network element defines the number of link aggregations and a maximal number of ports in each link aggregation.

11.7.2 View Link Aggregation

1. Select the **device** > **Link Aggregation** object in the Topology pane to view the specific object properties in the Attributes pane.

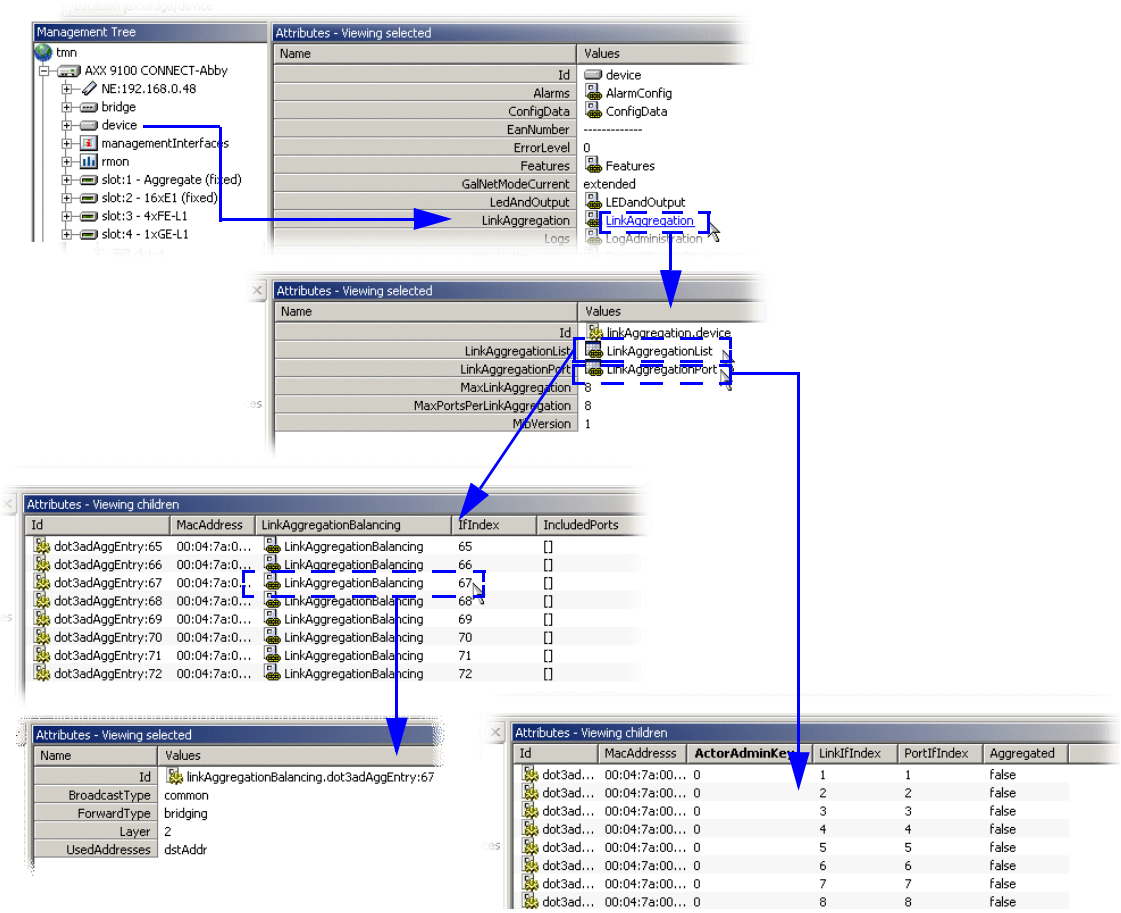


Figure 180 Attributes related to Link Aggregation

11.7.3 Modify Link Aggregation

You can modify the modifiable Link Aggregation parameters, and this involves:

- Adding of new port(s) to an aggregation
- Deletion of port(s) in an existing aggregation

The link aggregation feature, also known as trunking, allows you to link a group of ports together to form a single trunk (aggregated group). Link aggregation can be used to increase bandwidth between devices and/or to provide link redundancy.

The link aggregation feature has the following limitations:

- Only LAN and WAN ports can be part of a trunk
- Maximum 8 trunks can be defined on the network element
- Maximum 8 ports can be grouped within a single trunk

The number of trunks configured simultaneously is limited by equipped module type(s). Notice the following:

- Modules equipped with < 8 Ethernet LAN- and/or WAN-ports supports one link aggregation trunk each.
- Modules equipped with 9-16 Ethernet LAN- and/or WAN-ports supports two link aggregation trunks each, though limited within groups of bridge port numbers for configuration. Table below shows valid configurations for link aggregation using modules with 16 FE ports (FE = WAN- and/or LAN-ports).

Slot	Trunk	Valid groups of bridge port numbers
1	1	1-8
1	2	9-16
2	1	17-24
2	2	25-32
3	1	33-40
3	2	41-48
4	1	49-56
4	2	57-64

Table 18 Valid Link Aggregation configuration for 16xFE port module

In order to assign a port to a trunk, the port must comply with the following requirements:

- A layer 3 interface is not configured on the port.
- A VLAN is not configured on the port.
- The port is not assigned to a different trunk.
- An available MAC address exists which can be assigned to the port.
- Auto-negotiation mode is not configured on the port.
- The port is in full-duplex mode.
- All ports in a trunk must operate at the same rate.
- All ports in a trunk must have the same ingress filtering and tagged modes.
- All ports in a trunk must have the same back pressure and flow control modes.
- All ports in a trunk must have the same priority.
- All ports in a trunk must have the same transceiver type.
- All ports in a trunk (except the GE ports) must belong to the same module, i.e. they must be located on the same slot.

Procedure: **ASSIGN A PORT TO A TRUNK**

1. Make sure that the port to be added to a trunk complies with the requirements listed above.
2. Click on the **NE** managed object, and then on the **Device** managed object in the Management Tree.
3. Click on the **LinkAggregation** attribute in the attribute window.
4. Click on the **LinkAggregationPort** attribute in the attribute window.
5. Identify the port to add via its **Port Interface Index**.
6. Verify that the port can be part of a trunk by checking the **Aggregated** attribute. If **Aggregated** displays **true**, the port can be included in a trunk, please go to the next step. If **Aggregated** displays **false**, the port can only operate as an individual link, and cannot be part of a trunk. Select another port (go back to step 5).
7. Edit the **Actor Administrator Key** attribute. This attribute must be set to the **Interface Index** of the trunk to which the port shall be assigned[1]. Legal values are [**65 through 72**].

8. **Save**.

1. To find out the ifIndex used by the trunk, check the Device > LinkAggregation > LinkAggregationList attribute.

11.7.4 Trunk elements

Trunk elements used by management are named ifindex:

Regular ports, LAN and WAN, have ifIndexes from 1 to 64, depending on the slot and port number.

16 ifIndexes are reserved for each slot.

For example, an fast Ethernet (FE) module with 8 ports located in slot 3, have ifindex range from 33 for port 3/1 to 40 for port 3/8.

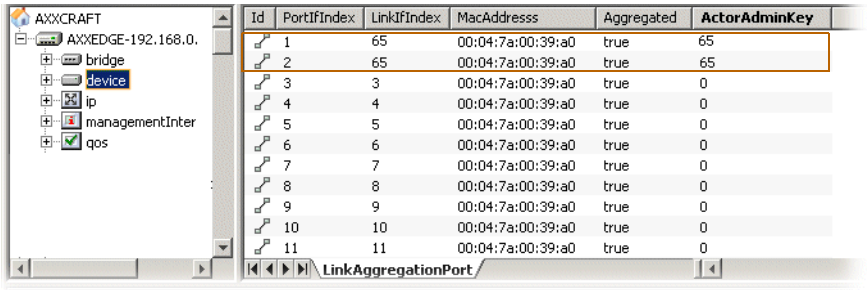
STM-1 modules are a bit special since they are a combination of 8 SDH ports and 8 WAN ports. WAN ports in an 8XSTM1 module are numbered x/9 to x/16 (x is the slot), while the ifIndexes corresponds to x/1. For an 8xSTM-1 module located in slot 2, the ifindex range is 17 to 24(17 for port 2/9, 24 for port 2/16).

Giga bit Ethernet (GE) ports use the first ifIndexes for the particular slot. For example, a 2XGE in slot 4 have ifindex numbers 49 for port 4/1 and 50 for port 4/2.

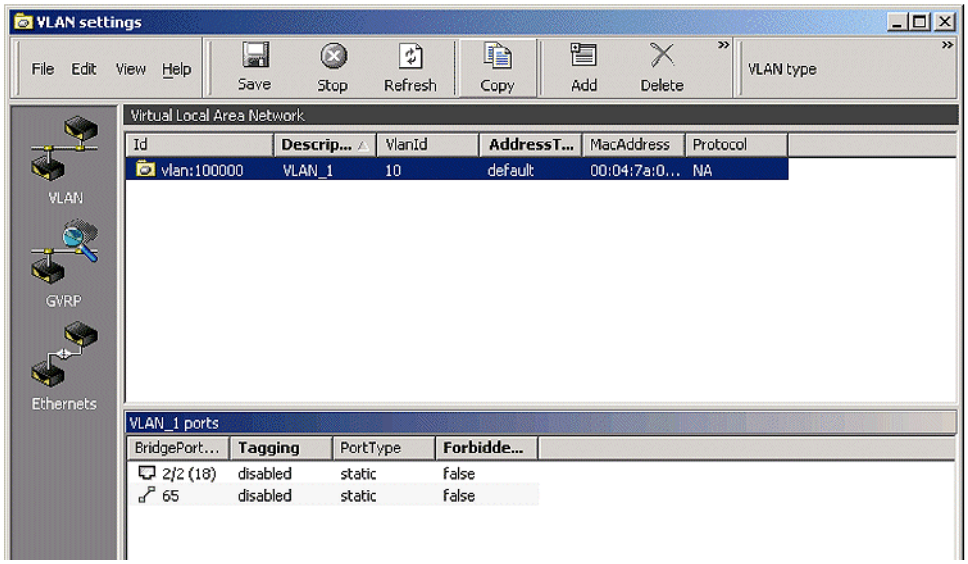
Maximum number of trunks in the system is 8, and the trunk ifindex range is 65 to 72. The trunk ifindex is used as port number when a trunk is assigned to a VLAN.

An example to illustrate the creation of a trunk and adding the trunk to a VLAN:

The first two WAN ports of slot 1 are used to create a trunk with ifindex 65:



The trunk and the second GE port in slot 2 are put together in a VLAN:



11.8 Troubleshooting and FAQ

11.8.1 Troubleshooting

11.8.1.1 Why is the Mac multicast feature not available in AXX 9840 INSITE?

To enable MAC multicast, the user must make sure that the maximum number of VLANs is less than 4000. This is because the maximum number of multicast entries allowed in the network element is fixed by the following equation:

$$\langle max\ \ number\ \ muticast\ \ entries \rangle = 4000 - \langle max\ \ number\ \ VLANs \rangle$$

Therefore, if the maximum number of VLANs is greater than 4000, no resources can be allocated for MAC multicast entries, and the MAC multicast feature is then disabled.

The maximum number of VLANs is set via the vlanMaxEntriesAfterReset attribute (under Bridge->VlanType). If this attribute is edited, the network element must be reset before the new value becomes effective.

11.8.2 FAQ

11.8.2.1 How many VLANs does the network element support?

The maximum number of VLANs supported by the network element is configurable by the user, and is indicated by the vlanMaxEntries attribute (under Bridge > VlanType).The maximum number of VLANs can be set to a new value via the vlanMaxEntriesAfterReset attribute (under Bridge > VlanType). If this attribute is edited, the network element must be reset before the new value becomes effective. Note that the network element cannot support more than 4000 VLANs (1000 for AXX 9300 METRO).

11.8.2.2 What is the VLAN ID?

IEEE 802.1Q standardizes a scheme for adding additional information, known as VLAN tag, to layer 2 frames in order for a switch to know which VLAN an incoming frame is intended for, and the priority of the frame[1]. The VLAN tag is a two-byte field containing 3 bits for indicating the priority of the frame, 12 bits for indicating the VLAN ID, and 1 bit indicating whether the addresses are in canonical format (see Figure 1).

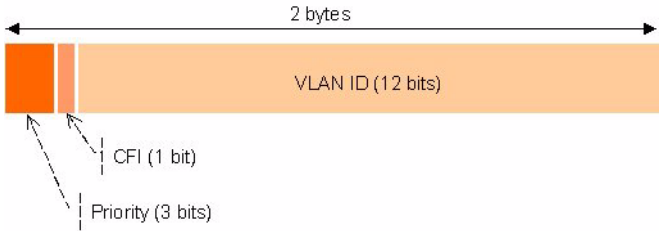


Figure 181 IEEE 802.1Q Tag header (VLAN tag)

The priority field is interpreted as a binary number, and therefore capable of representing eight priority levels, 0 through 7. The use and interpretation of this field is defined in ISO/IEC 15802-3.

The Canonical Format Indicator (CFI) is a single bit flag value. CFI reset indicates that all MAC Address information that may be present in the MAC data carried by the frame is in Canonical format.

The VLAN Identifier (VLAN ID) field uniquely identifies the VLAN to which the frame belongs. The VLAN ID is encoded as an unsigned

1. In the standard (IEEE 802.1Q), layer 2 frames carrying both VLAN identification and priority information in a tag are referred to as VLAN tagged frames. Layer 2 frames carrying priority information, but no VLAN identification information are referred to as priority tagged frames.

binary number. The user can associate any value in the range 1-4095 to a VLAN ID. The value null is reserved for priority-tagged frames[1], and the value 4096 (FFF in hexadecimal) is reserved for implementation use.

11.8.2.3 How to choose the maximum number of GVRP VLAN?

The Generic Attribute Registration Protocol (GARP) protocol is a general-purpose protocol that registers any network connectivity or membership-style information. GARP defines a set of devices interested in a given network attribute, such as VLAN or multicast address.

The GARP VLAN Registration Protocol (GVRP) protocol is specifically provided for automatic distribution of VLAN membership information among VLAN-aware bridges. GVRP allows VLAN-aware bridges to automatically learn VLANs to bridge ports mapping, without having to individually configure each bridge, and to register VLAN membership.

To minimize the memory requirements when running the GVRP protocol, two proprietary tuning variables have been added to the standard variables: gvrpVlanMaxEntries and gvrpVlanMaxEntriesAfterReset which control the number of GVRP VLANs allowed to participate in GVRP operation. The maximum number of GVRP VLANs includes all the VLANs participating in GVRP operation regardless if they are static or dynamic.

The following should be considered when specifying the maximum number of VLANs participating in GVRP by setting the gvrpVlanMaxEntriesAfterReset attribute:

- The default maximum number of GVRP VLANs is equal to 0 because of the memory restrictions.
- The maximum number of VLANs (managed through the bridge> vlanType > maxVlanEntriesAfterReset attribute) limits the maximum number of GVRP VLANs.
- To ensure the correct operation of the GVRP protocol, users are advised to set the maximum number of GVRP VLANs equal to a value which significantly exceeds the sum of:

The number of all static VLANs both currently configured and expected to be configured.

1. Priority tagged frames are layer 2 frames carrying priority information, but no VLAN identification information.

The number of all dynamic VLANs participating in GVRP both currently configured (initial number of dynamic GVRP VLANs is 0) and expected to be configured.

Increasing the value of maximum number of GVRP VLANs to value beyond the sum, allows users to run GVRP, and not reset the device to receive a larger amount of GVRP VLANs. For example, if 3 VLANs exist and another two VLANs are expected to be configured as a result of VLAN static or dynamic registration, set the maximum number of GVRP VLANs after reset to 10.

11.8.2.4 Adjust the maximum number of VLAN and GVRP entries

1. Click **Properties** in the VLAN Settings window.
2. The appearing dialog allows you to adjust the maximum number of VLAN and GVRP entries.

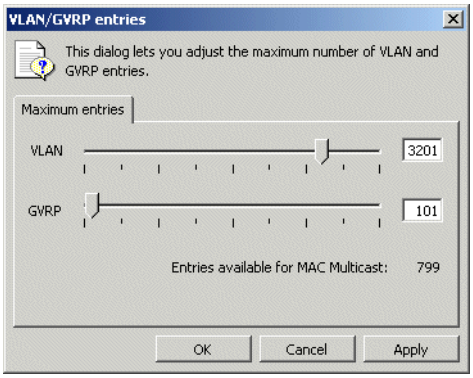


Figure 182 Adjustment of VLAN/GVRP entries

NOTE! To enable GVRP, ensure that the amount of maximum amount of VLANs is less than 4000 (check the bridge > vlanType > maxVlanEntries attribute).

11.8.2.5 How to represent a set of ports with an octet string?

When an octet string is used to represent a set of ports, each octet within the string specifies a set of eight ports, with the first octet specifying ports 1 through 8, the second octet specifying ports 9 through 16, etc. Within each octet, the most significant bit represents the lowest numbered port, and the least significant bit

represents the highest numbered port (see Figure 2). Each port of the bridge is then represented by a single bit within the octet string. If the bit has a value of '1' then the port is included in the set of ports; and the port is not included if the bit has a value of '0'.

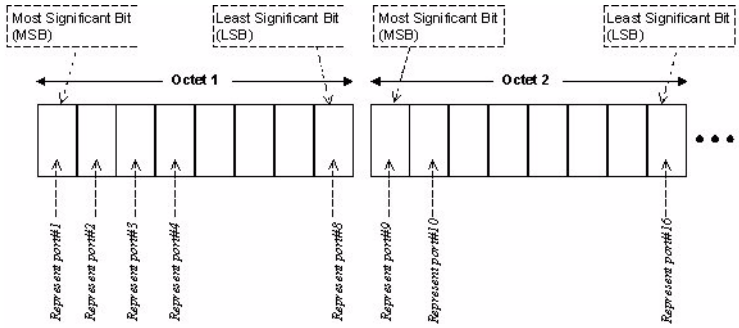


Figure 183 Definition of a set of ports through an octet string

Table 19 presents two examples of octet strings and their corresponding sets of ports.

52	0101 0010	port #2, port #4, and port #7
0c 01	0000 1100 0000 0001	port #5, port #6 and port #16

Table 19 Octet string and corresponding set of ports

12 Layer 3 - configuration

12.1 IP Router

12.1.1 Introduction

The purpose of this section is to guide your through management of the IP service on the network element, and it involves:

- Presentation and modification of IP, i.e. Layer 3 IP forwarding functionality
- Creation, presentation, modification, and deletion of IP interfaces
- Presentation and modification of RIP and OSPF
- Presentation and modification IP redundancy
- Presentation and modification of DHCP service
- QoS for IP
- Troubleshooting and FAQ

12.2 Examples

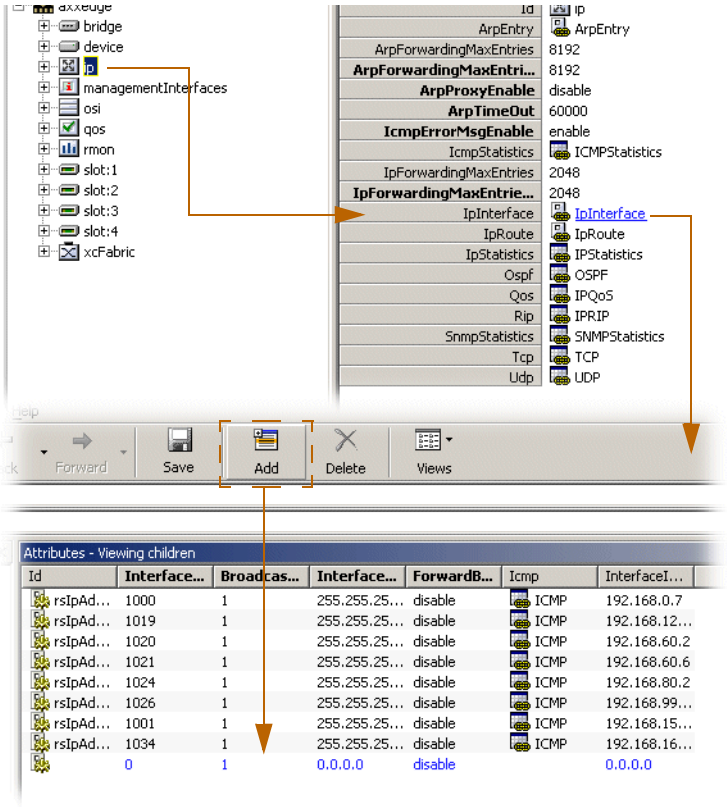
12.2.1 Configuration of an IP interface

An IP interface can be created only for a physical port, a management interface, or a VLAN (port based VLAN or IP-based VLAN only).

Procedure: **CONFIGURE AN IP INTERFACE WITH AN IP ADDRESS**

1. Click on the **AXX 9200 EDGE** managed object, and then the **ip** managed object in the Management Tree.
2. Click on **IpInterface** in the attributes window.

3. Click **Add** on the toolbar.



4. The following attributes have no default values, and must therefore be defined:

interfaceIpAddress: set the IP address according to your addressing plan.

interfaceNetworkMask: set the network mask according to your addressing plan.

interfaceNumber: the interface number. An IP interface can be defined for a LAN port, a WAN port, the Management Port, a DCC running IP, the OSI interface, or a VLAN. The interface number corresponding to these objects is specified by the ifIndex attribute present under their respective M.O.

5. Save.

NOTE! One interface (identified by a specific ifIndex) can be allocated several IP addresses. This enables the user to connect the interface to a network segment where multiple subnets are defined.

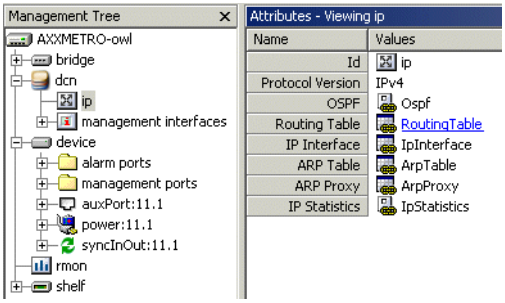
IP addresses and network masks associated with the Management interfaces, i.e. the Management Port, DCC and the OSI interface can also be edited via the Management Interfaces M.O.

12.2.2 Configuration of a static route

An IP static route is a route defined by the user through the management system. Such a route does not age out, and will stay in the network element routing table as long as it is not explicitly deleted by the user. As any other route, a static route is active, and therefore included in the forwarding table[1] provided that the interface associated with the route is up.

Procedure: **CREATE A STATIC ROUTE**

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.See the figure below

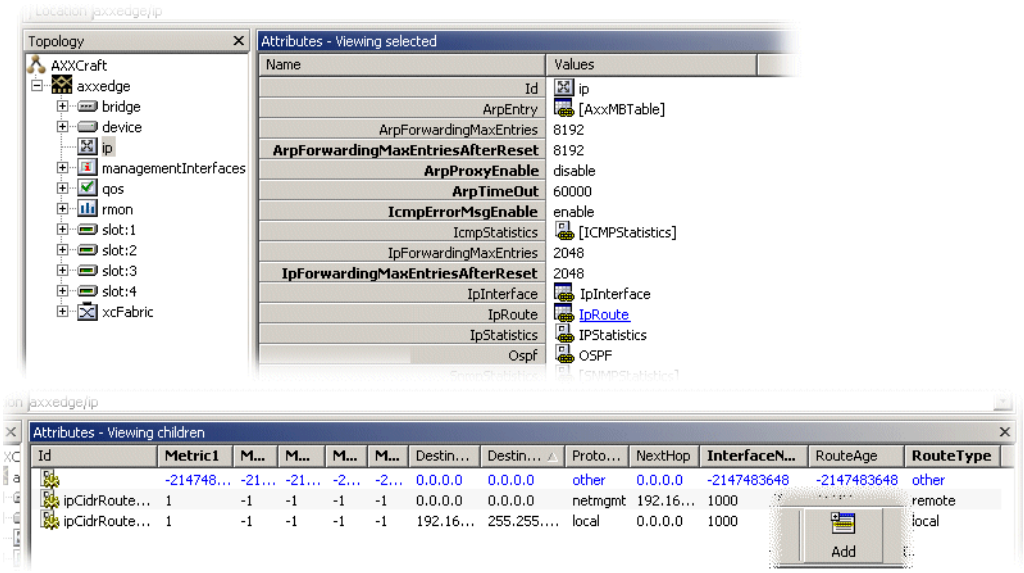


for AXX 9300 METRO:

2. Click the **ipRout**e attribute in the attributes window.

1. The forwarding table is a subset of the routing table. It contains only the active routes, i.e. routes being used by the network element to forward IP datagrams. Typically, a route becomes inactive, and is removed form the forwarding table when the operational status of its associated interface is down. Only the forwarding table is visible in AXX 9840 INSITE via the ipRoute attribute.

3. Click **Add** on the toolbar.



4. Set the **destinationIpAddress**, **destinationNetworkMask**, **nextHop**, **interfaceNumber** attributes.

5. Set the **routeType** attribute to either '**Remote' if** the route is meant to forward traffic, or '**Reject**' **if** the route is meant to discard traffic for the specified destination.

6. **Optionally**, one or more **metric attributes** can be set. Metrics are used by the routing process to select a preferential route (the route with the lowest metric) if there are several possible routes for a given destination.

7. Save.

NOTE! The value x set to the destinationNetworkMask attribute will be rejected by the network element if the bitwise logical-AND of x with the value of the destinationIpAddress attribute is not equal to the value of the destinationIpAddress attribute.
The IP address of the next router en route specified by the next-hop attribute must be directly reachable via the interface specified by the interfaceNumber attribute, i.e. the next-hop IP address must belong to the (one of the) subnet(s) defined for the interface identified by the interfaceNumber attribute.

Example:

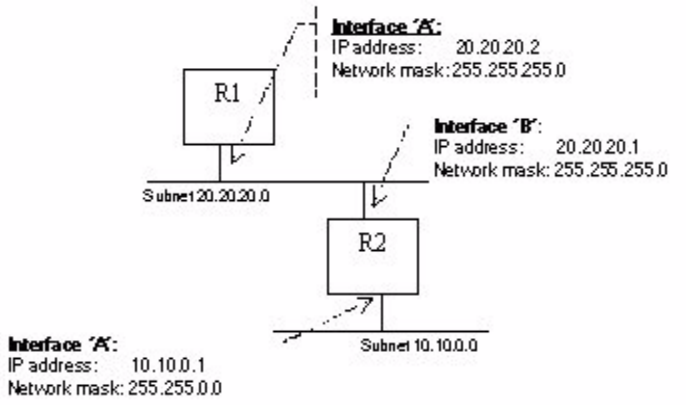


Figure 184 Figure - Static route in router R1

Procedure: **DEFINE A STATIC ROUTE TO THE SUBNET 10.10.0.0 IN ROUTER R1 ABOVE**

1. destinationIpAddress: **10.10.0.0**
2. destinationNetworkMask: **255.255.0.0**
3. nextHop: **20.20.20.1** (one must choose the IP address of router R2 which lies on the same subnet as the interface identified by the interfaceNumber attribute in R1)
4. interfaceNumber: ifIndex associated with interface '**A**'.
5. routeType: **Remote**
6. metric: **1**

12.2.3 Configuration of a default route

A default route is a particular static route which is used to by the network element to send all the traffic for which no other routing information exists. If no default route has been defined, and no specific routing information exists for an IP datagrams requesting forwarding, the datagram is discarded.

The default route is created by setting both the destinationIpAddress and the destinationNetworkMask attributes to 0.0.0.0. The router identified by the next-hop attribute is then referred to as default router, a.k.a. default gateway.

NOTE! There exists only one active default route in the network element.

The default gateway can also be edited via the Management Interfaces M.O.

Example:

To create a default route on router R1 (see “Figure - Static route in router R1” on page 587) using router R2 as default gateway:

1. destinationIpAddress: 0.0.0.0
2. destinationNetworkMask: 0.0.0.0

3. nextHop: 20.20.20.1
4. interfaceNumber: ifIndex associated with interface 'A'.
5. routeType: Remote
6. metric: 1

12.2.4 Configuration of a RIP filter

An IP RIP filter allows the user to control the propagation of RIP routing information, and eventually to modify the RIP routing by filtering out information about specific routes. In addition, IP RIP filters help reducing the size of the RIP table allowing for a faster table look-up, and releasing memory for other processes.

Procedure: **CREATE AN IP RIP GLOBAL FILTER**

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Double click on the **rip** attribute in the attributes window.
3. Double click on the **ripGlobalFilter** attribute in the attributes window.
4. Click **Add** on the toolbar.
5. **Set** the type, networkAddress, numberOfMatchBits, and filterAction **attributes**.
6. Save.

Examples

To define a RIP global filter which prevents the network element from advertising any route to the subnet 10.10.0.0, enter the following filter:

Type: output

NetworkAddress: 10.10.0.0

NumberOfMatchBits: 16

FilterAction: Deny

To define a RIP interface filter which prevents the network element from accepting routes for the subnet 192.168.0.0, but still accepts routes for the subnet 192.1680.1.0, enter the following two filters:

#1: Type: input

NetworkAddress: 192.168.0.0

NumberOfMatchBits: 16

FilterAction: Deny

#2: Type: input

NetworkAddress: 192.168.1.0

NumberOfMatchBits: 24

FilterAction: Permit

NOTE! The procedure to define a RIP interface filter is identical to the procedure described above. A RIP interface filter applies only to a specific interface (specified by the ripInterface attribute) instead of applying to every RIP-enabled interface on the network element.

RIP interface filters take precedence over RIP global filters.

12.2.5 Configuration of a QoS IP rule

QoS IP rules allow the user to tune the forwarding process. A QoS IP rule can either block (discard) traffic which would normally have

been forwarded, or shape some traffic flows, i.e. the traffic is forwarded according to a pre-defined profile.

A QoS rule consists in two parts:

- A set of attributes used to classify the incoming traffic.
- A policy action describing the forwarding decision taken for the incoming packets which match the rule.

To define the set of attributes used in the classification process, enable the desired attributes in the QoS->ipClassification attribute.

Example:

To define a QoS IP rule, which blocks all the UDP traffic destined for subnet 100.100.0.0:

Ensure that the attributes used to classify the traffic are enabled in the ipClassification attribute:

1. In our example, both the destination IP address, and the protocol are the attributes used to check if an incoming packet should be affected by the rule. Under **IP** > **QoS** > **ipClassification**, set the following attributes:
2. **destinationIpBitMask** = **16** (to check that an incoming packet is destined for subnet 100.100.0.0, only the first 16 bits of its IP destination address are relevant)
3. **protocol** = **true** (only UDP traffic should be stopped).
4. Save.

Create the IP rule in the IP rule table (IP > QoS> ipRule):

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Double click on the **QoS** attribute in the attributes window.
3. Double click on the **qosRule** attribute in the attributes window.
4. Click **Add** on the toolbar.
5. Set **destinationIpAddress** to 100.100.0.0, **destinationNetworkMask** to 16, **protocol** to 17 (the IP protocol number assigned to UDP is 17), and **action** to 'Block'.

6. Save.

NOTE! QoS policing applies to LAN and WAN ports only.

QoS policing applies only to forwarding traffic. Traffic addressed to the network element itself cannot be blocked via a QoS rule.

To enable QoS, make sure that the auto-negotiation feature is disabled, and that the output port(s) is (are) in full duplex mode.

12.3 Miscellaneous

12.3.1 Open Shortest Path First

The Open Shortest Path First (OSPF) is a link state routing protocol (unlike RIP which is distance vector routing protocol). Configuring the network element to run OSPF can be performed through **three basic steps**:

1.Configure one or several OSPF areas

2.Configuring the OSPF interfaces

3.Enable OSPF on the network element

Supported OSPF areas: Transit and Stub areas

Three OPSF area types are currently defined by the standards:

- Transit areas (including the backbone area 0.0.0.0) defined in OSPF version 2 (RFC2328). Transit areas accept intra-area, inter-area, and external routes.
- Stub areas defined in OSPF version 2 (RFC2328). Stub areas come in two flavours: they can either accept intra-area, inter-area, and default routes, or only intra-area and default routes. Stub areas which propagate only intra-area and default routes within the area are sometimes referred to as "totally-stub" areas.
- Not-so-stubby areas (NSSA) defined in OSPF NSSA option (RFC1587). NSSAs are a hybrid between transit and stub areas. They can import a few external routes into the area via an Autonomous System Border Router (ASBR) present in the area.

The network element currently supports only transit and stub areas. In addition, it is currently not possible to configure a stub area to

import only intra-are and default routes, i.e. it is not possible to configure an area as a "totally-stub" area.

12.3.1.1 Configure an OSPF area

Procedure: **CONFIGURE A NEW OSPF AREA**

1. Expand the **NE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **OSPF** attribute, and then on the **OspfArea** attribute in the attribute window.
3. Click **Add**.
4. Set the **areaID** attribute.
5. Set the **importAsExternal**[1] and **metric**[2] attributes as required.
6. Click **Save**.

12.3.1.2 Configure an OSPF interface

Procedure: **CONFIGURE AN OSPF INTERFACE**

1. Expand the **NE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **OSPF** attribute, and then on the **OspfInterface** attribute in the attribute window.
3. Identify the OSPF interface to configure via its IP address listed under the **interfaceIpAddress** attribute.

1. Setting the importAsExternal attribute to 'importAsExternal' define a transit area, while setting the importAsExternal attribute to 'importNoExternal' define a stub area.
2. The metric attribute is only relevant for stub areas, i.e. when the attribute importAsExternal is set to 'importNoExternal'.

4. Set the **areaId** attribute to the area to which you want to attach the interface. Note that the area must have been previously defined (see “Configure an OSPF area” on page 593.

5. Set the **interfaceType** attribute to the required type, and make sure that the **ospfEnable** attribute is set to **'Enabled'** (this is the default value).

6. Edit the **helloInterval**, **metricValue**, **authentificationType**, **authentificationKey**, t**ransitDelay**, **routerDeadInterval**, **pollInterval**, **retransmissionInterval**, and **priority** attributes if required.

7. Click **Save**.

Enabling OSPF on the network element

Procedure: **ENABLE OSPF GLOBALLY**

1. Expand the **NE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **OSPF** attribute in the attribute window.
3. Set the **ospfEnable** attribute to '**enabled**'.
4. Click **Save**.

12.3.2 IP Redundancy configuration

The IP redundancy feature allows the network element to be configured as a back-up router for other routers, referred to as main routers.

Procedure: **CONFIGURE THE NE AS A BACK-UP ROUTER FOR A MAIN ROUTER**

1. Expand the **NE** managed object, and then click the **IP** managed object in the Management Tree.
2. Click on the **Redundancy** attribute in the attribute window.
3. Set the i**pRedundancyEnable** attribute to '**enable**'.
4. Click **Save**.
5. Click on the **RedundancyInterface** attribute in the attribute window.
6. Click **Add**.
7. Set the **interfaceIpAddress** attribute to the **IP** address of the network element on which the redundancy feature is working.
8. Set the **mainRouterIpAddress** attribute to the **IP address** of the main router[1] to be backed-up by the network element.

1. Note that the IP address of the main router (mainRouterIpAddress attribute) must be on the same subnet as the IP address of the network element (interfaceIpAddress attribute).

9. Edit the **pollInterval**, and **timeout attributes** as required.

10. Click **Save**.

Example - back-up router

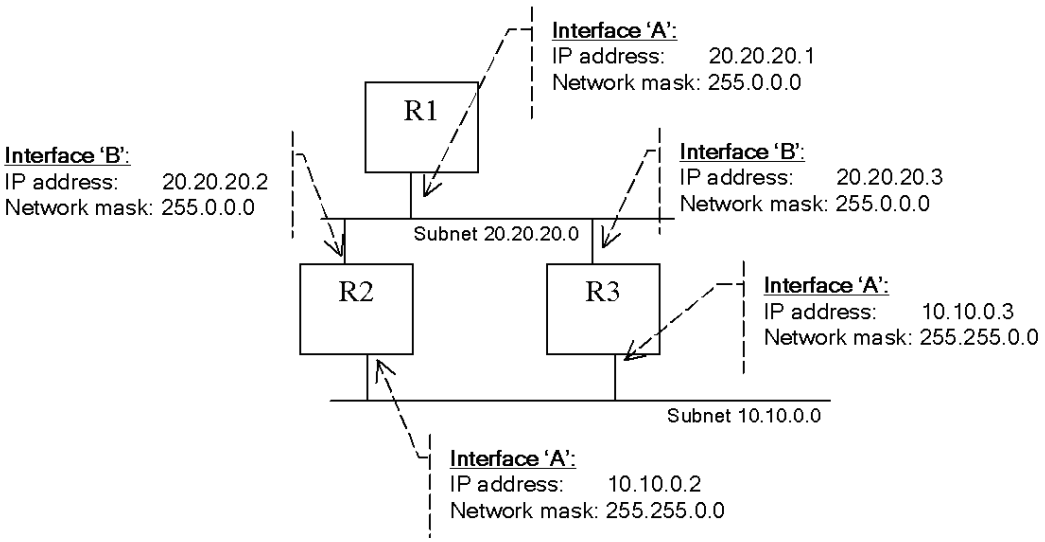


Figure 185 IP Redundancy: Main router R2 backed up by router R3

To back-up main router R2 (on the 20.20.20.0 subnet) by router R3:

Add the following entry in AXX 9200 EDGE > **IP**> **Redundancy** > **ipRedundancyInterface** for router R3 (see Figure 185):

1. Set interfaceIpAddress: **20.20.20.3**

2. Set mainRouterIpAddress: **20.20.20.2**

3. SetpollInterval: **3**

4. Set timeout: **12**

12.3.3 DHCP

The network element can be configured as a DHCP server (AXX 9200 EDGE > IP >DHCP >dhcpServerEnable set to 'enable') or as a DHCP relay (AXX 9200 EDGE > IP > DHCP > dhcpServerEnable set to 'disable').

If the network element is configured to relay DHCP requests, the IP address of the next DHCP server must be configured by setting the AXX 9200 EDGE > IP > DHCP > **nextServerIpAddress** attribute.

If the network element is configured as a DHCP server, the user can configure the ranges of available IP addresses for every IP interface on the network element (see “Configuring a range of IP addresses for the DHCP server” on page 597). In addition, by using DHCP manual allocation mechanism, the user can define the IP address to be allocated to a host based on its MAC address and optionally its name (see “Configure the DHCP server for manual allocation” on page 598).

Configuring a range of IP addresses for the DHCP server

Procedure: **CONFIGURE A RANGE OF IP ADDRESSES**

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **DHCP** attribute, and then on the **dhcpAddressRange** attribute in the attribute window.
3. Click **Add**.
4. Set the **interfaceIpAddress** attribute to the IP address of the network element on which the range of IP address shall be available.
5. Set the **ipAddressFrom** and **ipAddressTo** attributes to the **first** and the **last IP address** allocated for the range respectively.
6. Edit the **leaseTime**, **defaultRouter**, and **probeEnable** attributes as required.
7. **Save**.

NOTE! The range of available IP addresses [ipAddressFrom; ipAddressTo] must be on the same subnet as the IP address of the interface (interfaceIpAddress) on which the range applies.
If you want to allocate IP address permanently, i.e. to use the automatic allocation mode of DHCP, the leaseTime attribute must be set to -1.

Configure the DHCP server for manual allocation

Procedure: **CONFIGURE AN IP ADDRESS FOR MANUAL ALLOCATION**

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **DHCP** attribute, and then on the **dhcpAllocation** attribute in the attribute window.
3. Click **Add**.
4. Set the **ipAddress** attribute to the IP address to be allocated via the manual allocation mode of DHCP.
5. Set the **mechanism** attribute to **manual**.
6. Edit the **macAddress**, **hostName**, **defaultRouter**, **configurationServerIpAddress**, and **configurationFileName** attributes as required.
7. **Save**.

NOTE! To match any incoming MAC address, the macAddress attribute must be to “00:00:00:00:00:00”.

12.4 FAQ

What are the common UDP ports?

UDP Port #	Acronym	Application
37	TIME	Time
42	NAMESERVER	Host Name Server
43	NICNAME	Who Is
53	DOMAIN	Domain Name Server
67	BOOTPS	Bootstrap Protocol Server
68	BOOTPC	Bootstrap Protocol Client
69	TFTP	Trivial File Transfer
111	SUNRPC	Sun Microsystems Rpc
123	NTP	Network time
137	NetBiosNameService	NT Server to Station Connections
138	NetBiosDatagramService	NT Server to Station Connections
139	NetBios SessionService	NT Server to Station Connections
161	SNMP	Simple Network Management
162	SNMP	Simple Network Management Traps
513		Unix Rwho Daemon
514	syslog	System Log
525	timed	Time Daemon

What are the different types of link state advertisements?

1	Router-LSAs
2	Network-LSAs
3	Summary-LSAs (IP network)
4	Summary-LSAs (ASBR)
5	AS-external-LSAs

Table 20 Link state type (according to RFC2328, Appendix A.4.1)

12.5 IPM Router

12.5.1 Introduction

The purpose of this section is to guide you through management of the IP Multicast service on the NE, that involves:

- Presentation and modification of IPM, i.e. forwarding of IP multicast data grams
- Presentation and modification IGMP
- Presentation and modification of PIM.

It is assumed you have the appropriate rights to perform management operations.

12.5.2 IP Multicast configuration

The network element supports IP multicast (IPM). IP multicast is based on the concept of a group. A group is made up of the devices which have expressed interest in receiving a particular data stream. All members of the group receive the data sent by a source to the multicast group address.

In order to forward IP multicast traffic, the network element supports two protocols:

- The Internet Group Management Protocol (IGMP) used by the hosts to inform the router(s) on the LAN about which multicast addresses they want to receive.
- The Protocol-Independent Multicast - Dense Mode (PIM-DM) protocol used by the routers to exchange multicast information with other multicast routers.

12.5.2.1 Enable multicast routing on the network

To enable multicast routing on the network, the following basic steps can be followed:

1. **Enable IP multicast** feature on the network element. Set the AXX 9200 EDGE > IP >IPM > **ipmRouteEnable** attribute to '**enabled**'.

2. Configure **IGMP** interfaces
   (see “Configuring IGMP interfaces” on page 601)

3. Configure **PIM** interfaces
   (see “” on page 601)

12.5.2.2 Configuring IGMP interfaces

Procedure: CONFIGURE AN IGMP INTERFACE

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **IPM** attribute, then on the **IGMP** attribute, and then on the **igmpInterface** attribute in the attribute window.
3. Click **Add**.
4. Set the **interfaceNumber** attribute to the **ifIndex** of the interface on which IGMP shall be enabled.
5. Edit the **queryInterval**, **version**, **queryMaxResponseTime**, **robustness**, and **lastMemberQueryInterval** attributes as required.
6. Click **Save**.

Procedure: CONFIGURE A PIM INTERFACE

1. Click on the **AXX 9200 EDGE** managed object, and then on the **IP** managed object in the Management Tree.
2. Click on the **IPM** attribute, then on the **PIM** attribute, and then on the **pimInterface** attribute in the attribute window.
3. Click **Add**.
4. Set the **interfaceNumber** attribute to the **ifIndex** of the interface on which PIM shall be enabled.
5. Edit the **helloInterva**l, and **joinPruneInterval** attributes as required.
6. Click **Save**.

12.6 IPX Router

This chapter describes the configuration operations supported by the IPX managed object (M.O.).

- Introduction
- Examples this chapter is a repository of simple, but yet typical configuration scenarios.
- Troubleshooting and FAQ this chapter contains a few troubleshooting tips, and gives answers to a number of Frequently Asked Questions.

NOTE! The IPX M.O. exists only if the Router license has been downloaded to the network element.

Procedure: **CONFIGURE AN IPX INTERFACE WITH AN IPX ADDRESS**

1. Click on the AXX 9200 EDGE managed object, and then the IPX managed object in the Management Tree.
2. Double-click on ipxInterface in the attributes window.
3. Click Add on the toolbar.
4. The following attributes have no default values, and must therefore be defined:

circuit:
Set a number to identify this IPX circuit.

interfaceNumber:
Set the interface number. An IPX interface can be defined for a LAN port, a WAN port, or a VLAN. The interface number corresponding to these objects is specified by the ifIndex attribute present under their respective M.O.

netIpxAddress:
Set the network number portion of the IPX address according to your addressing plan. This is entered as eight hexadecimal digits.

timeToNetwork:
Set the time to network (in 1/18th of a second).

layer2Encapsulation: set the layer 2 encapsulation associated with the interface. Note that if the interface refers to a VLAN, layer2Encapsulation must be set to the same encapsulation as the one used by the VLAN. Possible encapsulations are[1]:

- Novell, a.k.a "802.3 raw" This corresponds to the initial encapsulation scheme Novell used It includes an IEEE 802.3 header (including the Length field) but no IEEE 802.2 (LLC) header. The IPX datagram immediately follows the 802.3 Length field.
- Ethernet a.k.a. "Ethernet Version 2", or "Ethernet-II" This corresponds to the standard Ethernet Version 2 header, which consists of Destination and Source Address fields followed by an EtherType field.
- LLC This corresponds to the standard IEEE 802.3 frame format, i.e. an 802.3 frame encapsulating an 802.2 (LLC) frame, which in turns encapsulates the IPX datagram.

1. For additional information about the different types of layer 2 encapsulation, refer to “What is the difference between the four IPX layer 2 encapsulation schemes?” on page 609, in the FAQ section.

- SNAP This corresponds to the Subnetwork Access Protocol (SNAP) extension to IEEE 802.2. IEEE 802.2 SNAP provides a means to define a field similar to the EtherType filed in the Ethernet Version 2 specification.

adminStatus:
Set the administrative status to 'on' to activate the circuit.

5. Save.

NOTE! One interface (identified by a specific ifIndex) can be allocated several IPX addresses. This enables the user to connect the interface to a network segment where multiple subnets are defined.

12.6.1 Configuration of a RIP filter

An IPX RIP filter allows the user to control the propagation of RIP routing information, and eventually to modify the RIP routing by filtering out information about specific routes. In addition, IPX RIP filters help reducing the size of the RIP table allowing for a faster table look-up, and releasing memory for other processes.

Procedure: **CREATE AN IPX RIP GLOBAL FILTER**

1. Click on the AXX 9200 EDGE managed object, and then on the IPX managed object in the Management Tree.

2. Double click on the ripGlobalFilter attribute in the attributes window.

3. Click Add on the toolbar.

4. Set the type, netIpxAddress, networkMask, and action attributes.

5. Save.

12.6.1.1 Examples

To define a RIP global filter which prevents the network element from advertising any route to the IPX networks starting with IPX network number 1A 20 3E, enter the following filter:

Type: output

NetIpxAddress: 1A 20 3E 00

NetworkMask: FF FF FF 00

Action: Deny

To define a RIP interface filter which prevents the network element from accepting routes for the IPX networks starting with IPX network number 1A 20 3E, but still accepts routes for the IPX network 1A 20 3E B1, enter the following two filters

#1 Type: input

NetIpxAddress: 1A 20 3E 00

NetworkMask: FF FF FF 00

Action: Deny

#2 Type: input

NetIpxAddress: 1A 20 3E B1

NetworkMask: FF FF FF FF

Action: Permit

NOTE! The default behaviour for the network element is to permit incoming and outgoing RIP information. To modify this default behaviour, a filter with networkMask set to 00 00 00 00 can be created with action set to Deny. Such a filter will per default deny any incoming or outgoing (depending on the value set for the type attribute) RIP information for which there is no more specific filter.

The procedure to define a RIP circuit filter is identical to the procedure described above. A RIP circuit filter applies only to a specific circuit (specified by the circuit attribute) instead of applying to every RIP-enabled circuit on the network element.

RIP interface filters take precedence over RIP global filters.

12.6.2 Configuration of a SAP filter

An IPX SAP filter allows the user to control the propagation of SAP information, and eventually to modify the SAP table by filtering out information about specific servers. In addition, IPX SAP filters help reducing the size of the SAP table allowing for a faster table look-up, and releasing memory for other processes.

Procedure: **CREATE AN IPX SAP GLOBAL FILTER**

1. Click on the AXX 9200 EDGE managed object, and then on the IPX managed object in the Management Tree.
2. Double click on the sapGlobalFilter attribute in the attributes window.
3. Click Add on the toolbar.
4. Set the type, netIpxAddress, networkMask, serviceType, serviceName, and action attributes.
5. Save.

NOTE! For a list over common SAP types (used for the serviceType attribute), refer to 5.2.2 in the FAQ section.

Note that the serviceName attribute corresponds to the user-defined name for this service defined on the server where this service resides. The service name may be up to 48 characters in length,

and the '*' wildcard can be used to replace part of the name, e.g. sh* indicates any name starting with sh.

The procedure to define a RIP circuit filter is identical to the procedure described above. A RIP circuit filter applies only to a specific circuit (specified by the circuit attribute) instead of applying to every RIP-enabled circuit on the network element.

The default behaviour for the network element is to permit incoming and outgoing RIP information. To modify this default behaviour, a filter with networkMask set to 00 00 00 00 can be created with action set to Deny. Such a filter will per default deny any incoming or outgoing (depending on the value set for the type attribute) RIP information for which there is no more specific filter.

12.7 FAQ

12.7.1 How to interpret an IPX address?

An IPX address consists of a 4-byte Network Number, a 6-byte Node Number, and a 2-byte Socket Number as shown in Figure 1.

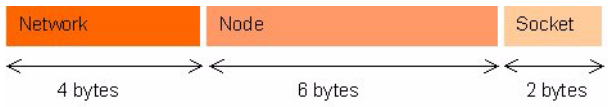


Figure 186 IPX address

The network number must be the same for all nodes on a particular physical network segment. The node number is usually the hardware address (MAC address) of the interface card, and must be unique inside the particular IPX network (specifies by the network number). The socket number corresponds to the particular service being accessed within the node. This is equivalent to the UDP/TCP port number in TCP-IP.

Note that to identify an IPX node, only the network and the node portion are required (sockets are "intra-node addresses" used for intra-node routing only).

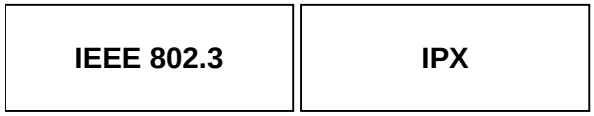
In the implementation of IPX supported by the network element, the node address is by default set to the MAC address of the interface configured for IPX, and cannot be edited. This enables IPX to know

directly the data link address (MAC address) of the destination (the address is encapsulated within the destination IPX address). Therefore no additional protocol is required to map between IPX address and data link address (MAC address).

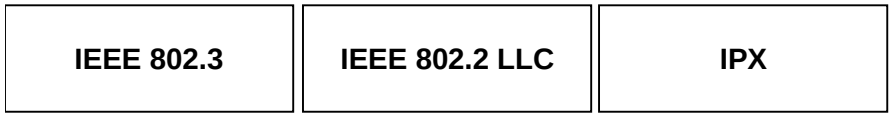
In AXX 9840 INSITE, the attributes xxxNetIpxAddress, xxxNodeIpxAddress, and xxxserverSocketIpxAddress represent the network number portion of an IPX address, the node portion of an IPX address, and the socket portion of an IPX address respectively.

12.7.2 What is the difference between the four IPX layer 2 encapsulation schemes?

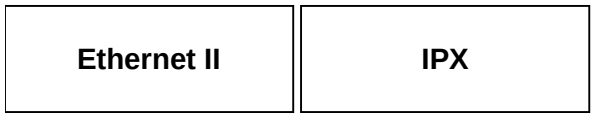
Novell encapsulation:



LLC encapsulation:



Ethernet II encapsulation:



SNAP encapsulation:

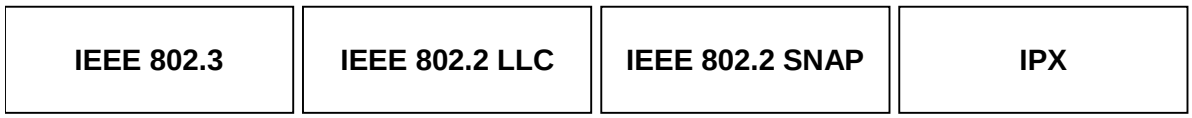


Figure 187 IPX layer 2 encapsulation types

12.7.3 What are the common SAP types?

in Table 21 below, you can see some common SAP types. A complete list of the SAP types is maintained by the Internet Assigned Numbers Authority (IANA), and can be accessed on the Web at the following address http://www.iana.org/assignments/novell-sap-numbers.

0004	File Server
0005	Job Server
0007	Print Server
0009	Archive Server
000A	Job Queue
0020	NetBIOS
0021	NAS SNA Gateway
0047	Advertising Print Server
004B	Btrieve VAP/NML 5.0
004C	Netware SQL VAP/NML Server
007A	TES - NetWare VMS
0098	Netware Access Server
0111	Test Server
0166	Netware Management
026A	Network Management (NMS) Service Console
026B	Time Synchronization Server
0278	Netware Directory Server

Table 21 Novell SAP types

13 Management of AXX155

13.1 AXX155 - Overview

13.1.1 Physical Overview

The AXX155 is a network element that combines IP and TDM traffic in an aggregate interface and maps it on to an STM-1 fiber optical network. It can be used both as CPE[1] and PoP[2] equipment.

The aggregate interface supports terminal multiplexer functions, and maps LAN / TDM to SDH VC12 containers only (no VC3 mapping).

The L2 Bridge/Switch switches Ethernet based LAN traffic between the different LAN and WAN ports.

The Tributary mapper maps up to four E1 synchronous bit streams to 4 VC12 containers in the STM-1 frame.

The Ethernet mapper maps the WAN traffic into configurable number VC-12 containers to provide the expected WAN bandwidth on the STM-1 trunk.

The CLI port and Management LAN port provides access to the management functions of the network element.

The synch. port may be used for external SDH frame synchronization sources, if required

The alarm ports provide inputs for external alarms, and relay outputs for external alarm indicators.

The user channel is a 64 Kb synchronous or 19.2 KBaud asynchronous channel for general use.

1. CPE: Customer Premises Equipment

2. PoP: (Service Provider) Point of Presence

13.1.2 Management of AXX155

Please refer to “Using AXX 9840 INSITE” for details on navigation and information about the different GUI applications.

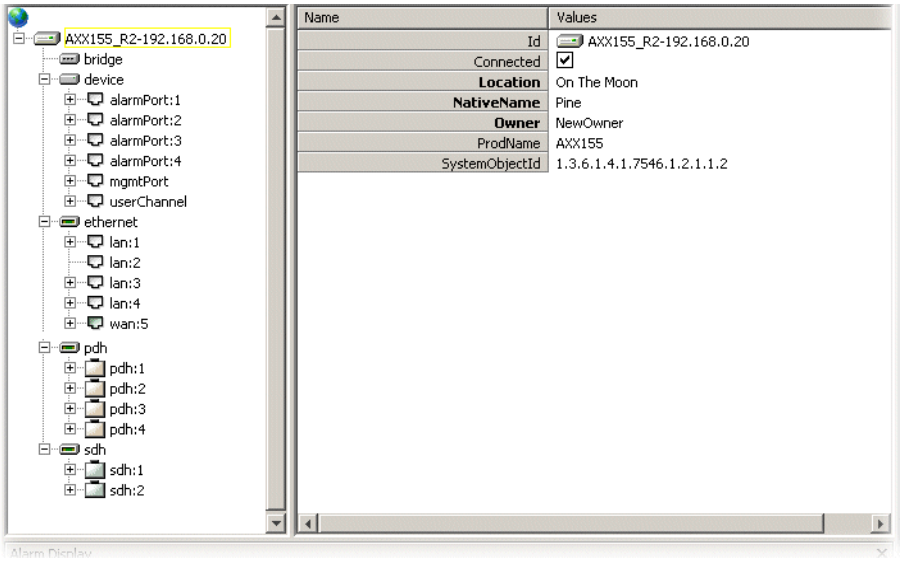


Figure 188 Example of AXX155 - viewed in AXX 9840 INSITE

NE general

Parent MO	Child MO	Attribute	Hyperlink
AXX155_R2	N/A	Id	
	N/A	Connected	
	N/A	Location	See “” on page 324
	N/A	NativeName	
	N/A	Owner	
	N/A	ProdName	
	N/A	SystemObjectid	

Bridge

Please see “Bridge” on page 531 and “Manage VLAN” on page 546

Device

Parent MO	Child MO	Attribute	Hyperlink
device	N/A	AlarmConfig	“Alarm and Event configuration” on page 351

	N/A	ConfigData	“How to backup and restore configuration data” on page 284
	N/A	Features	“Available features (licenses)” on page 327
	N/A	LedandOutput	“LEDs and alarm output” on page 332
	N/A	Ping	“Ping mechanism” on page 333
	N/A	PortMirroring	
	N/A	Restart	Please see page 7-331
	N/A	StatusReporting	
	N/A	Synchronization	“Manage synchronization” on page 336
	N/A	Time	“” on page 325
	N/A	Users	“Users” on page 326
	Alarmports [1:4]		“LEDs and alarm output” on page 332
	MngtPort		“Management Port Configuration - AXX 9200 EDGE” on page 302
	UserChannel		

Ethernet

Parent MO	Child MO	Attribute	Hyperlink
ethernet	lan [1:4]		“LAN Ports” on page 402
	wan		“WAN Ports - AXX155E” on page 474

IP

AXX155 does not support routing.

PDH

Parent MO	Child MO	Attribute	Hyperlink
pdh	pdh [1::4]		Please see “PDH ports” on page 395.

SDH

Parent MO	Child MO	Attribute	Hyperlink
sdh	sdh:1		Please see “SDH ports” on page 385

13.1.3 Miscellaneous

WAN to SDH mapping

“WAN Ports - AXX155E” on page 474.

13.1.4 Feature Overview

The features of the AXX155 network element are configurable and a target for management by a Craft Terminal or Network/Element Management system. The following sub chapters provides an overview of the main features.

SDH Features

- Carrying E1-type TDM synchronous traffic on an STM-1 trunk
- Transportation of LAN traffic on an STM-1 trunk. This includes both L2 switching between LAN/WAN ports, and carrying LAN/WAN traffic on an STM-1 trunk
- Linear Multiplex Section Protection (MSP) on the two optical STM-1 ports of the network element.
- G826 Performance Monitoring on RS, MS, VC-12 and VC4 section levels of the STM-1 frame.
- Selectable sources for SDH Frame synchronization
- General purpose User Channels (F1 bytes in RSOH part of the SDH frame) configurable to synchronous/asynchronous rates

IP Features

The AXX155 provides basic OSI layer 2 features (bridging) and optional layer 3 routing features.

L2 (Bridging) features

- MAC switching
- Self learning of MAC addresses
- Automatic aging of MAC addresses
- Transparent Bridging
- VLAN
- IEE 802.1Q VLAN tagging
- Back pressure and flow control handling
- Spanning tree protocol support

BootP/BootP Relay (installation and commissioning support)

OSI Features (Optional)

OSI stack to support alternate protocol modes in the MCN

TDM Features

- 4 x tributary ports configurable to TRA and PRA E1 modes
- Test looping of tributary ports, both internal and customer side

Alarm Port Features

- Four configurable alarm input ports for external alarm sources

General AXX155 Device Features

Automatic time reference support according to RFC 868, supported by a built-in TP server

MCN Features

Feature		AXX155
Communication	**IP/DCC-Broadcasted DCCR**	X
	IP/DCC & Broadcasted DCCM	X
	IP/DCC & Routed	-
	IP/PPP DCCR	-
	IP/PPP DCCM	-
	IP unnumbered	-
	IP-Forwarding	X
	IP-Routing	-
	CLNP Routing	X (b)
	IP/OSI (OSI-NE) DCCR	X (b)
	IP/OSI (OSI-NE) DCCM	X (b)
	IP/OSI (OSI-Gateway)	X (b)
	In-band	X (d)

Legend

X= Supported
NA= Not applicable
(a)= Software based routing if no license loaded.

(b)= OSI license required.
(c)= Dependent of equipped module(s)
(d)= Indirectly by using a crossed cable between MNGT port and a LAN port.
A separate VLAN must be configured to take care of management traffic

14 Management of AXX10 and AXX11

14.1 Management

14.1.1 General

NOTE! Throughout the chapter AXX10 and AXX11 will be denoted as AXX10/11.

NOTE! The AXX10/11 can only be used in conjunction with an AXX 9200 EDGE or AXX155A Network Element - hereafter denoted as the NE.
Only AXX155A 2.0 and greater support AXX11

The AXX10/11 is seen as an integrated part of the NE. It cannot function as a standalone NE. You can only perform management of AXX10/11 through the NE to which it is connected.

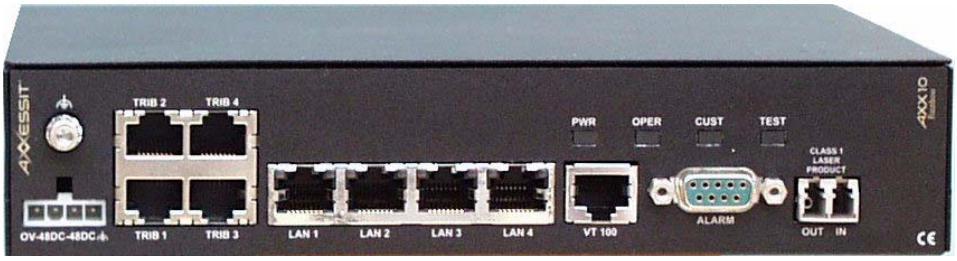


Figure 189 AXX10 panel

Figure 190 AXX11 panel

NOTE The only difference between AXX10 and AXX11 is the two extra legacy ports for V.35, V.36 or X.21data on the AXX11 unit.

Management for AXX10/11 supports:

14.1.1.1 SDH management

- Alarms
- Performance

14.1.1.2 PDH management

- Alarms

14.1.1.3 WAN port capacity

14.1.1.4 Bridge configuration

14.1.1.5 Software download

14.1.2 Fault Management

AXX10/11 forwards all its alarms and events to the NE. The NE will not acknowledge an alarm or event from AXX10/11.

The alarms are time stamped by the NE. The AXX10/11 alarms and events are then stored on the NE.

Alarm suppression

It is possible to inhibit alarm reporting for a specific source, i.e., managed object. The source can be specified on class level or one instance level.

Class level:

- all SDH related managed objects

Instance level:

- PDH managed objects

It is possible to inhibit all alarms from one AXX10/11.

The AXX10/11 provides alarm suppression for alarms detected on the AXX10/11 itself. An alarm is suppressed in the following cases:

- If the managed object subject to the alarm is disabled or irrelevant to the traffic payload.
- If the alarm is caused by a higher order alarm simultaneously present.

The AXX10/11 performs alarm suppression on a per second basis. The resulting alarm status is reported to the NE and is available for local displaying. For the AXX10/11, the alarm suppression scheme in Table 22 applies.

SUPPRESSED ALARMS											
SUPPRESSING ALARMS		**SPI**	**RS**	**MS**	**AU-4**	**VC4**	**TU3**	**VC3**	**TU12**	**VC12**	**PDH**
SPI	LOS	LOF	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALLRX
	LOF	-	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALLRX
RS	TIM	-	ALLOTHER	ALL	ALL	ALL	ALL	ALL	ALL	ALL	ALLRX
	CSF	-	-	-	-	-	-	-	-	-	-
	EXC	-	-	DEG	-	-	-	-	-	-	-
	DEG	-	-	-	-	-	-	-	-	-	-
MS	AIS	-	-	ALLOTHER	ALL	ALL	ALL	ALL	ALL	ALL	ALLRX
	CSF	-	-	-	-	-	-	-	-	-	-
	EXC	-	-	DEG	-	-	-	-	-	-	-
	DEG	-	-	-	-	-	-	-	-	-	-
	RDI	-	-	-	-	-	-	-	-	-	-
AU-4	LOP	-	-	-	AIS	ALL	ALL	ALL	ALL	ALL	ALLRX
	AIS	-	-	-	-	ALL	ALL	ALL	ALL	ALL	ALLRX
VC4	UNEQ	-	-	-	-	ALLOTHER	ALL	ALL	ALL	ALL	ALLRX
	TIM	-	-	-	-	PLMLOMEXCDEGRDI	ALL	ALL	ALL	ALL	ALLRX
	PLM	-	-	-	-	LOM	ALL	ALL	ALL	ALL	ALLRX
	LOM	-	-	-	-	-	ALL	ALL	ALL	ALL	ALLRX
	EXC	-	-	-	-	DEG	-	-	-	-	-
	DEG	-	-	-	-	-	-	-	-	-	-
	RDI	-	-	-	-	-	-	-	-	-	-
TU12	LOP	-	-	-	-	-	-	-	AIS	ALL	ALLRX
	AIS	-	-	-	-	-	-	-	-	ALL	ALLRX

SUPPRESSED ALARMS											
VC12	UNEQ	-	-	-	-	-	-	-	-	ALLOTHER	ALLRX
	TIM	-	-	-	-	-	-	-	-	PLMEXCDEGRDI	ALLRX
	PLM	-	-	-	-	-	-	-	-	-	ALLRX
	EXC	-	-	-	-	-	-	-	-	DEG	-
	DEG	-	-	-	-	-	-	-	-	-	-
	RDI	-	-	-	-	-	-	-	-	-	-
PDH	AISRX	-	-	-	-	-	-	-	-	-	LOFRX
	LOFRX	-	-	-	-	-	-	-	-	-	-
	LOS	-	-	-	-	-	-	-	-	-	AISTXLOFTX
	AISTX	-	-	-	-	-	-	-	-	-	LOFTX
	LOFTX	-	-	-	-	-	-	-	-	-	-

Table 22 AXX10/11 alarm suppression table

Alarm persistency filters

On the AXX10/11, alarm persistency filtering is not supported. However, the NE will perform persistency filtering to all retrieved AXX10/11 alarms before presenting them to the management system.

AXX10/11 alarm filtering is included in the NE alarm management strategy.

Alarm severity

The severity of alarms can be assigned by the management system. The assignment is on managed object type level and not managed object instance level, i.e. for each combination of managed object type and alarm id the severity can be assigned.

Legal values for severity are:

Severity
Critical
Major
Minor
Warning

The complete list of alarm ids and managed object types are presented in Table 23 The numbers indicate the maximum number of instances of each managed object that can generate the different alarm ids.

Alarmidentifier	**MangedObject**	**Device(Unit)**	**Power**	**SDH Port**	**RS**	**MS**	**AU-4**	**VC4**	**TU12**	**VC12**	**E12**	**WAN Port**	**LAN Port**	**AlarmPort**
UNIT		1												
PWRIN			2											
LOS				1							16	1	4	
LOF				1										
CSF					1	1								
LOP							1		63					
AIS						1	1		63					
RDI						1		1		63				
TIM					1			1		63				
LOM								1						
PLM								1		63				
EXC					1	1		1		63				
DEG					1	1		1		63				

Alarmidentifier	MangedObject	Device(Unit)	Power	SDH Port	RS	MS	AU-4	VC4	TU12	VC12	E12	WAN Port	LAN Port	AlarmPort
UNEQ								1		63				
AISTX											16			
AISRX											16			
LOFTX											16			
LOFRX											16			
AL_INP														4

Table 23 Managed objects and alarm ids

14.1.2.1 Comments to Table 23

- The BER alarms EXC/DEG are calculated by the AXX10/11 before sent to the NE
- In AXX10/11 there is no need to present T0_HOLDOVER as an explicit alarm condition (as an SPI failure is the only cause for the T0 clock to enter holdover)
- The UNIT alarm covers diagnostic alarms related to internal AXX10/11 hardware, such as the power supply, memory, FPGA devices, LAN switches etc.

14.1.3 Configuration Management

Software Download

The management system initiates download of a new software version from the NE to the remote unit, i.e. AXX10/11. The download process does not influence traffic processing. The new software is used by AXX10/11 when booting after the next restart. The previous software version is saved in the device. If booting with the new software fails, the AXX10/11 re-boots with the old software and raises an alarm.

Device Reset

It is possible to reset (reboot) the device with or without resetting the current configuration. Reboot does not affect the TDM traffic.

Device Replacement

It is possible to replace an AXX10/11 device with a new device with an identical physical configuration. The management system interprets the new device as the old device and no manual configuration on the device is required.

Connection between AXX10/11 and the NE

The management system reports an alarm if the NE has lost contact with the AXX10/11. This alarm is a result of correlation of the fact that an SDH port goes down and that an AXX10/11 is connected to this port.

14.1.4 Performance Management

General

For the AXX10/11, performance monitoring is provided for the STM-1 aggregate link with its subordinate RS, MS and VC layers. Performance parameters are calculated and presented individually for both directions of transmission (i.e. uplink and downlink). For the VC layers, performance data is calculated for terminated trails only.

Calculation of performance parameters

The NE and the AXX10/11 collect alarms and performance counters individually at each side of the STM-1 port (AXX10/11 link) on a per second basis. The performance calculations provided at the AXX10/11 is synchronized (slaved) to the NE on a per second and on a per 15 minutes basis.

The NE calculates performance parameters for all SDH layers terminated at the NE side. Similarly, the AXX10/11 calculates performance parameters for all SDH layers terminated at the AXX10/11 side. This is summarized in Table 24

RS, MS and VC-4 are always terminated (and monitored) at each side of the AXX10/11 link. The VC-12s are monitored only if terminated at the corresponding side of the link

	RS (B1)	**MS(B2)**		**VC4(B3)**		**VC-12 (V5)**	
Terminating side	Near	Near	Far	Near	Far	Near	Far
NE	x	x	X	x	x	x	X
AXX10/11	x	x	X	x	x	x	x

Table 24 Calculated performance parameters

Presentation of performance parameters

For each monitored (RS, MS or VC) instance, the following G.826 parameters are presented:

UAS	Unavailable Seconds
SES	Severely Errored Seconds
ES	Errored Seconds
BBE	Background Block Errors

The performance data is presented as periods containing counters for 15 minutes and 24 hours duration. Performance data is presented for the current (running) period as well as for a fixed number of recent periods.

The AXX10/11 presents performance parameters referring to the local side only.

The NE presents performance parameters referring to the local side and the remote (AXX10/11) side.

The parameters to be presented on each side of the link are summarized in Table 25 The numbers in the table indicate the number of periods to be presented on each side.

	Parameters referring to the NE side				**Parameters referring to the AXX10/11 side**			
Presentation at	Running 15 min	Recent 15 min	Running24 hour	Recent24 hour	Running15 min	Recent 15 min	Running24 hour	Recent 24 hour
NE	1	16	1	1	1	16	1	1
AXX10/11 (CLI terminal)	-	-	-	-	1	1	-	-

Table 25 Presented performance parameters

The 24 hour counters referring to the AXX10/11 side are calculated and stored on the NE. These counters are based on blocks retrieved from the AXX10/11 every 15 min.

Exchange of performance data

Performance parameters calculated in the AXX10/11 are reported to the NE upon request. In this context, the NE is responsible for the following tasks:

- Synchronization of the AXX10/11 (per second and per 15 minutes) via the S1 channel.
- Automatic retrieval of performance parameters for the recent 15 minutes interval.
- Validation of the performance parameters retrieved from the AXX10/11.

As long as the AXX10/11 is aligned (synchronized) to the NE timing, the measurement intervals on the AXX10/11 will have exactly the same boundaries as the measurement intervals on the NE side. When a 15 minutes synchronization command is received, the AXX10/11 will save the running performance counters into the local recent 15 minutes page and in turn restart the running counters. See Figure 191

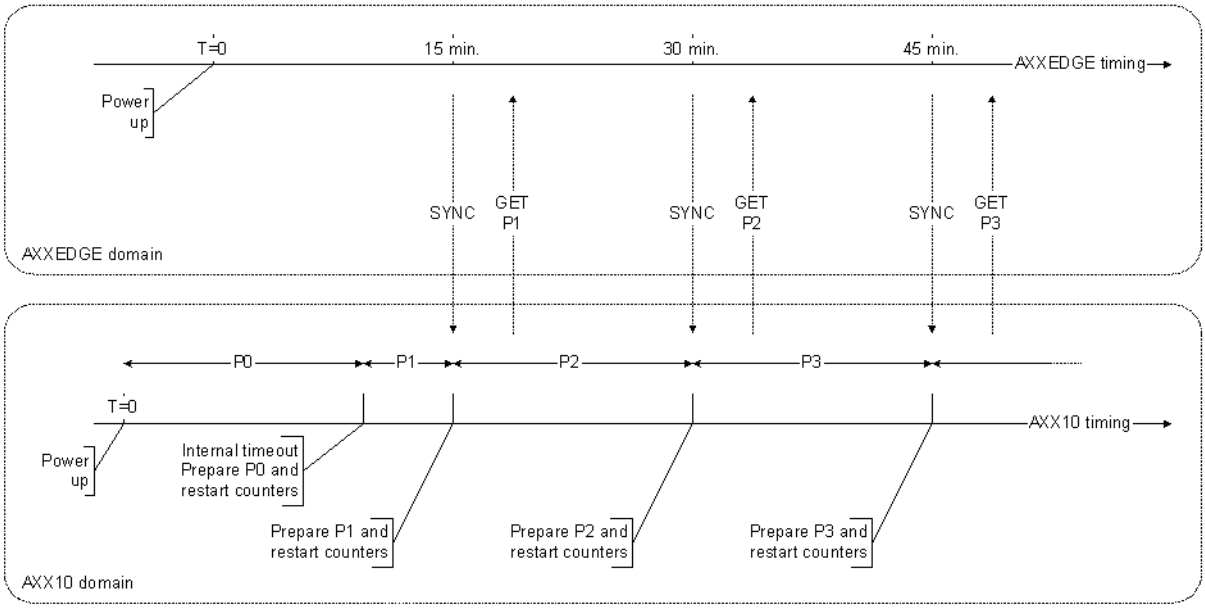


Figure 191 Synchronization and exchange of performance parameters

The NE will in turn issue requests to all connected AXX10/11 devices for retrieval of performance data for the recent 15 minutes period. The performance data packets returned by the AXX10/11 contain the following parameters:

MS	Measured Seconds
UAS	Unavailable Seconds
SES	Severely Errored Seconds
ES	Errored Seconds
BBE	Background Block Errors

The MS value contains the number of seconds elapsed since the previous AXX10/11 counter restart. This value is stored at the NE together with the corresponding performance parameters. As long as the AXX10/11 is synchronized, this value will be 900 (seconds). However, if the MS value for a 15 minutes period does not have this expected value, the NE will mark the interval as incomplete.

The NE will use the retrieved 15 minutes periods for updating the related 24 hour periods. These periods provide the MS parameter. When a 24 hour period expires and less than 24 x 3600 measured seconds (MS) are available, the NE marks the interval as incomplete.

If retrieval of a 15 minutes period fails, the performance counters and the MS value for that period will be cleared and the interval will be categorized as incomplete.

The MS values are available for reading at the management system. The NE is able to request the AXX10/11 to return the running counters for a given managed object.

14.2 Connect the AXX10/11 remote module

14.2.1 Brief description

The purpose of section is to describe the tasks involved in insertion, removal, and management of the remote module AXX10/11 for the NE.

Procedure: **CONNECT THE MODULE**

An AXX10/11 can be connected to any STM-1 interface on the NE modules. They are connected with a fiber.

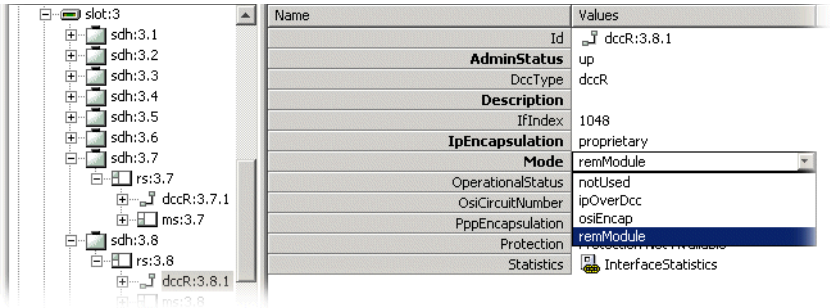
You can configure an expected module and assign it to a port without any physical module present. The system populates the Management Tree according to the specified expected module.

The system starts management of the new remote module.

The alarms from the newly connected remote module are presented in the Notification list.

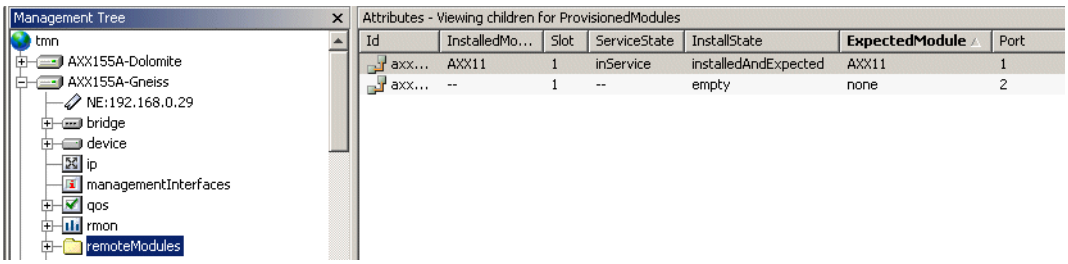
1. Select and **enable** the NE **SDH port** that shall be used for AXX10/11 intreconnection.

2. Set the DCC-R channel to **RemModule**.

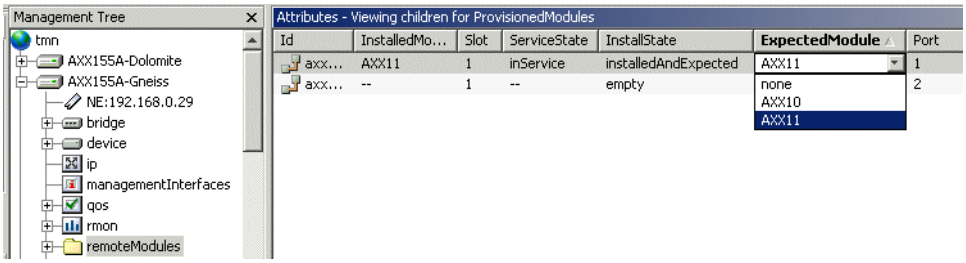


3. Click on **Remote Modules** in the Management Tree

4. Select **Modules** to view available port and slots for AXX10/11.



5. Select table entry according to **slot** and **port** number for the physical connection for the AXX10/11 you are adding.

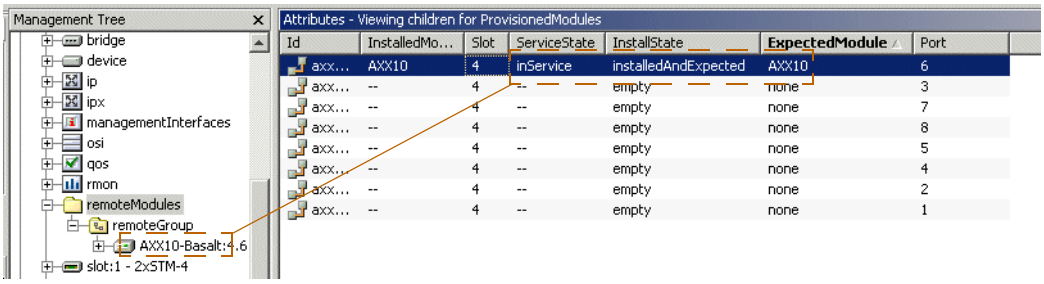


6. Set **Expected Module** to AXX10 or AXX11.

7. Press 

8. View the Management Tree to see the added AXX10/11

9. Click remoteModules and select modules.



10. Press 

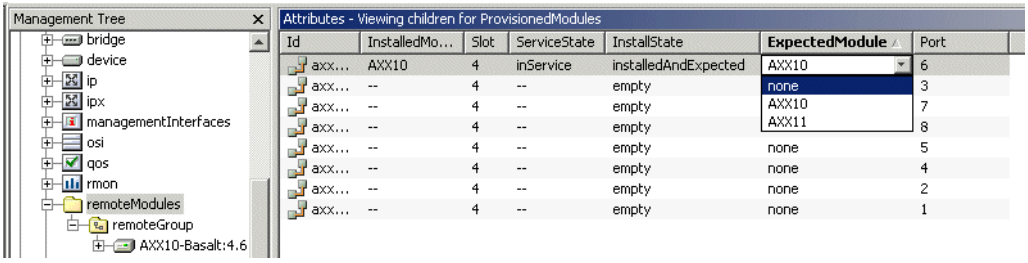
to update the Attribute Viewer

Procedure: **REMOVE AXX10/11 FROM MANAGEMENT**

1. Select **Modules**

2. Select the **AXX10/11** you want to remove from management.

3. Set **Expected Module** to **none**.



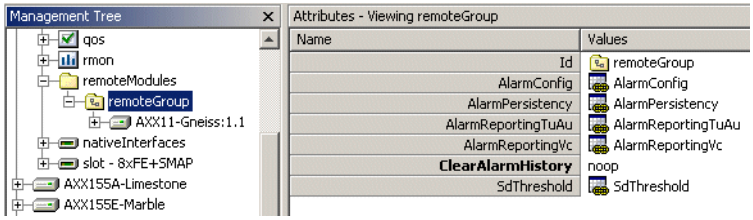
4. Press 

and view the Management Tree to verify that the AXX10/11 is removed.
5. Press 

14.3 Management of AXX10/11

14.3.1 Remote modules

All NEs will have a manage object called remoteModules. When expanding this object you will find the remoteGroup manage object. This object gather common object for all AXX10/11 connected to the NE you are viewing.



14.3.1.1 RemoteGroup

Alarm configuration

Please see “Modify Alarm severity and description” on page 357 for details.

Alarm persistency

Please see “Modify Alarm Persistency” on page 358.

Alarm reporting TU/AU

Please see “Suppress Specific Alarms” on page 353.

Alarm reporting VC

Please see “Suppress RDI, EXC, DEG, SSF alarms” on page 353.

Clear Alarm history

Please see “Logs (alarm logs, performance data logs)” on page 332.

SDH treshold

Please see “Set Signal Degrade Threshold” on page 355.

14.3.2 SW Download (through parent NE)

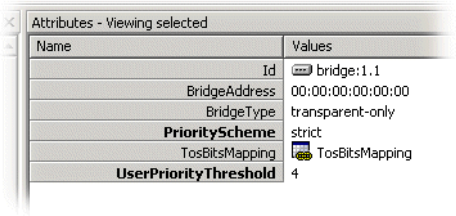
Software is loaded to AXX10/11 from the NE. See “Presentation of the NE Maintenance GUI” on page 257 and/ or “Software Download to the NE” on page 291.

14.3.3 Bridge settings

1. Select an AXX10/11 managed object in the Management Tree on the desktop. The system presents the containing managed objects on the AXX10/11.

2. Select the **Bridge** port.

The system presents the attributes for the Bridge.



Id

BrigdeAddress

BrigdeType (transparent only)

14.3.3.1 PriorityScheme

Packets with different priority are served according to a global setting programmable from bridge window. PriorityScheme has 4 options:

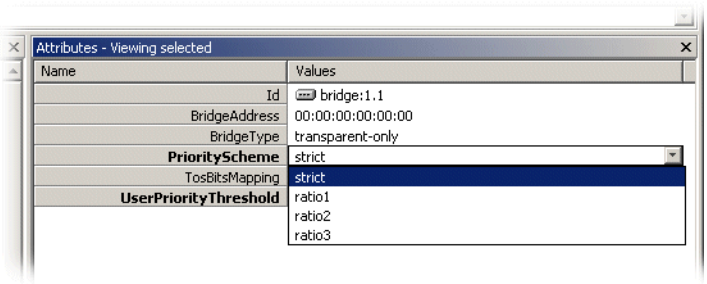
Strict = always deliver high priority packets first

Ratio1 = deliver high/low packets at ratio 10/1

Ratio2 = deliver high/low packets at ratio 5/1

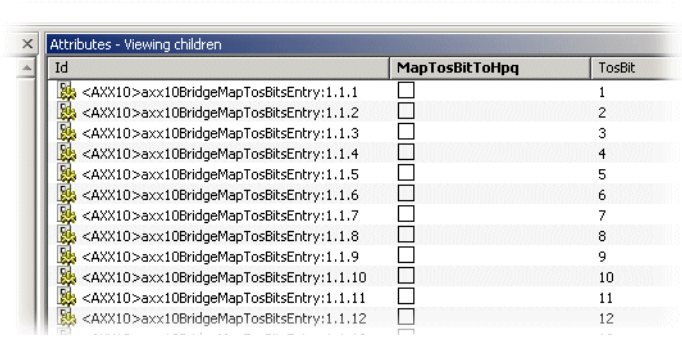
Ratio3 = deliver high/low packets at ratio 2/1

Default value is Strict.



14.3.3.2 ToBitsMapping

The IPv4 TOS priority control implement a fully decoded 64-bit



DSCP (Differentiated Services Code Point) used to determine priority from the 6bit TOS field in the IP header. The most significant 6 bits of the TOS field are fully decoded into 64 possibilities. If a TOS bit is enabled in the switch priority of a packet with corresponding header becomes high. TOS bits are set globally in the switch and the setting is valid for all ports.

Default value is disabled for all TOS bits.

TOS setting is done from the bridge window:

14.3.3.3 UserPriorityTreshold

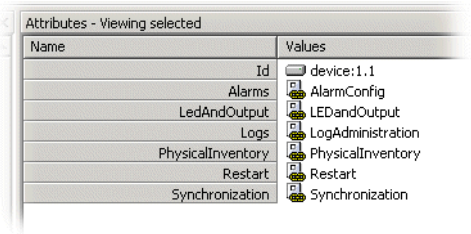
QoS / CoS packets prioritization

The switch operates with two packet queues one for high priority packets and one for low priority packets. To classify priority for incoming 802.1Q packets, "user priority" is compared against a predefined programmable value. If the priority of the incoming packet is greater or equal to the predefined priority the packet is classified as high priority, else the packet is classified as low priority.

This value can be changed from the bridge window and in the example below the user priority threshold is set to 4:

Default value is 4.

14.3.4 Device settings



14.3.4.1 Alarms

Alarm reporting

Enable/disable. Please see “Device Alarm Enabling” on page 352.

Alarm reporting PDH

Please see “Suppress Specific Alarms” on page 353.

LEDs
See “LEDs and alarm output” on page 332.

Logs
See “Logs (alarm logs, performance data logs)” on page 332

Physical inventory
See “” on page 330.

Restart
See “” on page 331.

Synchronization

AXX10/11 synchronization is fixed to STM-1 agg. The S1 byte is used proprietary, that is: Downwards, the S1 byte is used for RTC synchronization of all connected AXX10/11 devices (w.r.t. retrieval of alarms and performance data). Upwards, the S1 byte is used for immediate failure conditions related to the AXX10/11 (as for instance "AXX10/11 dying").

14.3.5 LAN Settings

The bridge in AXX10/11 consists of 4 LAN ports. The LAN ports physical interfaces support 10Base-T, 100Base-T or auto negotiation. If auto negotiation is disabled, DuplexAdminMode (half/full) and SpeedAdminMode (10M/100M) must be programmed.

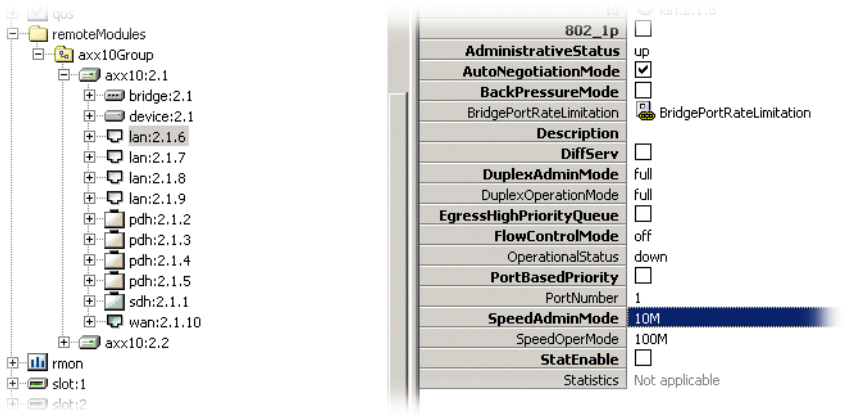
The switch conforms to auto negotiation protocol as described by 802.3 committee. Auto negotiation allows UTP (Unshielded Twisted Pair) link partners to select the best common mode of operation. In auto negotiation, link partners advertise capabilities across the link to each other. If auto negotiation is not supported or link partner is forced to bypass auto negotiation, then the mode is set by observing the signal at the receiver. This is known as parallel mode because while the transmitter is sending auto negotiation advertisements, the receiver is listening for advertisements or a fixed signal protocol.

Link parameters are managed from the Management Tree and in the example below, LAN port 6 is forced to 10Mbit/sec half duplex. Actual duplex and speed mode are shown in DuplexOperationMode and SpeedOperMode fields in the same window.

Default value is auto negotiation enabled.

For configuration of LAN ports see “AXX 9200 EDGE - LAN port attributes” on page 402.

Physical interface management



Administrative status

All ports can be taken out of service by changing AdministrativeStatus (default up) to down in LAN management. The actual status of the link(s) are shown as OperationalStatus in the same window:

Flow control

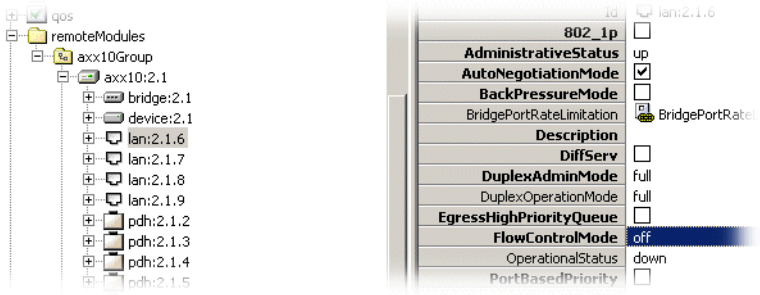
The AXX10/11 supports standard 802.3x flow control frames on both transmit and receive sides. The flow control is based on availability of the system resources, including available buffers, available transmit queues and available receive queues.

The switch will flow control a port, which just received a packet, if the destination port resource is being used up and will issue a flow control frame (XOFF), containing the maximum pause time defined in IEEE standard 802.3x. Once the resource is freed up, the switch will send out the other flow control frame (XON) with zero pause time to turn off the flow control (turn on transmission to the port).

A hysteresis feature is provided to prevent the flow control mechanism from being activated and deactivated too many times. Flow control can be set for the WAN port and all LAN ports if the actual ports are running in duplex mode.

Default value for flow control is off.

Management of this feature is done from LAN management:



Backpressure

A half duplex backpressure option (Note: not in 802.3 standards) is also provided and can be set individually for all the LAN ports. If backpressure is required, the switch will send preambles to defer the other stations' transmission (carrier sense deference).

To avoid jabber and excessive deference defined in 802.3 standard, after a certain time it will discontinue the carrier sense but it will raise the carrier sense quickly. This short silent time (no carrier sense) is to prevent other stations from sending out packets and keeps other stations in carrier sense deferred state.

If a port has packets to send during a backpressure situation, the carrier sense type backpressure will be interrupted and those packets will be transmitted instead. If there are no more packets to send, carrier sense type backpressure will be active again until switch resources free up.

If a collision occurs, the binary exponential back-off algorithm is skipped and carrier sense is generated immediately, reducing the chance of further colliding and maintaining carrier sense to prevent reception of packets.

Default value for backpressure is off.

Management of backpressure is done from LAN management:

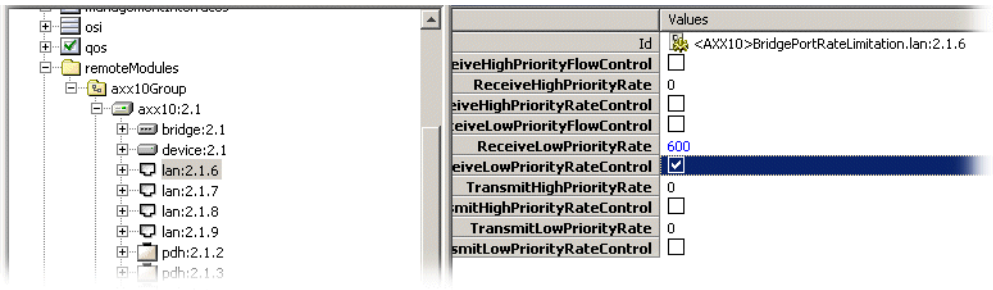
Rate Limit Support

(BridgePortRateLimitation)

The switch supports hardware rate limiting on "receive" and "transmit" independently and on a per port basis. It also supports rate limiting in a priority or non-priority environment. The rate limit starts from 0 kbps and goes up to the line rate in steps of 32 kbps. The rate limiting mechanism uses one second as an interval. At the beginning of each interval, the counter is cleared to zero, and the rate limit mechanism starts to count the number of bytes during this interval. For receive, if the number of bytes exceeds the programmed limit, the switch will stop receiving packets on the port until the "one second" interval expires. There is an option provided for flow control to prevent packet loss. If the rate limit is programmed greater than or equal to 128kbps and the byte counter is 8Kbytes below the limit, flow control is triggered. If the rate limit is programmed lower than 128kbps and the byte counter is 2Kbytes below the limit, flow control will be triggered.

For transmit, if the number of bytes exceeds the programmed limit, the switch will stop transmitting packets on the port until the "one second" interval expires. If priority is enabled, the switch can support different rate controls for both high priority and low priority packets.

This feature is managed from the LAN BridgePortRateLimitation window. In the example 9.2Mbit/sec (600x32Kbit/sec) receiving rate limitation with flow control is activated:

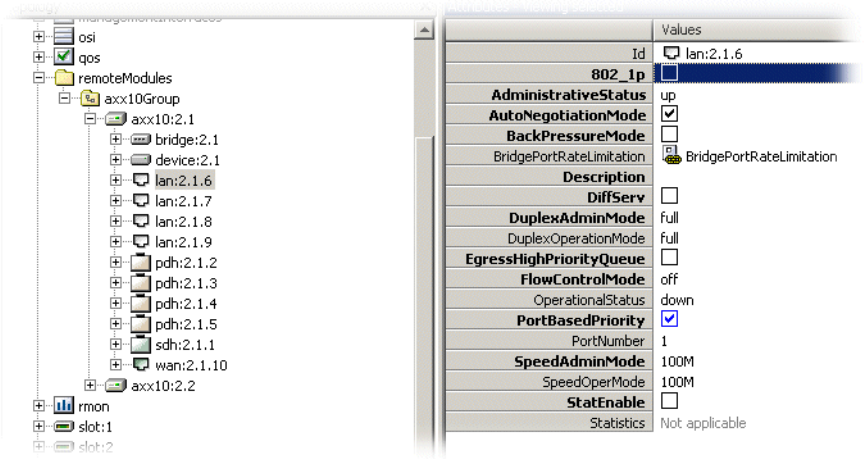


Default value is no rate limitation.

Egress packets prioritisation

When this feature is enabled the port output queue is split into high and low priority. Outgoing packets are sent according to PriorityScheme setting. If EgressHighPriorityQueue is disabled, there is no priority differentiation even though packets are classified into high or low priority. Management of this feature is done from LAN management:

Default value is disabled.



PortBasedPriority

If this feature is enabled ingress packets on the port will be classified as high priority if Diffserv or 802_1p classification is not enabled or fails to classify.

NOTE! "Diffserv", "802.1p" and port priority can be enabled at the same time. The result of 802.1p and DSCP overwrites the port priority.

Management of this feature is done from LAN management:

Default value: enabled.

802_1p

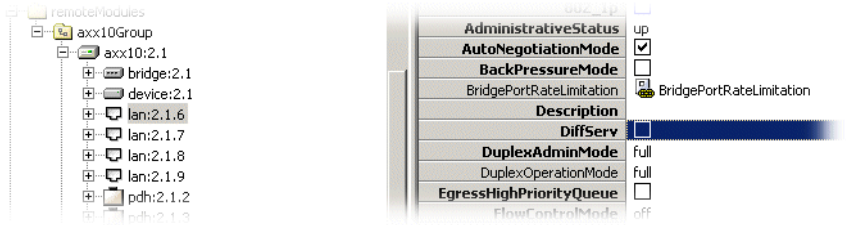
If this feature is enabled, 802.1p priority classification becomes active for ingress packets on the specified port. Management of this feature from LAN management:

Default value: disabled.

DiffServ

If this feature is enabled Diffserv priority classification for ingress packets on the port is activated. All 64 TOS bits are programmed

globally in the switch and Diffserv is only disabled/enabled on a port. Management of this feature is done from LAN management:



Default value: disabled.

14.3.6 PDH port settings

1. Select an AXX10/11 managed object in the Management Tree on the desktop.

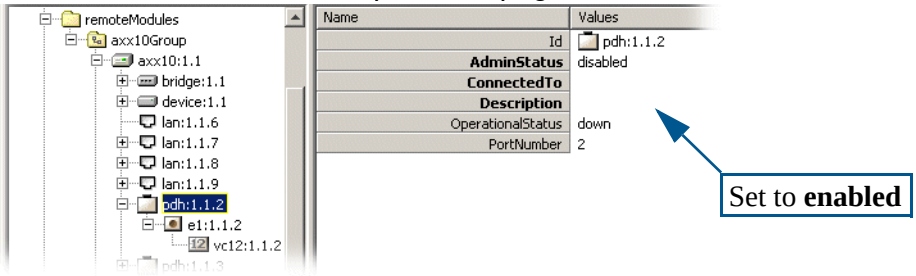
The system presents the containing managed objects on the AXX10/11.

2. Select one of the PDH ports.

The system presents the attributes for the PDH port as defined in the information model. Read and write accesses are defined in the information model.

NOTE! CBKLM on the E1 ports are fixed on AXX10/11, and should be remembered in order to be matched in cross connection or termination point in the NE.
I.e. the VC-12 reference for the E1 port will be “entering” the STM-1 port on the NE.

Please see “PDH ports” on page 395



G.826 data

Select an AXX10/11 managed object in the Management Tree on the desktop. The system presents the containing managed objects on the AXX10/11.

Select the SDH port or related contained managed objects.

These objects are:

- RS near end
- MS near end and far end
- VC-4 near end and far end
- VC-12 near end and far end

With near end and far end data for all but the RS managed object.The managed objects have PM attributes as defined in the information model.

Available time periods are

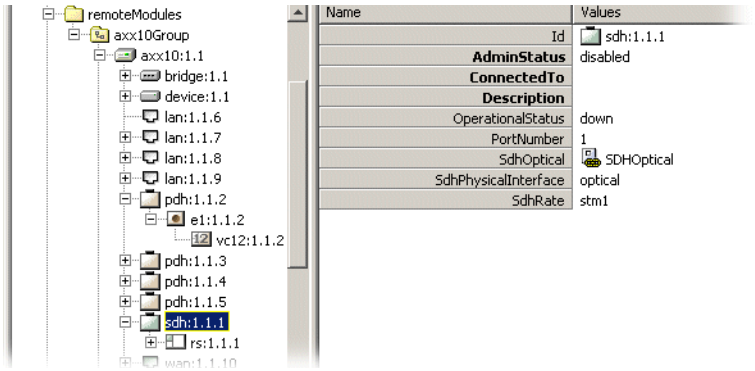
- 15 minutes
- 24 hours

The system presents current data and historical data. The number of historical stored periods are:

- 16x15 minutes
- 1x24 hours

14.3.7 SDH settings

See “Configuring SDH port structure (channelization)” on page 385



The WAN traffic is mapped into a number of VC-12 containers in a round-robin fashion with an inverse multiplexer function. The IP traffic is mapped into 1 to 50 VC-12 containers.

The AXX10/11 only have one WAN channel. The total bandwidth for one WAN channel cannot be greater than 100 Mbit/s or 47xVC-12 containers.

The mapping between the tributary interfaces and the WAN port is fixed:

Port	**KLM**
WAN	1.1.1 - 3.3.2
PDH-1	3.3.3
PDH-2	3.4.1
PDH-3	3.4.2
PDH-4	3.4.3

Table 26 AXX10/11 fixed VC-12 mapping

14.3.8 WAN Settings

This paragraph briefly describes WAN settings and how to enable Ethernet WAN capacity for AXX10/11.

14.3.8.1 WAN ports

Specific for the WAN port is that the bandwidth can be managed in steps of 2.16Mbits/sec. A bandwidth of 2.16Mbits/sec corresponds to the transmission rate of a VC12, and the numbers of VC12s connected are between 0 and 50. To ensure 100Mbits/sec Ethernet traffic is passing the WAN port, you set the number of VC12'S to 50. Default value for WAN bandwidth is 50 channels.

OperationalCapacity is a read- only attribute and shows the value of the actual bandwidth. Manage this setting as shown for **AdministrativeCapacity** in Figure 192

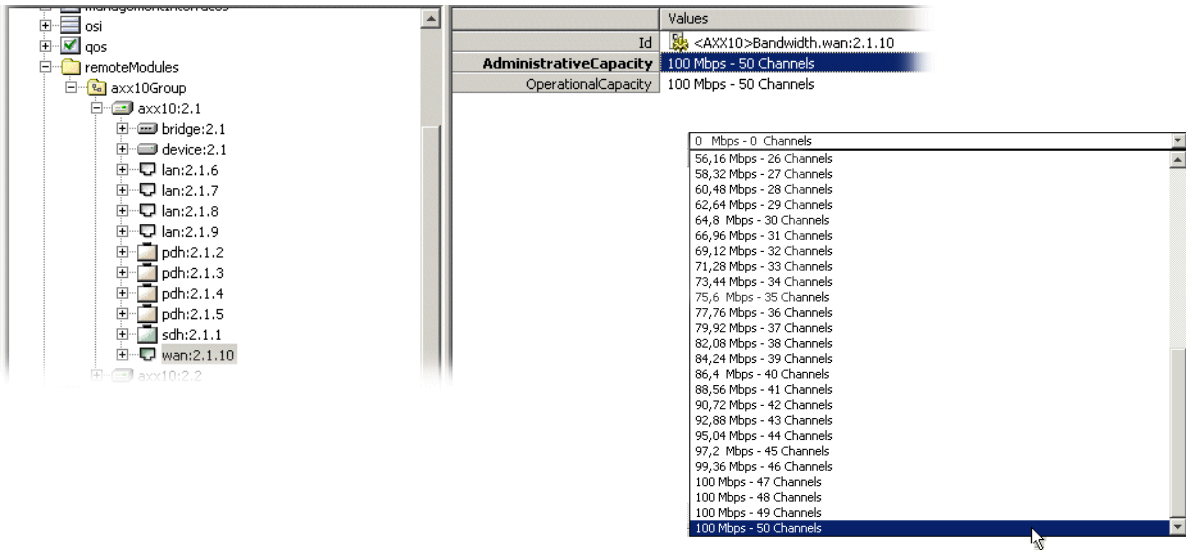


Figure 192 AXX10/11- capacity management of WAN- traffic

READ MORE: “WAN ports” on page 406.

14.3.8.2 Ethernet to/ through SDH for AXX10/11

VC-12 references for the Ethernet WAN-port in AXX10/11 have fixed references for the VC-12s starting at 1.1.1, as for the NE.

1. Double-click the targeted **WAN-port** in Management Tree.
   The view expands to all VC-12 references relevant to be used for the port.

2. Select the desirable amount of **Bandwidth**.
   (sufficient since AXX10/11 is a terminal mux).

14.3.8.3 Terminating WAN- traffic from AXX10/11 to the NE

AXX10/11 LAN-ports are provided with the VLANs from the NE or. If you want to terminate the WAN traffic from the AXX10/11 in a WAN port in the NE, use the following procedure:

1. Select the desired **Ethernet bandwidth in AXX10/11**, see Figure 192

2. Set the same amount of **Ethernet bandwidth** on an available WAN-port in the **NE**.

3. **Structure the SDH-port** (TU12 level) **on the NE** interfacing the AXX10/11, see “Configuring SDH port structure (channelization)” on page 385.

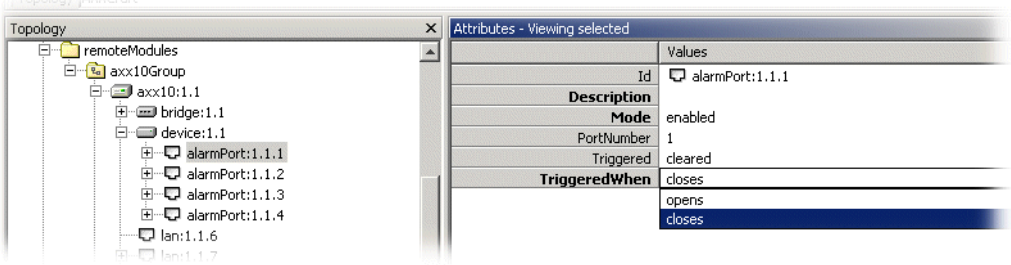
4. Open **Cross Connection Manager** from Equipment menu.

5. Set up cross-connection between the references from the SDH-port interfacing AXX10/11 with the TU12 references from the WAN-port in the NE.

14.3.9 Alarm port settings

1. Select an AXX10/11 managed object in the Management Tree on the desktop.

2. Select one of the Alarm ports.



READ MORE: “Alarm Ports” on page 334

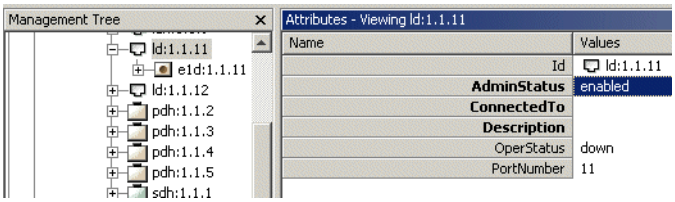
14.3.10 Legacy data - e1d ports (AXX11 only)

14.3.10.1 Enable the e1d port

The AXX11 has two e1d ports to transport V.35, V.36 or X.21 data.

1. Select the e1d port you want to use.

2. Set **AdminStatus** to enabled.



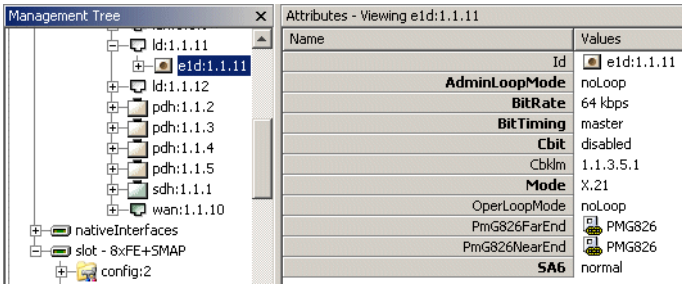
3. Fill in information:

ConnectedTo	Descriptive text string
Description	Descriptive text string

4. Click Save to store the settings.

14.3.10.2 e1d port settings

Expand the object to see the port settings, editable parameters are



bold:

Overview of the settings:

AdminLoopMode	NoLoop, ll2 or ll3
BitRate	Select desired bit rate
BitTiming	Select Master or slave
Cbit	Enable or disable
Cbklm	Fixed - Note value for x-connection or termination on NE
Mode	Select to transport V.35, V.36 or X.21 data
OperLoopMode	Showing active mode
PmG826NearEnd	Link to PM Near End settings

PmG826FarEnd	Link to PM Far End settings
SA6	Select Normal or Inverted signal