Nokia Siemens Networks

SURPASS hiX5750 R2.0

Installation and Test Manual

GPON OLT

The information in this document is subject to change without notice and describes only the product defined in the introduction of this documentation. This documentation is intended for the use of Nokia Siemens Networks customers only for the purposes of the agreement under which the document is submitted, and no part of it may be used, reproduced, modified or transmitted in any form or means without the prior written permission of Nokia Siemens Networks. The documentation has been prepared to be used by professional and properly trained personnel, and the customer assumes full responsibility when using it. Nokia Siemens Networks welcomes customer comments as part of the process of continuous development and improvement of the documentation.

The information or statements given in this documentation concerning the suitability, capacity, or performance of the mentioned hardware or software products are given "as is" and all liability arising in connection with such hardware or software products shall be defined conclusively and finally in a separate agreement between Nokia Siemens Networks and the customer. However, Nokia Siemens Networks has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. Nokia Siemens Networks will, if deemed necessary by Nokia Siemens Networks, explain issues which may not be covered by the document.

Nokia Siemens Networks will correct errors in this documentation as soon as possible. IN NO EVENT WILL NOKIA SIEMENS NETWORKS BE LIABLE FOR ERRORS IN THIS DOCUMENTATION OR FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA,THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT.

⚠ Important Notice on Product Safety

Elevated voltages are inevitably present at specific points in this electrical equipment. Some of the parts may also have elevated operating temperatures.

Non-observance of these conditions and the safety instructions can result in personal injury or in property damage.

Therefore, only trained and qualified personnel may install and maintain the system.

The system complies with the standard EN 60950 / IEC 60950. All equipment connected has to comply with the applicable safety standards.

The same text in German:

Wichtiger Hinweis zur Produktsicherheit

In elektrischen Anlagen stehen zwangsläufig bestimmte Teile der Geräte unter Spannung. Einige Teile können auch eine hohe Betriebstemperatur aufweisen.

Eine Nichtbeachtung dieser Situation und der Warnungshinweise kann zu Körperverletzungen und Sachschäden führen.

Deshalb wird vorausgesetzt, dass nur geschultes und qualifiziertes Personal die Anlagen installiert und wartet.

Das System entspricht den Anforderungen der EN 60950 / IEC 60950. Angeschlossene Geräte müssen die zutreffenden Sicherheitsbestimmungen erfüllen.

Table of Contents

This document has 150 pages.

List of Figures

List of Tables

Change History

4. Update (12.12.2008)

Presetting the hiX 5750 with CLI (4)

– Chapter changed

New Network Element (5)

– Automatic S-APS download added
– FTP configuration changed

ONT and MDU (7)

– ONT types added

Bridges (14)

– Enhanced tagging added
– Outer tag protocol ID of IU added

Security Features (22)

– IP anti-spoofing changed

Database Backup (28)

– Auto-backup procedure changed

3. Update (10.07.2008)

2. Update (18.04.2008)

1. Update (31.01.2008)

Initial release (20.11.2007)

1 Introduction

1.1 Scope of the ITMN

The Installation and Test Manual (ITMN) explains the commissioning procedures for the hiX 5750 R2.0 network element (NE).

1.2 Error Reports Concerning the Manual

In case of incorrect or unclear instructions of the ITMN, please inform the service-support team. Write a detail document error report (e.g. using “Helpdesk”).

1.3 Dealing with Defective Modules

If a module is defective, it should be carefully repacked and returned to the repair center along with the correct documentation.
For details, please contact the repair-service.

1.4 Procedure in the Event of Faults

Faults occurring during on-line operation should be identified and rectified in accordance with the instructions given in the “Branch to Maintenance” tool, see also the Maintenance Manual (MMN).

If there is no possibility to eliminate the fault, an error report is to be created in the “Helpdesk” including the following detailed information:

- Description of the test steps attempted
- Detailed list of the preceding operating and configuration actions at hiX 5750 and at other components in the network
- Description of the system responses
- Description of any system activities took place at the same time, such as work of other testers while hardware and software changes have been made.

1.5 Usage Hints

1. All information and values that are displayed in screenshots are only examples. Please pay attention always to the project-specific planning documentation for the commissioning of the hiX 5750 R2.0.
2. In the following description there are a few simplifications:
   - The hiX 5750 R2.0 can be provided with central unit **CXU**_F4 or CXU_VR. Both types require the same commissioning and configuration procedures. Therefore in the descriptions the abbreviation CXU represents both CXU_F4 and CXU_VR.
   - Subsequently, the abbreviation **EM** stands for the EM PX R2.0. That applies also to **LCT**.
   - There are no significant differences between the two standards **ETSI** and **ANSI** regarding the configuration of **OLT** modules. Therefore, the descriptions and figures base on ETSI standard. If there are differences, they will be described.
   - All figures are given only as examples and could differ in details from the current EM version.

- Changeable slot and port numbers of SNMP nodes (e.g. “GPON Port#1”, “IU_GPON:2512:E#101”) will not be specified in the navigation sequence. For example, “GPON Port#” could stand for “GPON Port#1”, “GPON Port#2”, etc.

1.6 Typographic Conventions

The following notations are used in this manual:

Representation	Meaning
`Courier`	Inputs and outputs, CLI commands Example: Enter `LOCAL` as the server name
<*Italic*>	Variables Example: *<ftp server>*
Bold	Special emphasis Example: Do **not** delete this name.
key	Keys and Key combinations that are to be pressed Example: Ctrl + C
“ ⇨ ”	Menu sequences Example: “File ⇨ Exit”
i	Additional Information
!	Warnings at critical points of the processing sequence

Table 1 Typographic Conventions

1.7 Protective Measures

1.7.1 General Notes

This Section contains requirements with regard to protection of people, equipment and environment.

All assembly, installation, operation and repair work may only be undertaken by service personnel.

In the event of any injury (e.g. burns and acid burns) being sustained, seek medical help immediately. Generally, to avoid danger, the operator is instructed to read the designated manual before beginning e.g. a maintenance task.

! The system can have several power supplies. Note that to switch off the power supply completely, you also have to switch off the redundant power supply. Switch off all concerned devices!

Please pay attention also to the high leakage current.

A ground connection is essential before connecting the system to the telecommunication network.

This section includes the following topics:

1.7.2 Protection Against Excessive Contact Voltage

When dealing with the power supply, observe the safety measures described in the specifications of the European Norm EN 50110, Part 1 and Part 2 (operation of electrical installations) and the valid applicable national standards as VDE 0105 (operation of high-voltage equipment) Part 1, Section 9.3 (safety measures to be carried out) at all times. Be sure to follow local national regulations regarding the handling of high-voltage equipment.

Figure 1 shows the label on the subrack with information on the subrack power supply (limits for battery voltage and load current). ** Numerical values for load current. Check the power rating label for the actual value.

In ANSI applications only 48 V is permitted!

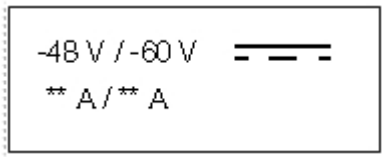

Figure 1 Power Rating Label

Figure 2 shows the label on the front side of the subrack with information that a high leakage current can occur if the shelf is not grounded.

Achtung	Warning
HOHER BERÜHRUNGSSTROM Vor dem Anschluss an den Versorgungsstromkreis oder an das Telekommunikationsnetz unbedingt Erdverbindung herstellen	HIGH LEAKAGE CURRENT Earth connection essential before connecting supply or making telecommunication network connections

Figure 2 High Leakage Current

1.7.3 Protection Against Escaping Laser Light

In order to avoid health risks, take care to ensure that any laser light escaping is not directed towards the eyes. Plug-in units equipped with laser light units may carry the laser symbol, but it is not required, see Figure 3. For operation in closed systems the laser light units comply with Laser class 1. Such units can be identified by an adhesive label as well as by a warning label, see Figure 4.

Figure 3 Warning Label According to IEC 60825/EN 60825

Never look directly into the beam, not even with optical instruments.

Figure 4 Warning Label for Class 1 Laser Equipment

1.7.4 Protection Against Fire in Racks or Housings

If shelves are used in housing, the shelves must comply with the conditions for fire protection housing according to DIN EN 60950-1.

To comply with fire protection standards as defined in DIN EN 60950-1, a protective plate (C42165-A320-C684) must be fitted into the floor of ETSI and 19-inch standard racks. The rack must also meet the requirements of fire-resistant housing as defined in DIN EN 60950-1.

1.7.5 Protection Against Hot Surfaces

If temperatures higher than 70°C can be present on components inside the transmission equipment, following labels are attached to this equipment, see Figure 5 and Figure 6.

Figure 5 Symbol Label for Hot Surfaces

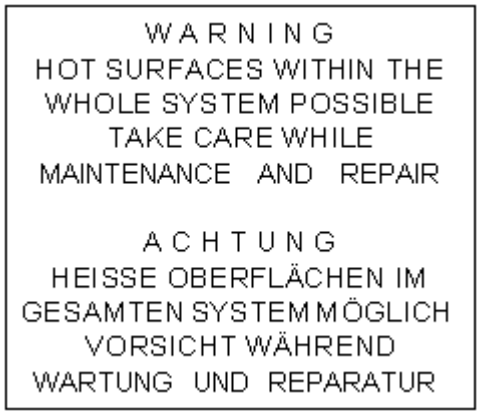

Figure 6 Text on Label for Hot Surfaces

1.7.6 Components Subject to Electrostatic Discharge

Figure 7 ESD Symbol

Plug-in units bearing the symbol shown in Figure 7, are equipped with components subject to electrostatic discharge (ESD). Adhere to the relevant safety provisions.

When packing, unpacking, touching, pulling out, or plugging in plug-in units bearing the ESD symbol, it is essential to wear a grounding bracelet. This ensures that the plug-in units are not subject to electrostatic discharge.

Under no circumstances should you touch the printed conductors or components of plug-in units. Take hold of plug-in units by the edge only.

Once removed, place the plug-in units in the conductive plastic sleeves intended for them. Keep or dispatch them in the special boxes or transport cases bearing the ESD symbol.

Treat defective plug-in units with the same degree of care as new ones in order to avoid further damage.

Plug-in units in a closed and intact housing are protected in any case.

European Norm EN 50082-1 provides information on the proper handling of components which are subject to electrostatic discharge.

1.7.7 Handling Modules (General)

To pull out or plug in plug-in units, use the front-mounted levers.

In shelters fans are used for cooling. To indicate positions where there is a danger of being caught up in a fan, following label is attached, see Figure 8.

Figure 8 Prohibition Label According to DIN 4844-2

When working with modules (plug-in units, subracks and shelters) the following points should be noted:

- Existing ventilation equipment must not be changed. To ensure a sufficient air circulation, the flow of air must not be obstructed.

  Beware of rotating parts.

- All slide-in units can be removed or inserted with the power still applied. To remove and insert the units you should use the two locking screws fitted to the front of the unit. A type label is fixed on the handhold above the locking screw on the bottom of the board providing information on the hardware and software version of the unit.
- A label with the words “HOT AREA” is fixed to hot surfaces. This indicates severe danger of injury.
- Shelters with a front door may only be operated when this door is closed.

  There is a danger of injury if the door is left open.

  You should therefore remove the front door before doing the necessary work and replace it once you have finished your work.
- When inserting and removing shelves and when transporting them, take their weight into consideration.
- Cables may never be disconnected by pulling on the cable. Disconnection/connection may only be undertaken by pushing in/pulling out the connector involved.

1.7.8 Handling Optical Fiber Connectors and Cables

Optical connectors are precision-made components and must be handled accordingly. To ensure faultless functioning, the following points must be observed:

- Install protective caps on unplugged optical connectors under all circumstances to protect against physical damage and dirt.
- Before making connections, use isopropyl alcohol and non-fibrous cellulose to clean the faces of the connectors.
- Avoid impact stresses when handling connectors.
  Physical damage to the faces of optical connections impair transmission quality (higher attenuation).
- Avoid a bend radius less than 30 mm for fiber optic links.
- Mechanical damage to the surfaces of optical connectors impairs transmission quality by higher attenuation.
  - For this reason, do not expose the connectors to impact and tensile load.
  - Once the protective dust caps have been removed, you must check the surfaces of the optical fiber connectors to ensure that they are clean, and clean them if necessary.
    For cleaning, the C42334-A380-A926 optical fiber cleaning tool or a clean, lint-free cellulose cloth or a chamois leather is suitable. Isopropyl alcohol can be used as a cleaning fluid.

1.7.9 Virus Protection

To prevent a virus infection you may not use any software other than that is released for the Operating System (OS based on Basis AccessIntegrator), Local Craft Terminal LCT) and transmission system.

Even when exchanging data via a network or external data media (e.g. floppy disks) there is a possibility of infecting your system with a virus. The occurrence of a virus in your system may lead to a loss of data and breakdown of functionality.

The operator is responsible for protecting against viruses and for carrying out repair procedures when the system is infected.

You have to do the following:

- You have to check every data medium (used data media as well as new ones) for viruses before reading data from it.
- You must ensure that an up-to-date virus scanning program is always available. This program has to be supplied with regular updates by a certified software provider.
- It is recommended that you make periodic checks for viruses in your OS.
- It is recommended to integrate the virus scanning program into the start-up sequence on the LCT.

1.7.10 RoHS Requirements

Nokia Siemens Networks considers the protection of the environment and the preservation of natural resources as a major duty and thus undertakes great efforts to design its

products to be environmental friendly. Therefore, as of July 1st, 2006, all contract products of Nokia Siemens Networks

- to which the RoHS (Restriction of Hazardous Substances) directive applies to
- and which are put on the market within the countries where the RoHS requirements are transposed into national law

are in compliance with the requirements of the RoHS.

Nokia Siemens Networks reserves the right to apply the exemptions to the RoHS requirements as set out in the Annex to the RoHS directive, in particular lead in solders for network infrastructure equipment for switching, signaling, transmission as well as network management for telecommunication.

1.7.11 Declaration of CE Conformity

The CE (Conformité Européenne) Declaration of Conformity for the product is fulfilled only if all construction and cabling is undertaken in accordance with the manual and the documentation listed therein, e.g. installation instructions, cabling lists, etc.

Deviations from the specifications or unstipulated changes during construction, e.g. the use of cable types with lower shielding values is a violation of the CE requirements. In such cases, the conformity declaration is invalidated and the manufacturer is refused from responsibility. All liability passes immediately to those persons undertaking any unauthorized deviations.

1.7.12 WEEE Requirements

Nokia Siemens Networks considers the protection of the environment and the preservation of natural resources as a major duty.

This includes waste recovery with a view to reducing the quantity of waste for disposal and saving natural resources, in particular by treatment, recycling and recovering energy from waste electrical and electronic equipment (WEEE). Therefore Nokia Siemens Networks complies with its obligations as “producer” in terms of the WEEE directive for all its products

- to which the WEEE directive applies to
- and which are put on the market within the countries where the WEEE requirements are transposed into national law,

unless any deviant allocation of such obligations have been agreed between Nokia Siemens Network’s and its contractual partners. According to WEEE-requirements since August 13, 2005 such products are marked with the symbol of a crossed out

wheeled bin with bar, indicating separate collection for electrical and electronic equipment, as shown below.

1.8 GPL/LGPLWarranty and Liability Exclusion

This product contains both proprietary software and „Open Source Software". The Open Source Software is licensed to you at no charge under the GNU General Public License (GPL) and the GNU Lesser General Public License (LGPL). This Open Source Software was written by third parties and enjoys copyright protection. You are entitled to use this Open Source Software under the conditions set out in the GPL and LGPL licenses indicated above. In the event of conflicts between Nokia Siemens Networks license conditions and the GPL or LGPL license conditions, the GPL and LGPL conditions shall prevail with respect to the Open Source portions of the software.

The GPL can be found under the following URL: http://www.gnu.org/copyleft/gpl.html

The LGPL can be found under the following URL: http://www.gnu.org/copyleft/lgpl.html

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

The use of Open Source Software contained in this product in any manner other than the simple running of the program occurs at your own risk, that is, without any warranty claims against Nokia Siemens Network. For more information about the warranties provided by the authors of the Open Source Software contained in this product, please consult the GPL and LGPL.

You have no warranty claims against Nokia Siemens Networks when a defect in the product is or could have been caused by changes made by you in any part of the software or its configuration. In addition, you have no warranty claims against Nokia Siemens Networks when the Open Source Software infringes the intellectual property rights of a third party.

Nokia Siemens Networks provides no technical support for either the software or the Open Source Software contained therein if either has been changed.

2 General Procedure

The hiX 5750 R2.0 is to be commissioned with CLI (Command Line Interface) and **EM PX R2.0** (LCT, Local Craft Terminal) which are locally connected to the **TMN** interface (RJ45 connector) on the **CXU**. The EM PX R2.0 is part of the AccessIntegrator Ethernet (**ACI-E**).

2.1 Visual Inspection

Check the following points before commissioning:

1. All deliveries were supplied and the installation activities are completed
   - The delivery of hiX 5750 R2.0 hardware is all right.
   - The racks and shelves are assembled.
   - Using the part lists, check that all deliverable were supplied.
   - The power supply is connected and constantly available. The emergency power supply system is operational. The circuit breakers for the power supply must be in position 0/OFF during the visual inspection.
   - The cabling and positioning of the modules should be checked with the installation instructions.
   - Both rack internal and external cables were correctly routed and connected.
   - The racks, shelves and cables are labeled correctly.
   - Visual check of the complete installation (particularly the protection devices).
   - The system power supply is connected but is not switched on yet.
2. The hardware modules are in delivery condition
   - The hardware settings of the racks and modules must be checked.
   - The modules are equipped with the current firmware and correspond to the correct hardware version (compare for this the existing software and hardware with the release note of the current **SAPS** package). Note the **MAC** addresses.
3. The hardware of the **OS** meets the requirements, the software is present.
4. The required documentation is available on site.
5. The required tooling/test equipment is available.
6. The **EM** (**LCT**) is installed and ready for service.

2.2 Plan of Commissioning Activities

The following tasks must be performed during commissioning.

1. **Preparatory measures**
   - Visual inspection of the hiX 5750 R2.0
   - Switch the circuit breakers to 1/ON
2. **Configuring the FTP server**
   - Configuring the **FTP** server
   - Configuring the hiX 5750 R2.0 as user
3. **Pre-configuring the hiX 5750 R2.0 with CLI**
   - Connect the **PC** to the console interface on the **CXU**
   - Configuring the outband management interface
   - Configuring the inband management channel
   - Configuring the **SNMP** trap host
4. **Commissioning the hiX 5750 R2.0**.
   - Connect the PC to the **TMN** interface on the CXU
   - Start the EM (**LCT**)

- Carry out the procedures in Chapter 2.3 Sequence of Commissioning in the given sequence.

The commissioning contains the required instructions to take the network element hiX 5750 R2.0 in operation. Detailed information about the parameter settings are provided by a context-sensitive online help and in the element manager EM PX R2.0 documentation.

2.3 Sequence of Commissioning

Steps		Actions
1.	Insert and configure a new **NE**.	see Section 5.
2.	Create and configure the **OLT** cards (CXU and **IU**'s).	see Section 6.
3.	Create ONT and **MDU**.	see Section 7.
4.	Create and configure MDU boards (optional).	see Section 8.
5.	Configure subscriber ports physically (Ethernet, **POTS**, **CATV**).	see Section 9.
6.	Configure XDSL services (**VDSL** and **ADSL**).	see Section 10.
7.	Configure **VoIP** (H.248 and **SIP**).	see Section 11.
8.	Configure **TDM** services **E1**/**DS1**.	see Section 12.
9.	Set the **MAC** mode	see Section 13.
10.	Configure the bridges (VLAN switching, tagging mode, ports)	see Section 14.
11.	Configure **VLAN**s.	see Section 15.
12	Configure QoS Queuing and Scheduling	see Section 16.
13.	Configure bandwidth, overbooking, **DBA**.	see Section 17.
14.	Configure **DHCP** and **PPPoE**.	see Section 18.
15.	Configure **IGMP**.	see Section 19.
16.	Configure routing **RIP**, **BGP**, **IS**-IS.	see Section 20.
17.	Configure spanning tree (**STP**, **RSTP**, **MSTP**)	see Section 21.
18.	Configure security feature **AES** and **IP** anti-spoofing.	see Section 22.
19.	Enable **FEC** mechanism.	see Section 23.
20.	Configure **LAG**.	see Section 24.
21.	Create rules.	see Section 25.
22.	Unlock/lock ports	see Section 27.
23.	Database backup	see Section 28.

Table 2 Sequence for Commissioning the NE hiX 5750 R2.0

3 FTP Server

This chapter describes step-by-step how to install and configure a File Transfer Protocol (FTP) server for SAPS and . The **FTP** server for the hiX 5750 R2.0 can be installed on the **PC**/workstation used for the ACI-E element manager EM PX R2.0 (**LCT**) or run separately on a PC located in the same management network. At least one FTP server for system application program software (SAPS) and remote backup must be accessible in the management network. The hiX 5750 R2.0 was tested with FTP servers running on both **OS** Windows Server 2003 and Solaris 10.

3.1 Configuring a Windows FTP Server

Requirements

The following software requirements must be fulfilled:

- Windows Server 2003 (32 bit) with service pack 1
- Microsoft Internet Information Services (IIS) is installed
- FTP Service is installed
- “Active directory service” is configured
- Virus scanner available (optional)
- Configuration files for the hiX 5750 R2.0 are available
- Released SAPS (System Application Program Software).

The FTP service is not automatically installed during installation of Windows Server 2003.

Installation

1. Click “Start ⇨ Control Panel ⇨ Add or Remove Programs”.
2. Click “Add/Remove Windows Components” to display the “Components” list.
3. Click “Application Server ⇨ Details ⇨ Internet Information Services (IIS)” (but do not select or clear the check box), and then click “Details”.
4. Click to select the check boxes (if they are not already selected): “Common Files”, “File Transfer Protocol (FTP) Service”, and “Internet Information Services Manager”. Click the “OK” button and then click the “Next” button.
5. When you are prompted, insert the Windows Server 2003 CD-ROM into the CD-ROM drive or provide a path to the location of the files, and then click “OK”.
6. Click the “Finish” button to finish the installation.

Configuration

To transmit data between Windows Server 2003 and hiX 5750 R2.0 via FTP, a user with login and password for hiX 5750 R2.0 must be configured with the Windows user management system.

1. Click “Start ⇨ Programs ⇨ Administrative Tools ⇨ Active Directory Users and Computers ⇨ Users” to expand the folder containing current user objects.
   Click “Action ⇨ New ⇨ User” in the window menu to display the “New Object - User” dialog box.
2. Enter a “User logon name” at least and then click the “Next” button.

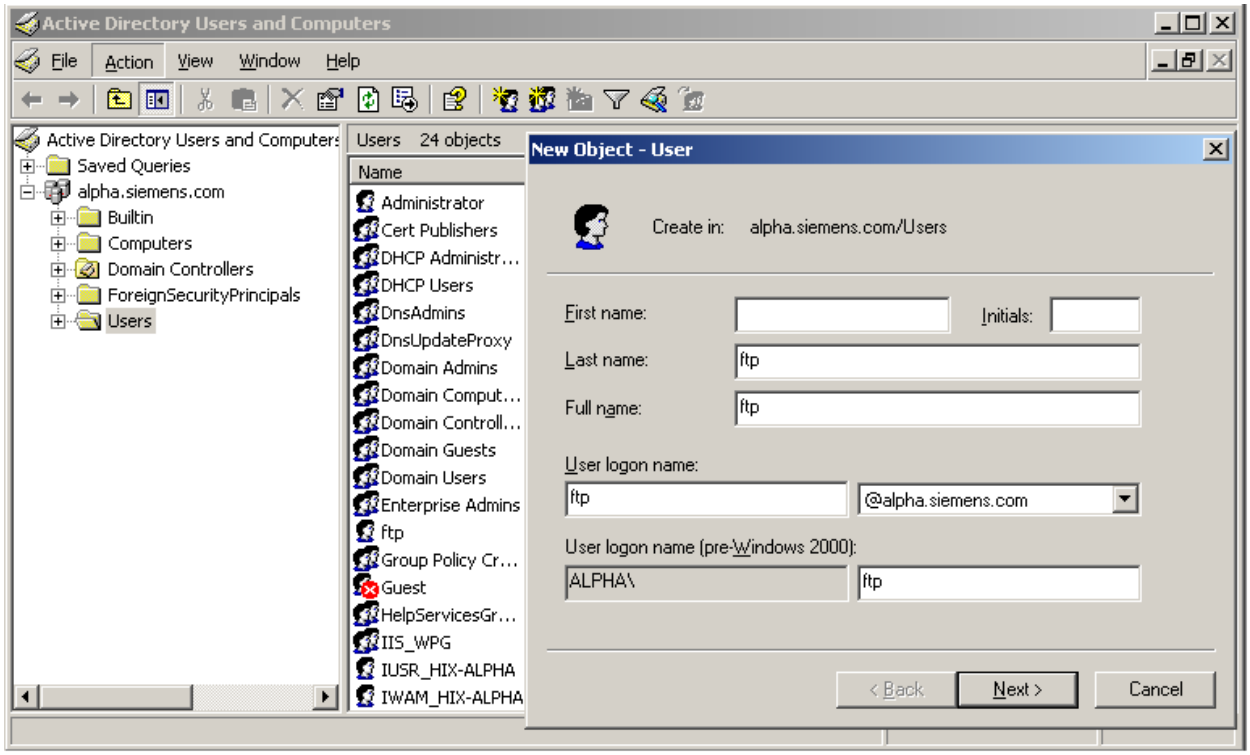

Figure 9 Defining a New User (Example)

3. Type the “Password” and retype it.
   Click to check mark the “Password never expires” box. Click to clear the other check marked boxes and then click the “Next” button.

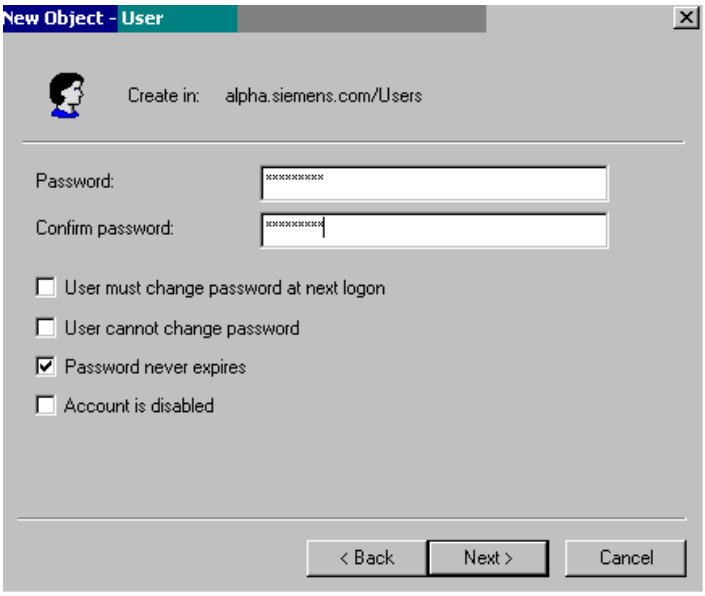

Figure 10 Defining the Password (Example)

4. Click the “Finnish” button to confirm the settings.

In order to give user locally logon rights following steps are required:

1. Click “Start ⇨ Programs ⇨ Administrative Tools ⇨ Domain Controller Security Policy” to display the “Default Domain Controller Security Settings” dialog box.

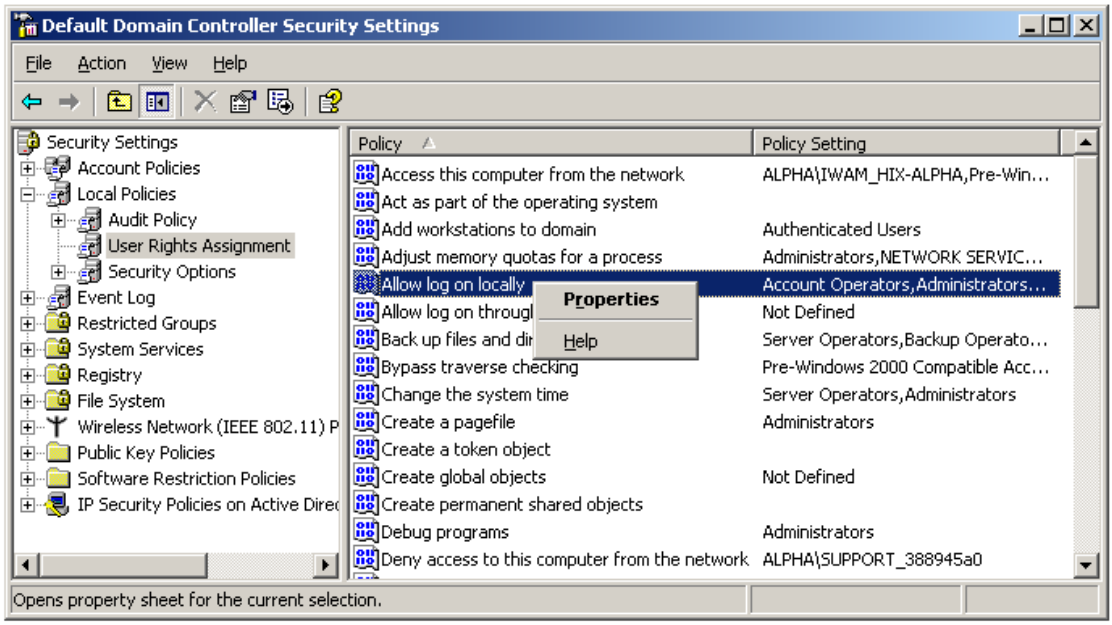

Figure 11 Assigning User Rights (Example)

In the console tree, click “User Rights Assignment” and then double-click “Allow log on locally” in the detail pane to change the user right.
Click the “Properties” command to display the “Security Policy Setting” dialog box.

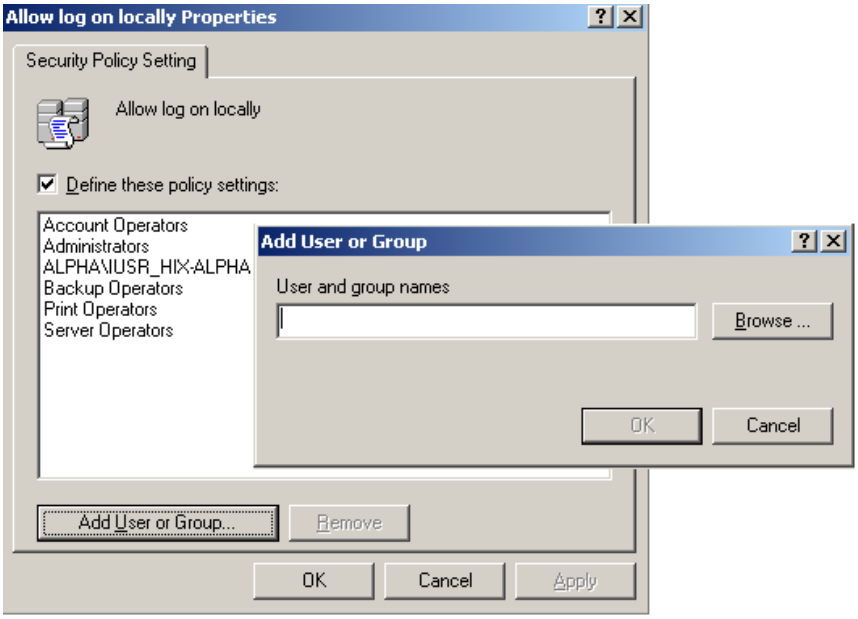

Figure 12 Dialog “Security Policy Setting” (Example)

2. Click the “Add User or Group...” button to display the “Add User or Group” search field.
3. Click the “Browse...” button to choose the created user (for example “ftp”) from the “Select Users or Groups” list. Then click “Add”.
4. Click the “OK” button to confirm.

1. Click “Start ⇨ Programs ⇨ Administrative Tools ⇨ Internet Services Manager” to display the “Internet Information Services” dialog.

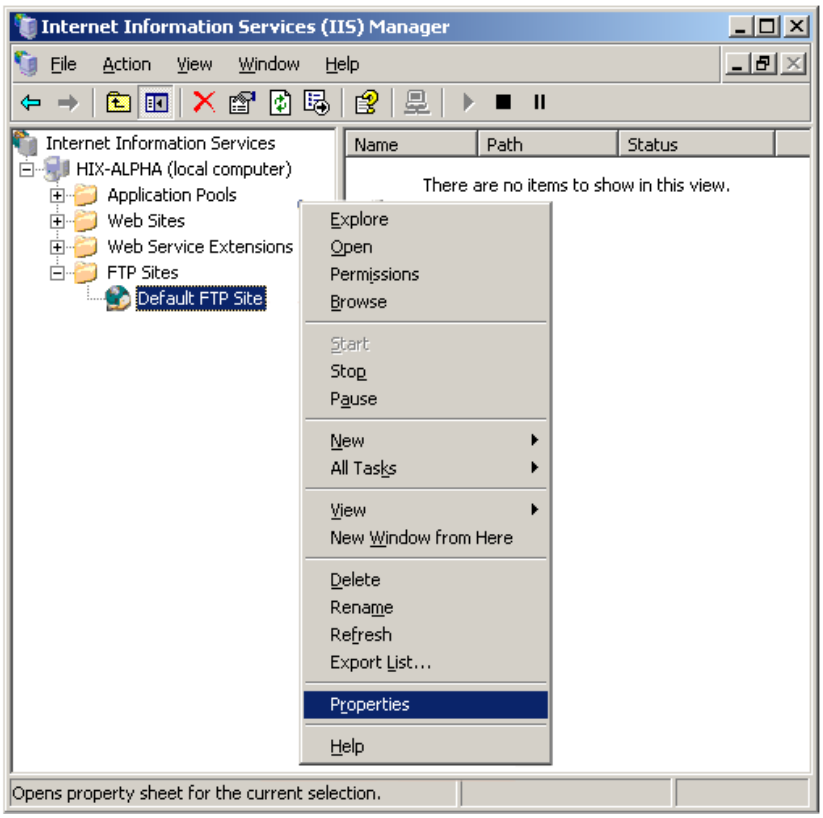

Figure 13 Dialog “Internet Information Services”

Click the “Default FTP Site” entry in the console tree and then click the “Properties” command to open the “Default FTP Site Properties” dialog.
Following properties must be set:

– On the “FTP Site” tab, enter the “IP Address” and click to select “Unlimited” in the “FTP site connections” section, see Figure 14.
  Click “OK” and then the “Apply” button to confirm the settings.

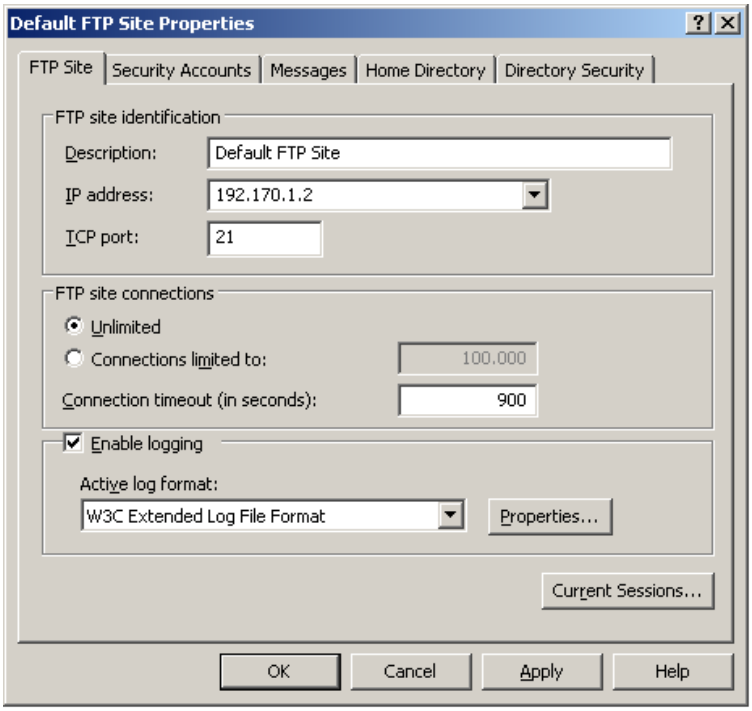

Figure 14 “FTP Site” Tab (Example)

– Click the “Home Directory” tab and enter the home directory into the “Local path” field (for example, drive c, e or d:\InetPub\ftproot), see Figure 15.
In order to write a backup file, the configured FTP user must be granted the write permissions on FTP server.
Click to check mark the boxes “Read” and “Write” (if they are not already selected).
Click “OK” and then the “Apply” button to confirm the settings.

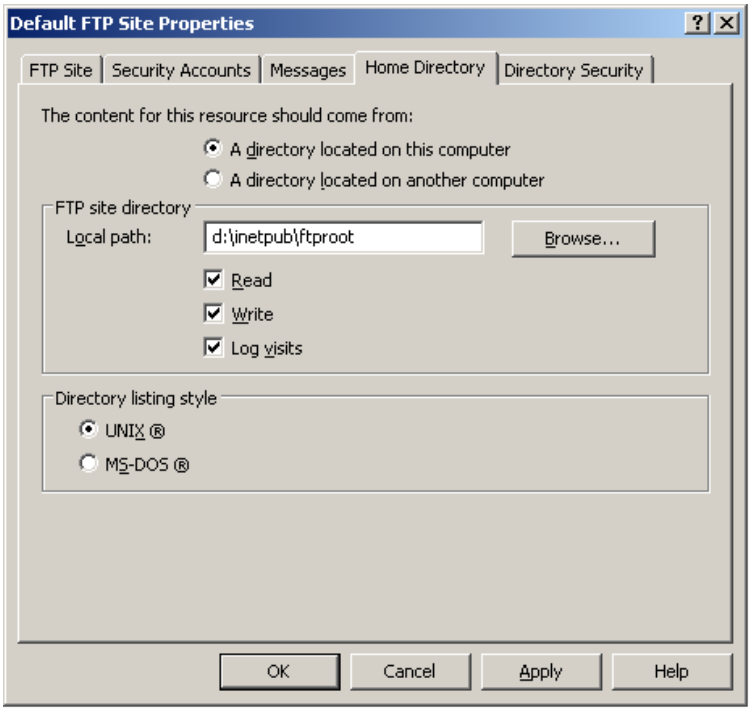

Figure 15 “Home Directory” Tab

2. After installation, the “ftproot” directory has to be configured for access via the network environment. To do this, the “ftproot” directory must be set on “shared” in the File Manager. Right-click “ftproot” in the Explorer, choose "Properties" from the context menu and then click the “Sharing” tab to display the “ftproot Properties” property panel.

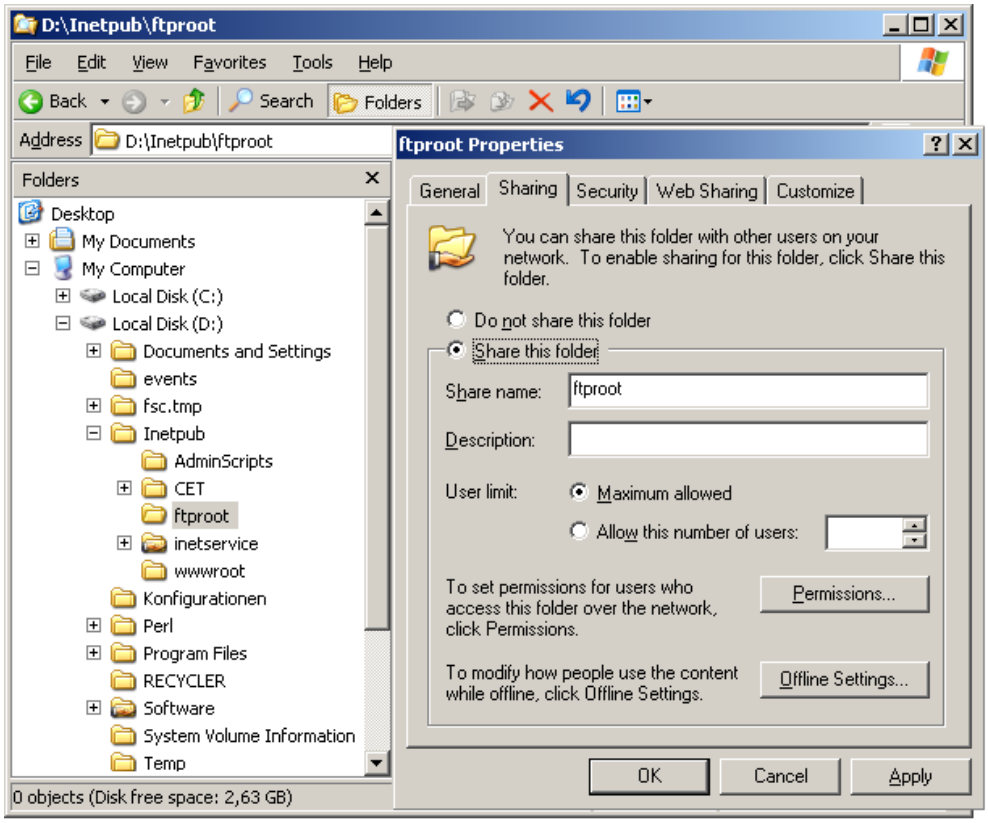

Figure 16 Change the Access to "ftproot"

3. Mark "Share this folder". Optionally, a different share name can be entered and the maximum number of allowed users can be set.
4. Click the “OK” button to confirm the settings.

3.2 Configuring a Solaris FTP Server

To establish a connection between Solaris clients and Solaris **FTP** server, the following steps are required:

1. Create a separate FTP-user on the Solaris machine that must be run the FTP server.
2. Create a directory for FTP server files. Give the FTP-user rights to transfer and change files for it.
3. Share this directory with “nfs share” command, for example:
   `share -F nfs -o rw -d` <*folder_name*> <*path_ftp_directory*>
   Store the share command in `/etc/dfs/dfstab` to undertake that after restart all will work.
4. Store at minimum one valid file in this directory.
5. Install and start FTP server on Solaris machine.

On a Solaris machine that will be run the ACI server:

Mount the FTP directory in “mounttab”:
`mount -F nfs` <*ftp server*>:<*mount point*>

After a restart, it is not necessary to repeat the command.

In order to configure the ACI Solaris client, following settings are necessary:

1. Folder “ftp” -> Section “FTP-folder”: write in the “mountpoint”.
2. In section “SAPS” write in the subfolder(s).

4 Presetting the hiX 5750 with CLI

4.1 Requirements

Be sure that the following checks have been finished successfully before power-on the hiX 5750 R2.0:

The boards are equipped correctly and all needed cable connections are plugged.
The voltage for the power feeding is in the allowed range.
The protective earth is connected as required.

- Connect the CXU's front access console interface (RJ45) via a straight serial V.24 connecting cable (see Figure 17) with e.g. PC running HyperTerminal. The required interface settings for the terminal program are:
  speed 38400 bit/s, 8 data bits, no parity, 1 stop bit, no flow control

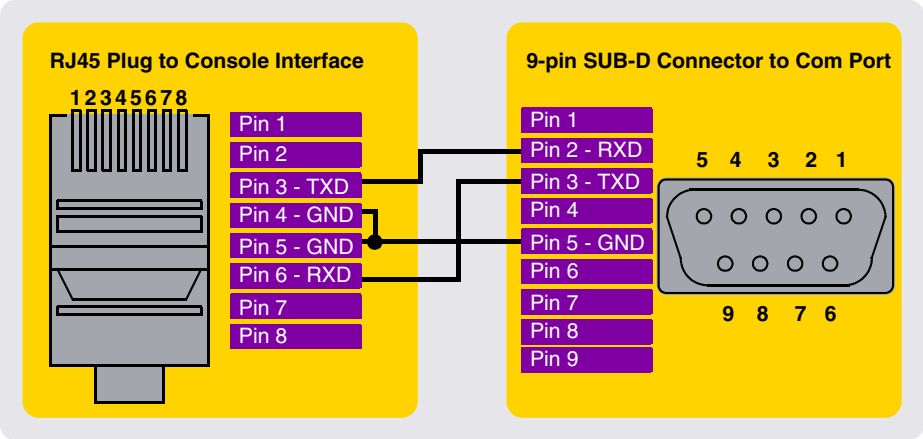

Figure 17 Console Cable for the Terminal Program

- The EM PX R2.0 (**LCT**) has been installed properly on the local workstation/PC.

4.2 Slot Numbering and Plug-in Units

The slot numbering in the G1100 shelf differs from the slot numbering in the Command Line Interface (CLI). Table 3 also contains the plug-in unit names used in the **NE**'s **OS** (mnemo code).

Slot Number on the Shelf		101 to 108	109	110	111 to 116
Slot Number in the ACI		101 to 108	109	110	111 to 116
Slot Number in the CLI		1 to 8	9	10	11 to 16
Plug-in Unit	Mnemo Code				
CXU_F4	M:CXUF4:1O:4E:E		x	x	
CXU_VR	M:CXUVR:1O:4E:E		x	x	

Table 3 G1100 Slot Numbering and Plug-in Units

Slot Number on the Shelf		101 to 108	109	110	111 to 116
Slot Number in the ACI		101 to 108	109	110	111 to 116
Slot Number in the CLI		1 to 8	9	10	11 to 16
Plug-in Unit	Mnemo Code				
IU_GPON2512:E (4-port GPON interface unit) with 8 E1 interfaces	M:IUGPON:2512:E	x			x
IU_GPON2512:L:E (4-port GPON interface unit without E1interfaces)	M:IUGPON:2512:L:E	x			x
IU_GPON2512:A (4-port GPON interface unit with 8 DS1 interfaces)	M:IUGPON:2512:A	x			x
IU_1x10G (interface unit with one interface for optical 10-Gbit/s Ethernet uplink)	M:IU10GE:1O:E	x			x
IU_10x1G (interface unit with 10 interfaces for optical 1-Gbit/s Ethernet uplink)	M:IU1GE:10O:E	x			x

Table 3 G1100 Slot Numbering and Plug-in Units (Cont.)

In case of an **OLT** equipped with two **CXU** boards, the following description refer to the active CXU plugged into slot #109 by default.

4.3 Configuring the Management Access

The **CXU** and the **IU_GPON** interface units are already pre-installed with software. The presetting procedure of the hiX 5750 R2.0 consists of the two parts:

- The outband management interface has to be configured in order to access the **NE** hiX 5750 R2.0 locally via **FE** interface on CXU by using the ACI-E EM PX R2.0 or **LCT**.
- An inband management channel has to be configured to access the NE hiX 5750 R2.0 from a remote place via Ethernet/IP network.

4.3.1 Outband Management Interface

1. When the NE is switched on, the CXU is starting up and the terminal program displays automatically the login prompt "`SWITCH login:`".
2. Execute the following commands after login with login-name **root** and password **siemens7** in order to configure the management interface and the default route:
   - `SWITCH> enable`
   - `SWITCH# configure terminal`
   - `SWITCH(config)# interface mgmt`
   - `SWITCH(config-if)# ip address` *<ip address of the management interface according to the project documentation>/<mask>*
   - `SWITCH(config-if)# no shutdown`
   - `SWITCH(config-if)# exit`
   - `SWITCH(config)# ip route default` *<default gateway ip address according to the project documentation>*
3. Configure the trap destination to be able to access the NE via **SNMP**:
   - `SWITCH(config)# snmp community ro public`
   - `SWITCH(config)# snmp community rw private`
   - `SWITCH(config)# snmp trap2-host` *<ip destination address for the trap-host>* `public`

4. After return from the **config** mode, the configuration must be stored in the persistent CXU memory:
   - `SWITCH(config)# exit`
   - `SWITCH# write memory`

   Wait for **OK** message!
5. Connect the workstation/PC running EM PX R2.0 (LCT) to the CXU's **FE** port. Local access to the NE using the EM PX R2.0 (LCT) should be possible.

4.3.2 Inband Management Channel

In order to configure the inband management interface, execute the following commands:

1. After login with login-name **root** and password **siemens7** enter:
   - `SWITCH> enable`
   - `SWITCH# configure terminal`
   - `SWITCH(config)# bridge`
2. A VLAN for inband communication has to be created and assigned to an uplink port. The **VLAN-ID** may be chosen from the range 1 to 4093; the port needs to be specified through the scheme: **CLI** slot number (see Table 3)/uplink port number from the range 1 to 5 (e.g. for CXU's first 1-**GE** port the sequence 9/2 has to be entered).
   - `SWITCH(bridge)# vlan create` *<vlan-id>*
   - `SWITCH(bridge)# vlan add` *<vlan-id>* *<port>* `tagged`
   - `SWITCH(bridge)# exit`
3. The next commands are used to define and configure the interface (e.g. br11) and the default route:
   - `SWITCH(config)# host-vlan` *<vlan-id>*
   - `SWITCH(config)# interface br`*<vlan-id>*
   - `SWITCH(config-if)# ip address` *<ip address of the management interface according to the project documentation>*/*<mask>*
   - `SWITCH(config-if)# no shutdown`
   - `SWITCH(config-if)# exit`
   - `SWITCH(config)# ip route` *<destination network>*/*<mask>* *<default gateway according to the project documentation>*
4. Configure the trap destination to be able to access the NE via **SNMP**:
   - `SWITCH(config)# snmp community ro public`
   - `SWITCH(config)# snmp community rw private`
   - `SWITCH(config)# snmp trap2-host` *<ip destination address for the trap-host>* `public`
5. The configuration must be stored in the persistent CXU memory:
   - `SWITCH(config)# exit`
   - `SWITCH# write memory`

   Wait for **OK** message!

5 New Network Element

Following steps are required to insert and configure a new **NE** hiX 5750 R2.0 in the **EM** PX:

1. Inserting a new NE hiX 5750
2. Configuring the FTP Server Access
3. Upgrading the S-APS
4. Synchronizing the Clock
5. Synchronizing Date and Time
6. Configuring the Alarm Severity Profiles
7. Setting the External Alarms and PON Alarm Thresholds
8. Saving the NE Configuration Data.

5.1 Inserting a new NE hiX 5750

1. Select “View ⇨ Network View” from the **EM** PX main menu to display the “**Network View**“ window.
2. Right-click the ”Root“ object and select the “Insert NE” command from the context menu to display the “**New NE**“ dialog page.

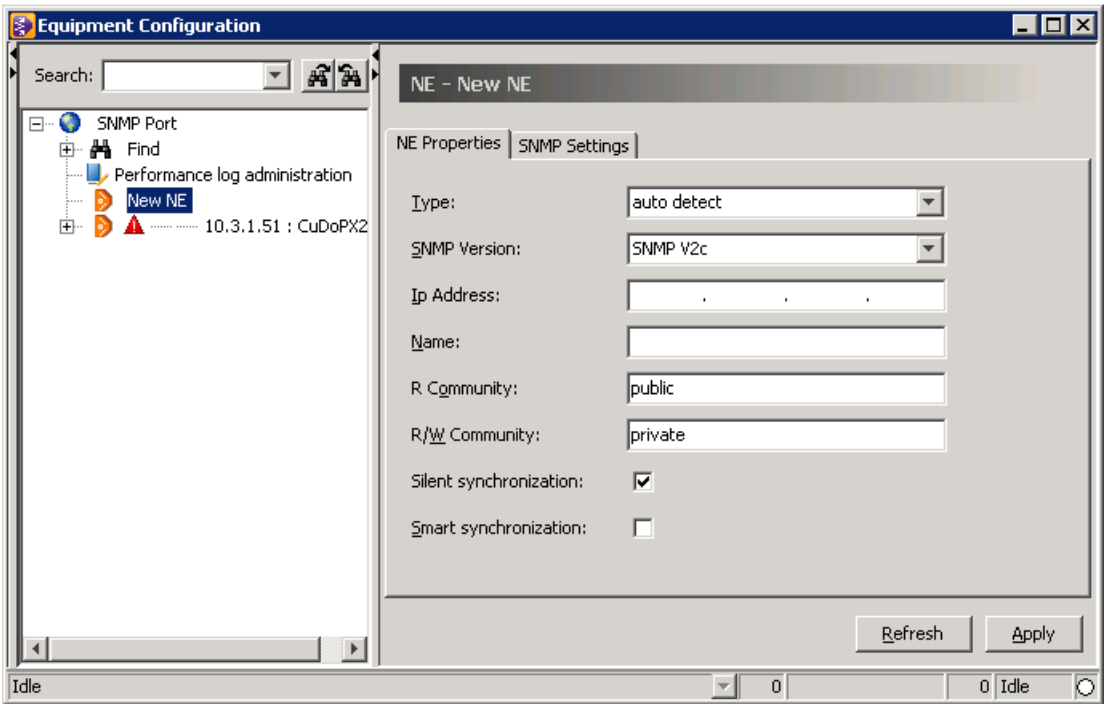

Figure 18 NE Properties

3. Enter the option values that are needed to access the NE over **SNMP**:

NE Property	Description
Type	Select the NE type from the drop-down list (e.g. `hiX 5750 R2.0`).
SNMP Version	The hiX 5750 R2.0 supports SNMP v2c.
IP Address	Enter the IP address of this NE in accordance with the project documentation

Table 4 NE Properties

NE Property	Description
Name	Optional Name according to project documentation If nothing is entered, the EM uses the combination <NE type#IP address> by default.
R Community	Default “public”
R/W Community	Default “private”
Silent synchronization	Presetting for consistency check: only process information is sent during verification, it is not possible to configure the NE until the process is finished.
Smart synchronization	Presetting for consistency check: reduces requests to the NE during the synchronization phase.

Table 4 NE Properties (Cont.)

4. Click the “Apply” button to confirm the settings.

Preset SNMP interface parameters of the NE can be changed after clicking the “SNMP Settings” tab.

If during startup inconsistencies should occur with access to the NE, start a consistency check in order to get detailed information about the causes.

1. Click “SNMP Port ⇨ Synchronize” tab.
2. Click to highlight the row of the NE and then click the “Start” button.
3. Check mark the required verification options and then click the “OK” button.

If alarms are displayed, see the EM PX “Maintenance Manual” before carrying out corrections to get detailed information on troubleshooting (Ctrl + M).

5.2 Starting the Equipment Configuration

1. Click “+” symbol on the left side of the “Root” icon in the “Network View”. The SNMP tree of the node expands and information on existing NEs hiX 5750 that have been started up are displayed.

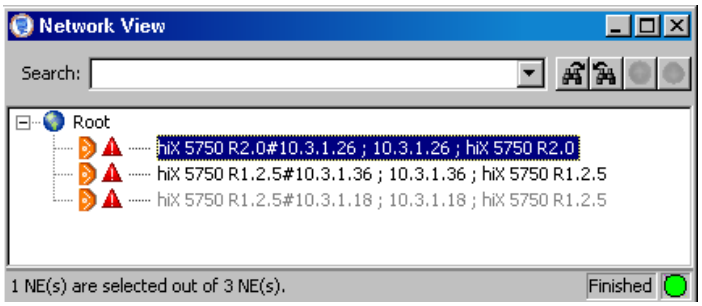

Figure 19 Network View

2. Highlight the new NE and then select “Configuration ⇨ Equipment Configuration” from the EM PX main menu.
   The **EM** PX configuration window is divided into two areas. The box on left side contains the **SNMP** navigation tree and the option pages on the right side contain the configuration dialogs. The SNMP tree is a view of NE’s equipment and features. It shows the hardware components, logical units and functionality with specific object icons. Each plug-in unit (module) is labeled with name and slot number. Use the SNMP tree to navigate between the various modules and functions on **OLT** and **ONT**.
3. In the SNMP navigation tree: click “+” symbol to expand the tree of the new NE.

4. Click an object in the tree to start a certain configuration procedure. Follow the step-by-step instructions as described in the appropriate chapter.

In the following instructions, the name “NE:hiX5750” is always used as start point in the SNMP navigation tree for the specific steps of commissioning.

5.3 Configuring the FTP Server Access

Configure users for the FTP servers as follows:

1. Click “NE:hiX5750 ⇨ FTP Server” tab.

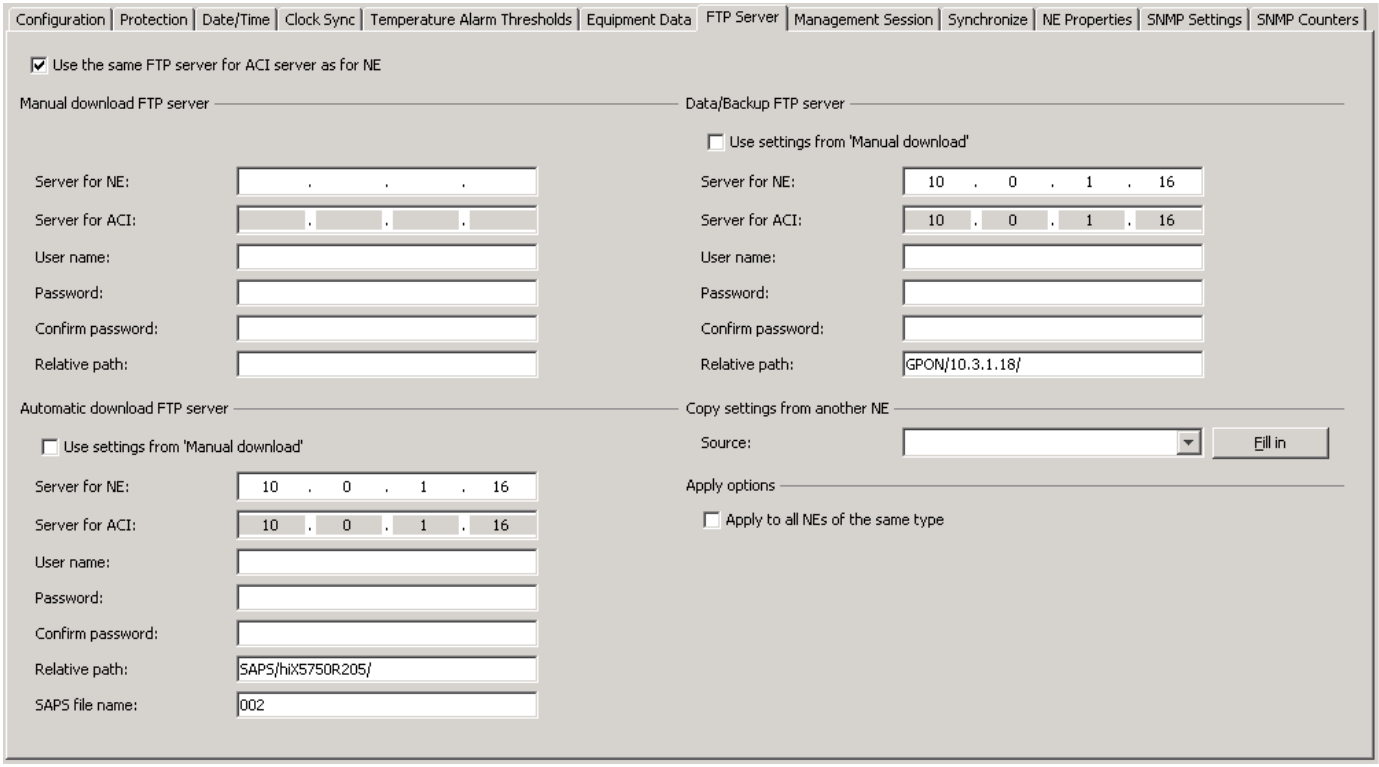

Figure 20 FTP Configuration

2. Decide by marking the corresponding check boxes whether different FTP servers need to be used for NE/ACI as well as for automatic or manual downloads of system application program software (S-APS).
   Fill out the required input fields (see Table 5) for an only FTP server or different FTP servers storing the S-APS and configuration data/backup.

   An automatic software upgrade can only start if all needed access data were configured. If a board does not run the correct software version, the hiX 5750 R2.0 will automatically download the new software version and activate.

Setting	Description
Server for NE	**IP** address of FTP server on which the NE **SAPS** is stored.
Server for ACI	IP address of FTP server on which the ACI SAPS is stored.
User name	User name of this FTP server.
Password	Password of this FTP server.

Table 5 Settings for FTP Server

Setting	Description
Confirm password	Repeat the password of this FTP server.
Rel. path	Path relative to root of this FTP server. Linux notation has to be used (/). Spaces in the path name are not allowed.
SAPS file name	File name of SAPS configuration file on FTP server.

Table 5 Settings for FTP Server (Cont.)

3. Click the “Apply” button to confirm.

To copy SAPS and data from an existing NE, choose this NE from the “Source” list and then click “Fill in” button.

5.4 Synchronizing Date and Time

The **NE** is normally synchronized automatically every 24 hours.

An immediate synchronization can be also performed manually during commissioning as follows:

1. Click “NE:hiX5750 ⇨ Date/Time” tab.
2. If necessary, the time zone can be changed.
3. Click the “Synchronize NE UTC time” button.
   The NE “hiX 5750” assumes date and time from the **EM**’s server.
4. Click the “Apply” button to confirm.

5.5 Upgrading the S-APS

When a hiX 5750 R2.0 software update/upgrade is required, the new system application program software (S-APS) has to be downloaded from the **(T)FTP** server to the **NE**. After finishing the download procedure, a reboot of updated units is required in order to activate the new S-APS. This means that the stored software load will be swapped with the running. The S-APS upgrade process can be performed automatically by the hiX 5750 R2.0. An automatic software upgrade can only start if all needed FTP user data are configured.

Please consider the current release notes in order to follow the correct upgrading procedures. Before starting the update/upgrade, execute a consistency check to be sure that the running software load is proper. Note that the units must be unlocked before starting the upgrade procedure.

1. Select “Maintenance ⇨ NE Maintenance” from the EM PX main menu to display the dialog page for the automatic S-APS download. Choose the new NE from the “NE” drop-down list.
2. Click to mark the “Selection” check box of the new NE.
3. Choose the appropriate software from the “SAPS file” drop-down list. This S-APS configuration file contains the software load information for units plugged in.
4. Choose “Enable SAPS” from the “Action” drop-down list to enable an automatic S-APS handling (a manual download of particular software modules will be only possible if “Disable SAPS” is selected).
5. Click the “Start” button. With the configured FTP user data, the system can request the S-APS configuration file from FTP server. This file is evaluated and checked whether the currently running software load is fitting to the expected one. Note that

this procedure may be time-consuming. From now the manual software download is disabled.

6. Choose “Download and activate” from the “Action” drop-down list.
7. Click the “Start” button to start the download process. If a unit does not run the correct software version, the system will start an automatic download and activate the new software for all existing units.

   The download process may be time-consuming. Do not switch-off the OLT or parts of it!

5.6 Switching-Over the CXU

A manual switch-over can be necessary for maintenance purposes. As a result, both the software load and configuration data states will be synchronized. Normally, a switch-over requires that the standby CXU is in better status than the currently active CXU.

1. Click “NE:hiX5750 ⇨ Protection” tab.
2. In order to force a switch-over to the standby CXU even if this one is in inferior status than the active CXU, click to mark the “Perform forced switch over” check box.
3. Click the “Switch” button to trigger a manual switch-over.

5.7 Synchronizing the Clock

1. Click “NE:hiX5750 ⇨ Clock sync” tab. The dialog page of **ETSI** (or **ANSI**) shelf will be opened as shown in Figure 21 (Figure 22).

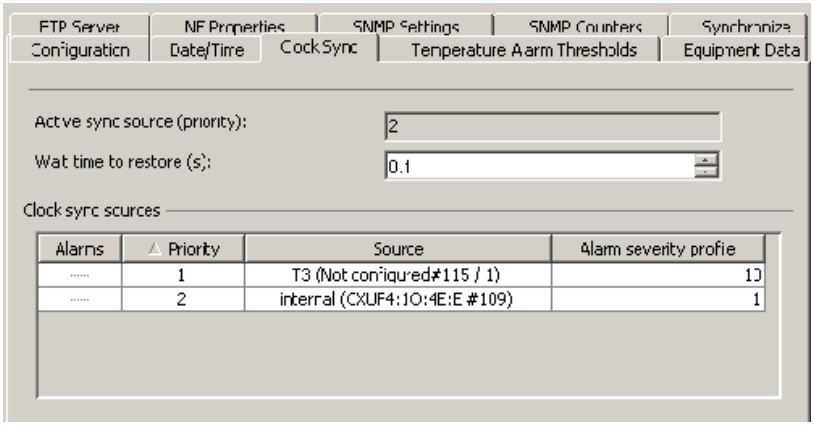

Figure 21 Clock Synchronization (ETSI)

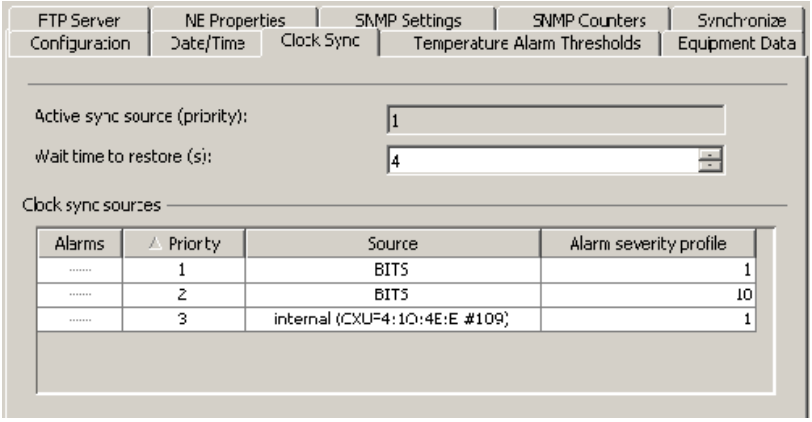

Figure 22 Clock Synchronization (ANSI)

Double-click into the input fields in order to change the settings:

Setting	Description
Wait time to restore (s)	The switch-over between the different clock sources is delayed for this time.
Alarm Severity Profile	Alarm severity profile in accordance with the planning documentation.

Table 6 Settings for the Register Card “Clock sync”

2. Click the “Apply” button to confirm.

5.8 Configuring the Alarm Severity Profiles

Each alarm severity profile sets a filter that determines whether an alarm will be forwarded to the external management system (e.g. EM PX R2.0 of ACI-E), and if yes, it determines the status of operator notification.

All alarms supported by the hiX 5750 R2.0 are listed in the profile dialog box, see Figure 23.

If an alarm occurs, the alarm and its severity is displayed to the operator.

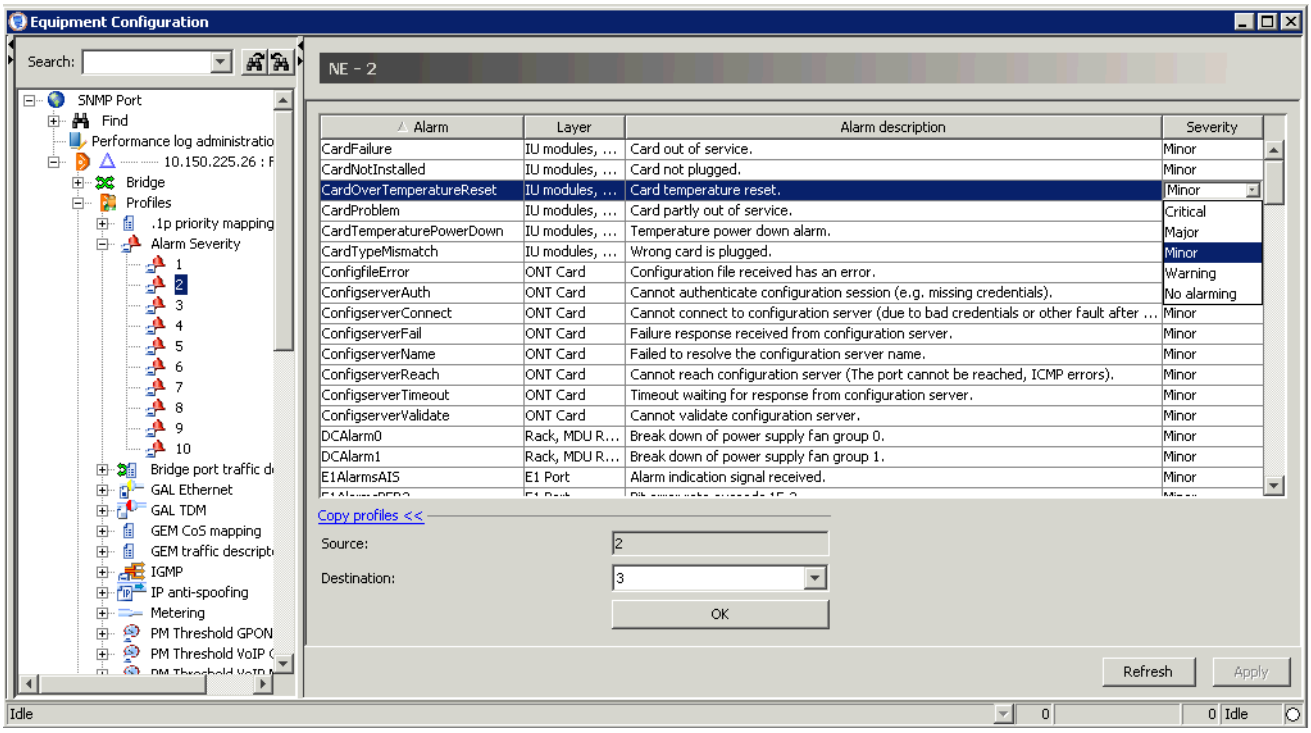

Figure 23 Alarm Severity Profile

1. Click “NE:hiX5750 ➪ Profiles ➪ Alarm Severity ➪ profile number”.
   To open the “Alarm Severity” profile subtree is time-consuming.
2. Double-click the “Severity” selection field of the alarm that needs to be configured and choose the severity level.
3. Click the "Apply” button to confirm all settings.

Click the “Copy profiles>>” action field to carry the made settings to another profile.

5.9 Setting the External Alarms and PON Alarm Thresholds

1. Click “NE:hiX5750 ➪ Configuration” tab, see Figure 24.
   Change the alarm severities of rack and shelf according to the planning documents.
2. Double-click the “Level” selection fields of alarm inputs and choose the needed levels.

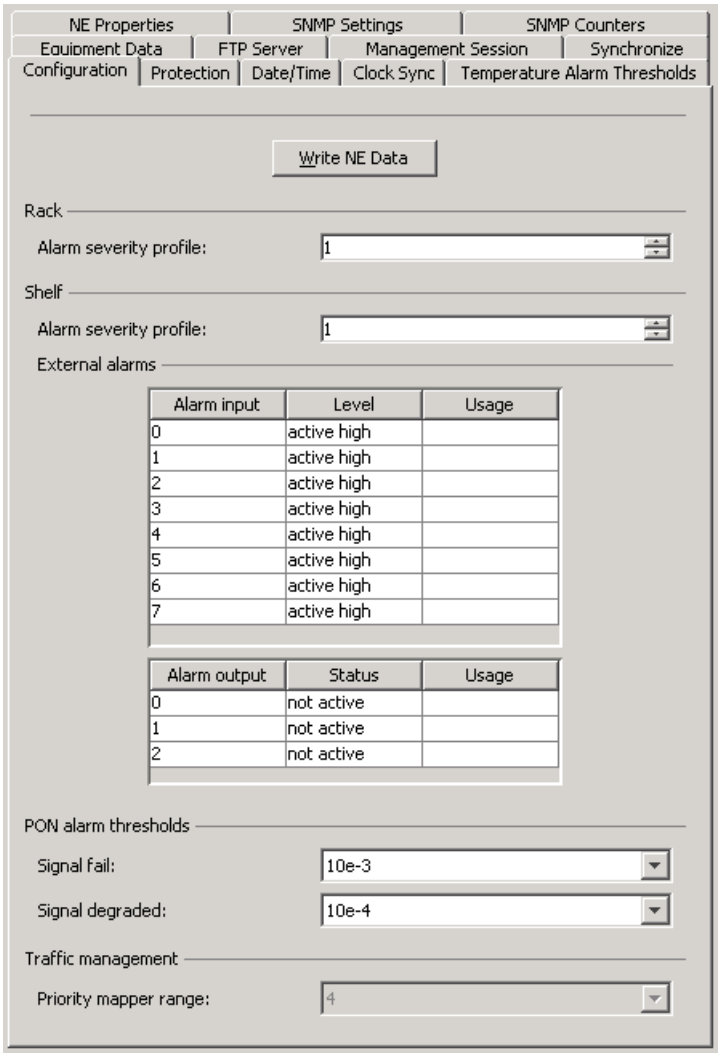

Figure 24 External Alarms

3. Double-click the “Usage” text input fields of “Alarm input” and “Alarm output” to enter significant descriptions.
4. Choose the alarm thresholds to alert the operator in case of signal failures on the GPON link.
5. Click the “Apply” button to confirm.

5.10 Saving the NE Configuration Data

Click the “Write NE Data” button to store the configuration data into the persistent memory of CXU, see Figure 24. This task must be performed after each configuration procedure.

Chapter 28 Database Backup describes how to configure an automatic backup of the NE’s configuration.

6 OLT Cards

Make sure that the current software load is running on the OLT.
See Chapter 5.5 Upgrading the S-APS to get information on how to update the software.

6.1 Using CXU and Uplink Redundancy

To use the CXU board and uplink line redundancy, be aware of the following procedures:

- Updating/upgrading of software load, see Chapter 5.5 Upgrading the S-APS
- Configuring of LACP for the CXU uplink ports, see Chapter 24 Link Aggregation Groups
- Configuring an LAG and LACP for uplink lines on the aggregation switch
- Synchronizing CXU boards by switch-over, see Chapter 5.6 Switching-Over the CXU.

6.2 Configuring the CXU Ethernet Ports

The 10-Gbps optical Ethernet Port #1 requires no settings. Each of the four 1-Gbps interfaces “Ethernet Ports #2” to “Ethernet Port# 5” can be used alternatively as optical or electrical Gigabit Ethernet interface depending on the **SFP** modules.

1. Click “NE:hiX 5750 ➪ CXUVR:1O:4E:E#109 ➪ Ethernet Port#” to display the “**Ethernet**” dialog page.
2. Choose the options according to the planning documents. The available settings are provided in Table 7.

Setting	Description
Type	Select “electrical” or “optical” according to the used **SFP** module.
Negotiation mode	Depending on the SFP: “auto” is recommended in any case, “forced” can only be used for electrical Ethernet ports of the CXU combined with defined bit rate setting.
Alarm severity profile	See Chapter 5.8 Configuring the Alarm Severity Profiles.

Table 7 Settings of CXU Ethernet Ports

3. Click the “Apply” button to confirm made changes.

See the following chapters to get further information:

- 14.1 Configuring the CXU Bridge
- 15.1 Creating a VLAN.

6.3 Resetting CXU and System

If the OLT is equipped with two CXU boards, the system reset can be only initiated by the working (active) CXU.

1. Click “NE:hiX5750 ➪ CXUVR:1O:4E:E#109” to display the “**General**” dialog page.

2. Choose “reset system” from the “Recovery Level” drop-down list.

The choice “Reset system with defaults” **OVERWRITES all previous configurations** and set the system values to the delivery state.

The inband and outband management interfaces must be re-configured via **CLI**. Choose this item only if the database is corrupt!

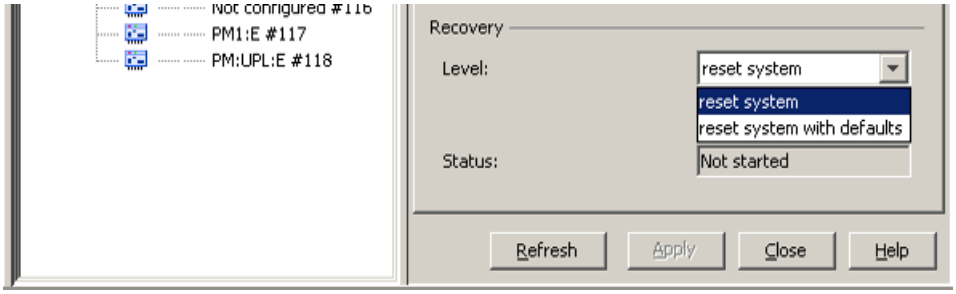

Figure 25 CXU - System Reset

3. Click the “Start” button to reset the system.

6.4 Creating an Interface Unit Card

An interface unit (IU) card can also be created in the **NE** when it is not physically plugged in the shelf. The “Admin state” of this IU is set to “planned” or “locked” and cannot be changed until the card is real plugged in.

The plug-in place #110 is not allowed for an IU card.

1. Click “NE:hiX5750 ⇨ Not configured#” to display the “**General**” dialog page.
2. Click the “<<create” action field to uncover the card selection fields.
3. Choose an IU card from the “New PIU type” drop-down list:

Setting	Description
IUGPON:2512:E	4xGPON 2,5G/1,2G, 8xE1 ETSI
IUGPON:2512:A	4xGPON 2,5G/1,2G, 8xDS1 ANSI
IUGPON:2512:L:E	4xGPON 2,5G/1,2G ETSI
IU10GE:1O:E	1x10GE subtending card ETSI
IU1GE:10O:E	10x1GE uplink card ETSI

Table 8 GPON Interfaces Units

4. Choose the admin state.
5. Click the “Create” button to insert the IU card.
6. Select the “General” tab.
7. Choose an “Alarm severity profile” (see Chapter 5.8 Configuring the Alarm Severity Profiles).
8. Click the “Apply” button to confirm.

6.5 Configuring Interface Unit Cards

GPON Ports

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port#” to display the “**PON**” dialog page.
2. Change the default settings according to the planning documentation:

Setting	Description
Alarm severity profile	For detailed information see Chapter 5.8 Configuring the Alarm Severity Profiles.
FEC	Mark to enable the “FEC” check box. For detailed information see Chapter 23 Forward Error Correction
Upstream bandwidth allocation	Select the **DBA** mode. For detailed information see Chapter 17 Bandwidth Management.

Table 9 GPON Port Settings

3. Fill in helpful “Information” into the text entry fields to specify the port.
4. Click the “Apply” button to confirm.

To get information about settings on the other dialog pages see the chapters:

- 14.2 Configuring the IU_GPON Bridge
- 15.2 Assigning VLANs to Ports.

E1/DS1 Ports

To get information about the configuration of **E1**/**DS1** ports see Chapter 12 TDM Leased Line Services.

Ethernet Ports

Configure the Ethernet ports of an additional uplink card IU_1x10G (“IU10GE:1O:E”) and subtending card IU_10x1G (“IU1GE:10O:E”) one after another as described in Chapter 6.2 Configuring the CXU Ethernet Ports on page 43.

6.6 Resetting an Interface Unit Card

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E#” and select the “**General**” tab.
2. Choose “reset module” from the “Recovery Level” drop-down list.
3. Click the “Start” button.
4. Confirm the hint message with the "Yes" button to start the reset of the IU card.

7 ONT and MDU

The operator creates an **ONT** or **MDU** with the attributes serial number, ONT-ID, type, **OLT GPON** interface (must exist), and alarm severity profile. The **NE** inserts two ONT cards automatically: one subscriber interface card and one PON interface card. All ONT entities (ONT shelf, ONT cards, ONT interfaces, **T-CONT**s, **GEM** ports, bridge ports), which are managed by alarms or operational state changes, always exist. By default, an ONT is created with the admin state “locked”.

The offline configuration of an ONT/MDU is also possible, but auto-configuration is not supported.

7.1 ONT and MDU Types

The table below contains ONT/MDU types which are provided by the hiX 5750 R2.0.

Name	Type	Ethernet 10/100bT	Ethernet 10/100/ 1000bT	POTS	xDSL	E1	CATV	SIP	H.248	AES	FEC	IGMP Snoop	WiFi	USB
hiX5701-003	E-SFU		1							X	X			
hiX5702-001	SFU		1	2				X	X	X	X	X		
hiX5702-002	SFU		1	2				X	X	X	X	X		
hiX5703-001	SFU	2		4				X	X	X	X	X		
hiX5703-003	SFU		2	4				X	X	X	X	X		
hiX5704-001	SFU		2	8					X	X	X	X		
hiX5705-001	SBU		1	8		2	1		X	X	X			
G25A-001	SFU	4		2			1	X		X	X	X		
G25A-002	SFU	4						X		X	X	X		
G25A-003	SFU	4		2				X		X	X	X		
G25C-001	SFU		1							X	X	X		
G25E-001	SFU	4		2				X		X	X	X		
G25E-002	SFU	4								X	X	X		
G80RG-001	SFU-RG		4	2			1	X	X	X	X	X	1	2
hiX5709-001	MDU[1]		16	48[2]	24[3]				X	X	X	X		
hiX5709-003			16	96[2]	32[4]		1	X	X	X	X	X		

Table 10 ONT/MDU Types

1) 4 slots for service boards
Max. number of ports, MDU equipped with:
2) SB_POTS24
3) SB_XDSL12 (12 VDSL2 and splitter)
4) SB_XDSL16 (16 VDSL2/ADSL2+, combo splitter) or SB_XDSL16P (16 VDSL2/ADSL2+, POTS splitter)

7.2 Creating an ONT/MDU

1. Click “NE:5750 ⇨ IUGPON:2512:E ⇨ GPON Port#” and select the “**ONT**” tab.
2. Click the “Create>>” action field to uncover the ONT properties dialog page.

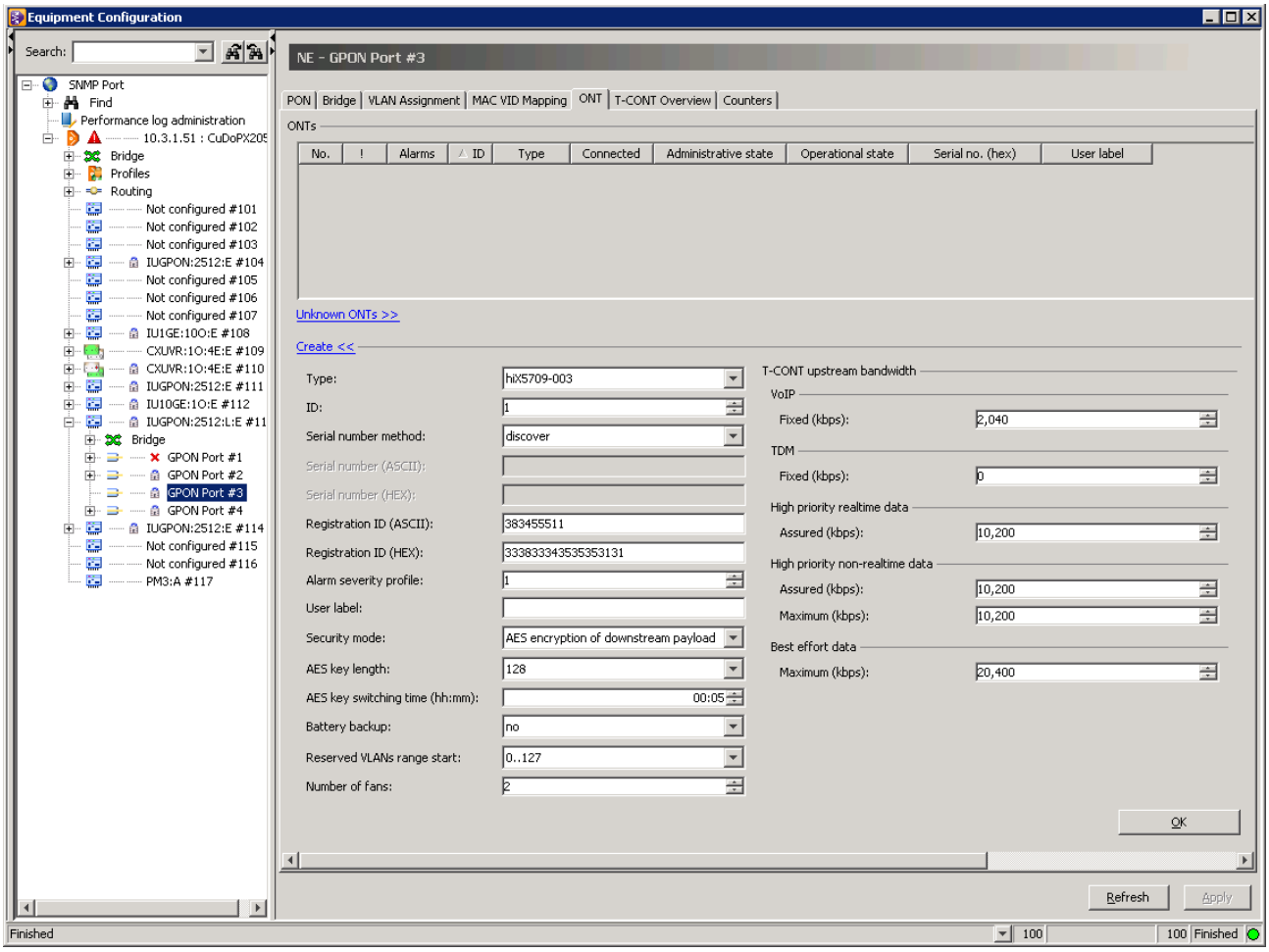

Figure 26 Creating an ONT

3. Select the new ONT/MDU from the “Type” drop-down list (see Chapter 7.1 ONT and MDU Types).
4. Enter an ONT “**ID**“ that has to be unique per **OLT** GPON interface from the range of 1 to 63.
5. Choose “Serial number method” and enter the configuration data:
   If “Serial number method” is set on “**configured**”, the ONT’s serial number must be entered into one of the serial number fields (ASCII/HEX). If an ONT/MDU with matching serial number is connected to the GPON link, it will be start up with the related data set. There are two ways to input the ONT serial number:
   - OLT and ONT/MDU are not yet connected (offline configuration):
     Enter the serial number according to the planning documentation.
   - OLT and ONT/MDU are connected (online configuration):
     Click the “Unknown ONTs>>” action field.
     The serial numbers of those ONTs are listed which were not yet configured.
     Click into the list to highlight an ONT/MDU and then click the “Copy to create” button.

   If “Serial number method” is set on “**discover**”, enter the password into one of the “Registration ID” fields (ASCII/HEX).
   The required settings are provided in Table 11. Some parameters can be configured only if a certain ONT type is selected, e.g. the MDU hiX5709.

Setting	Description
Serial number	see above.
Registration ID	Each ONT is assigned to an unique password. The password is only transmitted upstream and cannot be changed from OLT side. If the OLT reference password is initialized on operator command, the received ONT password is compared with the local stored OLT reference password. Therefore, if the OLT reference password is initialized, it must be valid, independent from the chosen “Serial number method”. If the OLT reference password is not initialized in advance, the ONT password is not requested. If an ONT with unknown serial number is detected at the GPON link and the Reg ID matches, it will be started up with the related data set, its serial number will be filled in and the “Serial number method” will be set to “configured”.
Alarm severity profile	Defines the actual alarm severities for all alarms per GPON ONT. For detailed information see Chapter 5.8 Configuring the Alarm Severity Profiles.
Security mode	Select “AES encryption of downstream payload” to configure the ONT with **AES** encryption. When encryption for the whole ONT is switched off, the affected GEM ports are automatically set to “no encryption”. For detailed information see Chapter 22.1 Advanced Encryption Support (AES).
T-CONT upstream bandwidth values (“TDM”, “VoIP”, “High priority realtime data”, “High priority non-realtime data”, “Best effort data”)	Input fields are displayed depending on the T-CONTs supported by the specific ONT type. The bandwidth values can be chosen in steps of 510 kbps (Ranges: VoIP 0..130050 kbps, other T-CONT types 0..1099560 kbps). Enter the values according to the planning documentation. See also Chapter 17.2 Changing the T-CONT Upstream Bandwidth.
User label	Any user string to identify the ONT (0...80 characters).
Battery backup	Select “yes” when the ONT uses a backup battery If deactivated, no related alarms (battery missing, battery failure, battery low) are generated.
Number of fans	The number of fans in the MDU hiX 5709 fan unit.
Reserved VLANs range start	A range of VLANs, that is reserved for internal use of MDU hix5709. The start value can be set in steps of 128.

Table 11 ONT Settings

6. Click the “OK” button to activate the values.
   The ONT appears in the ONT overview. A new created ONT is in “locked” state.
7. Click the “Apply” button to confirm.

7.3 Synchronizing the Time with OLT

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E ⇨ GPON Port# ⇨ ONT/MDU Type” to display the “**General**” dialog page.
2. Click the “Synchronize Time with OLT" button.
3. Click the “Apply” button to confirm.

7.4 Resetting an ONT/MDU

During software download to an ONT, do not initiate a reset of the same ONT. Wait until the software download is finished.

1. In the SNMP tree: click “NE:hiX5750 ⇨ IUGPON:2512:E ⇨ GPON Port# ⇨ ONT/MDU Type” to display the “**General**” dialog page.
2. Click the “Reset” button to reset the ONT immediately.

8 MDU Boards

The creation procedure for ONTs inserts in the case of MDU a shelf and the required empty containers. This chapter describes the tasks that need to be performed in order to create the uplink board of the MDU and its service boards.

8.1 Creating the Uplink Board UBGPON

The uplink board must be created as the first board (and deleted as the last one) on the reserved slot #3.

1. Click “NE:hiX5750 ⇨ IUGPON2512:E ⇨ GPON Port# ⇨ hiX5709-003# MDU ⇨ Not configured #3” to display the “**General**” dialog page.

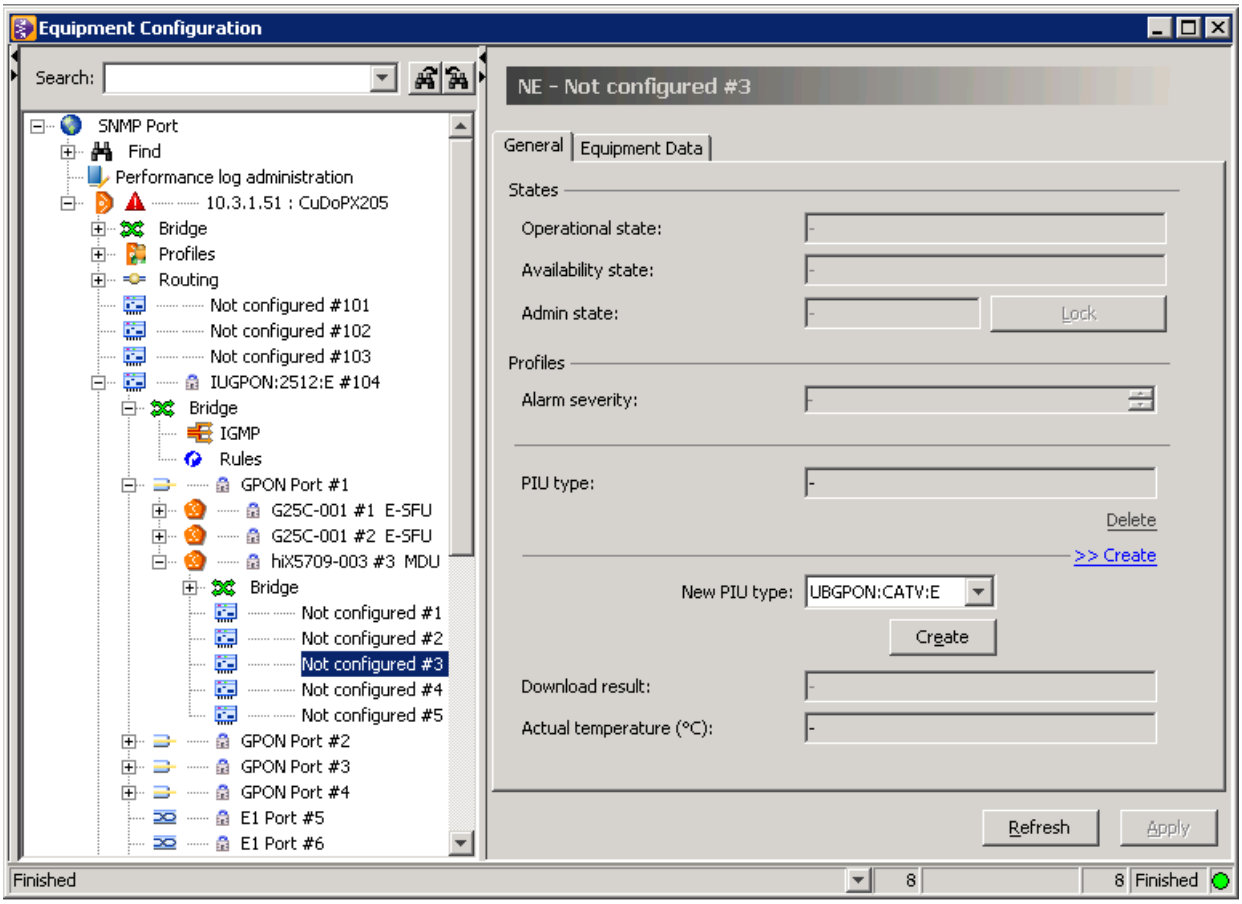

Figure 27 Creating an MDU Board

2. Click the “<<Create” action field to uncover the “New PIU type” selection field.
3. Choose the installed uplink board from the “New PIU type” drop-down list.

Type	Description
UBGPON:2512:E	Infrastructure and cascading interfaces, front access
UBGPON:CATV:E	Infrastructure and cascading interfaces, front access, CATV interface

Table 12 MDU GPON Uplink Boards

4. Click the “Create” button and wait until the module name is displayed in the SNMP tree.
5. Click “UBGPON:2512:E#3” to display the “**General**” dialog page and choose the “Alarm severity profile” (see Chapter 5.8 Configuring the Alarm Severity Profiles).
6. Click the “Apply” button to confirm.

To get more information about configuring the uplink interface see the chapters:

- 17 Bandwidth Management
- 23 Forward Error Correction
- 22.1 Advanced Encryption Support (AES)
- 9.4 Configuring CATV Ports.

8.2 Creating Service Boards

1. Click “NE:hiX5750 ⇨ IUGPON2512:E ⇨ GPON Port# ⇨ hiX5709-003# MDU ⇨ plug-in place of the service board” to display the “**General**” dialog page.
2. Click the “<<Create” action field to uncover the “New PIU type” selection field, see Figure 27.
3. Select the service board and follow the steps as described above.

Type	Description	Usable Slot #
SB:8P4GE:E	Service board with 8x **POTS** and 4x GE electric, front access	1, 2, 4, 5
SB:24P:E	Service board with 24x POTS, front access	
SBXDSL:12:E	Service board with 12x xDSL and splitter, front access, needs 2 plug-in places	1, 4
SBXDSL:16:E	Service board with 16x xDSL and combo splitter, front access, needs 2 plug-in places	
SBXDSL:16P:E	Service board with 16x xDSL and POTS splitter, front access, needs 2 plug-in places	
SBXDSL:16P:SL:E	Service board with 16x xDSL for splitter less applications, ADSL Annex A POTS, VDSL2 Region B, front access, needs 2 plug-in places	

Table 13 MDU Service Boards

4. Configure the subscriber ports as described in the chapters:
   - 9.1 Configuring Ethernet Ports
   - 9.2 Configuring POTS Ports
   - 11 VoIP Services
   - 10 xDSL Services.

9 Subscriber Ports

The number of physical ports depends on the type of ONT/MDU. To get more information see Chapter 7.1 ONT and MDU Types.

9.1 Configuring Ethernet Ports

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (SB:8P4GE:E#) ⇨ Ethernet Port#” to display the “**Ethernet**” dialog page.
2. Fill in helpful information into the text entry fields to specify the port.
3. Choose the “Alarm severity profile” (see Chapter 5.8 Configuring the Alarm Severity Profiles).
4. Click the “Apply” button to confirm.

To get information about the further settings see chapters:

- 14.5.4 Subscriber Bridge Ports
- 15.2 Assigning VLANs to Ports
- 15.3.4 MAC VID Mapping on Subscriber Port
- 14.5.5 .1p Priority Mapping on GEM Port Level
- 19 IGMP.

9.2 Configuring POTS Ports

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (SB:8P4GE:E#) ⇨ POTS#” to display the “**POTS**” dialog page.
2. Fill in helpful “Information” into the text entry fields to specify the port and enter the required values.
3. Choose the values as provided in Table 14:

Setting	Description
Alarm reporting	Is used to control alarm reporting from this managed port. Default value is “off”. Check mark the “Enable” box to activate this function.
Interval	Length of time for alarm reporting
Feeding	Feeding types: “ordinary phone” and “pay phone”
Impedance (Ohm)	The impedance for the POTS port can be configured by the operator. “unknown”, “600”, “900”,
On-hook transmission mode	Allows to set the POTS port to be put in either “full-time” or “part-time” on-hook transmission mode.
Rx gain (dB)	Gain value for the received signal. Valid values are from -12.0dB to +6.0dB in 0.1dB steps.
Tx gain (dB)	Gain value for the transmit signal. Valid values are from -6.0dB to +12.0dB in 0.1dB steps.

Table 14 POTS Settings

4. Click the “Apply” button to confirm.

See Chapter 11 VoIP Services for detailed information about VoIP/SIP configuration.

9.3 Configuring xDSL Ports

See Chapter 10 xDSL Services for details about configuring the xDSL ports.

9.4 Configuring CATV Ports

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ PON Card#1 (UBGPON:CATV:E) ⇨ CATV#” to display the “**CATV**” dialog page.
2. Fill in helpful “Information” into the text entry fields to specify the port.
3. Choose the “Alarm severity profile” (see Chapter 5.8 Configuring the Alarm Severity Profiles).
4. Change or confirm the preference settings:

Setting	Description
Alarm reporting control	Used to control alarm reporting from the managed port. Set a check mark to allow alarm reporting immediately Default: alarm reporting disabled.
ARC interval (min)	0- 254. An interval value of 255 has the special meaning of “infinity”.
Power control	Controls whether power is provided to an external equipment over the video PPTP. Value enables power over COAX. Default: power feed is disable.
Service control	Switching between two fixed pass band plans in order to differentiate the services delivered to the subscriber: - both frequency bands blocked - only low frequency band passed - both frequency bands passed.

Table 15 CATV Settings of the UNI

5. Click the “Apply” button to confirm.

10 xDSL Services

The hiX 5709 **MDU** supports **VDSL2** and **ADSL2+** standards via service boards.

10.1 Creating xDSL Profiles

Note the following hints:

- Existing default value profiles can be neither modified nor deleted.
- A subscriber port should become active only with non-default xDSL profiles if all values and options of these were configured completely.
- The xDSL ports must be “locked” before the values or option settings of xDSL profiles associated with these ports may be changed.

10.1.1 Channel Profile

There are specific default xDSL channel profiles for VDSL2 and ADSL2/ADSL2+, which should be duplicated to simplify the configuration.

1. Click “NE:hiX5750 ⇨ Profiles ⇨ xDSL Channel”, right-click the needed default profile object and select the “Duplicate” command from the context menu.

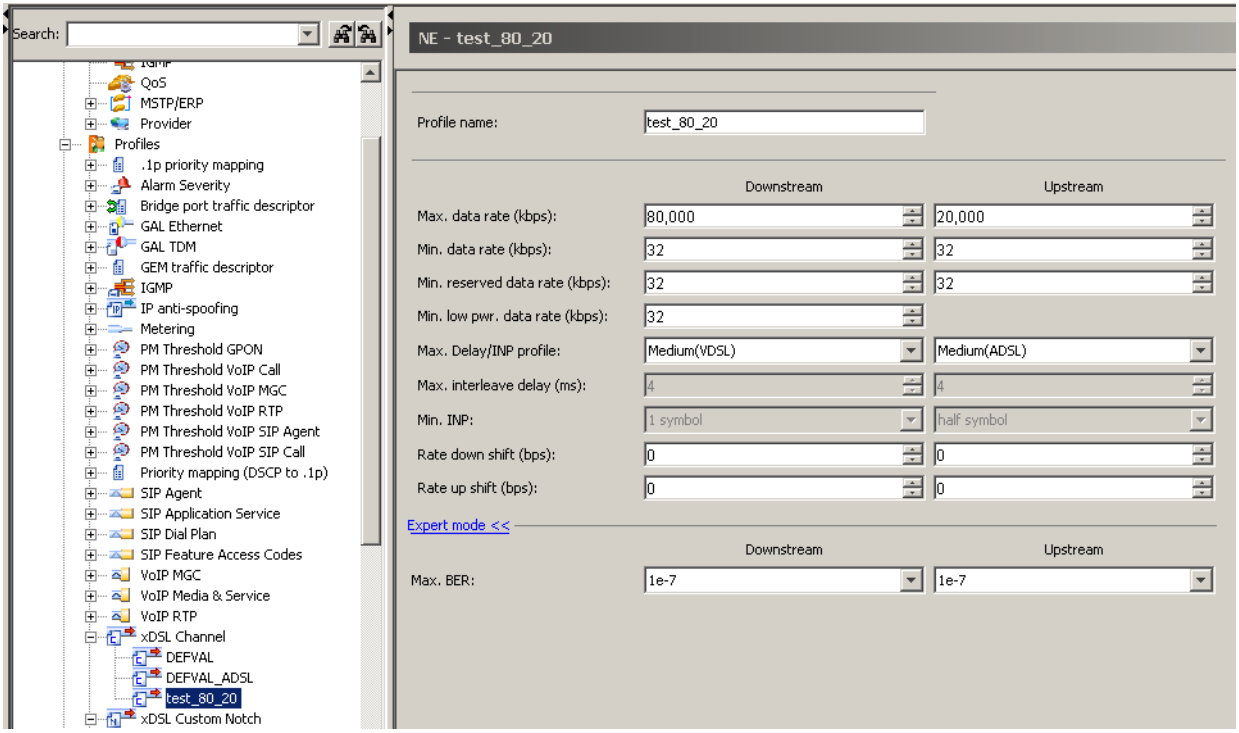

Figure 28 xDSL Channel Profile

2. Enter a unique profile name (space : ? , leading integer are not allowed).
3. Change the values depending on downstream and upstream direction according to the planning documentation (see Table 16 for more information).

Setting	Description
Max. data rate (kbps)	The maximum net data rate for the bearer channel. VDSL - DS/US: 32..240000; ADSL - DS: 32.. 32736/US: 32..3520
Min. data rate (kbps)	The minimum net data rate for the bearer channel. VDSL - DS/US: 32..103980; ADSL - DS: 32.. 32736/US: 32..3520
Min. reserved data rate (kbps)	The minimum reserved net data rate for the bearer channel. This parameter is used only if the Rate Adaptation Mode in the respective direction of the line is set to DynamicRa. VDSL - DS/US: 32..103980; ADSL - DS: 32.. 32736/US: 32...3520
Min.low pwr data rate (kbps)	The minimum net data rate for the bearer channel during the low power state (L1 in G.992.2, L2 in G.992.3). VDSL: 32..103980; ADSL: 32.. 32736
Max.Delay/INP profile	Choose the xDSL standard profile for DS/US to set the “Max.interleave Delay” and “Min.INP” values. The selection for DS and US may be different: “High(VDSL)”, “Medium(VDSL)”, “High(ADSL)”, “Medium(ADSL)”, “Low-Fast”, “Very high”, “user defined”
Max. interleave delay (ms)	These values are only configurable if “Max.Delay/INP profile” is set on “user defined”. The maximum one-way interleaving delay introduced by the PMS-TC on DS/US direction. The xTUs shall choose the S (factor) and D (depth) values such that the actual one-way interleaving delay is as close as possible to, but less than or equal to this parameter. Values: 0..63 or 255 There are three special values defined: 0 indicates no delay bound is being imposed 1 indicates the Fast Latency Path shall be used in the G.992.1 and S and D shall be selected such that S <= 1 and D = 1 in ITU-T Recommendations G.992.2, G.992.3, G.992.4, G.992.5 and G.993.2; 255 indicates a delay bound of 1 ms in ITU-T Recommendation G.993.2, same as value 1 for other Recommendations. If the value 1 or 255 is selected, then the following value for “Min. INP” should be 0.
Min. INP	These values are only configurable if “Max.Delay/INP profile” is set on “user defined”. The minimum impulse noise protection for the bearer channel, expressed in symbols. The parameter can take the following values: half symbol, 0..16 symbols Duration of impulse noise the system should with stand
Rate down shift (bps)	A trap will be produced when for DS/US direction: CurrTxRate <= PrevTxRate minus this value. If the DS/US rate falls below this threshold, the modem should attempt to decrease its transmit rate. Range: 0..1000000 (0 disables the trap)
Rate up shift (bps)	A trap will be produced when for DS/US direction: CurrTxRate >= PrevTxRate plus this value. If the DS/US rate pass this threshold, the modem should attempt to increase its transmit rate. Range: 0..1000000 (0 disables the trap)
Max. **BER**	Click the “Expert mode>>” action field to change the maximum value for allowed DS/US bit error rate: 1E-7 (default), 1E-5, 1E-3.

Table 16 xDSL Channel Profile

4. Click the “Duplicate” button to confirm.

10.1.2 Line Profile

This profile includes common properties describing both ends of the line. Besides the default VDSL2 line profile, there are different default line profiles for ADSL2 over POTS (DEFAULT_ADSL_A) and ADSL2 over ISDN (DEFAULT_ADSL_B), which should be duplicated to simplify the configuration.

Important remarks for the changing of used xDSL-standard via line profile:

- The change of a used xDSL standard is done by preparation of an ADSL profile and applying it to the VDSL port. Only this port can change the used standard between VDSL and ADSL.

- If the subscriber port is an ADSL2 type, a switch over to a VDSL mode is not possible.
- Only if the selected standard inside the line profile is reported as valid, the configuration can be done. See the release notes for further information.

1. Click “NE:hiX5750 ➪ Profiles ➪ xDSL Line”, right-click the needed DEFAULT profile object and select the “Duplicate” command from the context menu.
2. Enter a unique profile name (space : ? , leading integer are not allowed).
3. Change the settings according to the planning documentation.

   Refer to the current release notes to get detailed information on the supported VDSL2 band plans and profiles. These settings depend on the used DSL-chipset on the xDSL service boards of the MDU.

   Using ADSL and VDSL standards at the same time inside of one single profile is not possible.

Setting	Description
GS Standard	Select at least one standard by clicking the check box. The system will select the mode depending on the detected remote side. A mix of enabled VDSL and ADSL standards, or ADSL POTS and ISDN standards will be rejected by the NE.
VDSL2 band plan number	Choose a band plan that matches with the VDSL2 profile.
VDSL2 profile	Select the VDSL2 profile which should be used for configuration of basic parameters. The profile settings are defined in G.993.2. Supported profiles are: 8b, 12a, 17a, 17b (17A+US0), 30a.
Rate mode	Specify the rate selection behavior for the line in the DS/US direction: “manual”: forces the rate to the configured minimum rate “adapt at init”: adapts the line based upon line quality (default) “adapt at runtime”: seamless rate adapts during runtime based upon line quality.
Max. aggregate power (dBm)	Specify the maximum aggregate DS/US power level in the range of 0 to 25.5 dBm (0.1 dBm steps)
SRN margin (dB)	Specify the target DS/US Signal/Noise margin for a range of 0 to 31 dB (0.1 dB steps). This is the Noise Margin the transceivers must achieve with a **BER** of the selected “Max. BER” (see channel profile) or better to successfully complete initialization. Rule: Min. SRN < target SRN < Max. SRN
Max. SRN margin (dB)	Specify the maximum DS/US Signal/Noise margin from a range of 0 to 31 dB (0.1 dB steps).
Min. SRN margin (dB)	Specify the minimum DS/US Signal/Noise margin from a range of 0 to 31 dB (0.1 dB steps).

Table 17 xDSL Line Profile

4. Click the “Expert mode >>” action field to uncover the option fields and enter the values:

Setting	Description
Max. Rx power upstream (dBm)	Set the maximum received upstream power. The xTU-C will force the xTU-R to reduce transmitted power, if this value will be exceed (Range of -25.5 0 to +25.5 dBm, 0.1 dBm steps)
Upshift	**SNR** margin (dB): Configured Signal/Noise margin for rate upshift. If the DS/US noise margin falls below this level, the modem should attempt to increase its transmit rate. Range: 0 (default)..31 dB (0.1 dB steps) Min. time (s): Minimum time that the current DS margin is above upshift SNR margin before an upshift occurs. Range: 0 (default)..16383

Table 18 xDSL Line Profile - Expert Mode

Setting	Description
Downshift	SNR margin (dB): Configured Signal/Noise margin for rate downshift. If the DS/US noise margin falls below this level, the modem should attempt to decrease its transmit rate. Range: 0 (default)..31 dB (0.1 dB steps) Min. time (s): Minimum time that the current DS margin is below SNR margin before a downshift occurs. Range: 0 (default)..16383

Table 18 xDSL Line Profile - Expert Mode (Cont.)

5. Click the “**Extension Profile**” tab and the click the “Expert mode>>” action field to configure specific additional xDSL line options.
6. Configure the options such as “Power backoff downstream” and “Power backoff upstream” values according to the planning documentation.
7. Click the “Duplicate” button to create the new xDSL line profile.

10.1.3 PSD Mask Profile

The default **PSD** mask profiles “DEFAULT_UP” and “DEFAULT_DOWN” contain a set of VDSL2 breakpoints (G 993.2). They should be used only with VDSL2 profile 17A.

A new created PSD profile contains a set of default breakpoints with number and level depending on the configured usage type:

Downstream		Upstream	
Index	**PSD Level (dbm/Hz)**	**Index**	**PSD Level (dbm/Hz)**
65	-39.5	32	-38.0
256	-39.5	63	-38.0
376	-49.5	882	-54.5
705	-52.5	1193	-55.5
857	-54.0	1984	-58.0
1218	-55.5	2318	-58.5
1959	-58.0	2770	-59.5
2795	-59.5		
4083	-59.5		

Table 19 Default PSD Breakpoints

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “xDSL PSD Mask” profile object and select the “New xDSL PSD Mask profile” command from the context menu.
2. Enter a unique profile name (space : ? , leading integer are not allowed).
3. Choose the “Usage type” according to the downstream or upstream direction.
   After creating a PSK mask profile, this option cannot be changed.
4. Select the “Subcarrier spacing” value according to the used VDSL2 profile: 4.3125 kHz, 8.625 kHz (for 30a) or N/A.
5. Click the “Add>>” action field to insert each new subcarrier level set.

The maximum number of breakpoints that can be added is 32 for downstream and 16 for upstream direction (G.997.1). All needed breakpoints should be configured in a continuous way.

Setting	Range
Subcarrier	1..4095
Frequency (kHz)	Depending on the subcarrier: from 4.3125 for subcarrier 1 to 17659.6875 for subcarrier 4095.
Level (dBm/Hz)	-97,5 to 0

Table 20 PSK Subcarrier Option Ranges

6. Click the “OK” button to insert the breakpoint.
7. Click the “Create” to confirm.

10.1.4 Event Profile

1. Click “NE:hiX5750 ⇨ Profiles ⇨ xDSL Event”, right-click the “xDSL Event” profile object and select the “New xDSL Event profile” command from the context menu.
2. Enter a unique profile name (space : ? , leading integer are not allowed).
3. Click the “Init failure” check box to enable/disable whether a notification is generated when an initialization failure occurs or not.
4. Click the “Operational state” check box to decide whether a notification is generated if an operational status has been changed or not.
5. Enter the PM counter threshold values from the range of 0..900 seconds.
6. Click the “Create” button to confirm.

10.1.5 Custom Notch Profile

The transmit power spectral density mask code is used to avoid interference with Handheld Amateur Radio (HAM) radio bands by the introducing of power control (notching) in one or more of these bands. Notching can be enabled or disabled for each standard band. Amateur radio band (1..5) and GMDSS (6..8) notching is defined in the VDSL2 spectrum as follows:

	Frequency (kHz)		Carrier Profiles 8A and 17A Spacing 4.3125 kHz		Carrier Profile 30A Spacing 8.625 kHz	
	Start	Stop	Start	Stop	Start	Stop
1	1,800	2,000	417	464	209	232
2	3,500	3,800	811	881	406	441
3	7,000	7,200	1623	1670	812	835
4	10,100	10,150	2342	2354	1171	1177
5	14,000	14,350	3246	3328	1623	1664
6	2,173	2,191	504	508	252	254
7	4,200	4,215	974	977	487	489
8	6,300	6,320	1461	1466	730	733

Table 21 VDSL2 Notching

Already used custom notch profiles cannot be modified. The **NE** can handle only 16 notches per line at same time.

1. Click “NE:hiX5750 ⇨ Profiles ⇨ xDSL Custom Notch”, right-click the “xDSL Custom Notch” profile object and select the “New xDSL Custom Notch profile” command from the context menu.
2. Enter a unique profile name (space : ? , leading integer are not allowed).
3. Click the “Add>>” action field.
4. Enter the “Begin subcarrier” and “End subcarrier” values

   An overlapping of activated notches is not allowed.

Setting	Description
Begin subcarrier	Number of the subcarrier, where this notch starts 1...4095 (if 0 the notch is not valid).
End subcarrier	Number of the subcarrier, where this notch stops 1...4095 (if 0 the notch is not valid).

Table 22 xDSL Custom Notch Profile

5. Click the “OK” button to set the subcarrier.
6. Click the “Create” button to confirm.

10.2 Configuring xDSL Ports

To configure an xDSL port properties, it must be set on admin state “locked”. Only the “Action” option can be also changed in “unlocked” state.

If the subscriber port is of type ADSL2, the switch-over to a VDSL mode is not possible.

10.2.1 xDSL Line

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ hiX5709-001# MDU ⇨ SBXDSL12:E# ⇨ xDSL Port#” to display the “**xDSL Line**” dialog page (use the same procedure for other types of MDU service boards).
2. Fill in helpful “Information” into the text entry fields to specify the port.
3. Choose the “Alarm severity profile”.
4. Choose the required xDSL settings:

Setting	Description
xDSL Line	Select the xDSL Line Profile.
Custom Notch	Select the xDSL Custom Notch Profile.
Upstream **PSD** mask	Select the xDSL upstream PSD Mask Profile.
Downstream PSD mask	Select the xDSL downstream PSD Mask Profile.
Event	Select the xDSL Event Profile.
Channel 1	Select the xDSL Channel Profile.
Channel 2	Must be set “NO PROFILE”.

Table 23 xDSL Port Settings

Setting	Description
Action	Default is “startup”, required to start the modem. Select another action to check the line: “spectrum reverb”, “ATM loop back”, “spectrum medley”, “force L2”, “show time lock”.
Force impuls noise protection	Forced INP can be enabled/disabled per downstream and upstream direction.
Channel 1 rate adaptation (%)	The ratio refers to available data rate in excess of the Minimum Data Rate summarized over all bearer channels. 100 % is the ratio of excess data rate to be assigned to all other bearer channels on downstream/upstream direction. The sum of rate adaptation ratios over all bearers on the same direction shall be equal to 100 %

Table 23 xDSL Port Settings (Cont.)

5. Click the “Apply” button to confirm.

10.2.2 xDSL Bridge Ports

1. Click the “PVC(1,32) ➪ Bridge” tab.
   Enter the port specific settings, see Chapter 14 Bridges.
   For further information see also the chapters:
   - 15.2 Assigning VLANs to Ports
   - 18 DHCP and PPPoE
   - 19 IGMP
2. Click the “Apply” button to confirm.

10.2.3 Permanent Virtual Circuit (PVC) for ADSL

1. Expand the dialog page of xDSL port that needs to be configured.
2. Click the “PVC(1,32)” object to display its “**PVC**” dialog page.

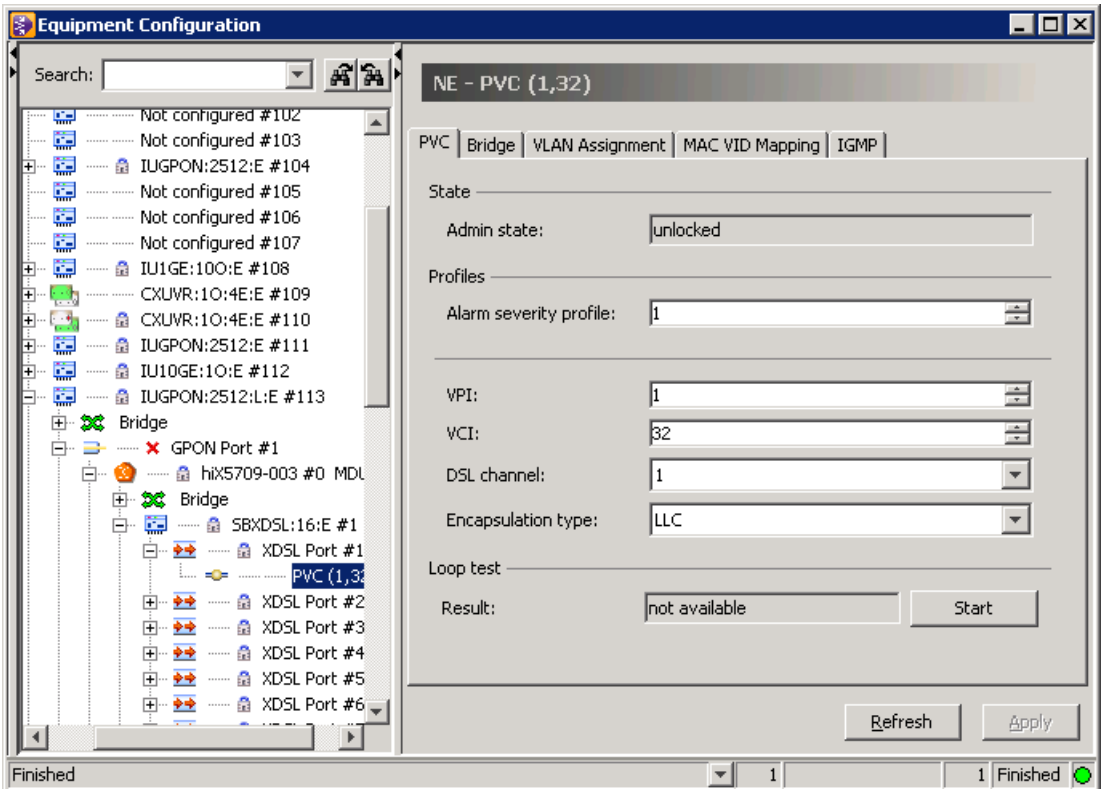

Figure 29 xDSL - PVC

3. Choose the “Alarm serverty profile”.
4. Change the xDSL values according to the planning documentation.

Setting	Description
VPI	Select the Virtual Path Identifier from the range: 0...255, default value: 1
VCI	Select the Virtual Circuit Identifier from the range: 32... 65535, default value: 32
DSL channel	This option defines the usage of a DSL bearer channel by this VCC. The availability of DSL channels depends on the configuration of the underlaying DSL line. 1: channel 1 always available. 2: channel 2 only in dual latency mode available.
Encapsulation type	Used encapsulation over AAL5: “LCC” or “VC multiplexing”

Table 24 PVC Settings

5. Click the “Apply” button to confirm.

If necessary, an additional PVC can be created by right-clicking the xDSL port object.

11 VoIP Services

Depending on the **ONT**/**MDU** type, it is possible to offer voice service via **SIP** or H.248. The set protocol version is always effective for all ports of ONT (MDU service board). The configuration can also be carried out when the ONT is offline.

Chapter 7.1 ONT and MDU Types provides information about such ONT types supporting **VoIP**.

Settings of physical **POTS** ports are described in Chapter 9.2 Configuring POTS Ports.

11.1 Creating the VoIP Profiles (H.248 and SIP)

Completed VoIP profiles (of the same major release number) can be also imported. See the online-help for more information on profile import/export.

The values and option settings of existing VoIP default profiles may also be changed.

11.1.1 VoIP RTP Profile

Up to 16 VoIP RTP (Real-Time Transport Protocol) profiles may be configured.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “VoIP RTP” profile object and select the “New VoIP RTP profile” command from the context menu.
2. Enter a unique “Profile name”.
3. Enter the option settings according to the planning documentation:

Setting	Description
Base RTP port (Min./Max.)	Defines the base RTP port that should be used for voice traffic. Default is RTP port 50000. The “Max.” port defines the top end range RTP port used for voice traffic. Default must be greater than “Min.” but is determined by vendor application.
DSCP mark	Diffserv code point to be used for outgoing RTP packets for this profile. Default value is Expedited Forwarding (EF) = 46 (bin 101110).
Events	Default: disable (Events according to RFC2833)

Table 25 Settings of VoIP - RTP Profile

4. Click the "Create" button.

11.1.2 VoIP MGC Profile

The VoIP MGC (Media Gateway Control) profile contains settings for the connection with the media gateway controller (softswitch) that controls the signaling messages.

All subscriber ports of the ONT (MDU service board) must use the same profile. Only one profile per ONT subscriber card / per internal VoIP gateway is possible. A maximal number of 16 different softswitches can be configured per OLT.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “VoIP MGC” profile object and select the “New VoIP MGC profile” command from the context menu.

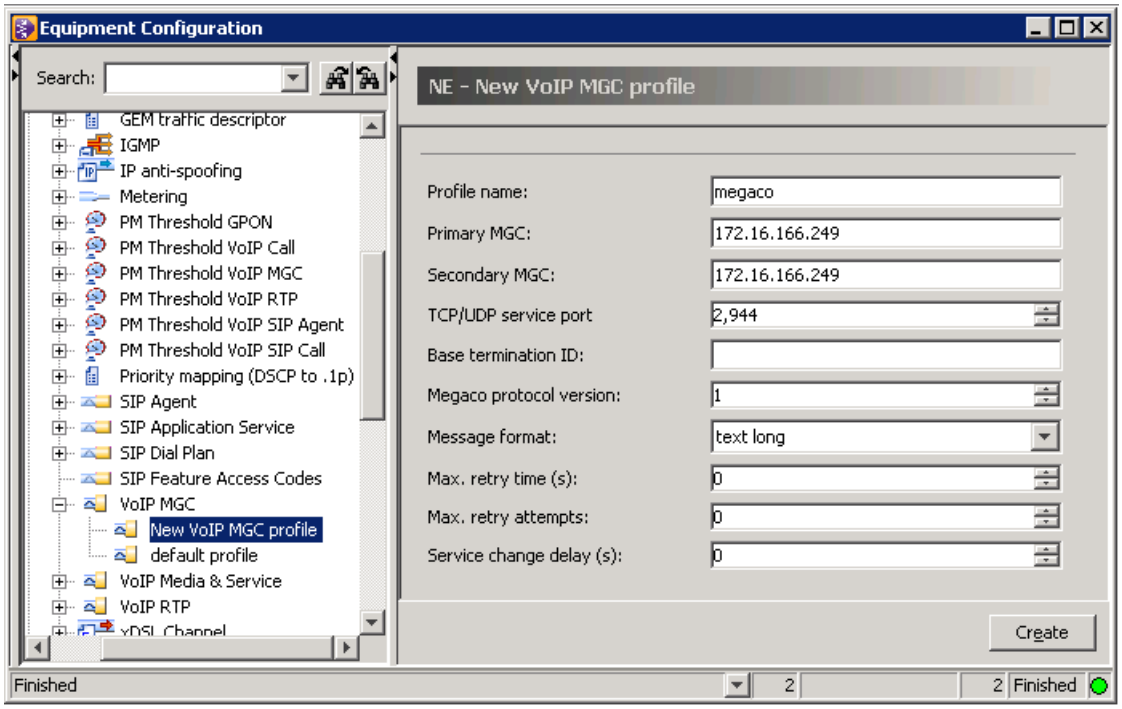

Figure 30 VoIP MGC Profile

2. Enter a unique “Profile name”.
3. Enter the option settings and values according to the planning documentation.

Setting	Description
Primary **MGC**	IP address of the first MGC (soft switch) that controls the signaling messages. The port is optional. Default value is 2944 for text message formats and 2955 for binary message formats.
Secondary MGC	IP address of the second soft switch (only necessary, if a second switch is used)
TCP/**UDP** service port	Port number of the UDP port, which was created in the “TCP/UDP Services“ window, This setting associates the MGC with the TCP/UDP service to be used for communication with the MGC. Default value is 0 unless the IP port is associated.
Base termination ID	The base string for the H.248 physical termination IDs must be set to “port_”.
Megaco protocol version	Defines the version of the Megaco protocol being used.
Message format	Defines the message format. Valid values are: “Text Long” (default), “Text Short”, “Binary”.
Max. retry time (s)	Defines the maximum retry time for transaction on associations to the MGC. Default is 0 = vendor specific implementation.
Max. retry attempts	Defines the maximum number of times a message is retransmitted to the MGC. Default is 0 = vendor specific implementation.
Service change delay (s)	Defines the service status delay time for changes in line service status. Default is 0 = no delay.

Table 26 Settings of VoIP - MGC Profile

4. Click the "Create" button.

11.1.3 VoIP Media & Service Profile

Note that first an RTP profile needs to be created/configured. The choice of an RTP profile is only possible during the creation of a VoIP media and service profile.

Up to 16 VoIP Media & Service profiles can be created.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “VoIP Media & Service” profile object and select the “New VoIP Media profile” command from the context menu.
2. Enter a unique “Profile name”.
3. Change the options and values according to the planning documentation.

Setting	Description
Fax mode	Defines the Fax mode “pass through” (default) or “T.38”
Out-of-band DTMF	Defines if the Out-of-band DMTF is enable.
RTP profile	Select a before configured RTP profile.
Echo cancellation	Enables/disables echo cancellation.
PSTN protocol variant	Controls which variant of POTS signaling shall be used on the associated **UNI**s. The value used is equal to the country code as defined by ISO recommendation ISO 3166.

Table 27 Settings of VoIP - Media and Services Profile

Choose these options per order 1..4 as needed:

Setting	Description
Codec	Current codec used for the VoIP POTS port. “PCMU”: “Auto select” is the default setting. Supported codecs are e.g. G.711, G.723, G.729 A, G.726 (according to RFC3551).
Packet period selection interval (ms)	Default value is 10. Valid intervals are 10..30ms (steps 1ms).
Silence suppression	Indicates whether silence suppression is “on” or “off”.

Table 28 Settings of VoIP - Media and Services Profile

4. Click the "Create" button.

11.2 Creating SIP Profiles

11.2.1 SIP Agent Profile

The SIP user agent connects to SIP server (proxy/registrar/location server) via SIP protocol and performs the basic registration, call control, and media processing functions. Each subscriber port can have a reference to another SIP agent.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “SIP Agent” profile object and select the “New SIP Agent profile” command from the context menu.
2. Enter a unique “Profile name”.
3. Configure the following parameters as needed:

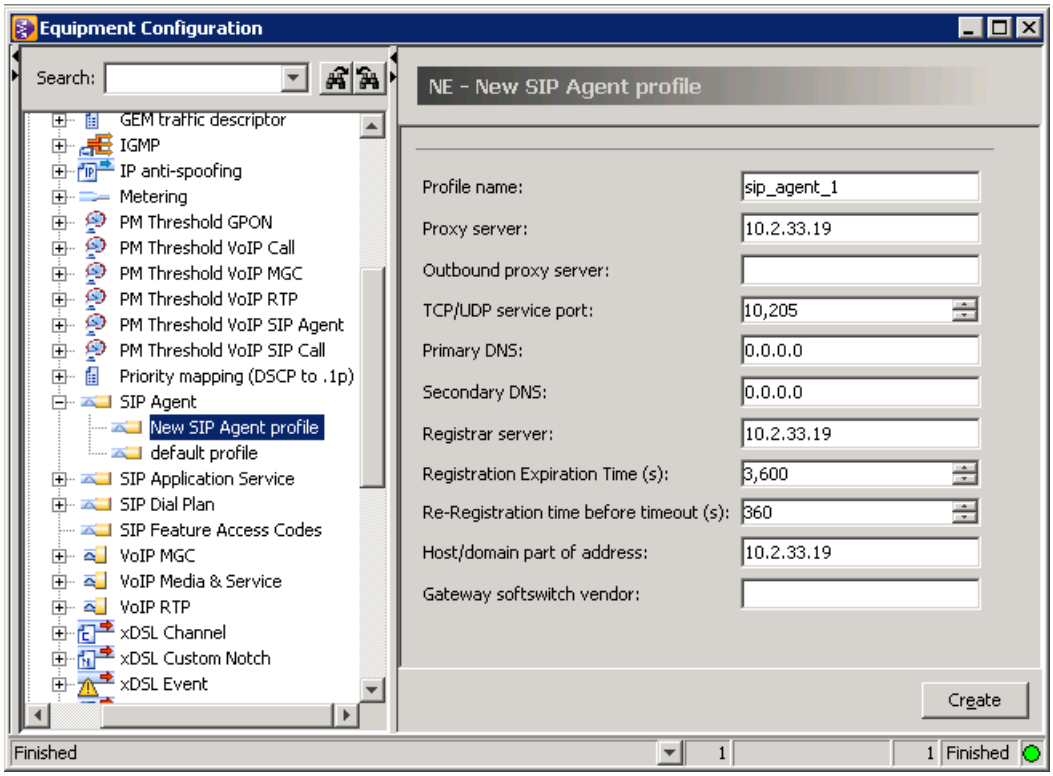

Figure 31 SIP Agent Profile

Setting	Description
Proxy server	IP address or URI of the SIP proxy server for SIP signaling messages.
Outbound proxy server	IP address or URI of the SIP outbound proxy server for SIP signaling messages.
TCP/UDP server port	Associates the SIP agent with the TCP/UDP service to be used for communication with the SIP Proxy Server. Default value is 0 unless the IP port is associated.
Primary DNS	Primary SIP DNS IP address. If this value is zero, the primary SIP DNS should not be used.
Secondary DNS	Secondary SIP DNS IP address. If this value is zero, the Secondary SIP DNS should not be used.
Registrar server	IP address or resolved name of the SIP Registrar Server for SIP signaling messages. Examples: '10.10.10.10' and 'proxy.voip.net'.
Registration Expiration time (s)	If this value is zero, the SIP Agent will not add an expiration time to the registration requests, and will not perform re-registration.
Re-Registration time before timeout (s)	This time prior to timeout that the SIP Agent should start the re-registration process.
Host/domain part of address	The host or domain part of the SIP address for users connected to this ONT. 0 indicates the current address in the IP Host Config ME is used.
Gateway softswitch vendor	The format is four ASCII coded alphabetic characters [A - Z] as defined in ANSI T1.220. All NULL characters indicates no particular vendor.

Table 29 Settings of SIP Agent Profile

4. Click the "Create" button.

11.2.2 SIP Dial Plan Profile

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “SIP Dial Plan” profile object and select the “New SIP Dial Plan profile” command from the context menu.

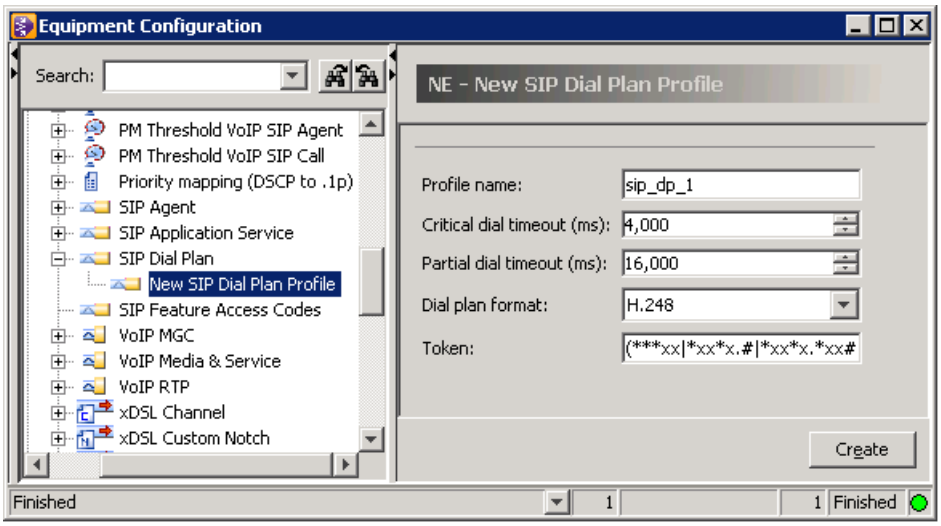

Figure 32 SIP Dial Plan Profile

2. Enter a unique “Profile name”.
3. Choose the values according to the planning documentation.

Setting	Description
Critical dial timeout (ms)	The critical dial timeout for digit map processing. Default: 4096ms
Partial dial timeout (ms)	The partial dial timeout for digit map processing. Default: 16384ms
Dial plan format	- H.248: dial plan format with specific plan (entries defined by the dial plan, see below) - NSC format - vendor specific format - not defined
Token	This option is supported only by the ONT types G25A and G25E. A dial plan token is a component of the whole dial plan. The length of dial plan token is limited to 28 Byte.

Table 30 Settings of SIP Dial Plan

4. Click the "Create" button.

Dial Plan Configuration for ONTs G25A and G25E

The format of dial plan is selected according to H.248:

- Valid characters are:
  - 0,1,2,3,...,9
  - *,#,(,), |
  - x
  - . and T

  All the dial plan profiles will be concatenated at the creation sequence instead of at alphabet sequence.
- The dial plan begins with "(" and ends with ")". Each item in the dial plan is delimited by "|", e.g. (1234|**##|x.T).

- A dial plan is completed by the integration of several separate dial plan token. The length of dial plan token is limited to 28 Byte.
  For example, with the tokens:
  Token 1: (***xx|*xx*x.#|*xx*x.*xx#|
  Token 2: *xx*x.*x#|*31*xxxxxxxx|
  Token 3: *xx#|#xx#|*#xx#|#001|x.T)
  the following dial plan is formed:
  (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)
- The two POTS ports of ONT share one dial plan. After the ONT is once locked/unlocked, the new dial plan takes effect.
- The ONT uses its default dial plan before any other dial plan has been configured. The default dial plan is:
  (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)
- The storing of a dial plan in the ONT does not replace its default dial plan. After a reboot of this ONT, the default dial plan takes effect again.

The following example shows a dial plan that is composed of three SIP dial profiles:

- The SIP dial profiles DP_1, DP_2, and DP_3 use the above token1, token2, and token3:

Setting	DP_1	DP_2	DP_3
Critical dial timeout (ms)	4.000	8.000	5.000
Partial dial timeout (ms)	16.000	20.000	12.000
Dial plan format	H.248	H.248	H.248
Token	(***xx|*xx*x.#|*xx*x.*xx#|	*xx*x.*x#|*31*xxxxxxxx|	*xx#|#xx#|*#xx#|#001|x.T)

Table 31 Example of SIP Dial Plan

- To construct the complete dial plan:
  (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)
  the three dial plan profiles must be assigned to the POTS ports, see Chapter 11.7 Configuring POTS Service via VoIP - SIP on page 70:
- In addition, the values for “Critical dial timeout” and “Partial dial timeout” are different in these dial plan profiles. In such a case, the values specified in the last profile take effect. For the above example, a “Critical dial timeout” of 5000ms and a “Partial dial timeout” of 12000ms will be valid for the ONT.

11.2.3 SIP Application Service Profile

This profile defines attributes of calling features used in conjunction with a VoIP line service.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “SIP Application Service” profile object and select the “New SIP Application Service profile” command from the context menu.

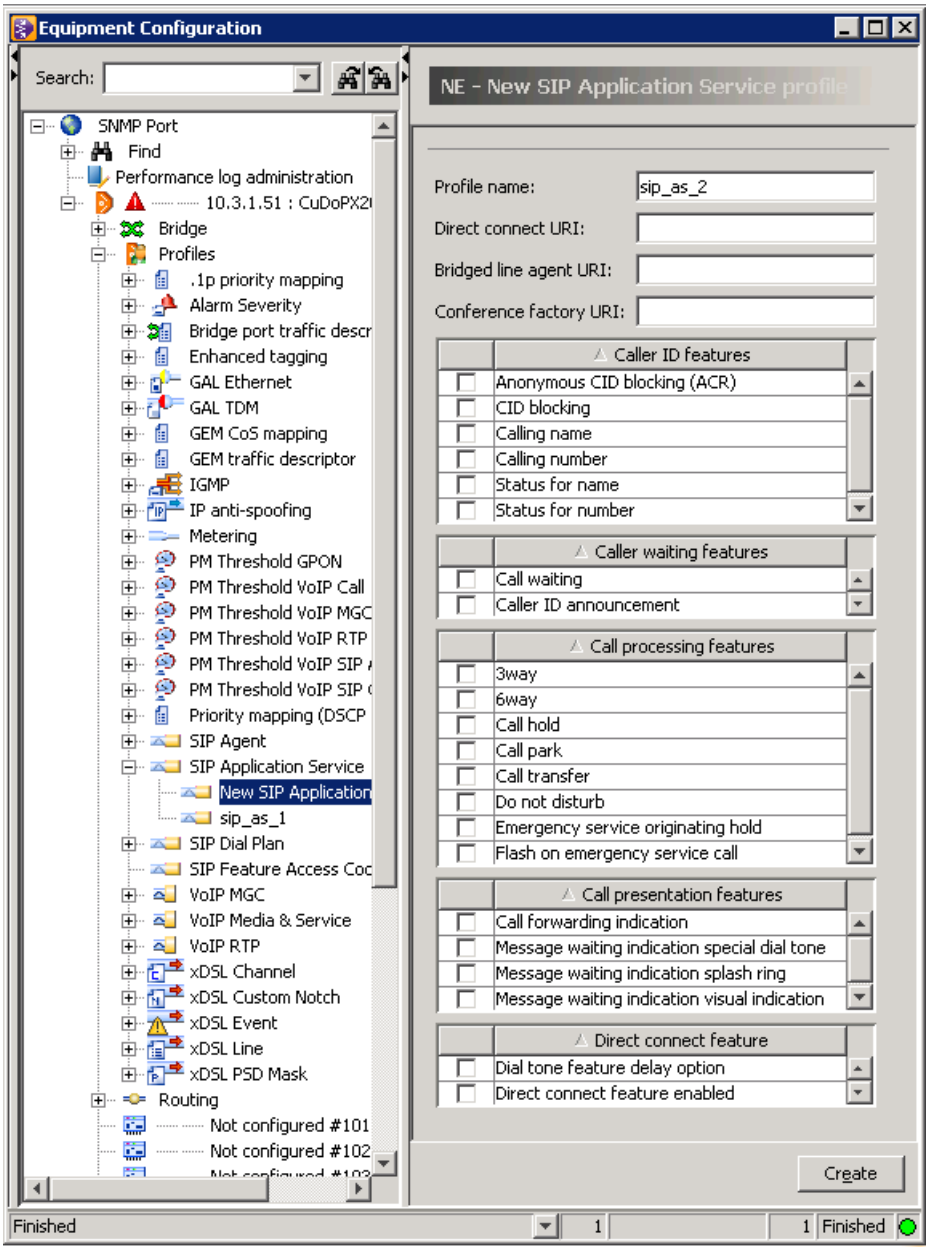

Figure 33 SIP Application Service Profile

2. Enter a unique “Profile name”.
3. Enter the URI (Uniform Resource Identifier) attributes.
   If one of the three input fields remains empty, no URI has been defined.
4. Click the check boxes of required features to enable/disable the specific functions.
5. Click the "Create" button.

11.2.4 SIP Feature Access Codes Profile

This profile defines the feature access codes for the administration of VoIP subscribers.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “SIP Feature Access Codes” profile object and select the “New SIP Feature Access Codes profile” command from the context menu.
2. Enter a unique “Profile name”.

3. Type the needed codes into the text entry fields.
4. Click the "Create" button.

11.3 Configuring Subscriber Cards

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E)” and select the “**VoIP**” tab.

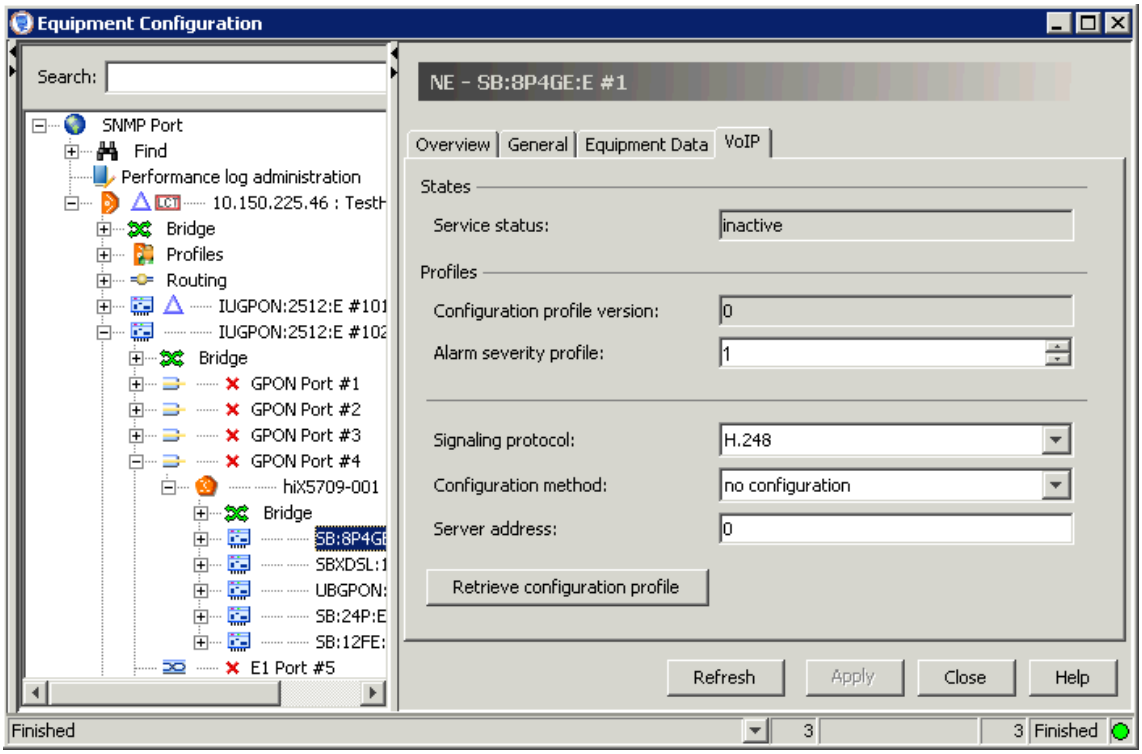

Figure 34 VoIP Subscriber Card

2. Enter the "Alarm severity profile" number.
3. Configure the options:

Setting	Description
Signaling protocol	Defines the VoIP Signaling Protocols supported in the ONT: “SIP” / “H.248” / “None” (VoIP not supported)
Configuration method	Indicates to the ONT, which method should be used to configure the VoIP Service: “no configuration” (default) or **OMCI**.
Server address	Address of the server to contact by using the method that is indicated in the “Configuration method” field.

Table 32 Setting on VoIP Subscriber Card

4. Click the "Apply" button to confirm.

11.4 Configuring the VoIP Port

The VoIP port administered configuration data of the IP interface providing the IP host services (e.g. services based on **TCP** and **UDP**).

The VoIP port configuration is required independently of whether VoIP bases on H.248 or SIP.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E) ⇨ VoIP#” to display the "**VoIP**" dialog page.
2. Fill in helpful “Information” into the text entry fields to specify this port.
3. Enter the interface data as specified in Table 33.

   If an IP address is entered, each IP address returned by **DHCP** session will be overwritten with it.

Settings	Description
IP address	Address used for all IP services hosted by this subscriber card. Default: is not set.
Subnet mask	Subnet mask for the IP services hosted by this subscriber card. Default: is not set.
Gateway address	Default gateway address used for all IP services hosted by this subscriber card. Default: is not set.
Primary DNS	Address used for the Primary DNS server for the IP service. Default: is not set.
Secondary DNS	IP address of optional secondary DNS server.
DHCP	Set a check mark to enable DHCP else configure the IP addresses.
ONT ID (DHCP)	A unique ONT identifier string. This string, if set is provided as part of the DHCP request to allow an alternative to MAC Address in retrieving the DHCP parameters of the specified ONT. The string may be up to 25 bytes long. For information see also Chapter 18.1 Configuring CXU Modes and ID Format.

Table 33 VoIP Port - Settings

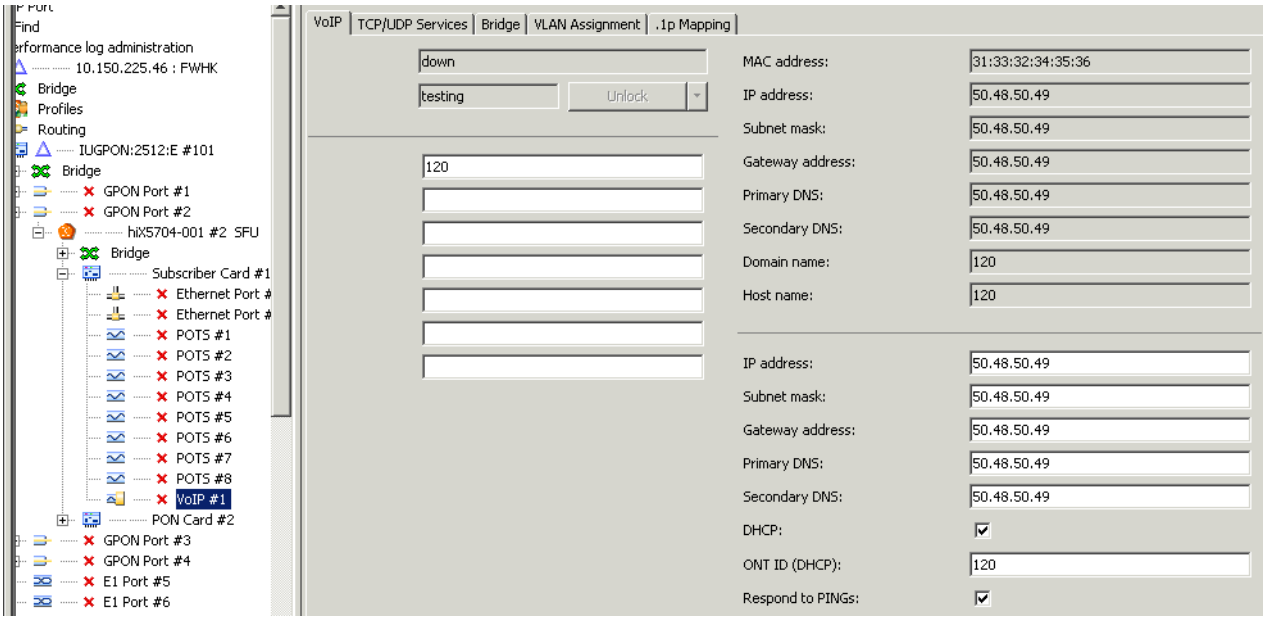

Figure 35 VoIP Port

4. Click the "**TCP/UDP Services**" tab.

   Only one source TCP/UDP port used for communication with MGC (softswitch) is supported.
5. Click the "Add >>" action field to uncover the input fields (if not already expanded).
6. Enter the UDP port number referring to the port number which offers the TCP/UDP service.

   For SIP, this UDP port number must be the same as set in SIP Agent Profile.
7. Choose the **ToS**/**DSCP** value (0..255).
8. Click the "OK" button to activate the values.

11.5 Assigning a VoIP VLAN

An existing VLAN (see Chapter 15.1 Creating a VLAN) for VoIP traffic has to be assigned to the VoIP port (if not just yet assigned). The following steps describe the configuration for SIP.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E) ⇨ VoIP#” and select the “**VLAN Assignment**” tab.
2. Click to highlight the VoIP VLAN in the “Available” selection box.
3. Click the “<<Add untagged” action field to assign the VLAN.
4. Click the “Apply” button to confirm.
5. Select the “**Bridge**” tab.
6. Choose the "**PVID**" of the VoIP VLAN for this VoIP port.
7. Click the “Apply” button to confirm.
8. Configure the settings on “**MAC VID Mapping**” tab as described in Chapter 15.3.4 MAC VID Mapping on Subscriber Port.

11.6 Configuring POTS Service via VoIP - H.248

This procedure is only necessary for **VoIP** over H.248 protocol.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E) ⇨ POTS#” and select the "**VoIP**" tab.
2. Choose the pre-configured VoIP profiles from the “MGC profile” and “Media profile” drop-down list.
3. Click the "Apply" button to confirm.

11.7 Configuring POTS Service via VoIP - SIP

The ONT/MDU terminates the POTS signaling and converts it to SIP signaling message by an SIP user agent. The following procedure is only necessary for VoIP over SIP.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E) ⇨ POTS#” and select the "**SIP**" tab.
2. Enter the needed configuration data, see Figure 36:

Setting	Description
User part of address	The user identification part of the address of record. This can take the form of an alphanumeric string or the directory number used to reference the user in the network. An empty field indicates that no user part AOR has been defined.
Display name	Customer ID used for outgoing SIP messages (ASCII string 0..25 characters).
User name	A SIP user name used for authentication (0..40).
User password	A SIP user password used for authentication (0..40).
Release timer (s)	Default: 0
ROH tone timer (s)	The length of time for the receiver off hook condition before ROH tone is applied. 0 = ROH is disabled.
Voice mail server address	IP address or URI of the SIP Voice Mail Server for SIP signaling messages. A value of 0 indicates that no Voice Mail subscription is required.

Table 34 POTS - Settings for SIP

Setting	Description
Voice mail server subscription expiration time (s)	If this value is zero, the SIP Agent will use the implementation specific default for this ONT.

Table 34 POTS - Settings for SIP (Cont.)

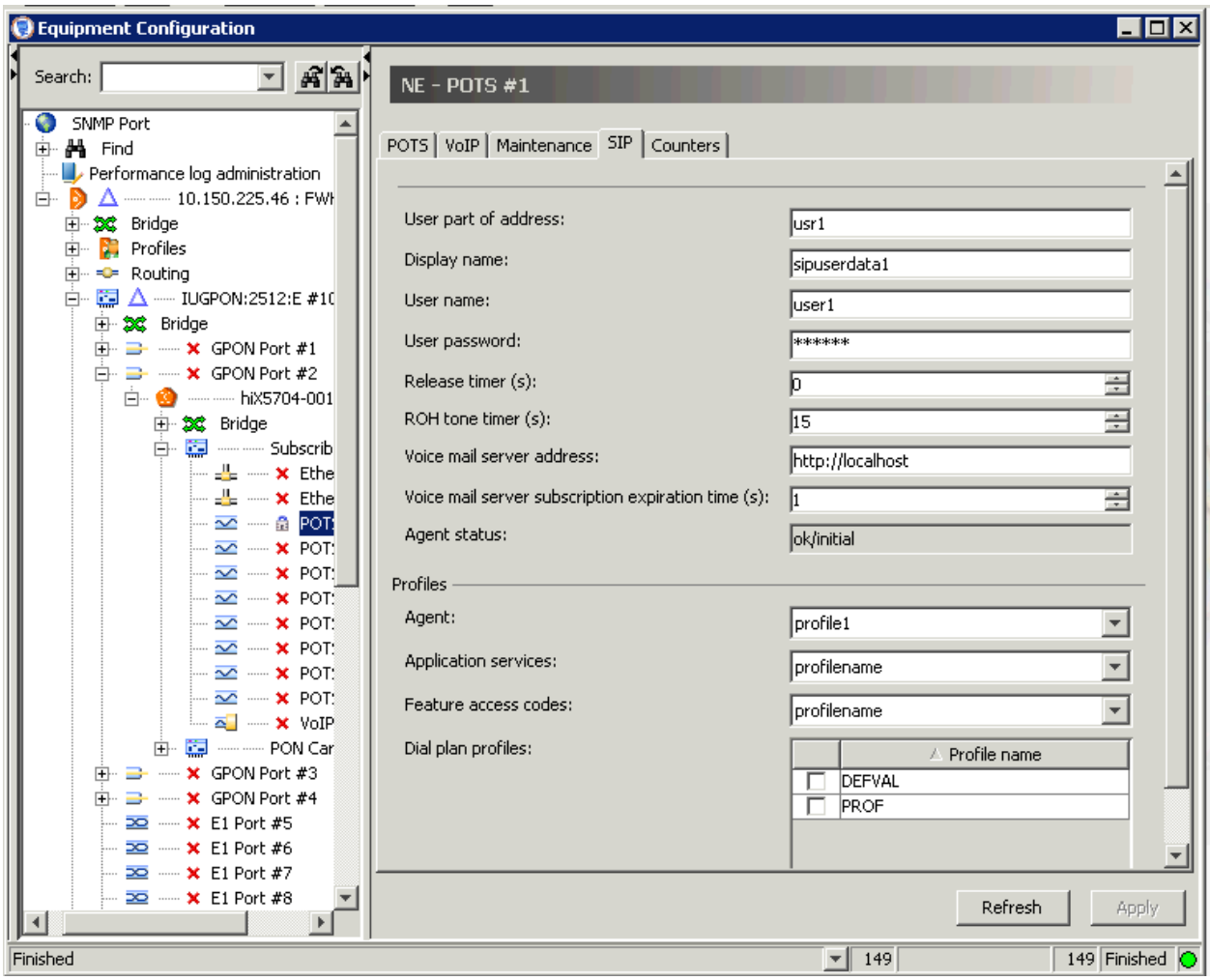

Figure 36 SIP over POTS Port

3. Choose the pre-configured SIP profiles “Agent”, “Application services”, “Feature access codes” and click to mark the needed “Dial plan profiles” check boxes.
4. Click the "Apply" button to confirm.

12 TDM Leased Line Services

The **ONT**'s **TDM** traffic is conducted transparently for the **OLT** via **E1**/**DS1** interfaces towards the backbone network. An **IU_GPON**2512:E (**ETSI** variant -A1) provides a total of 8 unstructured **E1** interfaces (2 E1 per GPON port). The interrelation between E1 ports and GPON ports on the IU_GPON as well as the ONT shows Figure 37.

The **SBU** hiX 5705 is an ONT featuring E1/DS1 interfaces.

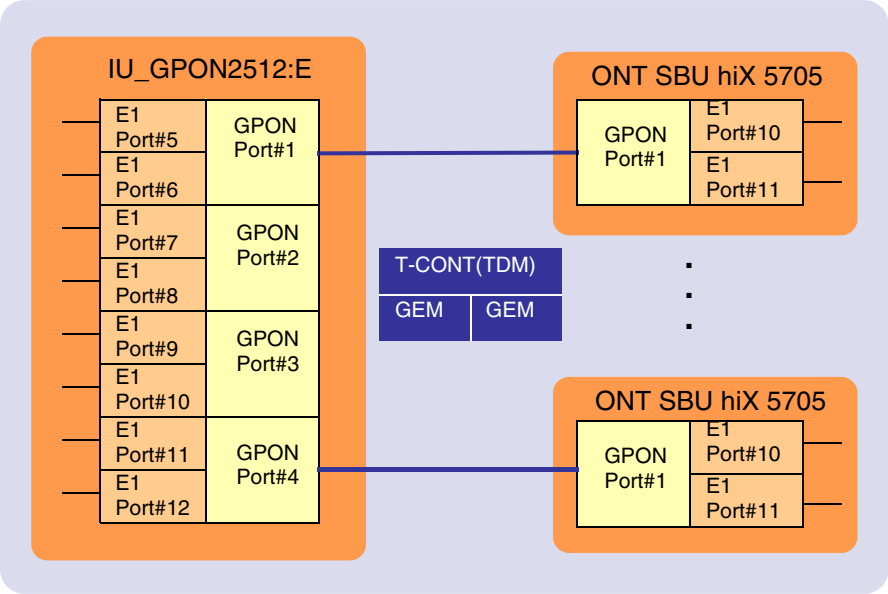

Figure 37 Assignment of E1 and GPON Ports

In order to configure the leased line service, the following configuration steps are required.

12.1 Configuring the E1 Ports of IU_GPON2512:E

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ E1 Port#” to display the “**E1**” dialog page.
2. Select the "Alarm severity profile" number (see Chapter 5.8 Configuring the Alarm Severity Profiles).
3. Fill in helpful information into the text entry fields to specify the port.
4. Click the “Apply” button to confirm the settings.

12.2 Configuring the E1 Ports of ONT

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ GPON Port# ⇨ hiX5705 SBU ⇨ Subscriber Card#2 ⇨ E1 Port#” to display the “**E1**” dialog page of the ONT's first E1 port.
2. Select the OLT connection from the "Port" drop-down list.
   T-CONT(**TDM**) is only available after assigning an E1 (DS1) connection.

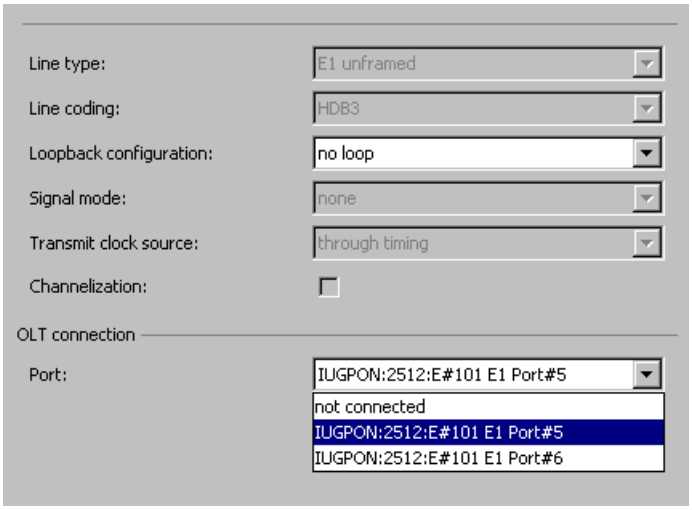

Figure 38 E1 Assignment

3. Fill in helpful information into the text entry fields to specify the port.
4. Select the "Alarm severity profile" number (see Chapter 5.8 Configuring the Alarm Severity Profiles).
5. **Only for the DS1 (ANSI) port configuration:**
   Choose the “Line coding” between “AMI” and “B8ZS”.
   E1 line coding is fixed set on “HDB3”.
6. Click the "Apply” button to confirm the settings.
7. Configure the ONT’s second E1 port.

Loopback Configuration

For trouble-shooting and debugging support the ports can be set into loopback mode according to the line segment that must be tested.

Setting	Description
no loop	default
Payload loop	Loop is used for testing the E1 network side The received signal at this interface is looped through the device. Typically the received signal is looped back for retransmission after it has passed through framing function of the device.
Line loop	Loop is used for testing including the optical network side The received signal at this interface does not go through the device (minimum penetration) but is looped back out.

Table 35 Loopback Configuration

13 MAC Mode

The **MAC** mode defines how the IU_GPONs map the Ethernet frames to different **GEM** port **ID**s in the downstream direction.

1. Click “NE:hiX5750 ⇨ Bridge”.

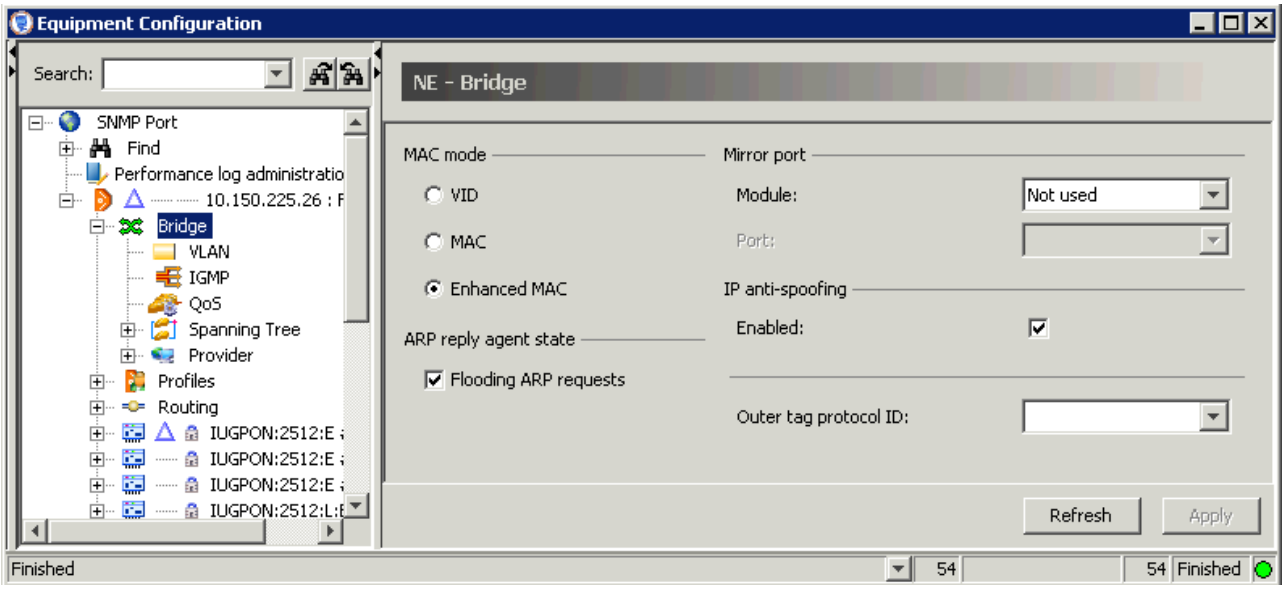

Figure 39 MAC Mode

2. Choose the "MAC Mode”:

Mode	Description
Enhanced MAC	The MAC mode depends on the only / inner upstream **UNI** VLAN tag. The GPON MAC defines the translation to the upstream **NNI** VLAN tag(s). The enhanced MAC functionality supports 1:1 (VLAN cross-connect = VLAN per customer and service) and N:1 (VLAN per service, common for all subscriber) switching models per GPON port of OLT simultaneously (MAC mode and VID mode per one port).
MAC	For **DS** frames the **GEM** ID is set dependent on the destination MAC address. The mapping of one or more destination MAC addresses to a GEM ID is learned from **US** frames. The mapping of one or more VLANs to a GEM ID must be configured and is used only for the US direction. VLAN translation between subscriber VLANs and service based VLANs is possible.
VID	For US/DS frames the GEM ID is set dependent on the outer VLAN tag. The mapping of one or more VLANs to a GEM ID must be configured and is used for both US and DS direction. VLAN translation between subscriber VLANs and service based VLANs is not possible. This mode is used for port based VLAN scenarios (1:1).

Table 36 MAC Modes

For changing the MAC mode, the CXU must be unlocked and all interface units (IU_GPON, IU_1x10G, IU_10x1G) must be locked, see Chapter 27 Lock / Unlock Ports.

3. Click the "Apply” button to confirm.

The change to the enhanced MAC mode occurs without influence on the performance of existing VLANs. To continue the traffic flows without interruption, at first all VLANs have to be set on the N:1 bridge mode. An additional profile needs to be configured (see Chapter 15.3.1 Creating an 802.1p Priority Mapping Profile) and addi-

tional VLAN settings are required for the bridge ports (see Chapter 15.3 Configuring an 1:1 VLAN Cross-Connect).

See the following chapters to get detailed information on the other settings on this dialog page:

- 26 VLAN Mirroring
- 22.2 IP Anti-Spoofing
- 14.2.2 Outer Tag Protocol ID.

14 Bridges

The configuration steps described in the following chapters decide about the VLAN operation mode of the hiX 5750 R2.0 in a certain VLAN scenario.

The supported VLAN operation modes are:

Setting	Description
VLAN switching	All frames are flooded in their VLANs.
Independent VLAN learning	The bridge maintains a MAC table to learn the information per each VLAN separately. The traffic is only forwarded to learned MAC addresses. MAC address information learned in one VLAN cannot be used in filtering decisions taken relative to any other VLAN.
Shared VLAN learning	Not supported in this release.

Table 37 Switching Modes

14.1 Configuring the CXU Bridge

14.1.1 Switching Mode and Tagging Mode

1. Click “NE:hiX5750 ⇨ CXUVR:1O:4E:E#109 ⇨ Bridge”.
2. Choose the "Switching mode”, see Table 37.

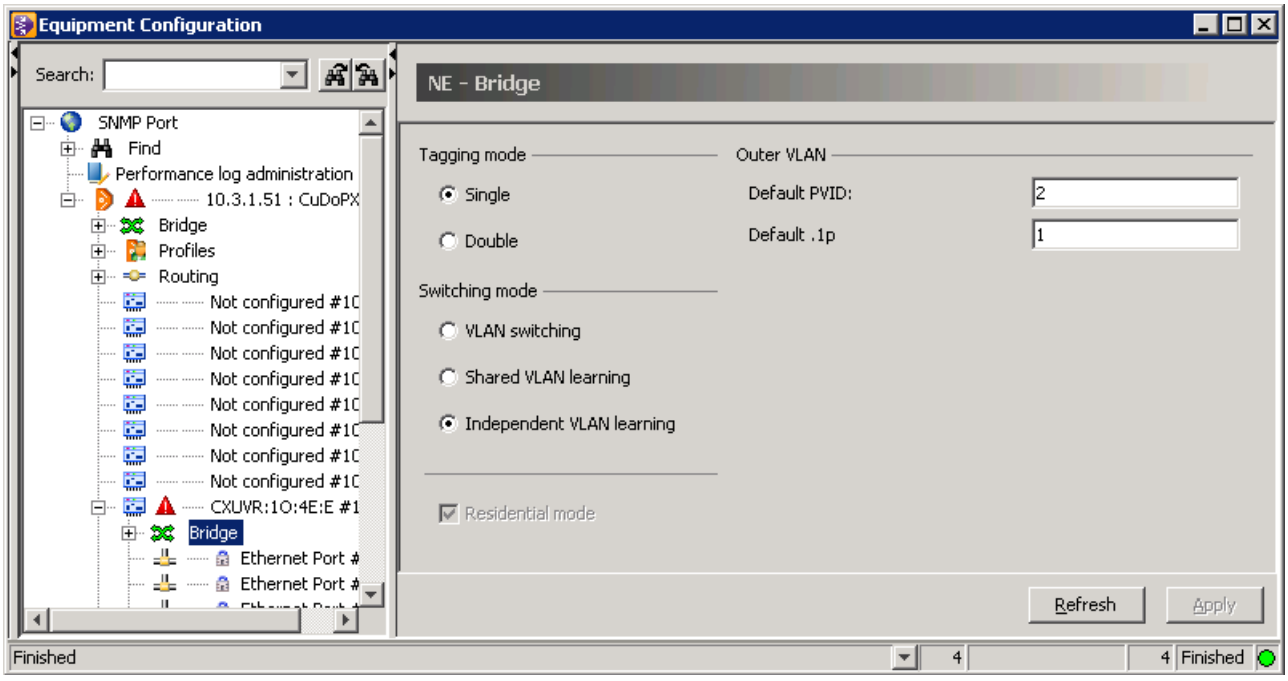

Figure 40 CXU Bridge

3. Click the "Apply” button to confirm.

See the following chapters for information on the further bridge configurations:

- 19 IGMP
- 25 Rules
- 24 Link Aggregation Groups.

14.1.2 Ethernet Ports

Configure CXU Ethernet ports depending on the used VLAN scenario.

1. Click “NE:hiX5750 ⇨ CXUVR:1O:4E:E#109 ⇨ Ethernet Port#” and select the “**Bridge**” tab.
2. Enter the "PVID" of the associated VLAN or follow the “Configure VLAN” link to create a new VLAN.

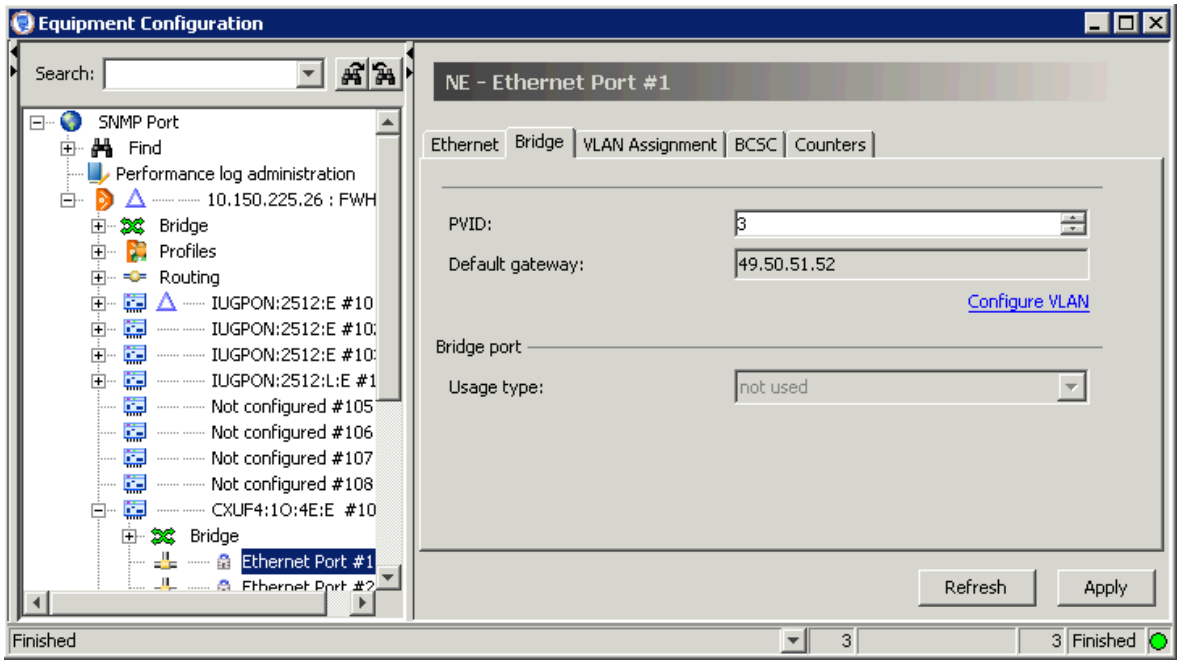

Figure 41 Bridge CXU Uplink Ports

3. Click "Apply” button to confirm.

The “Usage type” of the Ethernet ports must be “uplink” (default setting).

14.2 Configuring the IU_GPON Bridge

14.2.1 Switching Mode and Tagging Mode

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ Bridge”.
2. Choose the "Switching mode”, see Table 37.

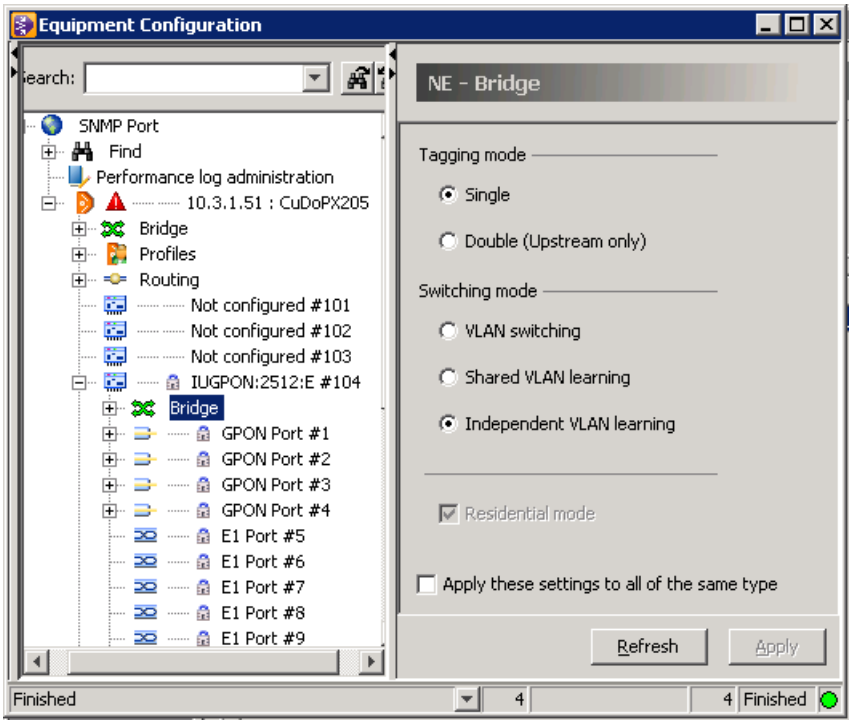

Figure 42 IUGPON Bridge

3. Choose the general "Tagging mode" of the IU_GPON bridge.
   When the IU_GPON bridge is set in double tagging mode, a second outer tag will be added in upstream frames at the edge per GPON link. Double tagging affects only the GPON interfaces not the interlink interfaces to the CXU.
4. If necessary, click to mark the "Apply these settings to all of the same type" check box in order to make these settings effective for all IU_GPON cards of the same type.
5. Click the "Apply" button to confirm.

See the following chapters for information on the further bridge configuration:

- 19 IGMP
- 25 Rules.

14.2.2 Outer Tag Protocol ID

For upstream frames tagged with a second VLAN (802.1Q) tag by the IU_GPON (or IU10x1G), the Ethertype of outer tag can be configured. If double-tagging mode is configured on the **IU**'s bridge, the **NE** uses this value only for bridge ports of OLT GPON interfaces (OLT downlink Ethernet interfaces).

1. Click “NE:hiX5750 ⇨ Bridge” to display the “**NE Bridge**” dialog page (see Figure 39).
2. Choose the "Outer tag protocol ID” to set the outer tag of Ethertype: 0x8100 (default), 0x88a8, 0x9100, 0x9200.
3. Click the “Apply” button to confirm.

14.2.3 GPON Bridge Ports

1. Click “NE:hiX5750 ➪ IUGPON2512:E# ➪ Bridge ➪ GPON Port#” and select the “**Bridge**” tab.

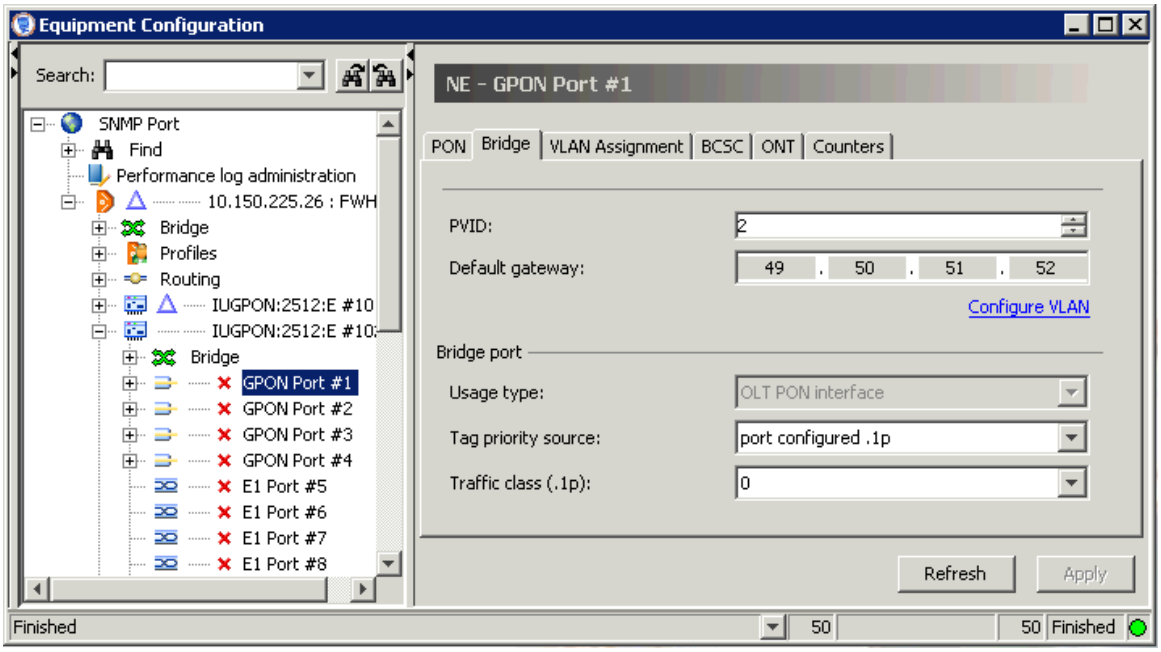

Figure 43 GPON Bridge Ports

2. Enter the "PVID" of the associated VLAN or follow the “Configure VLAN” link to create a new VLAN.
3. Choose the priority value of the bridge port.

Setting	Description
Tag priority source	“port configured .1p”: configured per bridge port value. This is the default setting.
Traffic class (.1p)	Default priority of the bridge port. Used if “Tag priority source” is set to “port configured .1p” (default). Range: 0...7

Table 38 GPON Port - Priority

If a tag is added to upstream user frames, the .1p priority bits will be set according to the “Tag priority source”.

4. Click the "Apply” button to confirm.

14.3 Configuring the IU_1x10G Bridge

Configure the bridge as described in Chapter 14.1 Configuring the CXU Bridge on page 76.
Only “VLAN switching” and tagging mode “Single” are possible.
If necessary, click to check mark the "Apply these settings to all of the same type” box to make these settings effective for all IU_1x10G cards.

See Chapter 25 Rules for information on the further bridge configuration.

14.4 Configuring the IU_10x1G Bridge

Configure the bridge as described in Chapter 14.2 Configuring the IU_GPON Bridge on page 77.
If necessary, click to check mark the "Apply these settings to all of the same type" box to make these settings effective for all IU_10x1G cards.

14.5 Configuring ONT/MDU Bridge Ports

The configuration steps of bridge ports depend on the specific port type.

14.5.1 Priority Mapping (DSCP to .1p) Profile

A profile for mapping a **DSCP** value to .1p value will be used if a tag is added to an upstream user frame (when bridge port tagging mode is untagged or transparent) and port priority option is DSCP. If a tag is already part of incoming upstream user frame (when bridge port tagging mode is tagged) and priority is DSCP, the profile will be used to filter the frames with allowed .1p priority bits.

The use of priority mapping profiles depends on the ONT type. Please refer to the release notes delivered with the hiX 5750 R2.0 in order to choose supported values.

1. Click "NE:hiX5750 ⇨ Profiles ⇨ Priority Mapping (DSCP to .1p)", right-click the "Priority Mapping (DSCP to.1p)" profile object and select the "New Priority mapping profile" command from the context menu.

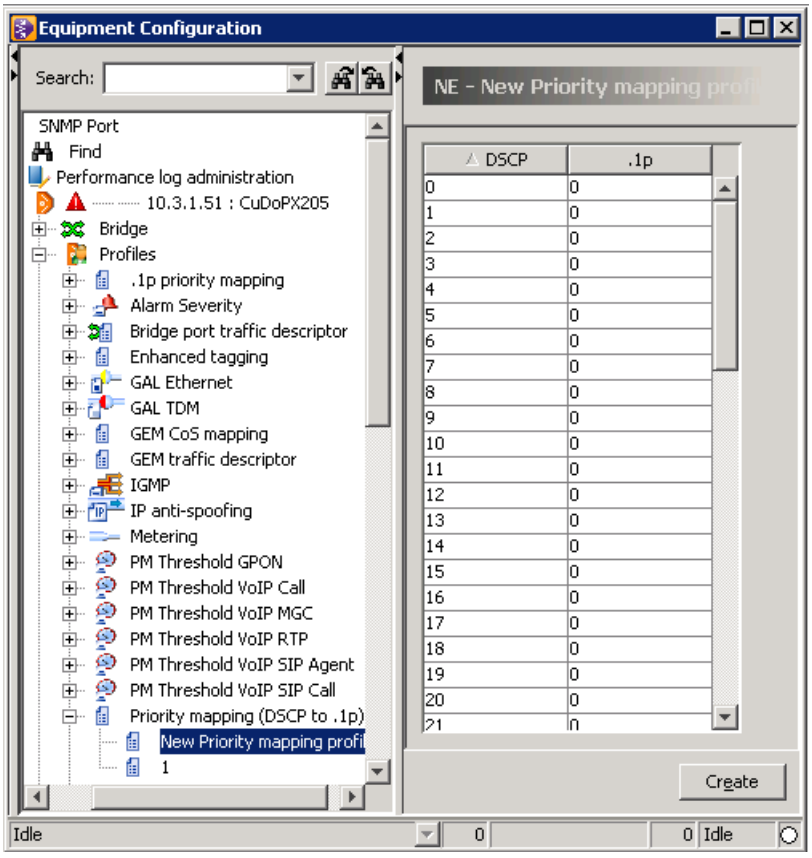

Figure 44 Priority Mapping Profile

2. Double-click the ".1p" fields to choose the priority values.

3. Click the “Create” button to insert the new profile (index).

14.5.2 Traffic Descriptor Profile

The hiX 5750 R2.0 supports traffic limitation per bridge port as specified in Table 39.

Type	Egress Rate Limiting	Ingress Rate Limiting
MDU hix 5709 R2.0	Shaping downstream for xDSL	Policing downstream for GE and xDSL, upstream for xDSL per **PVC**,
G-25A SFU	Shaping downstream for GE	-
G-25E SFU		

Table 39 Bridge Port Shaping and Policing

There are different traffic descriptor profiles configurable for in-bound and out-bound traffic. The out-bound traffic descriptor describes the limitations of traffic rates for frames leaving the **MAC** bridge upstream (traffic shaping towards the **UNI**). The in-bound descriptor describes the limitations of traffic rates for frames entering the MAC bridge downstream (traffic policing towards the **ANI**).

A traffic descriptor profile can be only created but afterwards the values cannot be changed anymore.

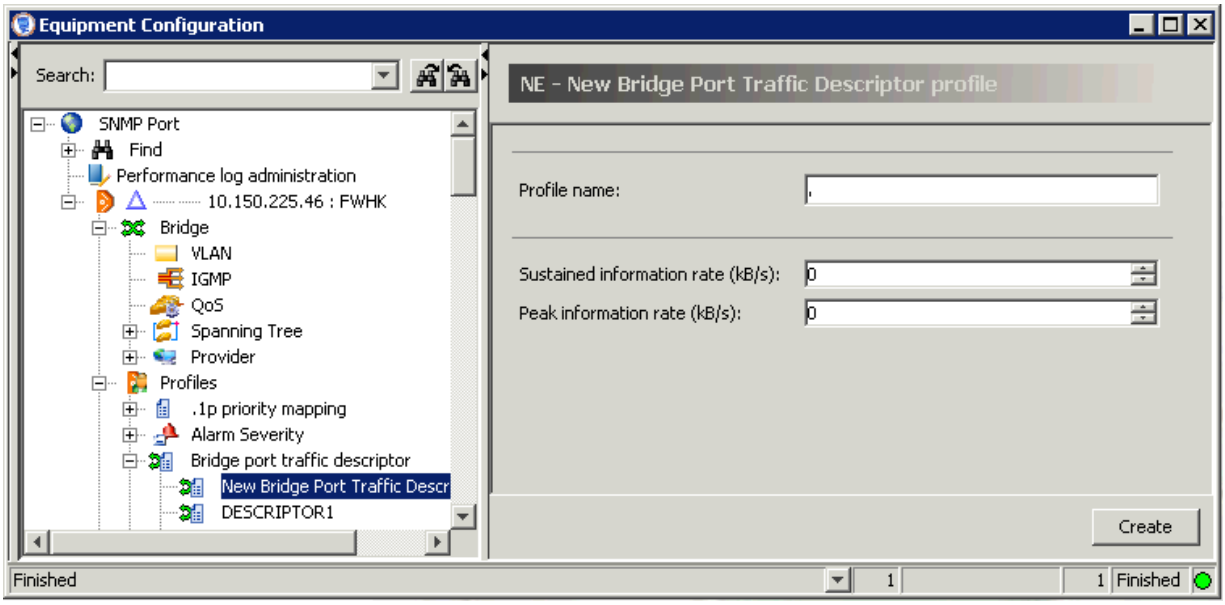

Figure 45 Bridge Port Traffic Descriptor

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “Bridge Port Traffic Descriptor” profile object and select the “New Bridge Port Traffic Descriptor profile” command from the context menu.
2. Enter a unique “Profile name”.
3. Enter the “Peak information rate” and “Sustained information rate” values from the range of 0 to 150,000 KBytes/sec.
4. Click the “Create” button.

14.5.3 Enhanced Tagging for MDU hiX 5709

The configuration of MDU subscriber ports to enhanced tagging of upstream frames can be divided into the tasks:

1. Creating Tagging Rules
2. Creating an Enhanced Tagging Profile
3. Enabling the tagging mode “enhanced” and assigning an enhanced tagging profile to the port (see Chapter 14.5.4 Subscriber Bridge Ports).

Creating Tagging Rules

The behavior of MDU bridge ports regarding tagging of upstream traffic can be defined by specific tagging rules, e.g. for VLAN translation. Each tagging rule consists of a filtering part and a treatment part. The filtering part must be unique.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Rules”.
2. Click the “New>>” action field to uncover the selection fields (if not already expanded).

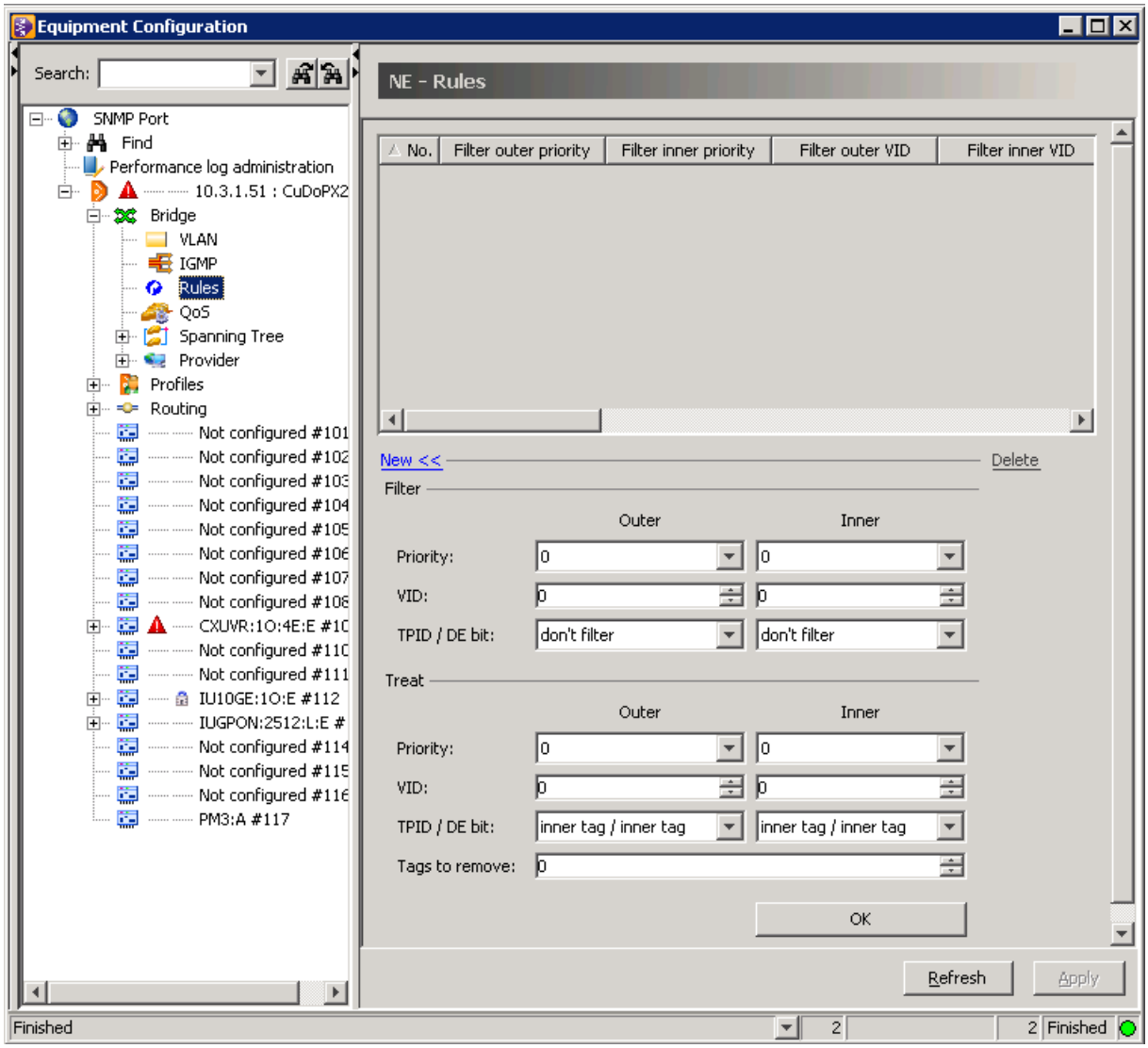

Figure 46 Tagging Rule

3. Choose the filter conditions for the frames transmitted in outer and inner VLAN:

Setting	Description
Priority	The outer/inner priority value on which to filter the received frames and some special functions. “0-7”: the value is used as the given outer/inner priority to filter the received frames “don’t filter”: indicates not to filter on outer/inner priority “default filter”: - Outer: indicates the default filter when no other double-tag rule matches - Inner: indicates the default filter when no other single-tag rule matches “no-tag filter”: - Outer: indicates that this entry is not a double-tag rule, and all other outer/inner tag filter fields should be ignored - Inner: indicates that this entry is the no-tag rule.
VID	The outer/inner VID value on which to filter the received frames and some special functions. 0000-4094: the value is used as the given outer/inner VID value to filter the received frames 4096: indicates not to filter on the outer/inner VID.
TPID / DE bit	The outer/inner TPID (Tag Protocol Identifier) value on which to filter the received frames and some special functions. “don’t filter”: don’t filter on outer/inner TPID field “0x8100/-”: outer/inner TPID = 8100 “Input TPID/don’t care”: outer/inner TPID = InputTPID, don’t care about DE bit “Input TPID/0”: outer/inner TPID = InputTPID, DE=0 “Input TPID/1”: outer/inner TPID = InputTPID, DE=1.

Table 40 Tagging Rule - Filters

4. Choose the tread conditions for the frames transmitted in outer and inner VLAN:

Setting	Description
Priority	The priority value for use in the outer/inner VLAN tag or some special functions. 0-7: the value is used as the given priority to insert in the outer/inner VLAN tag “use inner priority”: - Outer: the outer priority is to be copied from the inner priority of the received frame - Inner: the inner priority is to be copied from the inner priority of the received frame “use outer priority”: - Outer: the outer priority is to be copied from the outer priority of the received frame - Inner: the inner priority is to be copied from the outer priority of the received frame “don’t add”: Do not add an outer/inner tag.
VID	The VID to use in the outer/inner VLAN tag or some special functions. 0000-4094: the value is the VID to use in the outer/inner VLAN tag 4096: the outer/inner VID is to be copied from the inner VID of the received frame 4097: the outer/inner VID is to be copied from the outer VID of the received frame.
TPID / DE bit	The TPID value to use in the outer VLAN tag or some special functions. “inner tag / outer tag”: TPID (and DE, if present) copied from inner tag of received frame “outer tag / inner tag”: TPID (and DE, if present) copied from outer tag of received frame “output TPID / inner tag”: TPID = OutputTPID, and DE copied from inner tag of received frame “output TPID / outer tag”: TPID = OutputTPID, and DE copied from outer tag of received frame “0x8100/-”: TPID = 0x8100 “output TPID/0”: TPID = OutputTPID, DE=0 “output TPID/1”: TPID = OutputTPID, DE=1.
Tags to remove	Used to indicate initial treatment of the received frames. The chosen value indicates that 0, 1, or 2 tags, respectively, are to be removed. If one tag is specified, then it is the outer tag that should be removed.

Table 41 Tagging Rule - Treads

5. Click the "OK” button to create the new tagging rule.

Creating an Enhanced Tagging Profile

An enhanced tagging profile to be assigned to ONT subscriber bridge ports contains a list of up to 6 tagging rules. Each upstream incoming packet is matched against each rule, in list order. The first rule that matches the packet is selected as the active rule, and the packet is then treated according to this rule.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Profiles”, right-click the “Enhanced tagging” profile object and select the “New Enhanced tagging profile” command from the context menu.
2. Enter a unique “Profile name”.
3. Choose the following options:

Setting	Description
Input TPID (hex)	Special TPID value for operations on the input (filtering) side. For example: 0x8a88 and 0x9100.
Output TPID (hex)	Special TPID value for operations on the output (tagging) side. For example: 0x8a88 and 0x9100.
Downstream mode	“up and down”: the operation performed in the downstream direction is the inverse of that performed in the upstream direction. For one-to-one VLAN mappings, the inverse is trivially defined. Multi-to-one mappings are possible; however, and these are treated as follows. If the multi-to-one mapping results from multiple operation rules producing the same **ANI**-side tag configuration, then the first rule in the list will be used to define the inverse operation. If the multi-to-one mapping results from 'Don’t care' fields in the filter being replaced with provisioned fields in the ANI-side tags, then the inverse is defined to set the corresponding fields on the ANI-side with their lowest value. “up only”: no operation is performed in the downstream direction.

Table 42 Tagging Profile

4. Click to mark the “Tagging rule” check boxes in order to select pre-configured tagging rules to be assigned to subscriber ports with this profile.
5. Click the “Create” button to insert the new tagging profile.

14.5.4 Subscriber Bridge Ports

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU SB:8P4GE:E) ⇨ Ethernet Port# (xDSL Port#)” and select the “**Bridge**” tab.

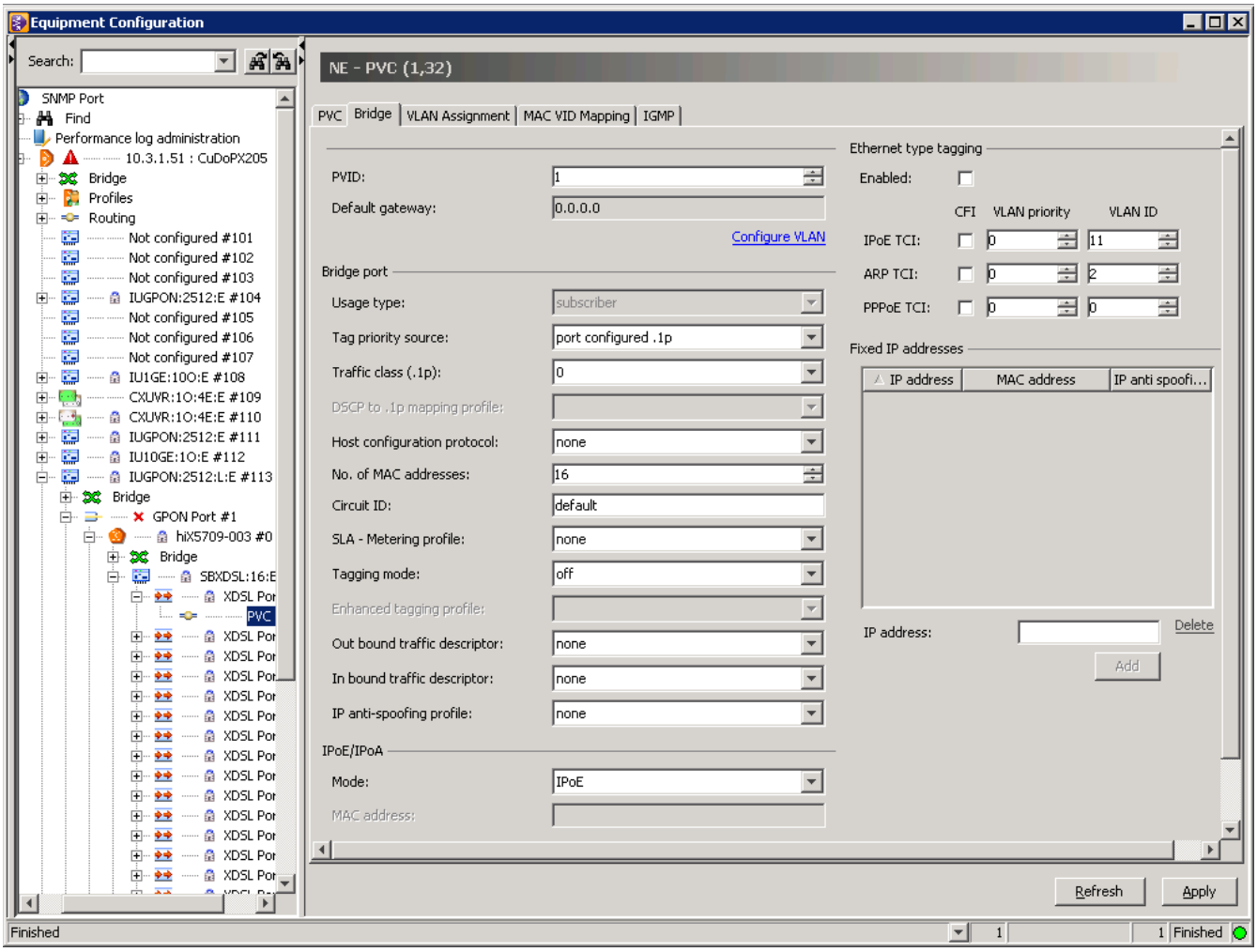

Figure 47 Subscriber Bridge Port (xDSL)

2. Choose the "Tagging mode":

Mode	Description
untagged	A VLAN ID has to be entered into "**PVID**" field. • Upstream: allowed untagged frames and dropped tagged frames • Upstream: add tag with configured PVID per port • Downstream: strip tag. This is the default setting for subscriber ports.
tagged	Only frames with the configured VID are forwarded. • Upstream: allowed tagged frames and dropped untagged frames and frames with unknown VIDs • Downstream: keep existing tag.
transparent	Can be used for QinQ mode. • Upstream: allowed with VID tagged and untagged user frames, • Upstream: add always a tag with configured PVID (untagged frames forwarded with single tag, tagged frames with double tag) • Downstream: strip outer tag.

Table 43 ONT Tagging Modes

Mode	Description
enhanced	Tagging depends on tagging rules specified in enhanced tagging profile. This mode is only available for the MDU hiX 5709.

Table 43 ONT Tagging Modes (Cont.)

One basic rule is that the **ONT** always add only one tag in upstream direction. If an additional outer tag for untagged user frames is necessary (double tagging) this tag must be added at the **OLT**. Additional, the outer tag can be translated by a rule, see Chapter 25 Rules.

3. Only, if the “Tagging mode “ of an MDU hiX 5709 is set on “enhanced”, the “Enhanced tagging profile” can be chosen.
4. Choose the bridge port priority values:

Setting	Description
Tag priority source	“port configured .1p”: configured per subscriber bridge port value. This is the default setting. “DSCP”: according DSCP of IP header.
Traffic class (.1p)	Default priority of the bridge port that is used if a tag is added to an upstream user frame (when “Tagging mode” is untagged or transparent) and “Tag priority source” is set to “port configured .1p” (default). Range: 0...7
DSCP to .1 mapping profile	In case of tag priority source DSCP, a 14.5.1 Priority Mapping (DSCP to .1p) Profile has to be selected.

Table 44 Subscriber Port Priority

Valid settings for handling the .1p priority bits depend on the “Tagging mode” of the bridge.

All subscribers of one ONT subscriber card (MDU service board) must use the same DSCP profile. Only one profile per ONT subscriber card is possible.

5. Choose the “Host configuration protocol” and “Circuit ID” (see Chapter 18 DHCP and PPPoE).
6. Select “Out bound traffic descriptor” and “In bound traffic descriptor” from the corresponding drop-down list. The respectively 14.5.2 Traffic Descriptor Profile contains the options for the shaping and policing of the traffic.

There are additional settings only for the MDU’s xDSL ports to enable or disable tagging according Ethertype independently from the chosen tagging mode of those bridge port.

7. Click the “Enable” check box to activate Ethernet type tagging.
8. Configure the needed TCI (Tag Control Identifier) values. The TCI consists of CFI (Canonical Format Indicator, 1 bit), “VLAN priority”, and “VLAN-ID”:

TCI	Description
IPoE	Upstream frames matching the Ethertype 0x0800 IP Internet Protocol (IPv4) are tagged with this TCI value (VLAN and priority).
ARP	Upstream frames matching the Ethertype 0x0806 Address Resolution Protocol (ARP) are tagged with this TCI value (VLAN and priority).
PPPoE	Upstream frames matching one of the Ethertypes for PPPoE (0x8863 PPPoE Discovery, 0x8864 PPPoE Session) are tagged with this TCI value (VLAN and priority).

Table 45 Ethertype Type Tagging

All frames not matching the activated condition are forwarded unchanged.

9. Click the "Apply" button to confirm.

14.5.5 .1p Priority Mapping on GEM Port Level

If necessary, the .1p priority can be changed on **GEM** port level.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU Service Board) ⇨ Subscriber Port” and select the “**.1p Mapping**” tab.
2. Change the preset values as needed after clicking the corresponding “GEM port ID” selection field.
3. Click the “Apply” button to confirm.

15 VLAN

15.1 Creating a VLAN

1. Click “NE:hiX5750 ⇨ Bridge ⇨ VLAN” to display the "**Overview**" page.
2. Click the "New>>” action field to uncover the VLAN configuration fields (if not already expanded).

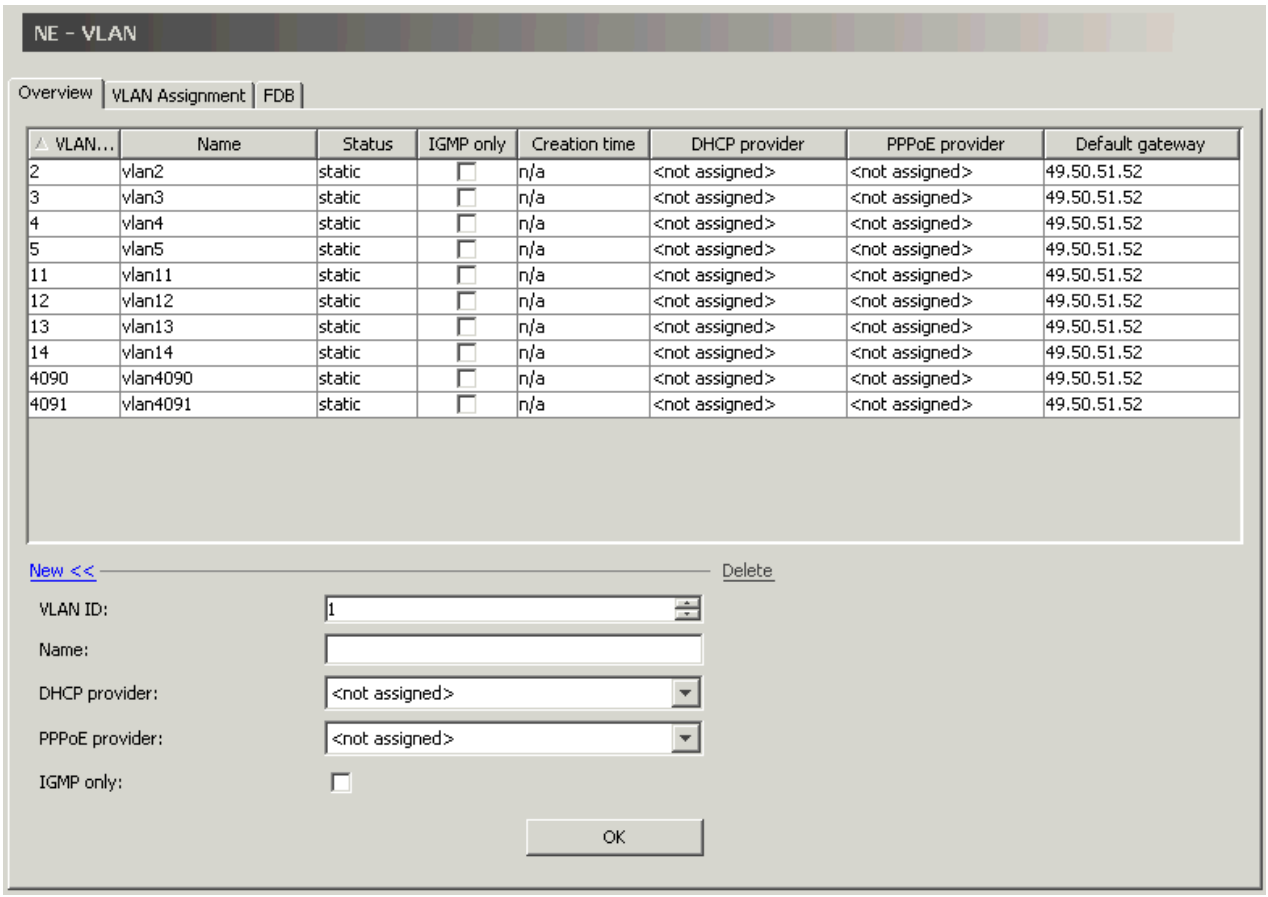

Figure 48 VLAN Configuration

3. Choose the **VLAN ID**.
4. Enter a unique name (space : ? are not allowed).
5. If necessary, choose a pre-configured "DHCP provider" and "PPPoE provider" from the corresponding drop-down list (see Chapter 18 DHCP and PPPoE).
6. Click the "**IGMP** only" check box to create a VLAN that transmits only multicast traffic or IGMP requests.
   This setting requires a CXU running in IGMP proxy mode (see Chapter 19 IGMP).
7. Only when the enhanced MAC mode was selected, additional VLAN operation modes can be configured (see Chapter 13 MAC Mode).
   Choose the VLAN operation mode from the “MAC mode” drop-down list.
   To convert the mode of an existing VLAN, click into the “MAC mode” field of the overview chart and choose the needed mode.

Setting	Description
N:1 change VLAN per C-tag	N:1 VLAN per service, means several subscriber share one VLAN for one service. GPON MAC uses the VLAN/MAC address to find the right **GEM**-port ID in downstream direction. In upstream direction the GPON MAC learns the relationship part of GEM-port ID to VLAN/MAC. The classifier for the **CoS** are the .1p priority bits.
1:1 CC add outer per C-tag	1:1 VLAN cross-connect mode. The c-tag coming from **UNI** side contains the service information, i.e. the user frame is already tagged with a VLAN-ID per service. The inner c-tag contains the UNI information and the outer s-tag contains the service information. The GPON MAC is translating the c-tag information coming from UNI to the related s-tag information at the **NNI** and the UNI-port related GEM-port ID part into the outer s-tag VID at the NNI side. The priority can be set per GEM-port.

Table 46 VLAN Operation Modes

8. Click the "OK" button to activate the settings.

15.2 Assigning VLANs to Ports

1. Click “NE:hiX5750 ⇨ Bridge ⇨ VLAN” and select the “**VLAN Assignment**” tab.

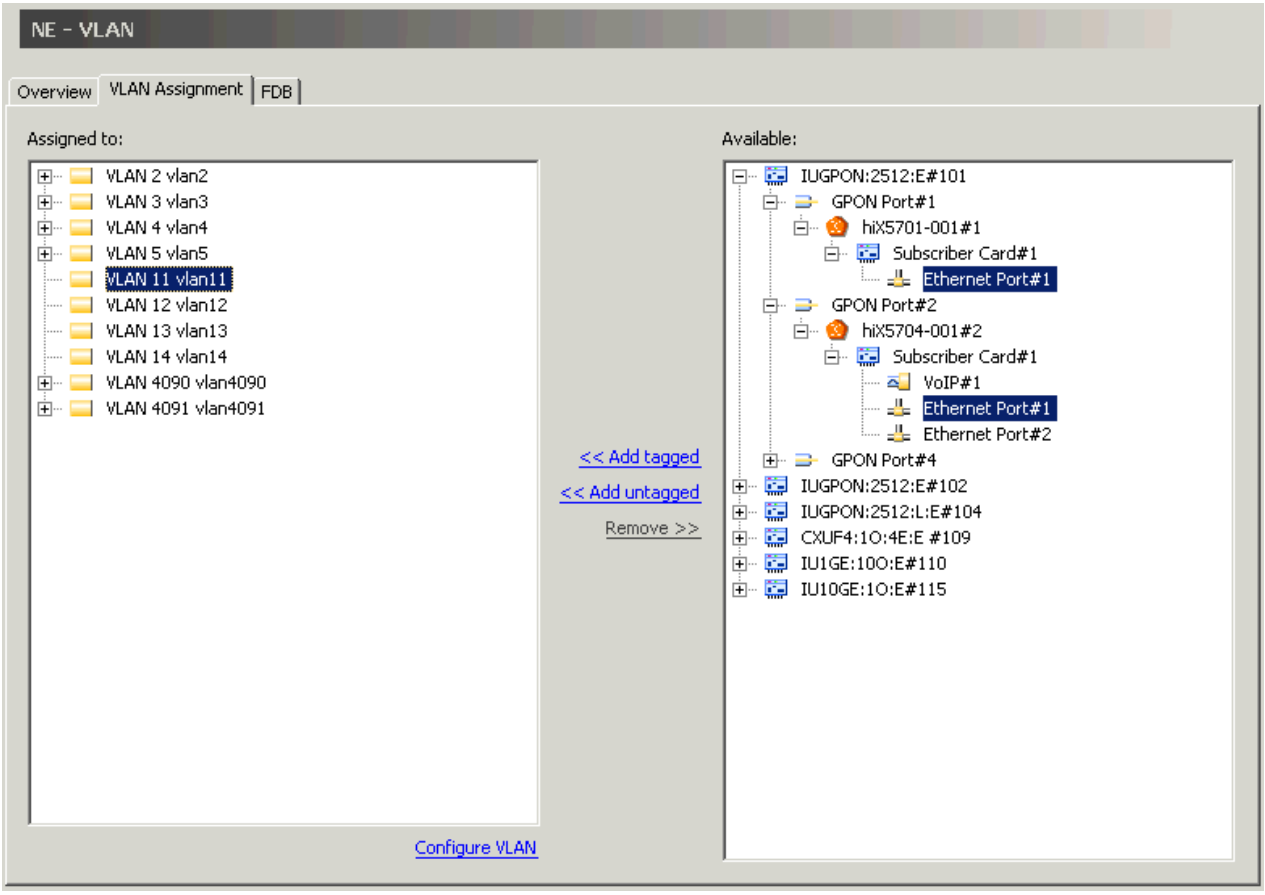

Figure 49 VLAN Assignment (Example MAC Mode)

2. Repeat the following steps for the created VLANs:

   To select several objects (ports, VLANs), press the Ctrl key while clicking the object icons.

   - In the "Assigned to" dialog box :
     Click to highlight the VLANs that must be assigned to the port(s).

- In the "Available" dialog box :
  Click to highlight all ports that must be associated with the marked VLANs.
- In case of “N:1 change VLAN per C-tag” mode:
  Click the “Enhanced MAC mode>>” action field to configure the “Outer VID” (VLAN ID of the only tag at the NNI that must be changed). The upstream MAC mode of this VLAN can be unlike the MAC mode handling the inner VID.
  The “Outer priority profile” sets the values as specified in the “.1p Priority mapping profile” (see Chapter 15.3.1 Creating an 802.1p Priority Mapping Profile on page 90).

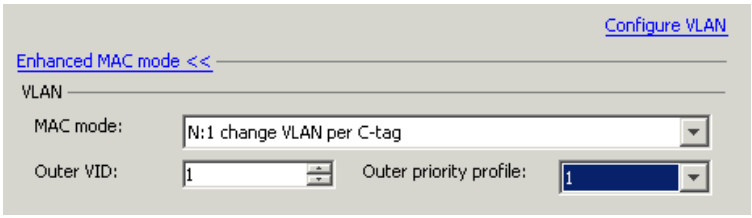

Figure 50 Enhanced MAC Mode Entries

- Select the behavior of egress port:
  - Click the “<<Add tagged” action field in order that the specified port sends tagged frames.
  - Click the “<<Add untagged” action field in order that the specified port sends untagged frames.

  To change the mode (tagged, untagged) of a port, this port must be removed from the VLAN and added again with the appropriate mode.

3. Click the "Apply" button to confirm all settings.

15.3 Configuring an 1:1 VLAN Cross-Connect

The mapping of cross-connect VLANs has to be configured per GPON port and per subscriber port.

15.3.1 Creating an 802.1p Priority Mapping Profile

If the enhanced MAC mode is set, configure the .1p priority mapping profile for the VLAN operation mode (only one profile available). The profile settings operate globally for all VLANs.

1. Click “NE:hiX5750 ⇨ Profiles ⇨ .1p priority mapping ⇨ 1”.

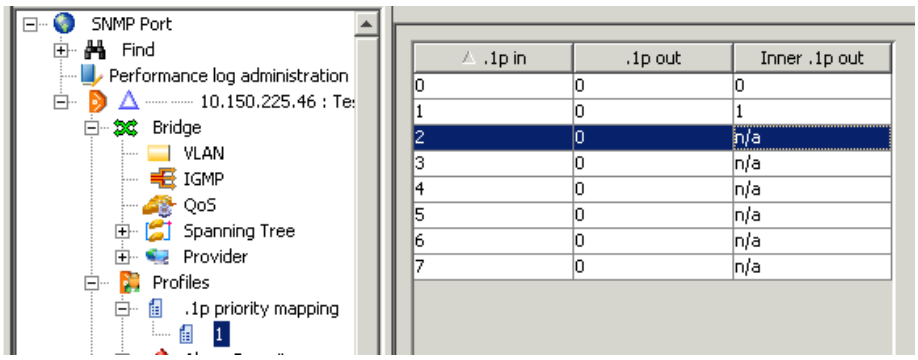

Figure 51 .1p Priority Mapping Profile

2. Double-click into the columns ".1p out" and "Inner .1p out" and enter the priority values according to the planning documentation.

Setting	Description
.1p in	Inner .1p priority (inner VID)
.1p out	Outer .1p priority (outer VID): the only tag at the **NNI** if the NNI is single tagged.
Inner .1p out	Priority of the inner tag at the NNI.

Table 47 .1p Priority Mapping Profile

3. Click the “Apply” button to confirm.

15.3.2 MAC VID Mapping on GPON Port

Perform the following steps to establish a cross-connect (CC) VLAN over GPON link.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port#” and select the “**MAC VID Mapping**” tab.
2. Click the “Create>>” action field to uncover the configuration fields (if not already expanded).

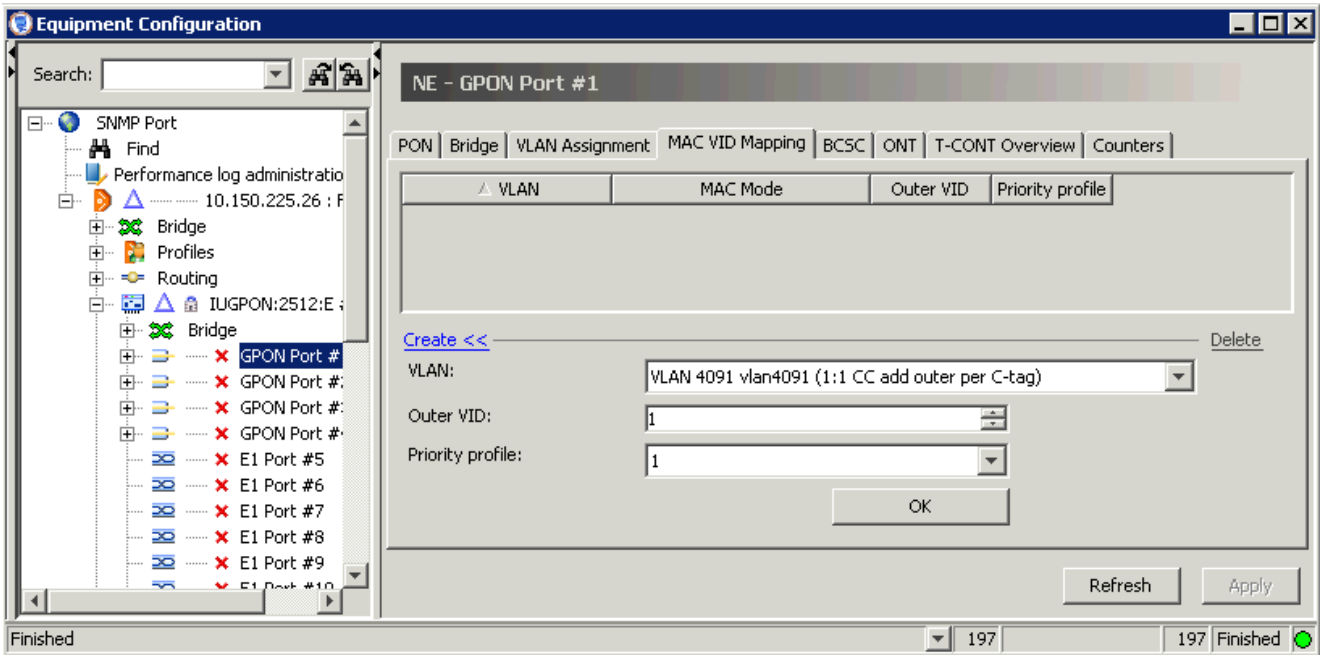

Figure 52 MAC VID Mapping on GPON Port

3. Choose the following options:
   - “VLAN” is the CC VLAN to be set for this GPON port. The MAC mode does not depend on this tag.
   - “Outer VID” is the added VID of the outer tag at the **NNI**. The upstream MAC mode of this VLAN can be unlike the MAC mode handling the inner VID.
   - “Priority profile” sets the priority as specified in the “.1p Priority mapping profile” (see Chapter 15.3.1 Creating an 802.1p Priority Mapping Profile on page 90).
4. Click the “OK” button to activate the mapping.

Afterwards, the “Outer VID” can be changed by clicking the respective list field on top of page.

15.3.3 Creating a GEM CoS Mapping Profile

In the enhanced MAC mode, the **GEM CoS** mapping profile determines the priorities of **GEM** ports. This mapping is associated with the priority of the inner s-tag VID at the **NNI**. Ethernet frames carried in an 1:1 CC VLAN are classified by priority and assigned to a group of up to 4 GEM ports.

Entries of GEM CoS mapping profile can be no more modified after clicking the "Create" button.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “GEM CoS mapping” profile object and select the “New GEM CoS mapping profile” command from the context menu. Up to 64 profiles are supported.

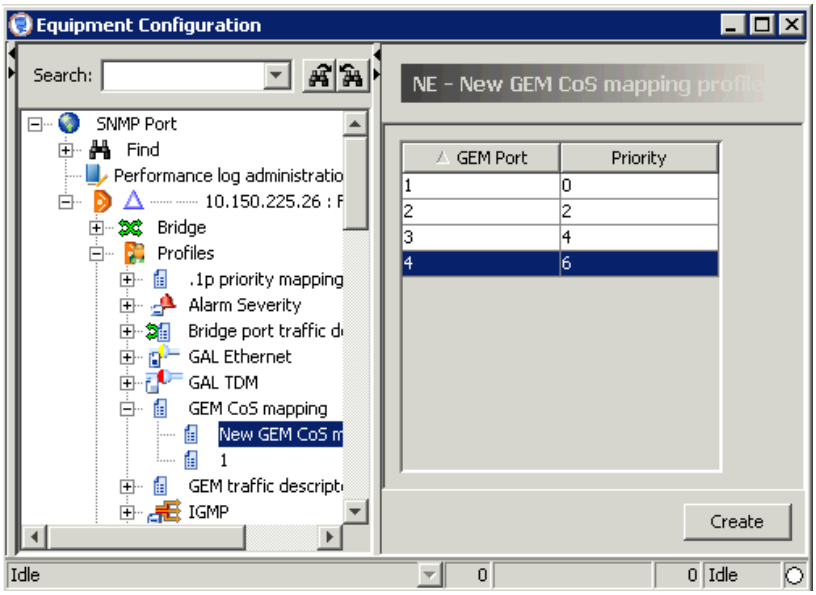

Figure 53 GEM CoS Mapping Profile

2. Choose the “Priority” of the inner tag at the **NNI** for the GEM ports #1 to #4.
3. Click the “Create” button.

15.3.4 MAC VID Mapping on Subscriber Port

Perform the following steps to configure the ONT’s subscriber ports (Ethernet, VoIP, XDSL-PVC) for cross-connect (CC) VLANs.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2 (⇨ MDU Service Board) ⇨ Subscriber Port (Ethernet, VoIP)” and select the “**MAC VID Mapping**” tab.
2. Click the “Create>>” action field to uncover the selection fields (if not already expanded).

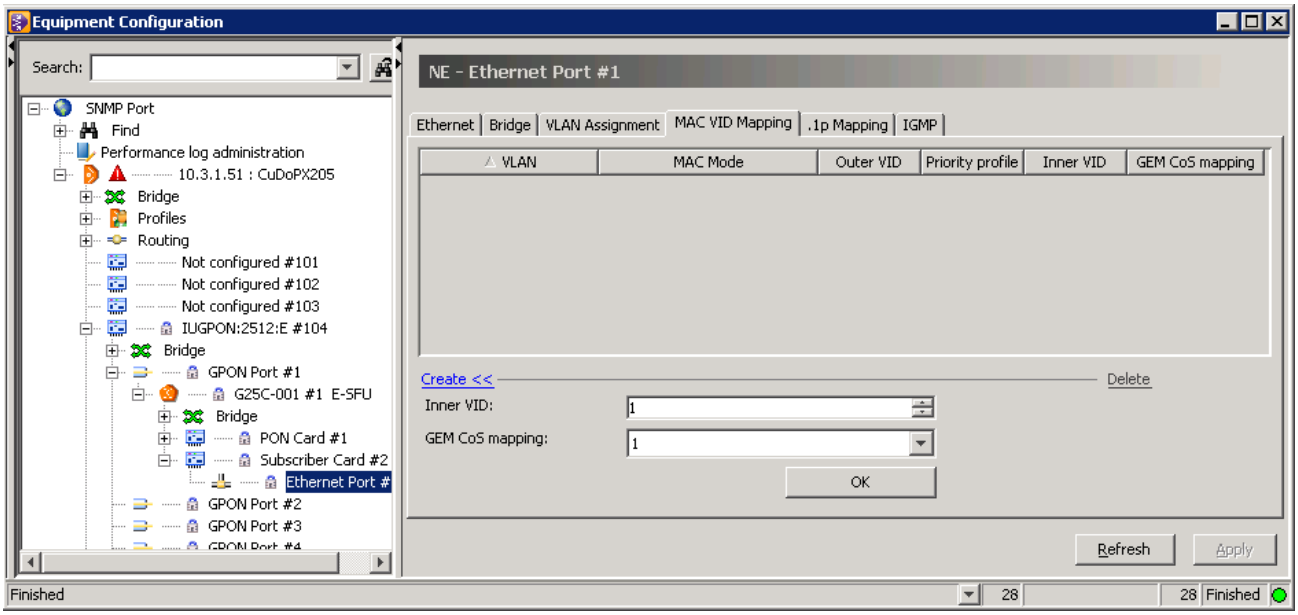

Figure 54 MAC VID Mapping on Subscriber Port

3. Choose the following values:
   - “Inner VID” changes the VID of the inner tag at the NNI. It is not required that a VLAN with this VID was created before.
   - “GEM CoS mapping” profile.

   These settings are valid for all CC VLANs assigned to this port.
4. Click the “OK” button to activate the settings.

Afterwards, the “Inner VID” and “GEM CoS mapping” can be changed by clicking the respective list field on top of page.

16 QoS

The hiX 5750 R2.0 **OLT** uses 8 **CoS** queues for the upstream and downstream direction. The queue classification is depending on the .1p priority of incoming packet.

Each of the scheduling algorithms can be assigned separately to uplink as well as downlink interfaces (cards) for both downstream and upstream traffic flow.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ QoS”.

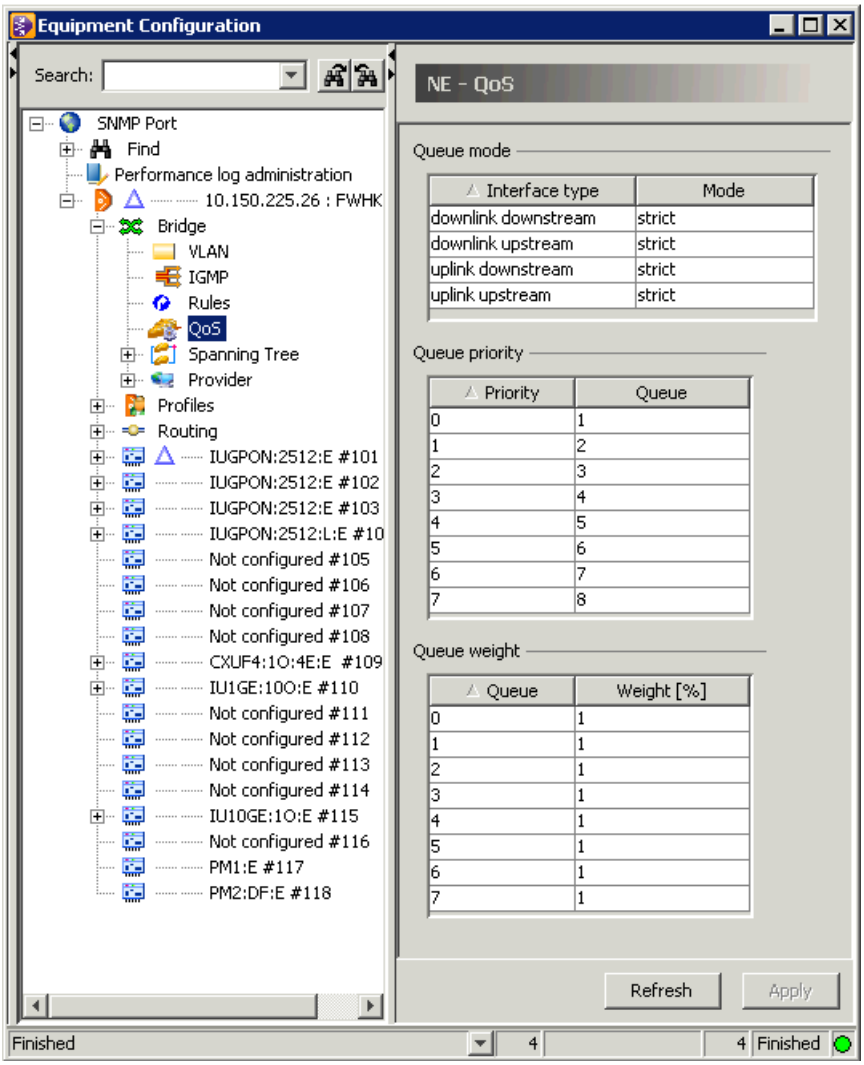

Figure 55 QoS Configuration

2. Choose the “Queue mode” per interface type by clicking the selection field. The hiX 5750 R2.0 supports two methods of QoS scheduling:

Queue Mode	Description
strict	The strict priority queuing can guarantee that in each case the CoS queue with the highest priority is always processed if packets needs to be transmitted. As long as the highest priority queue is not empty, packets from this queue are sent only and all other queues need to wait. This means that the highest CoS will finish before other queues are empty. This can lead to starvation of lower priority packet flows.

Table 48 Queue Modes

Queue Mode	Description
WRR	The WRR (Weighted Round Robin) queuing is a scheduling algorithm allowing different priorities in accordance to the data packet weight. Without different weights, all CoS queues are served one after another. Specifying weight values defines the time interval which certain queues may utilize for service. For example, if queue 4 has double weight than the others, it will be served like 1-2-3-4-4-1-2-3-4-4 etc.

Table 48 Queue Modes (Cont.)

3. Repeat these steps for each queue that needs to be configured:
   - Click the “Weight [%]” selection field of "Queue mapping" dialog box to determine the weight size of this queue.
     A weight value of 0% sets the queue to act with strict priority method. The other queues, which have been given nonzero values, follow the common WRR scheme depending on their weights.
   - Click the “Queue” selection field of "Queue priority" dialog box to classify this queue. Choose the appropriate .1p priority value from the drop-down list.
4. Click the "Apply” button to confirm.

17 Bandwidth Management

The points of bandwidth management are located on the **GPON** port dialog pages of **IU_GPON** cards and **ONT**s.

17.1 Overview

Bandwidth Allocation

- The **OLT** can create up to 6 **T-CONT**s (out of four T-CONT types) for an ONT. The number and types of T-CONTs depend on the ONT type.
- During the creation of an ONT, T-CONTs are created by the **NE** autonomously.
  The **TDM** T-CONT is only available after configuring an **E1** (**DS1**) connection.

T-CONT Type	Fixed BW	Assured BW	Assured and maximum (non-assured) BW	Maximum BW (Best Effort BW)
T-CONT 1 TDM, VoIP	Allocated			
T-CONT 2 Data high priority (real time)		Allocated		
T-CONT 3 Data high priority (non real time)		Allocated	Allocated	
T-CONT 4 Best effort services				Allocated
Remarks				
Overbooking			Overbooking	Overbooking
Application		For traffic with both delay and throughput requirements such as video and voice	Offering service at a guaranteed minimum rate while any surplus BW is assigned only upon request and availability.	For purely BE services and as such is serviced only upon BW availability up to provisioned maximum rate.

Table 49 T-CONTs and Bandwidth Allocation

Overbooking

Only "Maximum" (Best effort) bandwidth and "Assured and Maximum" bandwidth can be overbooked. The maximum available bandwidth is determined by the transmission capacity in upstream direction of 1.1Gbps per GPON link (IU_GPON2512).
Overbooking is only available if **DBA** is enabled.

The reserved bandwidth for best effort users should be between 20 % and 30 % of the total available bandwidth. See the white paper “Dynamic Bandwidth Allocation“, order no. A50028-A3-A257-02-76C8, for detailed information.

17.2 Changing the T-CONT Upstream Bandwidth

In order to change the upstream bandwidth values, choose the available T-CONTs one after another.

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ PON Card#1 (⇨ UBGPON:2512:E#3) ⇨ GPON Port#1”
2. Click the “**T-CONT**” object that needs to be configured.

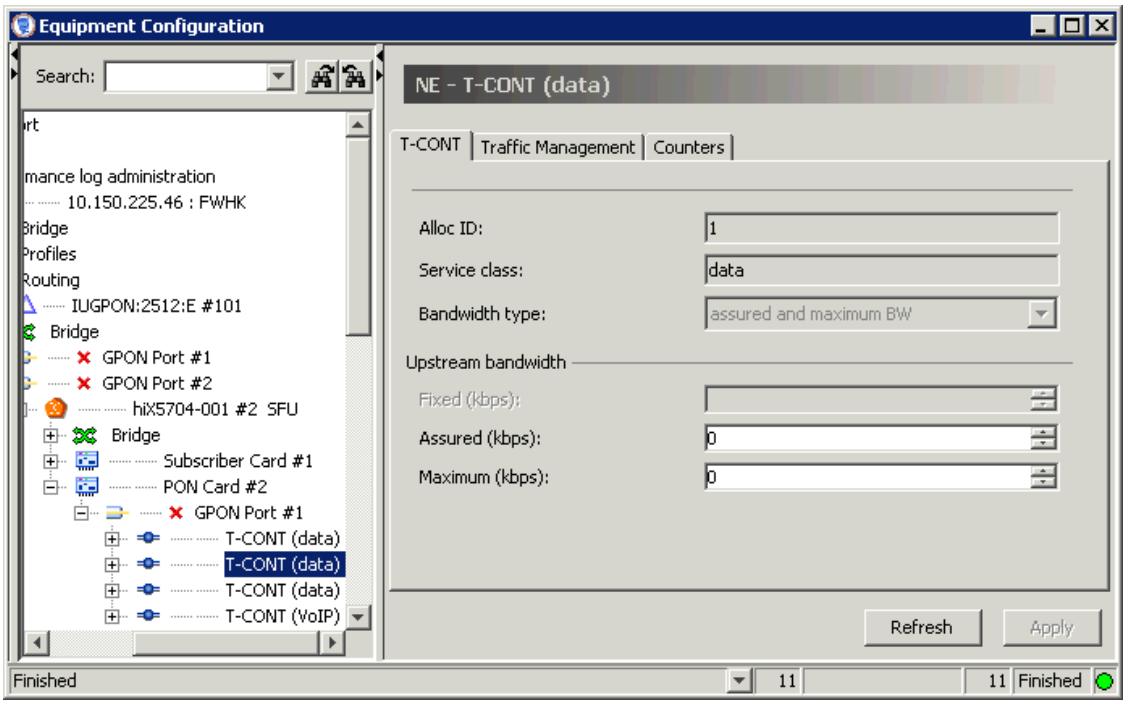

Figure 56 ONT Upstream Bandwidth Configuration

3. Chose the bandwidth values in accordance with the project-specific planning documentation (ranges: VoIP 0..130050 kbps, other T-CONT types 0..1099560 kbps).
   Smallest bandwidth unit is always 510 kbps.

T-CONT Upstream Bandwidth	Description
VoIP	Fixed bandwidth allocated for all POTS(VoIP) interfaces of this ONT. One POTS(VoIP) interface requires 113600 bps.
TDM	Fixed bandwidth allocated for all TDM interfaces of this ONT. - One E1 interface requires 2040000 bps. - One DS1 interface requires 1530000 bps.
High priority real time data	Assured bandwidth allocated for all high priority real-time data interfaces of this ONT (no delay minimizing).
High priority non real time data	Assured bandwidth allocated for all high priority non-real-time data interfaces of this ONT (no delay minimizing). Maximum bandwidth allocated for all high priority non-real-time data interfaces of this ONT. Additional non-assured or best-effort bandwidth can be dynamically assigned if requested from the pool of surplus bandwidth. It must be equal or greater than assured bandwidth.
Best effort data	Maximum bandwidth allocated for all best effort data interfaces of this ONT. Best-effort bandwidth can be dynamically assigned if requested from the pool of surplus bandwidth.

Table 50 T-CONT Upstream Bandwidth

4. Click the "Apply” button to confirm the settings.

17.3 Enabling the Dynamic Bandwidth Allocation (DBA)

By using the **DBA** mechanism, the **OLT** can rearrange upstream bandwidth to provide more resources to those ONT tightly loaded with traffic.

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ GPON Port#” to display the "**PON**” dialog page.
2. Select the "Upstream bandwidth allocation" method:

Static	Non Status Reporting Dynamic
Without DBA: Upstream bandwidth is allocated according to the port settings.	DBA with NSR: The OLT monitors the incoming traffic from the ONTs for each individual T-CONT. If traffic demand is recognized, bandwidth will be dynamically allocated (if configured and available). Otherwise bandwidth is available for other users (depending on configured T-CONTs).

Table 51 DBA Configuration

3. Click the "Apply” button to confirm the settings.

18 DHCP and PPPoE

The **DHCP**/**PPPoE** configuration can be divided into the tasks:

- Configuring CXU Modes and ID Format
- Configuring the Providers
- Configuring Subscriber Ports
- VLAN Configuration.

18.1 Configuring CXU Modes and ID Format

DHCP/PPPoE Modes for Telegram Handling

The **CXU** can work in one of three DHCP/PPPoE modes:

Mode	Description
Bridge	DHCP/PPPoE packets are forwarded inside switch circuit, i.e. CXU does not handle packets at all. So no permissions are checked and nothing is changed in its payload. Especially DHCP Option 82/PPPoE Option 105 is inserted.
Snoop	DHCP/PPPoE packets are just be forwarded if there are permissions for this VLAN bridge port combination. Payload remains unchanged. Especially DHCP Option 82/PPPoE Option 105 is inserted.
Relay	After checking permissions for this VLAN bridge port combination, the packets are forwarded and if necessary, DHCP Option 82/PPPoE Option 105 is inserted or deleted. DHCP header is changed e.g. with configured server and gateway IP address.

Table 52 DHCP/PPPoE Modes

DHCP Option 82/PPPoE Option 105

Depending on recent configuration, the DHCP relay agent can add option 82 strings into upstream packets and remove them in downstream direction again. With this information the DHCP server is able to perform a basic user authentication and can provide host configuration data for the client.

Setting	Description
none	No DHCP options 82 is added.
Circuit ID	The sent string contains a special token with information e.g. about the interface and the VLAN over which the DHCP request came in. It will be replaced dynamically when receiving a DHCP request with a VLAN depending string.
Remote ID	This string is unique for the CXU. It identifies the relay agent to the DHCP server by information about the system MAC (default), a free configurable MAC, an arbitrary IP address, or an arbitrary string.
Both	Circuit ID and remote ID are sent to the DHCP server.

Table 53 DHCP Options

Telegram Handling and Special Options

The following settings are effective for all configured DHCP/PPPoE providers.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Provider” to display the “**DHCP/PPPoE Provider**” dialog page.
2. Choose the mode of “Telegram handling” from the drop-down list, see Table 52.

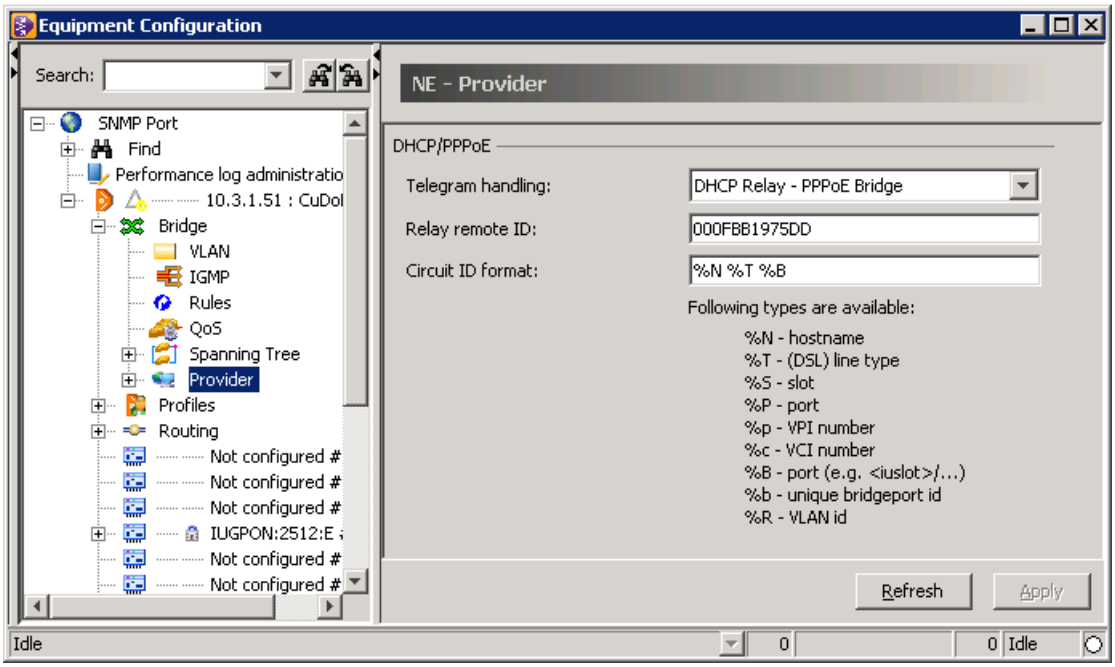

Figure 57 DHCP/PPPoE Provider

3. Enter the “Relay remote ID” string (default: system **MAC**).
4. Enter the “Circuit ID format” using the following place holder types:

Format Type	Description
%N	Host name
%T	DSL line type
%S	Slot
%P	Port
%p	Virtual Port Identifier (VPI number)
%c	Virtual Circuit Identifier (VCI number)
%B	Port string (<OLT slot>/.../<ONU port>)
%b	Unique bridge port ID
%R	VLAN ID

Table 54 Circuit ID Format Types

5. Click the “Apply” button to confirm the settings.

18.2 Configuring the Providers

18.2.1 Normal DHCP Provider

The DHCP relay agent adds the DHCP option 82 and modifies also the DHCP header (e.g. server and gateway IP address). DHCP client and server are fully separated and do not know each other. Both are only talking with the relay agent.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Provider ⇨ DHCP” to display the “**DHCP provider**” dialog page.

2. Click the “New >>” action field to uncover the input fields (if not already expanded).

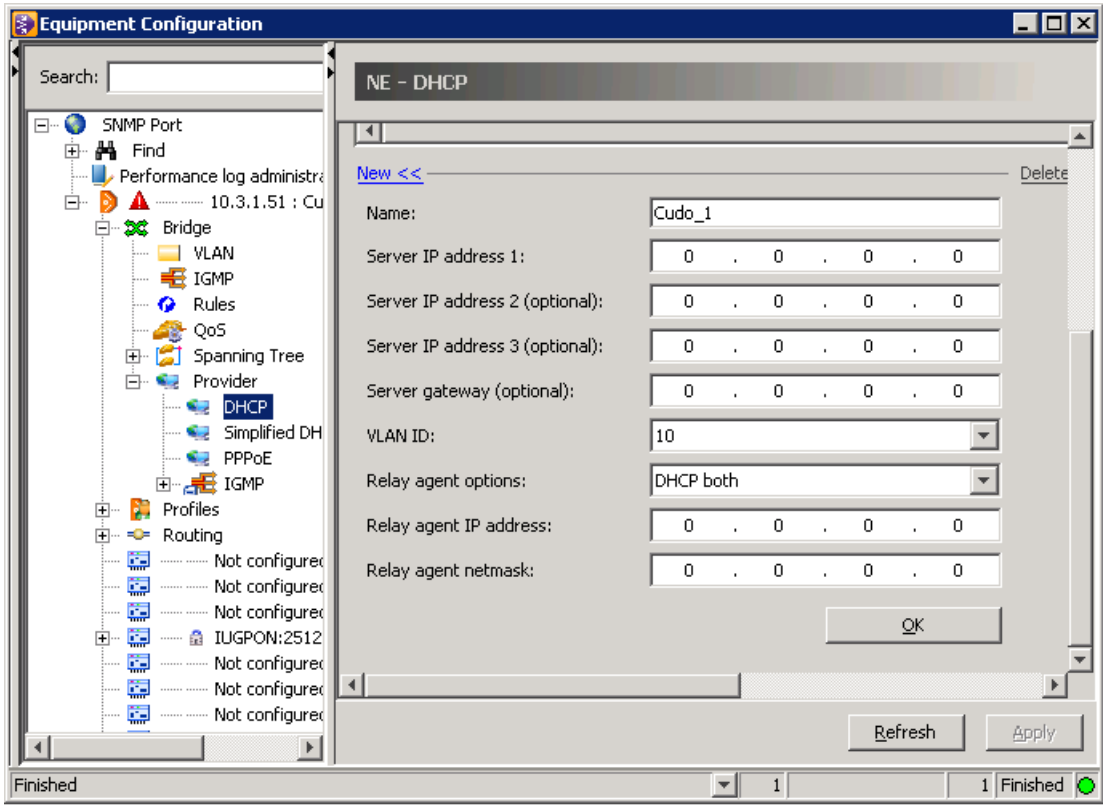

Figure 58 DHCP Provider Configuration

3. Enter a unique provider name (space is not allowed).
4. Enter the necessary IP addresses.
5. Choose the “**VLAN ID**” of the VLAN that is forwarding DHCP requests to the uplink.
   In case of using a PPPoE intermediate agent or a simplified DHCP agent, it is possible to set the “VLAN ID” option on “independent”. This means that the VLAN is used which is advertised from the received requests.
6. The use of DHCP option 82 depends on the DHCP server functionality.
   Select the “Relay agent options” to be used for DHCP option 82: “circuit ID”, “remote ID”, “both”, or “none”.
7. Enter the “Relay agent IP address” and “Relay agent netmask” to which DHCP requests need to be forwarded.
8. Click the “OK” button to complete the setting.

18.2.2 Simplified DHCP Provider

This type of provider only adds DHCP option 82 without changing anything else inside the DHCP header.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Provider ⇨ Simplified DHCP” to display the “**Simplified DHCP provider**” dialog page.
2. Click the “New >>” action field to uncover the input fields (if not already expanded).
3. Enter a unique provider name (space is not allowed).
4. Choose the **VLAN** ID of the VLAN that transmits the requests to the uplink or set this option on “independent”.
5. Select the “Relay agent options” to be used for DHCP option 82.

6. Click the “OK” button to complete the setting.

18.2.3 PPPoE Provider

PPPoE provides the ability to connect subscribers (e.g. ADSL customers) over a simple bridging access to the provider network. If the CXU works in immediate mode and the PPPoE relay agent is enabled, the tag 105 can be inserted.

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Provider ⇨ PPPoE” to display the “**PPPoE provider**” dialog page.
2. Click the “New >>” action field to uncover the input fields (if not already expanded).
3. Enter a unique provider name (space is not allowed).
4. Choose the **VLAN** ID of the VLAN that transmits the requests to the uplink or set this option on “independent”.
5. Select the “Relay agent options”, see Table 53.
6. Click the “OK” button to complete the setting.

18.3 Configuring Subscriber Ports

The following configuration steps are valid for both Ethernet and XDSL subscriber ports.

Activating DHCP/PPPoE

1. Click “NE:hiX5750 ⇨ IUGPON2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card #2” (MDU Service Board) ⇨ Subscriber Port” and select the “**Bridge**” tab.

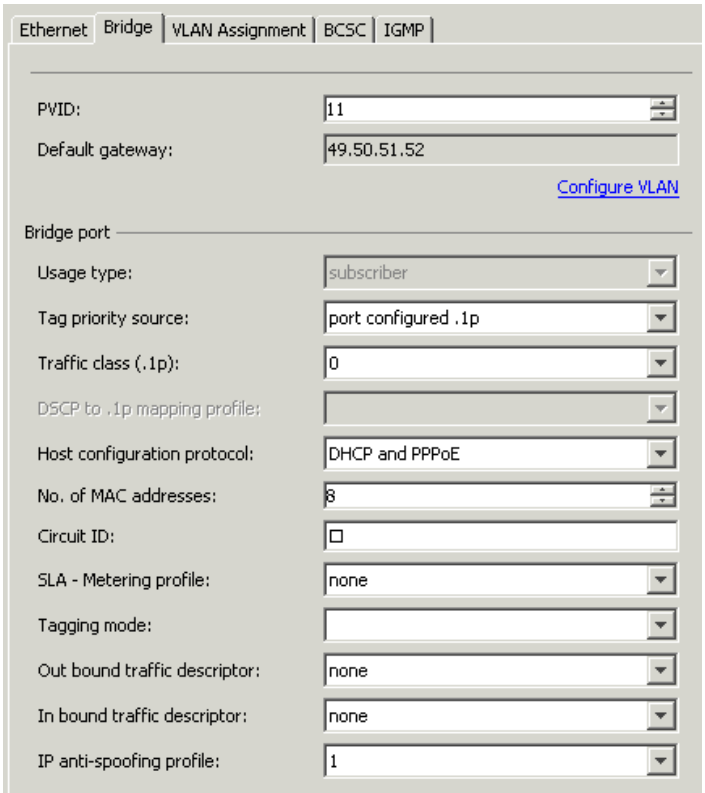

Figure 59 DHCP/PPPoE - Subscriber Configuration

2. If the “Tagging mode” is set on “untagged”, enter a PVID corresponding to the DHCP/PPPoE provider VLAN.
3. Choose the “Host configuration protocol”: “DHCP”, “PPPoE”, “DHCP and PPPoE”, or “none”.
4. Enter the “Circuit ID” that shall be used by this port for the DHCP option 82/PPPoE option 105.
5. Click the “Apply” button to confirm the settings.

DHCP for VoIP

To enable DHCP to a **VoIP** port, follow the steps as described in Chapter 11 VoIP Services.

18.4 VLAN Configuration

All subscriber ports of an ONT can only use one DHCP or/and one PPPoE provider. The DHCP and PPPoE provider must be assigned to the VLANs.
See Chapter 15.1 Creating a VLAN for detailed information.

19 IGMP

The hiX 5750 R2.0 supports IGMP (Internet Group Management Protocol) up to Version 2.

The IGMP provisioning can be divided into three parts:

1. Enabling IGMP for the VLAN (see Chapter 15.1 Creating a VLAN)
2. Configuring the OLT
3. Configuring the ONT.

19.1 Configuring the OLT

19.1.1 Configuring Providers

IGMP providers are required to use the Proxy functionality on the OLT (see Chapter 19.1.2 Configuring the CXU on page 105). The number of IGMP providers is limited to 16.

1. Click “NE:hiX5750 ⇨ Provider”, right-click the "IGMP” provider object and select the "New IGMP provider" command from the context menu.

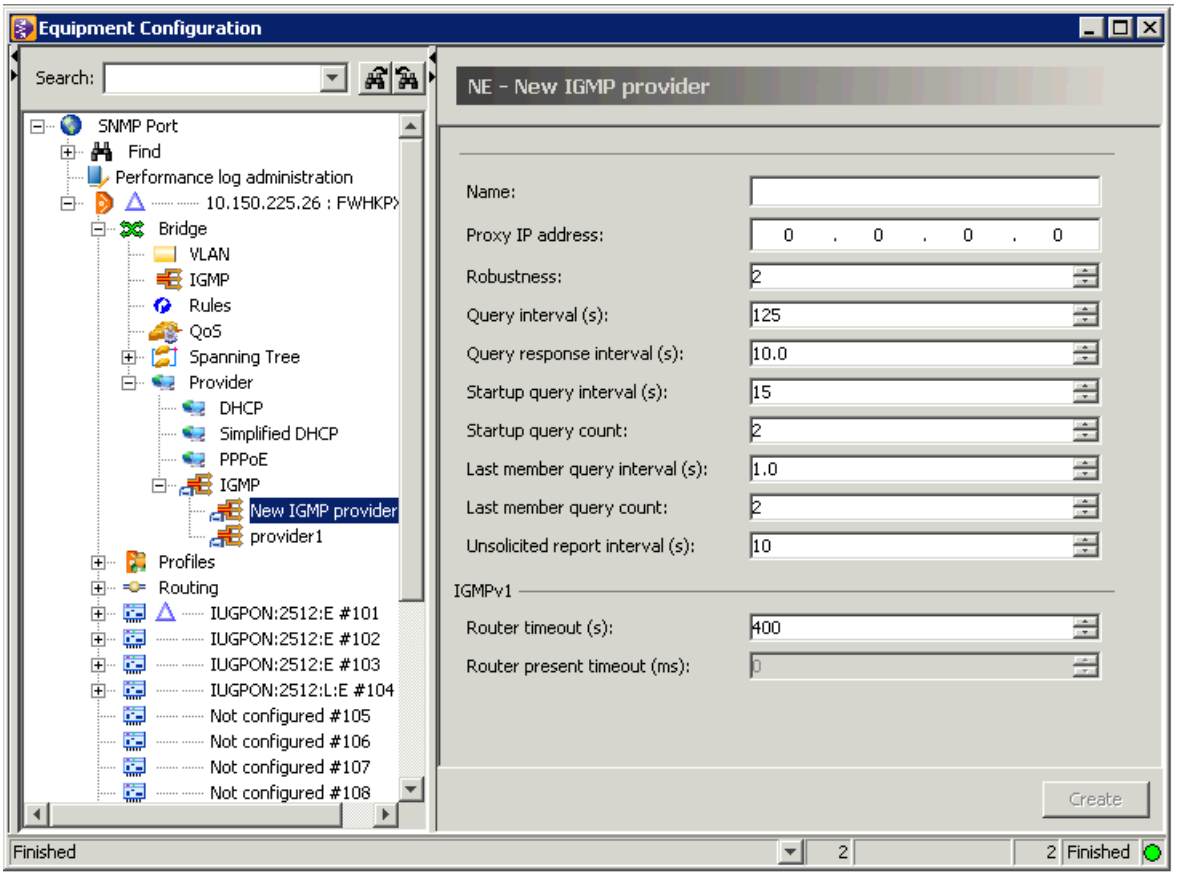

Figure 60 IGMP Provider

2. Enter a unique provider name (space : ? are not allowed).
3. Change or confirm the preference settings.

Setting	Description	Default Value
Proxy **IP** address	Proxy IPv4 address.	
Robustness	Tunes IGMP to expected packet losses on the link. The default value effects that IGMP is robust to a single packet loss. If a subnet is expected to be lossy, this variable may be increased. The robustness must not be zero, and should not be one.	2
Query interval (s)	Sets the interval in seconds between subscriber membership query messages are sent by the router (downstream). By varying this variable the number of IGMP messages on the network can be changed. Larger values cause IGMP queries to be sent less often.	125s
Query response interval (s)	Sets the interval between subscriber membership reports which are sent by the ONT. By varying this variable the burst rate of IGMP messages on the subnet can be tuned. Larger values make the traffic less bursty. Range: 0,1...25,5 s (0,1 s steps) The number of seconds must be less than the "Query interval".	10s
Startup query interval (s)	Interval between general queries sent by a router on startup (1/4 the "Query interval")	15s
Startup query count	Number of queries sent out on startup, separated by the "Startup query interval' (Equal the "Robustness")	2
Last member query interval (s)	Used by timer to calculate group-specific and group-and-source-specific queries. A reduced value results in reduced time to detect the loss of the last member of a group or source	1s
Last member query count	Number of group-specific queries sent before the router assumes there are no local members.	2
Unsolicited report interval (s)	Time between repetitions of a subscriber initial report of membership in a group	10s
Router timeout (s)	Used only for IGMPv1 streams. Sets the groups report delay timer	400s
Router present timeout (ms)	Used only for IGMPv1 streams. Sets the present timeout of the groups delay timer	0ms

Table 55 IGMP Provider Options

4. Click the "Create" button to add the new IGMP provider.
5. Click the “**VLAN Assignment**” tab to associate an **MC** VLAN with this provider.
   For the respective MC VLAN, the option "IGMP only" must be activated to display it in the “Available” selection box (see Chapter 15.1 Creating a VLAN).

19.1.2 Configuring the CXU

1. Click “NE:hiX5750 ⇨ CXUVR:10:4E:E#109 ⇨ Bridge ⇨ IGMP”.
2. Select the IGMP switching mode:

Mode	Decription
VLAN Switching	MC traffic is forwarded over all ports of the VLAN.
Snoop Only	IP based IGMP snooping is supported.
Proxy	Reduces IGMP network traffic by supporting Proxy function.
Off	Forwarding IGMP MC traffic is disabled.

Table 56 IGMP Switching Modes of CXU

In order that the "Proxy" mode can operate, two conditions have to be complied with:
- An IGMP provider is configured
- VLAN support for IGMP is enabled, see Chapter 15.1 Creating a VLAN ("IGMP only" option).

3. If the IGMP switching mode is set on "Snoop only", the preset timer values for "Robustness", "Query interval" and "Query response interval" may be changed.
   The timer values should be the same for OLT and ONT.
4. Click the "Apply" button to confirm.

19.1.3 Configuring the IU_GPON

1. Click "NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ Bridge ⇨ IGMP".
2. Chose the IGMP switching mode.
   This setting depends on the chosen IGMP switching mode of the CXU.

Mode	Decription
VLAN Switching	MC traffic is forwarded over all GPON ports of the VLAN.
Snoop Only	IP based IGMP snooping is supported.
Off	Forwarding IGMP MC traffic over the GPON ports is disabled.

Table 57 IGMP Switching Modes of IU_GPON

3. If the CXU's switching mode is set on "Snoop only", the preset timer values for "Robustness", "Query interval" and "Query response interval" may be changed.
4. Click the "Apply" button to confirm.

19.1.4 Configuring the IU_10x1G and IU_1x10G

Configure the IU10GE:1O:E/IU1GE:10O with the procedure as described for IU_GPON.

Not all functions are available for these IU cards. The attributes robustness, query interval and query response interval are not supported by IU_10x1G (downlink) and IU_1x10G (uplink). While the IU_10x1G supports both "VLAN switching" and "Snoop only" , the IU_1x10G provides only the VLAN switching mode.

19.2 Configuring Multicast Packages and Groups

1. Click "NE:hiX5750 ⇨ Bridge ⇨ IGMP" to display the "**General**" dialog page.
2. The number of "Max joined groups" can be changed.
   This is the maximum number of groups that can be active at the same time in the hiX 5750 R2.0. The value is initially valid for the whole system. However, a limitation of max. joined groups is also possible per bridge port, see Chapter 19.3.2 Configuring the ONT Subscriber Ports on page 110.
3. Click the "Apply" button to confirm.
4. Select the "**Packages**" tab.

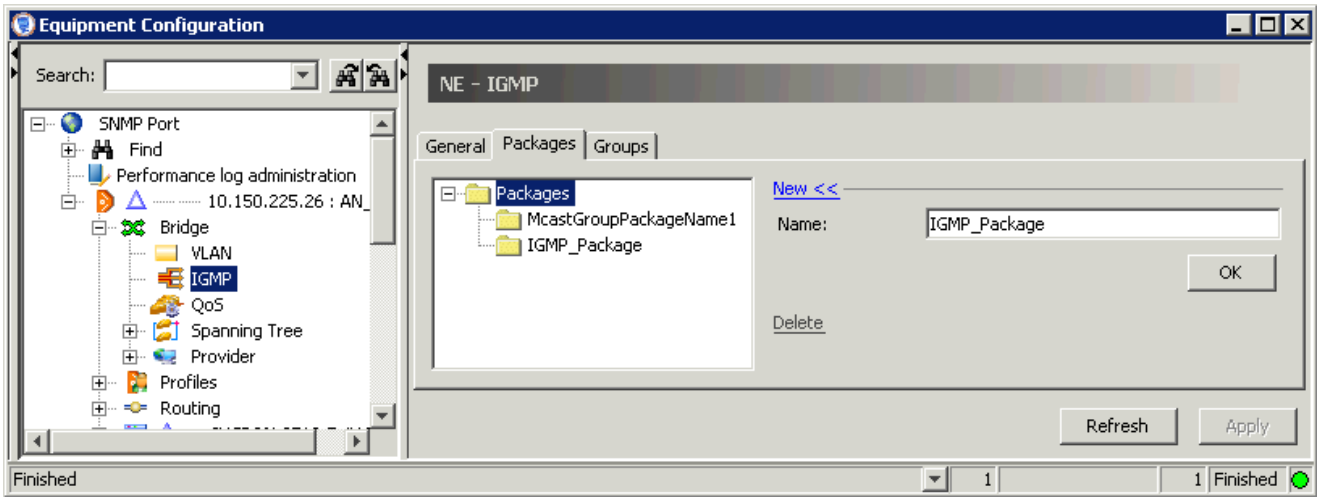

Figure 61 IGMP Package

5. Click the "New>>" action field to uncover the “Name” field (if not already expanded).
6. Enter a unique package name.
7. Click the "OK" button to insert the new package.
8. Click the "**Groups**" tab.
9. Click the "New>>" action field to uncover blank input fields (if not already expanded).

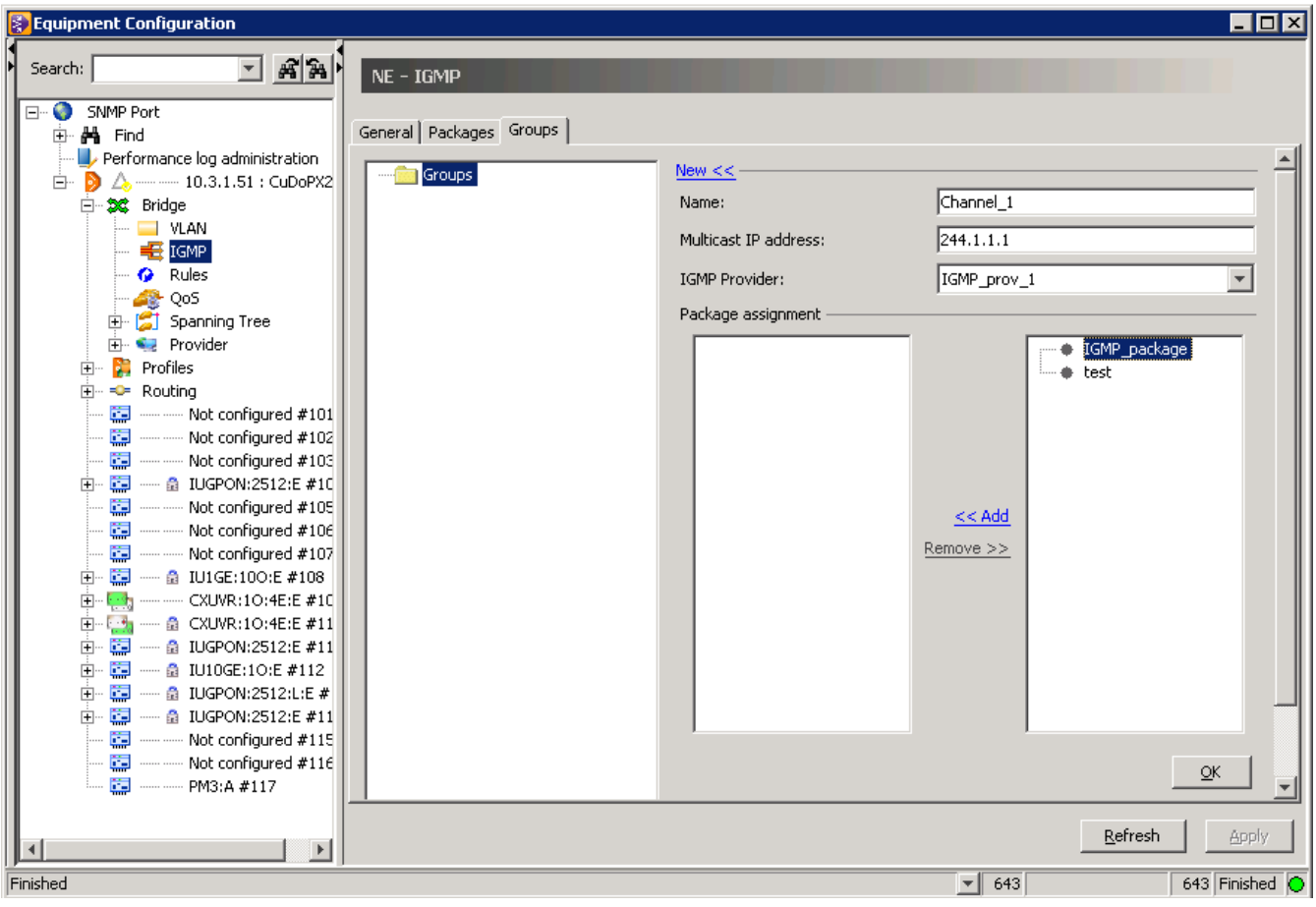

Figure 62 IGMP Group

10. Enter a unique group name.

11. Enter the IPv4 address of a specific **MC** source into the "Multicast IP address" field.
12. Select an "IGMP provider" from the drop-down list.
13. Click the “OK” button to insert the new group.

Repeat the following steps until the created MC groups and package are assigned each other:

1. Click to highlight an MC group in the selection box on the left-side and then click to highlight the MC package in the selection box on the right-side which the group shall be assigned to.
2. Click the “<<Add” action field.

19.3 Configuring the ONT

19.3.1 Creating IGMP Profiles

An IGMP profile can only be created or deleted but not modified.

1. Click “NE:hiX5750 ⇨ Profiles”, right-click the “IGMP” profile object and select the “New IGMP profile” command from the context menu.

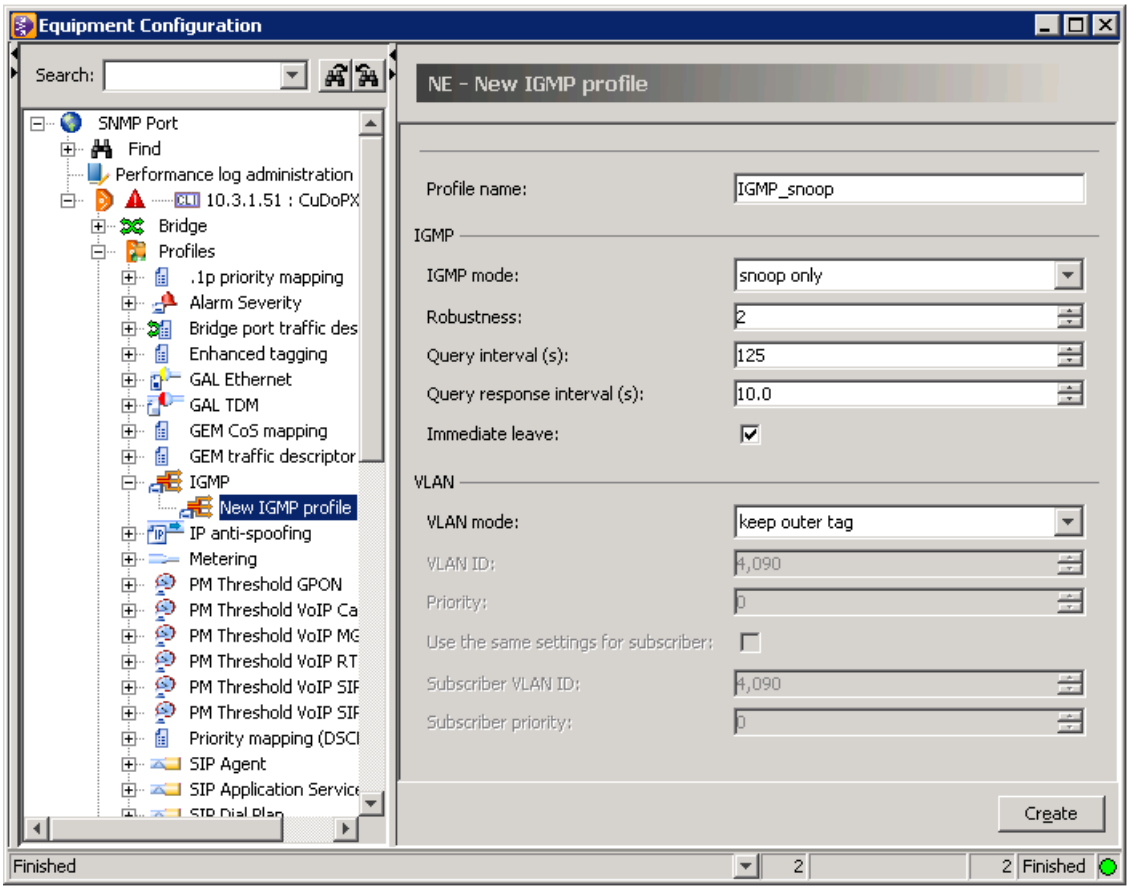

Figure 63 IGMP Profile

2. Enter a unique profile name (space : ? are not allowed).
3. Choose the IGMP mode:

Mode	Description
VLAN Switching	MC traffic is forwarded over all VLAN ports.
Snoop Only	Snooping avoids that all switch ports are flooded by MC traffic. The ONT supports MAC based on IGMP snooping functionality. Only subscriber ports which have joined an MC group are inscribed on the forwarding-table of the MC VLAN. Ports that leave the group will be deleted from the table.
Off	All IGMP messages and frames are dropped.

Table 58 IGMP Profile

Only if the IGMP mode is set on “Snoop only”, the further options may be configured:

1. The preset timer values for “Robustness”, “Query interval” and “Query response interval” may be changed.
2. Choose the “Immediate leave“ option to determine how the ONT/MDU acts when the last subscriber leaves the MC group:

Immediate Leave	Description
Enabled	The subscriber host will be deleted from the MC group intermediately when the port receives the leave message.
Disabled	If a subscriber host (e.g. set top box) sends a leave message, the ONT sends a query message to the host. When there is no response from the host, it will be deleted from the MC group. During the waiting period which is comprised of query intervals to determine the membership validity, the MC data are continuously forwarded over the ports. In this process unnecessary bandwidth is occupied.

Table 59 IGMP Immediate Leave

3. Choose the “VLAN mode” of the subscriber ports, this IGMP profile will be assigned to.
   This mode decides about how the outer VLAN tag of upstream IGMP user frames (user tag or **PVID**) has to be handled. If “VLAN mode” is set on “replace outer tag”, the VLAN ID and .1p priority in the outer VLAN tag will be replaced by the IGMP provider values.
4. Choose the “VLAN ID” (range is 2..4093) and "Priority" the outer VLAN tag will be overwritten with.
5. If necessary, VLAN forking of an MC VLAN and a unicast VLAN can be configured.
   Note that this setting is usable only for **XDSL** subscribers ports of the **MDU** hix 5709 R2.0 and the Ethernet port of **ONT** type G-25C.
   Choose the particular options:

Setting	Description
Use the same settings for subscriber	If check marked, the above settings will be used else the following both options.
Subscriber VLAN ID	In downstream direction of MC traffic, the ID of the IGMP provider MC VLAN is replaced by this user tag or PVID.
Subscriber priority	In downstream direction of MC traffic, the IGMP provider’s .1p priority is replaced by this user .1p priority.

Table 60 VLAN Forking Options

As a result of this translation function, both kinds of traffic will be carried in a combined subscriber VLAN.

6. Click the “Create” button to insert the new IGMP profile.

19.3.2 Configuring the ONT Subscriber Ports

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ Subscriber Card#2" (MDU SB:8P4GE:E) ⇨ Subscriber Port” and select the “**IGMP**” tab.

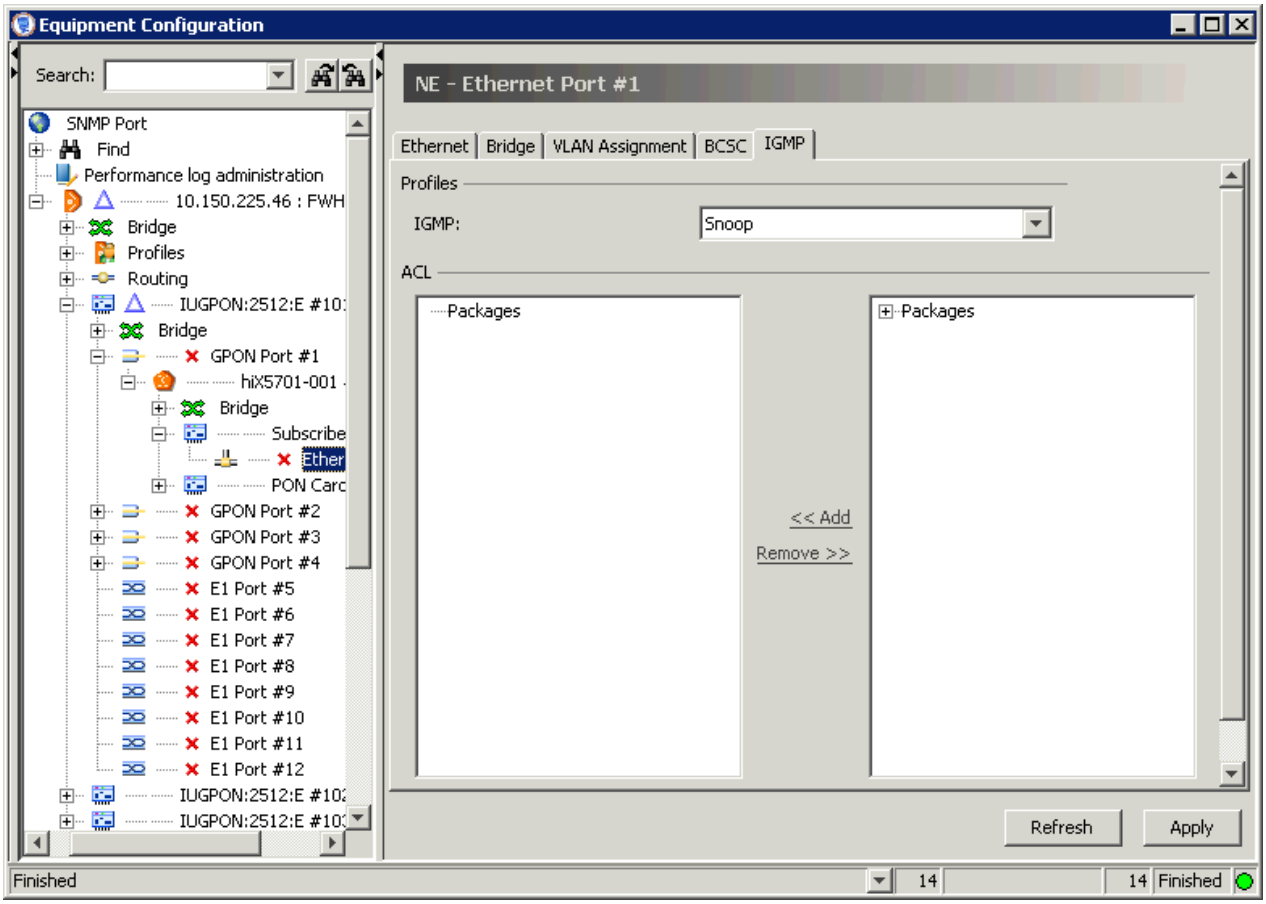

Figure 64 IGMP Port Configuration

2. Choose the “IGMP profile” from the drop-down list.
3. Click to highlight a package in the selection box on the right-side. Press the Ctrl key while clicking to mark more packages.
4. Click the “<<Add” action field to assign the package(s) to this port.
5. Click the "Apply” button to confirm.

20 Routing

20.1 Configuring the Routing Processes

The routing protocols **IS**-IS, **BGP**v4, and **RIP**v2, via which routes can be learned, are used between the hiX 5750 on uplink side and the provider edge router. All Layer 3 routed services such as High Speed Internet (with **DHCP**), video (VoD, Broadcast **TV**), and **VoIP** use **IPoE** transport. A home router which is connected via an **ONT** needs the **OLT** as default gateway and gets its Layer 3 configuration completely via DHCP.

20.1.1 Routing Information Protocol (RIP)

RIP calculates the best path to a remote destination based upon individual router hops. See the RFC 1058 and RFC 2453 for more information about RIPv2.

To configure RIP on the router, perform the following steps:

Configuring Redistribution and Timer Values

1. Click “NE:hiX5750 ⇨ Routing ⇨ Router#1 ⇨ RIP”.

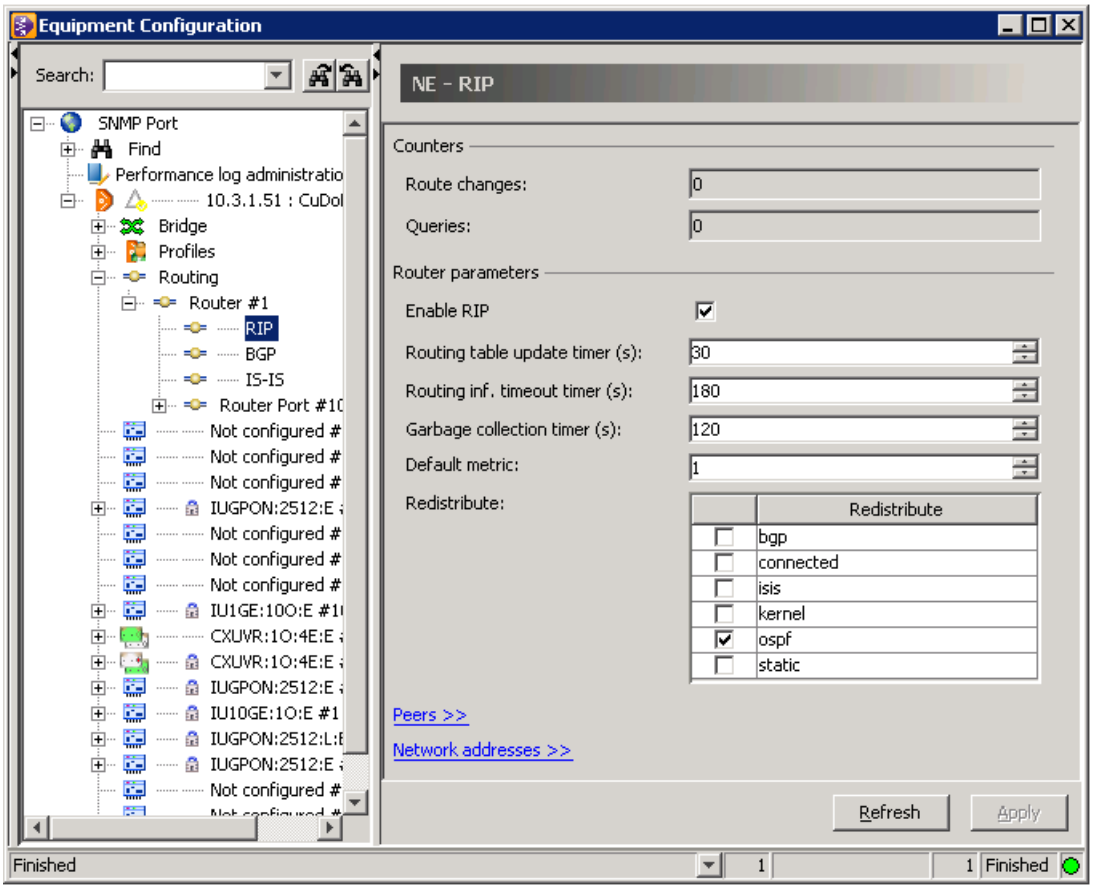

Figure 65 RIP Router Parameters

2. Click the “Redistribute” check boxes (if not already checked) to advertise routes that are learned by other routing protocols, static routes, or directly connected routes.
3. Confirm the preference settings or change the router parameters:

Setting	Description
Routing table update timer	Interval, each router broadcasts routing table to its neighbors (RIP default: 30 s).
Routing information timeout timer	If no update about the route is received in this time, it is marked as invalid and advertised unreachable (RIP default: 180 s).
Garbage collection timer	Upon expiration of this timer, the route is finally removed from the routing table (RIP default: 120 s).
Default metric	RIP metric is a value for distance for the network that will be incremented when the network information is received. Default metric specifies the metric to be assigned to redistributed routers (RIP default: 1).

Table 61 RIP Router Parameters

4. Click the “Apply” button to confirm.

Click the “Peers>>” action field to open a table that provides information about active peer relationships that are intended to assist in debugging. An active peer is a router from which a valid RIP update has been heard in the time depending on router’s timeout timer.

Specifying the Network

This configuration step specifies the network(s) to which routing updates are sent and from which they are received.

1. Click the “Network addresses>> ➪ New>>” action fields to uncover the input fields (if not already expanded).
2. Enter the “Network address” and “Mask length” of the network the distribution/ announcement of routing information is enabled for.
3. Click the “OK” button to activate the network.

20.1.2 Border Gateway Protocol (BGP)

BGP allows to set up an interdomain routing system that automatically guarantees the loop-free exchange of routing information between autonomous systems (AS). It calculates the best path to a remote destination based upon AS hops.

To configure BGPv4 on the router, perform the following steps.

Enabling a BGP Routing Process and Configuring the Local AS

1. Click “NE:hiX5750 ⇨ Routing ⇨ Router#1 ⇨ BGP”.

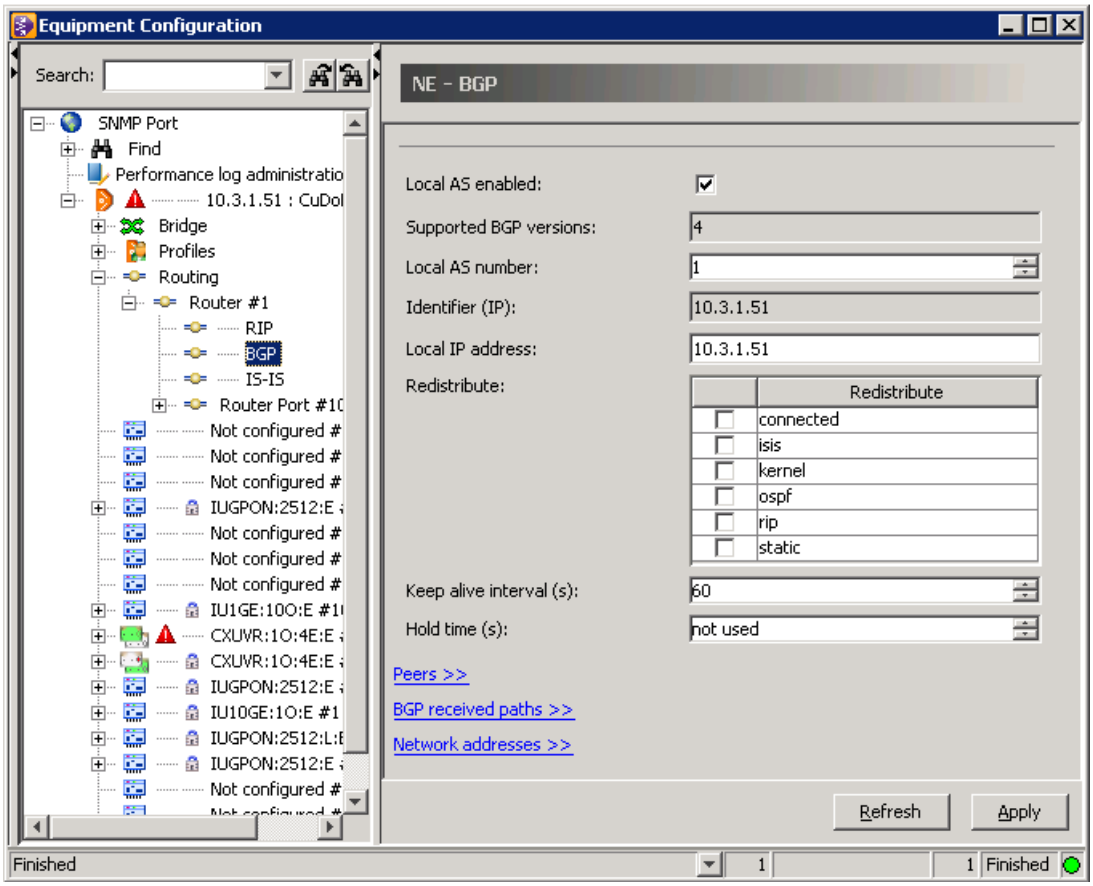

Figure 66 BGP Router Parameter

2. Click the “Local AS enabled” check box to enable BGP on the router.
3. Enter the “Local AS number” from the range of 1-65535 to identify the **AS** that is used for detecting the BGP connection.
4. Enter the “Local IP address”.
5. Set the timers for BGP neighbors:

Setting	Description
Keep alive interval (s)	Time at which a router sends keep alive messages to its neighbor. Range from 1 to 65535 seconds. The default is 60s.
Hold time (s)	Interval after which the BGP connection to the peer will be closed when no keep alive message is received. Choose a value from the range of 3 to 65535 seconds or “not used”. The default is 240s.

Table 62 BGP Timers

6. Click the “Redistribution” check boxes (if not already checked) to advertise routes which are learned by another routing protocol, static routes, or some other.
7. Click the “Apply” button to confirm all settings.

Configuring Peers and Networks

Specify the neighbor router(s):

1. Click the “Peers>> ⇨ New>>” action fields to uncover blank input fields (if not already expanded).
2. Enter the peer specific parameters:

Setting	Description
Remote IP	Remote IPv4 address of the BGP peer.
Remote AS	Remote AS number identifies the BGP peer. Range: 1..65535.

Table 63 BGP Peer Parameters

3. Click the “OK” button to activate the peer.

The admin states “Lock” and ”Unlock” can also be used to restart BGP peer connections.

Specifying the Network to be Advertised by the BGP Routing Process

1. Click the “Network addresses>> ⇨ New>>” action fields to uncover blank input fields (if not already expanded)
2. Enter the “Network address” and “Mask length” of the network the distribution/announcement of routing information is enabled for.
3. Click the “OK” button to activate the network.

20.1.3 Intermediate System - Intermediate System Protocol (IS-IS)

To configure IS-IS on the router, perform the following tasks:

Enabling IS-IS

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Routing ⇨ Router#1 ⇨ IS-IS”.

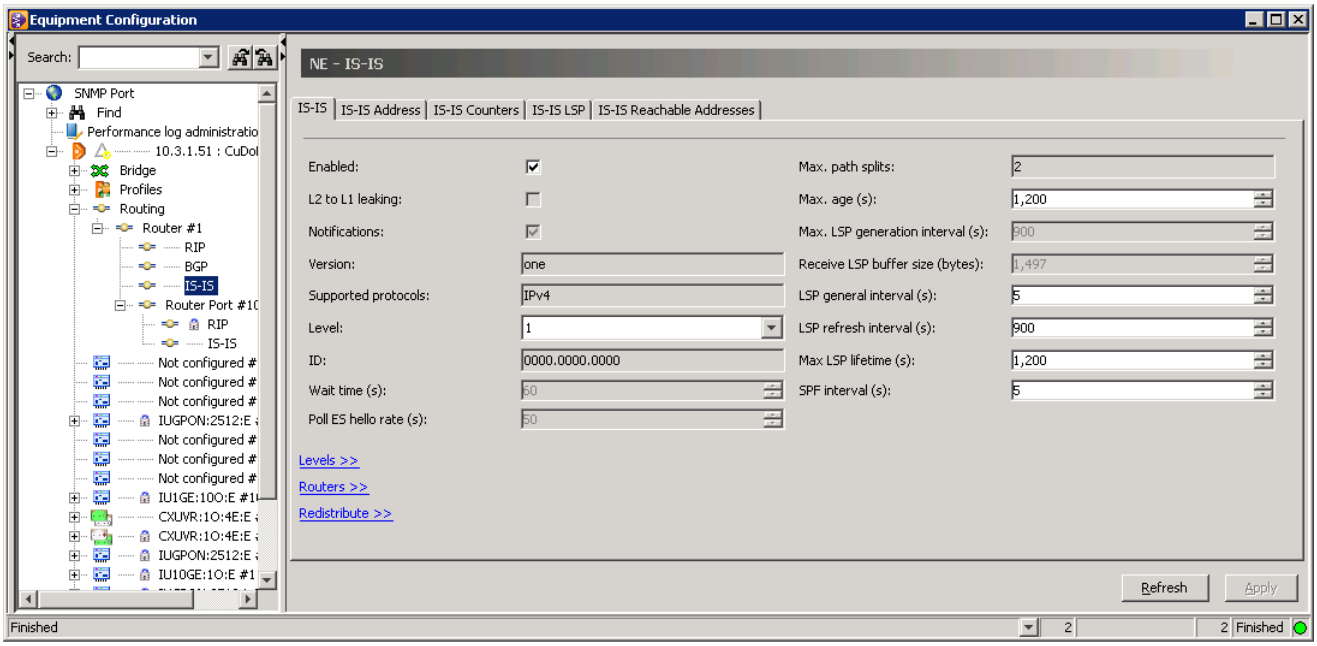

Figure 67 IS-IS Router Parameters

2. Configure the timer values and routing parameters:

Setting	Description
L2 to L1 leaking	Default: unchecked (disable).
Notifications	If checked, then it enables the emission of IS-IS Notifications (default), else these notifications are not sent.
Level	Level with that IS is running: L1, L2, L1 and L2. Default: L1 and L2.
ID	ID for this IS.This value is appended to each of the area addresses to form the Network Entity Titles.
Wait time (s)	Time to delay in state “waiting” before entering the state 'on'. Range: 1..65535, default: 60 seconds.
Poll ES hello rate (s)	Used for the suggested ES configuration timer in ISH PDUs when soliciting the ES configuration. Range: 1..65535, default: 50 seconds.
Max. path splits	Paths with equal routing metric value which it is permitted to split between. Default: 2 (fixed)
Max. age (s)	Range: 350..65535, default: 1200 seconds. The value should be at least 300s greater than “Max LSP generation interval.
Max. LSP generation interval (s)	Interval between generated LSPs by this IS. The value should be at least 300s less than “Max. age”. Range: 1..65535, default: 900.
Receive LSP buffer size (bytes)	Range: 1492..16000, default: 1497 bytes.

Table 64 IS-IS Parameters

These IS-IS options cannot be modified after the IS has been enabled.

3. Click the “Enabled” check box to enable the IS-IS routing process.

4. Click the “Redistribution>>” action field to advertise routes which are learned by another routing protocol, static routes, or some other.
5. Click into the “Level” selection fields to choose the level.
6. Click the “Apply” button to confirm.

Configuring the NET Address

Network entity titles (NET) define the area addresses for the IS-IS area and the system ID of the router. The following setting is used to add a NET for each routing process if a multi-area IS-IS has to be configured.

1. Click the “**IS-IS Addresses**” tab.
2. Click the “NET addresses>> ⇨ New>>” action fields (if not already expanded).
3. Enter the NET address, e.g., 49.0001.1111.2222.3333.00 means: area ID=49.0001 and system ID=1111.2222.3333.
4. Click the “OK” button to activate the parameters.

20.2 Creating Router Ports

The IP router is connected by ports to several networks. Each network is specified by network address (IP address and subnet mask) and metric (or a number of metric values, depending on the routing protocol) which represents the “routing costs” for this network. The router port provides the link between the L2 VLAN and the IP router and the IP interface attributes. Router ports are additional logical interfaces.

1. Click “NE:hiX5750 ⇨ Routing”, right-click the “Router#1” object and select the “New Router Port” command from the context menu.

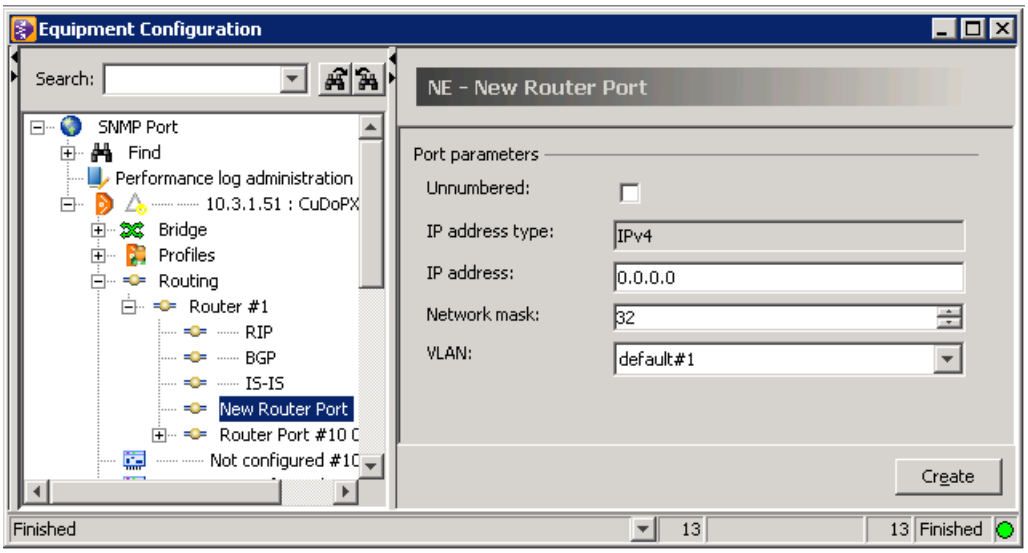

Figure 68 Router Port Configuration

2. Enter the port-specific data to configure routes:

Setting	Description
IP address	IPv4 address of the router on the connected subnet.
Network mask	Length of the IP network mask for this address.
VLAN	Select the **VID**, see also Chapter 15.1 Creating a VLAN.

Table 65 Router Port Parameters

Setting	Description
Unnumbered	An unnumbered interface has no unique IP address assignment. The address of the interface is "borrowed" from one of the router's other functional interfaces and used as the source address for routing updates and packets sourced from the interface. When IP unnumbered is configured, routes learned through the IP unnumbered interface have the interface as the next hop instead of the source address of the routing update. In this way, address space is conserved. IP unnumbered makes only sense for point-to-point links between routers.

Table 65 Router Port Parameters (Cont.)

3. Click the “Create” button to add the new router port with the name “Router Port#*VID IP address/mask*”.

Modifying of router port parameters is only possible if the “Admin state” of the interface is “locked”. It is not possible to modify the VLAN ID after creating the port.

Click the “Unlock”/”Lock” button to change the admin state of the router port.

20.3 Configuring Routing Protocols on a Router Port

Configuring the RIP Authentication

1. Click “NE:hiX5750 ⇨ Routing ⇨ Router#1 ⇨ Router Port # ⇨ RIP”.
2. Choose the version options and authentication for the routing process:
   The hiX 5750 R2.0 supports only RIPv2.

Setting	Description
Version for sending	do not send: interface passive. RIPv2: multicasting RIP-2 updates RIPv1: updates compliant with RFC1058
Version accepted	This option indicates which version of RIP updates are to be accepted.
Authentication key	The type of authentication used on this interface: none (no authentication), simple password, MD5
Auth key (for setting only)	The value to be used as the authentication key.

Table 66 RIP Options of Router Port

3. Click the “Apply” button to confirm the settings.
4. Click the “Enable RIP” button to choose RIP support for this router port.

Configuring an IS-IS Circuit

1. Click “NE:hiX5750 ⇨ Routing ⇨ Router#1 ⇨ Router Port # ⇨ IS-IS”.
2. Click the “Circuit>>” action field to uncover the selection fields (if not already expanded).
3. Click the “Create” button.
4. Configure the circuit type for this interface. IS-IS will send only the specified level of PDUs over the router port:

Setting	Description
Enable	Check to select IS-IS circuit support for this router port.
Type	Sets type of circuit: static in, static out, P2P, broadcast, DA.

Table 67 IS-IS Circuit Parameters

Setting	Description
Ext. domain	Check to suppress the normal transmission and interpretation of intra-domain IS-IS PDUs on this circuit.
Level	Select the level: 1, 2, 1 and 2
Passive	Check to includes this interface in LSPs even if the IS-IS protocol does not run.
Mesh group state	inactive: mesh group is not active blocked: blocks flooding LSPs over this router port. Routers cannot synchronize their link-state databases. set: allows unrestricted flooding over at least a minimal set of links in the mesh.
Mesh group	Sets the mesh group ID on this port.
Small Hellos	Determines which hello messages can be sent over this port. Checked: unpadded hellos Unchecked: padded hellos
3-way handshake	Determines whether 3-way handshake runs in this circuit.
Extended ID	Only used when 3-way handshake is enabled. Has to be unique across all circuits on this IS.

Table 67 IS-IS Circuit Parameters (Cont.)

5. Click the "**IS-IS Addresses**" tab.
6. Click the "Reachable addresses>> ⇨ New>>" action fields to uncover input fields (if not already expanded).
7. Configure the following options:

Setting	Description
Destination address	Reachable NSAP address. (Area ID [1-13 bytes]; System ID [6 bytes]; SEL [1 byte])
Mapping type	Type of mapping to be employed to ascertain the SNPA address that should be used in forwarding PDUs for this destination address prefix. "none": Choose if neighbor SNPA is implicit by nature of the subnetwork (e.g., a point-to-point linkage) "explicit": Subnetwork addresses specified in "SNPA address" fields will be used. "extract IDI": SNPA is embedded in the IDI of the destination NSAP address. "extract DSP": All, or a suffix, of the SNPA is embedded in the DSP of the destination address.
Metric	Metric value for reaching the specified prefix over this circuit. Range: 0...63
Metric type	"internal" or "external"
SNPA address	NSAP address (Area ID [1-13 bytes]; System ID [6 bytes]; SEL [1 byte])
SNPA mask	
SNPA prefix	

Table 68 IS-IS Reachable Address Parameters

8. Click the "OK" button to activate the values.

Click the "Lock"/"Unlock" action field to change the admin state of the connection.

20.4 Configuring a Static Route

Configuring static routes is only possible if the router ports were already created.

1. Click “NE:hiX5750 ⇨ Routing ⇨ Router#1” to display the “**Routing Table**” dialog page.
2. Click the “New>>” action field to uncover the input fields (if not already expanded).

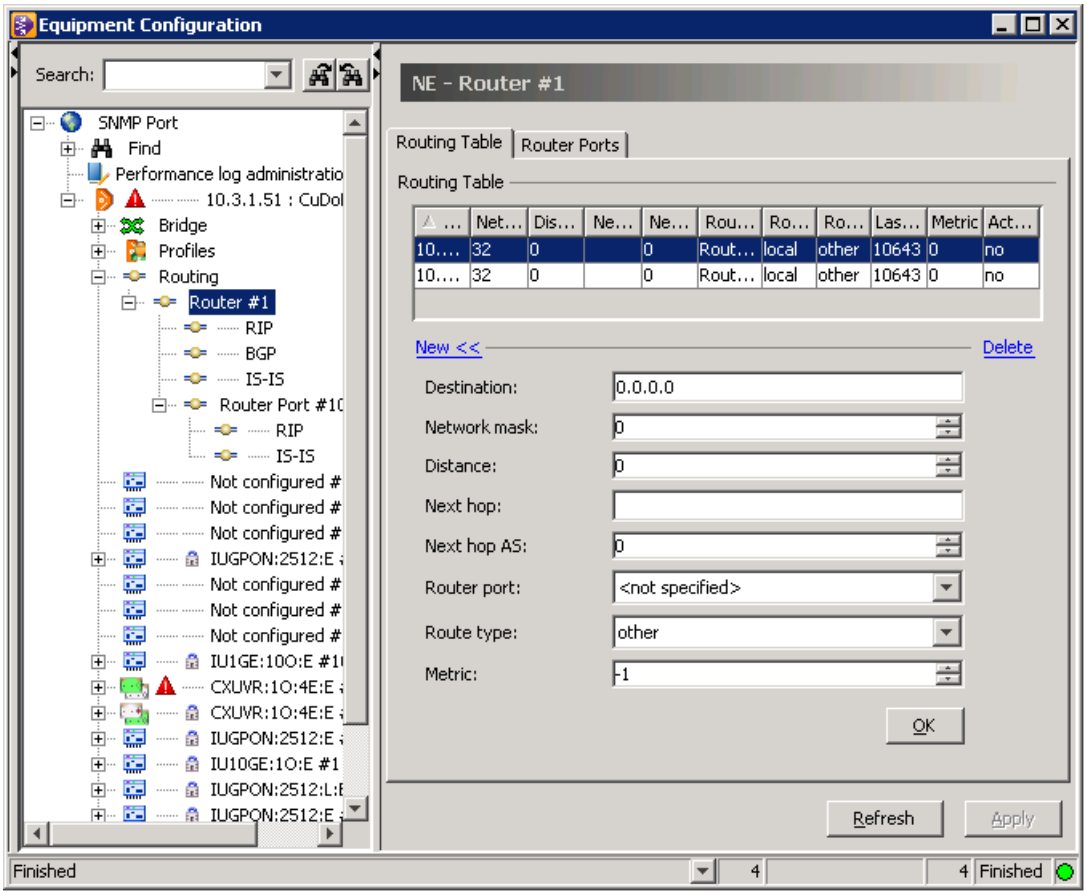

Figure 69 Static Route Configuration

3. Specify the routing table entries for the static route:

Setting	Description
Destination	Destination IP address of this route.
Network mask	Length of the IP network mask for this destination address.
Distance	Used to select the best path when there are two or more different routes to the same destination from two different routing protocols. Each routing protocol is prioritized in order of most to least reliable with the help of an administrative distance value. The router always picks the route whose routing protocol has the lowest administrative distance. Range: 0...255, default values are: IS-IS = 115, RIP = 120, OSPF = 110, internal BGP = 200.
Next hop	On remote routes, the address of the next system on route. For non-remote routes, a zero length string.
Next hop AS	The Autonomous System number of the next hop. When this number is unknown or not relevant, its value should be set to zero.
Router port	Select the router port.

Table 69 Static Route Parameters

Setting	Description
Route type	“local”: Refers to a route for which the next hop is the final destination “remote”: Refers to a route for which the next hop is not the final destination. Routes that do not result in traffic forwarding or rejection should not be displayed, even if the implementation keeps them stored internally. “reject”: Refers to a route that, if matched, discards the message as unreachable and returns a notification (e.g., ICMP error) to the message sender. This is used in some protocols as a means of correctly aggregating routes. “black hole”: Refers to a route that, if matched, discards the message silently.
Metric	The primary routing metric for this route. If metric is not used, its value should be set to -1.

Table 69 Static Route Parameters (Cont.)

4. Click the “OK” button to insert the static route into the routing table.

21 Spanning Tree

The Spanning Tree Protocol (STP) enables only one path between **NE**'s and disables all other paths with the objective of eliminating a logical network loop. If the enabled path is disconnected or fails for some reason, **STP** activates the other path and thus maintains the connectivity of the network. The hiX 5750 R2.0 supports the STP versions as specified in the Table 70 for the 4 **CXU** Ethernet uplink ports and 2 **LAG** ports.

The configuration steps for spanning trees are:

- Configuring the Common Internal Spanning Tree
- Configuring of Multiple Spanning Tree
- Enabling the Spanning Tree Configuration.

21.1 Configuring the Common Internal Spanning Tree

1. Click "NE:hiX5750 ➪ Bridge ➪ Spanning Tree ➪ CIST" to display the "**CIST**" dialog page.
2. Choose the version of the used xSTP from the "Force version" drop-down list:

Version	Description
STP	According to 802.1D
RSTP	Rapid STP according to 802.1D. Protocol for fast path recovery.
MSTP	Multiple Instance STP according to 802.1Q. Used for VLAN configurations.

Table 70 STP Versions

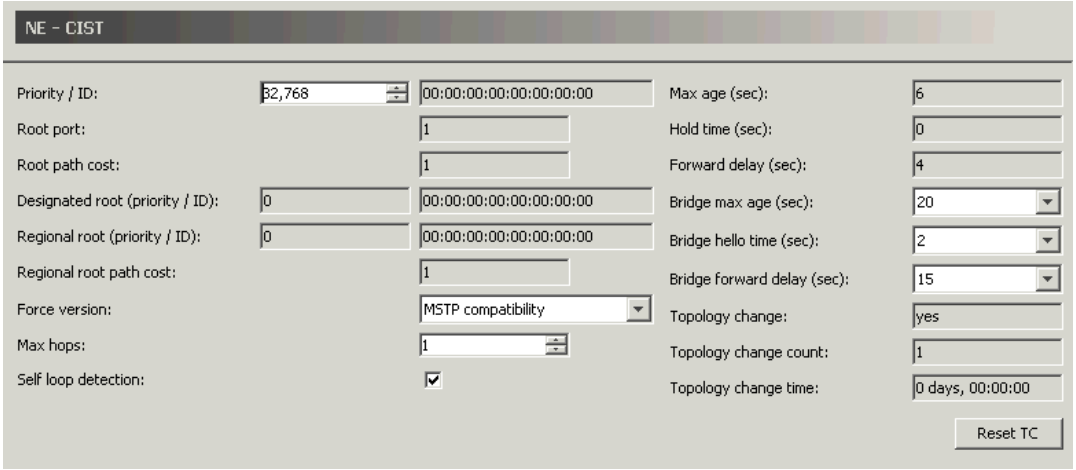

Figure 70 CIST Dialog Page

3. If "Force Version" is set on "MSTP compatibility" then the values "Max. hops" and "Self loop detection" can be configured.
4. Change or confirm the CIST values used by a bridge in the case that it is acting as root:
   - "Bridge max. age (s)": 6...40
   - "Bridge hello time (s)": 1...10
   - "Bridge forward delay (s): 4...30
5. Click the "Apply" button to confirm.

Port “Priority / ID” and “Path costs” can be changed per **CXU**/**LAG** port:

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Spanning Tree ⇨ CIST ⇨ Port object”
2. Change the preset values:
   - “Priority/ID”: 0 to 240 (default is 128).
     The lower the number, the higher the priority. Use only multiple of 16.
   - “Admin path cost”: 1 to 200000000 (default value is “autoselect” - derived from the media speed of the interface). A lower path cost means higher media speed transmission.
3. Click the “Apply” button to confirm.

The **STP** configuration must be activated, see Chapter 21.3 Enabling the Spanning Tree Configuration on page 123.

21.2 Configuring of Multiple Spanning Tree

If the network contains more than one **VLAN**, the logical network configured by single (traditional) STP does not work. The **MSTP** configures a separate spanning tree for each VLAN and blocks the links that are redundant within each spanning tree. So several VLANs can be mapped to a single spanning tree instance.

A multiple spanning tree (MST) configuration consists of three attributes:

- An alphanumeric “Region name” is needed to determine which VLAN is to be associated with which instance.
- A “Revision level” is a number of MST instance messages, conveying the spanning tree information for each instance.
- A VLANs-to-instance mapping that associates each VLAN to a given instance.

Creating an MST Region

1. Click “NE:hiX5750 ⇨ Bridge ⇨ Spanning Tree ⇨ MSTP” to display the “**MSTP**” dialog page.
2. Enter a unique “Region name”.
   Note that each MST region can only support up to 16 MST instances.

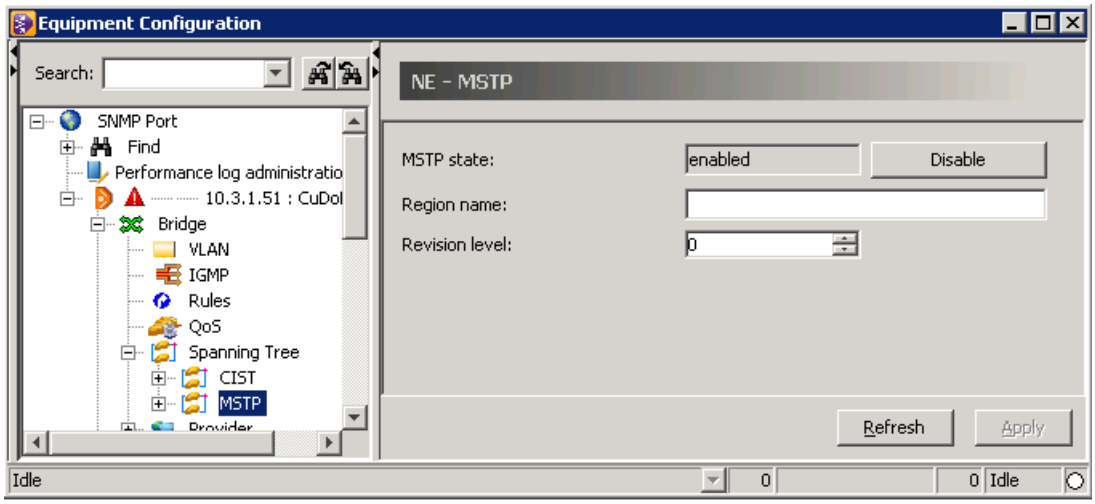

Figure 71 MSTP Dialog Window

3. Choose the “Revision level” value from the range of 0..65535.
4. Click the “Apply” button to confirm the entries.

Setting the Bridge Priority/ID

1. Click “NE:hiX5750 ➪ Bridge ➪ Spanning Tree ➪ MSTP ➪ InstanceID” to display the “**MST Instance**” dialog page.
2. Enter the “Bridge priority/ID” value from the range of 1 to 61440 (default 32768). This priority determines whether the bridge acts as root.
   Changing the “Bridge (priority/ID)” value on “MST instance” tab means changing the probability that the switch will be elected as the root switch.
   Configuring a higher value decreases the probability; a lower value increases the probability. Use only multiple of 4096 + MSTP-Instance ID.
3. Click the “Apply” button to confirm.

Assigning VLAN to MST Instance

To configure the VLAN-to-instance mapping, follow the steps for each MST instance used:

1. Click “NE:hiX5750 ➪ Bridge ➪ Spanning Tree ➪ MSTP ➪ InstanceID” and select the “**VLAN Assignment**” tab.
2. Configure a VLAN with MST port based on Ethernet uplink interface or LAG port. See Chapter 15.1 Creating a VLAN to get more information.
3. Click to highlight a VLAN in the “Available” dialog box or press the Ctrl key while clicking on each necessary VLAN to select multiple.
4. Click the “<<Add” action field to assign the VLAN(s) to the MST instance.
   A VLAN may be assigned to only one MST instance at a time.
5. Click the “Apply” button to confirm the settings.

21.3 Enabling the Spanning Tree Configuration

This step is always required to activate spanning trees independently of the xSTP version.

1. Click “NE:hiX5750 ➪ Bridge ➪ Spanning Tree ➪ MSTP”.
2. Click the “Enable” button to change “MSTP state” active, see Figure 71.

22 Security Features

22.1 Advanced Encryption Support (AES)

The hiX 5750 R2.0 **OLT** supports **AES** data encryption with a key length of 128 bit for the downstream direction. Each subscriber connection is independently encrypted. The payload encryption/decryption can be activated/deactivated per **GEM** port. Before the OLT can do this, the AES function must be enabled on ONT/MDU.

22.1.1 Configuring an ONT/MDU

See Chapter 7.1 ONT and MDU Types for information on ONTs supporting AES.

1. AES can be set during creation process of an ONT/MDU. In this case, the settings are done on the “**PON**” dialog page. In order to change the AES configuration, click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type” to display the “**General**“ dialog page.
2. Choose “AES encryption of downstream payload” from the “Active mode” drop-down list. When encryption for the ONT is switched off, the NE automatically switches of the encryption for the affected GEM ports.
3. Click the “Apply to all GEM ports” check box to enable AES generally for this ONT’s downstream traffic.
   If AES is required separate per GEM port, see Chapter 22.1.2 Configuring a GEM Port on page 124 to get information about needed configuration steps.
4. Configure the key update time in range from 5 min. to 37 hours (5 min. steps). The “AES key length” is always 128 bit.
5. Click the “Apply” button to confirm.

22.1.2 Configuring a GEM Port

Downstream payload encryption separately on GEM port level is only possible if encryption is enabled on ONT level (“Apply to all GEM ports” is enabled).

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ (UBGPON:2512:E#3) ⇨ GPON Port#1”.
2. Click “T-CONT ⇨ GEM” one after another to choose the encryption mode separately for each GEM port from the “Security mode” drop-down list.
3. Click the “Apply button to confirm.

22.2 IP Anti-Spoofing

IP anti-spoofing can be used for subscriber ports to control the IP traffic in the upstream direction. Only packets, incoming from valid IP addresses, are accepted. All other packets are discarded. IP anti-spoofing for a specific traffic flow is enabled if this function is set for both the VLAN and the bridge port.

IP anti-spoofing may be only enabled if the CXU runs in enhanced MAC mode.

22.2.1 Enabling IP Anti-Spoofing

To enable IP anti-spoofing generally on the hiX 5750 R2.0 perform the following steps:

1. Click “NE:hiX5750 ⇨ Bridge” (see Figure 39).
2. Click to mark the IP anti-spoofing “Enabled” check box.
3. Click the “Apply” button to confirm.

22.2.2 Configuring the IP Anti-Spoofing Profile

Only packets arriving for VLANs enclosed in this profile will be checked and forwarded if they have valid IP addresses. In the other VLANs, all packets will be transferred.

Only one IP anti-spoofing profile is possible for the hiX 5750 R2.0.

1. Click “NE:hiX5750 ⇨ Profiles ⇨ IP anti-spoofing ⇨ 1”.
2. Click to highlight a VLAN or press the Ctrl key while clicking on each necessary VLAN to select multiple.
3. Then click the “<<Add” action field to assign the chosen VLANs.
4. To activate all VLANs (forwarding packets with allowed IP addresses in any VLAN), click to mark the “All in system” check box.
5. Click the “Apply” button to confirm.

22.2.3 Configuring the Subscriber Port

The GPON **MAC** is capable to manage up to 8 IP addresses per subscriber port for IP anti-spoofing. To configure a white list, perform the following steps:

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E:# ⇨ GPON Port# ⇨ ONT/MDU Type ⇨ (UBGPON:2512:E#3) ⇨ Subscriber Port#2 ⇨ Ethernet Port# (xDSL Port#)” and select the “**Bridge**” tab, see Figure 72.

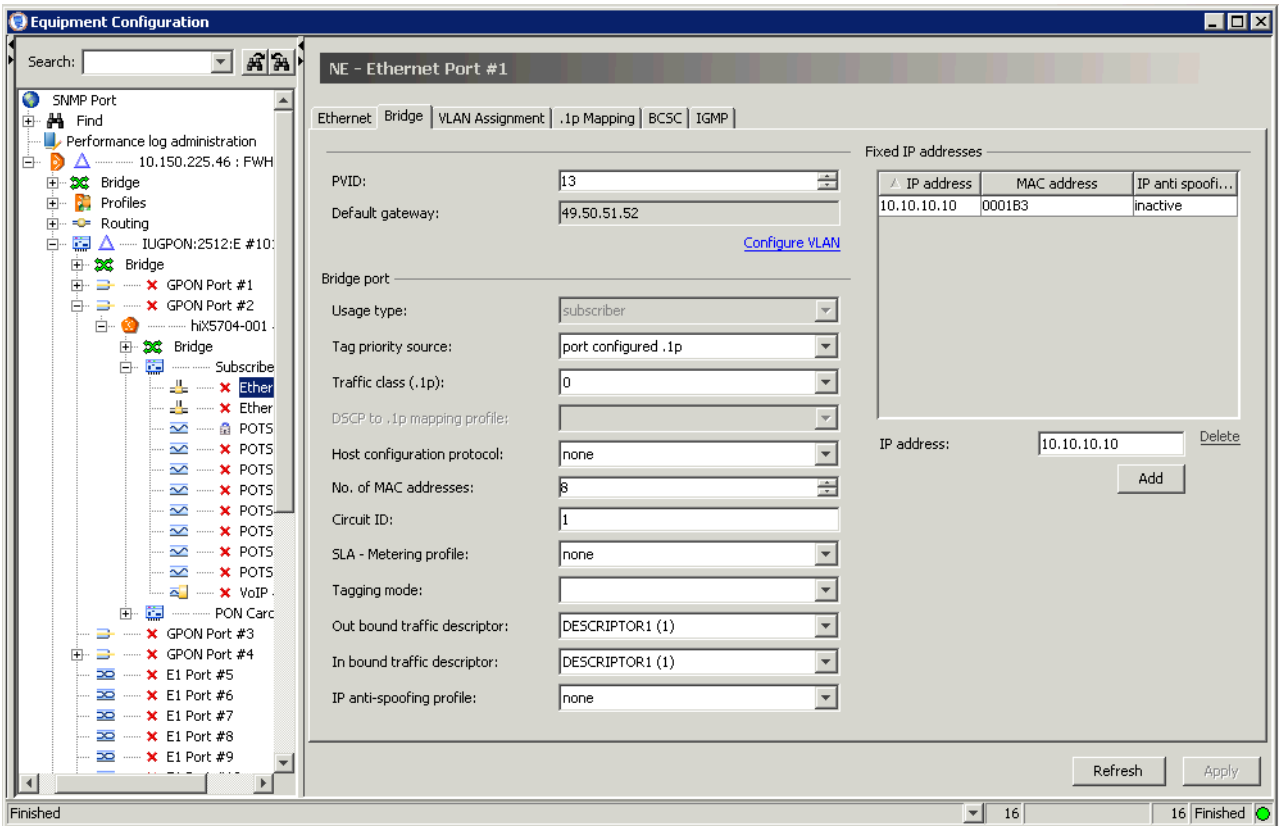

Figure 72 IP Anti-Spoofing - Port Configuration

2. Enter an “IP address” and then click the “Add” button.
   Repeat this step for up to 8 IP addresses.
3. Choose the “IP anti-spoofing profile” number “1” from the drop-down list.
4. Click the “Apply button to confirm.

23 Forward Error Correction

Chapter 7.1 ONT and MDU Types contains information about ONT's supporting FEC.

The hiX 5750 R2.0 supports FEC (Forward Error Correction) enhancement for both directions: downstream per **OLT** GPON link and upstream per **ONT**. The OLT can communicate independent of the fact whether FEC is supported by a certain ONT or not respectively it is enabled or disabled. Enabling FEC effects the following:

- The transmission overhead will be increased of about 7% resulting from the used Reed Solomon code. The bandwidth capacity will be decreased by this value.
- The **BER** can be reduced significantly corresponding to a signal to noise ratio (SNR) coding gain of up to 2,6 dB.

It is possible, but not recommended, to use the FEC improvement to increase the attenuation range of the optical link. More important is the possibility to have a higher safety margin for the upstream path.

23.1 Enabling FEC for an IU_GPON Port

Enabling FEC for the downstream direction is possible for IU_GPON2512:E and IU_GPON2512:L:E cards.

1. Click "NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port#" to display the "**PON**" dialog page.
2. Click to mark the "FEC" check box.
3. Click the "Apply" button to confirm.

23.2 Enabling FEC for an ONT/MDU

1. Click "NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ GPON Port# ⇨ ONT/MDU Type (⇨ UBGPON:2512:E#3)" to display the "**PON**" dialog page.
2. Click to mark the "FEC" check box.
3. Click the "Apply" button to confirm.

24 Link Aggregation Groups

A Link Aggregation Group (LAG) of ports can be regarded as one logical link. An LAG is useful when a high bandwidth and/or line redundancy between CXU and switches is required. It can be formed over the 1-Gbps Ethernet uplink ports of the **OLT** cards **CXU** (up to 4 interfaces per group) and IU_10x1G (up to 8 interfaces per group). The hiX 5750 R2.0 supports groups with dynamic trunk (IEEE 802.3ad) and groups with static trunk of ports.

A static LAG balances the traffic load across the links in the LAG port. If a physical link within the static LAG fails, the traffic that is carried over the failed link will be moved to the remaining links.

The Link Aggregation Control Protocol (LACP) provides a dynamically exchange of information in order to configure and maintain link aggregation groups automatically. The load sharing is automatically readjusted if a failure or recovery from failure occurs in any of the links that are member links in a dynamic LAG.

As an example, the CXU configuration is described below.

An aggregation of OLT uplink ports requires the two steps: Assigning of Uplink Ports to an LAG Group and VLAN Assignment.

In case of an OLT equipped with two CXU boards, all logical port setting must be always done on the CXU that is plugged into slot#109, independently of the current redundancy state of this board.

Assigning of Uplink Ports to an LAG Group

1. Click “NE:hiX5750 ⇨ CXUVR:1O:4E:E#109 ⇨ Bridge ⇨ LAG” and select the “**Groups**” tab, see Figure 73.
2. The setting of **LACP** decides whether an LAG group is handled dynamic or static:
   - Click to mark the “LACP enabled” check box of the “LAG Group” that needs to be a **dynamic LAG**.
   - In case of **static LAG**, LACP must not be used. Click to clear the “LACP enabled” check box (if not already disabled).
3. Click the “Groups>>” action field to uncover the configuration fields of the highlighted LAG group.
4. Select the method of distributing LAG traffic between the physical ports:

Method	Description
xor MAC	Link is chose by the result: Source MAC address XOR destination MAC address
Destination MAC	Destination MAC address
Source MAC	Source MAC address
Source IP	Source IP address
Destination IP	Destination IP address
xor IP	Link is chosen by the result: Source IP address XOR destination IP address

Table 71 LAG Distributing Methods

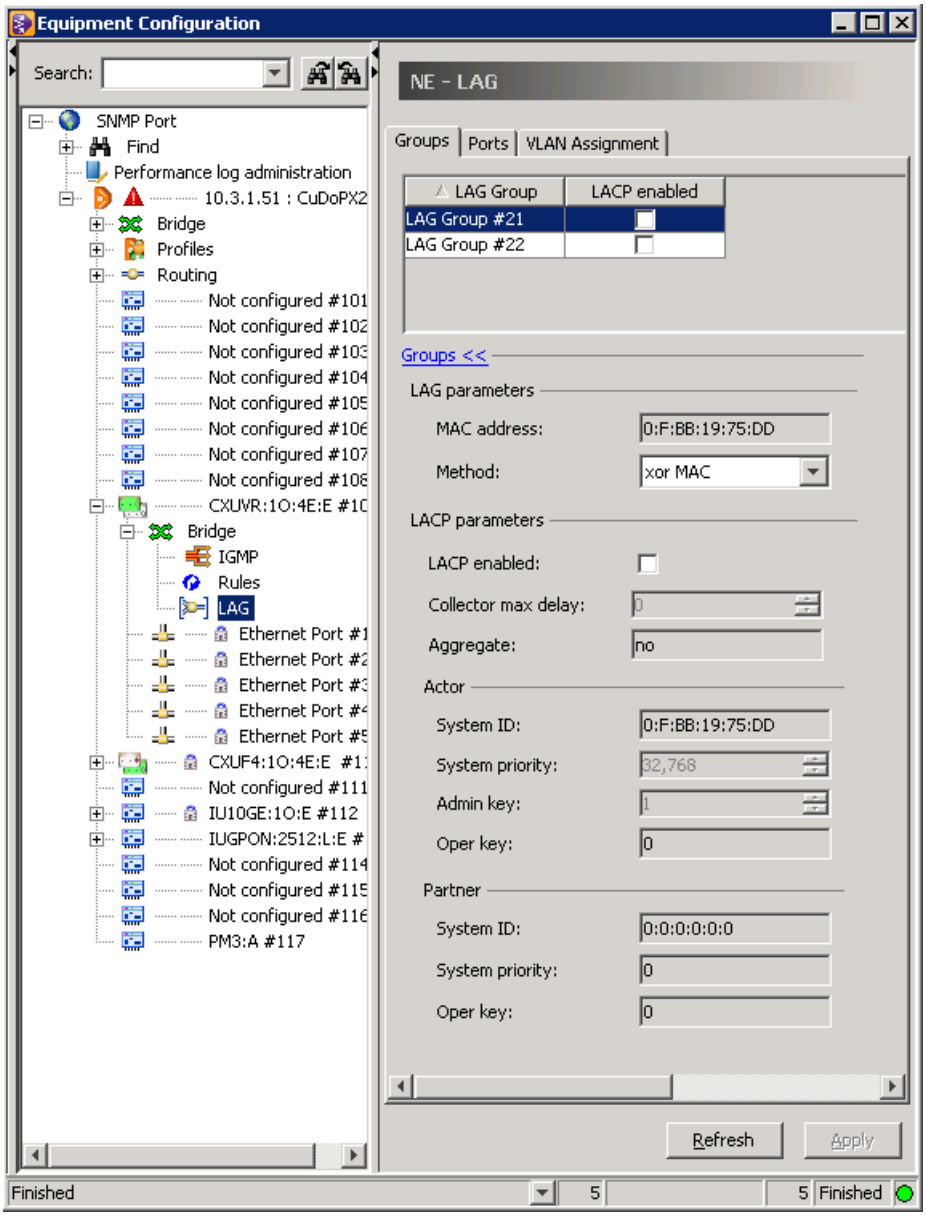

Figure 73 LAG Groups

5. If LACP is enabled for an LAG group, the further options can be configured:

Method	Description
System priority	Priority of the CXU/IU in LACP function. The value is associated with the system ID of the actor. Range: 1-65535 (Default value is 32768)
Admin key	Key for the designated aggregator. The admin key value may differ from the operational key value. The meaning of particular key values is of local significance. Range: 0-65535

Table 72 LACP Options

6. Click the "Apply" button to confirm.

Configuring a Static LAG Group

1. Click the "**Ports**" tab to assign physical ports to the LAG trunk.

The “LACP enable” check box of an LAG group that needs to be statically must be unchecked.

2. Click the “LAG Group” selection field of uplink ports that must be added to the static LAG port and choose the LAG group.

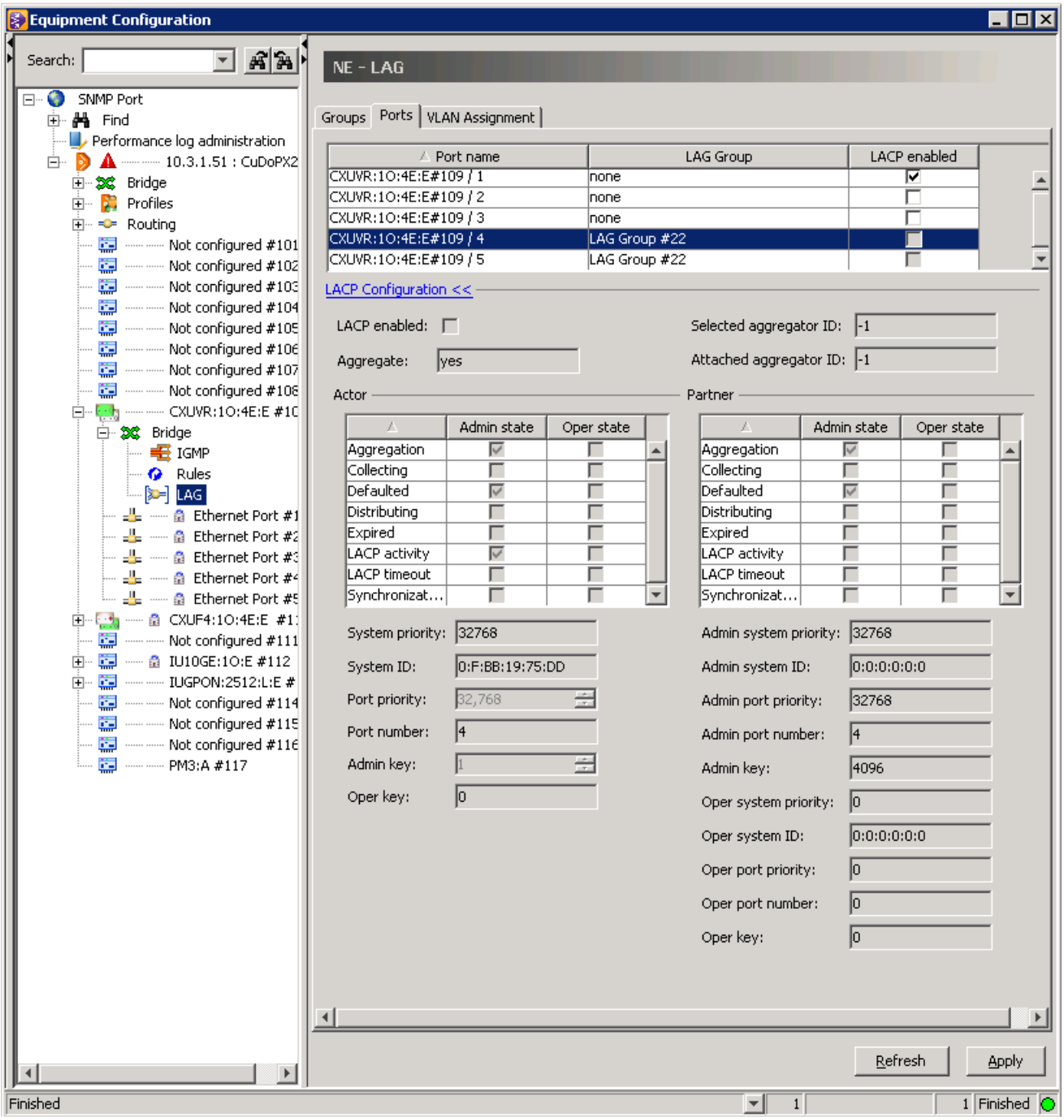

Figure 74 LAG Port

Groups can be established by selecting any combination of permitted ports. In order to change the LAG configuration, the LAG group assignment of an uplink port must be canceled first.

3. Click the "Apply” button to confirm.

Configuring a Dynamic LAG Group

1. Click the "**Ports**" tab (see Figure 74) to enable LACP per port.
2. Click to mark the “LACP enable” check boxes of uplink ports which must be added to the dynamic LAG group.
   This step is also necessary in case of using 10-GE line redundancy. Check mark only the “LACP enable” box of the CXU port#1.
3. Click the “LACP Configuration>>” action field to change specific LACP options of the LAG member port as required:
   - Enter the “Port priority” value
   - Enter the “Admin key”
   - Check mark the “Actor” option boxes.
4. Click the "Apply” button to confirm.

VLAN Assignment

See 15.1 Creating a VLAN for detailed information on the VLAN configuration.

In order to establish a static LAG, the uplink ports **and** the LAG have to use the same VLAN configuration.
For membership at a dynamic LAG, only the uplink ports must be added to the same VLAN.

1. Click the "**VLAN Assignment**" tab.
2. Click to highlight an “LAG Group#” in the "Assigned to” selection box.
3. Click to highlight the appropriate VLAN or press the Ctrl key while clicking to select more than one entry.
4. Click the "<< Add tagged" respective "<<Add untagged" action field to assign the VLAN(s) to LAG group.

25 Rules

Rules can be used to limit and control the access to switches by configuring filters for each switch port.

The number of rules supported by the GPON units is limited, see the table below.

Unit	Max. Number of Rules
CXU	2048
IU_GPON	128 per GPON port only in upstream direction
IU_10x1GE	2048

Table 73 Max. Number of Rules

1. Click “NE:hiX5750 ⇨ UNIT ⇨ Bridge ⇨ Rules” (“UNIT” stands for CXU, IU_GPON, IU_10x1GE, IU_1x10GE.

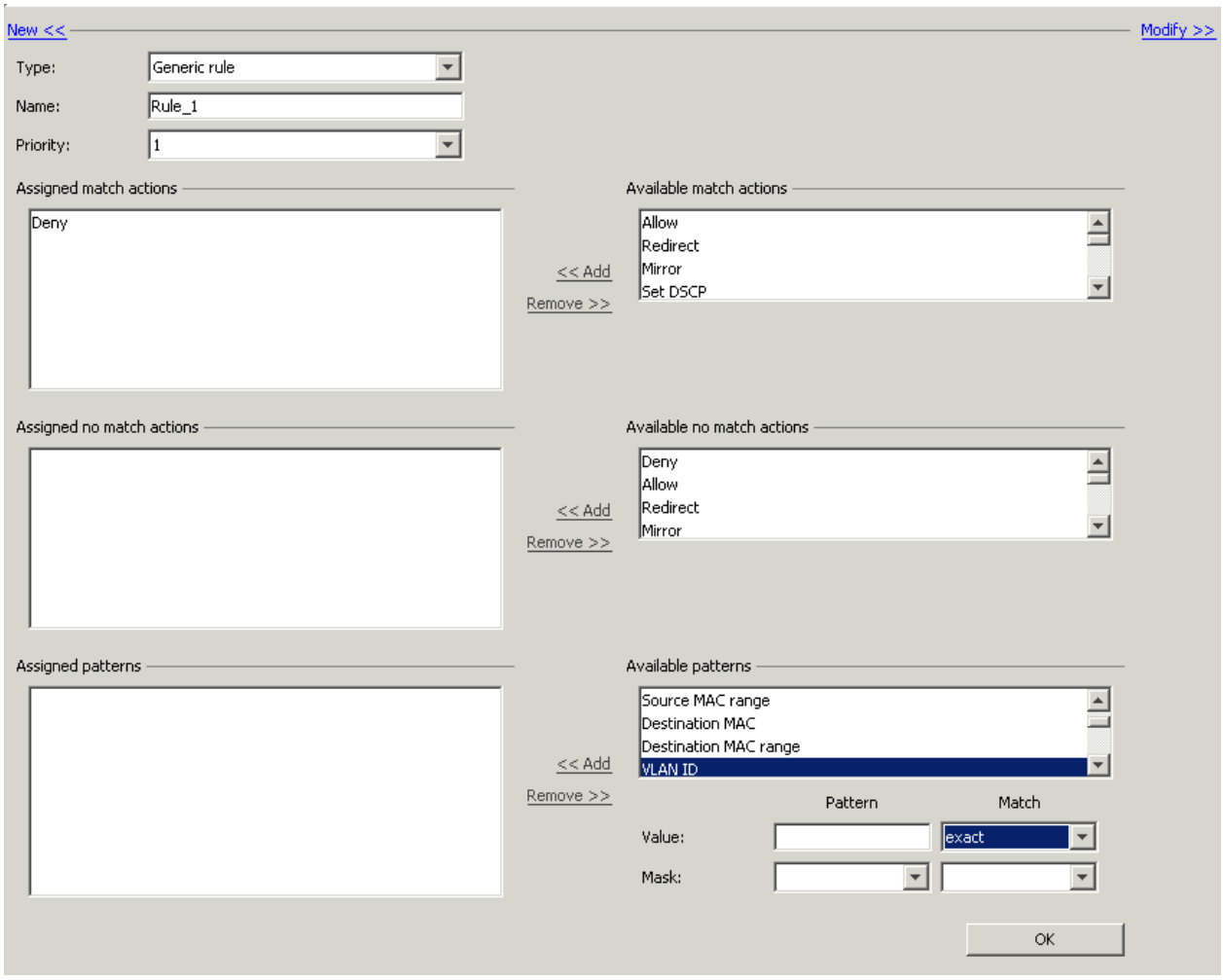

Figure 75 Rule Configuration Page (CXU)

2. Click the "New>>" action field to create a new rule, see Figure 75 (if not already expanded).
3. Select the rule type "Generic rule”.
4. Enter a unique rule name (space is not allowed).

5. Choose the “Tagging mode” (only for IU_GPON) if there is a double or single tag expected in the rule.
   If both “single tagged” and “double tagged” frames can arrive, two rules for one purpose are possible - one for single and one for double tagged frames. The **NE** automatically checks the Ethertype to exclude false matches.
6. Enter the rule “Priority” level (0...7).
7. Repeat the following steps until the pattern assignment is completed:
   See the current release notes to choose valid combinations of patterns and values for a particular unit.
   - Select a required pattern from the "Available patterns” drop-down list.
   - Choose the "Pattern value”:

Pattern	Value1/Value2	Description
Bridge Port	N/A	Not supported.
Ingress Port	Select: Port	Physical source GPON port that corresponds with the rule. The rule is only applied to frames coming from this port. Ingress port pattern and rule “Flow” pattern must not be used together in one rule. CXU: Not supported.
Source MAC		Selected port by a single source MAC address
Destination MAC		Selected port by single destination MAC address
VLAN ID	2..4093	Used if no inner VLAN is available else this is the outer VLAN ID
	Select: 1..12	VID mask bit number A valid mask consists of 1 to 12 consecutive 1, starting with 1 in MSB. The NE assumes 111111111111 as default if no mask is present.
Inner VLAN ID	2..4093	
	Select: 1..12	VID mask bit number
Priority	0..7	VLAN .1p priority level
Inner Priority	0..7	VLAN .1p priority level (inner tag).
ToS	0..255	Only one of this 3 patterns may be selected per rule.
DSCP	0..63	
IP precedence	0..7	
Ethernet type	4 Hex chars	e.g.: 0800 - IP, 8863 & 8864- PPPoE
Source IP address	A.B.C.D	A single IPv4 address
Source IP address Subnet mask	A.B.C.D	IPv4 subnet mask
Destination IP address	A.B.C.D	A single IPv4 address
Destination IP address Subnet mask	A.B.C.D	IPv4 subnet mask
Source Port		Selected TCP/UDP source port. Source port will only be evaluated if an “IP protocol” pattern equal UDP or TCP is given, otherwise it will be ignored.
Destination Port		Selected TCP/UDP destination port. Destination port will only be evaluated if an “IP protocol” pattern equal UDP or TCP is given, otherwise it will be ignored.
Flow	Select: - downstream - bidirectional	The flow-direction for which this rule should work. For IU_GPON due to hardware restrictions all rules work in upstream direction.

Table 74 Available Pattern Values

Pattern	Value1/Value2	Description
IP protocol	0..255	Used L4-protocol type. Needed to evaluate the correct IP-port pattern (see RFC 791)
Source MAC mask	12 Hex	Sets source MAC mask (e.g. FF:FF:FF:FF:00:00)
Destination MAC mask	12 Hex	Sets destination MAC mask
Message type		Used for IGMP MC, only if “IP protocol” pattern is set to ICMP (RFC 950).
Message code		Used for IGMP MC, only if “IP protocol” pattern is set to ICMP and a “Message type” pattern is given (RFC 950).

Table 74 Available Pattern Values (Cont.)

- Select the "Match type" per pattern value to configure how the corresponding pattern value becomes accepted by the traffic flow:
  Exact - If the frame matches with the defined pattern value, the “Assigned match action" is performed, else the “Assigned no match action" becomes active.
  Exclude - Match all excepts this value.
  Inside one rule, all used match values have to be “Exact” or “Exclude”.
- Click the "Add>>" action field to map the defined pattern to the “Assigned patterns” box.
  Several patterns are combined by logic-AND.

8. Repeat the following steps for "Available match actions" (“Available no match actions") until the assignment is completed:
   - Select an action from the "Available match actions" (“Available no match actions") drop-down list.

Action	Value	Description	Match Action	No-Match Action
Deny	N/A	Matching frames will not be forwarded	x	x
Allow	N/A	Matching frame will be forwarded	x	x
Redirect	Select "Module": CXU, IUGPON, IU Uplink cards Select "Port": CXU: 5 x Eth, IUGPON: 4 x GPON IU_10x1G: 10 x Eth.	Matching frame will be redirected over the selected bridge port (uplink interface).	x	x
Mirror	N/A	Copies matching frames to mirror monitor port.	x	x
Set **DSCP**	0..63	Sets DSCP value in matching frames.	x	x
Set Priority	0..7	Schedules matching frames (queue mapping) according given priority value.	x	x
Change tag priority	0..7	Changes .1p priority value in VLAN tag.	x	x
Change tag priority with ToS	N/A	Copies IP precedence bits of ToS field into .1p priority of VLAN tag.	x	x
Set IP precedence	0..7	Sets IP precedence bits in ToS field.	x	x
Change **ToS** with tag priority	N/A	Sets the ToS with tag priority.	x	x
Rate limit	0..1000	Applies rate limiting for matching frames. Enter the value for bandwidth modification in Mbps.	x	

Table 75 Available Actions

Action	Value	Description	Match Action	No-Match Action
Change VLAN ID	1..4093	Changes VLAN-ID in VLAN-Tag of matching frames by the "Action value".	x	
Copy to CPU	N/A	Copies matching frames to CPU port.	x	x
Count	N/A	Initiates counting of matching packets. The NE supports only a limited number of counters at same time and is rejecting this rule if the number of timers is exceeded.	x	

Table 75 Available Actions (Cont.)

- If necessary, enter the "Action value".
- Click the "<<Add" action field to map the defined action to the "Available match actions" (“Available no match actions") box.

Notice the following restrictions:

- Rules with set but not supported action values will be rejected by the **NE**.
- Conflicting actions:
  - The match actions may be “allow” and the no-match actions may be “deny”.
  - “Change tag priority” and “Change tag priority with ToS” actions, “Change ToS” and “Change ToS with tag priority” actions are not allowed together in one action bit field.
- If all rule matches are “Exclude”, the “Match action” and “No match action” including the action parameters will be handled by the NE as if they have been swapped.

9. Click the "OK" button to confirm the rule settings.

For an example of creating rules see Chapter 26 VLAN Mirroring.

26 VLAN Mirroring

This chapter contains the step-by-step instructions how to configure the mirroring of VLAN traffic over IU_GPON port to a particular VLAN associated with an IU_1x10GE port.

The Mirror port must be another than the destination port of the origin traffic flow. Due to this fact, an additional uplink card is necessary.

26.1 Configuring the Mirror Port

1. Click “NE:hiX5750 ⇨ Bridge”.
2. Define the mirror port through selecting the uplink interface “IU10GE:1O:E#” from the "Module" drop-down list.
3. Choose "Port" number “1”.
4. Click the "Apply” button to confirm the changes.

26.2 Creating the VLAN Rules

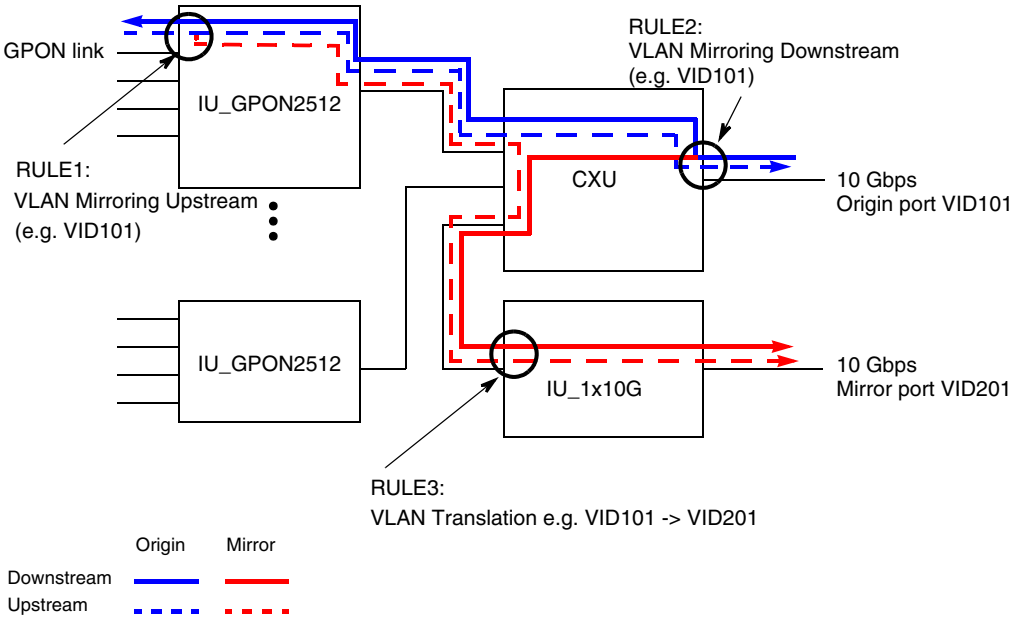

Figure 76 VLAN Mirroring (Principle)

The implementation of VLAN mirroring requires 3 rules:

- Rule 1 - Upstream Mirroring on IU_GPON
- Rule 2 - Downstream Mirroring on CXU
- Rule 3 - VLAN Translation on IU_1x10G.

To get basic information see the chapters:

- 25 Rules
- 15.1 Creating a VLAN.

Rule 1 - Upstream Mirroring on IU_GPON

1. Click “NE:hiX5750 ⇨ IUGPON:2512:E# ⇨ Bridge ⇨ Rules”.
2. Click the “New>>” action field to uncover the rule configuration area (if not already expanded).
3. Enter a unique rule name (space is not allowed).
4. Choose the “Tagging mode”.
5. Select the type "Generic rule” and set the rule priority level (0...7).
6. Select "Mirror" from the "Available match actions" drop-down list and then click the "<< Add" action field.
7. Select "VLAN ID" from the "Available patterns" drop-down list.

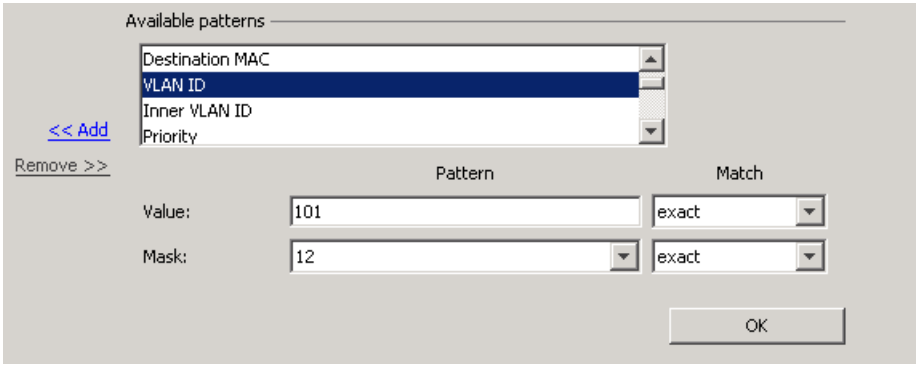

Figure 77 Rule 1: VLAN Selection for Mirroring

- Enter the VID of the origin VLAN into the "Pattern” value field (e.g. 101).
- Select the VID “Mask” bit number “12”.
- Choose the “Match” type "exact" for the two pattern values.
- Click the "<< Add" action field.

8. Click the "OK" button to confirm all settings.
   The new rule is listed on the top of the page.

Rule 2 - Downstream Mirroring on CXU

1. Click “NE:hiX5750 ⇨ CXUVR:1O:4E:E#109 ⇨ Bridge ⇨ Rules”.
   Select the type "Generic rule” and set the rule priority level (0...7).
2. Click the “New>>” action field to uncover the rule configuration area (if not already expanded).
3. Enter a unique rule name (space is not allowed).
4. Select the type "Generic rule” and set the rule priority level (0...7).
5. Choose "Mirror" from the "Available match actions" selection box and then click "<< Add".
6. Select "VLAN ID" from the "Available patterns" drop-down list.
   - Enter the VID of the origin VLAN into the "Pattern” value field (e.g. 101).
   - Select the VID “Mask” bit number “12”.
   - Choose the “Match” type "exact" for the two pattern values.
   - Click the "<< Add" action field.
7. Choose "Flow" from the "Available patterns" drop-down list.
   - Select pattern value "downstream".
   - Select the “Match” type "exact".
   - Click the "<< Add" action field.

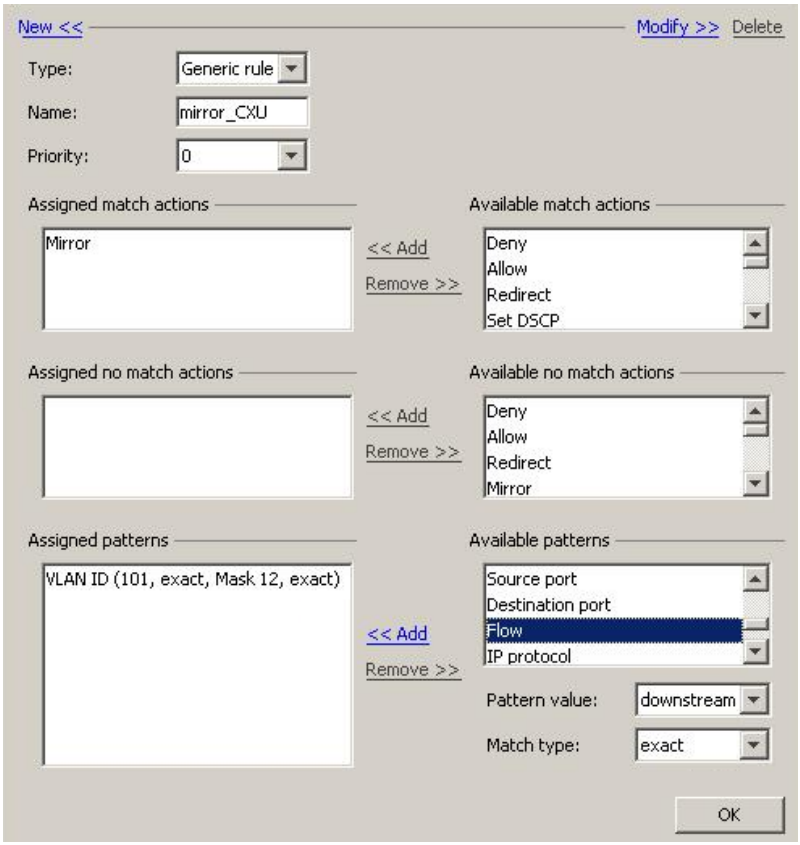

Figure 78 Rule 2: Selection of the Flow Direction on the CXU

8. Click the "OK" button to confirm all settings.
   The new rule is listed on the top of the page.

Rule 3 - VLAN Translation on IU_1x10G

1. Click “NE:hiX5750 ⇨ IU10GE:1O:E# ⇨ Bridge ⇨ Rules”.
2. Click the “New>>” action field to uncover the rule configuration area (if not already expanded).
3. Enter a unique rule name (space is not allowed).
4. Select the type "Generic rule” and set the rule priority level (0...7).
5. Select "Change VLAN ID" from the "Available match actions" drop-down list.
   - Enter the VID of the mirrored VLAN into the "Action value" field (e.g. 201).
   - Click the "<< Add" action field.

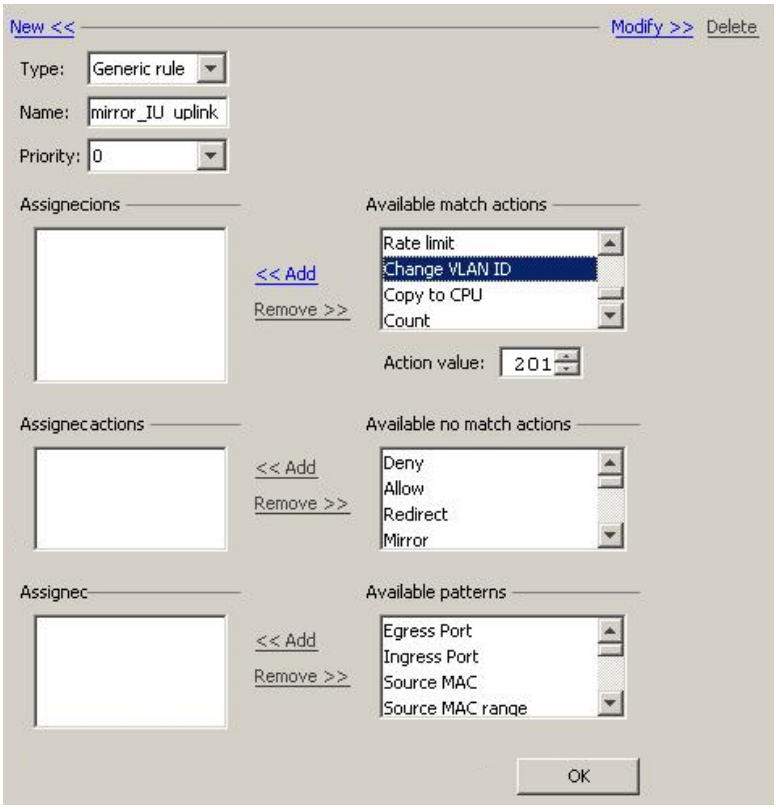

Figure 79 Rule: VLAN Translation

6. Select "VLAN ID" from the "Available patterns" drop-down list.
   - Enter the VID of the origin VLAN into the "Pattern" value field (e.g. 101).
   - Select the VID "Mask" bit number "12".
   - Choose the "Match" type "exact" for the two pattern values.
   - Click the "<< Add" action field.
7. Click the "OK" button to confirm all settings.
   The new rule is listed on the top of the page.

27 Lock / Unlock Ports

The “Admin state” of all physical ports (GPON ports, Ethernet uplink ports, E1/DS1 ports, subscriber ports) and logical ports (e.g. router ports) can be changed between “unlocked” and “locked”. After creating a new IU_GPON card or ONT/MDU, all its ports are locked. Units that were created offline have the status “planed”.

The “Unlock” (“Lock”) button of a specific unit is located on the “**General**” dialog page.

The button “Unlock” (“Lock”) for a specific port can be found on the dialog page (tab) that is designated as this port, e.g. “PON”, “Ethernet”, “E1”, “VoIP”, “POTS” etc.

The **CLI** or **LCT** must be used to lock/unlock the CXU uplink ports.

28 Database Backup

1. Click to highlight the NE root in the SNMP tree.
2. In the **EM** PX main menu, click the “Maintenance ⇨ NE Maintenance” commands to display the “**Backup**” dialog page.
3. Click the “Backup” button.

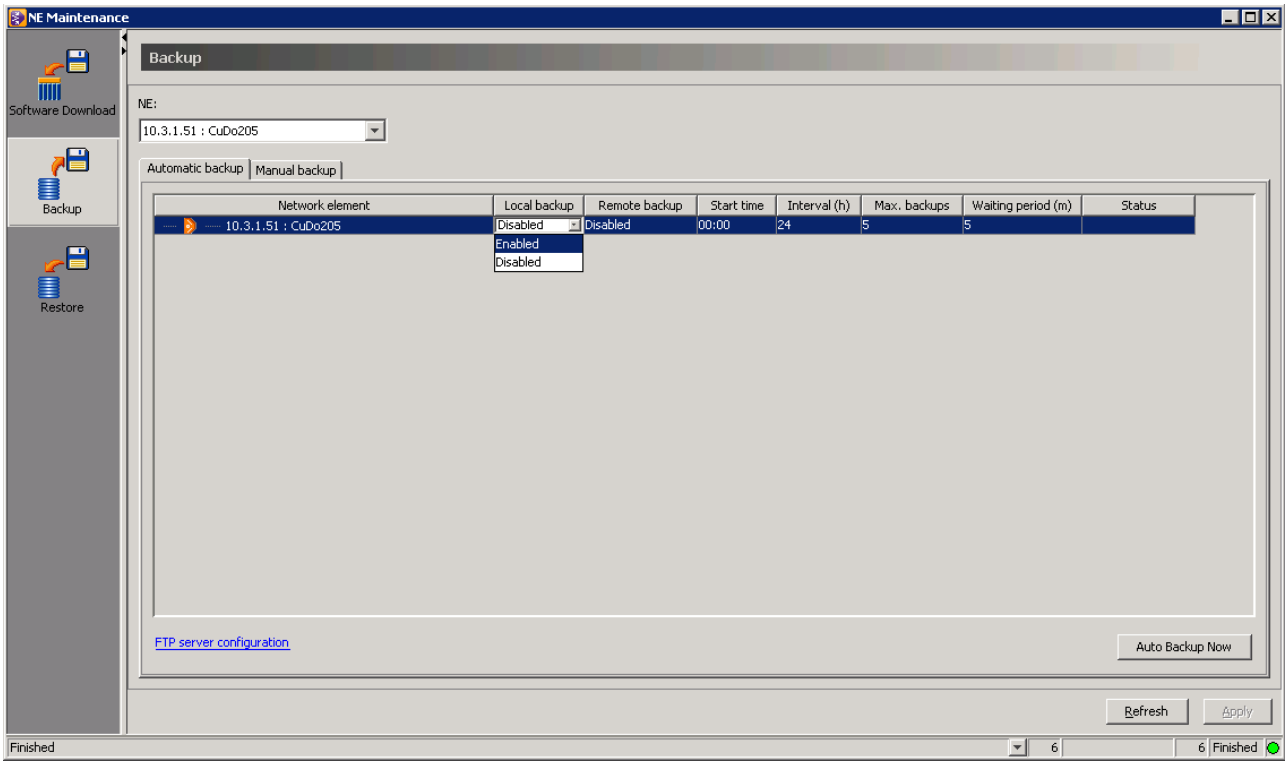

Figure 80 Database Backup

4. Choose the new NE from the “NE” drop-down list.

The destination of the backup file is the same as configured before. Follow the link “FTP server configuration” in order to change the FTP settings (see Chapter 5.3 Configuring the FTP Server Access).

Automatic Backup

In order to increase the reliability of the system and improve operation comfort, the configuration data can be stored automatically in the CXU's persistent memory (local) as well as remotely on the data **FTP** server. Note that the auto-backup will be performed by the **NE** itself. There is no necessity that the EM PX R2.0 is running for this task. To configure the auto-backup parameters perform the following tasks:

1. Click into the following input fields to set the backup options:

Setting	Description
Local backup	Choose “Enable” or “Disable” local backup on persistent memory of CXU.
Remote backup	Choose “Enable” (Note that local backup must also be enabled) or “Disable” remote backup on FTP server.

Table 76 Auto-Backup Options

Setting	Description
Start time	Start time basis (NE uses always a UTC time base) for remote backup of configuration database after system restart, backup timer re-configurations or system clock reset. The first backup will be started at this time + “Interval (h)” value and then after each interval. Valid values: 0:00 am - 23:59 pm, default: 0:00.
Interval (h)	Interval between two remote backup operations in hours. Backup is started only if there were relevant configuration changes during the last period. Valid values: 1..48 hours, default: 24 hours.
Max. backups	Maximum number of different backup files on the remote FTP server. Valid values: 1..32, default: 5.
Waiting period (m)	Enter the period in minutes the system waits after last changes of configuration before starting the local backup. Valid values: 1..59 minutes, default: 5 minutes.

Table 76 Auto-Backup Options (Cont.)

2. Click the “Apply” button to confirm.
3. If desired, click the “Auto Backup Now” button to start the procedure immediately.

Manual Backup

1. Click the “Manual backup” tab.
2. Click to mark the “Selection” check box.
3. Click the “Backup” button to start the procedure.

The name of the backup file is automatically set and displayed in the “Backup file” field. Afterwards, the file name can be changed through clicking in this field.

Schedule

In order to set periodic backups, a schedule job must be created as follows:

1. Click to mark the “Selection” check box.
2. Click the “Schedule” button to display the “**New schedule**” dialog box (Figure 81).

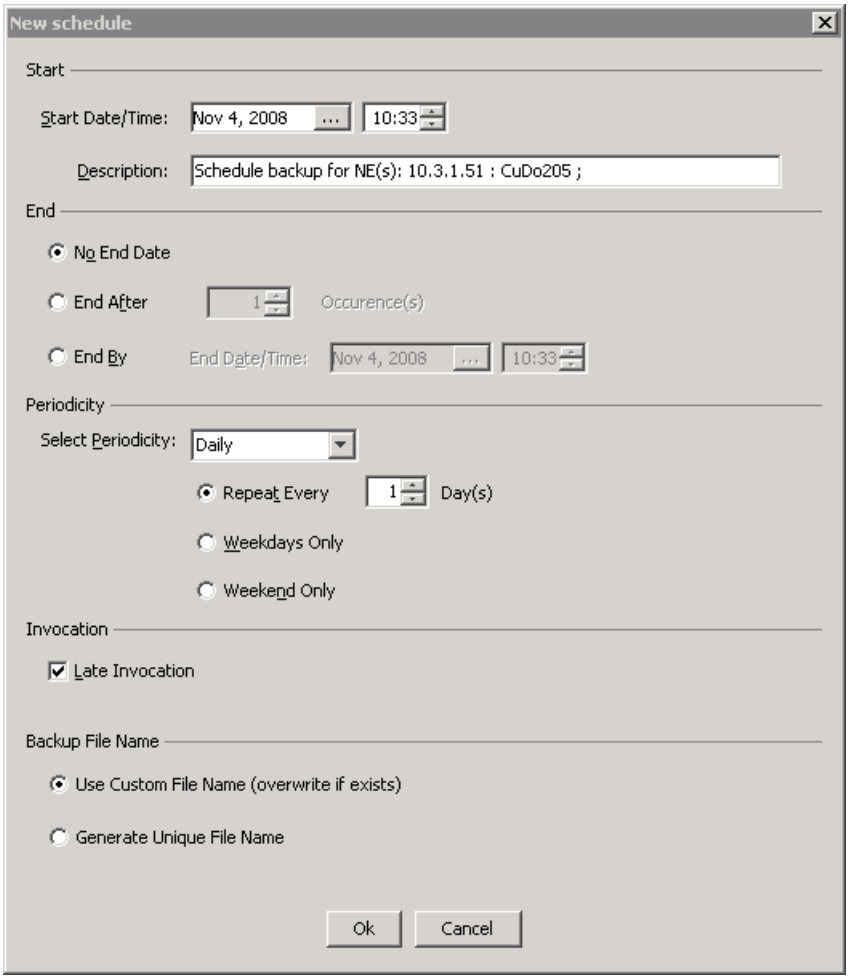

Figure 81 Backup Scheduler

3. Choose the properties of a periodic database backup.
4. Click the “OK” button to activate the settings.

29 Abbreviations

ACI AccessIntegrator

ACI-E AccessIntegrator Ethernet

ACL Access Control List

ADSL Asynchronous Digital Subscriber Line

AES Advanced Encryption Standard

AIS Alarm Indication Signal

AMI Alternative Mark Inversion

ANI Access Node Interface (PON Interface)

ANSI American National Standards Institute

APC Angled Polished Connector

APS Application Program Software

ARP Address Resolution Protocol

AS Autonomous System

ASCII American Standard Code for Information Interchange

ATM Asynchronous Transfer Mode

AWG American Wire Gauge

B8ZS Binary eight Zero Substitution

BCSC Broadcast Storm Control

BER Bit Error Rate

BGP Border Gateway Protocol

BITS Building Integrated Timing Supply

BPDU Bridge Protocol Data Unit

BRAS Broadband Remote Access Server

CAC Connection Admission Control

CAS Channel Associated Signaling

CATV **(1)** Community Antenna Television
(2) Cable Television

CE Conformité Européenne

CES Circuit Emulation Service

CFR Code Failure Rate

CLI Command Line Interface

CLIP Calling Line Identification Presentation

CMOS Complementary Metal Oxide Semiconductor

CNN Composite Network Node

CORBA Common Object Request Broker Architecture

CoS Class of Service

CPE Customer Premises Equipment

CTP Connection Termination Point

CXU Central Switch Fabric Unit

DA Destination Address

DBA Dynamic Bandwidth Allocation

DBMS Database Management System

DC Direct Current

DCE Data Communication Equipment

DFB Distributed Feedback (Laser)

DHCP Dynamic Host Configuration Protocol

DIN Deutsche Industrie Norm (German Standard)

DNS Domain Name System

DR Designated Router

DS Downstream

DS0 Digital Signal 0 (64 kbps)

DS1 First Level TDM hierarchy / Digital Signal 1 (1.544 kbps)

DSCP DiffServe Code Point

DSL Digital Subscriber Line

DSLAM DSL Access Multiplexer

DTMF Dual Tone Multi Frequency

E1 Europe - First level of TDM hierarchy (2.048 kbps)

EEPROM Electrically Erasable Programmable Read-Only Memory

EM Element Manager

EMC Electromagnetic Compatibility

EMI **(1)** Electromagnetic Interference
(2) External Machine Interface

EMS Element Management System

EN European Norm

ESD Electro Static Discharge

ESF Extended Service Frame

E-SFU Ethernet Single-Family Unit

ETSI European Telecommunications Standards Institute

FE Fast Ethernet

FEC Forward Error Correction

FP Febry Perot

FSAN Full Service Access Network

FTP File Transfer Protocol (TFTP = Trivial FTP)

FTTP Fiber to the Premises

GAL GEM Adaption Layer

GE Gigabit Ethernet

GEM GPON Encapsulation Method

GPON Gigabit Passive Optical Network

GR Generic Requirements

GTC GPON Transmission and Convergence

HOL Head of Line Blocking

I2C Inter Integrated Circuit

ICMP Internet Control Message Protocol

ID Identifier

IEC International Electronical Commission

IEEE Institute of Electrical and Electronics Engineers

IETF Internet Ingeneering Task Force

IF Interface

IGMP Internet Group Management Protocol

IP Internet Protocol

IP-DSLAM IP Digital Subscriber Line Multiplexer

IPoA IP over ATM

IPoE IP over Ethernet

IPTV Internet Protocol Television

IRL	Input Rate Limiting
IS	Intermediate System
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardisation
ISP	Internet Service Provider
IST	Internal Spanning-Tree
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union - Telecommunication Standardisation Sector
IU	Interface Unit
IU_GPON	Interface Unit with GPON Interfaces
LACP	Link Aggregation Control Protocol
LAG	Link Aggregation Group
LAN	Local Area Network
LCT	Local Craft Terminal
LOF	Loss of Frame
LOS	Loss of Signal
LRE	Long Reach Ethernet
LSA	Link State Advertisments
LSP	Link State Packet
MAC	Medium Access Control
MAN	Metro Area Network
MC	Multicast
MDU	Multi Dwelling Unit
MGC	Multi Gateway Controller
MIB	Management Information Base
MSTP	Multiple Spanning Tree Protocol
MTU	Multi Tenant Unit
NBMA	nonbroadcast Multi-access
NE	Network Element
NEBS	Network Equipment Business Systems
NMS	Network Management System
NNI	Network to Network Interface

NTR	Network Timing Reference
ODN	Optical Distribution Network
OLT	Optical Line Termination
OMCI	ONU Management and Control Interface
ONT	Optical Network Terminal
ONU	Optical Network Unit
OS	Operating System
OSPF	Open shortest Path first
PC	**(1)** Physical Contact **(2)** Personel Computer
PCM	Pulse Code Modulation
PID	Product Identification Data
PIM	Protocol Independent Multicast
PIM-DM	Protocol Independent Multicast - Dense Mode
PIM-SM	Protocol Independent Multicast - Sparse Mode
PIM-SSM	Protocol Independent Multicast - Source Specific Multicast
PLL	Phase Lock Loop
PLOAM	Physical Layer Operation Administration
PM	**(1)** Power Module **(2)** Performance Monitoring
PON	Optical Passive Network
POTS	Plain Old Telephone Service
PPPoE	Point to Point Protocol over Ethernet
PPTP	Point-to-Point Tunneling Protocol
PSD	Power Spectral Density
PSTN	Public Switched Telephone Network
PTC	Positive Temperature Coefficient
PVC	Permanent Virtual Connection
PVID	Port VLAN Identifier
QoS	Quality of Service
RF	Radio Frequency
RGW	Residential Gateway

RIP	Routing Information Protocol
RMON	Remote Monitoring
RP	Rendezvous Point
RSTP	Rapid Spanning-Tree Protocol
RTCP	Realtime Control Protocol
RTP	Rapid Transport Protocol
R-VLAN	Routing VLAN
SAPS	System Application Program Software
SBU	Single Business Unit
SC	Spherical Contact
SFP	Small Form-Factor Pluggable
SFU	Single-Family Unit
SGMII	Serial Gigabit Media Independent Interface
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SNR	Signal-to-Noise Ratio
STP	Spanning Tree Protocol
SW	Software
T-CONT	Traffic Container
TC	Transmission Convergence Layer
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TMN	Telecommunication Management Network
ToS	Type of Service
TP	Termination Point
TV	Television
UDP	User Datagram Protocol
UNI	User Network Interface
UPC	Ultra Polished Connector
US	Upstream
VCC	Virtual Cross Connection

VDE	Association for Electrical, Electronic & Information Technologies
VDSL	Very High Speed Digital Subscriber Line
VID	VLAN ID
VLAN	Virtual LAN
VoD	Video on Demand
VoIP	Voice over IP
VR	Virtual Router
VRF	Virtual Routing and Forwarding
WDM	Wavelength Division Multiplexing
WFQ	Weighted Fair Queuing
WRED	Weighted Random Early Detection/Discard
WRR	Weighted Round Robin Queuing
XFP	Optical Form-Factor Pluggable
xTU	xDSL Transmission Unit (xTU-C -> central office side, xTU-R -> remote side)