Nokia Siemens Networks

SURPASS hiX 5750 R2.0

Operation Manual CLI

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 272 pages.

List of Figures

List of Tables

Change History

5. Update (12.12.2008)

System Access (3)

- Chapter updated

System Basic Configuration (4)

- Automatic S-APS upgrade added
- Invalid commands deleted
- Commands added/changed

Alarms (6)

- New show command added

OLT Equipment (7)

- New show commands added

ONU Equipment (9)

- Create ONU command changed, invalid command deleted

Performance Monitoring (10.10)

- Calculation algorithms of PM objects added
- Commands added, changed

Payload-Counters (10.11)

- Commands modified

Voice over IP (12)

- Section PM changed
- Commands added, changed

Bridges (14)

- Tagging rules and enhanced tagging profile added

Quality of Service (QoS) (17)

- Invalid commands deleted

DHCP and PPPoE (18)

- Command changed

IP Anti-Spoofing (23)

- New show command added

4. Update (13.10.2008)

3. Update (10.06.2008)

2. Update (17.04.2008)

1. Update (31.01.2008)

Initial release (21.12.2007)

1 Introduction

The hiX 5750 R2.0 provides a series of CLI (Command Line Interface) commands for configuring and managing the **NE** from local or remote place by a console terminal that is installed on PC or workstation. This user manual explains how to access the CLI and how to use it to configure the NE hiX 5750 R2.0. Related commands are grouped together and organized into chapters based on their most common usage. In many cases, usage examples and configuration instructions are given.

For a detailed system overview refer to the documents itemized in section 1.4 Related Documents.

ℹ Depending on the software load used in the hiX 5750 R2.0, some features described in this document may not be supported. Refer to the current release notes of the hiX 5750 R2.0 to determine the provided features. If the information in the release notes differs from the information in this manual, follow the release notes.

1.1 Audience

This manual is intended for hiX 5750 R2.0 operators and maintenance personnel. It assumes knowledge of **OLT** and **ONU** configuration. In particular, users should be familiar with the following:

- Ethernet technology and standards
- Virtual local area networks (VLANs)
- Unicast IP routing concepts and protocols
- Internet IP protocols and concepts
- **DSL** technology and standards
- Basic knowledge about the personal computer and its applications.

1.2 Document Conventions

The following symbols are used in order to boost reader’s attention.

ℹ **NOTE**: This is the symbol for additional information that may be of special importance. Notes contain also helpful suggestions or references.

⚠ **DANGER**: This warning symbol means danger.

You are a situation that could causes bodily injury, equipment damage, or loss of data.

Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents by making quick guide based on this guide.

1.3 Typographical Conventions

Command Notation

This document uses the following conventions when presenting the syntax of a command.

Notation	Description
Bold style lowercase term	Indicates keywords that must be typed exactly as shown in the command description. For better readability keywords are structured with hyphen ("-"), Example: **show system-version**.
Italic style uppercase term	Indicates a user-supplied parameter that may be either required or optional. For better readability parameters are structured with underscore ("_"). Examples: *NAME*, *PROFILE*, *SEVERITY_TABLE_INDEX*, ...
{ }	Braces indicate a group of required keywords or variables. One, and only one, item inside the braces must be entered. Nesting is also possible. Example: {internal | external {1|2}} means internal or external 1 or external 2.
[ ]	Square brackets indicate optional parameters. Choose none; or select one or more of the listed keywords or variables. Nesting is also possible. Example: **show bridgeport** [*PORTS*]
< >	Angle brackets indicate the valid range of numbers, endpoints inclusive. Example: **qos watermark** <0-7> <0-100> <0-100>
|	A vertical bar indicates a choice of parameters, e.g. keywords placed within brackets are separated by vertical bars. Select one item from the list. Example: **bridgeport** *PORTS* **mode** { ipoa | ipoe }

Table 1 Command Notation of CLI

Do not enter brackets, braces, or vertical bars as part of the command.

1.4 Related Documents

In addition, other related documents are available, describing the AccessIntegrator Element Manager EM PX R2.0 software and the hiX 5750 R2.0 system. These documents are described in Table 2.

Title	Part number	Topics covered
AccessIntegrator Element Manager EM PX R2.0	A50010-X3-G200-*-76K5	Installation of Element Manager EM PX R2.0 software and its supporting software components. (IMN) Backup and restore of AccessIntegrator data, configuration of domain and permission. (ADMN) Operation and configuration of hiX 5750 network element using the Element Manager EM PX R2.0. (OGL)
SURPASS hiX 5750 R2.0	A50010-X3-G201-*-76K5	SURPASS hiX 5750 R2.0 functions and hardware descriptions. (SYD) Instructions for the commissioning of a hiX 5750 R2.0 Installation and Test Manual (ITMN) Commands for configuring the hiX 5750 R2.0 via console or telnet, Command Line Interface (CLI)

Table 2 Related Documentation

1.5 GPL/LGPL Warranty and Liability Exclusion

The product SURPASS hiX5750 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 Using CLI

This chapter describes the CLI (command line interface) modes in which configuration commands of the hiX 5750 R2.0 must be executed and provides helpful tips for the effective usage of CLI.

2.1 Command Modes Overview

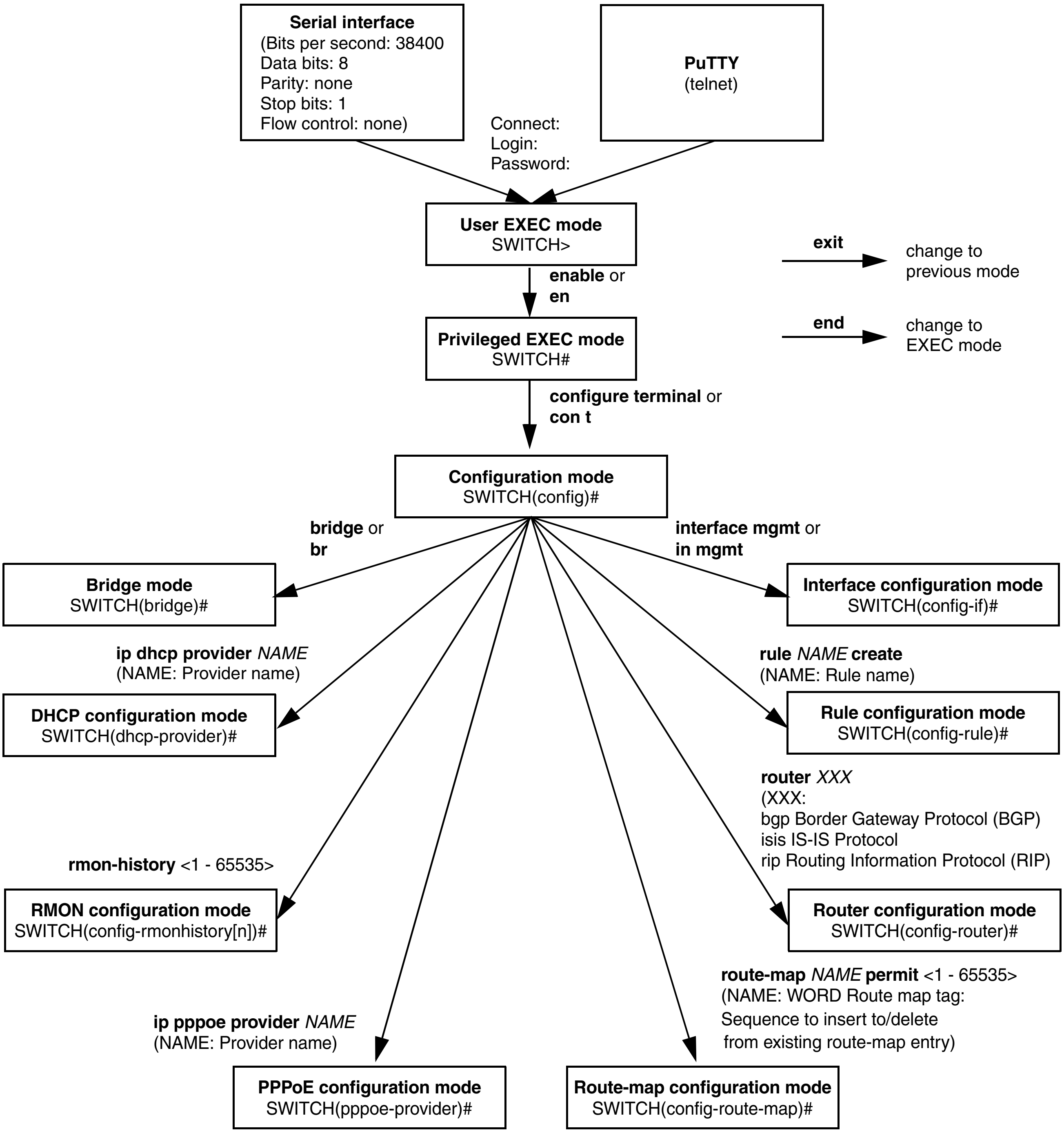


Figure 1 Overview of Configuration Modes

2.2 Entering a Command Mode

2.2.1 User Exec Mode

When a user logs in successfully, the command mode is on *User exec* mode. This is a read only mode provided to all users accessing to the **GPON**. The prompt is displayed as `SWITCH>` by default.
In *User e*xec mode, it is possible to check the system configuration.

Command	Function
show running-config	Shows running system information.

2.2.2 Privileged Exec Mode

In order to get the right to configure the system, enter to *Privileged exec* mode by using the **enable** command. After this, the command prompt changes from `SWITCH>` to `SWITCH#`.

Command	Mode	Function
enable	User	Changes from *User exec* mode into *Privileged Exec* mode.

To enhance the security, it is possible to assign a password to the *Privileged exec* mode.

The commands of *Privileged exec* mode shown in the below table are used to display the changes of terminal configuration, network status, and system information.

Command	Function
clock	Inputs time and date in system.
configure terminal	Enters into *Configuration* mode.
telnet	Connects to another device through telnet.
terminal line	Configures the number of lines to be displayed in screen.
traceroute	Traces transmission path of packet.
where	Finds users accessed to system through telnet.

Table 3 Main Commands of Privileged Exec Mode

2.2.3 Configuration Mode

In order to enter into *Configuration* mode, execute the command **configure terminal** on *Privileged exec* mode. The system prompt changes from `SWITCH#` to `SWITCH(config)#`.

Command	Mode	Function
configure terminal	Privileged	Enters from *Privileged* exec mode into *Configuration* mode.

Configuration mode is used to configure functions for general system management and **SNMP**. In addition, a user can enter into *Bridge/Interface configuration* mode from that level.

Table 4 shows a couple of important main commands of *Configuration* mode.

Command	Function
access-list	Configures policy to limit routing information on the standard of **AS**.
arp	Registers **IP** address and **MAC** address in **ARP** table.
bridge	Enters into *Bridge configuration* mode.
clear	Reset functions.
hostname	Changes hostname of system prompt.
exec-timeout	Configures auto-logout function.
interface	Enters into *Interface configuration* mode.
passwd	Changes the password.
qos	Configures **QoS**
restore factory-defaults	Initiates the configuration of switch.
route-map	Enters into *Config-route-map* mode.
router	Enters into *Router configuration* mode.
snmp	Configures SNMP
syslog	Configures syslog
time-zone	Configures time zone

Table 4 Main Commands of Configuration Mode

2.2.4 Rule Configuration Mode

To enter into *Rule configuration* mode, the **rule create** command is used in *Configuration* mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-rule[name])#`.

Command	Mode	Function
rule *NAME* **create**	Config	Changes from *Configuration* into *Rule configuration* mode.

In *Rule configuration* mode, it is possible to configure the condition and operational method for the packets which rule function is applied to.

Table 5 shows a couple of important main commands of *Rule configuration* mode.

Command	Function
apply	Configures rule and applies it to the GPON **OLT**.
mac	Configures the packet condition by MAC address.
match	Configures operational condition which meets the packet condition.
no-match	Configures the operational condition for the packet which does not meet the packet condition.
port	Configures the packet condition with port number.
prio	Configures the priority for rule.

Table 5 Main Commands of Rule Configuration

2.2.5 DHCP Configuration Mode

To enter into **DHCP** configuration mode, execute the **ip dhcp provider** command on *Configuration* mode. The system prompt changed from `SWITCH(config)#` to `SWITCH(dhcp-provider)#`.

Command	Mode	Function
ip dhcp provider *NAME*	Config	Enters into *DHCP configuration* mode to configure DHCP.

DHCP configuration mode is used to configure the DHCP relay agent, option82, and PPPoE option 105.

Table 6 shows main commands of DHCP configuration mode.

Command	Function
ip	Configures DHCP relay.
server	Configures DHCP server address.
option82	Configures DHCP option82.
option105	Configures PPPoE option 105.

Table 6 Main Commands of the DHCP Configuration Mode

2.2.6 RMON Configuration Mode

To enter into *RMON-history* mode, execute the **rmon-history** command on *Configuration* Mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-rmonhistory[n])#`.

Command	Mode	Function
rmon-history <1-65535>	Config	Changes into *RMON configuration* mode.

Table 7 shows a couple of important main commands of *RMON configuration* mode.

Command	Function
active	Activates the history.
owner	Shows the subject, which configures each RMON and uses related information.

Table 7 Main Commands of the RMON Configuration Mode

2.2.7 Bridge Configuration Mode

By executing the **bridge** command on *Configuration* mode, the system prompt changes from `SWITCH(config)#` to `SWITCH(bridge)#`.

Command	Mode	Function
bridge	Config	Changes from *Configuration* mode into *Bridge configuration* mode.

Bridge configuration mode is used to manage **MAC** addresses and to configure **GPON** functions of layer 2 such as **VLAN**, mirroring, **STP**.

Table 8 shows a couple of main commands of *Bridge configuration* mode.

Command	Function
lacp	Configure **LACP** function.
mirror	Configures mirroring function.
trunk	Configures trunk-function.
vlan	Configures VLAN function.

Table 8 Main Commands of the Bridge Configuration Mode

2.2.8 Interface Configuration Mode

To change into *Interface configuration* mode, execute the **interface** *command* on *Configuration* mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-if)#`.

Command	Mode	Function
interface *INTERFACE*	Config	Enters from *Configuration* mode into *Interface configuration* mode.

Interface configuration mode is used to assign **IP** addresses in Ethernet interface and to activate or deactivate interfaces.

Table 9 shows a couple of main commands of *Interface configuration* mode.

Command	Function
description	Makes description of interface.
ip	Assigns IP address.
shutdown	Deactivates interface.
mtu	Set mtu value to interface

Table 9 Main Commands of the Interface Configuration Mode

2.2.9 Router Configuration Mode

To change into *Router configuration* mode, execute the **router** command on *Configuration* mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-router)#`.

Command	Mode	Function
router *IP-PROTOCOL*	Config	Changes into *Router configuration* mode.

According to the used routing protocol, the *Router configuration* mode is divided into **BGP**, **RIP**, and **IS**IS.

Table 10 shows a couple of main commands.

Command	Function
distance	Configures distance value to find better route.
neighbor	Configures neighbor router.
network	Configures network to operate each routing protocol.
redistribute	Registers transmitted routing information to another router ’s table.

Table 10 Main RIP Commands oft the Router Configuration Mode

2.2.10 Route-Map Configuration Mode

To change into *Route-map configuration* mode, execute the **route-map** *command* on *Configuration* mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-route-map)#`.

Command	Mode	Function
route-map *NAME* { permit I deny } <1-65535>	Config	Changes into *Route-map configuration* mode.

On *Route-map configuration* mode routing filter can be configured.

Table 11 shows a couple of important main commands.

Command	Function
match	Transmits routing information to specified place.
set	Configures router address and distance.

Table 11 Main Commands of the Route-Map Configuration Mode

2.2.11 PPPoE Configuration Mode

To change into **PPPoE** configuration mode, execute the **ip pppoe provider** *command* on *Configuration* mode. The system prompt changes from `SWITCH(config)#` to `SWITCH(pppoe-provider)#`.

Command	Mode	Function
ip pppoe provider *NAME*	Config	Changes into *PPPoE configuration* mode.

2.3 Exiting a Command Mode

The following commands to exit the current command mode are always available.

Command	Function
exit	Closes current mode and returns to previous mode.
end	Closes current mode and returns to User EXEC mode.

Table 12 Return Commands

2.4 Useful Tips

The following sections provide useful functions for user’s convenience while using CLI commands:

- Listing Available Commands
- Calling Command History
- Using Abbreviation
- Using Privileged Mode Command
- Using Line Editing Keys
- Port Indices and Slot Assignments.

2.4.1 Listing Available Commands

Enter a question mark (**?**) on the particular command mode in order to display available commands used in this mode and the parameters following this commands.

Example for the *Privileged exec* mode:

```
SWITCH# ?
Exec commands:
clear       Reset functions
clock       Manually set the system clock
configure   Enter configuration mode
copy        Copy from one file to another
debug       Debugging functions (see also 'undebug')
enable      Turn on privileged mode command
exit        End current mode and down to previous mode
help        Description of the interactive help system
no          Negate a command or set its defaults
ping        Send echo messages
show        Show running system information
telnet      Open a telnet connection
terminal    Set terminal line parameters
traceroute  Trace route to destination
where       List active user connections
write       Write running configuration to memory, network, or
terminal
SWITCH#
```

ℹ The question mark (**?**) is not displayed and there is no need to press <ENTER> key in order to display the list.

In case of installed command shell, commands can be found out starting with specific alphabet. Enter the first letter and a question mark without space. The following is an example of finding out the commands starting with **s** in *Privileged exec* mode.

```
SWITCH# s?
 show Show running system information
SWITCH# s
```

To view required and possible parameters of a command, enter the command and a question mark delimited by one space. The following is an example of viewing the variables of **write** command.

```
SWITCH# write ?
 file Write to the file
 memory Write to NV memory
 terminal Write to terminal
SWITCH# write
```

Use the **show list command** to find out a detailed list of available commands with its parameters in each mode (press the arrow key to display more information), see the following example:

```
SWITCH# show list
clear ip bgp *
clear ip bgp * in
clear ip bgp * in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) in
clear ip bgp * ipv4 (unicast|multicast) in prefix-filter
clear ip bgp * ipv4 (unicast|multicast) out
clear ip bgp * ipv4 (unicast|multicast) soft
clear ip bgp * ipv4 (unicast|multicast) soft in
clear ip bgp * ipv4 (unicast|multicast) soft out
clear ip bgp * out
clear ip bgp * soft
clear ip bgp * soft in
clear ip bgp * soft out
clear ip bgp * vpnv4 unicast in
clear ip bgp * vpnv4 unicast out
clear ip bgp * vpnv4 unicast soft
clear ip bgp * vpnv4 unicast soft in
clear ip bgp * vpnv4 unicast soft out
clear ip bgp <1-65535>
clear ip bgp <1-65535> in
clear ip bgp <1-65535> in prefix-filter
clear ip bgp <1-65535> ipv4 (unicast|multicast) in
clear ip bgp <1-65535> ipv4 (unicast|multicast) in prefixfilter
clear ip bgp <1-65535> ipv4 (unicast|multicast) out
clear ip bgp <1-65535> ipv4 (unicast|multicast) soft
clear ip bgp <1-65535> ipv4 (unicast|multicast) soft in
clear ip bgp <1-65535> ipv4 (unicast|multicast) soft out
clear ip bgp <1-65535> out
clear ip bgp <1-65535> soft
clear ip bgp <1-65535> soft in
clear ip bgp <1-65535> soft out
clear ip bgp <1-65535> vpnv4 unicast in
clear ip bgp <1-65535> vpnv4 unicast out
clear ip bgp <1-65535> vpnv4 unicast soft
clear ip bgp <1-65535> vpnv4 unicast soft in
:
```

Press the RETURN- key to skip to the next list.

2.4.2 Calling Command History

By using command history, the last executed commands can be displayed. Press the arrow key < ↑ > repeated to display the commands in LIFO order one after another.

The following is an example of calling the command **history** after using the command sequence: show clock → configure terminal → interface 1 → exit.

```
SWITCH(config)# exit
SWITCH# show clock
Mon,  5 Jan 1970 23:50:12 GMT+0000
SWITCH# configure terminal
SWITCH(config)# interface 1
SWITCH(config-if)# exit
SWITCH(config)# exit
SWITCH# (press the arrow key ↑)
↓
SWITCH# exit (arrow key ↑)
↓
SWITCH# interface 1 (arrow key ↑)
↓
SWITCH#  configure terminal (arrow key ↑)
↓
SWITCH# show clock (arrow key ↑)
```

2.4.3 Using Abbreviation

Almost commands can be used also with abbreviated form. The following table shows some examples of abbreviated commands.

Command	Abbreviation
clock	clo
exit	exi
list	lis
configure terminal	con t

ℹ Press the tab key after entering the first letters of the command to complete it, e.g. `con` +tab key will be completed to `configure`.

2.4.4 Using Privileged Mode Command

By using the **do** command, *Exec* mode commands can also run in another as the Exec mode.

Command	Can be used in the following mode	Function
do	Config/bridge/config-rmonhistory/config-rule/dhcp-provider/pppoe-provider/config-if/config-touter/config-router-map	It is possible to use commands that are only valid in *Exec* mode, e.g. **do write**

Table 13 Privileged Exec Mode Command

An example for the **write ?** command.

```
SWITCH(config)# do write ?
LINEexec command
SWITCH(config)# do write
```

2.4.5 Using Line Editing Keys

Some commonly used key combinations in order to simplify the line editing are listed in the Table 14.

Keys	Function	
Ctrl+B or left arrow key	Moves cursor back one character.	Moving the CLI cursor
Ctrl+F or right arrow key	Moves cursor forward one character.	
Ctrl+A	Moves cursor to beginning of line.	
Ctrl+E	Moves cursor to end of line.	
Ctrl+I or tab key	Command completion.	Editing command line
Ctrl+D	Deletes character under cursor and shifts remainder of line to left.	
Ctrl+H	Deletes character to left of cursor.	
Ctrl+K	Deletes characters from under cursor to end of line.	
Ctrl+W	Deletes word to the left of cursor.	
Ctrl+U	Deletes entire line.	
Ctrl+N or down arrow key	Scrolls next command in command history buffer and places cursor at end of command.	Using command history
Ctrl+P or up arrow key	Scrolls previous command in command history buffer and places cursor at end of command.	
Ctrl+C	Aborts command and moves to next line.	
Ctrl+L	Clears screen and redisplays line.	
Ctrl+Z	Changes to *Privileged Exec* mode.	

Table 14 CLI Key Combinations

2.5 Port Indices and Slot Assignments

			CLI		SNMP
System (1)	Shelf slot (2)	Module type (3)	Slot for IUs, CXUs and PMs (4)	Slot number used in GPON OLT for port entry (5)	Slot number used in ACI (6)
hiX5750:E	101	IU	1	1	101
	102	IU	2	2	102
	103	IU	3	3	103
	104	IU	4	4	104
	105	IU	5	5	105
	106	IU	6	6	106
	107	IU	7	7	107
	108	IU	8	8	108
	109	CXU	9	9	109
	110	CXU	10	10	110
	111	IU	11	11	111
	112	IU	12	12	112
	113	IU	13	13	113
	114	IU	14	14	114
	115	IU	15	15	115
	116	IU	16	16	116
	117	PM1	17	not supported	117
	118	PM2	18		118
hiX5750:A	101	IU	1	1	101
	102	IU	2	2	102
	103	IU	3	3	103
	104	IU	4	4	104
	105	IU	5	5	105
	106	IU	6	6	106
	107	IU	7	7	107
	108	IU	8	8	108
	109	CXU	9	9	109
	110	CXU	10	10	110
	111	IU	11	11	111
	112	IU	12	12	112
	113	IU	13	13	113
	114	IU	14	14	114
	115	IU	15	15	115
	116	IU	16	16	116
	117	PM3	17	no supported	117

Table 15 Port Indices and Slot Assignment

Entry of the module and port number

The entries for **IU**s and **CXU**s are made as x/y with
x: shelf slot-number on **GPON OLT** according to Table 15, column (5)
y: used port of the module

Example for hiX 5750:E:

Entry **1/1** means port 1 of the module pluggend-in on shelf slot 101.
Entry **9/1** means Ethernet port 1 of the CXU plugged-in on shelf port 109.

3 System Access

3.1 Overview

The CLI of hiX 5750 R2.0 can be configured and managed via local terminal connection or a remote session using Telnet or Secure Shell (SSH). Both Telnet and SSH are enabled on the **NE** by default. The hiX 5750 R2.0 supports three methods to gain access to the NE for management and configuration tasks:

1. Local access to the NE through the RS232 console port on CXU's front panel, see 3.2 Login for the First Time on page 32.
2. Dedicated local Telnet/SSH connection to the NE by using the **FE LCT** port on CXU's front panel (outband interface).
3. Remote access over the provider's Ethernet/IP network by using Telnet/SSH. Therefore, an inband management channel, i.e., a specific management VLAN has to be configured.

3.2 Login for the First Time

3.2.1 Proceeding

Perform the following tasks to login for the first time:

1. To access local management on hiX 5750 R2.0 connect a PC/workstation directly to the RJ45 console port on CXU. Use a straight serial V.24 connecting cable that is wired as shown in Figure 2.
   There are two reasons that require the access to the hiX 5750 R2.0 over serial console port:
   - At initial startup, the hiX 5750 R2.0 is configured with standard features and default values. As the **NE**'s IP address depends on operator's network management concept, there is no IP assigned to the system for this purpose. Hence, if the system has booted successfully for the first time, the management channel for both inband and outband must be configured on this way in order to ensure that an IP connection can be established between an **NMS** and the NE.
   - For any reason, a restore of NE factory defaults was initiated.

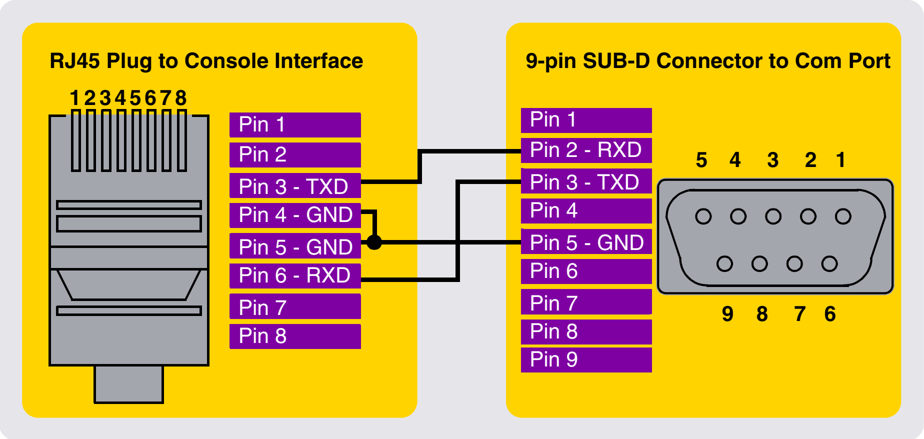


Figure 2 Serial Console Cable - Wiring and Signal Assignments

2. Run a VT terminal emulation software (e.g. HyperTerminal) with the attributes: **38400 8-N-1**, no flow control.
3. When the NE is switched on, the CXU is starting up and the terminal program displays automatically the login prompt “`SWITCH login:`”.
4. Login as described in Chapter 3.3 System Login.
5. Configure the outband, see Chapter 3.2.2 Configuring the Outband Interface.
6. Configure the inband, see Chapter 3.2.3 Configuring the Inband Management Channel.

3.2.2 Configuring the Outband Interface

To communicate with the **NE** over LCT port on CXU, after login configure an outband interface as follows:

1. Configure the management interface and a default gateway. See the Chapters 15.1 Enabling of an Interface, 15.2 Assigning an IP Address to the Interface, and 21.1 Static Routes for more information.

   ```
   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>
   ```

2. Configure the trap destination to communicate with the NE using **SNMP** (**ACI**-E EM PX R2.0/**LCT**), see Chapter 28.7 Configuring an SNMP Trap Host.

   ```
   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
   ```

3. After return from the *Configuration* mode, the made settings must be stored in the persistent CXU memory.

   ```
   SWITCH(config)# exit
   SWITCH# write memory
   ```

   ℹ Wait for **OK** message!

4. Connect the PC/workstation via LCT port. Local Telnet access as well as access using the EM PX R2.0 (LCT) should be possible.

3.2.3 Configuring the Inband Management Channel

To enable inband management communication the following tasks need to be performed:

1. Create a dedicated VLAN for inband management and assigned it to the CXU uplink port, see Chapter 16.1 Configuring a VLAN.

   ```
   SWITCH> enable
   SWITCH# configure terminal
   SWITCH(config)# bridge
   SWITCH(bridge)# vlan create <vlan-id>
   SWITCH(bridge)# vlan add <vlan-id> <port> tagged
   SWITCH(bridge)# exit
   ```

2. Configure the interface and the default route, see Chapters 16.2 Enabling a Host VLAN, 15.2 Assigning an IP Address to the Interface, and 21.1 Static Routes.

   ```
   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>
   ```

3. Configure the **SNMP** trap destination, see Chapter 3.2.2 Configuring the Outband Interface.
4. The configuration must be stored in the persistent CXU memory, see Chapter 3.2.2 Configuring the Outband Interface.

3.3 System Login

Access the hiX 5750 R2.0 as follows:

1. After starting the terminal session, the login prompt is displayed:

   ```
   SWITCH login:
   ```

2. Enter the login **ID** **root** (default) and the password siemens7 (default) to move into the *User exec* mode:

   ```
   SWITCH login:root
   Password: (entered characters are hidden)
   SWITCH>
   ```

3. From the *User exec* mode, the configuration of the hiX 5750 R2.0 can be only verified. To configure and manage the system, enter into the *Privileged exec* mode:

   ```
   SWITCH>enable
   SWITCH#
   ```

3.4 Telnet Access

Before a remote user can access the CLI via Telnet connection, the management IP interface (mgnt) must be configured (see 15 Interface Configuration).

Up to eight client systems can be connected at the same time. Use the following command to establish a Telnet connection between **NE** and remote place.

Command	Function
telnet *DESTINATION* [*tcp-port*]	Connects to the system with specified IP address. **DESTINATION**: IP address.

After applying a command in order to save the configuration over Telnet connection, wait for the **[OK]** message. When the Telnet session is disconnected before, all new settings will be deleted.

3.5 Modifying the Password of Privileged Exec Mode

Use the following commands to configure a password that enhances the security of the *Privileged exec* mode.

Command	Mode	Function
passwd enable [8] *LINE*	Config	Modifies enabled password parameters, **8**: specifies a HIDDEN password will follow **LINE**: HIDDEN 'enable' password string.
no passwd enable		Clears the password.

When it is not encrypted, the set password could be displayed with the **show running config** command. To avoid this, use the following command.

Command	Mode	Function
service password-encryption	Config	Encrypts system passwords.
no service password-encryption		Disables password encryption.

Example of configuring the password as *angpon*:

```
SWITCH#configure terminal
SWITCH(config)#passwd enable angpon
SWITCH(config)#
```

Example of accessing:

```
SWITCH login:root
Password:
SWITCH>enable
Password:
SWITCH#
```

3.6 Configuring the Auto-Logout Function

For security reasons, the user is automatically logged out when there is no command prompted within the configured inactivity time.

Use the following command to enable the auto-logout function and to configure the inactivity timer.

Command	Mode	Function
exec-timeout <0-35791> [< 0-59 >]	Config	If no command is entered within the configured inactivity time, the user is automatically logged out of the system. **0 - 35791**: time unit in minutes (by default 10 minutes) 0: releases auto-logout function **0 - 59**: time unit in seconds.

Command	Mode	Function
show exec-timeout	Privileged/ Config	Shows configured inactivity timer.

Example:

Example of configuring an auto-logout timeout of 50 seconds and displaying the configuration:

```
SWITCH(config)#exec-timeout 0 50
SWITCH(config)#show exec-timeout
Log-out time : 50 seconds
SWITCH(config)#
```

3.7 Configuring of Users

The administrator can configure up to 8 user accounts. Once a user account is configured, the user can login to the system using the user name/password combination.

Adding a User

An added user with "read only" right can only check for system information but cannot configure the system.

Command	Mode	Function
user add *NAME DESCRIPTION*	Config	Adds a user with read only right. **NAME**: user name **DESCRIPTION**: description of the user, e.g. admin

Example of adding the user "GPON" (The password is set to siemens7 by default):

```
SWITCH(config)#user add GPON admin
Changing password for GPON
Enter the new password (minimum of 5, maximum of 8 characters).
Please use a combination of upper and lower case letters and
numbers.
Enter new password:
Re-enter new password:
Password changed successfully
SWITCH(config)#
```

ℹ The entered password is not displayed, so be careful to make no mistake.

Example: User "GPON" logs in.

```
SWITCH login:GPON
Password:siemens7
SWITCH>
```

Enter a question mark (**?**) in order to display the executable user commands.

```
SWITCH>?
Exec commands:
@debug    Debug command
clear     Reset functions
debug     Debugging functions (see also 'undebug')
enable    Turn on privileged mode command
exit      End current mode and down to previous mode
help      Description of the interactive help system
no        Negate a command or set its defaults
show      Show running system information
terminal  Set terminal line parameters
SWITCH>
```

Configuring a User Password

To configure a password for the created user account, use the following command.

Command	Mode	Function
passwd *NAME*	Config	Configures the user's password. **NAME**: user name.

Example:

```
SWITCH(config)# passwd GPON
Changing password for GPON
Enter the new password (minimum of 5, maximum of 8 characters)
Please use a combination of upper and lower case letters and
numbers.
Enter new password:
Re-enter new password:
Password changed.
SWITCH(config)#
```

Deleting a User

After adding the user, it is impossible to change user's information such as ID, password, and description. Thus, if there is a need to change one of this parameters, delete the user and add it again with new properties.

Command	Mode	Function
user del *NAME*	Config	Deletes a user. **NAME**: user name.

Example of deleting the user "GPON":

```
SWITCH(config)#user del GPON
SWITCH(config)#
```

3.8 Limiting the Number of Management Sessions

To designate the number of open management sessions, enter the following command.

ℹ The counter will be incremented by Telnet sessions as well as a serial connection over console port.

Command	Mode	Function
login connect *COUNT*	Config	Limits the number of sessions accessing to the NE. **COUNT**: number of sessions (1 to 8 = default).

3.9 Checking the Management Sessions

Use the following command to get information about management sessions accessing the NE.

Command	Mode	Function
show management-session	Config	Shows information about the management sessions.

Example:

```
SWITCH(config)#show management-session

SNMP Session Aging Time: 300

Management Session Information
-------------------------------------------
        IP Address |  Type  | Expired Time
-------------------------------------------
     10.150.229.85   Telnet           0
-------------------------------------------
SWITCH(config)#
```

3.10 Checking Telnet Users

Use the **where** command to examine the users connected over console port or from remote place through Telnet.

Command	Mode	Function
where	Privileged/ Config	Shows users connected through Telnet.

Example of displaying users connected through Telnet:

```
SWITCH#where
root at  from console for 4 days 22 hours 15 minutes 24.88
secondsroot at ttyp0 from 10.0.1.4:1670 for 4 days 17 hours 53
minutes 28.76
secondsroot at ttyp1 from 147.54.140.133:49538 for 6 minutes
34.12 seconds
```

4 System Basic Configuration

4.1 Software and Configuration Management

For information about commands that are needed to operate the system software, see the following sections:

- Saving the Configuration
- Auto-Backup the Configuration
- Downloading and Uploading of Software
- Restarting the System
- Restoring default Configuration
- Displaying the System Version and Startup Information
- Checking the Running System Configuration.

The following sections describe the commands in order to check the utilization of system resources and the status of system values:

- Displaying the Running Time of System
- Checking the CPU Load
- Displaying Consumption Ratio of System Memory
- Displaying the Fan Status
- Displaying Running Processes.

4.1.1 Saving the Configuration

After download a new system image to the hiX 5750 R2.0 system from **FTP** server or changing the configuration, the operator has to save the files into the flash memory. Otherwise, the configuration data will be lost in case of rebooting.

Command	Mode	Function
write memory	All, exceed exec	Saves changed configuration in the flash memory.
show flash	Privileged/ Config	Displays flash info.

Examples:

```
SWITCH#write memory
[OK]
SWITCH#
```

ℹ Wait for [OK] message after starting this function without pressing any key.

```
SWITCH# show flash

Flash Information(Bytes)

Area         total        used       free  loadname
---------------------------------------------------------------------------
Load 1    32112640    12976156   19136484 gpon-r2.0.5-cxu_f-o.010
Load 2    32112640    14856192   17256448 gpon-r2.0.5-cxu_f-o.003
CONFIG     1310720      663552     647168
CONFIG     1441792      675840     765952
---------------------------------------------------------------------------
SWITCH#
```

Besides the **write** command, the system configuration can be also stored into flash memory through copying the configuration file with a particular file name. The configuration file stored in flash can be transferred to a remote FTP server as well.

In order to copy or erase a system configuration file, use the following commands.

Command	Mode	Description
copy running-config { *FILENAME* | startup-config }	Privileged/ Config	Copies a running configuration file. **FILENAME**: configuration file name **startup-config**: startup configuration file.
copy startup-config *FILENAME*	Privileged/ Config	Copies a startup configuration file.
copy *FILENAME* **startup-config**		Copies a specified configuration file to the startup configuration file.
copy *FILENAME1 FILENAME2*		Copies a specified configuration file to another configuration file.
erase *FILENAME*	Config	Deletes a specified configuration file.

Use the following command to display system configuration file.

Command	Mode	Description
show config-list	Privileged/ Config	Displays a list of saved configuration files.

4.1.2 Auto-Backup the Configuration

Auto-backup ensures that made configuration changes are valid after system reboot also if they were not stored explicitly by operator command. This function allows to store configuration data automatically to the CXU's background memory or/and to remote **FTP** server. The waiting time before storing the data after last change of configuration can be specified.

Configuring Local Auto-Backup

Command	Mode	Function
auto-backup local [enable | disable]	Config	Configures automatic save of the configuration data in persistent memory. **enable**: local save enabled **disable**: local save disabled. Use the **no** parameter with this command to disable the function.
auto-backup local waiting-time [1-59]		Configures auto-backup waiting time for local backup, **1 - 59**: waiting time in minutes after the last configuration action before the configuration data are saved in persistent memory.

Configuring the Auto-Backup to an FTP Server

Use the following commands in order to inform the NE about the FTP server that is used for auto-backups. If this is the default FTP server, the optional parameters may drop.

Command	Mode	Function
auto-backup ftp [enable | disable]	Config	Configures automatic save of the configuration data on an FTP server. **enable**: FTP save enabled **disable**: FTP save disabled. Use the **no** parameter with this command to disable the function.
auto-backup ftp file-count [1-32]		Configures the number of files on FTP-server, **1 - 32**: number of files on FTP-server.
auto-backup ftp ip [A.B.C.D]		Configures the IP address of the FTP-server. **A.B.C.D**: IP address of the FTP-server.
auto-backup ftp path [*PATH*]		Configures the path on FTP-server where to save the backup. **PATH**: path on FTP-server.
auto-backup ftp account [*USER PASSWORD*]		Configures the account to access the FTP-server, **USER**: user name of the FTP-account **PASSWORD**: password of the FTP-account.
auto-backup ftp interval [1-48>]		Configures the time between two backups, **1 - 48**: time [hours].
auto-backup ftp start-time [0-1439]		Configures the time of day when the first backup is written, **0 - 1439**: time of day [minutes].

ℹ Configuration data will be stored on FTP server only if the data in the persistent memory has been changed before.

Initiating an Auto-Backup

Command	Mode	Function
auto-backup now	Config	Forces an auto-backup immediately.

Verifying the Auto-Backup Configuration

Command	Mode	Function
show auto-backup ftp file-table	Config	Shows informantion about backup files located on FTP-server.
show auto-backup		Shows informantion about auto-backup configuration.

Example

Auto-backup that stores configuration data of the NE “GPON_1" local as well as remote on FTP server:

1. Configuration of local auto-backup

```
GPON_1(config)# auto-backup local enable
GPON_1(config)# auto-backup waiting-time 24
```

2. Configuration of remote auto-backup

```
GPON_1(config)# auto-backup ftp ip 10.2.30.19
GPON_1(config)# auto-backup ftp path GPON/loads/gpon_1
GPON_1(config)# auto-backup ftp account ftpuser ftpuser1
GPON_1(config)# auto-backup now
Jun 13 11:51:43  system: ERROR: swal_vlan_get_pvid port 2 data not found
Jun 13 11:51:43  system: ERROR: swal_vlan_get_pvid port 3 data not found
Jun 13 11:51:43  system: ERROR: swal_vlan_get_pvid port 4 data not found
Jun 13 11:51:43  system: ERROR: swal_vlan_get_pvid port 5 data not found
Jun 13 11:51:43  savecfg: write backup (-w)
Jun 13 11:51:45  savecfg: done

GPON_1(config)# auto-backup ftp interval 24
GPON_1(config)# auto-backup ftp start-time 800
GPON_1(config)# show auto-backup
--- current time ----------------------------------------------
current time: Fri Jun 13 11:52:49 2008
--- local backup ----------------------------------------------
automatic write of local backup: enabled
local backup up to data: no
last backup: Fri Jun 13 11:51:45 2008
automatic write after: 24 minutes
--- remote backup ---------------------------------------------
save of backup on FTP-server: enabled
backup on FTP-server up to data: no
last backup: Fri Jun 13 11:51:46 2008
last FTP access result: success
backup period: 24 hours
start time: 13:20:00
number of files on FTP-server: 5
FTP-server IP-address: 10.2.30.19
path on FTP-server: GPON/loads/gpon_1
FTP-account username: ftpuser1
FTP-account password: ********
next backup: Fri Jun 13 13:20:00 2008
```

3. Refresh file-table

```
GPON_1(config)# auto-backup ftp refresh-file-table

GPON_1(config)# show auto-backup ftp file-table

Index  | File Name                    | Timestamp
-------+------------------------------+------------------------
1      | gpon_080006263ce5.dat        | Fri Jun 13 11:40:00 2008

GPON_1(config)#
```

4.1.3 Auto-Upgrading the S-APS

For an automatic S-APS upgrade, the S-APS configuration file is needed on FTP server. This file contains the software load information on all units possible to plug in and also those ONT types that may be connected to the hiX 5750 R2.0. If automatic S-APS handling is enabled, most of the commands for manual software up- and download are blocked. Exceptions are commands like "upload cxu errorlog", "upload cxu/iu inventory".

In order to download SAPS, use one of the following commands.

Command	Mode	Function
download sapshandling *create sapsserverinfo ADDRESS USER PASSWORD SAPSFILE*	Config	Configures S-APS config data for upgrade. **ADDRESS**: S-APS FTP server IP address **USER**: S-APS FTP server user name **PASSWORD**: S-APS FTP server password **SAPSFILE**: S-APS file on SAPS server with complete file path, e.g. /SAPS/hiX5750R20.55/hix5750r20.55.012.
download sapshandling { enable I disable I restart-reset I restart-noreset I reload }	Config	Configures S-APS handling, S-APS use of S-APS data from now on. **enable**: S-APS configuration file will be read from FTP server. If it is not possible, S-APS handling will remain in ON condition but the operstate changes to disable. **disable**: S-APS handling disabled, manual up-/download possible **restart-reset**: S-APS handling restart (if S-APS enabled). All plugged units will be checked again against S-APS configuration file content and if needed an upgrade with load activation; automatic unit reset will be done. **restart-noreset**: S-APS handling restart without board. All plugged units will be checked again against S-APS configuration file content and if needed an upgrade will be done. NO automatic load activation is performed. **reload**: S-APS configuration file will be reload, if S-APS is disabled.

Example:

```
SWITCH(config)# download sapshandling create sapsserverinfo 172.18.104.252 usera asdf
/SAPS/hiX5750R20.55/hix5750r20.55.012
timeout (20 seconds) active
command complete

SWITCH(config)# download sapshandling enable
start upgrade script: PID(4731) now
command complete

SWITCH(config)# download sapshandling restart-reset
saps handling restarted with resettimeout (7200 seconds) activestart upgrade script: PID(4867) now..
```

4.1.4 Downloading and Uploading of Software

In order to guarantee a fail-safe upgrade process, the OLT stores two software images. One image is the active and committed load that is currently running. This load is always available and it will be used after a reset. The second image is inactive. It will be overwritten during a software download.

Depending on the number of equipped CXU boards, there are two operation cases:

1. If there is only one CXU in the system, the new load will be automatically activated and committed if the download process was successful and the load is valid. After reboot by operator command, the committed load is running and will be used also for later reboots by reset or cold starts. When something goes wrong (e.g. board crash), the CXU will disable the wrong load and will reboot automatically with the former good load.
2. In an OLT with two CXUs that provides redundancy measures, one CXU is in active mode and the other one is in standby mode. In this case, the download process replaces at first the active load of the standby CXU.

   ℹ During the load download process, the standby CXU performs automatically two resets.

   After the download process has been finished (load and configuration), the following tasks must be performed in order to update both CXU boards with the same load:
   - Check with **show table shelf** command the software consistence on both CXU boards. The new load on both boards must be identical (stored/backup).
   - Reset the **standby** CXU to pre-activate the new software, see 8.2 Resetting a CXU.
   - Check the consistence of the software loads on this board (identical running/stored/backup loads).
   - Reset the **active** CXU to initiate a switch-over that makes the standby CXU to the active one, causes the upgrade of the other CXU (by now in standby mode) and activates the new software on it.
   - Check the consistence of both boards software loads. (identical running/stored/backup loads).

ℹ To backup or restore the configuration data, use the FTP **upload** and download commands that are described in the following sections.

ℹ See 9.11 Managing the Software Load for information about how to manage the software load of an ONU.

FTP Download Process

Use the following commands to download the software load and configuration data from an **FTP** server towards the remote **NE**.

⚠ The load file name used in the following commands must have an extension that is composed of up to maximal 5 characters (e.g. "gpon-r205-cxu_f-o.004" or "gpon-r205-cxu_f-o.004_1"). File names without extension could damage the internal upgrade system.

Command	Mode	Function
download cxu { load I config } *ADDRESS FILE*	Config	Upgrades OS image or board configuration. **load**: software load **config**: configuration data **ADDRESS**: server ID address or hostname **FILE**: source file name according to the selected command (load file or configuration file).
download iu load *ADDRESS FILE*		Upgrades IU image or configuration. **ADDRESS**: server ID address or host name **FILE**: source file name (load file).
download iu load alloftype *ADDRESS FILE*		Upgrades IU image for all plug-in units of the same type. **ADDRESS**: server IP address or host name **FILE**: source file name (load file).
download remote load *ADDRESS FTP_SERVER FILE* [ignore-operstate]		Upgrades software load of remote system, **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID[/ONU-card]]]. **FTP_SERVER**: IP address of FTP server. **FILE**: source file name. **ignore-operstate**: force download to disabled cards.
download remote load help		Help shows the relations between address and download type.
download remote load stop_request		Stops current download job of upgrade software load remote system,

FTP Upload Process

Use the following commands to upload data to FTP server.

The file extension ".tgz" will be added by the system if the **upload cxu config** command is executed.

Command	Mode	Function
upload cxu { config I errlog I inventory I alarmlog I uptimelog } *ADDRESS FILE*	Config	Uploads specified CXU data. **config**: configuration data **errlog**: error log **inventory**: inventory data **alarmlog**: alarm log data **uptimelog**: board uptime log data **ADDRESS**: FTP server ID address or hostname **FILE**: destination file name acc. to the selected command.
upload iu { errlog I inventory } *ADDRESS FILE*	Config	Uploads IU data for slot number 1..x). **errlog**: error log **inventory**: use inventory data **ADDRESS**: server ID address or host name **FILE**: destination file name acc. to the selected command
upload iu inventory alloftype *ADDRESS FILE*	Config	Uploads IU inventory data for all IUs of same type. **ADDRESS**: server ID address or host name **FILE**: destination file name (inventory file).

Example:

```
SWITCH(config)#upload cxu config 192.168.156.16 alf/config
SWITCH(config)#FTP User Name:onus
SWITCH(config)#FTP Password :
SWITCH(config)#upload cxu config file alf/config.tar to server
192.168.156.16 complete
```

Timer Parameter

Command	Mode	Function
upgrade set-timeout { cxu | stb-cxu | iu | remote | config | errorlog | pm-data | label-data | snmp } ftp-timeout <25-65535> upgrade-timeout <25-65535>	Privileged/ Config	Sets upgrade option timeout value, **cpu**: set upgrade CXU timeout **stb-cxu**: set upgrade standby CXU timeout **iu**: set upgrade IU timeout **remote**: set upgrade ONT timeout **config**: set upgrade config timeout **errorlog**: set upgrade error log timeout **pm-data**: set upgrade performance data timeout **label-data**: set upgrade label data timeout **snmp**: set upgrade SNMP timeout, **ftp-timeout**: set FTP timeout **25 - 65535**: set FTP timeout value in sec. **upgrade-timeout**: set upgrade timeout **25 - 65535**: set upgrade timeout value in sec.

Checking the Upgrade Process

Use the following commands to verify such data that are relevant for upgrade process.

Command	Mode	Function
show upgrade	Privileged/ Config	Displays upgrade information.
show upgrade table		Displays upgrade information (table of slot, remote index (**ONT** number) or whole system).
show upgrade table *SLOT*		Displays upgrade information for specified slot number.
show upgrade table mnemocode		Displays slot based mnemocodes of whole system.
show upgrade table sapsjobs		Displays the S-APS upgrade jobs of whole system.
show upgrade sapsserverinfo		Displays S-APS server data known by upgrade.
show upgrade timeout-values		Displays upgrade information: timeout value.

Examples:

```
SWITCH(config)# show upgrade sapsserverinfo

S-APS server data known by upgrade:
S-APS handling       : disabled
S-APS server address: 10.0.1.16
S-APS user name      : sff00009
S-APS password       : *****
S-APS path name      : SAPS/hiX5750R205/
S-APS file name      : 002

SWITCH(config)#
SWITCH(config)# show upgrade table

file information table for whole system: (equipped slots)
,=========,====================,================================================,=========,==========,
| Slot    | type of file       | file                                           | version | size     |
|=========|====================|================================================|=========|==========|
| 09      | stored load        | gpon-r2.0.5-cxu_f-o.010                        | 010     | 12976156 |
| 09      | error log          | error.tgz                                      | none    |    23499 |
| 09      | configuration      | configuration.tgz                              | none    |     5952 |
| 09      | label data         | inventory.bin                                  | none    |      256 |
|---------|--------------------|------------------------------------------------|---------|----------|
| 13      | stored load        | gpon-r2.0.5-iu_gpon-o.006                      | 006     |        0 |
| 13      | error log          | error.log                                      | none    |    16962 |
|---------|--------------------|------------------------------------------------|---------|----------|
| 17      | stored load        | not available; mnemo(M:PM3:A)                  | unknown |        0 |
|---------|--------------------|------------------------------------------------|---------|----------|
`=end====='===================='================================================='========='=========='

SWITCH(config)#
```

4.1.5 Restarting the System

Execute the **reset** command in *Config* mode to reboot the system manually after downloading a new system image from the TFTP/**FTP** server or when a reboot is needed during installing or managing the system.

ℹ Execute the **write memory** command (see 4.1.1 Saving the Configuration) to save a new configuration before rebooting the system. Otherwise, all changes will be lost.

Command	Mode	Function
reset all	Config	Resets the system.

ℹ For information about restarting single cards see also:

- Reset of Interface Unit Cards
- Resetting a CXU.

4.1.6 Restoring default Configuration

ℹ After reloading the configuration by executing the **restore factory-defaults** command, all previous configuration data are lost. The **NE** access is only possible via console. The system must be rebooted manually.

Command	Mode	Function
Restore factory-defaults	Config	Restores factory default configuration.

Example:

```
SWITCH(config)#restore factory-defaults
SWITCH(config)#reset all
SWITCH(config)#
```

4.1.7 Displaying the System Version and Startup Information

Use one of the following commands to display system startup information and **OS** version.

Command	Mode	Function
show system-version	Privileged/ Config	Displays system information.
show system-feature-list		Displays the feature list of the system.
show startup-type		Displays the type of the last startup.
show startup-result		Displays the result of the last startup.
show startup-config	Privileged	Show a current startup configuration.

4.1.8 Checking the Running System Configuration

Command	Mode	Function
show running-config	Privileged/Config	Shows current system information
show running-config arp	Privileged/Config	Shows current **ARP** information
show running-config bridging	Privileged/Config	Shows current bridging information
show running-config dhcp	Config	Shows current **DHCP** information
show running-config dns	Privileged/Config	Shows current **DNS** information
show running-config full	Config	Shows current full information
show running-config hostname	Privileged/Config	Shows current hostname information
show running-config igmp	Config	Shows current **IGMP** information
show running-config interface *IFNAME*	Config	Shows current interface information **IFNAME**: name of logical interface.
show running-config l3	Config	Shows current fixed IP information
show running-config lacp	Privileged/Config	Shows current **LACP** information
show running-config login	Privileged/Config	Shows current login information
show running-config mac	Privileged/Config	Shows current **MAC** information
show running-config maxhosts	Config	Shows current maxhosts information
show running-config port	Privileged/Config	Shows current port information
show running-config qos	Privileged/Config	Shows current **QoS** information
show running-config rmon	Privileged/Config	Shows current **RMON** information
show running-config router bgp	Config	Shows current **BGP** router information
show running-config router isis	Config	Shows current **IS**-IS router information
show running-config router rip	Config	Shows current **RIP** router information
show running-config rule	Privileged/Config	Shows current Rule information
show running-config snmp	Privileged/Config	Shows current **SNMP** information
show running-config stp	Privileged/Config	Shows current **STP** information
show running-config switch	Privileged/Config	Shows current switch information
show running-config syslog	Privileged/Config	Shows current system log information
show running-config time-out	Privileged/Config	Shows current time out information
show running-config time-zone	Privileged/Config	Shows current time zone information

Command	Mode	Function
show running-config trunk	Privileged/Config	Shows current trunk information
show running-config xdsl alarm-profile	Privileged/Config	Shows current x**DSL** alarm profile
show running-config xdsl all-profiles	Privileged/Config	Shows all current xDSL profiles
show running-config xdsl chan-profile	Privileged/Config	Shows current xDSL channel profile
show running-config xdsl line-profile	Privileged/Config	Shows current xDSL line profile
show running-config xdsl notch-profile	Privileged/Config	Shows current xDSL notch profile
show running-config xdsl psd-profile	Privileged/Config	Shows current xDSL **PSD** profile
show running-config xdsl vcc	Privileged/Config	Shows xDSL and **VCC** information

4.2 Checking the Operating Values of System

4.2.1 Displaying the Running Time of System

Command	Mode	Function
show uptime	Privileged/Config	Displays running time of system after booting.

Example:

```
SWITCH#show uptime
10:41am  up 15 days, 10:55,  0 users, load average: 0.05, 0.07, 0.01
SWITCH#
```

4.2.2 Checking the CPU Load

Use this command to display the CPU utilization.

Command	Mode	Function
show cpuload	Config	Displays the average of CPU utilization in specific time intervals.

Example:

```
SWITCH(config)#show cpuload
----------------
Average CPU load
----------------
 5 sec:   7.73( 0.00) %
 1 min:   4.22( 0.00) %
10 min:   4.15( 0.00) %

cpuload threshold :        50
timer    interval :        60 seconds
SWITCH(config)#
```

4.2.3 Displaying Consumption Ratio of System Memory

Command	Mode	Function
show memory	Privileged/ Config	Displays memory information.
show memory { bgp I isis I dhcp I imi I igmp I lib I nsm I ospf I rip }		Displays memory information of **bgp**: BGP router **dhcp**: DHCP **igmp**: IGMP **imi**: integrated management interface **isis**: IS-IS router **lib**: libraries **nsm**: network services module **ospf**: OSPF router **rip**: RIP router.

4.2.4 Displaying the Fan Status

Command	Function	Mode
show status fan	Privileged/ Config	Displays hardware status.

4.2.5 Displaying Running Processes

The following **show** command displays information about the running processes on hiX 5750 R2.0 that may be very helpful to manage the NE.

Command	Mode	Description
show process	Privileged/ Config	Shows information of the running processes.

Example:

```
SWITCH(config)# show process
USER       PID %CPU %MEM   VSZ  RSS TTY      STAT START   TIME COMMAND
root         1  0.0  0.1  1448  596 ?        S    Oct07   0:01 init [3]
root         2  0.0  0.0     0    0 ?        SW   Oct07   0:00 [keventd]
root         3  0.0  0.0     0    0 ?        SWN  Oct07   0:00 [ksoftirqd_CPU0]
root         4  0.0  0.0     0    0 ?        SW   Oct07   0:00 [kswapd]
root         5  0.0  0.0     0    0 ?        SW   Oct07   0:00 [bdflush]
root         6  0.0  0.0     0    0 ?        SW   Oct07   0:00 [kupdated]
root         7  0.0  0.0     0    0 ?        SW   Oct07   0:00 [mtdblockd]
root        63  0.0  0.0     0    0 ?        SWN  Oct07   0:00 [jffs2_gcd_mtd2]
root        70  0.0  0.0     0    0 ?        SWN  Oct07   0:00 [jffs2_gcd_mtd4]
root       143  0.0  0.0     0    0 ?        SW<  Oct07   0:00 [bcmDPC]
root       147  0.0  0.0     0    0 ?        SW<  Oct07   0:00 [bcmCNTR.0]
root       148  0.0  0.0     0    0 ?        SW<  Oct07   0:00 [bcmTX]
root       149  0.0  0.0     0    0 ?        SW<  Oct07   0:00 [bcmLINK.0]
root       150  0.9  0.0     0    0 ?        SW<  Oct07  80:54 [bcmCNTR.1]
...
SWITCH(config)#
```

4.3 Checking the System Access

To prevent trouble or if there is any problem with the system access, the operator cannot get only information about the access status of system, but he can also check if the network configuration is correct to reach the system. This chapter describes the required **CLI** commands in following sections:

- Checking the Network Connection
- Tracing Packet Routes
- Checking Telnet-User
- Displaying Hosts Accessing the System.

4.3.1 Checking the Network Connection

The **ping** command can be executed to verify if the system is correctly connected to the network. In **IP** networks, this command uses **ICMP** (Internet control message protocol) echo messages to notify a fault situation and to provide information about the location where the IP packets were received from.

Command	Mode	Function
ping [*IP_ADDRESS*]	Privileged	Performs ping test to check network status. **IP_ADDRESS**: destination address.

ℹ Press Ctrl + C keys to stop the ping process.

4.3.2 Tracing Packet Routes

To identify the route used for host-to-host connectivity across the network, execute the **traceroute** command. If the waiting time to response has expired, an asterisk (*) will be printed on the screen.

Command	Mode	Function
traceroute [ip I *WORD*]	Privileged	Traces packet routes through the network. **ip**: destination IP address **WORD**: hostname.

Example: Tracing packet route sent to 10.2.2.20

```
SWITCH#traceroute 10.2.2.20
traceroute to 10.2.2.20 (10.2.2.20), 30 hops max, 38 byte packets
1 10.2.2.20 (10.2.2.20) 0.598 ms 0.418 ms 0.301 ms
SWITCH#
```

4.3.3 Checking Telnet-User

Command	Mode	Function
where	Privileged/ Config	Checks accessed Telnet user from remote place.

Example:

```
SWITCH#where
root at ttyp0 from 10.150.229.85:34260 via telnet for 12 minutes 8.38 seconds
SWITCH#
```

4.3.4 Displaying Hosts Accessing the System

The following commands show brief information about the number of hosts accessing the system.

Command	Mode	Function
show tmn-connect	Privileged/ Config	Shows whether a **TMN** (e.g. EM ACI-E) is connected to the network element (NE) or not.
show lct-connect		Shows whether an **LCT** is connected to the NE or not.
show cli-connect		Shows whether and how many **CLI** consoles are connected to the NEor not.

4.4 Operation Environment

4.4.1 Setting the Output Condition of Terminal Screen

By default setting, the hiX 5750 R2.0 is configured to display 24 lines each with 80 characters on console screen. With the **length** command, the number of displayed lines can be changed.

Command	Mode	Function
terminal length <0~512>	Privileged	Configures the number of displayed lines on terminal screen. **0 - 512**: line value.
terminal no length		Disables the configuration for the number of displayed lines.

Example: Sets the number of displayed lines on terminal screen as 20 lines.

```
SWITCH#terminal length 20
SWITCH#
```

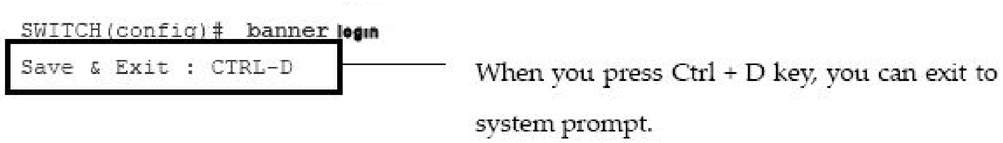
4.4.2 Configuring a Login Banner

Command	Mode	Function
banner	Config	Register message before login the system. Use the **no** parameter with this command to remove the banner.
banner login		Register message when successfully log in the system. Use the **no** parameter with this command to remove the banner.
banner login-fail		Register message when failing to login the system. Use the **no** parameter with this command to remove the banner.

Command	Mode	Function
show banner	Privileged/ Config	Displays login banner.

Example:

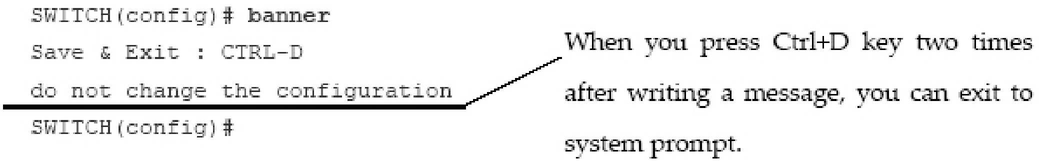
1. Execute the **banner login** command



```
SWITCH(config)#  banner login
Save & Exit : CTRL-D
```

When you press Ctrl + D key, you can exit to system prompt.

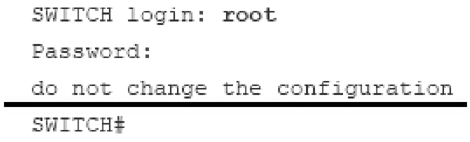
2. Write the message (e.g. do not change the configuration) and then press Ctrl+D key two times.



```
SWITCH(config)# banner
Save & Exit : CTRL-D
do not change the configuration
SWITCH(config)#
```

When you press Ctrl+D key two times after writing a message, you can exit to system prompt.

3. The banner will be displayed after user’s log-in.



```
SWITCH login: root
Password:
do not change the configuration
SWITCH#
```

5 System Properties

This chapter describes the following configuration steps:

- Setting the Host Name
- Configuring of System Date and Time
- Synchronizing the Clock
- Configuring the Time Zone.

5.1 Setting the Host Name

The host name displayed on prompt is necessary to distinguish each hiX 5750 R2.0 system that is connected to the network.

Command	Mode	Function
hostname *NAME*	Config	Creates host name of the system. **NAME**: enter the name. Host name distinguishes upper case and lower case!
no hostname [*NAME*]		Deletes all configured host names or the specified host name.

ℹ The default host name is `SWITCH`.

Example: Changing the host name to “AN_GPON”.

```
SWITCH(config)#hostname AN_GPON
AN_GPON(config)#
```

5.2 Configuring of System Date and Time

Command	Mode	Function
clock *.DATETIME*	Privileged/ Config	Configures the system time and date.
show clock		Displays the system date and time.

Available formats of “.DATETIME” are (examples):
10:20 Jul 04 2007 or 04 Jul 2007 10:20 pm or 04 Jul 2007 10:20.

```
AN_GPON#clock 20070604 10:20
AN_GPON#show clock
Mon,  4 Jul 2007 10:20:37 +0000
AN_GPON#
```

5.3 Configuring the Time Zone

Time Zone	Country/City	Time Zone	Country/City	Time Zone	Country/City
GMT-12	Eniwetok	GMT-3	Rio De Janeiro	GMT+6	Rangoon
GMT-11	Samoa	GMT-2	Maryland	GMT+7	Singapore
GMT-10	Hawaii, Honolulu	GMT-1	Azores	GMT+8	Hong Kong

Table 16 World Time Zones

Time Zone	Country/City	Time Zone	Country/City	Time Zone	Country/City
GMT-9	Alaska	GMT+0	London, Lisbon	GMT+9	Seoul, Tokyo
GMT-8	LA, Seattle	GMT+1	Berlin, Rome	GMT+10	Sydney
GMT-7	Denver	GMT+2	Cairo, Athens	GMT+11	Okhotsk
GMT-6	Chicago, Dallas	GMT+3	Moscow	GMT+12	Wellington
GMT-5	New York, Miami	GMT+4	Teheran		
GMT-4	George Town	GMT+5	New Delhi		

Table 16 World Time Zones (Cont.)

Command	Mode	Function
time-zone *TIMEZONE*	Config	Sets the time zone. **TIMEZONE**: GMT, GMT+0, GMT+1, ..., GMT+12, GMT-0, GMT-1, ..., GMT-12, GMT0, Greenwich, UCT, UTC, Universal
show time-zone	Privileged/ Config	Displays all time zones.

5.4 Synchronizing the Clock

Index/Priority	Clock Source ETSI	Clock Source ANSI
1 (High)	T3 input at PM_1	DS1 interface #1 at PM_3
2	Internal clock generator	DS1 interface #2 at PM_3
3		Internal clock generator

Table 17 Clock Source Indexes

Command	Mode	Function
modify clock-sync source *INDEX* <1-10>	Config	Modifies configuration of clock sync source. **INDEX**: clock source index **1 - 10**: alarm severity profile index.
modify clock-sync waittime *TIME*	Config	Modifies clock sync waittime to restore. **TIME**: time to has expire before switch back to a higher clock source after error condition (unit is 100 ms).
show clock-sync sources	Config	Displays all clock sync sources.

6 Alarms

The fault management system of the hiX 5750 R2.0 uses alarm profiles specifying alarm severities to inform the operator in case of system errors by **SNMP** traps. It is possible to configure different levels of error checking according to the service type and port.

For information about how to set the alarm severity profile for a specific unit see the chapters describing the configuration of OLT cards, ONUs and ports.

6.1 Configuring an Alarm Severity Profile

Prior use the **show alarm-id** command to get information about alarm ID values (see 6.2 Checking the Alarm Severity Configuration).

Command	Mode	Function
al-mgr set sev profile { *ALARM_ID* } {SEV1} {SEV2} {SEV3} {SEV4} {SEV5} {SEV6} {SEV7} {SEV8} {SEV9} {SEV10}	Config	Sets all severities for the chosen alarm. **ALARM_ID**: alarm ID value **SEV1**-**SEV10**: severity for profile 1-10. (the first profile is default and cannot be overwritten) severities values are: 1: critical 2: major 3: minor 4: warning 5: cleared.
modify alarm-severity *ALARM_ID PROFILE_INDEX SEVERITY*		Modifies the index of the severity profile in severity profile table. **ALARM_ID**: alarm ID value **PROFILE_INDEX**: index of the severity profile in severity profile table **SEVERITY**: new severity of the alarm (1 to 5)
update alarm-list		Updates the alarm list after changing the severity.

Example

```
SWITCH(config)# modify alarm-severity 6 3 2

Alarm ID         :  06
Severity Profile:   3
Old Severity     :   1
New Severity     :   2


SWITCH(config)# update  alarm-listAlarm list is now up to date.
```

6.2 Checking the Alarm Severity Configuration

In order to identify ID and name of alarms that can occur in system, use the following command. See the maintenance manual for more information about a particular alarm.

Command	Mode	Function
show alarm-id	Privileged/ Config	Displays assignment alarm and alarm ID.

Example:

```
SWITCH# show alarm-id
```

```
Assignment Alarm and Alarm-ID

 ID | Name                                 |
----|--------------------------------------|
 01 | gponPhysDCAlarm0
 02 | gponPhysDCAlarm1
 03 | gponPhysFanAlarm0
 04 | gponPhysFanAlarm1
 05 | gponPhysFanAlarm2
 06 | gponPhysFanAlarm3
 07 | gponPhysFanAlarm4
 08 | gponPhysFanAlarm5
 09 | gponPhysShelfMupState1
 10 | gponPhysShelfMupState2
 11 | gponPhysShelfExternalAlarm01
 12 | gponPhysShelfExternalAlarm02
 13 | gponPhysShelfExternalAlarm03
 14 | gponPhysShelfExternalAlarm04
 15 | gponPhysShelfExternalAlarm05
 16 | gponPhysShelfExternalAlarm06
 17 | gponPhysShelfExternalAlarm07
 18 | gponPhysShelfExternalAlarm08
 19 | gponPhysCardTypeMismatch
 20 | gponPhysCardFailure
-- More --
SWITCH#
```

The following commands display information about the configured severity of specific alarms.

Command	Mode	Function
show alarm-severity-table *SEVERITY_TABLE_INDEX*	Privileged/ Config	Displays the specified alarm severity profile. **SEVERITY_TABLE_INDEX**: index of alarm severity table index, range of 1-10.
show alarm-severity *ALARM_ID*		Displays the severity of a alarm. **ALARM_ID**: alarm ID value.

Examples

```
SWITCH(config)# show alarm-severity-table 5
AlarmSeverity table for index :
Alarm ID   | Severity |
----------|----------|
01         |    1
02         |    1
 ...
24         |    2
25         |    2
```

```
SWITCH(config)# show alarm-severity 4

AlarmSeverities for Alarm ID 4 :
```

```
Severity Profile Index  | Severity
------------------------|----------
01                      |  1
02                      |  1
03                      |  1
04                      |  1
05                      |  1
06                      |  1
07                      |  1
08                      |  1
09                      |  1
10                      |  1
```

6.3 Displaying the Occured Alarms

Command	Mode	Function
show alarm-list [critical I major I minor I warning I cleared]	Privileged/ Config	Displays the alarm list of the system. **without parameter**: all **critical**: only critical alarms **major**: only major alarms **minor**: only minor alarms **warning**: only warnings **cleared**: only cleared alarms.

Example:

```
SWITCH# show alarm-list critical

Alarm List :
 ID | Severity | Prof| Time and Date                |  rep src type    | rep | Name                      |
    |          | Idx |                              |                  | src |                           |
----|----------|-----|----------------------------|-----------------|-----|--------------------------|
 86 | critical | 01  | Tue 13 Jun 2000, 23:26:35  | SyncSource       | 01  | gponSyncClockSourceAlarm
 86 | critical | 01  | Tue 13 Jun 2000, 23:26:35  | SyncSource       | 02  | gponSyncClockSourceAlarm
All values are decimals...
```

Command	Mode	Function
show alarm-list-reportingsourcetyp { physical_entity I interface I vcctp I vlan I bridgeport I erpdomain }	Privileged/ Config	Displays the alarm list of the system. **physical_entity**: only alarms from physical entity **interface**: only alarms from interfaces **vcctp**: only alarms from **VCC TP** **vlan**: only alarms from **VLAN** **bridgeport**: only alarms from bridge port **erpdomain**: only alarms from ERP domain (Ethernet ring protection is not supported by GPON).
show alarm-list-cxu		Displays CXU alarms.
show alarm-list-iu-addr *SLOT*		Displays the alarms of a certain **IU** address (IU and ONTs). **SLOT**: OLT-slot of IU_GPON.
show alarm-list-gpon-port *ADDRESS*		Displays the alarms with a certain GPON port address (GPON-line/port and ONTs). **ADDRESS**: OLT-slot/GPON-port.
show alarm-list-ont-addr *ADDRESS*		Displays the alarms with a certain ONT address (ONT and ONT cards). **ADDRESS**:OLT-slot/GPON-port/ONU-ID.
show alarm-list-ont-card-addr *ADDRESS*		Displays the alarms with a certain ONT card address. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.
show alarm-list-oid		Displays alarm list of the system shown by OIDs.
show alarm-list-sync		Displays alarms which are synchronized by alarm manager to standby (standby available messages).

The list header of the above **show alarm-list** commands is shown below.

```
Alarm List :
 ID | Sev | SevProfIdx   | Time and Date              | rep src type | rep src | MIB Object ID |
----|-----|-------------|----------------------------|--------------|---------|---------------|

All values are decimals...
```

6.4 Configuring the GPON Alarm Thresholds

The GPON thresholds are used to calculate the alarms “signal failed” (Sf) and “signal degraded” (Sd). There is one pair of values for the whole NE. Note that the Sd-threshold value must be higher than Sf-threshold value.

The Sf-alarm as well as the Sd-alarm become active if the bit error rate is equal to or greater than 10E-X and it become inactive if the bit error rate is lower than 10E-(X+1).

Command	Mode	Function
gpon threshold <3-8> <4-9>	Config	Changes alarm threshold. **3 - 8**: 10^-SfThresh value (default 10E-3) **4 - 9**: 10^-SdThresh value (default 10E-4).
show gpon threshold		Shows alarm thresholds.

6.5 Configuring the CPU Overload Threshold

Command	Mode	Function
threshold cpu <20-100> { 5 I 60 I 600 }	Config	Configures CPU overload threshold. **20 - 100**: Threshold in percent **5, 60, 600**: Time interval in sec.

7 OLT Equipment

This chapter contains information about configuration of the OLT cards.

- Creating a new Card
- Changing the Admin State of Card
- Reset of Interface Unit Cards
- Deleting an Existing Card
- Converting of IU_GPON Cards
- Checking the MAC Table of Interface Unit Card
- Selecting Alarm Severity Profiles of Cards, Rack & Self
- Configuring External Alarms
- Checking the Physical Tables.

7.1 Creating a new Card

The creation of an OLT card is possible without the necessity that the card has to be equipped into shelf's slot. If this card is plugged-in later, the system will be check whether the equipped card type is matching the configured one or not. When the card's type is valid, the admin state changes automatically to "unlocked".

Command	Mode	Function
slot card create *SLOTNUM* { m_iugpon_2512_e | m_iugpon_2512_a | m_iugpon_2512_l_e | m_iu10ge_1o_e | m_iu1ge_10o_e | m_cxuvr_1o_4e_e | m_cxuf4_1o_4e_e } { planned | locked }	Config	Creates a new card. **SLOTNUM**: number of the slot **iugpon_2512_e**: IU with 4 port GPON (2,5/1,2G, class B) with 8x E1 (unstructured), front access **iugpon_2512_a**: IU with 4 port GPON (2,5/1,2G, class B) with 8x DS1 (unstructured), rear access **m_iugpon_2512_l_e**: IU with 4 ports GPON (2.5G/1.2G, Class B), front access **iu10ge_10_e**: IU with 10x1G optical Ethernet interface, 1x10G uplink **iu1ge_10o_e**: IU with 1x10G optical Ethernet interface **m_cxuf4_1o_4e_e**: central unit with 4x1 GigE uplinks, 150G switching capacity, 1x 10G uplink **m_cxuvr_1o_4e_e**: central unit with 4x1 GigE uplinks, 150G switching capacity, 1x 10G uplink, virtual routing support **planned**: set admin state to 'planned' **locked**: set admin state to 'locked'.

7.2 Changing the Admin State of Card

Command	Mode	Function
card admin-state *SLOTNUM* { planned | locked | unlocked }	Config	Changes the admin state of a card. **SLOTNUM**: number of the slot **planned**: set admin state to 'planned' **locked**: set admin state to 'locked' **unlocked**: set admin state to 'unlocked'.

7.3 Reset of Interface Unit Cards

Command	Mode	Function
reset type { m_iugpon_2512_e l m_iugpon_2512_a l m_iugopn_2512_l_e l m_iu10ge_1o_e l m_iu1ge_10o_e }	Config	Resets all modules of the same type. **m_iugpon_2512_e**: IU with 4 port GPON (2,5/1,2G, class B) with 8x E1 (unstructured), front access **m_iugpon_2512_a**: IU with 4 port GPON (2,5/1,2G, class B) with 8x DS1 (unstructured), rear access **m_iu_gpon_2512_l_e**: IU with 4 ports GPON (2.5G/1.2G, class B), front access **m_iu10ge_1o_e**: IU with uplink with optical 10G interface **m_iu1ge_10o_e**: IU with 10x 1G interfaces.

7.4 Deleting an Existing Card

Command	Mode	Function
slot card delete *SLOTNUM*	Config	Deletes an existing card. **SLOTNUM**: number of the slot.

7.5 Converting of IU_GPON Cards

Command	Mode	Function
slot card convert *SLOTNUM* { m_iu_gpon_2512_e l m_iugpon_2512_l_e }	Config	Converts an existing card. **SLOTNUMBER**: number of the slot **m_iu_gpon_2512_e**: converts card to IU_GPON_2512_E (IU with 4 ports GPON (2.5G/1.2G, class B) with 8 x E1 (unstructured), front access **m_iu_gpon_l_e**: converts card to IU_GPON_2512_L_E (IU with 4 ports GPON (2.5G/1.2G, class B), front access.

7.6 Checking the MAC Table of Interface Unit Card

Command	Mode	Function
show iu *ADRESS* **mac table**	Bridge	Displays information of IU's MAC table segmented per specified GPON link or certain ONU. **ADDRESS**: OLT-slot/GPON-port[/ONU-ID].
show iu *ADDRESS* **mac table vlan** [*VLANID*]		Displays information of IU's MAC table for specified GPON link or certain ONU that may be also segmented per VLAN. **ADDRESS**: OLT-slot/GPON-port[/ONU-ID] **VLANID**: show only MAC addresses in specified VLAN.

7.7 Selecting Alarm Severity Profiles of Cards, Rack & Self

Command	Mode	Function
card alarm-severity-profile *SLOTNUM* <1-10>	Config	Changes alarm severity profile. **SLOTNUM**: number of the slot **1 - 10**: index of the profile.
rack alarm-severity-profile <1-10>		Changes rack alarm severity profile.
shelf alarm-severity-profile <1-10>		Changes shelf alarm severity profile.

7.8 Configuring External Alarms

Command	Mode	Function
shelf ext-alarm-output <1-3> [*LINE*]	Config	Changes usage string of an external alarm output. **1 - 3**: number of the alarm output **LINE**: new usage string.
shelf ext-alarm-input <1-8> <0-1> [*LINE*]		Changes level and usage string of an external alarm input. **1 - 8**: number of the alarm input **0 - 1**: low or high active **LINE**: new usage string.

7.9 Checking the Physical Tables

Command	Mode	Function
show table physical-container	Config	Displays the **SNMP** table. **PHYSINDEX**: physical index to show information for.
show table physical-container *PHYSINDEX*		
show table physical-card		
show table physical-card *PHYSINDEX*		
show table physical-entity		
show table physical-entity *PHYSINDEX*		
show table shelf	Config	Displays the slot usage and configuration for all slots.
show table shelf *SLOTNUM*		Displays the slot usage and configuration. **SLOTNUM**: slot number.
show table physical-shelf	Config	Displays the slot usage and configuration for all slots.
show table physical-rack	Config	Displays the SNMP configuration of the rack.
show card config-state *SLOTNUM*	Config	Displays card specific information for specified slot. **SLOTNUM**: slot number.
show objects temperature	Config	Displays the temperature alarm tresholds of the shelf.

8 CXU Board and Line Redundancy

The hiX 5750 R2.0 provides CXU board redundancy to offer a high level of failure protection regarding to card errors, software failures, and when the uplink line fails. The shelf can be optionally equipped with a second CXU acting in standby mode until a failure condition of the active CXU or the operator trigger a switch-over. In all cases, the active CXU is responsible for the synchronization of the standby one. Measures of CXU board redundancy always implement also the possibility to establish uplink line redundancy for the 10-Gbps line and with reservations up to 4 x 1-Gbps lines.

The board redundancy needs following requirements:

- Both CXU cards must be of the same type.
- In case of upgrading an OLT, a primary CXU with **SW** older than release 2.02 must first be upgraded before the second (standby) board can be plugged-in.

Following redundancy aspects are supported:

- Switching is initiated autonomously by the CXU hardware in case of a watch-dog event (SW error on the currently active CXU).
- Switching can be initiated by the SW as result of a hardware state monitoring or on request of the management system.

ℹ Note that the standby CXU card must be first created in the slot 10, see 7.1 Creating a new Card for further information.

ℹ A plug-out of the currently active CXU board with the objective of initiating a switch-over could result in an interruption of **IU**'s control. Therefore, it must not be performed. At first, execute a **switchover** command.

8.1 Checking Redundancy-States

To check the redundancy states and software consistence between of the equipped CXU cards, use the following commands.

Command	Mode	Function
show redundancy-states	Config	Displays the redundancy states of all plug-in units.
show table shelf *SLOT*		Shows slot usage and slot configuration of the running system. **SLOT**: slot number to show information for.

8.2 Resetting a CXU

ℹ See following sections for further **reset** commands:

- Reset of Interface Unit Cards
- Restarting the System.

Use the following command to initiate a reset of a CXU. Be careful choosing the slot number.

Command	Mode	Function
reset card *SLOT*	Config	Reset of the specified CXU. **SLOT**: slot number.

8.3 Initiating a Switchover

The following commands initiate a manual switch-over. This may be done e.g. in the case of hardware maintenance purposes.

Command	Mode	Function
switchover *SLOT*	Config	Switchover to the standby CXU if the standby unit has no error. **SLOT**: slot number of the **active** CXU.
switchover-forced *SLOT*		Switchover to the standby CXU is forced also when it is in inferior state than the active one.

8.4 Uplink Line Redundancy

Uplink line redundancy measures are supported for 10-GE lines and 1-GE lines.

Using uplink line redundancy requires an LAG (LACP) configuration on the OLT (see 24.3 Configuring LACP) and the aggregation switch(es). Note that configuration steps referring to logical ports must be performed using the default CXU slot#9.

In case of the 10-GE port, the LAG on the OLT contains only one line. The required cabling diagram using 1-GE line redundancy is shown in Figure 3. CXU#A is the active one in this case.

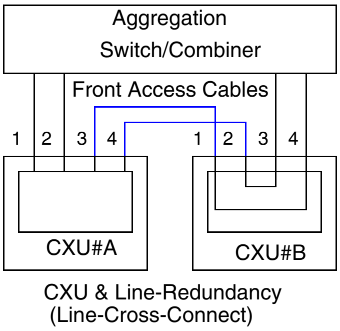


Figure 3 CXU and 1-GE Redundancy (Example)

9 ONU Equipment

In order to configure the **ONU** equipment, use the commands described in the following sections:

- Creating an ONU
- Modifying ONU Parameter
- Deleting an ONU
- Checking the List of Alarms
- Checking the Configuration.

For further information about how to configure the hiX5709 MDU equipment see chapter 9.15 MDU hiX 5709.

9.1 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 18 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)

9.2 Creating an ONU

An ONU can be created in one of two modes:

- **Configured serial number**: In this mode the serial number, as printed on the ONU, must be set. If an ONU is detected with a serial number that is equal to the configured one, this ONU starts up with the associated configuration data set.
- **Discover mode**: Each ONU is assigned a unique password. The password is only transmitted upstream and cannot be changed from OLT side. If the OLT reference password is initialized with the appropriate command, the received ONU password can be compared with the local stored OLT reference password. If an ONU with unknown serial number is detected and the password “Reg ID” is matching with the stored one, the configuration will be completed with this ONU's serial number.

Command	Mode	Function
create onu { hiX5701-001 | hiX5701-002 | hiX5701-003 | hiX5701-004 | hiX5702-001 | hiX5703-001 | hiX5703-003 | hiX5704-001 | hix5705-001 | hix 5705-003 | g25a-001 | g25a-002 | g25a-003 | g25c-001 | g25e-001 | g25e-002 | g50a-001 | g50a-002 | g80rg-001 | hiX5709-001 | hiX5709-003 } *ADDRESS* { configured *SERIAL_NUMBER* { nopassword | password *PASSWD* } | discover *REG_ID* } <1-10> { on | off } {0 | { 1 <1-444> } } <0-1099560000> <0-1099560000> <0-1099560000> <0-1099560000> <0-1099560000> <0-1099560000> *LINE*	Config	Creates specific entries (ONU type), see list above. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **SERIAL_NUMBER**: serial number of the ONU/ONT as hexadecimal number (8 signs if all is ASCII, 12 signs if the first 4 are ASCII and the remaining are HEX, 16 signs if all is HEX), must be set in this mode with or without password. **PASSWD**: Registration ID of the ONU/ONT (max .10 signs) **REG_ID**: registration ID of the ONU/ONT (max. 10 signs) must be set in this mode **1 - 10**: alarm severity profile **on/off**: **GPON** battery backup on/off. If “off”, no related alarms (battery missing, battery failure, battery low) are generated. **0 - 1**: security mode: 0 - no encryption. When encryption for the whole ONT is switched off, the NE automatically switches off the encryption for the affected GEM ports. 1 - **AES** encryption (of downstream payload) **1 - 444**: time for periodical key switchover in units of 5 minutes from 1 (5 minutes) up to 444 (37 hours) The bandwidth values in bps: **0 - 1099560000**: fixed bandwidth allocated for all **TDM** interfaces of this ONU **0 - 1099560000**: fixed bandwidth allocated for all POTS (VoIP) interfaces of this ONU **0 - 1099560000**: assured bandwidth allocated for all high priority realtime data interfaces of this ONU **0 - 1099560000**: assured bandwidth allocated for all high priority priority non-realtime data interfaces of this ONU **0 - 1099560000**: maximum bandwidth allocated for all high priority non-realtime data interfaces of this ONU **0 - 1099560000**: maximum bandwidth allocated for all best effort data interfaces of this ONU **LINE**: user data (max. 80 characters).

Example:

```
SWITCH#enable
SWITCH#configure terminal
SWITCH(config)#create onu g25e-001 3/1/0 configured
4349474707074602 nopassword 3 off 0 45000 45000 45000 45000 45000
28000000 YourString
```

```
ONU 3/1/0 created successful!
```

9.3 Modifying ONU Parameter

Command	Mode	Function
modify onu configuremode *ADDRESS SERIAL_NUMBER* [*PASSWD*]	Config	Sets the configure mode for the ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **SERIAL_NUMBER**: sets the new serial number of the ONU (8 signs if all is ASCII, 12 signs if the first 4 are ASCII and the remaining are HEX, 16 signs if all is HEX) **PASSWD**: (optional) sets the new password or registration ID as hexadecimal (max. 20 signs for 10 bytes).
modify onu discovermode *ADDRESS PASSWD*	Config	Modifies the discover mode for the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **PASSWD**: set the new password or registration ID as hexadecimal (max. 20 signs for 10 bytes).
modify onu password *ADDRESS* { set *PASSWD* | delete }	Config	Modifies the password for the ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **PASSWD**: password or registration ID of the ONU/ONT (max. 20 signs for 10 bytes) **delete**: delete the set password.
modify onu adminstate *ADDRESS* { unlock | lock }	Config	Modifies the administrative state of the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.
modify onu alarm-severity-profile *ADDRESS* <1-10>	Config	Modifies the alarm severity profile of the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **1 - 10**: index alarm severity profile.
modify onu batterybackup *ADDRESS* { on | off }	Config	Modifies the battery backup mode of the specified ONU. **ADDRESS**: slot/port/ONU ID.
modify onu securitymode *ADDRESS* <0-1>	Config	Modifies the security mode of the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **0 - 1**: security mode: 0 - no encryption. When encryption for the whole ONT is switched off, the NE automatically switches off the encryption for the affected GEM ports. 1 - AES encryption (of downstream payload)
modify onu securityuserdata *ADDRESS* { 128 |192 | 256 } <1-144>	Config	Modifies the security user data for the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **128/192/256**: AES encryption with 128/192/256 bit ℹ The AES key length is fixed to 128 Bit. **1 - 144**. time for periodical key switchover in 5 min steps from 5 min to 37 h
modify onu userdata *ADDRESS LINE*	Config	Modifies the user data of the specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **LINE**: userdata (max. 80 characters).

9.4 Deleting an ONU

Command	Mode	Function
delete onu *ADDRESS*	Config	Deletes specified entry. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

9.5 Getting List of Unknown ONTs

Command	Mode	Function
gpon get unknown-onu-list *ADDRESS*	Config	Gets the current list of unknown ONTs at a GPON link. **ADDRESS**: OLT-slot/GPON-port.

9.6 Replacing an ONU

The ONU replacement bases on commands described in other sections of this document. It is mentioned here also as example for these commands.

1. Verifying the Alarm List and the Unknown ONU List

The example below shows alarms indicated by an unknown ONU.

ℹ The registration ID of an unknown ONU will be displayed only if there is at least one ONU configured in “discover” mode on the GPON link. The registration ID is displayed as long as the ONU is not configured.

```
SWITCH(config)# show alarm-list

Alarm List :
ID | Severity | Prof| Time and Date              |  rep src type   | rep | Name
   |          | Idx |                            |                 | src |
---|----------|-----|----------------------------|-----------------|-----|-------------------------
80 | critical | 01  | Mon 14 Jul 2008, 13:34:34 | SyncSource      | 01  | gponSyncClockSourceAlarm
59 | critical | 01  | Mon 14 Jul 2008, 13:35:51 | Interface       | 201 | gponGponLineAlarmOnuMismatch
39 | critical | 01  | Mon 14 Jul 2008, 13:36:50 | Physical Entity | 270497 | gponGponOnuNotInstalled
All values are decimals...

SWITCH(config)# show gpon unknown-onus
address |   #  ||     serial       |        registrationID
=====================================================================
2/ 1    |   1  || 4349474707021259  |        -- -- -- -- --
```

2. Verifying the Configuration of the Unknown ONU

```
SWITCH(config)# show onu table 2/1/1
-----------------------------------------------------------
OltSlot: 2, GponPort: 1, OnuId: 1
Configured onu type       : G25A-001
Serialnumber method       : 1 (configured mode)
Serialnumber    (ASCII)   : CIGG°°°°
Serialnumber    (HEX)     : 0x4349474707020000
Password/Reg-Id (ASCII)   : °°°°°°°°°°
Password/Reg-Id (HEX)     : 0x00000000000000000000
Equipment-Id    (ASCII)   : °°°°°°°°°°°°°°°°°°°°
Equipment-Id    (HEX)     : 0x0000000000000000000000000000000000000000
Version         (ASCII)   : °°°°°°°°°°°°°°
Version         (HEX)     : 0x0000000000000000000000000000
Vendor-Id       (ASCII)   : °°°°
Vendor-Id       (HEX)     : 0x00000000
Vendor product code       : 0
Pptp index                : 201
Physical index            : 270369
Alarmseverity profile     : 1
Onu is detected           : 2   (false)
Adminstate                : 1   (ONU unlocked)
Operstate                 : 2   (ONU disabled)
Security option           :-1   (SecurityOption unknown)
Security mode             : 0   (no encryption selected)
Key length                : 128 (bit)
Key switching time        : 1   (5 min)
Battery backup option     :-1   (BackupOption unknown)
Battery backup mode       : 2   (Backup disabled)
Traffic management option : 1   (cellRateControlled)
Powerlevel                : 0
Pvid                      : 0
Number of Fans            : 0
Distance                  : 0 metre
User data                 : 2/1/1_G25-A
-----------------------------------------------------------
Found 1 entrie(s)!
-----------------------------------------------------------
```

3. Configuring the ONU Registration-ID in Discover-Mode

At first, the unknown (replaced) ONU must be "locked". In order to configure the ONU registration ID, the serial number method must be set to “discover” mode. Note that the registration ID is only sent in upstream direction. Hence, the registration ID that is now set has to match with the ID that was directly configured on ONU before. This step should be finished with a configuration check.

```
SWITCH(config)# modify onu adminstate 2/1/1 lock
SWITCH(config)# modify onu discovermode 2/1/1 30303037303231323539
SWITCH(config)# show onu table 2/1/1
-----------------------------------------------------------
OltSlot: 2, GponPort: 1, OnuId: 1
Configured onu type       : G25A-001
Serialnumber method       : 2 (discover mode)
Serialnumber    (ASCII)   : °°°°°°°°
Serialnumber    (HEX)     : 0x0000000000000000
Password/Reg-Id (ASCII)   : 0007021259
Password/Reg-Id (HEX)     : 0x30303037303231323539
Equipment-Id    (ASCII)   : °°°°°°°°°°°°°°°°°°°°
Equipment-Id    (HEX)     : 0x0000000000000000000000000000000000000000
Version         (ASCII)   : °°°°°°°°°°°°°°
Version         (HEX)     : 0x0000000000000000000000000000
Vendor-Id       (ASCII)   : °°°°
Vendor-Id       (HEX)     : 0x00000000
Vendor product code       : 0
Pptp index                : 201
Physical index            : 270369
Alarmseverity profile     : 1
Onu is detected           : 2   (false)
Adminstate                : 2   (ONU locked)
Operstate                 : 2   (ONU disabled)
Security option           :-1   (SecurityOption unknown)
Security mode             : 0   (no encryption selected)
Key length                : 128 (bit)
Key switching time        : 1   (5 min)
Battery backup option     :-1   (BackupOption unknown)
Battery backup mode       : 2   (Backup disabled)
Traffic management option : 1   (cellRateControlled)
Powerlevel                : 0
Pvid                      : 0
Number of Fans            : 0
Distance                  : 0 metre
User data                 : 2/1/1_G25-A
-----------------------------------------------------------
Found 1 entrie(s)!
-----------------------------------------------------------
```

4. Unlocking the ONU

Unlock the ONU and wait until the discovery method is finished. The serial number is filled in and the “Serial number method” is set to “configured”. There are no further configuration steps required, the OLT ranges the replacement ONU with the original configuration data.

```
SWITCH(config)# modify onu adminstate 2/1/1 unlock
SWITCH(config)# show onu table 2/1/1

-----------------------------------------------------------
OltSlot: 2, GponPort: 1, OnuId: 1
Configured onu type       : G25A-001
Serialnumber method       : 1 (configured mode)
Serialnumber    (ASCII)   : CIGG°°°Y
Serialnumber    (HEX)     : 0x4349474707021259
Password/Reg-Id (ASCII)   : 0007021259
Password/Reg-Id (HEX)     : 0x30303037303231323539
Equipment-Id    (ASCII)   : 00000000109-00120-05
Equipment-Id    (HEX)     : 0x3030303030303030313039 2D30303132302D3035
Version         (ASCII)   : 00109-00120-05
Version         (HEX)     : 0x30303130392D30303132302D3035
Vendor-Id       (ASCII)   : CIGG
Vendor-Id       (HEX)     : 0x43494747
Vendor product code       : 0
Pptp index                : 201
Physical index            : 270369
Alarmseverity profile     : 1
Onu is detected           : 1   (true)
Adminstate                : 1   (ONU unlocked)
Operstate                 : 2   (ONU disabled)
Security option           : 1   (AES encryption implemented)
Security mode             : 0   (no encryption selected)
Key length                : 128 (bit)
Key switching time        : 1   (5 min)
Battery backup option     :-1   (BackupOption unknown)
Battery backup mode       : 2   (Backup disabled)
Traffic management option : 1   (cellRateControlled)
Powerlevel                : 3
Pvid                      : 0
Number of Fans            : 0
Distance                  : 28 metre
User data                 : 2/1/1_G25-a
-----------------------------------------------------------
Found 1 entrie(s)!
-----------------------------------------------------------
```

9.7 Setting the Number of Fans

Command	Mode	Function
modify onu fans ADDRESS <0-2>	Config	Sets the number of ONU fans. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **0 - 2**: fan number 0: without fan 1: fan unit equipped with 1 fan 2: fan unit equipped with 2 fans.

9.8 Synchronizing the ONU Time

Command	Mode	Function
synchronize onu time *ADDRESS*	Config	Synchronize the start time of all monitoring managed entities of this ONU with the reference time of the OLT. All ONU's performance data are reset. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

9.9 Reset an ONU

Command	Mode	Function
reset onu *ADDRESS* [ignore-operstate]	Config	Resets a certain ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **ignore-operstate**: ignore operstate of ONU (optional).

9.10 Performing the ONU Selftest

Command	Mode	Function
selftest onu *ADDRESS*	Config	Triggers an ONU Selftest. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

9.11 Managing the Software Load

The ONT stores 2 images. One image is the active and committed load. This load is currently running and will be used after a reset. It is always available. The second image is inactive. It will be overwritten during a software download. After successful download process (the load is valid) the new load is automatically activated and committed (the images are swapped). With the following commands, this process can be further specified.

Command	Mode	Function
modify onu setcommittedload *ADDRESS* { stored-inactive I running-active I not-available } [activate] [ignore-operstate]	Config	Sets the committed load of a line card. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **stored-inactive**: commits the stored inactive load **running-active**: commits the running active load **not-available**: does not commit any load **activate**: optional, activate inactive load **ignore-operstate**: optional, does not check the operstate.
modify onu activate-inactive-load *ADDRESS* [ignore-operstate]	Config	Activates the inactive load of a line card. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **ignore-operstate**: does not check the operstate.

9.12 Checking the List of Alarms

Command	Mode	Function
show alarm-list-ont-addr *ADDRESS*	Config	Displays the alarms with a certain ONT address (ONT and ONT cards). **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

Command	Mode	Function
show alarm-list-ont-card-addr *ADDRESS*	Exec/ Config	Displays the alarms with a certain ONT card address. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot

9.13 Checking the Configuration

Command	Mode	Function
show onu type { hiX5701-002 I hiX5701-003 I hiX5701-004 I hiX5702-001 I hiX5703-001 I hiX5703-003 I hiX5705-001 I hiX5705-003} I hix5709-001 I hix5709-003 I g25a-001 I g25a-002 I g25a-003 I g25c-001 I g25e-001 I g25e-002 I g50a-001 I g50a-002 I g80rg-001 } [*ADDRESS*]	Config	Search for the specified ONU type. **ADDRESS**: OLT-slot/GPON-port/ONU-ID
show onu adminstate { unlocked I locked } [*ADDRESS*]	Config	Displays ONU IDs with the specified administrative state. **unlocked**: show unlocked ONUs **locked**: show locked ONUs **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show onu operstat { enabled I disabled } [*ADDRESS*]	Config	Displays ONU IDs with specified operational state. **enabled**: show enabled ONUs **disabled**: show disabled ONUs **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show onu serialnumber *SERIAL_NUMBER*	Config	Search for the specified serial number of an ONU. **SERIAL_NUMBER**: Enter the serial number.
show onu ids { used I free } [*ADDRESS*]	Config	Search for the specified ONU IDs on an interface. **used**: for displaying ONU IDs, which are used on an interface **free**: for displaying ONU IDs, which are not used on an interface **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show gpon ont-config *ADDRESS*	Config	Show a ONT configuration data. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show onu flags *ADDRESS*	Config	Shows the flags for an ONU entry. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show gpon unknown-onus	Config	Shows all unknown ONUs.
show onu table [*ADDRESS*]	Config	Displays the ONU table of system. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show onu *ONUINDEX* **mac table**	Bridge	Shows ONU specific information of MAC address table. **ONUINDEX**: address OLT-slot/GPON-port/ONU-ID.
show onu *ONUINDEX* **mac table vlan** [*VLANID*]		Shows ONU specific information of MAC address table segmented per port. **VLANID**: show only MAC addresses in one VLAN.
show ponpptp ont { table I list} [*ADDRESS*]	Config	Displays PON interface on ONT/ONU. **table**: table with config data **list**: list **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show table onu-physical-container *ADDRESS*	Config	Displays **SNMP** table for a specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.
show table onu-physical-entity *ADDRESS*	Config	Displays SNMP table for a specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.
show table onu-physical-rack *ADDRESS*	Config	Displays SNMP table for a specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.
show table onu-physical-shelf *ADDRESS*	Config	Displays SNMP table for a specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

Command	Mode	Function
show table onu-physical-card *ADDRESS*	Config	Displays SNMP table for a specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.
show onu-loads [*ADDRESS*]	Config	Shows load versions of MDU cards and ONUs. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.
show onu description *ADDRESS LINE*	Config	Displays ONU IDs with the specified user data. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]] **LINE**: The full matching user data.
show onu first-entry	Config	Displays the first ONU table entry.
show linecard table [*ADDRESS*]	Config	Displays the specified linecard entries. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID[/ONU-slot]]].
show linecard first-entry	Exec/ Config/ Bridge	Displays first entry of linecard table.
show linecard config-state { not-configured I running I failed I finished } [*ADDRESS*]	Exec/ Config	Shows the specified linecard entries, The linecard-table with the specified configuration state. **not-configured**: show the not configured cards **running**: show the cards, where configuration is running **failed**: show the cards, where configuration has failed **finished**: show the cards, where configuration has finished. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].
show port onu [*ONUS*]	Exec/ Config/ Bridge	Displays the Ethernet interface on ONU. **ONUS**: ONU address (slot/port/ONU ID).
show port onu saved-data		Displays the saved ONU Ethernet configuration.
show port onu dte-dce *ONUS*		Displays the DTE/DCE status of Ethernet interfaces on ONU. **ONUS**: ONU address (OLT-slot/GPON-port/ONU-ID).

9.14 Checking the MAC Table

Use the following commands to examine the switch MAC addresses.

Command	Mode	Function
show onu *ONUINDEX* **mac table**	Bridge	Shows ONU specific information about MAC table. **ONUINDEX**: OLT-slot/GPON-port/ONU-ID.
show onu *ONUINDEX* **mac table vlan** [VLANID]		Shows ONU specific information segmented per port or VLAN. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **VLANID**: show only MAC addresses in one VLAN.

9.15 MDU hiX 5709

Use the commands described in the following sections to configure the hiX 5709 **MDU**:

- Creating of MDU Cards
- Changing the Admin State
- Setting of Alarm Severities and External Alarms
- Setting the Number of Fans
- Checking the Configuration Data.

9.15.1 Creating of MDU Cards

Command	Mode	Function
mdu card create *ADDRESS* { m_sb_8p4ge_e I m_sb_24p_e I m_sbxdsl_12_e I m_sbxdsl_16_e I m_sbxdsl_16p_e I m_sbxdsl_16p_sl_e I m_ubgpon_2512_e I m_ubgpon_catv_e } { locked I unlocked }	Config	Creates a new MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **m_sb_8p4ge_e**: service board with 8x**POTS** and 4x GE electric, front access **m_sb_24p_e**: service board with 24x POTS, front access **m_sbxdsl_12_e**: service board with 12x x**DSL**, front access **m_sbxdsl_16_e**: service board with 16x xDSL, front access **sbxdsl_16p_e**: service board with 16x xDSL and splitter, Annex A POTS VDSL2, front access **sbxdsl_16p_sl_e**: service board with 16x xDSL for splitter less applications, ADSL Annex A POTS, VDSL2 Region B, front access **m_ubgpon_2512_e**: **GPON** uplink board, infrastructure and cascading interfaces, front access **m_ubgpon_catv_e**: GPON uplink board, infrastructure and cascading interfaces, CATV interface, front access **locked**: set adminstate to locked **unlocked**: set adminstate to unlocked.
mdu card create <1-32> *GPON_PORT ONU_ID MDU_SLOT* { m_sb_8p4ge_e I m_sb_24p_e I m_sbxdsl_12_e I m_sbxdsl_16_e I m_sbxdsl_16p_e I m_sbxdsl_16p_sl_e I m_ubgpon_2512_e I m_ubgpon_catv_e } { locked I unlocked }		Creates a new MDU. **1 - 32**: MDU number **GPON_PORT**: enter GPON port number **ONU_ID**: enter ONU ID number **MDU_SLOT**: enter MDU SLOT number.
mdu card delete *ADDRESS*		Deletes a card. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.

9.15.2 Changing the Admin State

Command	Mode	Function
mdu card adminstate *ADDRESS* { locked I unlocked }	Config	Changes the adminstate of a specified MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **locked**: set adminstate to locked **unlocked**: set adminstate to unlocked.

9.15.3 Setting of Alarm Severities and External Alarms

Command	Mode	Function
mdu card alarm-severity-profile *ADDRESS* <1-10>	Config	Changes the alarm severity profile of a specified MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **1 - 10**: profile index.
mdu rack alarm-severity-profile *ADDRESS* <1-10>		Changes the rack alarm of a specified MDU.
mdu shelf alarm-severity-profile *ADDRESS* <1-10>		Changes the shelf alarm of a specified MDU.
mdu shelf ext-alarm-output *ADDRESS* <1-3> [*LINE*]	Config	Changes the usage string of the external alarm output of a specified MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **1 - 3**: number of external alarm output **LINE**: new usage string.

Command	Mode	Function
mdu shelf ext-alarm-input *ADDRESS* <1-8> <0-1> [*LINE*]	Config	Changes the usage string of the external alarm input of a specified MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot **1 - 8**: number of external alarm input **0 - 1**: input is low or high-active **LINE**: new usage string.

9.15.4 Setting the Number of Fans

Command	Mode	Function
modify onu fans ADDRESS <0-2>	Config	Sets the number of MDU fans. **ADDRESS**: OLT-slot/GPON-port/ONU-ID **0 - 2**: fan number 0: without fan 1: fan unit equipped with 1 fan 2: fan unit equipped with 2 fans.

9.15.5 Checking the Configuration Data

Command	Mode	Function
show onu card config-state *ADDRESS*	Config	Displays state of configuration for a specified MDU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.

10 Ports

Ports can be configured in *Configuration* mode and *Bridge configuration* mode. Execute the **bridge** command to change the system prompt from `SWITCH(config)#` to `SWITCH(bridge)#`.

The port configuration is described in following sections:

- General Configuration
- GPON Port Configuration
- Ethernet Port Configuration
- E1/DS1 Port Configuration and Test
- Traffic Management
- Checking Port Configuration
- Port Statistics
- Performance Monitoring
- Payload-Counters.

10.1 General Configuration

Command	Mode	Function
port *PORTS* { enable I disable I test }	Bridge	Enables/disables a port. **PORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **test**: configures a port as test port.
port *PORTS* **alarm-severity-profile** <1-10>		Configures port specific alarm severity profile index. **1 - 10**: profile index.
port *PORTS* **description** *LINE*		Port specific description. **LINE**: text (max.number of characters is 100).
clear port *PORTS* **description**		Clears specific description.

Command	Mode	Function
port { gpon I eth I pots I e1ds1ll I xdsl I catv I ces } *PORTS* { enable I disable I test }	Bridge	Enables/disables a port. **PORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **gpon**: GPON port **eth**: Ethernet port **pots**: POTS port **e1ds1ll**: E1 or DS1 leased line port **xdsl**: xDSL port **catv**: CATV port **ces**: CES port **test**:: configures a port as test port.
port { gpon I eth I pots I e1ds1ll I xdsl I ces } *PORTS* **alarm-severity-profile** <1-10>		Configures port alarm severity for. **1 - 10**: alarm severity profile index.
port { gpon I eth I pots I e1ds1ll I xdsl I catv I ces } *PORTS* **description** *LINE*		Port specific description. **LINE**: text (max. number of characters is 100).
clear port { gpon I eth I pots I e1ds1ll I xdsl I catv I ces } *PORTS* **description**		Clears port specific description,

Command	Mode	Function
gpon olt-alarm *ADDRESS* <1-10>	Config	Sets alarm severity profile for OLT interface: **ADDRESS**: OLT-slot/OLT-port **1 - 10**: alarm severity profile index.
gpon ont-alarm *ADDRESS* <1-10>		Sets alarm severity profile for **ONT**/ONU interface: **ADDRESS**: OLT-slot/GPON-port/ONU-ID **1 - 10**: alarm severity profile index.

10.2 GPON Port Configuration

This chapter is divided in the following sections:

- T-CONTs
- DBA and Overbooking
- GEM Port GAL Profiles
- GEM Traffic Description Profiles
- GEM Ports
- Forward Error Correction.

10.2.1 T-CONTs

A **T-CONT** represents a logical connection group, since it accommodates GEM packets. The **NE** sets all bandwidth parameters according to the ONU type when it creates the T-CONTs. Smallest bandwidth unit is always 510000 bps (an entered bandwidth value is rounded down to the next multiple of 510000).

Required bandwidth for one interface:

- E1 interface 2040000 bps
- DS1 interface 1530000 bps
- POTS-VoIP interface 113600 bps
- OMCI channel per ONU requires 38400 bps.

Type	Fixed BW	Assured BW	Max. BW	CoS
1	X			TDM, VoIP
2		X		Data rt
3		X	X	Data hp
4			X	Data BE

Table 19 T-CONT Bandwidth Types

Command	Mode	Function
modify t-cont bandwidth { tdm | voip | data-be | data-hp | data-rt } *TCONTS* <0-1099560000> <0-1099560000> <0-1099560000>	Bridge	Configures bandwidth of T-CONT depending on its type. Note that there are some bandwidth values will be ignored and set to ZERO. **tdm**: time division multiplexing (1) **voip**: voice over internet protocol (1) **data-rt**: data-real time (2) **data-hp**: data-high priority (3) **data-be**: data-best effort (4) **TCONTS**: assigned ONU address (slot/port/ONU-ID) Use multiple of 510000 to configure the following bandwidth values. **0 - 1099560000**: fixed bandwidth (bit/s), only valid for T-CONT type 1. Must be set to ZERO for other T-CONT types. Configurable ranges: - voip: 0-130050000 - tdm: 0-1099560000 **0 - 1099560000**: assured bandwidth (bit/s), only valid for T-CONT types 2, and 3. Must be set to ZERO for other T-CONT types. **0 - 1099560000**: maximum bandwidth (bit/s), only valid for T-CONT types 3 and 4. Must be set to ZERO for other T-CONT types. ℹ The command fails in case of overbooking.
t-cont { tdm | voip | data-be | data-hp | data-rt } *TCONTS* **modify bandwidth** <0-1099560000> <0-1099560000> <0-1099560000>		
modify t-cont { tdm | voip | data-be | data-hp | data-rt } *TCONTS* **bandwidth** <0-1099560000> <0-1099560000> <0-1099560000>		

Command	Mode	Function
show tcont { table | list } [*ADDRESS*] [tdm | voip | data-be | data-hp | data-rt | data]	Config/ Bridge	Displays transmission container. **table**: table with config data **list**: list with config data **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]] **tdm**: time division multiplexing **voip**: voice over Internet protocol **data-be**: data - best effort **data-hp**: data - high priority **data-rt**: data - real time **data**: all data.

10.2.2 DBA and Overbooking

Dynamic Bandwidth Allocation (DBA) is a technique for allocating bandwidth based on current traffic requirements. If the DBA mechanism is used, the OLT can rearrange the upstream bandwidth to provide more resources for those ONTs that are tightly loaded with traffic. The OLT monitors the incoming traffic from the ONTs for each single T-CONT. If the ONT has to send no traffic, it transmits GEM-idle frames. If the OLT observes that a certain ONT is sending at least one user GEM frame, it increases the bandwidth allocation for this ONT.

Command	Mode	Function
gpon bamode *ADDRESS* { staticba | nsrdba }	Config	Sets type of upstream bandwidth allocation on T-CONT level provided by the OLT. **ADDRESS**: OLT-slot/OLT-port **staticba**: static BA **nsrdba**: non status reporting dynamic BA.

10.2.3 GEM Port GAL Profiles

The **GAL** profile of a **GEM** port can only be modified if such **ONT**s/**MDU** cards, which are using it, were set in admin state “locked” or they are offline.

The command parameter *priority-ID* (1-8) is an internalal index to address GEM ports on an interface. By default, packets with a higher .1p priority will be forwarded over a GEM port with higher (or equal) priority-ID than packets with lower .1p priority.

Command	Mode	Function
gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **modify gal-profile** <1-16>	Bridge	Configures GEM adaption layer profile. **eth**: Ethernet interface **voip**: internal voice over IP interface **e1ds1ll**: E1DS1 leased line interface **xdsl**; xDSL port **GEMPORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **1- 8**: priority-ID of GEM port **1-16**: profile table index.
modify gemport gal-profile { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> <1-16>		
modify gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **gal-profile** <1-16>		

The following GAL profiles are related to a GEM IW TP. One default profile with index 1 always exists.

Command	Mode	Function
gal-eth-profile create <1-65535>	Bridge	Creates GEM adoption layer ethernet profile. **1 - 65535**: payload size.
create gal-eth-profile <1-65535>		
gal-eth-profile delete <2-16>	Bridge	Deletes GEM adoption layer ethernet profile. **2 - 16**: gal-eth-profile table index.
delete gal-eth-profile <2-16>		
gal-tdm-profile create { byte-stuffing I bit-stuffing I sync-residual-timestamp } *LOF*	Bridge	Creates GEM adoption layer time-division-multiplexing profile. **byte-stuffing**: byte stuffing **bit-stuffing**: bit stuffing **sync-residual-timestamp**: synchronous residual time-stamp **LOF**: duration of the GEM frame loss integration period (ms).
create gal-tdm-profile { byte-stuffing I bit-stuffing I sync-residual-timestamp } *LOF*		
gal-tdm-profile delete <2-16>	Bridge	Deletes GEM adaption layer time-division-multiplexing profile. **2 - 16**: GAL-TDM-profile table index.
delete gal-tdm-profile <2-16>		

Command	Mode	Function
show gal-eth-prof table	Config/ Bridge	Displays **GEM** adaption layer Ethernet profile table.
show gal-tdm-prof table		Displays GEM adaption layer time-division-multiplexing profile table.

10.2.4 GEM Traffic Description Profiles

The traffic descriptor profile of a GEM port can only be modified if such ONTs/MDU cards, which are using it, were set in admin state “locked” or they are offline.

The command parameter *priority-ID* (1-8) is an internal index to address GEM ports on an interface. By default, packets with a higher .1p priority will be forwarded over a GEM port with higher (or equal) priority-ID than packets with lower .1p priority.

Command	Mode	Function
create traffic-desc-profile <0-150000> <0-150000>	Bridge	Creates traffic description profile. **0 - 150000**: SIR sustained information rate (kbps) **0 - 150000**: PIR peak information rate (kbps).
traffic-desc-profile create <0-150000> <0-150000>		
gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **modify traffic-desc-profile** <0-16>	Bridge	Configures traffic descriptor profile of GEM port. **eth**: Ethernet port **voip**: internal voice over IP interface **e1ds1ll**: E1DS1 leased line interface **xdsl**: xDSL port **GEMPORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **1 - 8**: priority-ID of GEM port **0 - 16**: index of profile table (1-16) - 0 no profile used.
modify gemport traffic-desc-profile { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> <0-16>		
modify gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **traffic-desc-profile** <0-16>		
traffic-desc-profile delete <1-16>	Bridge	Deletes traffic description profile. **1 - 16**: index of traffic description profile.
delete traffic-desc-profile <1-16>		

Command	Mode	Function
show traffic-desc-prof table	Config/ Bridge	Shows traffic description profile.

10.2.5 GEM Ports

This section describes the settings of security mode, alarm severity, and loop state.

ℹ Enabling **AES** on **GEM** port level requires an activation of AES for the ONU, see 9.3 Modifying ONU Parameter.
Related commands are:

- **modify onu securitymode** for enabling/disabling AES
- **modify onu securityuserdata** for setting key update time

If encryption is switched off for an ONU, the **NE** itself switches off the encryption for the affected GEM ports. This takes place without any notification.

ℹ The command parameter *priority-ID* (1-8) is an internal index to address GEM ports on an interface. By default, packets with a higher .1p priority will be forwarded over a GEM port with higher (or equal) priority-ID than packets with lower .1p priority.

Command	Mode	Function
gemport all-of-ont *ONUADDR* **modify security-mode** { off I on }	Bridge	Enables/disables GPON encryption method for all GEM ports of ONT. **ONUADDR**: OLT-slot/GPON-port/ONU-ID **off / on**: no encryption / encryption
modify gemport all-of-ont *ONUADDR* **security-mode** { off I on }		
modify gemport all-of-ont security-mode *ONUADDR* { off I on }		
gemport { eth I voip I e1ds1ll I xdsl} *GEMPORTS* <1-8> **modify security-mode** { off I on }	Bridge	Configures encryption for specified GEM ports of ONT. **eth**: Ethernet port **voip**: internal voice over IP interface **e1ds1ll**: E1DS1 leased line interface **xdsl**: xDSL port **GEMPORTS**: interface address (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **1 - 8**: priority-ID of GEM port **off**: no encryption **on**: AES encryption.
modify gemport security-mode { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> { off I on }		
modify gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **security-mode** { off I on }		

Command	Mode	Function
gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **modify alarm-severity-index** <1-10>	Bridge	Configures alarm severity profile on GEM port. **eth**: Ethernet interface **voip**: internal voice over IP interface **e1ds1ll**: E1DS1 leased line interface **xdsl**: xDSL port **GEMPORTS**: interface address (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **1 - 8**: priority-ID of GEM port **1 - 10**: severity table index.
modify gemport alarm-severity-index { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> <1-10>		
modify gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **alarm-severity-index** <1-10>		
gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **modify loopstate** { loopback I no-loopback }	Bridge	Enables/disables loopback on GPON encapsulation method board. **eth**: Ethernet interface **voip**: internal voice over IP interface **e1ds1ll**: E1DS1 leased line interface. **xdsl**; xDSL port **GEMPORTS**: interface address (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **1 - 8**: priority-ID of GEM port **loopback**: loopback enabled **no-loopback**: loopback disabled.
modify gemport loopstate { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> { loopback I no-loopback }		
modify gemport { eth I voip I e1ds1ll I xdsl } *GEMPORTS* <1-8> **loopstate** { loopback I no-loopback }		

Command	Mode	Function
show gemport { table I list } [*ADDRESS*]	Config/ Bridge	Displays **GEM** port. **table**: table with config data **list**: list with config data **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID[/ONU-slot]]].
show gemport iftype { eth I voip I e1ds1ll I xdsl } *ADDRESS* <1-8>	Config/ Bridge	Displays GEM port table of one specified interface. **eth**: Ethernet interface **voip**: voice over Internet protocol **e1ds1ll**: **E1DS1** Leased Line interface **xdsl**: x**DSL** interface **ADDRESS**: OLT-slot/OLT-port/ONU-ID/ONU-slot/ONU-port **1 - 8**: priority-ID of GEM port.

10.2.6 Forward Error Correction

FEC (Forward Error Correction) is supported for both upstream and downstream transmission. When FEC is enabled, this results in a **SNR** coding gain of about 2.6 dB but the overhead of transmission is increased about 7%.

Command	Mode	Function
gpon fecmode *ADDRESS* { enable I disable }	Config	Enable / disable FEC for downstream transmission. If enabled, non - FEC supporting **ONU**s operate without FEC simultaneously with FEC supporting ONUs. **ADDRESS**: OLT-slot/GPON-port.
gpon fecmode-ont *ADDRESS* { enable I disable }		Enable / disable FEC for upstream transmission. Non - FEC supporting ONUs ignore the command. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.

10.3 Traffic Management

10.3.1 Priority Mapping

One mapper for 802.1p priority queues is associated with one physical ONT user interface or with an internal IP interface. There is a restriction in the priority mapper configuration. Upstream, the incoming tagged packets are mapped to GEM ports with GEM Port ID values that differ in the last 0, 1, 2 or 3 LSB depending on ONT type. A priority mapper serves a group of 1, 2, 4 or 8 consecutive GEM Port ID values.

Command	Mode	Function
prio-map-range { 1 I 2 I 4 I 8 }	Bridge	Configures maximum numbers of GEM ports each priomapper can serve: **1, 2, 4, 8**: max. number is 1 ... 8.
modify prio-map-range { 1 I 2 I 4 I 8 }		
priomapper { eth I xdsl } *INTERFACE* **modify** <0-8> <0-8> <0-8> <0-8> <0-8> <0-8> <0-8> <0-8>	Bridge	Configures .1p mapping. **eth**: Ethernet port **xdsl**: xDSL port **INTERFACE**: OLT-slot/OLT-port/ONU-ID/ONU-slot/ONU-port **1- 8**: select index of GEM port for .1p priority 0 **1- 8**: select index of GEM port for .1p priority 1 **1- 8**: select index of GEM port for .1p priority 2 **1- 8**: select index of GEM port for .1p priority 3 **1- 8**: select index of GEM port for .1p priority 4 **1- 8**: select index of GEM port for .1p priority 5 **1- 8**: select index of GEM port for .1p priority 6 **1- 8**: select index of GEM port for .1p priority 7 **0**: drop.
modify priomapper { eth I xdsl } *INTERFACE* <0-8> <0-8> <0-8> <0-8> <0-8> <0-8> <0-8> <0-8>		

Command	Mode	Function
show base-settings	Config/ Bridge	Displays GPON MAC mode and prio map range.
show priomapper { table I list } [*ADDRESS*]		Displays .1p priority mapper. **table**: table with configuration data **list**: list with configuration data **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID[/ONU-slot]]].
show priomapper iftype { eth I voip I e1ds1ll I xdsl } *ADDRESS*		Displays .1p priority mapper for one specified interface. **eth**: Ethernet interface **voip**: internal voice over IP interface **e1ds1ll**: E1 or DS1 leased line interface **xdsl**: XDSL port **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port.

10.3.2 Queuing

An upstream priority queue is referenced by GEM ports.

Command	Mode	Function
show queue { table I list } [*ADDRESS*]	Config/ Bridge	Displays priority queue (upstream) table/list with config data **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]]

Command	Mode	Function
queue *ADDRESS NUMBER* **modify** <0-65535> <0-255> { enabled I disabled } *TIME* <0-65535> <0-65535>	Bridge	Modifies priority queue (upstream). **ADDRESS**: OLT-slot/GPON-port/ONU-ID **NUMBER**: queue on ONT **0 - 65535**: alloccated queue size in GEM block lengths (Default value is 10) **0 - 255**: queue weight for the WRR algorithm used by the traffic scheduler. (Default value is 1). **enabled**: enable back pressure operation (default) **disabled**: disable back pressure operation **TIME**: back pressure time duration in which the customer terminal temporarily suspends sending data in microseconds. (Default value is 0) **0 - 65535**: back pressure start threshold (Default value is 8) **0 - 65535**: back pressure stop threshold (Default value is 6) Note: BackPressureStartThresh > BackPressureStopThresh.
modify queue *ADDRESS NUMBER* <0-65535> <0-255> { enabled I disabled } *TIME* <0-65535> <0-65535>		

10.3.3 Scheduling

The traffic scheduler accommodates upstream GEM packets after priority queue and transfers the GEM packets toward the T-CONT. The following command shows table entries that are created automatically by the **NE**.

Command	Mode	Function
show scheduler { table I list } [*ADDRESS*]	Bridge	Displays traffic scheduler (upstream) table/list with config data. **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].

10.4 Ethernet Port Configuration

10.4.1 CXU Ports

Command	Mode	Function
port cu *PORTS* { enable I disable I test }	Bridge	Enables/disables a port on CXU. **PORTS**: port number (OLT-slot/OLT-port) **test**: configures a port as test port.
port cu *PORTS* **description** *LINE*		Enables port specific description. **LINE**: max. number of characters is 100.
port cu *PORTS* **alarm-severity-profile** <1-10>		Configures port alarm severity for CXU. **1 - 10**: severity index.

10.4.2 Large Reach Ethernet (LRE) Port

Command	Mode	Function
port lre *PORTS* { enable I disable I test }	Bridge	Enables/disables a **LRE** port on CXU. **PORTS**: port number (OLT-slot/OLT-port) **test**: configures a port as test port.
port lre *PORTS* **description** *LINE*		Enables **LRE** port specific description. **LINE**: max.number of characters is 100).
port lre *PORTS* **alarm-severity-profile** <1-10>		Configures LRE port specific alarm severity profile index. **1 - 10**: profile index.

10.4.3 Type and Negotiation

Command	Mode	Function
port type *PORTS* { electrical I optical }	Bridge	Configures the port type. **PORTS**: port number (OLT-slot/OLT-port) **electrical**: internal electrical mode (default) **optical**: external optical **SFP**.
port nego *PORTS* { force I auto }		Configures the auto-negotiation of specified port. **force**: auto-negotiation disabled **auto**: auto-negotiation enabled.

ℹ Auto-nego is activated in 10/100BASE-TX ports by default.

Even when auto-nego was configured, the transmit rate or the duplex mode of the connected equipment can be changed furthermore.

ℹ It is impossible to configure auto-nego in 100BASE-FX ports (external optical **SFP**).

10.4.4 Link Discovery

Command	Mode	Function
port link-discovery chassis *PORTS A.B.C.D*	Bridge	Configures link discovery (remote shelf IP address) for a specified port. **PORTS**: port number (OLT-slot/OLT-port) **A.B.C.D**: remote chassis IP address.
port link-discovery slot *PORTS RMSLOT*		Configures link discovery (slot value on remote shelf) for a specified port. **RMSLOT**: remote slot number.
port link-discovery port *PORTS RMPORT*		Configures link discovery (port value on remote shelf) for a specified port. **RMPORT**: remote port number.
port link-discovery mode *PORTS* { none I manual I automatic }		Configures link discovery (link discovery mode value) for a specified port. **none, manual, automatic**: Set the mode.

10.5 E1/DS1 Port Configuration and Test

The **NE** automatically creates the entries for each **E1**/**DS1** interface with default settings. The following commands can be used to modify these E1 /DS1 interface settings.

Command	Mode	Function
modify e1-config { local I remote } *ADDRESS* { normal I crc I unframed } { hdb3 I ami } { no I payload I line } { none I bit I message } { loop I local I through } { disabled I enabled }	Config	Modifies E1 interface configuration. **local**: local interface **remote**: remote interface **ADDRESS**: local (OLT-slot/OLT-port) or remote (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **normal**: line type normal **crc**: line type CRC **unframed**: line type unframed - **fixed set!** **hdb3**: line coding HDB3 - **fixed set!** **ami**: line coding **AMI** **no**: loopback config not in loopback state **payload**: loopback config loop through the device **line**: loopback config only looped back out **none**: signal mode no bits are reserved **bit**: signal mode channel associated signaling **message**: signal mode common channel signaling **loop**: transmit clock source recovered receive clock is used **local**: transmit clock source local clock source is used **trough**: transmit clock source uncovered receive clock from another interface **disabled**: channelization is disabled **enabled**: channelization is enabled.
modify ds1-config { local I remote } *ADDRESS* { esf I d4 } { jbzs I b8zs I zbtsi } { no I payload I line} {none I robbedt I message } { loop I local I through } { ansi I att I none }	Config	Modifies DS1 interface configuration. **local**: local interface **remote**: remote interface **ADDRESS**: local (OLT-slot/OLT-port) or remote (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **esf**: line type extended super frame **d4**: line type AT & T D4 format **jbzs**: line coding jammed bit zero suppression **b8zs**: eight zero bits **zbtsi**: zero byte time slot interchange **no**: loopback config not in loopback state **payload**: loopback config loop through the device **line**: loopback config only looped back out **none**: signal mode no bits are reserved **robbed**: signal mode channel associated signaling **message**: signal mode common channel signaling **loop**: transmit clock source recovered receive clock is used **local**: transmit clock source local clock source is used **trough**: transmit clock source covered receive clock from another interface **disabled**: channelization is disabled **enabled**: channelization is enabled

Connecting of two E1/DS1 Interfaces

Note the following restrictions:

- At one GPON link can be connected not more than 8 E1/DS1-ONT interfaces. The NE accepts no other connection commands.
- At all GPON links of one IU_GPON can be connected not more than 8 E1/DS1-ONT interfaces.
- Only the following connections are possible:
  1. and 2. E1 port of IU_GPON -> 1. GPON port of IU_GPON
  3. and 4. E1 port of IU_GPON -> 2. GPON port of IU_GPON
  5. and 6. E1 port of IU_GPON -> 3. GPON port of IU_GPON
  7. and 8. E1 port of IU_GPON -> 4. GPON port of IU_GPON

Command	Mode	Function
create e1ds1 connection *ADDRESSOLT ADDESSSONT*	Config	Creates connection between 2 E1DS1 interfaces of the same type. **ADDRESSOLT**: OLT-slot/OLT-port for interface on OLT side **ADDRESSONT**: OLT-slot/GPON-port/ONU-ID/ONT-slot/ONT-port on ONT side.
delete e1ds1 connection *CONNECTIONID*	Config	Deletes connection between 2 E1DS1 interfaces of the same type. **CONNECTION**: ID of existing connection.

Command	Mode	Function
show e1ds1 connections [[*OLT_SLOT* [[*OLT_PORT*]]]]	Config	Displays a table of connections between 2 E1DS1 interfaces. **OLT_SLOT**: OLT-slot of the IU_GPON (optional) **OLT_PORT**: OLT-port for E1DS1 interface (optional).

Configuring Loopback Test

Command	Mode	Function
modify loopback-config-e1ds1 remote *ADDRESS* { no I payload I line }	Config	Modifies loopback configuration of remote E1DS1 interface. **ADDRESS**: remote address (OLT-slot/GPON-port/ONU-ID/ONT-slot/ONT-port) **no**: a device that is not capable of performing a loopback on the interface shall always return this as its value. **payload**: 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**:The received signal at this interface does not go through the device (minimum penetration) but is looped back out.

10.6 POTS Configuration and Test

Command	Mode	Function
pots changedata *PORTS* <0-1> <0-255> <0-255> <0-1> *RXGAIN TXGAIN* <0-5> <0-2> <0-1>	Bridge	POTS port configuration. **PORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **0 - 1**: alarm reporting control, 0=off. 1=on **0 - 255**: alarm reporting control interval (0-254 in minutes, 255 for infinity) **0 - 4**: impedance, 0=600 Ohm, 1=900 Ohm, 2=complex1, 3=complex2, 4=complex3, 255=invalid (ONU) **0 - 1**: transmission path, 0=POTS full, 1=POTS part time **RXGAIN**: Rx Gain in 0.1 dB steps from -120 (12 dB) to 60 (6 dB) **TXGAIN**: Rx Gain in 0.1 dB steps from -60 (6 dB) to 120 (12 dB) **0 - 5**: maintenance mode, 0=off, 1=test tone, 2=normal polarity, 3=reversed polarity, 4=send metering pulses, 5=send ringing pulses **0 - 2**: metering signal type, 0=on, 1=silent reversal only, 2=frequency only **0 - 1**: feeding, 0=ordinary phone, 1=pay phone.
pots getstateinfo *PORTS*	Config	POTS port state information. **PORTS**: OLT slot/GPON-port/ONU-ID/ONU-slot/ONU-port.

Command	Mode	Function
show port pots *PORTS* **table**	Privileged/ Config/ Bridge	Displays POTS port configuration. **PORTS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port

10.7 CATV Port Configuration

For detailed information refer to the current release notes.

Command	Mode	Function
modify catv ani adminstate *ADDRESS* { lock | unlock }	Config	Sets admin state of CATV port. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port.
modify catv ani-config *ADDRESS* { off | on } <0-255> <0-5> { none | broadband | optical | <0-255> } *AGCSETTINGS*	Config	Configures the ANI of CATV interface. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **off**: alarm reporting allowed immediately **on**: alarm reporting inhibited **0 - 255**: length of time in minutes. An interval value of 255 has the special meaning of 'infinity'. **0 - 5**: indicates the frequency of the pilot channel receiver. The unit is Hz. If SignalCapability =0 or 1, this attribute is undefined; If SignalCapability =2 or 3, this attribute is functionally read only; If SignalCapability =4 or 5, this attribute is read-write. The following parameter allows the discovery and configuration of the ONT's AGC capabilities. It contains code points for the several AGC types. The ONT displays the currently used AGC mode. The OLT can discover new modes via the set command.The code points are: **none**: no AGC is used (0) **broadband**: broadband RF AGC is used (1) **optical**: optical AGC is used (2) **0 - 255**: 3-255, reserved for future use **AGCSETTINGS**: indicates the measurement offset that the ONT should use if using broadband RF signal level or total optical power as a basis for AGC. Enter AGC value (Step-size of 0.1 dB).
modify catv uni-config *ADDRESS* { off | on } <0-255> { enable | disable } { bothBlocked | lowPassed | bothPassed }	Config	Configures the UNI of CATV interface. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port **off**: alarm reporting allowed immediately **on**: alarm reporting inhibited **0 - 255**: length of time in minutes. An interval value of 255 has the special meaning of 'infinity'. Following parameter controls whether power is provided to an external equipment over the video PPTP. **enable**: power over COAX **disable**: disables power feed Switching between two fixed pass band plans in order to differentiate the services delivered to the subscriber **bothBlocked**: both frequency bands blocked **lowPassed**: only low frequency band passed **bothPassed**: both frequency bands passed.

Command	Mode	Function
show catv ani if-table	Config	Shows ANI interface table.
show catv uni if-table	Config	Shows UNI interface table.

10.8 Checking Port Configuration

Command	Mode	Function
show port { *PORTS* I all }	Privileged/ Config/ Bridge	Shows configured state of port. **PORTS**: port number OLT-slot/OLT-port **all**: shows all ports
show port *PORTS* **description**		Shows port specific description (max.number of characters is 100).
show port { gpon I eth I pots I e1ds1lI I xdsl I catv I ces} *PORTS* **description**		Shows port specific description. **gpon**: GPON port **eth**: Ethernet port **pots**: POTS port **e1ds1ll**: E1DS1 leased line port **xdsl**: xDSL port **catv**: CATV port **ces**: CES port.
show port link-discovery *PORTS*		Shows configured link state of port.
show e1ds1 if-table local [*OLT_SLOT* [*OLT_PORT*]]	Config	Shows table of configured local E1DS1 interfaces. **OLT_SLOT**: OLT-slot of the IU_GPON (optional) **OLT_PORT**: OLT-port for E1DS1 interface (optional).
show e1ds1 if-table2 local [*OLT_SLOT* [*OLT_PORT*]]		
show e1ds1 if-table remote [*OLT_SLOT* [*GPON_PORT* [*ONU_ID* [*ONT_SLOT* [*ONT_PORT*]]]]]		Shows table of configured remote E1DS1interfaces. **OLT_SLOT**: OLT-slot of the IU_GPON (optional) **GPON_PORT**: GPON-port from the IU_GPON (optional) **ONU_ID**: the ONU-ID (optional) **ONT_SLOT**: the ONT-slot (optional) **ONT_PORT**: ONT-port of E1DS1 interface (optional).
show e1ds1 if-table2 remote [*OLT_SLOT* [*GPON_PORT* [*ONU_ID* [*ONT_SLOT* [*ONT_PORT*]]]]]		
show traffic-desc-prof table	Config	Shows traffic description profile table.

Example

Showing the state of Ethernet ports:

```
SWITCH(bridge)# show port 9/1-9/4
===============================================================
S/P TYPE ROLE PVID  LINK NEGO DUPLEX SPEED  FLOWCTRL SFP
===============================================================
9/1 ETH01 Uplk 1 Up/Up Auto Full/Full 10/10 Dis/Dis No/E1
9/2 ETH02 Uplk 1 Up/Up Auto Full/Full 1000/10 Dis/Dis No/E1
9/3 ETH03 Uplk 1 Up/Up Down Full/Full 100/10 Dis/Dis No/E1
9/4 ETH04 Uplk 1 Up/Up Down Full/Full 10/10 Dis/Dis No/E1
SWITCH(bridge)#
```

The information provided in Table 20 can be verified using the **show port** command.

Parameter	Description
TYPE	Shows type of port,

Table 20 Information displayed by Show Port Command

Parameter	Description
PVID	Shows port VLAN-ID.
STATUS	Shows status of port. ADMIN is up/down status by user's configuration and OPER is the real connection status of the GPON.
MODE	Shows the status for the rate of the port, Duplex mode, auto-nego
NEGO	Shows the auto-negotiation configuration of the port.
DUP	Shows the transmit rate of Ethernet port.
SPEED	shows the full duplex mode of the port,
FLOWCTRL	Shows flow control of port,
ROLE	Shows the configured role of the port.

Table 20 Information displayed by Show Port Command (Cont.)

Command	Mode	Function
show ponpptp olt { table | list} [*ADDRESS*]	Config	Displays information of PON interface on OLT **table**: table with config data **list**: list, **ADDRESS**: OLT-slot[/GPON-port].
show ponpptp ont { table | list} [*ADDRESS*]	Config	Displays information of PON interface on ONT/ONU. **table**: table with config data **list**: list **ADDRESS**: OLT-slot[/GPON-port[/ONU-ID]].

10.9 Port Statistics

10.9.1 Checking Port Statistics

In order to display traffic average of each port or interface MIB, use the following commands.

Command	Mode	Function
show port statistics avg-pkt { *PORTS* | all }	Bridge	Shows average packets statistic counters of specified port. **PORTS**: port number OLT-slot/OLT-port **all**: show all ports.
show port statistics interface { *PORTS* | rcu }	Privileged/ Config/ Bridge	Shows MIB data of specified port. **PORTS**: port number OLT-slot/OLT-port **rcu**: redundant central unit.
show port statistics ethernet [*PORTS*]		Shows Ethernet statistic counters of specified port.
show port statistics dot3 { *PORTS* | all }		Shows DOT3 statistic counters of specified port.
show port state mirror *PORTS*		Shows state information of mirrored port.
show port { gpon | eth | pots | e1ds1ll | voip | xdsl | catv | ces } *PORTS* **statistics interface**		Shows port statistic. **gpon**: GPON port **eth**: Ethernet port **pots**: POTS port **e1ds1ll**: E1DS1 leased line port **voip**: VoIP interface **xdsl**: xDSL port **catv**: CATV port.

Example:

Viewing interface MIB data.

```
SWITCH(bridge)#show port statistics interface 9/1
  ifIndex                    4
  ifDescr                    Siemens-hiX5750-CCXUVR:1O:4E:E
  ifType                     6
  ifMtu                      1500
  ifSpeed                    0
  ifPhysAddress              08:00:06:26:1a:6d
  ifAdminStatus              UP
  ifOperStatus               DOWN
  ifLastChange               0
  ifInOctets                 0
  ifInUcastPkts              0
  ifInDiscards               0
  ifInErrors                 0
  ifInUnknownProtos          0
  ifOutOctets                0
  ifOutUcastPkts             0
  ifOutDiscards              0
  ifOutErrors                0
  ifName                     eth4
  ifInMulticastPkts          0
  ifInBroadcastPkts          0
  ifOutMulticastPkts         0
  ifOutBroadcastPkts         0
  ifHCInOctets               0
  ifHCInUcastPkts            0
  ifHCInMulticastPkts        0
  ifHCInBroadcastPkts        0
  ifHCOutOctets              0
  ifHCOutUcastPkts           0
  ifHCOutMulticastPkts       0
  ifHCOutBroadcastPkts       0
  ifLinkUpDownTrapEnable     1
  ifHighSpeed                0
  ifPromiscuousMode          2
  ifConnectorPresent         1
  ifAlias
  ifCounterDiscontinuityTime 0
SWITCH(bridge)#
```

10.9.2 Clearing Port Statistics

Use the following commands to clear all recorded statistics of port.

Command	Mode	Function
clear port statistics interface { *PORTS* I all }	Bridge	Clears all recorded port statistics: **PORTS**: port number OLT-slot/OLT-port **all**: clears all information.
clear port statistics dot3 [*PORTS*]		Clears all recorded port statistics.
clear port statistics ethernet [*PORTS*]		Clears specified or all recorded port statistics.
clear port statistics avg-pkt [*PORTS*]		Clears specified or all recorded port statistics.

10.10 Performance Monitoring

Use the commands that are described in the following chapters to configure PM objects for **ANI** services. There are GTC PM managed entities related to **GEM** port, GAL Ethernet, ONU, **T-CONT**, and PonPptp.

10.10.1 Configuring the Threshold Profiles

This profile contains threshold values for the performance monitoring parameters. A default profile with index 1 always exist.

Command	Mode	Function
create threshold-profile-wi *GALETHDISCFRAMES GEMLOSTPACKETS GEMMISINSPACKETS GEMIMPAIREDBLOCKS* <0-15>	Config	Creates a threshold profile with index. **GALETHDISCFRAMES**: threshold GAL Ethernet disc frames **GEMLOSTPACKETS**: threshold GEM lost packets **GEMMISINSPACKETS**: threshold GEM miss inserted packets **GEMIMPAIREDBLOCKS**: threshold GEM impaired blocks **0 - 15**: profile index.
modify threshold-profile <2-16> *GALETHDISCFRAMES GEMLOSTPACKETS GEMMISINSPACKETS GEMIMPAIREDBLOCKS*		Modifies a threshold profile. **2 - 16**: profile index
delete threshold-profile <2-16>		Deletes a threshold profile. **2 - 16**: profile index.

10.10.2 Calculation Algorithms for PM Objects

The algorithms to calculate valid PM objects are the following:

- **GAL Ethernet Index:**
  slot * 0x08000000 +
  port * 0x00800000 +
  onuId * 0x00008000 +
  onuSlot * 0x00000400 +
  onuPort * 0x00000008 + gemPortPrio-ID
- **GEM Port Index:**
  slot * 0x08000000 +
  port * 0x00800000 +
  onuId * 0x00008000 +
  onuSlot * 0x00000400 +
  onuPort * 0x00000008 + gemPortPrio-ID
- **T-CONT Index:**
  slot * 0x80000 +

port * 0x08000 +
onuId * 0x00080 + serviceClass
Service classes are:0 = tdm1 = voip3 = data-be4 = data-nrt5 = data-rt

- **PON PPTP Index:**
  slot * 100 + port
- **Interface Index:**
  IfIndex = ((OltSlot - 1) * 10240000) + ((OltPort - 1) * 2560000) + ((OnuId + 1) * 10000) + (OntSlot * 100) + OntPort
- **Physical Index MDU Service Board (SB):**
  Left shelf side:
  SB-CARD: Slot * 2^17 + Port * 2^13 + OnuId * 2^5 + OnuCard * 2 + 1
  Right shelf side:
  SB-CARD: (Slot - 2) * 2^17 + Port * 2^13 + OnuId * 2^5 + OnuCard * 2 + 1
- **ONU Physical Port:**
  Left shelf side:
  ONU: Slot * 2^17 + Port * 2^13 + OnuId * 2^5 + 1
  MDU: Slot * 2^17 + Port * 2^13 + OnuId * 2^5
  Right shelf side:
  ONU: (Slot - 2) * 2^17 + Port * 2^13 + OnuId * 2^5 + 1
  MDU: (Slot - 2) * 2^17 + Port * 2^13 + OnuId * 2^5

10.10.3 Configuring of PM Objects

Command	Mode	Function
create pm-object <1-6> <1-4294967295> <1-3> <1-96> <1-16>	Config	Creates a PM object. **1 - 6**: type of PM object (1=GEM port, 2=not used, 3=GAL Ethernet, 4=ONU, 5=T-CONT, 6=PonPptp) **1 - 4294967295**: type index of PM object (GEM Port/GAL-Ethernet - GEM port index; ONU - phys. index; TCONT - TCont Index; PON-Pptp - Interface index) **1 - 3**: endpoint of PM object (1-ONT; 2-OLT; 3-no endpoint) If the PM data are collected for the managed entities GEM port, GAL Ethernet, this attribute is used to select between monitoring points that are located at ONT or OLT. If the PM data are collected for the managed entities ONU, T-CONT or PonPptp, this attribute is don't care. **1 - 96**: history entry size The default value is 1 and means at least one history entry is desired. In case of PM object creation the number of 15 min. entries is set and the number of 24 h entries is always 1. **1 - 16**: index of threshold profile.
create pm-object { gem-port | gal-ethernet | onu | tcont | ponpptp } <1-4294967295> { olt | ont | no } <1-96> <1-16>		Creates a PM object of specified type, **gem-port**: 1-GEM Port **gal-ethernet**: 3-GAL Ethernet **onu**: 4-ONU **tcont**: 5- TCONT **ponpptp**: 6-PON Pptp **1 - 4294967295**: type index of PM object (GEM Port/GAL-Ethernet - GEM port index; ONU - phys. index; TCONT - TCont Index; PON-Pptp - Interface index) **olt**: endpoint of PM object is the OLT **ont**: endpoint of PM object is ONT **no**: no endpoint **1 - 96**: history entry size **1 - 16**: index of threshold profile.
delete pm-object <1-1024>		Deletes a PM object. **1 - 1024**: index of the PM object.
modify pm-object <1-1024> {1 | 2 } <1-96> <1-16>		Modifies a PM object. **1 - 1024**: index of the PM object **1 | 2**: interval type (15 min./24 h) **1 - 96**: history entry size **1 - 16**: index of threshold profile.
change adminstate pm-object <1-1024> { 1 | 2 } *ADMIN_STATE*	Config	Used to activate and deactivate performance monitoring for both interval types of the PM object. **1 - 1024**: index of the PM object **1 | 2**: interval type (15 min./24 h) **ADMIN_STATE**: 0 locked,1 active.

10.10.4 Displaying the PM Data

Command	Mode	Function
show gpon-pm table	Config	Shows the whole GPON PM table.
show gpon-pm table-list	Exec/ Config	Shows the whole GPON PM table in list format (Overview).
show gpon-pm remaining-history-entries	Config	Shows the number of remaining history entries.

Command	Mode	Function
show tcont pm-data <1-1024>	Config/ Bridge	Shows list of PM data for TCONT. **1 - 1024**: PM object index.
show tcont pm-object-list		Displays all T-CONT PM objects.
show gemport pm-data <1-1024>	Config/ Bridge	Shows GPON encapsulation method port. pm-data: list PM data for gemport **1 - 1024**: PM object index.
show gemport pm-object-list [<1-1024> [<1-1024>]]		Shows GPON encapsulation method port. pm-object-list: list PM objects **1 - 1024**: start index for searching, shows all if left blank **1 - 1024**: end index for searching, shows only the first if left blank.
show gal-eth pm-data <1-1024>	Config/ Bridge	Shows GPON adaption layer Ethernet. pm-data: shows **PM** data for gal-eth (gemport) **1 - 1024**: PM object index.
show gal-eth pm-object-list [<1-1024> [<1-1024>]]		Shows GPON adaption layer Ethernet. pm-object-list: list PM objects **1 - 1024**: start index for searching, shows all if left blank **1 - 1024**: end index for searching, shows only the first if left blank.
show ponpptp pm-data <1-1024>	Config	Show PM data for PON PPTP, **1 - 1024**: PM object index.
show ponpptp pm-object-list	Config	Show all PON PPTP PM objects.
show onu pm_records [<1-1024>]	Config	Displays the ONU PM record table. **1 - 1024**: PM object index.

10.11 Payload-Counters

Payload-counters allow the operator to have a differentiated view on the current status of Ethernet traffic on the optical link between IU_GPON and **ONU** in upstream and downstream direction. Several counters can be set in the configuration that count the number of payload bytes of a specific traffic flow up to a total of 2^{64}.

10.11.1 Configuring of Payload-Counter

In order to prepare payload-counters in the configuration, the following steps are required:

1. Loading the Configuration
2. Modifying the configuration as described in the sections
   - Assigning the User Ports to Counter Group
   - Assigning of Multicast/Broadcast Traffic to Counter Group
   - Mapping VLAN to Counter
3. Activating the Configuration with Payload-Counters.

10.11.1.1 Loading the Configuration

Before a command that configure the payload-counters for a particular traffic flow through the GPON link can be executed, the configuration needs to be loaded from CXU’s persistent memory. When the configuration is loaded for the first time, the groups of counters are not assigned (default). Consecutively, the last activated configuration is available.

Command	Mode	Function
modify payload-counter *ADDRESS* **config load**	Config	Loads the configuration from background. Necessary before all further payload-counter configurations. **ADDRESS**: IU_GPON port (OLT-slot/GPON-port).

Example

```
SWITCH(config)# modify payload-counter 2/1 config load
SWITCH(config)# show payload-counter config

config for pon link 2/1 is available

PAYLOAD-COUNTER VLAN TABLE

counter# |  vlan
---------+--------
       1 |   none
       2 |   none
       3 |   none
       4 |   none
       5 |   none
       6 |   none
       7 |   none
       8 |   none


PAYLOAD-COUNTER MULTICAST CONFIGURATION

counter group    :     none
vlan mapping bit :  invalid


PAYLOAD-COUNTER UNICAST CONFIGURATION

           |  interface    || counter  |  vlan
    type   |   address     ||  group   | mapping
-----------+---------------++----------+--------
  ethernet | 2/ 1/20/ 1/ 1 ||     none | invalid
  ethernet | 2/ 1/20/ 1/ 2 ||     none | invalid
  ethernet | 2/ 1/20/ 1/ 3 ||     none | invalid
  ethernet | 2/ 1/20/ 1/ 4 ||     none | invalid
      VoIP | 2/ 1/20/ 1/ 1 ||     none | invalid
      VoIP | 2/ 1/20/ 5/ 1 ||     none | invalid
      VoIP | 2/ 1/24/ 2/ 1 ||     none | invalid
  ethernet | 2/ 1/24/ 4/ 1 ||     none | invalid
  ethernet | 2/ 1/24/ 4/ 2 ||     none | invalid
  ethernet | 2/ 1/24/ 4/ 3 ||     none | invalid
  ethernet | 2/ 1/24/ 4/ 4 ||     none | invalid
      VoIP | 2/ 1/24/ 4/ 1 ||     none | invalid
```

```
PAYLOAD-COUNTER NAMES

1   ""
2   ""
3   ""
4   ""

...
64 ""
```

10.11.1.2 Naming of Counter Groups

Each counter group can be marked with a specific name. Use the following command to configure names for counter groups. Changes made by this command take effect immediately, i.e. without the necessity of activation and they remain valid independently of executing a **config load** command.

Command	Mode	Function
modify payload-counter *ADDRESS* **set config-name** <1-64> [*LINE*]	Config	Configures name for specified counter group. **ADDRESS**: OLT-slot/GPON-port as specified with **config load** command **1 - 64** : counter group **LINE**: name for counter group (max. 24 characters) Use this command without LINE option to delete the name of specified counter group.

Example:

Setting the name of counter group number 4 to “name with spaces   “ (24 characters including spaces)

```
SWITCH(config)# modify payload-counter 2/1 set counter-name 4
test with spaces
SWITCH(config)# show payload-counter config names
PAYLOAD-COUNTER NAMES

1   ""
2   "nsn 2"
3   "nsn 3"
4   "name with spaces        "
5   ""

...
63  "nsn63"
64  ""
```

10.11.1.3 Assigning the User Ports to Counter Group

Use the following set of commands in order to modify the configuration so that counter groups are assigned to unicast traffic flows on the path between IU_GPON port and **UNI** port. Each of up to 64 counter groups consist of 8 counters for downstream respectively upstream. One counter group may be assigned to one or more UNI ports. The number of bytes through the addressed ports is counted in the dedicated group.

Note the following remarks for the usage of **set** and **clear** commands:

- The sequence of entering the commands decides about the operative configuration. This means that the last executed command overwrites settings of the previous one (e.g. **uc** command after **onu** command and vice versa). Hence, in this case there is no necessity to enter a **clear** command between.
- All configuration changes caused by these commands are only temporary as long as the **activate** command is not executed.
- VLANFLAG has to be considered only if the **OLT** runs in “enhanced **MAC** mode” for **VLAN** operation, see 13.1 Setting the GPON MAC Mode.
- OLTADDRESS must be the same IU_GPON port that was specified in ADDRESS of **config load** command.
- The **clear** commands cancel for the addressed ports the assignment of counter groups. This is the default status that will be reported as “none”.

Command	Mode	Function
modify payload-counter *OLTADDRESS* **set interface** { ces I eth I voip I xdsl } *ADDRESS* <1-64> <0-1>	Config	Modifies the configuration for counting unicast bytes via one ONU port of specified interface type. **OLTADDRESS**: OLT-slot/GPON-port **eth, voip, xdsl, ces**: type of interface can be eth, voip, xdsl, ces (Circuit Emulation Services - whole Ethernet traffic encapsulating ONU’s TDM traffic of unstructured least lines **E1** or **DS1**) **ADDRESS**: address from UNI port (OLT-slot/GPON-port/ONU-ID/ONU-slot/ONU-port) **1 - 64** : counter group **0 - 1**: flag controls whether the used counter depends on VLAN or not, see 10.11.1.5 Mapping VLAN to Counter. 1: true - count VLAN traffic enable 0: false - count VLAN traffic disable.
modify payload-counter *OLTADDRESS* **set onu-card** *ADDRESS* <1-64> <0-1>		Modifies the configuration for counting unicast bytes via all ports of specified ONU-card. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.
modify payload-counter *OLTADDRESS* **set onu** *ADDRESS* <1-64> <0-1>		Modifies the configuration for counting unicast bytes via all ports of specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID
modify payload-counter *OLTADDRESS* **set uc** <1-64> <0-1>		Modifies the configuration for counting unicast bytes via all USED/CONFIGURED interfaces of loaded GPON link.

Use the following commands to clear the payload-counters associated with the **UNI** ports.

Command	Mode	Function
modify payload-counter *OLTADDRESS* **clear interface** { ces I eth I voip I xdsl } *ADDRESS*	Config	Clears the configuration for one ONU port of specified interface type. **OLTADDRESS**: OLT-slot/GPON-port **eth, voip, xdsl, ces**: type of interface **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot/ ONU-port.
modify payload-counter *OLTADDRESS* **clear onu-card** *ADDRESS*		Clears the configuration for all ports of specified ONU-card. **ADDRESS**: OLT-slot/GPON-port/ONU-ID/ONU-slot.
modify payload-counter *OLTADDRESS* **clear onu** *ADDRESS*		Clears the configuration for all ports of specified ONU. **ADDRESS**: OLT-slot/GPON-port/ONU-ID.
modify payload-counter *OLTADDRESS* **clear uc**		Clears the configuration for all USED/CONFIGURED unicast interfaces.

Example

```
SWITCH(config)# modify payload-counter 2/1 set interface eth
2/1/24/4/3 13 1
SWITCH(config)# show payload-counter config uc
PAYLOAD-COUNTER UNICAST CONFIGURATION

            |   interface    || counter |   vlan
    type    |   address      ||  group  | mapping
------------+----------------++---------+--------
   ethernet |  2/ 1/20/ 1/ 1 ||      52 | invalid
   ethernet |  2/ 1/20/ 1/ 2 ||      52 | invalid
   ethernet |  2/ 1/20/ 1/ 3 ||      52 | invalid
   ethernet |  2/ 1/20/ 1/ 4 ||      52 | invalid
       VoIP |  2/ 1/20/ 1/ 1 ||      52 | invalid
       VoIP |  2/ 1/20/ 5/ 1 ||    none | invalid
       VoIP |  2/ 1/24/ 2/ 1 ||      11 |   valid
   ethernet |  2/ 1/24/ 4/ 1 ||    none | invalid
   ethernet |  2/ 1/24/ 4/ 2 ||    none | invalid
   ethernet |  2/ 1/24/ 4/ 3 ||      13 |   valid
   ethernet |  2/ 1/24/ 4/ 4 ||    none | invalid
       VoIP |  2/ 1/24/ 4/ 1 ||    none | invalid
```

10.11.1.4 Assigning of Multicast/Broadcast Traffic to Counter Group

Use the following commands to configure payload-counters for MC /BC traffic flow through the GPON link.

Command	Mode	Function
modify payload-counter *OLTADDRESS* **set mc** <1-64> <0-1>	Config	Modifies the configuration for counting multicast bytes. **OLTADDRESS**: OLT-slot/GPON-port **1 - 64** : counter group **0 - 1**: flag controls whether the used counter depends on VLAN or not, see 10.11.1.5 Mapping VLAN to Counter 1: true - count VLAN traffic enable 0: false - count VLAN traffic disable.
modify payload-counter *OLTADDRESS* **clear mc**		Clears the configuration for counting multicast bytes.

Example

```
SWITCH(config)# modify payload-counter 2/1 set mc 23 1
SWITCH(config)# show payload-counter config mc
PAYLOAD-COUNTER MULTICAST CONFIGURATION

counter group    :       23
vlan mapping bit :    valid

SWITCH(config)# modify payload-counter 2/1 clear mc
SWITCH(config)# show payload-counter config mc
PAYLOAD-COUNTER MULTICAST CONFIGURATION

counter group    :     none
vlan mapping bit :  invalid
```

10.11.1.5 Mapping VLAN to Counter

The following requirements must be fulfilled in order to use counters for a certain **VLAN** traffic:

1. The “enhanced **MAC** mode” is set for OLT’s VLAN operation
2. VLANFLAG is set true for the addressed ports.

In case of former “MAC mode” and “**VID** mode”, or if the VLANFLAG is set to false, the whole interface traffic will be always counted in the first counter of group.

Note that the configured relation between VLAN and counter is valid for all counter groups of the chosen GPON link.

Use the following commands to allocate payload-counters for VLAN related services.

Command	Mode	Function
modify payload-counter *OLTADDRESS* **set vlan** <1-8> <1-4094>	Config	Modifies the configuration for counter assigned to VLAN. **OLTADDRESS**: OLT-slot/GPON-port **1 - 8**: counter in group **1 - 4094**: VLAN-ID.
modify payload-counter *OLTADDRESS* **clear vlan** <1-8>		Clears the assignment of counter to VLANs.

Example

```
SWITCH(config)# modify payload-counter 2/1 set vlan 1 100
SWITCH(config)# modify payload-counter 2/1 set vlan 2 300
SWITCH(config)# modify payload-counter 2/1 set vlan 3 400
SWITCH(config)# modify payload-counter 2/1 set vlan 4 600
SWITCH(config)# modify payload-counter 2/1 set vlan 5 800
SWITCH(config)# modify payload-counter 2/1 set vlan 7 1000
SWITCH(config)# show payload-counter config vlan
PAYLOAD-COUNTER VLAN TABLE

 counter# |  vlan
----------+--------
        1 |    100
        2 |    300
        3 |    400
        4 |    600
        5 |    800
        6 |   none
        7 |   1000
        8 |   none

SWITCH(config)# modify payload-counter 2/1 clear vlan 7
SWITCH(config)# show payload-counter config vlan
PAYLOAD-COUNTER VLAN TABLE

 counter# |  vlan
----------+--------
        1 |    100
        2 |    300
        3 |    400
        4 |    600
        5 |    800
        6 |   none
        7 |   none
        8 |   none
```

10.11.1.6 Activating the Configuration with Payload-Counters

When all required **set** and **clear** commands were entered, there is the necessity to activate the new configuration for following reasons:

- In order that the modified configuration can be restored after the active CXU or the IU_GPON have been rebooted, it must be stored back into CXU's persistent memory. Otherwise, all made changes will be lost.
- Without activation, the counter settings will be overwritten when a new temporary configuration (for another GPON link or same as before) is loaded from background.
- If the **config load** command is executed the next time, then the new configuration will be loaded.

Use the following command to activate the new configuration.

ℹ On active IU_GPON, the counting starts immediately from zero.

Command	Mode	Function
modify payload-counter *ADDRESS* **config activate**	Config	Activates the new configuration. The CXU sets the new configuration on IU_GPON. **ADDRESS**: OLT-slot/GPON-port.

Example

```
SWITCH(config)# modify payload-counter 2/1 config activate
SWITCH(config)# show payload-counter config

config for pon link 2/1 is available

PAYLOAD-COUNTER VLAN TABLE

 counter# |  vlan
----------+--------
        1 |    100
        2 |    300
        3 |    400
        4 |    600
        5 |    800
        6 |   none
        7 |   none
        8 |   none

PAYLOAD-COUNTER MULTICAST CONFIGURATION

counter group    :       23
vlan mapping bit :    valid

PAYLOAD-COUNTER UNICAST CONFIGURATION
```

```
            |    interface    || counter |    vlan
    type    |     address     ||  group  | mapping
------------+-----------------++---------+---------+--------
   ethernet |  2/ 1/20/ 1/ 1 ||      63 | invalid
   ethernet |  2/ 1/20/ 1/ 2 ||      63 | invalid
   ethernet |  2/ 1/20/ 1/ 3 ||      63 | invalid
   ethernet |  2/ 1/20/ 1/ 4 ||      63 | invalid
       VoIP |  2/ 1/20/ 1/ 1 ||      63 | invalid
       VoIP |  2/ 1/20/ 5/ 1 ||      63 | invalid
       VoIP |  2/ 1/24/ 2/ 1 ||       2 |   valid
   ethernet |  2/ 1/24/ 4/ 1 ||    none | invalid
   ethernet |  2/ 1/24/ 4/ 2 ||    none | invalid
   ethernet |  2/ 1/24/ 4/ 3 ||      12 |   valid
   ethernet |  2/ 1/24/ 4/ 4 ||    none | invalid
       VoIP |  2/ 1/24/ 4/ 1 ||    none | invalid
```

PAYLOAD-COUNTER NAMES

1 ""
2 "nsn 2"

...
63 "nsn63"
64 ""

10.11.1.7 Checking the Configuration

Use the following command to verify the payload-counters of loaded configuration.

Command	Mode	Function
show payload-counter config [names | ponlink | vlan | mc | uc [*ADDRESS*]]	Config	Shows specified of all payload-counter information. **names**: names of counter groups **ponlink**: currently loaded GPON link **vlan**: assignment of VLANs to the counter of groups **mc**: counter group for multicast/broadcast traffic and the VLAN flag **uc**: assignment of counter groups to user ports and the corresponding VLAN flags **ADDRESS**: limits the shown user ports as specified by slot/port/ONU-ID[/ONU-slot].

10.11.2 Checking the Payload-Counter Values

Perform the following tasks in order to get information about the status of payload-counters:

1. Getting and Resetting the Payload-Counter Values
2. Displaying the Counter Values.

payload-counter values will be not saved in the history. This means:

- During operation, only such data, which were released by the last executed **get** command, can be displayed.
- Rebooting the active CXU causes the loss of counters.

10.11.2.1 Getting and Resetting the Payload-Counter Values

Data may get from all counters or from a particular counter, with or without resetting the counters, by using the following commands.

Note that **reset** commands are executed without displaying any information.

Command	Mode	Function
modify payload-counter get single *ADDRESS* <1-64> <1-8> <0-1>	Config	Gets the value from ONE counter. **ADDRESS**: slot/port **1 - 64** : counter group **1 - 8**: counter in group **0 -1**: flag controls whether counters are reset after the data have been got or not 1: true - reset counter 0: false - no reset.
modify payload-counter reset single *ADDRESS* <1-64> <1-8>		Resets the current counter value to ZERO.
modify payload-counter get all *ADDRESS* <0-1>	Config	Gets all counter values from specified GPON link.
modify payload-counter reset all *ADDRESS*		Resets all current counter values from GPON link to ZERO.

Examples

Get counter 4 of group 2 without reset:

```
SWITCH(config)# modify payload-counter get single 2/1 2 4 0
SWITCH(config)# show payload-counter counter single
single PAYLOAD COUNTER
ponlink 2/1
counter group 2 "nsn 2"
counter 4

time of request : 2008-06-09 11:10:30
upstream  :                      0
downstream:                      0
```

Reset counter 4 of group 2:

```
SWITCH(config)# modify payload-counter reset single 2/1 2 4
```

Reset of all counter on GPON link 2/1:

```
SWITCH(config)# modify payload-counter reset all 2/1
```

10.11.2.2 Displaying the Counter Values

After executing the last **get** command, use the following commands to display the counter information.

Note the following remarks:

- Not assigned counter groups are marked as UNUSED.
- Counters without assigned VLAN are not displayed
- For each used counter group, the total is displayed.

Command	Mode	Function
show payload-counter counter ponlink [<1-64> [<1-64>]]	Config	Shows information for all or specified counter groups from last "get all" request. **1 - 64**: counter group - start-index group1 for show **1 - 64**: counter group - end-index group2 for show -- show only group1 if goup2 is left blank.
show payload-counter counter single		Shows the counter information from last "get single" request.

Examples

The following examples illustrates the reports for the case that the OLT runs in enhanced MAC mode.

1. Displaying of all counter groups which were got and reset:

```
SWITCH(config)# modify payload-counter get all 2/1 1
SWITCH(config)# show payload-counter counter ponlink

PAYLOAD COUNTER for ponlink 2/1

time of last request: 2008-06-09 11:09:15
group | # |   vlan   ||      upstream         |     downstream
================================================================
1       ""
      |   |  UNUSED  ||
------|---|----------||-----------------------|----------------
2       "nsn 2"
      | 1 | all/ 100 ||                     0 |               0
      | 2 |      300 ||                     0 |               0
      | 3 |      400 ||                     0 |               0
      | 4 |      600 ||                     0 |               0
      | 5 |      800 ||                     0 |               0
------|---|----------||-----------------------|----------------

      |   |   S U M  ||                     0 |               0

------|---|----------||-----------------------|----------------
3       "nsn 3"
      |   |  UNUSED  ||
------|---|----------||-----------------------|----------------
4       "name with spaces        "
      |   |  UNUSED  ||
------|---|----------||-----------------------|----------------

...

------|---|----------||-----------------------|----------------
62      ""
      |   |  UNUSED  ||
------|---|----------||-----------------------|----------------
63      "nsn63"
```

```
      | 1 | all/ 100 ||                     0 |               0
      | 2 |      300 ||                     0 |               0
      | 3 |      400 ||                     0 |               0
      | 4 |      600 ||                     0 |               0
      | 5 |      800 ||                     0 |               0

      |   |   S U M  ||                     0 |               0

------|---|----------||-----------------------|----------------
64      ""
      |   |  UNUSED  ||
------|---|----------||-----------------------|----------------
```

2. Displaying of the used payload-counters of single counter group #32:

```
SWITCH(config)# show payload-counter counter ponlink 32
PAYLOAD COUNTER for ponlink 2/1

time of last request: 2008-06-09 11:09:15
group | # |  vlan    ||       upstream        |      downstream
===============================================================
32      ""
------|---|----------||-----------------------|----------------
      | 1 | all/ 100 ||                     0 |               0
      | 2 |      300 ||                     0 |               0
      | 3 |      400 ||                     0 |               0
      | 4 |      600 ||                     0 |               0
      | 5 |      800 ||                     0 |               0

      |   |   S U M  ||                     0 |               0
```

3. Displaying of the payload-counter #1 of group #63

```
SWITCH(config)# modify payload-counter get single 2/1 63 1 0
SWITCH(config)# show payload-counter counter single
single PAYLOAD COUNTER
ponlink 2/1
counter group 63 "nsn63"
counter 1
time of request : 2008-06-09 11:11:03
upstream  :                      0
downstream:                      0
```

11 XDSL

This chapter contains all needed information for line configuration, line supervision, and performance data for **ADSL**2+ and **VDSL**2 interfaces. In the hiX 5750 R2.0, xDSL functionality is provided by the hiX 5709 **MDU** which supports VDSL2 and ADSL2+ standards via service boards. In order to configure the xDSL services following steps are necessary:

1. Configuring of XDSL profiles
    - Line Profiles
    - Channel Profile
    - Notch Profile
    - PSD Mask Profiles
    - Alarm Profile
2. Configuring of LRE-Port
3. DELT Configuration.

Note the following hints and conditions of application before starting ADSL configuration:

- 1 : 1 relation between **VCC** and bridge port
- 1 to 8 VCC, bridge ports per physical port
- 1 to 2 channels per physical port possible
- By default exist 1 channel, 1 VCC, bridge port per physical port
- VCC can be assigned to any channel
- Additional channel can be created/deleted by operator (switch between single and dual latency)
- Before deleting a channel the assigned VCCs/bridge ports must be deleted or assigned to another channel (no unassigned VCC with invalid used channel possible)
- Additional VCCs and bridge ports can be created/deleted by operator (no automatic creation or deletion with channel)
- To switch the configuration from ADSL2+ to VDSL2, not more than 1 VCC/bridge port must be assigned to each channel. Additional VCC/bridge ports must be deleted by the operator before.

11.1 Line Profiles

This profile includes common attributes describing both ends of the line. It is required for all physical xDSL interfaces.

ℹ This characters are not allowed for profilename (size 1..32): space : ? , leading integer.

11.1.1 Creating/Deleting a Profile

Command	Mode	Function
xdsl add line-config-profile *PROFILE*	Bridge	Creates xDSL line-config profile. **PROFILE**: enter the profile name.
xdsl delete line-config-profile *PROFILE*		Deletes xDSL line-config profile.

Command	Mode	Function
xdsl duplicate line-config-profile *SOURCE-PROFILE NEW-PROFILE*	Bridge	Copies a line profile. **SOURCE-PROFILE**: name of origin line profile. **NEW-PROFILE**: name of new line profile.

11.1.2 Configuration

The commands configuring the line profile are contained in the sections:

- VDSL2 Profile, GS Standard, Bandplan
- Line Type
- Rate Mode, RX Power, Max. Aggregate Power
- Max. nominal PSD, Bit-Swapping, Subcarrier Mask
- SNR Magin Values
- Power Back-off (PBO)
- Power Managment
- Loop Length and Burst Mode.

ℹ Before parameters of line profile can be modified, the port has to be in locked state.

ℹ Preconditions for profile modification are:

- The profile should not be in use by active ports.
- A modification of VDSL2 profile number, in a way that it causes new subcarrier spacing is not allowed for profiles, which are assigned to a VDSL2 line.
- A modification of GS standard, in a way that it causes a new DSL standard (VDSL2 -> ADSL2+ or back) is not allowed for profiles, which are assigned to a DSL line.
- The activation of ADSL2+ and VDSL2 standard's inside one profile is not allowed.

VDSL2 Profile, GS Standard, Bandplan

A clear target of the VDSL2 standard was to adopt a single line code in cooperation with established DSL standardization bodies. Therefore, VDSL2 is based on both the VDSL1 and ADSL2/ADSL2+ recommendations. It is spectrally compatible with existing services and enables multimode operability with ADSL2 and ADSL2+. The hiX 5750 R2.0 uses VDSL2 configuration profiles and bandplans to meet regional service provider requirements. VDSL2 also defines asymmetric (Plan 998) and symmetric (Plan 997) bandplans for the
transmission in upstream and downstream direction. As in ADSL, the lower part of the spectra is allocated for POTS and ISDN service and a splitter is used to separate such frequencies from the VDSL2 band. Annex A specifies bandplans for the North American region and enables VDSL2 to be deployed with POTS service. Annex B specifies bandplans for Europe and enables VDSL2 deployment with underlying POTS and ISDN services. Annex C describes VDSL2 found primarily in Japan.

ℹ A mix of enabled VDSL and ADSL standards, or ADSL POTS and ISDN standards will be rejected by the NE.

ℹ **Refer to the current release notes for information about supported xDSL bandplans and profiles. Note that the possibility of settings can change with new firmware updates for the DSL chipset.**

The HiX 5709-003 MDU is prepared to provide via its xDSL service boards the following bandplans and profiles:

- Profiles: 8b, 12a, 17a + US0 (17b), 30a (SB_xDSL12 only)
- Band plan: 998
- VDSL2 over ISDN - PSD:
  - B8-6/998-M2x-B
  - B8-8/998E17-M2x-NUS0
  - B8-12/998ADE17-M2x-B
  - B8-15/998ADE30-M2x-NUS0-M
- VDSL2 over POTS - PSD:
  - B8-4/998-M2x-A
  - B8-11/998ADE17-M2x-A

Command	Mode	Function
xdsl line-config-profile *PROFILE* **use-profile-number** { profile8a | *profile8b* | profile8c | profile8d | *profile12a* | profile12b | *profile17a* | *profile17b* | *profile30a* }	Bridge	Selects VDSL2 profile which should be used for basic parameter configuration on xDSL line. **PROFILE**: enter the profile name. **profile8a**: 8A (8.8 MHz bandwidth, 2048 tones, 17.5 dBm line power) **profile8b**: 8B (8.8 MHz bandwidth, 2048 tones, 20.5 dBm line power) **profile8c**: 8C (8.5 MHz Bandwidth, 1972 Tones, 11.5 dBm Line Power) **profile8d**: 8D (8.8 MHz bandwidth, 2048 tones, 14.5 dBm line power) **profile12a**: 12A (12 MHz bandwidth, 2783 tones, 14.5 dBm line power) **profile12b**: 12B (12 MHz bandwidth, 2783 tones, 14.5 dBm line power) **profile17a**: 17A (17 MHz bandwidth, 4096 tones, 14.5 dBm line power) **profile17b**: 17A + US0 **profile30a**: 30A (30 MHz bandwidth, 3479 tones, 14.5 dBm line power)
xdsl line-config-profile *PROFILE* **profile-gs-standard** { ansi-t1-413 | adsl-pots | adsl-isdn | adsl2-pots | adsl2-isdn | reach-ext-adsl2-pots-m1| reach-ext-adsl2-pots-m2 | ext-up-adsl2-pots | adsl2plus-pots | adsl2plus-isdn | ext-up-adsl2plus-pots | vdsl2-region-a | vdsl2-region-b | vdsl2-region-c }	Bridge	Configures the used standard compliance (selects either single mode or combine all and system selects) on xDSL line. **PROFILE**: enter the profile name. **ansi-t1-413**: ANSI T1.413-1998 Standard **adsl-isdn**: G.992.1 ADSL ISDN non overlapped **adsl-pots**: G.992.1 ADSL POTS non overlapped **adsl2-pots**: G.992.3 ADSL2 POTS non overlapped **adsl2-isdn**: G.992.3 ADSL2 ISDN non overlapped **reach-ext-adsl2-pots-m1**: G.992.3 Reach Ext ADSL2 POTS non overlapped M1 **reach-ext-adsl2-pots-m2**: G.992.3 Reach Ext ADSL2 POTS non overlapped M2 **ext-up-adsl2-pots**: G.992.3 Ext Up ADSL2 POTS non overlapped **adsl2plus-pots**: G.992.5 ADSL2+ POTS non overlapped **ext-up-adsl2plus-pots**: G.992.5 Ext Up ADSL2+ POTS non overlapped **adsl2plus-isdn**: G.992.5 ADSL2+ ISDN non overlapped **vdsl2-region-a**: G.993.2 VDSL2 non overlapped Region A **vdsl2-region-b**: G.993.2 VDSL2 non overlapped Region B **vdsl2-region-c** : G.993.2 VDSL2 non overlapped Region C

Command	Mode	Function
xdsl line-config-profile *PROFILE* **band-plan-number** {itu-annexa-m1-eu32 | itu-annexa-m9-eu64 | itu-annexa-m1-adlu32 | itu-annexa-m9-adlu64 | 997-m1c-a-7 | 997-m1x-m-8 | 997-m1x-m | 997-m2x-m-8 | 997-m2x-a | 997-m2x-m | 998-m1x-a | 998-m1x-b | 998-m1x-nus0 | 998-m2x-a | 998-m2x-m | 998-m2x-m17 | 998-m2x-b | 998-m2x-b17 | 998-m2x-nus0 | 998-m2x-nus017 | itu-annexc | itu-annexc-8k | 997e30-m2x-nus0 | itu-annexc-1m1 | itu-annexc-8k-1m1 | 998e17-m2x-a | 998e17-m2x-nus0 | anfp-cal0-long | anfp-cal0-medium | anfp-cal0-short | anfp-cal0e-short | korea-fttcab | korea-fttcab-8k | hanaro-fttcab-8k | itu-annexc-fttex-a | itu-annexc-fttex-m | itu-annexc-fttcab-a | itu-annexc-fttcab-a-8k | itu-annexc-fttcab-m | itu-annexc-fttcab-m-8k | itu-annexa-m10-eu128 | annexa-m1-eu32 | annexa-m2-eu36 | annexa-m3-eu40 | annexa-m4-eu44 | annexa-m5-eu48 | annexa-m6-eu52 | annexa-m7-eu56 | annexa-m8-eu60 | annexa-m9-eu64 | annexa-eu128 | annexa-m1-adlu32 | annexa-m2-adlu36 | annexa-m3-adlu40 | annexa-m4-adlu44 | annexa-m5-adlu48 | annexa-m6-adlu52 | annexa-m7-adlu56 | annexa-m8-adlu60 | annexa-m9-adlu64 | annexa-adlu128 | annexb-997-m1c-a-7 | annexb-997-m1x-m-8 | annexb-997-m1x-m | annexb-997-m2x-m-8 | annexb-997-m2x-a | annexb-997-m2x-m | annexb-997-hpe17-m1-nus0 | annexb-997-hpe30-m1-nus0 | annexb-997-e17-m2x-nus0 | annexb-997-e30-m2x-nus0 | annexb-998-m1x-a | annexb-998-m1x-b | annexb-998-m1x-nus0 | annexb-998-m2x-a | annexb-998-m2x-m | annexb-998-m2x-b | annexb-998-m2x-nus0 | annexb-998-e17-m2x-nus0 | annexb-998-e17-m2x-nus0-m | annexb-998-ade17-m2x-nus0-m | annexb-998-ade17-m2x-a | annexb-998-ade17-m2x-b | annexb-998-e30-m2x-nus0 | annexb-998-e30-m2x-nus0-m | annexb-998-ade30-m2x-nus0-m | annexb-998-ade30-m2x-nus0-a | annexb-998-ade17-m2x-m | annexb-998-e17-m2x-a | itu-vdsl2-annexc-fttcab-a | itu-vdsl2-annexc-fttcab-m | itu-vdsl2-annexc-fttex-a | itu-vdsl2-annexc-fttex-m | itu-vdsl2-annexc-o-adsl | itu-vdsl2-annexc-o-tcmisdn | ansi-fttcab-m1 | ansi-fttcab-m2 | ansi-fttex-m1 | ansi-fttex-m2 | etsi-fttcab-pcab-m1 | etsi-fttcab-pcab-m2 | etsi-fttex-p1-m1-o-isdn | etsi-fttex-p1-m2-o-isdn | etsi-fttex-p2-m1-o-pots | etsi-fttex-p2-m2-o-pots | itu-vdsl1-annexe-e2-pcaba-m1 | hanaro-fttcab | anfp-cal0 }	Bridge	Selects the band plan number which should be used for basic parameter configuration. **PROFILE**: enter the profile name. Enter a supported band plan.

Line Type

Command	Mode	Function
xdsl line-config-profile *PROFILE* **linetype** { no-channel I fast-only I interleaved-only I fast-or-interleaved I fast-and-interleaved }	Bridge	Configures channelization of the line i.e. which channel type(s) are supported. **PROFILE**: enter the profile name. **no-channel**: no channels exist. **fast-only**: only fast channel exists. **interleaved-only**: only interleaved channel exists. **fast-or-interleaved**: either fast or interleaved channel exists (only one at a time) **fast-and-interleaved**: both fast and interleaved channels exist.

Rate Mode, RX Power, Max. Aggregate Power

Command	Mode	Function

xdsl line-config-profile *PROFILE*
{ down-rate-mode I up-rate-mode }
{ fixed I adapt-at-init I adapt-at-runtime }
	Bridge	Configures rate mode on xDSL line.
		PROFILE: enter the profile name.
		down-rate-mode: rate selection behaviour downstream
		up-rate-mode: rate selection behaviour upstream
		fixed: force to configured rate
		adapt-at-init: adapt to line quality
		adapt-to-runtime: seamless rate adapts during runtime based upon line quality

xdsl line-config-profile *PROFILE* **max-up-rx-pwr** *MAX_RCV_POWER*	Bridge	Configures max. Rx power upstream on xDSL line. **PROFILE**: enter the profile name. **MAX_RCV_POWER**: value from 0 to 25.5 dBm in steps of 0.1 dBm (default 25.5 dBm)
xdsl line-config-profile *PROFILE* { down-max-pwr I up-max-pwr } <0-255>	Bridge	Configures max. aggregate power on xDSL line. **PROFILE**: enter the profile name. **down-max-pwr**: max. aggregate downstream power **up-max-pwr**: max. aggregate upstream power **fixed**: force to configured rate **0 - 255**: value from 0 to 25.5 dBm in steps of 0.1 dBm (default 0 dBm)

Max. nominal PSD, Bit-Swapping, Subcarrier Mask

Command	Mode	Function
xdsl line-config-profile *PROFILE* { down-max-nom-psd I up-max-nom-psd } *MAX_NOM_PSD*	Bridge	Set max nominal transmit **PSD** during initialization and showtime. **PROFILE**: enter the profile name. **down-max-nom-psd**: max. nominal transmit PSD in downstream direction during initialization and showtime. **up-max-nom-psd**: max. nominal transmit PSD in upstream direction during initialization and showtime. **MAX_NOM_PSD**: Value between -600...-300 in 0.1 dBm/Hz.
xdsl line-config-profile *PROFILE* { down-bitswap I up-bitswap } { enable I disable }	Bridge	Enables/disables downstream/upstream bit swapping on xDSL line. **PROFILE**: enter the profile name.

Command	Mode	Function
xdsl line-config-profile *PROFILE* **custom-subc-mask** { upstream I downstream } [*BINSET*]	Bridge	Sets user selection for any of the 512 ADSL bins (1 bit per Bin). **PROFILE**: enter the profile name. **upstream**: upstream subcarrier mask **downstream**: downstream subcarrier mask **BINSET**: 128 values like 123456789ABCDEF (CR resets mask to 64 x FF) - only for ADSL. Depending on the used standard, only a subset of bin's will be used. Example: G992.1 (ADSL) AnnexA bin 1-32 related to US and bin 33-256 related to DS direction. G992.1 (ADSL) AnnexB bin 1-64 related to US and bin 65-256 related to DS direction. For G.992.3, G.992.4, and G.992.5, it is defined in the corresponding recommendations.
xdsl line-config-profile *PROFILE* **subcarrier-mask-use** { enable I disable }	Bridge	Enables/Disables usage of the subcarrier mask. **PROFILE**: enter the profile name.

SNR Magin Values

Command	Mode	Function
xdsl line-config-profile *PROFILE* { down-max-snr-mgn I down-min-snr-mgn I down-tgt-snr-mgn I up-max-snr-mgn I up-min-snr-mgn I up-tgt-snr-mgn } <0-310>	Bridge	Configures max./min SNR margin on xDSL line. **PROFILE**: enter the profile name. **down-max-snr-mgn**: max. downstream SNR margin **down-min-snr-mgn**: min. downstream SNR margin **down-tgt-snr-mgn**: target downstream SNR margin the tranceiver must achieve **up-max-snr-mgn**: max. upstream SNR margin **up-min-snr-mgn**: min. upstream SNR margin **up-tgt-snr-mgn**: target upstream SNR margin the tranceiver must achieve **0 - 310**: value from 0-31 dBm in steps of 0.1dBm
xdsl line-config-profile *PROFILE* { vtuc-down-snr-mgn I vtuc-up-snr-mgn I vtur-down-snr-mgn I vtur-up-snr-mgn } <0-310>	Bridge	Sets SNR margin for rate downshift/upshift on xDSL line. **PROFILE**: enter the profile name. **vtuc-down-snr-mgn:** SNR margin for rate downshift **VTU**-C(upstream) **vtuc-up-snr-mgn**: SNR margin for rate upshift VTU-C (upstream) **vtur-down-snr-mgn**: SNR margin for rate downshift VTU-R (downstream) **tur-up-snr-mgn:** SNR margin for rate upshift VTU-R (downstream)) **0 - 310**: value from 0-31 dBm in steps of 0.1dBm
xdsl line-config-profile *PROFILE* { vtuc-down-snr-time I vtuc-up-snr-time I vtur-down-snr-time I vtur-up-snr-time } <0-16383>	Bridge	Sets SNR margin the downshift/upshift min. time on xDSL line. **PROFILE**: enter the profile name. **vtuc-down-snr-time**: min. time that current margin < DownshiftSnrMgnbefore downshift **VTU**-C (upstream) occurs. **vtuc-up-snr-time**: min. time that current margin > UpshiftSnrMgnbefore upshift VTU-C (upstream) occurs. **vtur-down-snr-time**: min. time that current margin < DownshiftSnrMgnbefore downshift VTU-R (downstream) occurs. **vtur-up-snr-time**: min. time that current margin > UpshiftSnrMgnbefore upshift VTU-R (downstream) occurs. **0 - 16383**: value in seconds
xdsl line-config-profile *PROFILE* { msg-min-up I msg-min-down } <4-248>	Bridge	Configures the min. rate of message based overhead maintained by the xTU in the upstream / downstream direction **PROFILE**: enter the profile name **4 - 248**: value in kbps

Power Back-off (PBO)

To improve spectral compatibility, VDSL systems on short lines need to reduce their transmit PSDs such that the performance of other broadband systems will not be unfairly compromised. The process of reducing the PSDs of VDSL according to frequency and electrical loop lengths is known as power back-off (PBO).

Downstream PBO

Command	Mode	Function
xdsl line-config-profile *PROFILE* { down-pbo-esel I down-pbo-esel-min } <0-512>	Bridge	Configures power backoff assumed electrical length of xDSL line. **PROFILE**: enter the profile name. **down-pbo-esel**: downstream power backoff assumed electrical length 0 - 255.5: values in steps of 0.5 dB (0 = PBO disabled) **down-pbo-esel-min**: downstream power backoff assumed minimum electrical length. **0 - 512**: values in steps of 0.5 dB (default 512). If this value is not 512 (default) and DownPboEsel is not zero, DownPboEsel >= DownPboEselMin is required!
xdsl line-config-profile *PROFILE* **down-pbo-mus** <0-255>	Bridge	Sets min. usable receive signal PSD on xDSL line. **PROFILE**: enter the profile name. **0 - 255**: values in steps of 0.5 dB/Hz (-127.5 to 0 dB/Hz)
xdsl line-config-profile *PROFILE* **down-pbo-fmin** <0-2048>	Bridge	Sets start value of frequency range where PBO is applied on xDSL line. **PROFILE**: enter the profile name. **0- 2048**: value*4.3125 kHz
xdsl line-config-profile *PROFILE* **down-pbo-fmax** <32-4095>	Bridge	Sets end value of frequency range where PBO is applied on xDSL line. **PROFILE**: enter the profile name. **32 - 4095**: value*4.3125 kHz
xdsl line-config-profile *PROFILE* **dpbo-epsd add** <1-4095> <0-255>	Bridge	Adds one subcarrier/level pair (PSD mask) on xDSL line. **PROFILE**: enter the profile name. **1 - 4095**: subcarrier index **0 - 255**: PSD mask leve
xdsl line-config-profile *PROFILE* **dpbo-epsd delete index** <1-16>	Bridge	Deletes one entry (pair subcarrier/level) by index on xDSL line. **PROFILE**: enter the profile name. **1 - 16**: EPSD mask index
xdsl line-config-profile *PROFILE* **dpbo-epsd delete subcarrier** <1-4095>	Bridge	Deletes one entry (pair subcarrier/level) by subcarrier on xDSL line. **PROFILE**: enter the profile name. **1 - 4095**: EPSD subcarrier index
xdsl line-config-profile *PROFILE* { down-pbo-escma I down-pbo-escmb I down-pbo-escmc } <0-640>	Bridge	Configures cabel model parameter on xDSL line in terms of three scalars DPBOESCMA, DPBOESCMB and DPBOESCMC that are used to estimate the frequency dependent loss of E-side cables calculated from the DPBOESEL parameter using the formula: ESCM(f) = (DPBOESCMA + DPBOESCMB * sqrt(f) + DPBOESCMC * f) *DPBOESCL where ESCM is expressed in dB and f is expressed in MHz. **PROFILE**: enter the profile name. **down-pbo-escma**: cabel model parameter A (fixed part of ESCM(f) equation). Default ESCMa: 270-> 0.0546875. **down-pbo-escmb**: cabel model parameter B (linear part of ESCM(f) equation). Default ESCMb: 490 -> 0.9140625. **down-pbo-escmc**: cabel model parameter C (square root part of ESCM(f) equation). Default ESCMc: 264 -> 0.03125 **0 -640**: value in multiples of 2E-8, the effective range for ESCMx is: -1 (coded as 0) .. 1.5 (coded as 640) with stepping 2E-8.

Upstream PBO

Command	Mode	Function
xdsl line-config-profile *PROFILE* **up-pboa** { us1 I us2 I us3 I us4 I us5 } <4000-8095>	Bridge	Configures the value A in the reference PSD on xDSL line - PSDREF(f)= -A - B * sqrt(f). The value is given for each US band except US0. Each single value consists of 2 octets. First couple of octets representing the value for band US1. Second for band US2, third for US3, fourth for US4 and the last couple represent the value for US5. All values can be set, but only if the respective band is realy in use the values will be taken, otherwise **NE** will ignore the settings. The simultaneous setting of values of UPBOA = 40 dBm/Hz and UPBOB = 0 dBm/Hz for a band shall cause UPBO to be disabled. This are the default setting for all band's. **PROFILE**: enter the profile name. **us1**: UPBOA for US1 band **us2**: UPBOA for US2 band **us3**: UPBOA for US3 band **us4**: UPBOA for US4 band **us5** UPBOA for US5 band **4000 - 8095**: value in 0.01 dBm/Hz (40 to 80.95)
xdsl line-config-profile *PROFILE* **up-pbob** { us1I us2 I us3 I us4 I us5 } <0-4095>	Bridge	Configures the value B in the reference PSD on xDSL line - PSDREF(f)= -A - B * sqrt(f). The value is given for each US band except US0. Each single value consists of 2 octets. First couple of octets representing the value band US1. Second for band US2, third for US3, fourth for US4 and the last couple represent the value for US5. All values can be set, but only if the respective band is realy in use the values will be taken, otherwise NE will ignore the settings. The simultaneous setting of values of UPBOA = 40 dBm/Hz and UPBOB = 0 dBm/Hz for a band shall cause UPBO to be disabled. This are the default setting for all band's. **PROFILE**: enter the profile name. **us1**: UPBOB for US1 band **us2**: UPBOB for US2 band **us3**: UPBOB for US3 band **us4**: UPBOB for US4 band **us5** UPBOA for US5 band **0 - 4095**: Value in 0.01 dBm/Hz (if 0 + up-pboa=4000 => UPBO disabled for this band)

Power Managment

The hiX 5750 R2.0 provides power management saving power at three levels (L0/L2/L3). The L2 level enables statistical power saving at the xDSL transceiver unit in the central office (xTU-C) by rapidly entering and exiting low power mode based on Internet traffic running over the xDSL connection. For example, when large files are being downloaded, ADSL2 operates in full power mode (called "L0" power mode) in order to maximize the download speed. When Internet traffic decreases, such as when a user is reading a long text page, ADSL2 systems can transit into L2 low power mode, in which the data rate is
significantly decreased and overall power consumption is reduced. The L3 power mode enables overall power savings at the xTU-C by entering into sleep mode when the connection is not being used for extended periods of time. L3 is the sleep mode that enables overall power savings at both the xTU-C and the remote xDSL transceiver unit (xTU-R) when the connection is not being used for extended periods of time.

Command	Mode	Function
xdsl line-config-profile *PROFILE* { pwr-mgmt-l0time I pwr-mgmt-l2time } <0-255>	Bridge	Configures the L0/L2 time on xDSL line. **PROFILE**: enter the profile name. **pwr-mgmt-l0time**: minimum time between an exit from the L2 state and the next entry into the L2 state. **pwr-mgmt-l2time**: minimum time between an Entry into the L2 state and the first Power Trim in the L2 state and between two consecutive Power Trims in the L2 State. **0 - 255**: range in seconds
xdsl line-config-profile *PROFILE* { pwr-mgmt-l2atpr I pwr-mgmt-l2atprt } <0-31>	Bridge	Configures the maximum aggregate transmit power reduction. **PROFILE**: enter the profile name. **pwr-mgmt-l2atpr**: maximum aggregate transmit power reduction performed through a single Power Trim, **pwr-mgmt-l2atprt**: total max. aggregate transmit power reduction performed in L2 state (L2 req.s + Power Trims. **0 - 31**: value in dB (step 10 dB)
xdsl line-config-profile *PROFILE* **pwr-mgmt-mode** { disabled I l3-enabled I l1-l2-enabled I l1-l2-l3-enabled }	Bridge	Configures the enabled power management state and where the line may autonomously transition to. **PROFILE**: enter the profile name. **disabled**: none **l3-enabled**: idle state **l1-l2-enabled**: low power state **l1-l2-l3-enabled**: both idle and low power state
xdsl line-config-profile *PROFILE* **pwr-mgmt-l2rate** <8000-1024000>	Bridge	Configures the power management L2 rate. **PROFILE**: enter the profile name. **8000 - 1024000**: L2 rate value in bps.

Loop Length and Burst Mode

Command	Mode	Function
xdsl line-config-profile *PROFILE* **up-pbo-kl** <0-1280>	Bridge	Configures the upstream electrical loop length expressed in dB at 1 MHz on xDSL line. **PROFILE**: enter the profile name. **0 - 1280**: value insteps of 0.1 dB (0=0 dB ...1280=128 dB)
xdsl line-config-profile *PROFILE* **up-pbo-ko** { enable I disable }	Bridge	Enables/disables usage of electrical loop length on xDSL line. If not enabled, the electrical loop length shall be autonomously derived be the xTU's. Default value is disabled. **PROFILE**: enter the profile name.
xdsl line-config-profile *PROFILE* **boost-mode** { enable I disable }	Bridge	Enables/disables usage of boost mode on xDSL line. If disabled, the UPBO standard mode is used with the LOSS function calculated according to G.997.1. **PROFILE**: enter the profile name.

11.1.3 Checking of Profiles

Command	Mode	Function
show xdsl line-config-profile	Privieged/ Global/ Bridge	Shows all configured line profiles.
show xdsl line-config-profile *PROFILE*		Shows one configured line profile. **PROFILE**: enter the profile name.
show xdsl line-config-profile *PROFILE* **margin**		Shows all SNR margins of selected profile. **PROFILE**: enter the profile name.

Command	Mode	Function
show xdsl line-config-info	Privieged/ Global/ Bridge	Shows all line-config profiles and their assigned ports.
show xdsl line-config-info *PROFILE*		Shows one line-config profile and its assigned ports. **PROFILE**: enter the profile name.

11.2 Channel Profile

The channel profile provides all settings of data rates, interleaving delay, performance monitoring, and error handling. In order to remove errors, the hiX 5750 R2.0 provides impulse noise protection (INP) values up to 16.

11.2.1 Creating/Deleting a Profile

ℹ If the channel profile for channel 2 should be deleted, the **VCC TP** assignment has to be checked and corrected. In case of ADSL mode, all available VCC TP’s has to be moved to channel 1. In case of VDSL2 mode, the VCC TP which was assigned to channel 2 has to be deleted first.

Command	Mode	Function
xdsl add chan-config-profile *PROFILE*	Bridge	Creates a channel profile. **PROFILE**: enter the profile name.
xdsl delete chan-config-profile *PROFILE*		Deletes the specified channel profile.
xdsl duplicate chan-config-profile *SOURCE-PROFILE NEW-PROFILE*	Bridge	Copies a channel profile. **SOURCE-PROFILE**: name origin channel profile. **NEW-PROFILE**: name new channel profile

11.2.2 Configuration

ℹ The port has to be in locked state, before parameters can be modified.

Command	Mode	Function
xdsl chan-config-profile *PROFILE* { datarate-min-ds I datarate-min-us I datarate-min-res-ds I datarate-min-res-us I datarate-max-ds I datarate-max-us I datarate-min-low-pwr-ds) <32-103980>	Bridge	Configures the maximum and minimum data rate of downtream / upstream channel. **PROFILE**: enter the profile name. **datarate-min-ds**: Min. data rate of downstream channel **datarate-min-us**: Min. data rate of upstream channel **datarate-min-res-ds**: Min. reserved data rate of downstream channel (only used in dynamic RA mode) **datarate-min-res-us**: Min. reserved data rate of upstream channel (only used in dynamic RA mode **datarate-max-ds**: Max. data rate of downstream channel **datarate-max-us**: Max. data rate of upstream channel **datarate-min-low-pwr-ds**: Min. data rate of downstream channel in low power state **32 - 103980**: data rate in kbps. ℹ Be aware, that for an ADSL/ADSL2/ADSL2+ profile, the definied maximum values for datarates could not be used. For lines using an ADSL standard the maximum datarate value in downstream direction is limited to 32736 kbps, in upstream direction to 3520 kbps.

Command	Mode	Function
xdsl chan-config-profile *PROFILE* { max-interdelay-ds | max-interdelay-us } <0-255>	Bridge	Configures maximum interleave delay in milliseconds on downstream / upstream direction introduced by the PMS-TC on downstream / upstream direction. The xTUs shall choose the S (factor) and D (depth) values such that the actual one-way xDSL channel interleave delay is as close as possible to, but less than or equal to this parameter. **PROFILE**: enter the profile name. **max-interdelay-ds**: Max. interleave delay for downstream channel. **max-interdelay-us**: Max. interleave delay for upstream channel. **0 - 255**: value in milliseconds 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 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 G.993.2 same as value 1 for other recommendations. If the value 1 or 255 is selected, then the configured value for channel profile min INPDs should be “off” (0).
xdsl chan-config-profile *PROFILE* { min-inp-ds | min-inp-us } { off | halfsymbol | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 }	Bridge	Configures minimum Impulse noise protection (INP) on xDSL line. **PROFILE**: enter the profile name. **off**: off **halfsymbol**: 0.5 symbol. **0**: 0 symbol (= off) **1...16**: 1 symbol ... 16 symbols
xdsl chan-config-profile *PROFILE* { max-bit-errorrate-ds | max-bit-errorrate-us } { 10E-7 | 10E-5 | 10E-3 }	Bridge	Configures maximum value for allowed bit error rate for the bearer channel. **PROFILE**: enter the profile name. **max-bit-errorrate-ds**: maximum value for allowed bit error rate on downstream direction. **max-bit-errorrate-us**: maximum value for allowed bit error rate on upstream direction
xdsl chan-config-profile *PROFILE* { thresh-downshift-ds | thresh-upshift-ds | thresh-downshift-us | thresh-upshift-us } <0-1000000>	Bridge	Configures rate change threshold causing a downshift/upshift trap on downstream/upstream channel. **PROFILE**: enter the profile name. **thresh-downshift-ds**: rate change threshold causing a downshift trap on downstream channel. **thresh-downshift-us**: rate change threshold causing a downshift trap on upstream channel. **thresh-upshift-ds**: rate change threshold causing an upshift trap on downstream channel. **thresh-upshift-us**: rate change threshold causing an upshift trap on upstream channel. **0 - 1000000**: rate change threshold in bps.

11.2.3 Checking of Profiles

Command	Mode	Function
show xdsl chan-config-profile	Privileged/ Config/ Bridge	Shows all configured channel profiles.
show xdsl chan-config-profile *PROFILE*	Privileged/ Config/ Bridge	Shows one configured channel profile. **PROFILE**: enter the profile name.
show xdsl chan-config-info	Privileged/ Config/ Bridge	Shows information of xDSL channel config profiles.

Command	Mode	Function
show xdsl chan-config-info *PROFILE*	Privileged/ Config/ Bridge	Shows information of xDSL channel config profile. **PROFILE**: enter the profile name.

11.3 Notch Profile

The VDSL spectrum covers a number of Handheld Amateur Radio (HAM) radio bands. To avoid interference it is necessary to introduce power control (notching) in one or more of these bands.The hiX 5750 R2.0 does not use RFI band masks. This feature is supported by the notch profiles. The standard notches defined in the VDSL spectrum representing the subcarrier-indices if a spacing of 4.3125 kHz is used (profiles 8A .. 17A) are provided in the following table:

Band	Start Frequency	Start Subcarrier	End Frequency	End Subcarrier
HAM	1810 kHz	417	2000 kHz	464
	3500 kHz	811	3800 kHz (ETSI), 4000 kHz (ANSI)	881
	7000 kHz	1623	7100 kHz (ETSI), 7300 kHz (ANSI)	1670
	10100 kHz	2342	10150 kHz	2354
	14000 kHz	3246	14350 kHz	3328
GMDSS	2173 kHz	504	2191 kHz	508
	4200 kHz	974	4215 kHz	977
	6300 kHz	1461	6320 kHz	1466

Table 21 RFI in VDSL Spectrum

11.3.1 Creating/Deleting a Profile

Command	Mode	Function
xdsl add notch-config-profile *PROFILE*	Bridge	Create Notch profile. **PROFILE**: enter the profile name.
xdsl delete notch-config-profile *PROFILE*		Delete a specified Notch profile.
xdsl duplicate notch-config-profile *SOURCE-PROFILE NEW-PROFILE*	Bridge	Copies a notch profile. **SOURCE-PROFILE**: name of origin notch profile. **NEW-PROFILE**: name of new profile.

11.3.2 Configuration

General restriction for notch profile configuraion and assignment:

- Inside of one notch profile, the **NE** will not accept a subcarrier overlapping – otherwise the configuration will be rejected.
- Be aware, that the NE can handle only 16 notches per line at time (RFI band's + used notches).

- A modification of an existing notch profile is not allowed, if this profile is already in use (that means, this profile is assigned directly to a XDSL line).

Command	Mode	Function
xdsl notch-config-profile *PROFILE* **add-notch** <1-4095> <2-4095>	Bridge	Add one Notch to the table, (up to 16 Notches possible). **PROFILE**: enter the profile name. **1 - 4095**: start index of subcarrier for Notch **2 - 4095**: stop index of subcarrier for Notch
xdsl notch-config-profile *PROFILE* **delete-notch** <1-16>	Bridge	Delete one Notch from the Notch profile table. **PROFILE**: enter the profile name. **1 - 16**: Notch index

11.3.3 Checking of Profiles

Command	Mode	Function
show xdsl notch-config-profile	Privileged/ Config/ Bridge	Shows all configured notch profiles.
show xdsl notch-config-profile *PROFILE*	Privileged/ Config/ Bridge	Shows one configured notch profile. **PROFILE**: enter the profile name.
show xdsl notch-config-info	Privileged/ Config/ Bridge	Shows all notch-config profiles and their assigned ports.
show xdsl notch-config-info *PROFILE*	Privileged/ Config/ Bridge	Shows one notch-config profile and its assigned ports. **PROFILE**: enter the profile name.

11.4 PSD Mask Profiles

To provide coexistence with other services PSD masks can be configured for VDSL2 regional bandplan annexes.

11.4.1 Creating/Deleting a Profile

A **downstream** PSD profile could support up to **32 breakpoints**. A **upstream** profile could support up to **16 breakpoints**.

When a new PSD profile is created, all breakpoints are zero. The table below contains a set of default breakpoints according to the VDSL2 specification G.993.2.

Downstream		Upsteem	
Index Subcarrier	Level dBm/Hz	Index Subcarrier	Level dBm/Hz
65	-39.5	32	-38.0
256	-39.5	63	-38.0
376	-49.5	882	-54.5

Table 22 Default PSD Mask Profile for VDSL2 G.993.2

Downstream		Upsteem	
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 22 Default PSD Mask Profile for VDSL2 G.993.2 (Cont.)

Command	Mode	Function
xdsl add psd-config-profile *PROFILE* { downstream I upstream }	Bridge	Creates PSD mask profile (max. number of index is 32). Usage of profile for upstream or downstream direction . ℹ This parameter can only be set during profile creation! **PROFILE**: enter the profile name.
xdsl delete psd-config-profile *PROFILE*		Deletes specified PSD mask profile. ℹ The profile should not be in use by any line.
xdsl duplicate psd-config-profile *SOURCE-PROFILE NEW-PROFILE*	Bridge	Copies a PSD profile. **SOURCE-PROFILE**: name origin PSD profile. **NEW-PROFILE**: name new PSD profile.

11.4.2 Configuration

Command	Mode	Function
xdsl psd-config-profile *PROFILE* **add-psd** <1-4095> <0-195>	Bridge	Adds one PSD breakpoint to the table, **PROFILE**: enter the profile name. **1 - 4095**: index of subcarrier, where breakpoint will be placed **0 - 195**: PSD mask level 0 to -97.5 dBm/Hz (coded as 0 to 195) in steps of 0.5 dBm/Hz
xdsl psd-config-profile *PROFILE* **delete-psd index** <1-32>	Bridge	Deletes one PSD mask from the PSD mask profile by mask index. **PROFILE**: enter the profile name. **1 - 32**: PSD mask index
xdsl psd-config-profile *PROFILE* **delete-psd subcarrier** <1-4095>	Bridge	Deletes one PSD mask from the PSD mask profile by subcarrier index. **PROFILE**: enter the profile name. **1 - 4095**: subcarrier index

11.4.3 Checking of Profiles

Command	Mode	Function
show xdsl psd-config-profile	Privileged/ Config/ Bridge	Shows all configured PSD profiles.
show xdsl psd-config-profile *PROFILE*		Shows selected PSD profile. **PROFILE**: enter the profile name.
show xdsl psd-config-info		Show all PSD profiles with assigned ports
show xdsl psd-config-info *PROFILE*		Shows PSD profile and its assigned ports. **PROFILE**: enter the profile name.

11.5 Alarm Profile

11.5.1 Creating/Deleting a Profile

Command	Mode	Function
xdsl add alarm-config-profile *PROFILE*	Bridge	Creates the new alarm-config profile. **PROFILE**: enter the profile name.
xdsl delete alarm-config-profile *PROFILE*		Deletes the alarm-config profile.
xdsl duplicate alarm-config-profile *SOURCE-PROFILE NEW-PROFILE*	Bridge	Duplicates the alarm-config profile. **SOURCE-PROFILE**: enter source profile name. **NEW-PROFILE**: enter new profile name.

11.5.2 Configuration

Command	Mode	Function
xdsl alarm-config-profile *PROFILE* { thres-lofs I thres-loss I thres-lprs I thres-lols I thres-es I thres-ses I thresuas } <0-900>	Bridge	Configure the alarm threshold profile. **PROFILE**: enter the profile name. **thres-lofs**: loss of frame seconds alarm threshold **thres-loss**: loss of signal seconds alarm threshold **thres-lrps**: loss of power seconds alarm threshold **thres-lols**: loss of link seconds alarm threshold **thres-es**: errored seconds alrm threshold **thres-ses**: severely errored seconds alarm thresholdthres-uas: unavailable seconds alarm threshold **0 - 900**: value in seconds
xdsl alarm-config-profile *PROFILE* { opstate-notify I initfailure-notify } { enable I disabe }		Enable/disable the the state notification. **PROFILE**: enter the profile name. **opstate-notify**: operation state notification **initfailure-notify**: init failure notification

11.5.3 Checking of Profiles

Command	Mode	Function
show xdsl alarm-config-profile	Privileged/ Config/ Bridge	Show all configured alarm profiles
show xdsl alarm-config-profile *PROFILE*		Show one configured alarm profile. **PROFILE**: enter the profile name.
show xdsl alarm-config-info		Show all alarm-config profiles and their assigned ports.
show xdsl alarm-config-info *PROFILE*		Show one alarm-config profile and its assigned ports. **PROFILE**: enter the profile name.

11.5.4 Verifying the Running XDSL Profiles

Use the following commands to examine the currently on system running xDSL profiles.

Command	Mode	Function
show running-config xdsl all-profiles	Config	Shows all current xDSL profiles.
show running-config xdsl { line-profile I chan-profile I alarm-profile I notch-profile I psd-profile }	Exec/ Config	Shows specified current xDSL profile.

11.6 Configuring of LRE-Port

The VDSL technologies base on Ethernet in the Fist Mile (EFM) to end users (so called Long Reach Ethernet - LRE) to provide a complete suite of IP based services. Therefore, the access network can be simplified into an end-to-end Ethernet access architecture that provides the preconditions of features such as VLAN-per-service and DHCP authentication using Option 82.

11.6.1 Assigning xDSL Profiles to Port (EFM)

ℹ Note the following requirements before changing the used DSL-Standard via line profile:

- Enabling ADSL2 and VDSL2 standard is not supported inside of one single profile at the same time
- If the subscriber port is of ADSL2, a switch over to a VDSL2 mode is not possible.

Command	Mode	Function
lre *PORTS* **xdsl line-config** [*PROFILE*]	Bridge	Assigns xDSL line-config profile to specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **PROFILE**: enter line profile name.
lre *PORTS* **xdsl chan-config** { channel1 | channel2 } [*PROFILE*]		Sets channel profile for channel1/channel2. Channel1 is always available, channel2 only in dual latency mode. **PORTS**: enter slot/port/ONU ID/ONT slot. **PROFILE**: enter the channel profile name. ℹ Profile name for channel 1 must be set, profile name for channel2 can be left empty.
lre *PORTS* **xdsl notch-config** [*PROFILE*]		Assigns xDSL Notch profile to specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **PROFILE**: enter notch profile name or nothing if profile has to be removed from port.
lre *PORTS* **xdsl psd-config** { up | down } [*PROFILE*]		Assigns PSD upstream/downstream profile to specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **PROFILE**: enter PSD profile name (or nothing to reassign profile from ports).
lre *PORTS* **xdsl alarm-config** [*PROFILE*]		Assigns the alarm profile to specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **PROFILE**: enter alarm profile name.

11.6.2 ATM Configuration

In addition to EFM the classical **ATM** transport can be used. The hiX 5750 R2.0 supports ATM networks with virtual channel (VC). A VC can be configured by virtual circuit identifier (VCI) and virtual path identifier (VPI).

Configuring of Virtual Channel

Command	Mode	Function
lre *PORTS* **xdsl atm vc create vpi** <0-255> **vci** <32-65535>	Bridge	Creates a VC by VCI and VPI on specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **0 - 255**: range VPI values (default is 1) **32 - 65535**: range VCI values (default is 32)
lre *PORTS* **xdsl atm vc delete vpi** <0-255> **vci** <32-65535>		Deletes a VC specified by VCI and VPI. **PORTS**: enter slot/port/ONU ID/ONT slot. **0 - 255**: VPI values **32 - 65535**: VCI values
lre *PORTS* **xdsl atm vcc** <1-8> **vpi** <0-255> **vci** <32-65535>		Configures VCC TP on specified port. **PORTS**: enter slot/port/ONU ID/ONT slot. **1 - 8**: index **VCC** **0 - 255**: VPI values **32 - 65535**: VCI values
lre *PORTS* **xdsl atm vcc** <1-8> **encap** { llc | vc-mux }		Sets the used encapsulation over ATM adaption layer 5 (AAL5) to LLC or VC-MUX. **PORTS**: enter slot/port/ONU ID/ONT slot. **1 - 8**: index VCC
lre *PORTS* **xdsl atm vcc** <1-8> **alarmseverity** <1-10>		Sets alarm severity value for specified VCC. **PORTS**: enter slot/port/ONU ID/ONT slot. **1 - 8**: index VCC **1 - 10**: index alarm severity

Checking of VC Configuration

Command	Mode	Function
show lre *PORT-ADDRESS* **xdsl atm vcctp-info**	Privileged/ Global/ Bridge	Shows **VCC TP** detailed information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl atm vcctp-overview**		Shows VCC TP information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.

11.6.3 Checking the XDSL Configuration of LRE Port

Command	Mode	Function
show lre *PORT-ADDRESS* **xdsl line-config-info**	Privieged/ Global/ Bridge	Shows xDSL line configuration information for a specified port. **PORT-ADDRESS**: slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl line-table**		Shows xDSL line status information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl line-conf**		Shows line table configuration. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORTS* **xdsl band-table**	Privileged/ Config/ Bridge	Show xDSL line band table **PORTS**: enter slot/port/ONU ID/ONT slot.

Command	Mode	Function
show lre PORTS **xdsl chan-table**	Privileged/ Config/ Bridge	Shows xDSL channel status information **PORTS**: enter slot/port/ONU ID/ONT slot.
show lre *PORTS* **xdsl chan-config-info**		Shows **LRE** port xDSL channel config profile information. **PORTS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl chan-table**		Shows xDSL channel status information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl notch-config-info**	Privileged/ Config/ Bridge	Shows LRE port xDSL notch config information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORTS* **xdsl psd-config-info**	Privileged/ Config/ Bridge	Shows LRE port xDSL PSD profile information. **PORTS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl alarm-config-info**	Privileged/ Config/ Bridge	Shows the xDSL relation between ports and assigned alarm profiles. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl alarm-table**		Shows xDSL alarm status information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl atm vcctp-info**	Privileged/ Global/ Bridge	Shows **VCC TP** information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl atm vcctp-overview**		Shows VCC TP information. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORTS* **xdsl phys-table detail** { xtuc | xtur }	Privileged/ Global/ Bridge	Shows detailed information of xDSL physical status. **PORTS**: enter slot/port/ONU ID/ONT slot. **xtuc**: VDSL LIU = vtuC **xtur**: VDSL modem = vtuR
show lre *PORTS* **xdsl phys-table linerates**		Shows xDSL physical status: only linerates (up/downstream) **PORTS**: enter slot/port/ONU ID/ONT slot.
show lre *PORTS* **xdsl phys-table alarm**		Shows xDSL physical status: alarm/failure state **PORTS**: enter slot/port/ONU ID/ONT slot.

11.7 Verifying of the XDSL Databases

Use the following commands in order to get information about the values stored in xDSL databases.

Command	Mode	Function
show xdsldb { line-tbl | name-table | phys-tbl | chan-tbl | band-tbl | vcc-tbl | alm-tbl | xdsl-port-tbl | operstate | db-checksum }	Exec/ Config/ Bridge	Shows information about a specified xDSL database table, **line-tbl**: line table **name-table**: profile name table **phys-tbl**: physical table **chan-tbl**: channel table **band-tbl**: line-band table **vcc-tbl**: **VCC** table **alm-tbl**: alarm table **xdsl-port-tbl**: port table **operstate**: card operstate **db-checksum**: checksum.
show liudb version	Exec/ Config/ Bridge	Shows version of the line interface unit.

Command	Mode	Function
show xdsldb xdslMode *PROFILEINDEX*	Exec/ Config/ Bridge	Shows information about the xDSL mode. **PROFILEINDEX**: profile name index from line profile.

11.8 DELT Configuration

DELT(Dual Ended Line Test) allows to test a single line on xTU-C/xTU-R side. Result data are requested from the xDSL interface, where DELT was running before.

Command	Mode	Function
lre *PORTS* **xdsl delt** { force | inhibit }	Privieged/ Global/ Bridge	Enables/disables DELT mode on selected ports. **PORTS**: slot/port/ONU ID/ONT slot. **force**: force loop diagnostics by xTU-C **inhibit**: stop loop diagnostics process
show lre *PORT-ADDRESS* **xdsl delt status**		Shows information about port DELT status. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot.
show lre *PORT-ADDRESS* **xdsl delt all** { downstream | upstream } [<1-4096> [<1-4096>]]		Shows all subcarrier group values of one port for downstream/upstream direction. **PORT-ADDRESS**: enter slot/port/ONU ID/ONT slot. **1 - 4096**: start subcarrier group (press ENTER to show all), **1 - 4096**: end subcarrier group (press ENTER to show only one).
show lre *PORT-ADDRESS* **xdsl delt bit-allocation** { downstream | upstream } [<1-4096> [<1-4096>]]	Privieged/ Global/ Bridge	Shows Bit allocation table for different subcarriers of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier (press ENTER to show all), 1 - 4096: end subcarrier (press ENTER to show only one).
show lre *PORT-ADDRESS* **xdsl delt gain-allocation** { downstream | upstream } [<1-4096> [<1-4096>]]		Shows Bit allocation table for different subcarriers of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier (press ENTER to show all), 1 - 4096: end subcarrier (press ENTER to show only one). The gain value is represented as a multiple of 1/512 on linear scale.
show lre *PORT-ADDRESS* **xdsl delt snr-allocation** { downstream | upstream } [<1-4096> [<1-4096>]]		Shows **SNR** allocation table for different subcarrier groups of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier group (press ENTER to show all), 1 - 4096: end subcarrier group (press ENTER to show only one).
show lre *PORT-ADDRESS* **xdsl delt qln-allocation** { downstream | upstream } [<1-4096> [<1-4096>]]		Shows Quiet Line Noise allocation table for different subcarrier groups of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier group (press ENTER to show all), 1 - 4096: end subcarrier group (press ENTER to show only one).
show lre *PORT-ADDRESS* **xdsl delt hlin-allocation** { downstream | upstream } [<1-4096> [<1-4096>]]		Shows H(f) linear representation for subcarrier groups of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier group (press ENTER to show all), 1 - 4096: end subcarrier group (press ENTER to show only one).

Command	Mode	Function
show lre *PORT-ADDRESS* **xdsl delt hlog -allocation** { downstream | upstream } [<1-4096> [<1-4096>]]	Privileged/ Config/ Bridge	Shows H(f) logarithmic representation for subcarrier groups of one port for downstream/upstream direction. PORT-ADDRESS: enter slot/port/ONU ID/ONT slot. 1 - 4096: start subcarrier group (press ENTER to show all), 1 - 4096: end subcarrier group (press ENTER to show only one).

12 Voice over IP

Depending on the **ONT**/**MDU** type, it is possible to provide VoIP service via **SIP** or Megaco/H.248. The protocol version is valid for a whole ONT/ONT card (MDU service board).
Figure 4 illustrates the relations between the configuration modules.

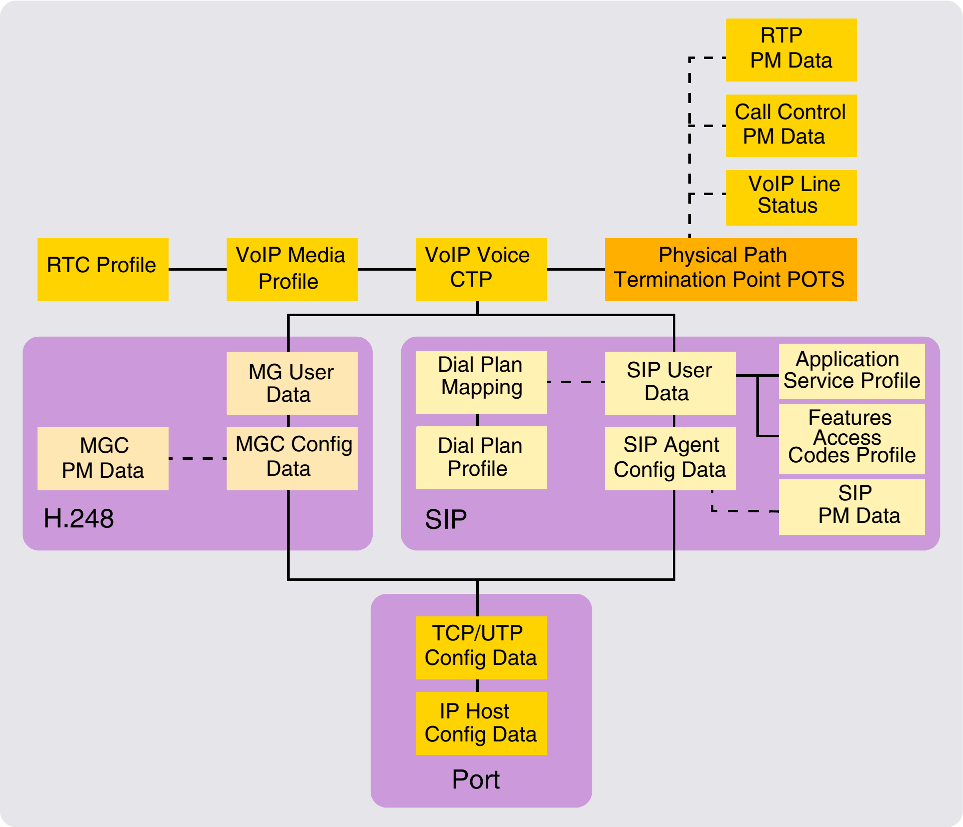


Figure 4 VoIP Configuration Structure

12.1 VoIP Profiles

12.1.1 RTP (Real-Time Transport Protocol) Profile

To configure the RTP profile, use the following commands.

Command	Mode	Function
create voip voip rtp-profile-table-entry <1-16> *LOCPORTMIN LOCPORTMAX* <0-255> { 0 I 1 } { 0 I 1 } { 0 I 1 } { 0 I 1 } [*LINE*]	Config	Creates RTP profile table entries. **1 - 16**: table entry index **LOCPORTMIN**: base RTP port used for voice traffic (0..65535), default 50000 **LOCPORTMAX**: top end range RTP port used for voice traffic, must be greater than base RTP port **0 - 255**: diffserv code point to be used for outgoing RTP packets, default: expedited forwarding=46 Events according to RFC 2833 disable (0) or enable (1): **0 I 1**: piggyback events **0 I 1**: tone events **0 I 1**: **DTMF** events **0 I 1**: **CAS** events **LINE**: the whole line (up to 64 characters allowed) will be taken as profile name, spaces included.
modify voip voip rtp-profile-table-entry <1-16> *LOCPORTMIN LOCPORTMAX* <0-255> { 0 I 1 } { 0 I 1 } { 0 I 1 } { 0 I 1 } [*LINE*]		Modifies RTP profile table entry.
delete voip voip rtp-profile-table-entry <1-16>		Deletes RTP profile table entry.

12.1.2 VoIP Media Profile

The media profile table contains entries for the connection to the media gateway controller (soft-switch) that controls the signaling messages.
Use the following commands to configure the media profile table.

Command	Mode	Function
create voip voip media-profile-table-entry <1-16> <0-1> <0-1> <0-1> <0-1> <1-16> { 1 I 2 I 3 I 4 I 255 } { on I off } <0-999> [*LINE*]	Config	Creates media profile table. **1 - 16**: table entry index Specified codec selection as defined in RFC 3551is 0-PCMU. Silence suppression (0=off, 1=on): **0 - 1**: 1st order **0 - 1**: 2nd order **0 - 1**: 3rd order **0 - 1**: 4th order **1 - 16**: pointer to the **RTP** profile Voice service prof announce type: **1**: silence **2**: recorder tone **3**: fast busy **4**: voice announcement **255**: not applicable **on/off**: echo cancellation indication **0 - 999**: **PSTN** protocol variant controls which variant of POTS signaling must be used on the associated UNIs (ISO 3166 country code), e.g 124 Canada, 156 China, 276 Germany, 414 Kuwait, 840 USA **LINE**: descriptive profile name (size max. 20), the whole line until CR will be pressed, spaces included.
modify voip voip media-profile-table-entry <1-16> <0-1> <0-1> <0-1> <0-1> <1-16> { 1 I 2 I 3 I 4 I 255 } { on I off } <0-999> [*LINE*]		Modifies media profile table entry.
modify voip voip media-profile-table-entry-name <1-16> [*LINE*]		Modifies media profile name.
modify voip voip media-profile-pstn-protocol-variant <1-16> <0-999>		Modifies media profile PSTN protocol variant. **Valid after reboot or lock/unlock of ONT**.
delete voip voip media-profile-table-entry <1-16>		Deletes media profile table.

12.1.3 Checking the Media and RTP Profiles

To show media and RTP profiles, use the following commands.

Command	Mode	Function
show voip voip media-profile-table	Exec/ Config	Shows the whole media profile table.
show voip rtp-profile-data-table	Exec/ Config	Shows the whole **RTP** profile data table.

12.2 VoIP IP Host

The following two configuration data tables contain the information about services based on **TCP** and **UDP** that are offered from the IP hosts. The entries of these tables are unconditionally required for such **ONT**s which provide TCP/UDP IP services. Additional, the IP host configuration allows further features to support through the ONTs. There is usually one entry per ONT card, i.e., only one source TCP / UDP port used for communication with **MGC** (soft-switch) is supported. Table indices are the IP interface of the ONT (first index) and the TCP / UDP port (second index).

12.2.1 IP Host Configuration Table

Creating/Deleting an IP Host Configuration Table

The IP host's config-data-table contains configuration data of IP interfaces. There is one table entry per ONT card that is providing IP host services.

Use the following commands to create or delete an IP host's config-data-table by means of the interface index or the ONT address.

Command	Mode	Function
create voip ip-host config-data-table *INDEX*	Config	Creates a VoIP IP-host config table. **INDEX**: Interface index of ONT which provides IP host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.
create voip ip-host config-data-table-addr *ADDRESS*		
delete voip ip-host config-data-table *INDEX*		Deletes a VoIP IP-host config table.
delete voip ip-host config-data-table-addr *ADDRESS*		

Configuring the IP Host Parameters

Use the following commands to configure the VoIP options of ONT interfaces that provide IP host services, e.g. servises based on TCP and UDP.

Command	Mode	Function
modify voip ip-host ip-options *INDEX OPTIONS*	Config	Modifies IP related options. **INDEX**: interface index of ONT card, which provides IP host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **OPTIONS**: this attribute is a bit-field that is used to enable (0) or disable (1) IP related options. The options are assigned as follows: 0x1 = Enable **DHCP** (default = 0) 0x2 = Respond to PINGs (default = 0) 0x4 = Respond to Trace Route messages.
modify voip ip-host-addr ip-options *ADDRESS OPTIONS*		

Command	Mode	Function
modify voip ip-host ont-identifier *INDEX* [*LINE*]	Config	Modifies ONT identifier string. **INDEX**: physical index of ONT card providing IP-Host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **LINE**: identifier string (up to 25 Byte).
modify voip ip-host-addr ont-identifier *ADRESS* [*LINE*]		
modify voip ip-host ip-mask-gateway *INDEX A.B.C.D A.B.C.D A.B.C.D*	Config	Modifies the IP address, mask, default gateway. **INDEX**: interface index of ONT card providing IP-host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **A.B.C.D**: address used for all IP services hosted by the ONT **A.B.C.D**: subnet mask for IP services hosted by the ONT **A.B.C.D**: default gateway address used for all IP services hosted by this ONT. If values are set, they will override any values returned in DHCP.
modify voip ip-host-addr ip-mask-gateway *ADDRESS A.B.C.D A.B.C.D A.B.C.D*		
modify voip ip-host dns-server *INDEX A.B.C.D A.B.C.D*	Config	Modifies primary, secondary DNS server. **INDEX**: interface index of ONT card providing IP-Host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **A.B.C.D**: address of primary DNS server **A.B.C.D**: address of secondary DNS server. If values are set, they will override any values returned in DHCP.
modify voip ip-host -addr dns-server *ADDRESS A.B.C.D A.B.C.D*		

Updating/Retrieving an IP Host Configuration Table

Use the following commands to show the update/retrieve the IP host’s config-data-table.

Command	Mode	Function
update voip ip-host config-data-table *INDEX*	Exec/ Config	Updates VoIP IP-host config table. **INDEX**: Interface index of ONT which provides IP host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.
update voip ip-host config-data-table-addr *ADDRESS*		
retrieve voip ip-host config-data-table *INDEX*	Exec/ Config	Retrieves VoIP IP-host config table. **INDEX**: Interface index of ONT which provides IP host services **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.
retrieve voip ip-host config-data-table-addr *ADDRESS*		

12.2.2 Configuring the TCP/UDP Port Table

Use the following commands to configure the TCP/UDP port.

Command	Mode	Function
create voip ip-host tcp-udp-port *IF_INDEX PORT_ID PROTOCOL DIFFSERVFIELD*	Config	Creates TCP/UDP port. **IF_INDEX**: physical interface index of IP host service - primary index of ONT **PORT_ID**: port ID of TCP/UDP port (1..65535) Default value is 2944 for text message formats and 2955 for binary message formats. **PROTOCOL**: protocol type available as defined by IANA. Default value is UDP (0x11). **DIFFSERVFIELD**: TOS/diffserv field of the IPv4 header. The contents of this attribute may contain the Type of Service as per RFC 1349 or the DSCP. Valid values for DSCP are as defined by IANA. Default value is 0x0.
modify voip ip-host tcp-udp-port tosdiffser *IF_INDEX PORT_ID VAL*		Modifies TCP/UDP port parameter. **VAL**: value for TOS/diffserv field.
delete voip ip-host tcp-udp-port *IF_INDEX PORT_ID*		Deletes TCP/UDP port.

Command	Mode	Function
create voip ip-host tcp-udp-port-addr *ADRESS PORT_ID PROTOCOL DIFFSERVFIELD*	Config	Creates TCP/UDP ports. **ADDRESS**: slot/port/ONT-ID/ONT slot.
modify voip ip-host tcp-udp-port-addr tosdiffser *ADDRESS PORT_ID VAL*		Modifies TCP/UDP port parameter.
delete voip ip-host tcp-udp-port-addr *ADDRESS PORT_ID*		Deletes TCP/UDP port address.

12.2.3 Checking the Configuration

To show configuration data, use the following commands.

Command	Mode	Function
show voip ip-host config-data-table	Exec/ Config	Shows the whole VoIP IP host config data table.
show voip ip-host config-data-table-addr *ADDRESS*		Shows the specified VoIP IP host config data table. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.
show voip ip-host tcp-udp-table	Exec/ Config	Shows the whole VoIP IP host TCP UDP table.
show voip ip-host tcp-udp-table-addr *ADDRESS*		Shows the specified VoIP IP host TCP UDP table. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.

12.3 VoIP Configuration Data Table

The VoIP configuration data table contains information about VoIP services per gateway. There is one table entry per ONT card that is providing VoIP services. Table entries are automatically created/deleted by the NE.

12.3.1 Modifying the VoIP Configuration Data Table

To modify entries of configuration data table, use the following commands.

Command	Mode	Function
modify voip voip config-data-signaling-protocol-used *PHYS_INDEX PROTOCOL*	Config	Modifies used signaling protocol. **PHYS_INDEX**: physical index **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **PROTOCOL**: type of VoIP signaling protocol used for ONT. Only one type of protocol is allowed. Valid values are: 0x00 = None, 0x01 = SIP, 0x02 = H.248, 0x03 = MGCP,
modify voip voip config-data-signaling-protocol-used-addr *ADDRESS PROTOCO*L		
modify voip voip config-data-configures-method *PHYS_INDEX METHOD*	Config	Modifies configured method in config table entry. **PHYS_INDEX**: physical index **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **METHOD**: method indicates to the ONT, which method should be used to configure the VoIP service of the ONT. 0x00 the ONT default (do not configure). indicate use of 0x01 **OMCI**, 0x02 configuration file retrieval, 0x03 TR-69, 0x04 **IETF** sipping config framework for VoIP service configuration of the ONT. 0x05 - 0xF0 are reserved for future use. 0xF1 - 0xFF are reserved for proprietary vendor configuration methods.
modify voip voip config-data-configured-method-addr *ADDRESS METHOD*		
modify voip voip config-data-server-address *PHYS_INDEX* [*LINE*]	Config	Modifies server address in config table entry. **PHYS_INDEX**: physical index **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **LINE**: server address to contact using the method indicated in the above attribute. The whole line will be taken until CR.
modify voip voip config-data-server-address-addr *ADDRESS LINE*		

Command	Mode	Function
modify voip voip config-data-alarm-severity *PHYS_INDEX* <1-10>	Config	Modifies alarm severity in config table entry. **PHYS_INDEX**: physical index **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **1 - 10**: alarm severity index.
modify voip voip config-data-alarm-severity-addr *ADDRESS* <1-10>		

12.3.2 Checking the VoIP Configuration Data Table

To show configuration data, use the following commands.

Command	Mode	Function
show voip voip config-data-table	Exec/ Config	Shows the VoIP config data table of all or specified ONT. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot.
show voip voip config-data-table-addr *ADDRESS*		

12.4 Voice CTP (Connection Termination Point) Table

A CTP table entry is automatically created and will be numbered identically with the POTS PPTP.

12.4.1 Modifying the Voice CTP Table

To modify entries of voice CTP table, use the following commands.

Command	Mode	Function
modify voip voip voice-ctp-table-entry *IF_INDEX* <1-16>	Config	Modifies **CTP** table entry. **IF_INDEX**: physical index **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1..max.) **1 - 16**: VoIP media profile table.
modify voip voip voice-ctp-table-entry-addr *ADDRESS* <1-16>		

12.4.2 Checking the Voice CTP Table

To show configuration data, use the following commands.

Command	Mode	Function
show voip voip voice-ctp-table	Exec/ Config	Shows the VoIP **CTP** table of all or specified port. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port (POTS port number 1..max.).
show voip voip voice-ctp-table-addr *ADDRESS*		

12.5 Line Status Table

A line status table entry is automatically created and will be numbered identically with the POTS PPTP. It contains status information related to the VoIP session for the specified POTS port.

12.5.1 Retrieving the Line Status

Use following commands to retrieve the line status.

Command	Mode	Function
retrieve voip voip line-status-table *IF_INDEX*	Config	Retrieves the line status table. **IF_INDEX**: interface index of the **POTS** port **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1..max.).
retrieve voip voip line-status-table-addr *ADRESS*		

12.5.2 Checking the Line Status

To show line status data, use the following commands.

Command	Mode	Function
show voip voip line-status-table	Exec/ Config	Shows the line status table of all or specified port. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ port (POTS port number 1..max.).
show voip voip line-status-table-addr *ADDRESS*		

12.6 Performance Monitoring

The following tables contain the completed 15-minute and 24-hours interval performance monitoring data collected with regard to the Call Control channel. All the attribute counters are only updated at the end of each period or on request, see 12.6.3 Updating the PM Data.

i See 10.10.2 Calculation Algorithms for PM Objects for information on the PM object indexes.

12.6.1 Configuring of Call-Control PM

The call control table contains an entry for each call control PM object related to a POTS PPTP supporting VoiP. This table contains the current performance monitoring data of the running 15-minute interval collected with regard to the Call Control channel.

Call-Control Thresholds

The table entries are thresholds for Call Control performance monitoring. Use the following commands to configure the call control thresholds. One call control table always exist and cannot be deleted. The thresholds are used to send a notification to the management system when the actual counter crosses this value. The notification 'on' will be sent at the crossing of the threshold by the actual counter; the notification 'off' will be sent at the end of the 15 min period, since that is when the actual counters are reset to 0

Command	Mode	Function
create voip-performance callctrl threshold <2-16> *SETFAIL SETTIMER TERMFAIL PORTREL PORTOFFHOCK SEVPTR*	Config	Creates VoIP performance call control ’threshold’ object. **2 - 16**: table index **SETFAIL**: threshold for call setup failures **SETTIMER**: threshold for call setup timer longest time period of a single call setup **TERMFAIL**: threshold for terminated calls number of calls that were terminated with cause **PORTREL**: threshold for abandon calls number of analog port releases without dialing **PORTOFFHOCK**: Threshold for off-hock timer - longest time period of a single off-hock **SEVPTR**: pointer to alarm-severity profile.
modify voip-performance callctrl threshold <1-16> *SETFAIL SETTIMER TERMFAIL PORTREL PORTOFFHOCK SEVPTR*		Modifies VoIP performance ’threshold’ table. **1 - 16**: table index.
delete voip-performance callctrl threshold <2-16>		Deletes VoIP performance ’threshold’ table.

Call-Control Objects

To configure call control objects, use the following commands.

Command	Mode	Function
create voip-performance callctrl object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>	Config	Creates VoIP performance ’call control’ object. **INDEX**: object index **lock/unlock**: deactivates/activates performance monitoring (admin state 15min/24hrs) **0 - 96**: number of history entries configured for the **PM** object and the 15min interval **0 - 1**: number of history entries configured for the PM object and the 24hrs interval **1 - 16**: pointer to ’threshold’ object.
modify voip-performance callctrl object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		Modifies VoIP performance ’call control’ object.
delete voip-performance callctrl object *INDEX*		Deletes VoIP performance ’call control’ object.

Verifying Call-Control Configuration Data

To show call control configuration data, use the following commands.

Command	Mode	Function
show voip-performance callctrl object-table	Exec/ Config	Shows the whole call control object table.
show voip-performance callctrl threshold-table		Shows the whole call control threshold table.

12.6.2 Configuring of RTP PM

RTP Objects

The table contains an entry for each RTP monitoring PM object related to a POTS PPTP supporting VoiP. To configure RTP monitoring objects, use the following commands.

Command	Mode	Function
create voip-performance rtpmon object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>	Config	Creates VoIP performance ’**RTP** monitoring threshold’ table. **INDEX**: object index **lock/unlock**: deactivates/activates performance monitoring (admin state 15min/24hrs) **0 - 96**: number of history entries configured for the **PM** object and the 15min interval **0 - 1**: number of history entries configured for the PM object and the 24hrs interval **1 - 16**: pointer to ’threshold’ object.
modify voip-performance rtpmon object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		Modifies VoIP performance ’RTP monitoring object table.
delete voip-performance rtpmon object *INDEX*		Deletes VoIP performance ’RTP monitoring threshold’ table.

RTP Thresholds

The table entries are thresholds for Call Control performance monitoring. To configure RTP thresholds, use the following commands.

Command	Mode	Function
create voip-performance rtpmon threshold <2-16> *RTPERRORS LOSS JITTER RTCPTIME BUFFUNDER BUFFOVER SEVPTR*	Config	Creates VoIP performance ’RTP monitoring threshold’ object. **2 - 16**: table index **RTPERRORS**: threshold for RTP errors **LOSS**: threshold for fraction of Loss from total packets **JITTER**: threshold for max jitter **RTCPTIME**: threshold for time between RTCP packets **BUFFERUNDER**: threshold for buffer underflow **BUFFEROVER**: threshold for buffer overflow **SEVPTR**: pointer to alarm-severity profile.
modify voip-performance rtpmon threshold <1-16> *RTPERRORS LOSS JITTER RTCPTIME BUFFUNDER BUFFOVER SEVPTR*		Modifies VoIP performance ’RTP monitoring threshold’ object. **1 - 16**: table index.
delete voip-performance rtpmon threshold <2-16>	Config	Deletes VoIP performance ’RTP monitoring threshold’ object.

Verifying RTP Configuration

To verify the RTP configuration, use the following commands.

Command	Mode	Function
show voip-performance rtpmon object-table	Exec/ Config	Shows the whole RTP monitoring object table.
show voip-performance rtpmon threshold-table		Shows the whole RTP monitoring threshold table.

12.6.3 Updating the PM Data

Use the following commands to update the PM data.

Command	Mode	Function
update voip-performance callctrl current-data *INDEX*	Config	Updates VoIP performance ’call control’ object. **INDEX**: physical index of the ONU card.
update voip-performance rtpmon current-data *INDEX*		Updates VoIP performance ’RTP monitoring’ object.

12.6.4 Checking the Current and History PM Data

Use the following commands to verify the PM data.

Command	Mode	Function
show voip-performance callctrl current-data-table	Exec/ Config	Shows the whole call control current data table.
show voip-performance callctrl history-data-table [*INDEX*]		Shows the whole call control history data table. **INDEX**: interface index of POTS port.
show voip-performance rtpmon current-data-table	Exec/ Config	Shows the whole RTP monitoring current data table.
show voip-performance rtpmon history-data-table		Shows the whole RTP monitoring history data table.

12.7 Megaco/H.248 Protocol

12.7.1 MGC Configuration Data Table

To configure the H.248 MGC configuration data table, use the following commands.

Command	Mode	Function
create voip mgc-config-data-table-entry *UDP_TCP_PTR PROTOCOL_VERSION MESSAGE_FORMAT MAX_RETRY_ATTEMPTS* [<2-16>]	Config	Creates **MGC** config data table entries. **UDP_TCP_PTR**: pointer to the **TCP**-**UDP** config data table (Default value is 2944 for text message formats and 2955 for binary message formats.) **PROTOCOL_VERSION**: protocol version of Megaco Protocol being used **MESSAGE_FORMAT**: 0=text long (default), 1= text short, 2=binary **MAX_RETRY_ATTEMPTS**: max. number of times a message is retransmitted to the MGC, default=0 **2 - 16**: table entry index or CR for automatically generated index.
modify voip mgc-config-data-table-entry <1-16> *UDP_TCP_PTR PROTOCOL_VERSION MESSAGE_FORMAT MAX_RETRY_TIME* *MAX_RETRY_ATTEMPTS SERVICE_CHANGE_DELAY*		Modifies MGC config data table entries. **1 - 16**: table entry index **MAX_RETRY_ATTEMPTS**: max. number of times a message is retransmitted to the MGC **SERVICE_CHANGE_DELAY**: service change delay.
delete voip mgc-config-data-table-entry <2-16>		Deletes MGC config data table entry.
modify voip mgc-config-data-table profile-name <1-16> [*LINE*]	Config	Modifies config data table profile name. **1 - 16**: profile index **LINE**: profile name (up to 64 characters, spaces included)
modify voip mgc-config-data-table primary-mgc <1-16> [*LINE*]	Config	Modifies primary MGC (soft-switch) controlling the signal messages. **1 - 16**: profile index **LINE**: the name (IP address or resolved name CR, the whole line will be taken as name, spaces included)
modify voip mgc-config-data-table secondary-mgc <1-16> [*LINE*]		Modifies secondary MGC (soft-switch).
modify voip mgc-config-data-table termination-id-base <1-16> [*LINE*]	Config	Modifies base string for the H.248 physical termination ID. **1 - 16**: profile index **LINE**: up to 25 chars will be taken as termination ID base, spaces included.

12.7.2 MGC User Data

Use the following commands to modify MGC user data.

Command	Mode	Function
modify voip mgc-user-data mgc-pointer *INDEX* <1-16>	Config	Modifies pointer to **VoIP** MGC config data table entries. **INDEX**: index of user data table (**POTS** PPPT) **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1..max.) **1 - 16**: table entry index.
modify voip mgc-user-data-addr mgc-pointer *ADDRESS* <1-16>		
modify voip mgc-user-data user-url *INDEX LINE*	Config	Modifies user URL. **INDEX**: index of user data (POTS PPPT) **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1..max.) **LINE**: new user URL; until CR, the whole line will be taken as organization name spaces included, maximum 256 characters
modify voip mgc-user-data-addr user-url *ADDRESS LINE*		

12.7.3 MGC Performance Monitoring

The MGC monitor object table contains an entry for each H.248 agent PM object. Index for PM objects is the physical index of the ONT containing the H.248 agent. One ONT contains one H.248 agent. All MGC user data table entries of one ONT must use the same MGC configuration data entry (only one profile per ONT possible). Since one MGC configuration data entry can be used for several ONTs, MGC configuration data table and MGC monitor object table have different indices.

ℹ See 10.10.2 Calculation Algorithms for PM Objects for information on the PM object indexes.

Configuring of MGC Objects

To configure MGC objects, use the following commands.

Command	Mode	Function
create voip-performance mgcmon object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>	Config	Creates VoIP performance '**MGC** monitoring' object. **INDEX**: object index **lock/unlock**: deactivates/activates performance monitoring (admin state 15min/24hrs) **0 - 96**: number of history entries configured for the **PM** object and the 15min interval **0 - 1**: number of history entries configured for the PM object and the 24hrs interval **1 - 16**: pointer to 'threshold' object.
modify voip-performance mgcmon object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		Modifies VoIP performance 'MGC monitoring' object.
delete voip-performance mgcmon object *INDEX*		Deletes VoIP performance 'MGC monitoring' object.

Configuring of MGC Thresholds

The table entries are thresholds for Call Control performance monitoring. To configure MGC thresholds, use the following commands.

Command	Mode	Function
create voip-performance mgcmon threshold <2-16> *PROTERRORS TRANSPLOSS SEVPTR*	Config	Creates VoIP performance ’MGC monitoring threshold’ object. **2 - 16**: table index **PROTERRORS**: threshold for protocol errors **TRANSPLOSS**: threshold for transport losses **SEVPTR**: pointer to alarm-severity profile.
modify voip-performance mgcmon threshold <1-16> *PROTERRORS TRANSPLOSS SEVPTR*		Modifies VoIP performance ’MGC monitoring threshold’ table. 1 - 16: table index.
delete voip-performance mgcmon threshold <2-16>		Modifies VoIP performance ’MGC monitoring threshold’ table.

Verifying the MGC PM Configuration

To show MGC configuration data, use the following commands.

Command	Mode	Function
show voip-performance mgcmon object-table	Exec/ Config	Shows the whole MGC monitoring object table.
show voip-performance mgcmon object-table-index *INDEX*		Shows the MGC monitoring object table. **INDEX**: physical index of the ONT card.
show voip-performance mgcmon threshold-table		Shows the whole MGC monitoring threshold table.

Updating the MGC PM Data

Use the following command to update the MGC performance monitoring data.

Command	Mode	Function
update voip-performance mgcmon current-data *INDEX*	Config	Updates VoIP performance ’mgc monitoring’ object.

Checking the MGC PM Data

Use the following commands to verify the MGC performance monitoring data.

Command	Mode	Function
show voip-performance mgcmon current-data-table	Exec/ Config	Shows the whole MGC monitoring current data table.
show voip-performance mgcmon current-data-table-index *INDEX*		Shows the MGC monitoring current data table for specified ONT. **INDEX**: physical index of the ONT card.
show voip-performance mgcmon history-data-table	Exec/ Config	Shows the whole MGC monitoring history data table.
show voip-performance mgcmon history-data-table-index *INDEX*		Shows the MGC monitoring history data table for specified ONT. **INDEX**: physical index of the ONT card.

12.7.4 Checking the MGC Configuration and User Table

Command	Mode	Function
show voip mgc user-data-table	Exec/ Config	Shows the whole MGC user data table or specified table. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1..max.).
show voip mgc user-data-table-addr *ADDRESS*		
show voip mgc config-data-table	Exec/ Config	Shows the whole MGC config data table.

12.8 Session Initiation Protocol (SIP)

12.8.1 SIP Profiles

This section describes the following SIP profile tables:

- Feature Access Codes Profile
- Application Service Profile
- Dial Plan Profile.

Feature Access Codes Profile

The feature access codes define administrable feature access codes for the VoIP subscribers. A table entry can be referenced by the VoIP Voice CTP object. One default profile always exists.

To configure the feature access profile table use the following commands.

Command	Mode	Function
create voip sip feature-access-codes-profile-table-entry [*LINE*]	Config	Create the feature access codes profile table. **LINE**: descriptive name for profile handling (Size 0..64).
modify voip sip feature-access-codes-profile-table-entry profile-name *INDEX [LINE]*		Modifies the profile name. **INDEX**: index of profile **LINE**: descriptive name for profile handling.
delete voip sip feature-access-codes-profile-table-entry *INDEX*		Deletes the feature access codes profile table.

To modify entries of feature access profile table, use the following commands.

Command	Mode	Function
modify voip sip feature-access-codes-profile-table-entry cancel-call-waiting *INDEX [LINE]*	Config	Modifies table entry ’cancel call waiting’ **INDEX**: index of profile **LINE**: new code for specified parameter, size 0..5
modify voip sip feature-access-codes-profile-table-entry call-hold *INDEX [LINE]*		Modifies table entry ’call hold’.
modify voip sip feature-access-codes-profile-table-entry call-park *INDEX [LINE]*		Modifies table entry ’call park’.
modify voip sip feature-access-codes-profile-table-entry cids-activate *INDEX [LINE]*		Modifies table entry ’cids activate’.
modify voip sip feature-access-codes-profile-table-entry cids-deactivate *INDEX [LINE]*		Modifies table entry ’cids deactivate’.
modify voip sip feature-access-codes-profile-table-entry do-not-disturb-activation *INDEX [LINE]*		Modifies table entry ’do no not disturb activation’.
modify voip sip feature-access-codes-profile-table-entry do-not-disturb-deactivation *INDEX [LINE]*		Modifies table entry ’do no not disturb deactivation’.
modify voip sip feature-access-codes-profile-table-entry do-not-disturb-pin-change *INDEX [LINE]*		Modifies table entry ’do no not disturb pin change’.
modify voip sip feature-access-codes-profile-table-entry emergency-service-number *INDEX [LINE]*		Modifies table entry ’emergency service number’.
modify voip sip feature-access-codes-profile-table-entry intercom-service *INDEX [LINE]*		Modifies table entry ’intercom service’.

To show the feature access codes table use the following command:

Command	Mode	Function
show voip sip fac-codes-table	Exec/ Config	Shows the feature access codes table

Dial Plan Profile

A dial plan profile may be referenced by a SIP user data entry.
To configure a dial plan profile table, use the following commands.

Command	Mode	Function
create voip sip dial-plan-profile-table-entry *<0-65535> <0-65535> <0-3>*	Config	Creates a dial plan profile table. **0 - 65535**: critical dial time-out, common value (default in OMCI) is 4000 ms **0 - 65535**: partial dial time-out, common value (default in OMCI) is 16000 ms **0 - 3**: dial plan format , 0...not defined, 1...H248, 2...NSC, 3...venor specific format.
modify voip sip dial-plan-profile-table-entry *INDEX <0-65535> <0-65535> <0-3>*		Modifies a dial plan profile table entry. **INDEX**: entry index.
modify voip sip dial-plan-profile-table-entry profile-name *INDEX* [*LINE*]		Modifies a dial plan profile name. **LINE**: descriptive name for profile handling.
delete voip sip dial-plan-profile-table-entry *INDEX*		Deletes a dial plan profile table.

To modify a dial plan profile token, use the following command.

Command	Mode	Function
modify voip sip dial-plan-profile-table-entry dialplan-token *INDEX* [*LINE*]	Config	Modifies a dial plan profile table entry 'dialplan token'. **INDEX**: entry index **LINE**: new dial plan token, see Dial Plan Token Format.

To show the dial plan profile profile table, use the following command.

Command	Mode	Function
show voip sip dial-plan-profile-table	Exec/ Config	Shows the network dial plan profile table.

Dial Plan Token Format

ℹ Configuring of dial plan token is only possible for the ONTs G25A and G25E.

The format of dial plan is selected to 1 (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 completes by integrating several separate dial plan token. A dial plan token is a component of the whole dial plan. The length of dial plan token is limited to 28 Byte. For example, with the token:
  Token 1: (***xx|*xx*x.#|*xx*x.*xx#|
  Token 2: *xx*x.*x#|*31*xxxxxxxx|
  Token 3: *xx#|#xx#|*#xx#|#001|x.T)
  the whole dial plan forms:
  (***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 lock/unlock the ONT the new dial plan takes effect.
- The ONT uses its default dial plan before any other dial plan is configured.
  The current default dial plan is:
  (***xx|*xx*x.#|*xx*x.*xx#|*xx*x.*x#|*31*xxxxxxxx|*xx#|#xx#|*#xx#|#001|x.T)
- Configure empty dial plan to the ONT will not replace the current dial plan, although the empty dial plan can be stored in ONT, when the ONT reboots the default dial plan will take effect.
- In addition, in the three dial plan profiles, “Critical dial timeout”, and “Partial dial timeout” are different from each other. In such condition, the last one takes effect.

Application Service Profile

This table defines attributes of calling features used in conjunction with a VoIP line service. An entry may be referenced by one or more entries of the SIP user data table. One default profile always exists. To configure the application service profile table, use the following commands.

Command	Mode	Function
create voip sip appl-service-profile-table-entry <0-63> <0-63> <0-255> <0-15> <0-3> [*LINE*]	Config	Creates application service profile table. Bit clear is disabled and bit set is enabled. **0 - 63:** CID features, a bitmap of caller ID features, the bit position values are: 0x01 Calling Number, 0x02 Calling Name, 0x04 CID blocking (both number and name), 0x08 CID number- Permanent presentation status for number (0 = Public, 1 = Private), 0x10 CID name - Permanent presentation status for name (0 = Public, 1 = Private), 0x20 - Anonymous CID blocking (ACR), 0x40 - 0x80 not used, is set to 0. **0 - 63:** call waiting features, the bit position values are: 0x01 Call waiting, 0x02 Caller ID Announcement, 0x04 - 0x80 not used, is set to 0. **0 - 255:** call processing features, the bit position values are: 0x0001 - 3way, 0x0002 - Call transfer, 0x0004 - Call hold, 0x0008 - Call park, 0x0010 - Do not disturb, 0x0020 - Flash on Emergency Service call. (Flash is to be processed during an Emergency Service call), 0x0040 - Emergency Service originating hold (determines if a call clearing is to be performed on an on-hook during and Emergency Service call), 0x0080 6way, 0x0100 - 0x8000 not used, is set to 0. **0 - 15:** call presentation features, the bit position values are: 0x0001 - Message Waiting Indication Splash Ring, 0x0002 Message Waiting Indication Special Dial tone, 0x0004 - Message Waiting Indication Visual Indication, 0x0008 - Call Forwarding Indication, 0x0010 - 0x8000 not used, is set to 0. **0 - 3:** direct connect features, the bit position values are: 0x01 - direct connect feature enabled, 0x02 - dial tone feature delay option **LINE**: profile name.
modify voip sip appl-service-profile-table-entry <0-63> <0-63> <0-255> <0-15> <0-3>		Modifies application service profile table entry.
modify voip sip appl-service-profile-table-entry profile-name *INDEX* [*LINE*]		Modifies profile name of application service profile table. INDEX: index of profile LINE: descriptive name for profile handling
delete voip sip appl-service-profile-table-entry *INDEX*		Deletes application service profile table. **INDEX**: index.

To modify the application service profile table entries, use the following commands.

Command	Mode	Function
modify voip sip appl-service-profile-table-entry direct-connect-uri *INDEX* [*LINE*]	Config	Modifies table entry ’direct connect uri’. **INDEX**: index of profile **LINE**: new direct connect URI.
modify voip sip appl-service-profile-table-entry conference-factory-uri *INDEX* [*LINE*]		Modifies table entry ’service conference factory’. **LINE**: new service-conference-factory.
modify voip sip appl-service-profile-table-entry bridge-line-agent-uri *INDEX* [*LINE*]		Modifies table entry ’bridge line agent uri’. **LINE**: new direct connect URI.

To show the application service profile table, use the following command.

Command	Mode	Function
show vip sip appl-service-profile-table	Exec/ Config	Shows the application service profile table.

12.8.2 SIP Agent

The VoIP SIP agent configuration data table contains the configuration attributes necessary to establish communication for signaling between a SIP user agent and a SIP server. Each entry may be referenced by one or more SIP user data entries. Each entry is related to one or more TCP/UDP configuration data entries. One default profile always exists. All table entries of one ONT card must use the same profile (only one profile per ONT card possible).

Configuring a SIP Agent

To configure the **SIP** agent configuration data table, use the following commands.

Command	Mode	Function
create voip sip agent-config-data-table *EXP_TIME START_TIME UDP_TCP_PTR* [*OPT*]	Config	Creates SIP agent configuration table. **EXP_TIME**: SIP Registration Expiration **START_TIME**: time (sec.) prior to time-out that SIP agent should start registration process **UDP_TCP_PTR**: TCP/UDP service used for communication service with SIP proxy server **OPT**: parameter for startup configuration only, can not be used for normal configuration.
modify voip sip agent-config-data-table profile-name *INDEX [LINE]*		Modifies the profile name of the agent configuration data table. **INDEX**: profile index **LINE**: descriptive name for profile handling.
delete voip sip agent-config-data-table *INDEX*		Deletes SIP agent configuration table.

Modifying the SIP Agent Parameters

To modify an entry of specified SIP agent profile index, use the following commands.

Command	Mode	Function
modify voip sip agent-config-data-table *IF_INDEX EXP_TIME START_TIME*	Config	Modifies the agent configuration data table. **IF_INDEX**: interface index (similar to **TCP**/**UDP** port) **EXP_TIME**: SIP Registration Expiration **START_TIME**: time (sec.) prior to time-out that SIP agent should start registration process.

Command	Mode	Function
modify voip sip agent-config-data-table proxy-ip-address *INDEX* [*LINE*]	Config	Modifies an IP address in the agent configuration data table. **INDEX**: profile index **LINE**: IP address or URI of the SIP proxy server for SIP signaling messages.
modify voip sip agent-config-data-table outband-proxy-ip-address *INDEX* [*LINE*]		Modifies an IP address in the agent configuration data table. **LINE**: IP address or URI of the SIP outband proxy server.
modify voip sip agent-config-data-table primary-sip-dns *INDEX [LINE]*	Config	Modifies an IP address in the agent configuration data table. **LINE**: IP address of the SIP primary **DNS**. If this value is zero, the Primary SIP DNS should not be used.
modify voip sip agent-config-data-table secondary-sip-dns INDEX [*LINE*]		Modifies an IP address in the agent configuration data table. **LINE**: IP address of the SIP secondary DNS. If this value is zero, the Secondary SIP DNS should not be used.
modify voip sip agent-config-data-table primary-sip-dns-addr *INDEX* A.B.C.D	Config	Modifies an IP address in the agent configuration data table. **A.B.C.D**: IP address of the SIP primary DNS.
modify voip sip agent-config-data-table secondary-sip-dns-addr *INDEX* A.B.C.D		Modifies an IP address in the agent configuration data table. **A.B.C.D**: IP address of the SIP secondary DNS.
modify voip sip agent-config-data-table host-part-uri *INDEX* [*LINE*]	Config	Modifies an IP address in the agent configuration data table. **LINE**: IP address of the SIP host part URI.
modify voip sip agent-config-data-table sip-registrar *INDEX* [*LINE*]	Config	Modifies an IP address in the agent configuration data table. **LINE**: IP address or name of the SIP registrar server for SIP signaling messages. Examples: '10.10.10.10' and 'proxy.voip.net'.
modify voip sip agent-config-data-table sip-softswitch *INDEX* [*LINE*]	Config	Modifies the agent configuration data table. **LINE**: SIP gateways softswitch vendor (4 **ASCII** alphabetical characters [A-Z]) as defined in ANSI T1.220. All NULL characters indicates no particular vendor.
modify voip sip agent-config-data-table udp-tcp-ptr *INDEX PTR*	Config	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. The attribute represents the second index of the VoIP TCP/UDP config data table (the TCP/UDP port). **PTR**: UDP/TCP pointer.

Checking the SIP Agent Configuration

To show SIP agent configuration data table, use the following command.

Command	Mode	Function
show voip sip agent-config-data-table	Exec/ Config	Shows the agent configuration data table.

Checking the SIP Agent Status

To check the SIP agent status, use the following command.

Command	Mode	Function
get voip sip agent-status *ADDRESS*	Config	SIP agent status. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1...max.).

12.8.3 SIP User Data Table

Configuring the SIP User Data Table

The table contains the user specific configuration attributes associated with a specific VoIP CTP. Table entries are created and deleted by the NE. An entry exists for each POTS UNI port using SIP protocol for a VoIP service offering. Table index is the interface index (of the POTS PPTP). All SIP user data entries related to one ONT must refer the same VoIP SIP agent configuration data table entry, see 12.8.2 SIP Agent.

To modify **SIP** user data parameters, use the following commands.

Command	Mode	Function
modify voip sip user-data-table *IF_INDEX* *PTR PWD TME A_PTR FC_PTR REL_TMR ROH_TMR*	Config	Modifies SIP user data table. **IF_INDEX**: interface index (**POTS** PPTP) **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1 to max.) **PTR**: pointer to SIP agent config data table **PWD**: pointer to authentication security method table (0xFFFF no user name/Password) **TME**: voice mail server subscription time (sec.) **A_PTR**: pointer to application service profile table (0xFFFF no application services profile is available) **FC_PTR**: pointer to access code table (0xFFFF no feature access code table is available) **REL_TMR**: release timer (sec.) - 0: use internal default **ROH_PTR**: receive off-hook condition time (sec.).
modify voip sip user-data-table-addr *ADDRESS* *PTR PWD TME A_PTR FC_PTR RL_RMR ROH_TMR*		
modify voip sip user-data-table user-part-aor *INDEX* [*LINE*]		Modifies SIP user identification part. **LINE**: user identification part of the address of records. This can take the form of an alphanumeric string or the directory number used to reference the user in the network.
modify voip sip user-data-table-addr user-part-aor *ADDRESS* [*LINE*]		
modify voip sip user-data-table display-name *INDEX* [*LINE*]		Modifies SIP display name. **LINE**: customer ID used for outgoing SIP messages display attribute in ASCII string format (Size 0..25).
modify voip sip user-data-table-addr display-name *ADDRESS* [*LINE*]		
modify voip sip user-data-table voice-mail-server-sip-uri *INDEX* [*LINE*]		Modifies SIP voice mail server SIP URI. **LINE**: IP address or URI of the SIP voice mail server for SIP signaling messages.
modify voip sip user-data-table-addr voice-mail-server-sip-uri *ADDRESS* [*LINE*]		
modify voip sip user-data-table user-name *INDEX* [*LINE*]		Modifies SIP user name. **LINE**: a SIP user name used for authentication.
modify voip sip user-data-table-addr user-name *ADDRESS* [*LINE*]		
modify voip sip user-data-table user-password *ADDRESS* [*LINE*]		Modifies SIP user password. **LINE**: a SIP user password used for authentication.
modify voip sip user-data-table-addr user-password *ADDRESS* [*LINE*]		

Verifying SIP User Data Table

To show SIP user data parameters, use the following commands.

Command	Mode	Function
show voip sip user-data-table	Exec/ Config	Displays SIP user data table.
show voip sip user-data-table-addr *ADDRESS*		Displays SIP user data table. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1 to max.).

12.8.4 SIP User Dial Plan Mapping

This table maps SIP user data entries to user dial plan entries. First table index is the IF-Index of the SIP user data entry. Second table index is the pointer to a user dial plan entry, see Dial Plan Profile. Each SIP user data entry can refer to a flexible number of user dial plan entries.

Configuring of SIP User Dial Plan Mapping

To configure SIP user dial mapping table entries, use the following commands.

Command	Mode	Function
create voip sip user-dialplan-mapping-table-entry-addr *ADDRESS DIAL_PLAN_INDEX*	Config	Creates a user dial mapping table entry. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1 to max.) **IF_INDEX**: interface index of SIP user data entry (primary index) **DIAL_PLAN_INDEX**: user dial plan index.
create voip sip user-dialplan-mapping-table-entry *IF_INDEX DIAL_PLAN_INDEX*		
delete voip sip user-dialplan-mapping-table-entry *IF_INDEX DIAL_PLAN_INDEX*		Deletes a user dial mapping table entry.
delete voip sip user-dialplan-mapping-table-entry-addr *ADDRESS DIAL_PLAN_INDEX*		

Verifying the SIP User Dialplan Mappings

To verify SIP user dial mapping table, use the following command.

Command	Mode	Function
show voip sip user-dialplan-mapping-table	Exec/ Config	Shows the user dialplan mapping table.

12.8.5 SIP Performance Monitoring

Configuring of PM Thresholds

To configure VoIP SIP performance thresholds, use the following commands.

Command	Mode	Function
create voip-performance sip-agent-pm threshold <2-16> *RXINVITEREQ RXIVITREQRETRANS RXNONIVITEREQ RXNONINVITEREQRETRANS RXRESP RXRESPRTRANS SEVERITY*	Config	Creates threshold table for SIP agent performance monitoring. **2 - 16**: table index **RXINVITEREQ**: threshold for ReceiveInviteReq **RXIVITREQRETRANS**: threshold for ReceiveInviteReqRetrans **RXNONIVITEREQ**: threshold for ReceiveNonInviteReq **RXNONINVITEREQRETRANS**: threshold for ReceiveNonInviteReqRetrans **RXRESP**: threshold for ReceiveResp **RXRESPRTRANS**: threshold for ReceiveRespretrans **SEVERITY**: pointer to alarm severity alarm.
modify voip-performance sip-agent-pm threshold <1-16> *RXINVITEREQ RXIVITREQRETRANS RXNONIVITEREQ RXNONINVITEREQRETRANS RXRESP RXRESPRTRANS SEVERITY*		Modifies threshold table for SIP agent performance monitoring. **1 - 16**: table index.
delete voip-performance sip-agent-init-pm threshold <2-16>		Deletes threshold table for SIP agent performance monitoring.

Command	Mode	Function
create voip-performance sip-call-init-pm threshold <2-16> *FAILEDTOCONNECT FAILEDTOVALIDATE TIMEOUT FAILURERECEIVED FALILEDTOAUTENTICATE SEVERITY*	Config	Creates threshold table for SIP agent performance monitoring. **2 - 16**: table index **FAILEDTOCONNECT**: threshold for FailedToConnect **FAILEDTOVALIDATE**: threshold for FAILEDTO Validate **TIMEOUT**: threshold for Time-out **FAILURERECEIVED**: threshold for FailureReceived **FALILEDTOAUTENTICATE**: threshold for FailedTAuthorizstion **SEVERITY**: pointer to alarm severity alarm.
modify voip-performance sip-call-init-pm threshold <1-16> *FAILEDTOCONNECT FAILEDTOVALIDATE TIMEOUT FAILURERECEIVED FALILEDTOAUTENTICATE SEVERITY*		Modifies threshold table for SIP agent performance monitoring. **1 - 16**: table index.
delete voip-performance sip-call-init-pm threshold <2-16>		Deletes threshold table for SIP agent performance monitoring.

Configuring of PM Objects

To configure VoIP SIP performance objects, use the following commands.

ℹ See 10.10.2 Calculation Algorithms for PM Objects for information on the PM object indexes.

Command	Mode	Function
create voip-performance sip-agent-pm object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>	Config	Creates **SIP** agent performance monitoring. **INDEX**: object index, physical index of ONT card **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT slot **lock/unlock**: deactivates/activates performance monitoring (admin state 15 min.) **lock/unlock**: deactivates/activates performance monitoring (admin state 24 h) **0 - 96**: history size 15 min., number of history entries for the PM object and the interval type **0 - 1**: history size 24 h., number of history entries for the PM object and the interval type **1 - 16**: pointer to the threshold object.
create voip-performance sip-agent-pm object-addr *ADDRESS* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		
modify voip-performance sip-agent-pm object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> 1-16>		Modifies the SIP agent performance monitoring object table.
modify voip-performance sip-agent-pm object-addr *ADDRESS* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		
delete voip-performance sip-call-agent-pm object *INDEX*		Deletes object table for SIP agent performance monitoring.
delete voip-performance sip-call-agent-pm object-addr *ADDRESS*		
create voip-performance sip-call-init-pm object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>	Config	Creates SIP agent performance monitoring. **INDEX**: object index, physical index of ONT card **lock/unlock**: deactivates/activates performance monitoring (admin state 15 min.) **lock/unlock**: deactivates/activates performance monitoring (admin state 24 h.) **0 - 96**: history size 15 min., number of history entries for the PM object and the interval type **0 - 1**: history size 24 h, number of history entries for the PM object and the interval type **1 - 16**: pointer to the threshold object.
modify voip-performance sip-call-init-pm object *INDEX* { lock I unlock } { lock I unlock } <0-96> <0-1> <1-16>		Modifies SIP agent performance monitoring.
delete voip-performance sip-call-init-pm object *INDEX*		Deletes object table for SIP agent performance monitoring.

Checking the SIP Agent PM Tables

To show VoIP SIP performance objects, use the following commands.

Command	Mode	Function
show voip-performance sip-agent-pm object-table	Exec/ Config	Displays object table for SIP agent performance monitoring.
show voip-performance sip-call-init-pm object-table		Displays object table for SIP call init monitoring.
show voip-performance sip-agent-pm threshold-table		Displays threshold table for SIP agent performance monitoring.
show voip-performance sip-call-init-pm threshold-table		Displays threshold table for SIP call init monitoring.

Updating and Verifying SIP Agent PM Data

To update VoIP SIP performance data, use the following command.

Command	Mode	Function
update voip-performance sip-agent-pm current-data *INDEX*	Config	Updates the SIP agent PM current data table. **INDEX**: object index.

To show VoIP SIP performance data, use the following commands.

Command	Mode	Function
show voip-performance sip-agent-pm current-data-table	Exec/ Config	Displays current data table for SIP agent PM.
show voip-performance sip-agent-pm history-data-table		Displays history data table for SIP agent PM.
show voip-performance sip-call-init-pm current-data-table		Displays current data table for SIP call init monitoring.
show voip-performance sip-agent-pm history-data-table		Displays history data table for SIP call init monitoring.

12.8.6 Checking the User Status Information

Use the following commands to check information about a single SIP user (POTS port).

Command	Mode	Function
get voip sip user-status port *ADDRESS*	Exec/ Config	Starts a request of the SIP user status attributes for the specified port. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/port number (POTS port number 1 to max.).
show voip sip user-status port *ADDRESS*		Shows the attributes of operation state, voice server status, and SIP agent status for the specified port.

Use the following commands to check information about all SIP users (POTS ports) of an ONT.

Command	Mode	Function
get voip sip user-status onu *ADDRESS*	Exec/ Config	Starts a request of the SIP user status attributes for all user ports of specified ONT. **ADDRESS**: OLT-slot/GPON-port/ONT-ID/ONT-slot/ONT-port.
show voip sip user-status onu *ADDRESS*		Shows the attributes of operation state, voice server status, and SIP agent status for all user ports of specified ONT.

Use the following command to stop a running SIP user status request.

Command	Mode	Function
clear get voip sip user-status	Exec/ Config	Stops a running SIP user status request.

12.8.7 Verifying SIP Error Codes

To show SIP error codes, use the following command.

Command	Mode	Function
show sip error-codes	Exec/ Config	Shows all possible error codes for SIP.

13 MAC

13.1 Setting the GPON MAC Mode

ℹ Before changing the MAC mode, the CXU must be unlocked and all interface units (IU_GPON, IU_1x10G, IU_10x1G) must be locked.

Command	Mode	Function
gpon-mac-mode { vid I mac I enhanced-mac }	Bridge	Configures the GPON **MAC** mode (**all IUs must be locked**). **vid**: (**VLAN** mode) mapping of VLANs to **GEM ID** is configured (downstream and upstream) by the outer tag. VLAN translation between subscriber VLANs and service based VLANs is not possible. **mac**: (MAC mode) downstream: mapping of MAC address to GEM ID is learned from upstream frames. VLAN translation between subscriber VLANs and service based VLANs is possible. **enhanced-mac**: 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).
modify gpon-mac-mode { vid I mac I enhanced-mac }		Configures the GPON MAC mode (**all IUs must be locked**). **vid**: (VLAN mode) mapping of VLANs to GEM ID is configured (downstream and upstream). **mac**: (MAC mode) downstream: mapping of MAC address to GEM ID is learned from upstream frames. **enhanced-mac**: MAC mode with special features, see above.
show base-settings	Config/ Bridge	Displays GPON MAC mode and prio map range.

Example:

```
SWITCH(config)# show base-settings
gpon mac mode  : (enhanced) mac
prio map range : 4
SWITCH(config)#
```

13.2 Configuring of Priority Mapping Profiles

The priority mapping profile defines the translation from a tag priority to another, depending on the MAC mode was defined for a certain VLAN.
Use the following command to set the priorities of traffic flows in an “enhanced MAC mode” environment.

Command	Mode	Function
prioprofilemap modify *INPRIOOUT OUTPRIOOUT*	Bridge	Modifies a entry of the priority mapping profile. **INPRIOOUT**: 0..7 with 0 = not applicable for this MAC mode **OUTPRIOOUT**: 0..7 If the **NNI** is single tagged, OUTPRIOOUT means the only tag at the NNI. In this case INPRIOOUT is not used.
show prioprofilemap	Bridge	Shows information about the current priority mapping for VLANs in cross-connect.

Example:

```
SWITCH(config)#
SWITCH(config)# bridge
SWITCH(bridge)# show prioprofilemap

Prio in | Inner prio | Outer prio
----------------------------------
   0    |     0      |     0
   1    |     1      |     1
   2    |     2      |     2
   3    |     3      |     3
   4    |     4      |     4
   5    |     5      |     5
   6    |     6      |     6
   7    |     7      |     7

SWITCH(bridge)#
```

13.3 Configuring of CoS Mapping Profiles

The **CoS** mapping profile sets for the inner VLAN the priorities per GEM port of the ONU. The MAC mode defined for a certain VLAN depends on the priority values of this profile. Use the following commands to configure the CoS mapping profile.

Command	Mode	Function
cosprofilemap *INPRIOOUT*	Bridge	Creates a CoS mapping profile with an index given by system. The maximum number of profiles is 64. **INPRIOOUT**: 4 character string of priority values. Valid values are from 0..7. Setting of default profile: 0, 2, 4, 6.
no cosprofilemap *COSPROFILE*		Deletes the specified CoS profile. **COSPROFILE**: profile index. A profile that is assigned to a VLAN cannot be deleted.
show cosprofilemap [*COSPROFILE*]	Bridge	Shows information about all or specified CoS mapping profile. **COSPROFILE**: profile index.

Examples:

Verifying the CoS mapping profiles with show-command (only default profile #1 is present):

```
SWITCH(bridge)# show cosprofilemap

Profile | Number   | Inner prio Out
------------------------------------
   1    |    0     |     0
        |    1     |     2
        |    2     |     4
        |    3     |     6
```

Creating a CoS mapping profile (profile index #2) with priority values 0, 1, 2, 3:

```
SWITCH(bridge)# cosprofilemap 0123
SWITCH(bridge)# show cosprofilemap
Profile | Number   | Inner prio Out
------------------------------------
```

```
   1     |     0     |     0
         |     1     |     2
         |     2     |     4
         |     3     |     6
-----------------------------------
   2     |     0     |     0
         |     1     |     1
         |     2     |     2
         |     3     |     3
```

Deleting the CoS mapping profile #2:

```
SWITCH(bridge)# no cosprofilemap 2
SWITCH(bridge)# show cosprofilemap

Profile | Number   | Inner prio Out
-----------------------------------
   1     |     0     |     0
         |     1     |     2
         |     2     |     4
         |     3     |     6
```

13.4 Configuring of Enhanced MAC Modes

The following commands configure the VLAN ID mapping table which determines the translation from a tagged VLAN to another in order to define rules of traffic aggregation, security in the last mile and traffic shaping.

ℹ If in an OLT running in enhanced MAC mode IU_GPON cards that were offline configured start up, the VLANs using this MAC mode will be sent to such IU_GPONs. For online configuration the enhanced MAC mode must be enabled and the IU_GPONs must be ready for service.

13.4.1 N : 1 Bridge Mode

In an N:1 VLAN scenario, several subscriber share one VLAN for one service. The CoS classification depends on the .1p priority bits.

Use the following command to configure the enhanced MAC mode 1.

Command	Mode	Function
enhanced-mode nto1-ChangeVlanPerC-tag *VLANID CHANGEDVID PRIOPROFILE*	Bridge	Adds or modifies an entry in the VLAN mapping table. MAC mode 1 (N:1) - changing VLAN per c-tag. **VLANID**: VLAN-ID (customer c-tag) **CHANGEDVID**: VLAN-ID (service s-tag) **PRIOPROFILE**: index of priority mapping profile.

13.4.2 1: 1 VLAN Cross-Connect Mode

The c-tag incoming from UNI side contains the service information. That means 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. Therefore, the GPON-MAC provides two translation tables. The first one is used for the translation of the c-tag information into the related s-tag information at the NNI. The second one is needed, to translate the ID part of GEM-port, which is related to the UNI-port, into the inner s-tag VID at the NNI side.

Therefore, the configuration of 1:1 cross-connect (CC) mode is divided into the two configuration tasks:

– per GPON port
– per subscriber port

The following commands must be used always in conjunction to configure the enhanced MAC mode 2.

Command	Mode	Function
enhanced-mode 1to1-CCAddOuterPerC-tag *VLANID PONPORT OUTERVID PRIOPROFILE*	Bridge	Adds or modifies an entry in the VLAN mapping table. MAC mode 2 (1:1- cross-connect by adding outer tag (service tag) per c-tag. **VLANID**: port VID **PONPORT**: slot/port **OUTERVID**: service VID **PRIOPROFILE**: index of priority mapping profile.
enhanced-mode 1to1-CCChangeInnerPerPort { *VLANID* | all } *SUBSCRPORT INNERVID COSPROFILE*	Bridge	Adds or modifies an entry in the VLAN mapping table. **all**: all VLANs **VLANID**: port VID **SUBSCRPORT**: slot/port/ONU-ID/ONU-slot / ONU-port **INNERVID**: inner VLAN-ID **COSPROFILE**: CoS profile index 1..64,

13.4.3 Disabling the Enhanced MAC Mode of VLAN

To disable the enhanced mode of a VLAN, use the following command.

Command	Mode	Function
no enhanced-mode *VLANIDS* [*PORT*]	Bridge	Deletes an entry in the VLAN mapping table. **VLANIDS**: specify VLANs **PORT**: slot/port [/ONU-ID/ONU-slot/ONU-port].

13.4.4 Checking VLAN Mapping Information

Command	Mode	Function
show vidmap { database | subscriber } [*VLANID*]	Config/ Bridge	Shows information of all or specified VLAN. **database**: shows all configured VID map table entries **subscriber**: shows the translation for the subscriber, depending on the VLAN table.

13.4.5 Modifying the MAC Mode of VLAN

Use the following commands to read or modify the MAC mode parameters of a VLAN.

Command	Mode	Function
macmode *VLANID MODE*	Bridge	Defines a behavior per VLAN, based on configurations defined by the previous **prioprofilemap** command. Modifies the MAC mode value of specified VLAN. **VLANID**: enter the VLAN-ID **MODE**: number of MAC mode to be new set for the specified VLAN: 1 = N:1 bridge mode 2 = 1:1 VLAN cross-connect mode with tagged uses frames.
show macmode *VLANID*	Config/ Bridge	Shows the current MAC mode of specified VLAN-ID.

Changing a VLAN to Enhanced MAC Mode

Perform the following tasks in order to change the MAC mode of VLAN:

1. Check if the VLAN fulfills the requirements for the new MAC mode.
2. Change the GPON MAC mode. The existing VID mapping entries will be deleted automatically.
3. Create default VID mapping entries.

Example:

The following commands set the MAC in enhanced mode and assign the MAC mode 2 to VLAN 100:

```
SWITCH(bridge)#gpon-mac-mode enhanced-mac
SWITCH(bridge)#show base-settings
SWITCH(bridge)#macmode 100 2
SWITCH(bridge)#show macmode 100
```

13.5 MAC Table

There are two hardware address types that are registered in a MAC table: dynamic MAC addresses and static MAC addresses. A static MAC address can be configured by the operator and remains unaffected even after the system was rebooted. Dynamic MAC address entries of this table are formed during a learning process in upstream direction.

13.5.1 Dynamic Addresses

Enabling of Address Learning

Dynamic addresses are automatically added to the MAC table and dropped from it when they are not in use.

Command	Mode	Function
mac learning-uplink { enable I disable }	Bridge	MAC learning configuration (only uplinks affected). **enable** (default) / **disable** MAC address learning on uplink ports .

MAC Aging-Time

If an **NE** was not accessed during a specified interval called “MAC aging-time”, its registered MAC address will be deleted from the table.

Command	Mode	Function
mac aging-time <10-4080>	Bridge	Sets the maximum amount of time a dynamically "learned". MAC address remains in the MAC table. **10 - 4080**: aging time in seconds (default value is 300 s).
show mac aging-time	Bridge	Shows the aging time.

Clearing dynamically Addresses

A dynamic address can also be deleted manually from MAC table when it is unnecessary.

Command	Mode	Function
clear mac	Bridge	Deletes the specified dynamically address(es) from MAC table. **NAME**: enter the bridge name **PORT**: enter the port number **XX.XX...**: enter the MAC address.
clear mac *NAME*		
clear mac *NAME PORT*		
clear mac *NAME PORT XX:XX:XX:XX:XX:XX*		

13.5.2 Static Addresses

From *Bridge configuration* mode, use the following command to manage static address entries of a MAC table.

Command	Mode	Function
mac *NAME PORT* XX:XX:XX:XX:XX:XX	Bridge	Registers static address in MAC table. **NAME**: enter the bridge name **PORT**: enter the port number **XX:XX...**: enter the MAC address.

Example of registering the MAC address 00:01:02:9a:61:17 in port 12 of MAC table for VLAN 1:

```
SWITCH(bridge)#mac 1 12 00:01:02:9a:61:17
SWITCH(bridge)#
```

Unnecessary static MAC addresses will not be removed regardless after the cycle of MAC aging time. They have to be removed manually. In another case, if an static MAC address needs to be assigned to a new port, this MAC address must first be deleted from the MAC address table in order to assign it afterwards to the other interface.

Command	Mode	Function
no mac	Bridge	Deletes the specified static address(es) from MAC table. **NAME**: enter the bridge name. **PORT**: enter the port number. **XX.XX...**: enter the MAC address.
no mac *NAME*		
no mac *NAME PORT*		
no mac *NAME PORT XX:XX:XX:XX:XX:XX*		

13.5.3 Showing MAC Table Information

ℹ Up to 32k (CXU_VR) of MAC addresses can be registered in a MAC table. Hence, it is difficult to find out the information you need at one sight. When the **show** command is executed, only a small number of addresses will be displayed. If the line

-more- appears, press any key to search more. After you have found the needed information, press q to go back to the system prompt without displaying the other table entries.

Command	Mode	Function
show mac vlan *NAME*	Exec/ Config/ Bridge	Shows MAC addresses selected by VLAN (MAC address learned at IU only are invisible). **NAME**: VLAN name **PORT**: port number.
show mac vlan *NAME PORT*		
show mac vlan *NAME PORT* **detail**	Bridge	Shows MAC table details with ONU index, selection by VLAN (MAC addresses learned at IU only are invisible), **NAME**: VLAN name **PORT**: port number.

Example of showing the MAC address of destination, specified port number, VLAN ID, and time the address is registered in table.

The first table entry is the switches own MAC address and hence is the permission static.

```
SWITCH (bridge)# show mac 1 12

port (id)      mac addr           permission   in use

eth24(12)    00:01:02:9a:61:1a  static      0.00

eth24(12)    00:10:5a:84:46:76  OK          0.01

eth24(12)    00:e0:4c:1a:37:17  OK          0.07

eth24(12)    00:d0:cb:0a:a0:b7  OK          0.15

eth24(12)    00:c0:ca:33:5b:90  OK          0.18

eth24(12)    00:03:47:70:e3:30  OK          0.50

 (omitted)
SWITCH (bridge)#
```

14 Bridges

The bridge configuration is described in the following chapters:

- Configuring the Bridge Base
- Configuring of Bridge Ports
- Port Mirroring.

14.1 Configuring the Bridge Base

This chapter describes commands which are set the switching mode, tagging mode, and residential mode of **CXU**, **IU**, and **ONU**.

14.1.1 Common Bridge Base Commands

The following command takes effect without restriction of a specific OLT card.

Command	Mode	Function
bridgebase outerEtherType *ETHERTYPE*	Bridge	Sets QinQ encapsulation configurable outer tag ethertype without CXU specific scope. **ETHERTYPE**: 0x8100, 0x88a8, 0x9100 or 0x9200.

14.1.2 CXU Bridge

Command	Mode	Function
bridgebase cxu bridgemode { basic I diffserv I enhanced }	Bridge	Configures the general mode of the CXU bridge that will influence some QoS-features.
bridgebase cxu switching-mode { independent-vlan-learning I shared-vlan-learning I vlan-switching }	Bridge	Configures bridgebase outer tagging. **vlan-switching:** no learning of MAC addresses, all frames are flooded in their VLANs **independent-vlan-learning:** bridge learns MAC addresses. MAC addresses must be unique for all VLANs. **shared-vlan-learning:** bridge learns MAC addresses and all existing VLANs. MAC addresses must be unique in one VLAN.
bridgebase cxu taggingmode { single I double }	Bridge	Configures the taggingmode of CXU. **single**: bridgebase tagging mode - single **double**: bridgebase tagging mode - double.
bridgebase cxu residential-mode { on I off }	Bridge	Configures the **CXU** residential mode. **on**: internal routing of frames between subscribers is disabled (default setting) **off**: internal routing of frames between subscribers is enabled if not separated by VLAN.
bridgebase cxu outertagging *PVID PRIORITY*	Bridge	Sets the outertag defaults. **PVID**: default outer **PVID** **PRIORITY**: default outer tag priority.
bridgebase cxu outerEtherType *ETHERTYPE*	Bridge	Sets QinQ encapsulation configurable outer tag ethertype with/without CXU specific scope. **ETHERTYPE**: 0x8100, 0x88a8, 0x9100 or 0x9200
bridgebase cxu dlf-filter { enable I disable }	Bridge	Configures destination-lockup-failure filter. **enable**: destination-MAC unknown unicast towards subscriber ports blocked. **disable**: destination-MAC unknown unicast towards subscriber ports allowed.

Command	Mode	Function
show bridgebase cxu	Privileged/ Config/ Bridge	Displays bridge base for CXU.

14.1.3 Bridge of Interface Unit

Command	Mode	Function
bridgebase iu *IUSLOT* **switching-mode** { independent-vlan-learning I shared-vlan-learning I vlan-switching }	Bridge	Configures bridgebase IU outertagging. **IUSLOT**: slot in main shelf **vlan-switching**: no learning of MAC addresses, all frames are flooded in their VLANs (switch key VLAN) **independent-vlan-learning**: bridge learns MAC addresses. MAC addresses must be unique for all VLANs (switch key MAC+ VLAN) **shared-vlan-learning**: bridge learns MAC addresses and all existing VLANs. MAC addresses must be unique in one VLAN (switch key MAC).
bridgebase iu *IUSLOT* **bridgemode** { basic I diffserv I enhanced }	Bridge	Configures general mode of the bridge that will influence some QoS-features. **IUSLOT**: slot in main shelf.
bridgebase iu *IUSLOT* **taggingmode** { single I double }	Bridge	Configures bridgebase IU tagging mode. Double tagging affects only the GPON uplink interfaces, not the hiG interlink interfaces to CXU. **IUSLOT**: slot in main shelf **single**: bridgebase tagging mode - single **double**: bridgebase tagging mode - double.
bridgebase iu *IUSLOT* **residential-mode** { on I off }	Bridge	Configures bridgebase IU residential mode. **IUSLOT**: slot in main shelf **on**: no traffic between GPON links possible (default) **off**: traffic between GPON links possible.
show bridgebase iu *IUSLOT*	Privileged/ Config/ Bridge	Displays bridge base for IUs on specified slot: **IUSLOT**: slot in main shelf.

14.1.4 ONU Bridge

Command	Mode	Function
bridgebase onu *ONU* **switching-mode** { independent-vlan-learning I shared-vlan-learning I vlan-switching }	Bridge	Configures bridgebase ONU switching mode. ONU: ONU address (IU slot/GPON link/ONU ID) **vlan-switching**: no learning of MAC addresses, all frames are flooded in their VLANs (switch key VLAN) **independent-vlan-learning**: bridge learns MAC addresses. MAC addresses must be unique for all VLANs (switch key MAC+ VLAN) **shared-vlan-learning**: bridge learns MAC addresses and all existing VLANs. MAC addresses must be unique in one VLAN (switch key MAC).
bridgebase onu *ONU* **residential-mode** { on I off }	Bridge	Configures bridgebase **ONT** residential mode. **ONU**: ONU address (IU slot/GPON link/ONU ID) **on**: no traffic between GPON links possible **off**: traffic between GPON links possible.
show bridgebase onu [*ONU*]	Privileged/ Config/ Bridge	Displays bridge base for ONU. **ONU**: address (IU slot/GPON link/ONU ID).

14.2 Configuring of Bridge Ports

14.2.1 Tagging Rules

Tagging rules are defined for upstream direction. Each table entry represents a tagging rule, consisting of a filtering part and a treatment part. The filtering part must be unique.

There are three categories of rules: zero-tag, single-tag and double-tag rules. Logically, these categories are separate, and apply to their respective incoming frame types. Single tag rules have a filter outer prio = 15. zero-tag rules have both filter priority fields = 15.

The tagging rule table has 3 default entries that list the default treatment (of normal forwarding) for untagged, single tagged, and double tagged frames. As an exception to the ordered processing, these default rules are always considered as a last resort for frames that do not match any other applicable rule. The 3 default entries can neither be deleted nor modified.

Use the following commands to configure tagging rules.

Command	Mode	Function
taggingrule create <0-15> <0-4096> <0-7> <0-15> <0-4096> <0-7> <0-3> <0-2> <0-15> <0-4097> <0-7> <0-15> <0-4097> <0-7>	Bridge	Creates an entry of tagging rule table (free running rule index). **0 - 15**: filter outer prio 0-7: the given outer priority to filter the received frames 8: indicates not to filter on outer priority 14: indicates the default filter when no other double-tag rule in this table applies 15: indicates that this entry is not a double-tag rule and all other outer tag filter fields should be ignored. **0 - 4096**: filter outer VID (0..4094, 4096 indicates not to filter on the outer VID) **0 - 7**: filter outer TPID 0: do not filter on outer TPID field 4: outer TPID = 8100 5: outer TPID = input TPID, “don’t care” about DE bit 6: outer TPID = input TPID, DE=0 7: outer TPID = input TPID, DE=1 **0 - 15**: filter inner prio 0-7: the given inner priority value to filter the received frames 8: indicates not to filter on inner priority 14: indicates the default filter when no other one-tag rule in this table applies 15: indicates that this entry is the no-tag rule **0 - 4096**: filter inner VID (0..4094, 4096: indicates not to filter on the inner VID) **0 - 7**: filter inner TPID 0: do not filter on inner TPID field 4: inner TPID = 8100 5: inner TPID = input TPID, “don’t care” about DE bit 6: inner TPID = input TPID, DE=0 7: inner TPID = input TPID, DE=1 **0 - 3**: filter EtherType **0 - 2**: indicates that 0, 1, or 2 treat tags, respectively, are to be removed. If one tag is specified, then it is the outer tag that should be removed. **0 - 15**: treat outer prio 0-7: the given priority to insert in the outer VLAN tag 8: the outer priority is to be copied from the inner priority of the received frame 9: the outer priority is to be copied from the outer priority of the received frame 15: do not add an outer tag **0 - 4097**: treat outer VID (0..4094; 4096: the outer VID is to be copied from the inner VID of the received frame; 4097: the outer VID is to be copied from the outer VID of the received frame) **0 - 7**: treat outer TPID 0: TPID (and DE, if present) copied from inner tag of received frame 1: TPID (and DE, if present) copied from outer tag of received frame 2: TPID = output TPID, and DE copied fron inner tag of received frame 3: TPID = output TPID, and DE copied from outer tag of received frame 4: TPID = 0x8100 6: TPID = output TPID, DE=0 7: TPID = output TPID, DE=1 **0 - 15**: treat inner prio 0-7: the given priority to insert in the inner VLAN tag 8: the inner priority is to be copied from the inner priority of the received frame 9: the inner priority is to be copied from the outer priority of the received frame 15: do not add an inner tag **0 - 4097**: treat inner VID (0..4094; 4096: the inner VID is to be copied from the inner VID of the received frame; 4097: the inner VID is to be copied from the outer VID of the received frame) **0 - 7**: treat inner TPID, meaning of values as specified for treat outer TPID.
taggingrule <1-255> **create** <0-15> <0-4096> <0-7> <0-15> <0-4096> <0-7> <0-3> <0-2> <0-15> <0-4097> <0-7> <0-15> <0-4097> <0-7>		Creates an entry of tagging rule table with specific index. **1 - 255**: index of tagging rule.

Command	Mode	Function
taggingrule modify <1-255> <0-15> <0-4096> <0-7> <0-15> <0-4096> <0-7> <0-3> <0-2> <0-15> <0-4097> <0-7> <0-15> <0-4097> <0-7>	Bridge	Modifies values of specified tagging rule.
taggingrule delete <1-255>		Deletes the specified tagging rule.

Use the following command to verify the tagging rule table.

Command	Mode	Function
show taggingrule table	Bridge	Displays information of tagging rule table.

14.2.2 Enhanced Tagging Profile

An enhanced tagging profile contains a list of tagging rules that are assigned to ONT subscriber bridge ports.

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 that rule.

If enabled, 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, 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.

Command	Mode	Function
enhtagprofile create *NAME ITPID OTIPD* <0-1> *RULELIST*	Bridge	Creates an enhanced tagging profile, Besides a free running profile index, an enhanced tagging profile can be also created through a specific index. **NAME**: name of profile **ITPID**: inner TPID value for operations on the input (filtering) side of the profile **OTIPD**: outer TPID for operations on the output (tagging) side of the profile. Typical values for ITPID ans OTIPD include 0x8a88 and 0x9100. **0 - 1**: downstream mode 0 - downstream operation is performed as described above. 1 - no operation is performed in the downstream direction **RULELIST**: index of tagging rule table (1.. 255) **1 - 65535**: index of enhanced tagging profile.
enhtagprofile <1-65535> **create** *NAME ITPID OTIPD* <0-1> *RULELIST*		
enhtagprofile modify <1-65535> *ITPID OTIPD* <0-1> *RULELIST*		Modifies parameters of specified enhanced tagging profile.
enhtagprofile delete <1-65535>		Deletes the specified enhanced tagging profile.

Use the following command to verify the enhanced tagging profiles.

Command	Mode	Function
show enhtagprofile table	Bridge	Displays information of enhanced tagging profiles.

14.2.3 DSCP-to-Dot1p Mapping Profile

A **DSCP** to .1p mapping profile is necessary dependent on the configured tagging mode of the bridge port (see 14.2.4 Bridge Port Parameters) as follows. If ingress packets are already tagged (tagging mode is “tagged”) and the port priority is DSCP, the profile will be used to filter frames with allowed .1p priority bits. If the tagging mode is set “untagged” or “transparent” and the port priority is DSCP, a tag will be added to user’s upstream frames. One default profile always exists and cannot be deleted but modified. Use the following commands to manage up to 16 DSCP to .1p mapping profiles.

Command	Mode	Function
dscp-dot1p-map-profile create [[*PROFID* [[*DSCPPOS DSCPFIELD*]]]	Bridge	Creates a new profile. **PROFID:** profile ID (1 to 16) of DSCP-dot1p-map-profile (0 means looking for next free entry) **DSCPPOS:** start index in map table for next parameter (undeclared .1p elements have prio 0) **DSCPFIELD:** character string with characters between 0 and 7, e.g. 112270123.
dscp-dot1p-map-profile modify *PROFID DSCPPOS DSCPFIELD*		Modifies a profile.
dscp-dot1p-map-profile delete *PROFID*		Deletes a profile.
show dscp-dot1p-map-profile [*PROFID*]	Privileged/ Config/ Bridge	Displays DSCP .1p map profile.

14.2.4 Bridge Port Parameters

Use the following commands to configure the ONT bridge port parameters.

Command	Mode	Function
bridgeport *PORTS* **taggingmode** { off I tagged I untagged I transparent I enhanced }	Bridge	Configures bridge port tagging mode. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **off**: untagged, tagged and double tagged frames are forwarded unchanged **tagged**: tagged and double tagged frames are forwarded, untagged frames are dropped **untagged**: untagged frames are forwarded, tagged and double tagged frames are dropped **transparent**: add a tag frame, untagged -> tagged, tagged -> double tagged (0x8100) Q-in-Q **enhanced**: ONT bridge ports are tagged according tagging profile.
bridgeport *PORTS* **enhtaggprof** <1-65535>	Bridge	Sets enhanced tagging profile for bridge port. **1 - 65535**: enhanced tagging profile index, see 14.2.2 Enhanced Tagging Profile for more information.
no bridgeport *PORTS* **enhtaggprof**		Deletes the enhanced tagging profile from port.
bridgeport *PORTS* **pvid** *PVIDS*	Bridge	Configures **PVID**. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **PVIDS**: list of PVIDs, e.g., 101-172, 101.

Command	Mode	Function
bridgeport *PORTS* **priority** *PRIORITY*	Bridge	Sets new priority for bridgemode. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **PRIORITY**: .1p priority (0-7).
bridgeport *PORTS* **priority-option dot1p** *PRIORITY*		Configures bridgeport priority option. Incoming frames gets configured .1p. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **PRIORITY**: .1p priority (0-7).
bridgeport *PORTS* **priority-option dscp** *DSCPPROFILE*		Sets **DSCP** mode for bridgeport priority option. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **DSCPPROFILE**: DSCP-to .1p profile ID See 14.2.3 DSCP-to-Dot1p Mapping Profile for more information.
bridgeport *PORTS* **host-protocol** { none I dhcp I pppoe I dhcp-pppoe }	Bridge	Configures host configuration protocol. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20. **none**: no host protocol **dhcp**: **DHCP** host protocol **pppoe**: **PPPoE** host protocol **dhcp-pppoe**: DHCP and PPPoE host protocol See 18 DHCP and PPPoE for more information.
bridgeport *PORTS* **circuitid** *CIRCUITID*	Bridge	Configures DHCP circuit ID, needed for special Options in DHCP or PPPoE. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/72/1,0/1 **CIRCUITID**: DHCP circuit ID (“““““ means no circuit ID) See 18.4 DHCP Option 82 / PPPoE Option 105 for more information.
bridgeport *PORTS* **maxhosts** *MAXHOST*	Bridge	Configures maximum number of usable MAC addresses per subscriber port. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20 **MAXHOSTS**: max. value for learned MAC per port.
no bridgeport *PORTS* **maxhosts**		Deletes max hosts.
bridgeport *PORTS* **mode** { ipoa I ipoe | vcc-aggr { enable | disable } }	Bridge	Configures mode of this bridgeport **IPoE** or **IPoA**. The activation of mode IPoA is only possible, if a default gateway in the corresponding VLAN-table entry (PVID) is configured. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20 **ipoa**: **IPoA** mode **ipoe**: **IPoE** mode **vcc-aggr**: **VCC** aggregator can be enabled/disabled.
bridgeport *PORTS* **srcmacaddr** { auto I *SRCMACADR* }	Bridge	Configures source for MAC address if this port is running in **IPoA** mode. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20 **auto**: no source **MAC** address configuration for IPoA **SRCMACADR**: source MAC address, e.g., 00:11:22:33:44:55.
no bridgeport *PORTS* **srcmacaddr**		Deletes source for MAC address for IPoA,
bridgeport *PORTS* **ethertype** { disable | enable *IPoE-VLAN IPoE-Prio ARP-VLAN ARP-Prio PPPoE-VLAN PPPoE-Prio* }	Bridge	Configures ethertype based tagging. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20 **disable**: disables ethertype based tagging **enable**: enables ethertype based tagging (IPoE, **ARP**, **PPPoE**) **IPoE-VLAN**: TCI's VLAN value for upstream tagging of IPoE frames **IPoE-Prio**: TCI's priority value for upstream tagging of IPoE frames **ARP-VLAN**: TCI's VLAN value for upstream tagging of ARP frames **ARP-Prio**: TCI's priority value for upstream VLAN tagging of ARP frames **PPPoE-VLAN**: TCI's VLAN value for upstream tagging of PPPoE frames **PPPoE-Prio**: TCI's priority value for upstream tagging of PPPoE frames.

Command	Mode	Function
bridgeport *PORTS* **antispoofing** { enable I disable }	Bridge	Bridge port IP anti-spoofing configuration. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20. **enable**: enables IP anti-spoofing **disable**: disables IP anti-spoofing For further settings see 23 IP Anti-Spoofing.
bridgeport *PORTS* **mode vcc-aggr** { enable I disable }	Bridge	Enables/disables **VCC** aggregator. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20.
no bridgeport *PORTS* **mode vcc-aggr**		Deletes VCC aggregator.
bridgeport *PORTS* **multicast-packagegroup** *MCPKGGPR*	Bridge	Configures multicast package group. **PORTS**: port number/range of port numbers, e.g., 1/1-1/48,2/20. **MCPKGGPR**: multicast package group, e.g., 1.2.3 ("" means no list) For further settings see 19.7 IGMP Subscriber Port

To check the port configuration, use the follwing command.

Command	Mode	Function
show bridgeport [*PORTS*]	Privi-leged/ Config/ Bridge	Displays bridge port configuration. **PORTS**: port number/range of port numbers, e.g., 1/1/1-1/12/1,0/1.

14.2.5 Traffic Limitation

The hiX 5750 R2.0 supports traffic bridge port shaping and policing as denoted in Table 23. To set the limitations, the following tasks must be performed:

1. Creating of Traffic Descriptor Profiles
2. Configuring Shaping and Policing on Bridge Port.

Type	Egress Rate Limiting	Ingress Rate Limiting
hix 5709 MDU 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 23 Bridge Port Shaping and Policing

Creating of Traffic Descriptor Profiles

This profile states the sustained and peak data rate. There are different traffic descriptor profiles (up to 64) configurable for in-bound and out-bound traffic. The out-bound traffic descriptor describes the limitations on traffic rate leaving the **MAC** bridge (traffic shaping towards the **UNI**, upstream), the in-bound descriptor describes the limitations on traffic rate entering the MAC bridge (policing towards the **ANI**, downstream).

ℹ Traffic Descriptor Profiles can be only created or deleted but they cannot be modified.

Command	Mode	Function
bridgeport-traffic-desc-profile create { sust_rate } { peak_rate }	Bridge	Creates a bridgeport traffic descriptor profile that specifies a sustained data rate and a peak data rate. Rate ranges: 0..150,000 KBytes/sec. **sust_rate**: sustained data rate **peak_rate**: peak data rate.
bridgeport-traffic-desc-profile delete { profile_index }		Deletes a bridgeport traffic descriptor profile with index. profile_index: specifies the profile.
bridgeport-traffic-desc-profile create <0-150000> <0-150000> [*NAME*]	Bridge	Creates a traffic descriptor profile. **1 - 64**: index of bridgeport-traffic-desc-profile table **0 - 150000**: SIR (Sustained Information Rate) in kByte/s **0 - 150000**: PIR (Peak Information Rate) in kByte/s **NAME**: traffic descriptor name.
bridgeport-traffic-desc-profile <1-64> **create** <0-150000> <0-150000> [NAME]		
bridgeport-traffic-desc-profile delete <1-64>		Deletes specified traffic descriptor profile. **1 - 64**: index of bridgeport-traffic-desc-profile table.

Use the following command to check the traffic-descriptor-profile table.

Command	Mode	Function
show bridgeport-traffic-desc-profile table	Bridge	Shows the table with config data.

Configuring Shaping and Policing on Bridge Port

Traffic shaping and policing permit to define sustained and peak data rates for a customer bridge port. For this, there are two steps necessary:

1. Configuring of Creating of Traffic Descriptor Profiles.
2. Assigning of the profile(s) to the desired bridgeport. Two profiles are provided, one for upstream traffic (shaping) and another for downstream traffic (policing).

Command	Mode	Function
bridgeport *PORTS* **policing** <1-64>	Bridge	Ingress traffic policing. Specifies for this bridgeport an downstream traffic profile. **PORTS**: port number slot/port/ONU_ID/ ONU_slot/ONU_port **1 - 64**: bridgeport inbound traffic descriptor ID.
no bridgeport *PORTS* **policing**		Disables policing feature for specified bridgeport.
bridgeport *PORTS* **shaping** <1-64>	Bridge	Egress traffic shaping. Specifies for this bridgeport an upstream traffic profile. **PORTS**: port number slot/port/ONU_ID/ ONU_slot/ONU_port **1 - 64**: bridgeport outbound traffic descriptor ID.
no bridgeport *PORTS* **shaping**		Disables shaping feature for specified bridgeport.

14.3 Port Mirroring

To enable/disable an IU_1x10G mirror monitor port, use the following command.

Command	Mode	Function
mirror monitor *PORT*	Bridge	Enables the monitoring port. **PORT**: select uplink port number Use the **no** parameter with this command to delete the monitor port.
show mirror monitor	Bridge	Shows the monitor port.

15 Interface Configuration

15.1 Enabling of an Interface

Before an IP address can be assigned to the network interface, the interface communication must be enabled. Use the **show running-config interface** command to verify the interface status.

By default, the hiX 5750 R2.0 system is set to communicate over the interface *mgmt*.

An interface can be enabled on *Configuration* mode or *Interface configuration* mode.

Interface Configuration Mode

At first, use the following command to change into *Interface configuration* mode.

Command	Mode	Function
interface *INTERFACENAME*	Config	Choose *Interface configuration* mode of the specified interface. **INTERFACENAME**: interface that has to be configured. For the outband management connection choose mgmt.

After this, use the **no shutdown** command to enable the interface.

Command	Mode	Function
no shutdown	Interface	Enables the interface on *Interface Configuration* mode.
shutdown		Disables the interface on Interface Configuration mode.

Return to *Configuration* mode or *Privileged exec* mode with the following commands.

Command	Mode	Function
exit	Interface	Returns to *Configuration* mode.
end		Returns to *Privileged exec* mode.

Example of enabling the interface 1:

```
SWITCH# configure terminal
SWITCH# interface 1
SWITCH(config-if)# no shutdown
SWITCH(config-if)#
```

Configuration Mode

Execute the following command to enable/disable an interface on *Configuration* mode.

Command	Mode	Function
interface { shutdown I noshutdown } *INTERFACENAME*	Config	Disables/enables the interface on *Configuration* mode. **INTERFACENAME**: interface that should be deactivated/activated.

To manage multiple interfaces, use the delimiter “-“ or “, ”.

15.2 Assigning an IP Address to the Interface

After enabling the network interface, assign an IP address and subnet mask to this interface by using the **ip address** commands in the *Interface* mode.

Command	Mode	Function
ip address *ADDRESS/M*	Interface	Sets IP address of an Interface. **ADDRESS/M**: specifies the IP address prefix and length of this IP Use the **no** parameter with this command to clear designated IP address.
ip address *ADDRESS/M* **scope** { host | link }		Sets link/host IP address. **ADDRESS/M**: specifies the IP address prefix and length of this IP **host**: IP address for the appropriate equipment **link**: IP address for the appropriate network.
ip address *ADDRESS/M* **secondary**		Sets secondary IP address of an Interface. **ADDRESS/M**: specifies the IP address prefix and length of this IP Use the **no** parameter with this command to clear secondary IP address.

Example of assigning the IP address 192.168.1.10 to 1:

```
SWITCH(config-if)# ip address 192.168.1.10/16
SWITCH(config-if)#
```

All assigned IP addresses can be cleared with the following commands.

Command	Mode	Function
no ip address	Interface	Clears all IP addresses.

15.3 Displaying the IP Address of Interface

Use the following command to display an assigned IP address.

Command	Mode	Function
show ip	Interface	Displays an assigned IP address of the interface.

```
SWITCH(config-if)# show ip
IP-Address          Scope   Status
-------------------------------------
10.7.24.199/16      global

SWITCH(config-if)#
```

15.4 Displaying the Interface Status

To check the interface status and configuration, use the following command.

Command	Mode	Function
show interface [*INTERFACENAME*]	Privileged/ Config/ Interface	Shows Interface status and configuration.

Example:

```
SWITCH(config)# show interface
Interface lo
Hardware is Loopback
index 1 metric 1 mtu 16436 <UP,LOOPBACK,RUNNING>
VRF Binding: Not bound
Bandwidth 100m
input packets 318223, bytes 56058589, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 318223, bytes 56058589, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0   collisions 0
Interface mgmt
Hardware is Ethernet, address is 0800.0626.1a69
index 2 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Bandwidth 100m
inet 10.2.2.20/24 broadcast 10.2.2.255
input packets 16085, bytes 8778585, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 9245, bytes 2955103, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0    collisions 0
Interface br4094
Hardware is Ethernet, address is 0800.0626.1a69
index 41 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
Bandwidth 100m
inet 10.254.254.100/27 broadcast 10.255.255.255
input packets 19418, bytes 13580234, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 0, missed 0
output packets 26948, bytes 12872892, dropped 0
output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0   collisions 0
SWITCH(config)#
```

16 VLAN

The first step in setting up a bridging network is to define **VLAN**. A VLAN is a bridged network that is logically segmented by subscriber or function. Each VLAN contains a group of ports. Packets on the VLAN which are received on a port will be forwarded only to ports that are member of the same VLAN. Network devices in different VLANs cannot communicate with one another without a Layer 3 switching device to route traffic between the VLANs. These VLANs improve performance because they reduce the propagation of local traffic, and they improve security benefits because they completely separate traffic.

The IEEE 802.1q based ports on the switches support simultaneous tagged and untagged traffic. An 802.1q port is assigned to a default port VLAN ID (PVID), and all untagged traffic is assumed to belong to the port default PVID. Thus, the ports participating in the VLANs accept packets bearing VLAN tags and transmit them to the port VLAN ID.

VLAN configuration is described in the chapters:

- Configuring a VLAN
- Enabling a Host VLAN
- Assigning the VLAN to Bridgeports
- Assigning the VLAN to DHCP/PPPoE Provider
- Assigning the VLAN to Default Gateway
- Enabling of Multicast Permission for the VLAN
- Checking the VLAN Configuration.

ℹ For detailed information about the configuration of VLAN scenarios using the enhanced MAC modes, see chapter 13.1 Setting the GPON MAC Mode.

16.1 Configuring a VLAN

Command	Mode	Funciton
vlan create *VLANS MODE*	Bridge	Creates new VLAN by assigning VLAN ID. **VLANS**: enter the number of VLAN ID (from 1 to 4093) **MODE**: enter number of enhanced MAC mode 1: MAC mode 1 (N:1) - changing VLAN per ctag 2: MAC mode 2 (1:1- cross-connect by adding outer tag (service tag) per c-tag (default).
no vlan *VLANS*		Deletes the specified VLAN. ℹ Before deleting a VLAN, all ports must be removed.
vlan name *VLANS* { none I *NAME* }	Bridge	Configures VLAN name. **VLANS**: select VLAN IDs, e.g., 101-148, 1000 **NAME**: enter a VLAN name.
no vlan name *VLANS*		Deletes VLAN name.

The variable *VLANS* is a particular set of bridged interfaces. Frames are bridged only among interfaces of the same VLAN.

The VLAN ID is contained in the VLAN tag of transmitted packets. If a port is configured in tagging mode, it will send tagged traffic.

Deleting a VLAN

The following tasks must be performed in order to delete a VLAN:

Step 1 Delete all ports associated with the VLAN (see 16.3 Assigning the VLAN to Bridgeports)

Step 2 Delete the VLAN.

Example:

```
SWITCH(bridge)#vlan del 10 0/1-0/4
SWITCH(bridge)#no vlan 10
SWITCH(bridge)#show vlan 10
%vlan 10 doesn't exist--------------------------------
```

16.2 Enabling a Host VLAN

In order to enable a host-VLAN, use the following command.

Command	Mode	Funciton
host-vlan *<1-4093>*	Config	Adds host to a specified VLAN. **1 - 4093**: enter the VLAN ID Use the **no** parameter with this command to delete a host VLAN.

16.3 Assigning the VLAN to Bridgeports

Command	Mode	Function
vlan add *VLANS PORTS* { tagged I untagged } [{ PORTS { tagged I untagged } }]	Bridge	Adds port to specified VLAN. **VLANS**: enter the VLAN IDs, e.g., 101-148, 1000 **PORTS**: enter the port number for tagged or untagged traffic.
vlan del *VLANS PORTS*		Deletes associated ports from specified VLAN.

i To assign several ports to a VLAN, enter each port separated by a comma without space. Use dash mark “-“ to arrange port range.

Example:

The example shows the following steps:
Enter the *Configuration* mode, enable a switching process, and perform the configuration tasks:
Create a VLAN, add a untagged port to the VLAN, add a PVID to port (see 14.2.4 Bridge Port Parameters), show VLAN configuration (see 16.7 Checking the VLAN Configuration), enable VLAN interface (see 15.1 Enabling of an Interface), show interface configuration.
Enter *Interface* mode:
Add IP address, enable interface, exit interface mode, show interface configuration.

```
SWITCH# configure terminal
SWITCH(config)#bridge
SWITCH(bridge)#vlan create 4
SWITCH(bridge)#vlan add 4 9/1 untagged
SWITCH(bridge)#bridgeport 9/1 pvid 4
SWITCH(bridge)#exit
SWITCH(config)#show vlan
SWITCH(config)#host-vlan 4
SWITCH(config)#show vlan
SWITCH(config)#show interface br4
SWITCH(config)#interface br4
SWITCH(config-if)#ip address 172.0.0.1/26
SWITCH(config-if)#no shutdown
SWITCH(config-if)#exit
SWITCH(config)#show interface br4
```

16.4 Assigning the VLAN to DHCP/PPPoE Provider

Use the following commands in order to assign a DHCP/PPPoE provider to the specified VLAN.

ℹ For detailed information see also 18.2 DHCP/PPPoE Provider.

Command	Mode	Function
vlan provider { dhcp I pppoe } *VLANS* { none I *PROVIDER* }	Bridge	Configures VLAN provider. **dhcp**: configure DHCP provider **pppoe**: configure PPPoE provider **VLANS**: select VLAN IDs, e.g., 101-148, 1000 **none**: delete provider from VLAN **PROVIDER**: configure provider index.

16.5 Assigning the VLAN to Default Gateway

A default gateway is only needed for a subscriber VLAN (PVID for a bridge port), if the corresponding bridge port uses the **IPoA** mode. In this case, a default gateway is required in order to activate the IPoA mode.

To configure the default gateway, use the following command.

Command	Mode	Function
vlan default-gateway *VLANS* { *DEFGATEWAY* I none }	Bridge	Configures default gateway. **VLANS**: select VLAN IDs, e.g., 101-148, 1000 **DEFGATEWAY**: IPv4 address of default gateway, e.g., 10.0.0.1.
no vlan default-gateway *VLANS*		Deletes specified default gateway.

16.6 Enabling of Multicast Permission for the VLAN

Executing the following command, the VLAN will transmit only multicast-traffic or IGMP requests.

Command	Mode	Function
vlan multicast-permission *VLANS* { disable I enable }	Bridge	Configures multicast permission. **VLANS**: select VLAN IDs, e.g., 101-148, 1000 **disable/enable**: multicast permission.

16.7 Checking the VLAN Configuration

Command	Mode	Function
show vlan [*VLANS*]	Privileged/ Config/ Bridge	Shows the configuration for specific VLAN or for all VLANs. **VLANS**: enter VLAN ID.

Command	Mode	Function
show port-in-vlan *PORTS*	Privileged/ Config/ Bridge	Lists ports VLAN. **PORTS**: enter the port number, e.g.,1/1-1/48,0/1,1/2/1.
show host-vlan	Config	Shows assignment of host to a VLAN.

17 Quality of Service (QoS)

The hiX 5750 R2.0 provides QoS functions for traffic management. QoS is a useful function to provide the users more convenient services for the network traffic. This function is very good serviceable in order to prevent an overloading, the delaying or the failing of traffic through the setting of specific priorities for the different kinds of traffic flows. QoS can basically give a priority for a specific traffic or limit it. When data are processed, they are usually supposed to be processed in a defined time-order like first-in/first-out. It is possible to use strict priority and WRR (Weighted Round Robin) for queuing. The case that certain data are processed not immediately, might result in the loss of all data in case of overloaded traffics. However, in case of an overloading situation, the QoS of the traffic flows can determine the order of processing for these traffic flows by the reorganizing of priorities according to the importance of the single traffic flows. By favor of QoS, the user can predict network performance in advance and manage bandwidth more effectively.

QoS operates as follow:

- Class-of-service (Dot1p priority) mapping to queues
  These mappings will be applied on all uplink and downlink interfaces within the system.
- Scheduling modes
  In order to handle overloading of traffic flows, differently processing orders are possible through using scheduling algorithms. The hiX 5750 R2.0 provides two methods of queue scheduling and the combination of both:
  - Strict priority queuing is used to process certain important data more preferentially than the others. Since all data are processed by their priorities, data with high priorities can be processed fast but data without low priorities might be delayed and piled up. This method has a strong point of providing the distinguished service with a simple way. However, if the packets having higher priority enter, the packets having lower priority are not processed and can drop.

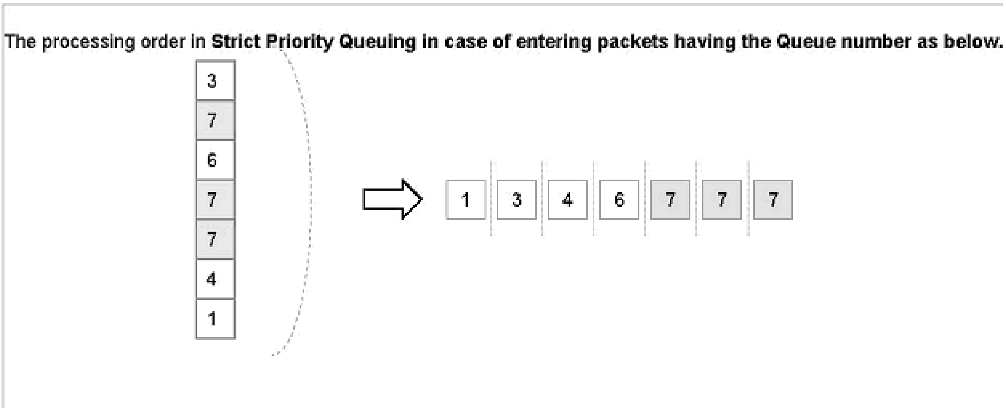

The processing order in Strict Priority Queuing in case of entering packets having the Queue number as below.
3
7
6
7
7
4
1
1
3
4
6
7
7
7

Figure 5 User-defined Setting for CPU Packet

  - The WRR queuing is a scheduling algorithm allowing different priorities depending on the queue weight. Queue weight controls the scheduling precedence of the internal packet queues. The higher the weight value the higher the scheduling precedence of this queue.

  Each of the scheduling algorithms can be assigned separately to uplink as well as downlink interface types for both downstream and upstream traffic flow.
  This means that each interface type can operate in another scheduling mode.

ⓘ For information about how to configure QoS on ONUs see 10.3 Traffic Management.

17.1 Configuring the Dot1p Priority-to-Queue Mapping

This configuration specifies the queues storing packets with a certain .1p priority.

In order to create the QoS map and to classify the rules of queueing, use the following commands in *Configuration mode*.

Command	Mode	Function
qos map { <0-7> I be I bg I spare I ee I cl I video I voice I ctrl } <0-7>	Config	Priority to queue number mapping. **0 - 7**: priority value acc. to .1p Default queue mappings. 0 = lowest: best effort (**be**) 1: background (**bg**) 2: space (**space**) 3: excellent effort (**ee**) 4: controlled load (**cl**) 5: video (**video**) 6: voice (**voice**) 7: highest: network control (**ctrl**) **0 - 7**: queue number.

17.2 Configuring the Scheduling Method

The hiX 5750 R2.0 supports different scheduling methods that can be assigned to different interface modes.

Command	Mode	Function
qos scheduling-mode { uplink_cards I downlink_cards I all } { downstream I upstream } { sp I wrr }	Config	Decides the queue scheduling mode for interfaces. **uplink_card**: all uplink card interfaces **downlink_card**: all downlink card interfaces **all** : all interface will get the following mode at once **downstream**: mode operates downstream traffic flow **upstream**: mode operates upstream traffic flow The mode of the selected interface: **sp**: strict priority-based queuing **wrr**: Weighted Round Robin queuing.

ⓘ Strict priority is the default setting of the hiX 5750 R2.0.

If WRR is selected, the weight size per queue can be determined by using the following commands. Weight in % is the value of time the queue is set to get service. For example, if queue 3 has double weight than the other ones, it will be served like 3-3-2-1-0-3-3-2-1-0 etc. A unlimited weight sets strict priority for the queue. The other queues which have been given a percent value, follow the common WRR scheme.

Command	Mode	Function
qos weight <0-7> { <1-100> I unlimited }	Config	Sets the weight values. **0 - 7**: queue number **1 - 100**: weight value in %, defines the value of time the queue is set to get service. **unlimited**: strict priority queuing.

17.3 Checking the QoS Configuration

Commands	Mode	Function
show qos { map I scheduling-mode I weight I all }	Privileged/ Config	Displays a configuration of QoS. **map**: priority to queue mapping **scheduling-mode**: scheduling mode **weight**: queue weights **factory defaults**: default values **all**: all information.

18 DHCP and PPPoE

The dynamic host control protocol (DHCP) enables a DHCP server to manage a pool of available IP addresses and to assign them automatically to devices upon request. Depending on its configuration, the hiX 5750 R2.0 can work as DHCP relay agent forwarding DHCP packets between clients and servers. A DHCP relay agent extends the reach of a DHCP server so that it is unnecessary to use several DHCP servers to accommodate several IP subnets.

PPPoE provides the ability to connect subscribers (e.g. **ADSL** customers) over a simple bridging access to the provider network. PPPoE offers a solution for providing high-speed, broadband Internet access that simplifies user configuration, utilizes standard Ethernet devices, and provides a familiar user interface.

The DHCP/PPPoE configuration is described in the following sections:

- Configuring of the DHCP/PPPoE Telegram Handling
- DHCP/PPPoE Provider
- DHCP Relay Agent
- DHCP Option 82 / PPPoE Option 105
- Configuring Subnet Default Gateway
- Verifying the DHCP Configuration
- Checking and Clearing the DHCP Statistics
- Configuring of ARP Flooding
- Showing Entries of DHCP/ARP Table
- Deleting an Entry Learned by DHCP/ARP.

ℹ For information about how to assign DHCP/PPPoE to VLAN see chapter 16.5 Assigning the VLAN to Default Gateway. For commands configuring the bridge port, see 14.2.4 Bridge Port Parameters.

18.1 Configuring of the DHCP/PPPoE Telegram Handling

When the **CXU** works in intermediate mode and the DHCP/PPPoE relay agent is enabled, option 82/option 105 can be inserted or deleted.
Enter the following commands to configure the DHCP/PPPoE mode of CXU.

Command	Mode	Function
ip dhcp { relay I snoop I bridge }	Config	Sets DHCP mode. **relay**: valid telegrams are handled. If necessary, DHCP option82 will be inserted or deleted. DHCP header will be changed e.g. with configured server and gateway IP address, **snoop**: valid telegrams are forwarded, invalid telegrams are dropped Invalid telegrams will be dropped. **bridge**: all telegrams are forwarded.
ip pppoe { relay I snoop I bridge }		Sets PPPoE intermediate agent. **relay**: valid telegrams are handled. If necessary option105 will be inserted or deleted. Invalid telegrams are dropped. **snoop**: valid telegrams are forwarded, invalid telegrams are dropped **bridge**: all telegrams are forwarded.

18.2 DHCP/PPPoE Provider

In order to configure a DHCP or PPPoE provider pool use the following commands in the respective configuration mode.

18.2.1 Changing into the DHCP/PPPoE Configuration Mode

Enter the following commands to change into DHCP or PPPoE configuration mode and to configure the specified provider.

Command	Mode	Function
ip dhcp provider *NAME*	Config	Changes into *DHCP/PPPoE configuration* mode to create/modify a DHCP/PPPoE provider pool. **NAME**: provider name. Use the **no** parameter with this command to delete the specified DHCP/PPPoE provider pool entry.
ip pppoe provider *NAME*		

Use the commands below to exit the DHCP/PPPoE configuration mode and to save made settings.

Command	Mode	Function
exit { secure I forced }	DHCP/ PPPoE	Exits *DHCP/PPPoE config* mode to *config* mode. **secure**: only if some valid data are committed (default) **forced**: exits *DHCP/PPPoE configuration* mode without saving.
commit { exit I end }		Saves values after having verified them successfully. **exit**: commits data and leave *DHCP/PPPoE configuration* mode to *Config* mode **end**: commits data and leave *DHCP/PPPoE configuration* mode to *Privileged exec* mode
quit		Exits *DHCP/PPPoE configuration* mode without saving.
end		Goes up to *Privileged exec* mode without saving.

18.2.2 Configuring the DHCP/PPPoE Provider

To configure the DHCP/PPPoE provider, enter the following commands.

Command	Mode	Function
simplified { on I off }	DHCP	Configures DHCP provider's type. **on**: simplified DHCP (default). The relay agent just adds DHCP option 82 without changing anything else inside DHCP header. **off**: normal DHCP. The relay agent adds the DHCP option 82 and modifies also the DHCP header (e.g. change the source IP).
no simplified		Sets the DHCP provider to normal.
vlanid <2-4094>	DHCP/ PPPoE	Specifies a VLAN for the DHCP/PPPoE provider pool. **2 - 4094**: provider's **VLAN** ID.
no vlanid		Deletes a VLAN ID from DHCP/PPPoE provider pool.

18.2.3 Verifying the Consistence of DHCP Provider Pool

To verify the consistence of provider pool entries, use the following command.

Command	Mode	Function
verify	DHCP	Checks if the provider entry's values are consistent.

18.2.4 Checking a Provider Pool

Enter the following command in order to display the provider pool entries.

Command	Mode	Function
show ip provider [*NAME* l index]	Exec/ Config/ DHCP/ PPPoE	Shows DHCP/PPPoE provider pool. **NAME**: provider pool name **index**: sorted by index.
show ip dhcp vlan [<2-4094>]	Config	Displays all or specified DHCP VLANs.
print [name l vlanid l option82 l gateway l remote-id l server l all]	DHCP	Displays actual values. **name**: provider's name **vlanid**: VLAN ID **option82/option105**: option82/ option105 flag **gateway**: gateway IP address **server**: DHCP server IPs **remote-id**: remote ID **all**: all (default).
print [name l vlanid l option105 l remote-id l all]	PPPoE	

18.3 DHCP Relay Agent

A DHCP relay agent has to transfer DHCP messages between the DHCP clients and associated servers when they do not reside on the same IP network or subnet. In the hiX 5750 R2.0 a DHCP relay agent is available to manage a wide DHCP subnet by forwarding IP addresses which are requested from the DHCP clients. A DHCP relay agent also extends the reach of a DHCP server so that it is not necessary to use multiple DHCP servers to accommodate multiple IP subnets.

18.3.1 Enabling the DHCP Relay Agent

Use the following commands to enable/disable the DHCP relay agent.

Command	Mode	Function
dhcp-relay *A.B.C.D*	Config	Enables DHCP relay agent for the *mgmt* interface. A.B.C.D: IP address of DHCP server
no dhcp-relay		Disables DHCP relay agent for the *mgmt* interface.
ip { { address A.B.C.D } l A.B.C.D/M l { netmask { A.B.C.D l <1-31> } } }	DHCP	Configures DHCP relay IP address and netmask.
no ip dhcp relay		Disables DHCP relay.

18.3.2 Registering the DHCP Server

After configuring the relay agent, enter the following command to register the DHCP server(s).

Command	Mode	Function
server [A.B.C.D [[A.B.C.D [A.B.C.D]]]	DHCP	Configures new DHCP server IP address(es). Enter first, second or third DHCP server's address.
no server { A.B.C.D I all }		Deletes DHCP server IP address(es). Enter IP address value or "all" (default).

18.3.3 Checking the Configuration of DHCP Relay

Enter the following commands to display the relay information.

Command	Mode	Function
show dhcp-relay	Config	Shows DHCP-relay agent configuration.
show ip dhcp relay		

18.4 DHCP Option 82 / PPPoE Option 105

Option 82 is used by the relay agent to insert additional information into the subscriber's DHCP request. This information can be used to implement policies intended to improve security and efficiency.

The DHCP option 82 field is defined by the two sub-options "Circuit ID" and "Remote ID". The sent circuit ID string contains e.g. information about the port and the VLAN over which the DHCP request is coming in. It will be replaced dynamically when a DHCP request is received with a VLAN depending on the string. The remote ID is unique for the system. 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 configurable string. The circuit ID priority is higher than the remote ID priority. When the system receives request packets without option 82 information, it attached its own information. When the remote ID recorded in option 82 is equal to system's MAC address, it transmits the packets after removing option 82 via the designated port number.

18.4.1 Enabling the Option 82 / Option 105

To enable DHCP option82/PPPoE option 105, use the following commands.

Command	Mode	Function
option82 { <0-3> I remote-id I circuit-id I all }	DHCP	Configures DHCP provider's option82 flags. **0 - 3**: sets option82 suboption flags by number **remote-id**: enables using remote ID suboption **circuit-id**: enables using circuit ID suboption **all**: enables flags for using all suboptions.
no option82		Disables DHCP provider's option82 flags.
option105 { <4-7> I remote-id I circuit-id I all }	PPPOE	Configures PPPoE provider's option105 flags. **4 - 7**: sets option105 suboption flags by number **remote-id**: enables using remote ID suboption **circuit-id**: enables using circuit ID suboption **all**: enables flags for all suboptions.
no option105		Disables using suboptions at all.

18.4.2 Configuring the Remote-ID

ℹ By default, the system's MAC address is the remote ID.

To configure DHCP option82 - sub-option remote ID, use the following commands.

Command	Mode	Function
ip dhcp option82 remote-id { A.B.C.D I XX:XX:XX:XX:XX:XX }	Config	Configures option82 remote-ID of the system. **A.B.C.D**: remote ID address in IP style **XX.XX..**.: remote ID address in MAC style.
ip dhcp option82 remote-id { { hex *HEXSTRING* } I { ascii *TEXT* } I circuitid }		Configures remote ID of the system. **HEXSTRING**: remote ID of hex type **TEXT**: remote ID of ascii type **circuitid**: the circuit ID will be used as remote ID.
no ip dhcp option82 remote-id		Disables the configuration of remote ID.

Enter the command below to display the remote ID.

Command	Mode	Function
show ip dhcp { remote-id I system-remote-id }	Config	Displays the specified DHCP remote-ID.

18.4.3 Setting the Circuit ID Format

To set and verify the circuit ID format, use the following commands.

Command	Mode	Function
circuitid-format *STRING*	Bridge	Sets the default format string for circuit IDs. Format string (describer replacement): %N -> hostname %S -> slot %P -> port %R -> VLAN %T -> line type (DSL) %V -> VCC ID %p -> VPI %c -> VCI %B -> bridgeport not., e.g.iuslot/... %b -> unique bridgeport ID Separator: space.;,/*-:

Enter the command below to display the default format string.

Command	Mode	Function
show circuitid-format	Bridge	Displays the default format string for circuit IDs.

18.4.4 VLAN Handling depending on Circuit ID

To add, delete, or modify VLAN depending circuit ID part, use the following commands.

Command	Mode	Function
ip dhcp circuitid2 { *BRIDGEPORTINDEX* | * | all } <2-4094> *CIRCUITID*	Config	Adds VLAN depending circuit ID part. **BRIDGEPORTINDEX**: bridge port index or / IU_slot/GPON_link/ONU_ID/ONU_slot/ONU_port *****, **all**: all bridgeports that currently exist **2 - 4094**: VLAN tag **CIRCUITID**: tag depending string.
no ip dhcp circuitid2 { *BRIDGEPORTINDEX* | * | all } <2-4094>		Deletes VLAN depending circuit ID part.
ip dhcp circuitid2 token *STARTTOKEN* { *TK1* | default } [*TK2* | default]	Config	Modifies token for VLAN depending circuit ID part. **STARTTOKEN**: token start identifier, e.g. % **TK1**: token1 for VLAN replacement, e.g. V **default**: default Token1 for VLAN replacement **TK2**: token2 for VLAN service replacement, e.g. R **default**: default Token2 for VALNreplacement.

18.4.5 Configuring the DHCP Packet Policy

The operator can configure how to process packets with DHCP option 82 coming to DHCP server or DHCP relay agent.

Use the following command to configure the policy for option 82/option 105 packets.

Command	Mode	Function
ip dhcp option82 policy { replace | keep | drop }	Config	Configures the policy of option82 packets. **replace**: relay agent replaces the existing address with option82 information of relay or server, **keep**: relay agent transmits packets without changing the received option82 information (default), **drop**: relay agent drops the option82 packe.

18.5 Configuring Subnet Default Gateway

A default gateway allows the **DHCP** server to communicate with unspecified IP addresses.

Command	Mode	Function
gateway A.B.C.D	DHCP	Configures DHCP provider’s gateway IP. **A.B.C.D**: IP address of gateway.

18.6 Verifying the DHCP Configuration

To check the current DHCP configuration, use the following commands.

Command	Mode	Function
show ip dhcp config	Config	Displays current DHCP configuration.
show ip dhcp bridge [*BRIDGEPORTINDEX* | all]		Displays a fixed IP entry: **BRIDGEPORTINDEX**: shows bridge port index **all**: shows all entries (default).

An example of viewing the DHCP configuration:

```
SWITCH(config)#show ip dhcp config
!Begin of DHCP daemon's configuration
no debug dhcp all
no debug dhcp kernel
no debug arp-reply all
ip arp-reply flood
ip dhcp bridge
ip pppoe bridge
ip dhcp option82 remote-id 08:00:06:26:24:b3
ip dhcp option82 policy keep
!
!DHCP provider pool
$2 @ip dhcp provider simple_indepent 1 0 11
$2 @ip dhcp provider vlan_501 2 501 3 192.168.51.56 255.255.255.0
0.0.0.0 192.168.51.10
!End of DHCP provider pool
!
!PPPoE provider pool
$2 @ip pppoe provider test 3 0 7
!End of PPPoE provider pool
!
ip dhcp circuitid2 token % R
!End of DHCP daemon's configuration
SWITCH(config)#
```

18.7 Checking and Clearing the DHCP Statistics

To show or clear the statistics of sent and received packets, use the following commands.

Command	Mode	Function
show ip dhcp statistics	Config	Displays DHCP packet sent/received statistics.
ip dhcp clear statistics		Clears DHCP status (packet sent/received statistics).

18.8 Configuring of ARP Flooding

ARP (Address Resolution Protocol) is used to associate IP addresses with **MAC** addresses. Once determined, the IP address/MAC association is stored in an ARP table for rapid retrieval. For handling ARP requests, which are L2 broadcasts, from the network side, there is an ARP relay agent in the hiX 5750 R2.0. In switched VLANs, the ARP relay agent responds to ARP requests from GPON clients as well as subtended clients and handles ARP requests from the DHCP relay agent to learn IP addresses of DHCP gateways or DHCP servers.

In downstream direction, the NE should not flood broadcast ARP requests towards the subscriber ports since the MAC to IP mapping is known.

Use the following command to enable/disable ARP flooding.

Command	Mode	Function
ip arp-reply flood	Config	Enables flooding of ARP requests. Use the **no** parameter with this command to disable flooding.

To check information about ARP state use the following command.

Command	Mode	Function
show ip arp-reply flood	Exec/ Config	Shows ARP replies’ flooding state.

18.9 Showing Entries of DHCP/ARP Table

Use the following commands to display the entries of ARP/DHCP table.

Command	Mode	Function
show ip dhcp learned-table	Config	Shows learned entries of DHCP table.
show arp-reply learned-table		Shows learned reply entries of ARP table.
show arp-reply fixed-table		Shows fixed entries of ARP table.

18.10 Deleting an Entry Learned by DHCP/ARP

Use the following commands to delete an entry of kernel’s IP table learned by DHCP.

Command	Mode	Function
no ip dhcp learned-table { { A.B.C.D I XX:XX:XX:XX:XX:XX } I { A.B.C.D XX:XX:XX:XX:XX:XX } }	Config	Deletes an entry from DHCP learned table in kernel, **A.B.C.D**: entrie's IP address **XX:XX:XX:XX:XX:XX**: entrie's MAC address,
ip dhcp learned-table delete { { A.B.C.D I XX:XX:XX:XX:XX:XX } I { A.B.C.D XX:XX:XX:XX:XX:XX } }		

Use the following commands to delete an entry of kernel’s IP table learned by ARP.

Command	Mode	Function
no arp-reply learned-table A.B.C.D	Config	Deletes an entry from ARP learned table in kernel, **A.B.C.D**: entrie's IP address.
arp-reply learned-table delete A.B.C.D		

19 IGMP

IGMP (Internet Group Management Protocol) is a host-to-router protocol used to announce multicast (MC) group membership by interested subscriber hosts.

IGMP supports an **MC** distribution service where only one data stream from the source is replicated in the OLT to serve a large number of receivers on behalf of its requests. A router serving a multicast VLAN sends only IGMP query message in request of ports receiving multicast packets. If a subscriber port sends the join message to the multicast router, the router transmits the multicast packet only to that port.

The hiX 5750 R2.0 provides the following IGMP operation modes:
- IGMP switching mode
- IGMP snooping mode
- IGMP proxy mode.

In the “IGMP switching” mode MC traffic is forwarded over all ports of the MC VLAN. IGMP snooping is a function to find those ports, which send a join message to join in specific MC group to receive MC packets or leave message to get out of the MC group because it does not need packets anymore. Only when the OLT is connected to an MC router, IGMP snooping can be enabled.

IGMP proxy acts in a dual mode as IGMP router and IGMP host. When interacting with the subscribers, the proxy appears as an IGMP router sending queries downstream. When interacting with the MC router, the proxy appears as an IGMP host sending IGMP membership report and leave group messages on behalf of subscribers.

IGMP configuration is described in the following chapters:

- Global Settings
- IGMP RFC Profile
- IGMP Provider
- Multicast Package and Group
- IGMP Operation Mode
- Configuring of Queries Parameters
- IGMP Subscriber Port
- Assigning of an ONU Port to static Multicast Groups.

ℹ For information about how to enable MC VLAN see 16.6 Enabling of Multicast Permission for the VLAN.

19.1 Global Settings

To disable/enable global IGMP and configure the maximum number of subscribers joining a multicast group, use the following commands.

Command	Mode	Function
igmp { enable I disable }	Config	Enables (default) /disables global IGMP.
igmp traffic max-joined-groups <1-5000>}	Config	Sets maximum number of subscribers that can join a multicast group in the system. **1 - 5000**: maximum joined MC groups.

Use the following commands to verify the global IGMP configuration.

Command	Mode	Function
show igmp	Config	Displays IGMP status.
show igmp traffic max-joined-groups	Config	Displays max.number of subscribers that can join MC groups in system.

19.2 IGMP RFC Profile

Overview Query Parameters

In the hiX 5750 R2.0 RFC profiles are used to modify the preset IGMP query parameters. In order to configure IGMP queries, the following options can be set:

- **Robustness** value allows tuning for the expected packet loss on a subnet. If a subnet is expected to be lossy, the robustness variable may be increased. IGMP is robust to (robustness variable - 1) packet losses. The robustness variable MUST NOT be zero, and SHOULD NOT be one.
- **Query Interval** in seconds sets the frequency at which IGMP host-query packets (downstream) are transmitted on the interface.
- **Response Interval** in seconds sets max. response time inserted into the periodic general queries. When the subscriber host doesn't respond to IGMP query messages, it is unsubscribed from the multicast group. It must be less than the query interval (default: 10 s).

  i The query response interval value must be set in steps of 0,1 s.
- **Startup Query Interval** is the startup frequency at which IGMP host-query packets (downstream) are transmitted on the interface.
- **Startup Query Count** is the number of queries sent out on startup, separated by the startup query interval.
- **Last Member Query Interval** is the max. response time inserted into group-specific queries sent in response to leave group messages, and is also the amount of time between group-specific query messages. This value may be tuned to modify the leave latency of the network. A reduced value results in reduced time to detect the loss of the last member of a group.
- **Last Member Query Count** is the number of group-specific queries sent before the router assumes there are no local members.
- **Unsolicited Report Interval** is the time between repetitions of a host's initial report of membership in a group (upstream).
- **Unsolicited Report Count** indicates the number of times unsolicited report has been sent. Such reports are sent after every unsolicited report interval.
- **Version1 Router Timeout** is how long a host must wait after hearing a version-1 query before it may send any IGMPv2 messages. The time until the local router will assume that there are no longer any IGMPv1 members on the IP subnet attached to this interface. Upon hearing any IGMPv1 membership report, this value is loaded to a timer. While the timer is running, the local router ignores any IGMPv2 leave messages for this group that it receives on this interface.

Configuring of RFC Profiles

Use the following commands to configure IGMP profiles.

Command	Mode	Function
igmp rfc-profile [<1-30>] *NAME* { inactive I vlan-switching I snooping I acl } { <1-255> I default } {<1-65535> I default} { <1-255> I default } { normal I fast } <1-4093> [<0-7>] { keep I replace } [<1-4093> [<0-7>]]	Config	Creates an IGMP RFC related profile. **1 - 30**: profile index (max. 16) **NAME**: profile name Switching modes: **inactive**: Disabled forwarding IGMP MC traffic **vlan-switching**: MC traffic will be forwarded over all ports of the VLAN. **snooping**: supports MAC based IGMP snooping functionality. Only subscriber ports which have joined at the MC group will be inscribed on the forwarding-table of the MC VLAN. Ports that leave the group will be deleted from the table. **acl**: snooping with ACL. The ACL contains the allocations of the customer (subscriber ports) to their allowable MC groups. Selecting this feature the ONU will be filtered the MC packages according to the determination of the ACL. **1 - 255**: robustness, **default**: 2 **1 - 65535**: set query interval in seconds, **default**: 125 **1 - 255**: set query response interval (0,1 seconds), **default**: 100 Leave modes: **normal**: when IGMP snooping sees a Leave message, it waits for a membership query message before setting the entry time-out to configured value. The group entry will be expired when the group membership timer interval is ending. **fast**: enables fast leave configures IGMP snooping to stop the transmission of a group multicast stream to a port as soon as it receives a Leave message on that port. The group entry is expired intermediately. No time-outs are observed. **1 - 4093**: VLAN ID **0 - 7**: multicast priority, setting overwrites the current .1p value of the VLAN. VLAN tagging operation mode: **keep**: keep outer tag unchanged (==remain/remain/remain) **replace**: replace outer tag by IGMP provider VLAN ID and priority (==add/rewrite/rewrite) **1 - 4093**: downstream VLAN ID (forking) **0 - 7**: downstream multicast VLAN priority (forking).
no igmp rfc-profile *NAME*	Config	Deletes IGMP RFC related profile. **NAME**: profile name.

Example:

Creating of an IGMP profile with index 4 and name “prof1” needed to be used for VLAN forking. All downstream MC traffic from the port assigned to this profile will be translated from the first VLAN-ID 10 to the second VLAN-ID 13, both VLANs have the priority 0.

```
igmp rfc-profile 4 prof1 snooping 2 15 50 normal 10 0 replace 13 0
```

Assigning “prof1” to the ONU port (see Assigning of an IGMP Profile).

```
igmp onu-port rfc-profile 2/2/7/4/9/1 prof1
```

Verifying of RFC Profiles

Command	Mode	Function
show igmp rfc-profile [*NAME*]	Config	Shows RFC related profile. **NAME**: profile name.

19.3 IGMP Provider

Configuring of Providers

IGMP provider are required to use proxy functionality on the OLT. Use the following commands to create an IGMP provider and to modify its parameters.

Command	Mode	Function
igmp provider <1-16> A.B.C.D [*NAME*] [<1-4093>]	Config	Creates an IGMP provider. **1 - 16**: provider index **A.B.C.D**: IGMP proxy IP address **NAME**: name of IGMP provider **1 - 4093**: multicast VLAN ID.
igmp provider A.B.C.D *NAME* [<1-4093>]		
no igmp provider { <1-16> | all }		Deletes specified or all IGMP provider(s). **1 - 16**: provider index **all**: all providers (default).

igmp query-parameter { <1-255> | recent | default }
{ <1-65535> | recent | default }
{ <1-255> | recent | default } { <1-65535> | default }
{ <1-255> | default } { <1-65535> | default }
{ <1-255> | default } { <1-65535> | default }
{ on | off | default } { <1-16>}
	Config	Sets provider's query parameters.
		1 - 255: Robustness value
		recent: does not change robustness, **default**: 2
		1 - 65535: Query interval value
		recent: does not change query interval, **default**: 125
		1 - 255: Response interval (0,1 sec.)
		recent: does not change response interval, **default**: 100
		1 - 65535: startup query interval (sec.)
		1 - 255: startup query count, **default**: 2
		1 - 65535: last member query interval. **default**: 1
		1 - 255: last member query count, **default**: 2
		1 - 65535: version 1 router time-out, **default**: 400
		on: immediate leave on
		off/default: immediate leave off
		1 - 16: provider index (default: 1).

igmp host-parameter <1-65535> [<1-16>]		Sets host parameter. **1 - 65535**: unsolicited report interval, default: 10 **1 - 16**: provider index (default: 1).
igmp provider <1-16> dot1p <0-7>	Config	Modifies an IGMP provider priority dot1p (QoS). **1 - 16**: provider index **0 - 7**: priority index.

Verifying the Providers

Command	Mode	Function
show igmp provider	Config	Displays a list of created IGMP providers.
show igmp version <1-16>		Displays IGMP version currently running. **1 - 16**: provider index
show igmp query-parameter [<1-16>]		Displays query parameters. **1 - 16**: provider index (default: 1).
show igmp provider egress-port-list <1-16>		Displays subscriber list per provider. **1 - 16**: provider index
show igmp host-parameter [<1-16>]		Displays host parameter. **1 - 16**: provider index (default: 1).

Assigning of Provider to VLAN

Use the following commands to assign a VLAN to the provider.

Command	Mode	Function
igmp provider-vlan <1-16> <1-4093>	Config	Connects IGMP provider to a VLAN. **1 - 16**: provider index **1 - 4093**: VLAN ID of IGMP provider.
no igmp provider-vlan <1-16>		Disconnects IGMP provider from a VLAN.

The following command can be used to check VLANs with MC permission.

Command	Mode	Function
show igmp vlan	Config	Displays a list of VLANs with multicast permission.

Example:

Creating of an IGMP provider with index 1 and name “prov_123” and assigning it to VLAN-ID 123.

```
igmp provider 1 192.168.151.15 prov_123
igmp provider-vlan 1 123
```

19.4 Multicast Package and Group

A mulicast group is a MC stream that clients can join. Groups have IP addresses in the 224.0.0.0/24 network (class D). There are some permanent MC group addresses, such as 224.0.0.1 (IGMP queries), 224.0.0.2 (all routers on the subnet), 224.0.0.5(6) (OSPF routers), 224.0.0.9 (RIPv2 routers) which should be not used.

Creating of Multicast Groups and Packages

To configure IGMP multicast group and packages, use the following command.

Command	Mode	Function
igmp multicast-group <1-16> A.B.C.D *NAME* [<1-512>]	Config	Creates an IGMP multicast group. **1 - 16**: provider index (default: 1) **A.B.C.D**: multicast IP address **NAME**: multicast group name **1 - 512**: index of multicast group.
no igmp multicast-group { <1-512> I *NAME* }		Deletes specified multicast group.
igmp multicast-package *NAME* [<1-100>]	Config	Creates a multicast package. **NAME**: multicast package name. **1 - 100**: index of multicast package.
no igmp multicast-package { <1-100> I *NAME* }		Deletes specified multicast package.
igmp add-group-to-package <1-512> <1-100>	Config	Adds IGMP multicast group to package. **1 - 512**: index multicast group **1 - 100**: multicast package index.
no igmp add-group-to-**package** <1-512> <1-100>		Deletes multicast group from package.

Example:

Creating of “package_123” and “group_123” and assigning of this group to the package.

```
igmp multicast-package package_123 1
igmp multicast-group 2 224.1.1.1 group_123 1
igmp add-group-to-package 1 1
```

Verifying the Multicast Groups and Packages

To check IGMP package of multicast group, use the following commands.

Command	Mode	Function
show igmp multicast-package	Config	Displays a list of created package of multicast group.
show igmp multicast-group	Config	Displays a list of created multicast groups.
show igmp group-ports <1-512>	Config	Displays assigned subscribers per multicast group. **1 - 512**: group index.
show igmp supplied cards <1-512>	Config	Displays index of supplied cards (physical entity). **1 - 512**: group index.

19.5 IGMP Operation Mode

To configure the operation mode of **OLT** units, use the following commands.

Command	Mode	Function
igmp cxu { inactive I vlan-switching I snooping I proxy }	Config	Configures IGMP operation mode of **CXU**. **inactive:** switching mode is off **vlan-switching:** **MC** traffic will be forwarded over all ports of the **VLAN**. **snooping:** **IP** based IGMP snooping will be supported. **proxy:** Reduces IGMP network traffic by supporting proxy functionality. Provider necessary, see 19.3 IGMP Provider.
igmp iu-gpon *SLOT* { inactive I vlan-switching I snooping }	Config	Configures IGMP operation mode of specified **IU_GPON**. **SLOT**: **IU** slot number **inactive:** Disabled forwarding IGMP MC traffic over the **GPON** ports. **vlan-switching:** MC traffic will be forwarded over all GPON ports of the VLAN. **snooping:** IP based IGMP snooping will be supported.
igmp iu *SLOT* { inactive I vlan-switching I snooping }	Config	Configures IGMP the operation mode of this IU. **SLOT**: IU slot number **inactive:** Disabled forwarding IGMP MC traffic over the GPON ports. **vlan-switching:** MC traffic will be forwarded over all GPON ports of the VLAN. **snooping:** IP based IGMP snooping will be supported.

To verify the IGMP status, use the following commands.

Command	Mode	Function
show igmp cxu	Config	Displays IGMP status on CXU.
show igmp snooping-table cxu	Config	Displays the CXU snooping table.
show igmp iu	Config	Shows all IUs with regard to IGMP.
show igmp snooping-table iu *IUSLOT*	Config	Displays the IU snooping table. **IUSLOT**: slot.
show igmp joined-ports-list <1-16> <1-512>	Config	Displays list of joined ports. **1 - 16**: IU slot **1 - 512**: group index.

The following command sets the IGMP operation mode of ONUs.

Command	Mode	Function
igmp onu *ID* { inactive I vlan-switching I snooping I acl }	Config	Configures IGMP on **ONU** side. **ID**: ONU slot/link/ID/slot **inactive**: switching mode is off **vlan-switching:** MC traffic will be forwarded over all ports of the VLAN. **snooping:** supports MAC based IGMP snooping functionality. Only subscriber ports which have joined at the MC group will be inscribed on the forwarding-table of the MC VLAN. Ports that leave the group will be deleted from the table. **acl:** the **ACL** contains the allocations of the customer (subscriber ports) to their allowable MC groups. Selecting this feature, the ONU will filter the MC packages according to the determination of the ACL. Provider necessary, see 19.3 IGMP Provider.

Use the following commands to check the IGMP information of ONUs.

Command	Mode	Function
show igmp onu *ADDR*	Config	Shows ONU port with regard to IGMP. **ADDRESS**: slot/link/ONU-ID/slot.
show igmp snooping-table onu *ID*	Config	Displays the ONU snooping table. **ID**: address slot/link/ONU-ID[/slot[/port[/VCC]]].
show igmp onu-card *ADDR*	Config	Shows ONU port with regard to IGMP. **ADDRESS**: slot/link/ONU-ID/slot.
show igmp onu-port *PORT*	Config	Shows ONU port with regard to IGMP. **PORT**: slot/link/ONU-ID/slot.

19.6 Configuring of Queries Parameters

Use the following commands to configure different query parameters for CXU, IUs, and ONUs.

Command	Mode	Function

igmp cxu query-parameter
{ <1-255> I recent I default } { <1-65535> I recent I default }
{ <1-255> I recent I default }
	Config	Sets query parameters at CXU.
		1 - 255: Robustness value
		recent: does not change robustness, **default**: 2
		1 - 65535: Query interval value in seconds
		recent: does not change query interval, **default**: 125
		1 - 255: Response interval (0,1 sec.)
		recent: does not change response interval, **default**: 100.

igmp iu-gpon *SLOT* **query-parameter**
{ <1-255> I recent I default } { <1-65535> I recent I default }
{ <1-255> I recent I default }
	Config	Sets the query parameters at IUGPON.
		SLOT: IU slot number.

igmp iu *SLOT* **query-parameter**
{ <1-255> I recent I default } { <1-65535> I recent I default }
{ <1-255> I recent I default }
		Sets the query parameters at IU card.
		SLOT: IU slot number.

igmp onu *ID* **query-parameter**
{ <1-255> I recent I default } { <1-65535> I recent I default }
{ <1-255> I recent I default }
	Config	Sets the query parameters on ONU side.
		ID: ONU - slot/link/id/slot.

19.7 IGMP Subscriber Port

Assigning of Multicast VLAN and Package

To assign a subscriber port to MC VLAN and package use the following command.

Command	Mode	Function
igmp subscriber { { <1-16> <1-72> <1-8> } I *BRIDGEPORT* } <1-4093> <1-100>	Config	Configure an IGMP subscriber port. **1 - 16**: logical IU slot **1 - 72**: IU port **1 - 8**: ADSL VCC **BRIDGEPORT**: bridge port specified by slot/port/VCC **1 - 4093**: port based VLAN ID **1 - 1 00**: package index.
no igmp subscriber { { <1-16> <1-72> <1-8> } I *BRIDGEPORT* } <1-100>		Deletes an IGMP subscriber.

Assigning of Multicast Package Group

To assign a package with multicast groups to the subscriber ports, use the following command on *Bridge configuration* mode.

Command	Mode	Function
bridgeport *PORTS* **multicast-packagegroup** *MCPKGGPR*	Bridge	Configures multicast package group. **PORTS**: port number, e.g., 1/1-1/48,2/20 **MCPKGGPR**: multicast package group ("" means no list).

Assigning of an IGMP Profile

To assign an RFC related profiles to an ONU port, use the following command.

Command	Mode	Function
igmp onu-port rfc-profile *PORT RFCPROFILE*	Config	Assigns a RFC related profile to an ONU port. **PORT**: ONU port address - slot/link/ONU-ID/slot/port **RFCPROFILE**: name of the RFC related profile.
no igmp onu-port rfc-profile *PORT*		Deletes a RFC related profile from ONU port.

Verifying the IGMP Subscribers

To check an IGMP subscriber, use the following command.

Command	Mode	Function
show igmp subscriber	Config	Shows a list of enabled IGMP subscribers.
show igmp port-groups *BRIDGEPORT*	Config	Displays joined multicast group list per subscriber. **BRIDGEPORT**: bridge port specified by slot/port/VCC.
show igmp joined-mc-addresses *ONUPORT*	Config	Displays list of joined MC addresses per port. **ONUPORT**: slot/link/ONU-ID/slot.

19.8 Assigning of an ONU Port to static Multicast Groups

A static MC group-to-port mapping guarantees that a specific MC stream is instantly available on a port, without any delay from the joining process. Additional, it enables to include subscribers that cannot send IGMP membership reports.

To create or delete IGMP static table entries, use the following commands.

Command	Mode	Function
igmp onu-port static-group *PORT* A.B.C.D <1-4093> [A.B.C.D <1-4093> [A.B.C.D <1-4093>]]	Config	Creates a static table entry for an ONU port. **PORT**: ONU port address - slot/link/ONU-ID/slot/port **A.B.C.D**: IP address of multicast group (1) **1 - 4093**: VLAN ID (1) **A.B.C.D**: IP address of multicast group (2) **1 - 4093**: VLAN ID (2) **A.B.C.D**: IP address of multicast group (3) **1 - 4093**: VLAN ID (3) Use the **no** parameter with this command to delete a static table entry.

20 ARP Table

Hosts connected to an IP network have two addresses, a physical MAC address and a logical IP network address. The 48-bit-MAC address is used on Layer 2 level by the switch to transmit packets. Using the address resolution protocol (ARP), the switch finds the MAC hardware address that matches to a given IP address. Once determined, the IP address/MAC association is stored in an ARP table for rapid retrieval. Referring to the entries in this table, a packet which is containing a known IP address is transmitted to the network. ARP is enabled by default and cannot be disabled.

20.1 Managing of ARP Table Entries

Becauce most of the hosts support dynamic address resolution, the contents of the ARP table will be automatically registered when a MAC address corresponding to a gathered IP address is found.

To install a permanent entry in the ARP table that maps a specific IP address to a MAC address, use the following commands.

Command	Mode	Function
arp A.B.C.D XX.XX.XX.XX.XX.XX	Config	Sets a static ARP entry. A.B.C.D: enter the IP address XX....XX.XX: enter the MAC address IFNAME: enter a interface name.
arp A.B.C.D XX.XX.XX.XX.XX.XX *IFNAME*		

Example of static registering IP address 10.1.1.1 and MAC address 00:d0:cb:00:00:01:

```
SWITCH (config)# arp 10.1.1.1 00:d0:cb:00:00:01
```

Use the following commands to delete a specified IP address and its related MAC address or all the contents from the ARP table.

Command	Mode	Function
no arp *A.B.C.D*	Config	Negates a static ARP entry or sets its entries default. A.B.C.D: enter the IP address IFNAME: enter the interface name.
no arp *A.B.C.D IFNAME*		
clear arp	Config	Deletes all the contents from the ARP table. IFNAME: enter the interface name.
clear arp *IFNAME*		

20.2 Checking the ARP Table

The **show** commands display all the IP and hardware addresses that are directly connected to an interface on the switch and addresses that have been learned dynamically by the switch.

Use following commands to examine the contents of the ARP table.

Command	Mode	Function
show arp	Privileged/ Config	Checks ARP table for specified interface. IFNAME: enter the interface name (br1, br2, ...).
show arp *IFNAME*		

Example of displaying the ARP table:

```
SWITCH (config)# show arp
---------------------------------------------------------
 Address            HWaddress       Type     Interface
------------------------------------------------------------
10.254.254.105    00:bb:cc:dd:ee:05  DYNAMIC    br4094
10.1.1.1          00:00:cd:01:82:d0  DYNAMIC    mgmt
SWITCH (config)#
```

20.3 ARP Alias

For security reasons, the communication between hosts connected to the same switch may be impossible. However, the hiX 5750 R2.0 can use ARP alias to connect hosts with each other by supporting the response of ARP requests from the host network through the concentrating switch.

To register a range of IP addresses from the host network in an ARP alias, use the following command.

Command	Mode	Function
arp-alias A.B.C.D A.B.C.D [XX:XX:XX:XX:XX:XX]	Config	Registers IP start and end address and MAC address in ARP-alias to make user's equipment response ARP request. Use the **no** parameter with this command to delete specified IP address range from ARP table.

Unless you have specified a MAC address, the MAC address of user's equipment will be used for ARP response.

To view ARP alias, use the following command.

Command	Mode	Function
show arp-alias	Privileged/ Config	Shows registered ARP-Alias.

Example of configuring ARP alias by registering IP addresses from 10.1.1.2 to 10.1.1.5.

```
SWITCH (config)# arp-alias 10.1.1.2 10.1.1.5
SWITCH (config)#
```

21 IP Routing

The hiX 5750 R2.0 supports the following routing protocols:

- BGP Routing
- RIP Routing
- IS-IS Routing

21.1 Static Routes

Static routing is the simplest form of routing. A static route remains in the router configuration until it will be removed. Thus, it does not work well when the routing information has to be changed frequently or needs to be configured on a large number of routing devices. Static routes must consist of a valid destination IP address, neighbor router receiving the packets, and number of hops that packets have to pass through.

From *Configuration* mode, use the **ip route** commands to add/delete a static IP route.

Command	Mode	Function
ip route A.B.C.D A.B.C.D { A.B.C.D | *INTERFACE* } [<1-255>]	Config	Establishes a static route. **A.B.C.D**: destination IP prefix **A.B.C.D** or **/M**: destination IP prefix mask **A.B.C.D**: forwarding router's IP address **INTERFACE**: interface **1 - 255**: administrative distance **src A.B.C.D**: binding source IP address Use the **no** parameter with this command to remove the specified static route from the routing table.
ip route A.B.C.D/M { A.B.C.D | *INTERFACE* } [<1-255> | src A.B.C.D]		

Each dynamic routing protocol has a default administrative distance. When there are two or more routes to the same destination, the router uses the administrative distance to decide which routing protocol (or static route) to trust more. When a static route is entered that is the same as a dynamic route, it will be used over the dynamic route. Default administrative distances are, e.g. connected interface = 0, static route = 1, RIP = 120, OSPF = 110, and IS-IS = 110. The lower the number, the more trustworthy the type of route is.

Determine the administrative distance of a static route higher than that of the dynamic protocol to allow that the static route can be overrode by information from a dynamic routing protocol.

Example of configuring static routes to reach three destinations which are not directly connected.

```
SWITCH(config)#ip route 100.1.1.0/24 10.1.1.2
SWITCH(config)#ip route 200.1.1.0/24 20.1.1.2
SWITCH(config)#ip route 172.16.1.0/24 30.1.1.2
```

There is a special kind of static route called a default route. The default route is the last route (gateway of last resort) tried by the router when all other routes fail. To configure the default route, use the following command in *Configuration* mode.

Command	Mode	Function
ip route default { A.B.C.D | *INTERFACE* } [1-255]	Config	Configures a default gateway. **A.B.C.D**: gateway IP address **INTERFACE**: interface **1 - 255**: administrative distance Use the **no** parameter with this command to delete the default route from the routing table.

Use one of the following commands, to display the static routes.

Command	Mode	Function
show ip route { A.B.C.D | A.B.C.D/M | summary }	Privileged/ Config	Displays the specified routing information.
show ip route [database] { bgp | connected | isis | kernel | ospf | rip | static }		Displays the configured routing information within the IP routing table database.

Example of viewing static routes.

```
SWITCH(config)# show ip route database
Codes: K - Kernel,
C - connected,
S - static,
R - RIP,
B - BGP
O - OSPF,
IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1,
E2 - OSPF external type 2
i - IS-LS,
L1 - IS-IS level 1,
L2 - IS-IS level 2,
ia - IS-IS inter area
> - selected route,
* - FIB route,
p - stale info
SWITCH(config)#
```

A static route for network 0.0.0.0 to default gateway configures a default route.

The following example shows the configuring of a static route for network 0.0.0.0 to default gateway 10.2.2.1. It can be checked by using the command **show ip route**.

```
SWITCH(config)#ip route 0.0.0.0/0 10.2.2.1
SWITCH(config) show ip route
Codes: K - kernel,
C - connected,
S - static,
R - RIP,
B - BGP
O - OSPF,
IA - OSPF inter area
N1 - OSPF NSSA external type 1,
N2 - OSPF NSSA external type 2
E1 - OSPF external type 1,
E2 - OSPF external type 2
i - IS-IS,
L1 - IS-IS level-1,
L2 - IS-IS level-2,
ia - IS-IS inter area
* - candidate default Gateway of last resort is 10.2.2.1 to
network 0.0.0.0S*
0.0.0.0/0 [1/0] via 10.2.2.1, mgmtC
10.2.2.0/24 is directly connected,
mgmtC 10.254.254.96/27 is directly connected,
br4094
SWITCH(config)#
```

21.2 BGP Routing

The Border Gateway Protocol (BGP) is an Autonomous System (AS) routing protocol designed to provide loop-free routing between separate routing domains. AS stands for a set of routers under common administration. The hiX 5750 R2.0 supports BGP version 4 as defined in RFC 1771. The protocol provides a set of mechanisms for supporting Classless Inter-Domain Routing (CIDR). These mechanisms include the support for advertising a set of destinations as IP prefix and enable the creation of aggregate routes to minimize the size of routing tables. Smaller BGP routing tables can reduce the convergence time of the network and improve network performance.

Using BGP, the hiX 5750 R2.0 is intended to exchange information about **AS** and the paths reaching between the BGP equipment.

The BGP basic configuration includes the following tasks:

- Enabling a BGP Routing Process
- Announcing the Network to Neighbors
- Configuring BGP Neighbor Routers
- Managing BGP Peer Groups.

21.2.1 Enabling a BGP Routing Process

Command	Mode	Function
router bgp <1-65535>	Config	Enables a BGP routing process by assigning AS number. **1 - 65535**: enter the AS number. Use the **no** parameter with this command to disable a routing process.

The **AS** number is used to identify the AS and for detecting whether the BGP connection is internal one or external one. The range from 65512 to 65535 contains the private AS numbers which must not be advertised on the network configuration.

21.2.2 Announcing the Network to Neighbors

For data to be advertised by BGP, its routing table must include a route to the specified network. The following command specifies the networks to be advertised.

Command	Mode	Function
network A.B.C.D/M	Config	Adds the announcement network to neighbors. **A.B.C.D**: specifies the IP address of network being advertised. Use the **no** parameter with this command to remove an entry.

21.2.3 Configuring BGP Neighbor Routers

A BGP router must completely understand the relationships with its neighbors.
To configure BGP peers, use the following commands.

Defining Neighbors

First, the following command must be used before configuring a neighbor.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **remote-as** <1-65535>	Router	Configures an internal or external BGP (iBGP or eBGP) TCP session with another router. **A.B.C.D** : IPv4 address of BGP neighbor **WORD**: name of an existing peer-group **1 - 65535**: AS number of neighbor.

ℹ A peer-group support is configured only after creating a specific peer-group.

Example:

Following tasks are performed:
Definition of a BGP routing process. The number 65001 specifies the AS number of the router. Definition of BGP neighbors and establish of a TCP session. 1.2.3.4 is the IP address of the neighbor and 65000 is the neighbor's AS number.

```
SWITCH# configure terminal
SWITCH(config)# router BGP 650001
SWITCH(config-router)# neighbor 1.2.3.4 remote-as 65000
SWITCH(config-router)# exit
```

Clearing BGP Neighbor Routes

Use the following command to delete all contents of specific cache, table, and database when some factors are invalid or unreliable.

Command	Mode	Function
clear ip bgp { * I A.B.C.D I as-number } [in I out I soft [in I out]]	Privileged	Reconfigures information about BGP neighbor router, *****: reset a BGP connection for all peers. **A.B.C.D**: specifies the address of the BGP route to be cleared. **as-number**: AS number for which all routes will be cleared **in**: incoming advertised routes will be cleared. **out**: outgoing advertised routes will be cleared. **soft**: both incoming and outgoing routes will be cleared.

21.2.4 Managing BGP Peer Groups

A BGP peer group is a group of BGP neighbors that share the same update policies. Members of a peer group inherit all of the configuration options of the peer group. A peer group facilitates the updates of various policies, such as distribute and filter lists. Use the following commands to create a peer-group and to add neighbors to this group.

Command	Mode	Function
neighbor *WORD* **peer-group**	Router	Creates a peer-group. **WORD**: name of the peer-group. Use the **no** parameter with this command to disable this function.
neighbor A.B.C.D **peer-group** *WORD*		Adds a neighbor to an existing peer-group. **A.B.C.D**: address of the BGP neighbor in IPv4 format **WORD**: name of an existing peer-group. Use the **no** parameter with this command to disable this function.

21.2.5 Extended Neighbor Commands

Unless otherwise noted, common parameters of all following commands are:

- **A.B.C.D**: IPv4 address of BGP neighbor
- **WORD**: name of an existing peer-group

  ℹ When this parameters are used, the command applies on all peers in the specified group.

Command	Mode	Function
neighbor A.B.C.D **interface** *WORD*	Router	Configures the interface name of a BGP speaking neighbor. **A.B.C.D**: Neighbor IPv4 address. **WORD**: Interface name. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **port** <0-65535>	Router	Specifies the BGP port of a neighbor. **0 - 65535**: TCP port number Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **activate**	Router	After the TCP connection is opened with the neighbor this command enables the exchange of the specified AF routes with a neighboring router. Use the **no** parameter with this command to disable exchange of information with a neighbor.
neighbor { A.B.C.D I *WORD* } **timers** <0-65535> <0-65535>	Router	Sets the timers for a specific BGP neighbor. **0 - 65535**: holdtime in seconds at which a router sends keepalive messages to its neighbor. The default is 60 seconds. **0 - 65535**: interval in seconds after which, on not receiving a keepalive message, the router declares a neighbor dead. The default is 180 seconds.
neighbor { A.B.C.D I *WORD* } **shutdown**	Router	Administratively shut down this neighbor.Terminates any active session for a specified neighbor and clears all related routing information. In case a peer group is specified for shutdown, a large number of peering sessions could be terminated. Use the **no** parameter with this command to re-enable a neighbor.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **next-hop-self**	Router	Configures the router as the next hop for a neighbor or peer group to allow the router to change the nexthop information that is sent to the iBGP peer. Use the **no** parameter with this command to disable this feature.
neighbor { A.B.C.D I *WORD* } **description** *LINE*	Router	Associates a description with a neighbor. **LINE**: Up to 80 characters describing this neighbor Use the **no** parameter with this command to remove the description.
neighbor { A.B.C.D I *WORD* } **update-source** *WORD*	Router	Allows internal BGP sessions to use any operational interface for TCP connections. **WORD**: name of loopback interface name Use the **no** parameter with this command to restore the interface assignment to the closest interface.
neighbor { A.B.C.D I *WORD* } **weight** <0-65535>}	Router	Sets default weight for routes from this neighbor. **0 - 65535**: weight this command assigns to the route. Use the **no** parameter with this command to remove a weight assignment.
neighbor { A.B.C.D I *WORD* } **passive**	Router	Sets a BGP neighbor as passive. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **version** { 4 }	Router	Set the BGP version to match a neighbor. **4**: Neighbor’s BGP version.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **attribute-unchanged**	Router	Advertises unchanged BGP attributes to the specified neighbor. **as-path**: AS-path attribute. **med**: MED attribute (Multi Exit Discriminator used for best path selection). **next-hop**: Next hop attribute. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **attribute-unchanged** { as-path I next-hop I med }		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged as-path** { next-hop I med }		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged as-path med next-hop**		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged as-path next-hop med**		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged med** { as-path I next-hop }		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged med as-path next-hop**		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged next-hop** { as-path I med }		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged next-hop as-path med**		
neighbor { A.B.C.D I *WORD* } **attribute-unchanged next-hop med as-path**		
neighbor { A.B.C.D I *WORD* } **timers connect** <0-65535>	Router	Configures neighbor router to transmit routing information. **0 - 65535**: connect timer in seconds. Use the **no** parameter with this command to clear the timers for a specific neighbor.
neighbor { A.B.C.D I *WORD* } **collide-established**	Router	Specifies including a neighbor, already in an 'established' state, for conflict resolution when a TCP connection collision is detected. The associated functionality is automatically enabled when neighbor is configured for BGP restart.
neighbor { A.B.C.D I *WORD* } **ebgp-multihop** [<1-255>]	Router	Allows BGP connections to external peers on indirectly connected networks. **1 - 255**: maximum hop count. (If not set the hop count is 255) Use the **no** parameter with this command to return to the default.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **enforce-multihop**	Router	Enforces eBGP neighbors to perform multihop. Use the **no** parameter with this command to turn off this feature.
neighbor { A.B.C.D I *WORD* } **transparent-as**	Router	Configures not appending your AS number even when peer is an eBGP.
neighbor { A.B.C.D I *WORD* } **transparent-nexthop**	Router	Configures not changing nexthop even if the peer is eBGP.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **advertisement-interval** <0-600>	Router	Sets minimum interval between sending BGP routing updates. **0 - 600**: advertise -interval value in seconds Use the **no** parameter with this command to set the interval time to default.
neighbor { A.B.C.D I *WORD* } **allowas-in** [<1-10>]	Router	Configures PE routers to allow re-advertisement of all prefixes containing duplicate AS numbers (Accept AS-path with own AS present in it). **1 - 10**: Number of occurrences of AS number Use the **no** parameter with this command to disable the re-advertisement of a PE router's AS number.
neighbor { A.B.C.D I *WORD* } **capability dynamic**	Router	Enables the dynamic capability for a specific peer to allow a BGP speaker to advertise or withdraw an address family capability to a peer in a non-disruptive manner. Use the **no** parameter with this command to disable the dynamic capability.
neighbor { A.B.C.D I *WORD* } **capability orf prefix-list** { both I receive I send }	Router	Configures to advertising prefixlist ORF (Outbound Route Filter) capability to the peer. **both**: the local router can SEND ORF entries to its peer as well as RECEIVE ORF entries from its peer. **receive**: Capability to RECEIVE the ORF from specified peer. **send**: Capability to SEND the ORF to specified peer. ℹ Only an individual router or a peer-group (but no peer-group member) can be configured to be in receive or send mode.
neighbor { A.B.C.D I *WORD* } **capability route-refresh**	Router	Configures advertising route-refresh capability to the specified neighbor.
neighbor { A.B.C.D I *WORD* } **default-originate** [route-map *WORD*]	Router	Allows a BGP local router to send the default route 0.0.0.0 to a neighbor for use as a default route. **route-map**: Route-map to specify criteria to originate default **WORD**: route-map name. Use the **no** parameter with this command to send no route as a default.
neighbor { A.B.C.D I *WORD* } **filter-list** *WORD* { in I out }	Router	Establish BGP filters. **WORD**: name of AS path access-list. **in**: incoming advertised routes will be filtered. **out**: outgoing advertised routes will be filtered. Use the **no** parameter with this command to disable this function.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **prefix-list** *WORD* { in I out }	Router	Distributes neighbor information as specified in a prefix list by filtering the updates to/from this neighbor. **WORD**: Name of a prefix list. **in**: access list applies to incoming advertisements. **out**: access list applies to outgoing advertisements. ℹ The **neighbor distribute-list** command is an alternative to the this command and only one of them can be used for filtering to the same neighbor in any direction.
neighbor { A.B.C.D I *WORD* } **maximum-prefix** <1-4294967295> { <1-100> I warning-only }	Router	Configures the number of prefixes that can be received from a neighbor. **1 - 429496729**: maximum number of prefixes permitted. **1 - 100**: Threshold-value, 1 to 100 percent **warning-only**: Only give warning message when limit is exceeded. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **maximum-prefix** <1-4294967295> [<1-100> warning-only]		
neighbor { A.B.C.D I *WORD* } **remove-private-as**	Router	Remove private AS number from outbound updates. Use with external BGP peers only. The router removes the AS numbers only if the update includes private AS numbers 64512-65535. Use the **no** parameter with this command to revert to default.
neighbor { A.B.C.D I *WORD* } **route-reflector-client**	Router	Configures the router as a BGP route reflector and configure the specified neighbor as its client. By route reflection the number of iBGP peers within an AS is reduced. An AS can have more than one route reflector. One route reflector treats the other route reflector as another iBGP speaker. Use the **no** parameter with this command to indicate that the neighbor is not a client.
neighbor { A.B.C.D I *WORD* } **route-server-client**	Router	Configure a neighbor as route server client. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **send-community** [{ both I extended I standard }]	Router	Send community attribute to this neighbor. both: send standard and extended community attributes. extended: send extended community attributes. standard: send standard community attributes By default, on receiving the communities attribute the router reannounces them to the neighbor. Only when the **no** parameter is used with this command the community attributes are not reannounced to the neighbor.
neighbor { A.B.C.D I *WORD* } **soft-reconfiguration inbound**	Router	Starts storing updates for inbound soft reconfiguration. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **strict-capability-match**	Router	Closes the BGP connection if capability value does not completely match to remote peer. Use the **no** parameter with this command to disable this function.
neighbor { A.B.C.D I *WORD* } **dont-capability-negotiate**	Router	Disables capability negotiation. Use the **no** parameter with this command too enable capability negotiation.
neighbor { A.B.C.D I *WORD* } **override-capability**	Router	Override capability negotiation result. Use the **no** parameter with this command to disable this function
neighbor { A.B.C.D I *WORD* } **unsuppress-map** *WORD*	Router	Configures Route-map to selectively unsuppress suppressed routes. WORD: Name of route map.

21.2.6 Redistribute Routing Information

In order to to inject routes from another routing process into the BGP routing table, use the following command.

Command	Mode	Function
redistribute { kernel I connected I static I rip I ospf I isis } [route-map *WORD*]	Router	Registers transmitted routing information from another router's table. Optional: specify route to be redistibuted by **route-map** reference. **WORD**: pointer to route-map entries Use the **no** parameter with this command to disable this function.

21.2.7 Routing Map

By default, all routing protocols place their routes into a routing table. Only the routes that pass the route map are sent or accepted in updates. On both inbound and outbound updates, the hiX 5750 R2.0 supports matches based on AS path, community, and network number. AS path matching requires the **as-path access-list** command, community based matching requires the **community-list** command and network-based matching requires the **access-list** command.

To configure routing policy, use the following command.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **route-map** *WORD* { in I out }	Router	Applies a route map to filter updates and modify attributes. **WORD**: name of the route-map. **in**: access list applies to incoming advertisements. **out**: access list applies to outgoing advertisements. Use the **no** parameter with this command to a route map.

21.2.8 Distribution List

To restrict the routing information, **BGP** routing updates can be filtered from or to particular neighbors. To do this, define an access list and apply it to the updates. Distribute-list filters are applied to network numbers and not autonomous system paths.

Use the following command to configure **BGP** route filtering.

Command	Mode	Function
neighbor { A.B.C.D I *WORD* } **distribute-list** { <1-199> I <1300-2699> I *WORD* } { in I out }	Router	Filters BGP updates to/from this neighbor. **A.B.C.D**: Neighbor IPv4 address. **WORD**: Name of an existing peer-group **1 - 199**: IP access-list number. **1300 - 2699**: IP access-list number (expanded range). **WORD**: name of IP access-list. **in**: filters incoming updates **out**: filters outgoing updates Use the **no** parameter with this command to remove an entry.

21.2.9 Prefix List

A IP prefix list provides a sequential collection of permit and deny conditions that apply to IP addresses in order to achive a powerful prefix based filtering mechanism. In addition to access-list functionality, prefix-list has prefix length range specification (the number of bits applied to the base to determine the network prefix) and sequential number specification. The BGP router switches IP addresses one by one against the conditions in a prefix list. The first match determines whether the router accepts or rejects the address. Using a prefix list is preferred to an access list because of following reasons:

- time-saving when searching and applying data in large filter lists
- unlimited registration in filter lists
- easy usage.

To configure a IP prefix list, the operator has to assign a sequential number to each policy registered in the list.

Filtering by an IP prefix list processes routing information with more detail rules as follows:

- Allows all network information if there is no policy defined in prefix list.
- Rejects specified network information, unless the policy applied to network is defined in prefix list.
- Distinguishes each policy with the assigned number and applies policy which has the lowest number in network.

In order to view assigned number to policy, use the **show ip prefix-list** command.

Policies configured by operator will be automatically assigned to a sequential number. However, that assignment is also possible manually by executing the **ip prefix-list seq** command.

Creating a Prefix List

Command	Mode	Function
ip prefix-list *WORD* { deny | permit } A.B.C.D/M **ge** <0-32> [le <0-32>]	Config	Creates a IP prefix list. **WORD**: list name **deny**: denies matching IP address **permit**: permits maching IP address **A.B.C.D/M**: specifies the network **0 - 32**: **ge** parameter specifies prefix length. The prefix list will be applied if the prefix length is greater than or equal to the ge prefix length. **0 - 32**: **le** paramter specifies prefix length. The prefix list will be applied if the prefix length is less than or equal to the le prefix length.
ip prefix-list *WORD* { deny | permit } A.B.C.D/M **le** <0-32> [ge <0-32>]		
ip prefix-list *WORD* { deny | permit } { A.B.C.D/M | any }		
ip prefix-list *WORD* **description** *LINE*		Makes additional description to prefix list. **LINE**: description.

The following example creates a prefix list plist1 that permits routes with a prefix length up to 24 in the 151.0.0.0/8 network:

```
SWITCH(config)#ip prefix-list plist1 permit 151.0.0.0/8 le 24
```

Creating the Prefix List Policy

Use the following command in order to add or delete prefix based filters to arbitrary points of prefix-list using sequential number specification.

Command	Mode	Function
ip prefix-list *NAME* **seq** <1-4294967295> { deny | permit } { A.B.C.D/M | any }	Config	Configures policy of prefix list and assigns number to the policy. **NAME**: list name **deny**: denies matching IP address **permit**: permits maching IP address **A.B.C.D/M**: specifies the network **1 - 4294967295**: specifies the position of each entry in the prefix list. **0 - 32**: ge parameter specifies prefix length. The prefix list will be applied if the prefix length is greater than or equal to the ge prefix length. **0 - 32**: le paramter specifies prefix length. The prefix list will be applied if the prefix length is less than or equal to the le prefix length.
ip prefix-list *NAME* **seq** <1-4294967295>{ deny | permit } A.B.C.D/M **ge** <0-32> [le <0-32>]		
ip prefix-list *NAME* **seq** <1-4294967295> { deny | permit } A.B.C.D/M **le** <0-32> [**ge** <0-32>]		

The parameter **ge** and **le** may be used optionally if there are more than one network configured. Using neither **ge** nor **le**, network range can be more clearly configured.

Checking the Prefix List Policies

Command	Mode	Function
show ip prefix-list [detail | summary]	Privileged/ Config	Shows prefix lists in detail or briefly.
show ip prefix-list [detail | summary] *WORD*		Shows prefix list of specified name.
show ip prefix-list *WORD* [seq number]		Shows policy of specified number.
show ip prefix-list *WORD* A.B.C.D/M		Shows policy applied to specified network.
show ip prefix-list *WORD* A.B.C.D/M **longer**		Shows all policies of prefix list applied to specified network.
show ip prefix-list *WORD* A.B.C.D/M **first-match**		Shows policy first applied to specified network.

Deleting Number of Inquiring Prefix List

By default, system records number how many times prefix list is inquired.
To delete the number, use the following command.

Command	Mode	Function
clear ip prefix-list *WORD* [A.B.C.D/M]	Privileged	Deletes the number how many times prefix list is inquired. **WORD**: list name **A.B.C.D/M**: specifies the network.

21.2.10 AS Route Filtering

Policies applies to decide routes are registered in an access list. In order to filter routing information with AS standard, configure filtering policy in the access list and apply the policy to the neighbor router.

Command	Mode	Function
ip as-path access-list *WORD* { permit | deny } *LINE*	Config	Defines specific AS in access list. **WORD**: enter the access list number **LINE**: enter a regular expression.

21.2.11 Communities

Communities are the most flexible way to implement routing policies. **BGP** supports transmit policy distributing routing information. Distributing routing information is operated based on not only community list but also IP address and **AS** route. Community list makes community according to each destination and routing policy is applied based on community standard.

It helps configure BGP speaker that distributes routing information.

A community is a destination group that shares some common attributes. One destination can be belonged to more than one community. An administrator can configure to which community the destination is belonged. By default, all destinations are configured to be in the **internet** community.

The other defined and well-known communities are:

- **no-export:**
  Do not distribute this route to exterior BGP neighbor routers
- **no-advertise:** (either exterior or interior)
  Do not distribute this route to neighbor routers.
- **local-as:**
  Distribute this information to neighbor routers of low level AS located on the BGP united network. Do not distribute it to exterior routers.

To create a community list, use the following commands.

Command	Mode	Function
ip community-list *WORD* { permit | deny } *LINE*	Config	Creates community list. **WORD**: specifies the community listname. **permit**; specifies the community to accept. **deny**: specifies the community to reject. **LINE**:
ip community-list { *<1-99>* | standard *WORD* } { permit | deny } [*LINE*]	Config	Creates community list. **1 - 99**: standard community list number. **WORD**:
ip community-list *<100-199>* { permit | deny } [*LINE*]	Config	Creates community list. **100 - 199**: expanded community list number.

A **community** is notated with a form, AA:NN as defined in RFC. AA is the local AS number and NN is a number of 2 bytes.

i Use the **no** parameter with this commands to delete community list entries.

21.2.12 Determining the State of BGP

Specific statistics such as contents of BGP routing table, cache, and database can be displayed to determine resource utilization and solve network problems. Displaying information about node reachability and discover the routing path the packets are taking through the network is also possible.

To display various routing statistics, use following commands.

Command	Mode	Function
show ip bgp prefix-list *NAME*	Privileged/ Config	Shows peers to which the prefix has been advertised.

Command	Mode	Function
show ip bgp cidr-only	Privileged/ Config	Displays all BGP routes including subnetwork and upper network.
show ip bgp community [number | local-AS | no-advertise | no-export]	Privileged/ Config	Displays route belonged in specific community. Community Number is formed as AA:NN.
show ip bgp community-list *WORD* [exact-match]	Privileged/ Config	Shows all routes that are permitted by the community list: WORD: enter the name of the list.
show ip bgp community-info	Privileged/ Config	Displays all information of BGP community.
show ip bgp filter-list *WORD*	Privileged/ Config	Shows routes that are matched by the specified autonomous system route in access list, enter the name of the list.
show ip bgp regexp *LINE*	Privileged/ Config	Shows routes that match the specified regular expression entered on the command line, enter a regular expression for LINE.
show ip bgp attribute-info	Privileged/ Config	Shows all information of BGP attributes.
show ip bgp neighbors [ip-address]	Privileged/ Config	Shows detail information on **TCP** and BGP connections to individual neighbors.
show ip bgp neighbors [ip-address [advertised-routes | received-routes | routes]	Privileged/ Config	Shows information about the TCP and BGP connections to neighbors. The advertised-routes option displays all the routes the router has advertised to the neighbor. The received-routes option displays all received routes (both accepted and rejected) from the specified neighbor. The routes option displays all routes that are received and accepted.
show ip bgp paths	Privileged/ Config	Shows all BGP routes in database.
show ip bgp summary	Privileged/ Config	Shows all BGP connections.

21.3 RIP Routing

RIP (Routing Information Protocol) calculates the best path (route with the lowest metric value) to a remote destination based upon individual router hops. A RIP router sends routing-update messages at regular intervals and when the network topology changes. When the RIP router receives a routing update from another one that includes changes to an entry, it updates its routing table to reflect the new route. The metric value for the path is increased by 1, and the sender is indicated as the next hop. A directly connected network has a metric of zero; an unreachable network has a metric of 16. After updating its routing table, the router immediately begins transmitting routing updates to inform other network routers of the change. These updates are sent independently of the regularly scheduled updates that RIP routers send. If an interface's network is not specified, it will not be advertised in any RIP update. For more information about RIPv2 refer to RFC 1058, RFC 1723, and RFC 2453.

The RIP commands are described in the following sections:

- Basic Configuration of RIP
- Allowing Unicast Updates for RIP
- Configuring of Static Routes
- Redistributing of Routing Information
- Configuring of Routing Metrics
- Configuring the Administrative Distance

- Extended RIP Configuration
- Managing the Authentication Key
- Checking of Router and Protocol Information.

21.3.1 Basic Configuration of RIP

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

1. Enabling RIP Process on the Router
2. Specifying the Network.

Enabling RIP Process on the Router

Change to *Router configuration* mode and enable a RIP routing process.

Command	Mode	Function
router rip	Config	Enables RIP routing process and enters router configuration mode. Use the **no** parameter with this command to disable the RIP routing process.

Specifying the Network

Once the router is enabled, specify which network it should be routing for.

Command	Mode	Function
network { A.B.C.D/M | *WORD* }	Router	Specifies networks to which routing updates will be sent and received. **A.B.C.D/M**: IP address prefix and length of this IP network. **WORD**: interface name. Use the **no** parameter with this command to remove the specified network as one that runs RIP.
network A.B.C.D/M **route-map** *WORD*	Router	Configures networks to operate as RIP using a route map. **A.B.C.D/M**: IP address prefix and length of this IP network. WORD: specifies route map

To verify that the protocol is up and ready to go, enter a **show ip protocols** command. This would generally show details of all running IP routing protocols.

21.3.2 Allowing Unicast Updates for RIP

RIP is a broadcast protocol. When a neighbor does not understand multicast, the following command is used to specify a router as a RIP neighbor by establishing a point-to-point link between the routers.

Command	Mode	Function
neighbor *A.B.C.D*	Router	Configure neighbor router with which the routing information will be exchanged. **A.B.C.D**: IP address of a neighboring router Use the **no** parameter with this command to disable the specific router.

Sending of routing updates on specified interfaces can be disabled by configuring the **passive-interface** command.

21.3.3 Configuring of Static Routes

The route command makes a static route only inside RIP.

This command is mostly used for debugging purposes. If you are not familiar with RIP protocol, you would better create a static route and redistribute it in RIP using the **redistribute static** command.

Command	Mode	Function
route A.B.C.D/M	Router	Adds a static RIP route. **A.B.C.D/M**: specifies the IP address prefix and length. Use the **no** parameter with this command to disable this function.

Default Route

A router can generate a default route and inject it in the network. If no other routes qualify, this one is used. You can force an Autonomous System (AS) boundary router to generate a default route into an **RIP** routing domain. Whenever you specifically configure redistribution of routes into an RIP routing domain (21.3.4 Redistributing of Routing Information), the router automatically becomes an AS boundary router. However, an AS boundary router does not, by default, generate a default route into the RIP routing domain.

Command	Mode	Function
default-information originate	Router	Forces the AS boundary router to generate a default route into the RIP routing domain. Use the **no** parameter with this command to disable this feature.

21.3.4 Redistributing of Routing Information

The system can redistribute routing information from a source route entry into the RIP tables. For example, you can instruct the router to re-advertise connected, kernel, or static routes as well as routing protocol-derived routes. This capability applies to all the IP-based routing protocols.

In order to redistribute routing information from a source route entry into the RIP table, use one of the following commands.

Command	Mode	Function
redistribute { kernel I connected I static I ospf I bgp I isis }	Router	Registers transmitted routing information from another router's RIP table. **kernel**: redistribute from kernel routes **connected**: redistribute from connected routes **static**: redistribute from static routes **ospf**: redistribute from **OSPF** **bgp**: redistribute from **BGP** **isis**: redistribute from **IS**-IS **1 - 16**: metric value to be used in redistributing information **WORD**: pointer to route-map entries Use the **no** parameter with this command to disable the function.
redistribute { kernel I connected I static I ospf I bgp I isis } **metric** <1-16>		
redistribute { kernel I connected I static I ospf I bgp I isis } **route-map** *WORD*		

Route Map

Controlling the redistribution of routes between two domains is possible by using the **route-map** command.

Command	Mode	Function
route-map *WORD* { deny | permit } <1-65535>	Config	Creates route map and sets permission. **WORD**: map name **1 - 65535**: index

One or more **match** and **set** commands typically follow **route-map** command. If there are no match commands, then everything matches. If there are no set commands, nothing is done. Therefore, at least one match or set command is needed. To define conditions for redistributing routes from a source route entry into the RIP tables, perform at least one of the following tasks in *route-map* configuration mode.

Command	Mode	Function
match interface *IFNAME*	Route-map	Transmits information to only specified interface. IFNAME: interface name
match ip address prefix-list *WORD*	Route-map	Matchs if route destination is permitted by access-list.Transmits information to only neighbor router in list. **WORD**: name prefix list Use the **no** parameter with this command to disable this match.
match metric <0-4294967295>	Route-map	Transmits information matched with specified metric, **1 - 16**: Enter a valid metric value. Use the **no** parameter with this command to disable this match.
set ip next-hop A.B.C.D	Route-map	Specifies where the packets that pass the match criteria are output. **A.B.C.D**: IP address of next hop. This command set next hop value in RIPv2. This command does not affect RIPv1 because there is no next hop field in the packet. Use the **no** parameter with this command to disable this setting.

21.3.5 Configuring of Routing Metrics

Metrics of Redistributed Routes

RIP metric is a value for distance for the network that will be incremented when the network information is received. Redistributed route’s metric is set to 1.

ℹ This command is used with the **redistribute** command in order to determine RIP to use the specified metric value for all redistributed routes. Default metric is useful in redistributing routes with incompatible metrics. Every protocol has different metrics and cannot be compared directly. For example, the RIP metric is a hop count and the **OSPF** metric is a combination of five quantities. Default metric provides the standard to compare. All routes that are redistributed will use the default metric. In such situations, an artificial metric is assigned to the redistributed route.

In order to set metrics for redistributed routes, use the following command.

Command	Mode	Function
default-metric <1-16>	Router	Specifies the metrics to be assigned to redistributed routers. **1- 16**: metric value (default value is set to 1). Use the **no** parameter with this command to disable this feature.

ℹ This command does not affect a connected route even if it is redistributed by **redistribute connected**. To modify the metric value of connected routes, use **redistribute connected metric** or **route-map**. The command **offset-list** also affects connected routes.

Applying Offsets to Routing Metrics

An offset list is the mechanism for increasing incoming and outgoing metrics to routes learned via RIP. Offset list can be limited with an access list.

Command	Mode	Function
offset-list *WORD* { in | out } <0-16> [*IFNAME*]	Router	Adds an offset to in and out metrics to routes learned through RIP. **WORD**: access-list number or names **in**: access list will be used for metrics of incoming advertised routes. **out**: access list will be used for metrics of outgoing advertised routes. **0 - 16**: offset used for metrics of networks matching the access list. **IFNAME**: specifies the interface to match. Use the **no** parameter with this command to remove the offset list.

21.3.6 Configuring the Administrative Distance

Administrative distance is a feature used by the routers to select the path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicating a more reliable protocol.

i The router always selects route created by routing protocol of the smallest distance value. Each network has its own features. Therefore, there is no general rule for distance configuration. You should consider overall network to configure distance value.

Command	Mode	Function
distance <1-255> [A.B.C.D/M [*WORD*]]	Router	Sets the administrative distance. **1 - 255**: distance value. Default value of distance is 120. **A.B.C.D/M**: network prefix and length. Sets default RIP distance to specified value when the route's source IP address matches the specified prefix. **WORD**: access-list name. Sets default RIP distance to specified value when the route's source IP address matches the specified prefix and the specified access-list. Use the **no** parameter with this command to disable this function.

21.3.7 Extended RIP Configuration

- Blocking an Interface
- Split-Horizon
- RIP Version
- Timers

Blocking an Interface

On a blocked interface, all receiving packets are processed as normal and router does not send either multicast or unicast RIP packets except to RIP neighbors specified with **neighbor** command.

Command	Mode	Function
passive-interface *IFNAME*	Router	Blocks RIP broadcast on the interface. **IFNAME**: interface name. Use the **no** parameter with this command to disable this function.

Split-Horizon

Normally, routers that are connected to broadcast-type IP networks and that use distance-vector routing protocols employ the split horizon mechanism to reduce the possibility of routing loops. Split horizon blocks information about routes from being advertised by a router out any interface from which that information originated. This behavior usually optimizes communications among multiple routers, particularly when links are broken. However, with non broadcast networks, such as Frame Relay, situations can arise for which this behavior is less than ideal. For these situations, you might want to disable split horizon.

If an interface is configured with secondary IP addresses and split horizon is enabled, updates might not be sourced by every secondary address. One routing update is sourced per network number unless split horizon is disabled.

In order to activate or deactivate or disable split horizon, perform the following tasks in interface configuration mode.

Command	Mode	Function
ip split-horizon	Interface	Performs the split-horizon action on the interface. The default is split-horizon poisoned. Use the **no** parameter with this command to disable this function.

RIP Version

RIP version is used globally by the router. The router of the hiX 5750 R2.0 basically supports only **RIP** version 2.

However, it is possible to configure the router to receive only version 1 type packet or only version 2 type packet.

Command	Mode	Function
version <1-2>	Router	Configures the version of RIP processing. Default is RIP v2. Use the **no** parameter with this command to restore the default version.

The following commands apply to a specific interface and overrides any the version specified by the version command.

Command	Mode	Function
ip rip send version 1	Interface	Specifies sending of RIPv1 packets out of an interface.
ip rip send version 2		Specifies sending of RIPv2 packets out of an interface.
ip rip send version 1 2		Permits sending of both RIPv1 and v2 packets out of an interface.
ip rip receive version 1		Specifies acceptance of RIPv1 packets on the interface.
ip rip receive version 2		Specifies acceptance of RIPv2 packets on the interface.
ip rip receive version 1 2		Specifies acceptance of RIPv1 and v2 packets on the interface.

Use the **no** parameter with the commands above to use the global RIP version control rules.

Timers

Routing protocols use several timers that determine such variables as the frequency of routing updates, the length of time before a route becomes invalid, and other parameters. You can adjust these timers to tune routing protocol performance to better suit your internet needs.

Command	Mode	Function
timers basic *update timeout garbage*	Router	Adjusts routing protocol timers. Values in seconds Range of the values is 5-2147483647. **update**: routing table update timer (default is 30). **timeout**: routing information timeout timer. After this interval has elapsed and no updates for a route are received, the route is declared invalid (default is 180) **garbage**:routing garbage collection timer. Upon expiration of the garbage-collection timer, the route is finally removed from the routing table (default is 120) Use the **no** parameter with this command to restore the defaults.

21.3.8 Managing the Authentication Key

Only RIP version 2 supports authentication on an interface.

Command	Mode	Function
ip rip authentication key-chain *LINE*	Interface	Enables RIPv2 authentication on an interface. **LINE**: name of the key chain. Use the **no** parameter with this command to disable this function.

The hiX 5750 R2.0 supports two modes of authentication on an interface for which RIP authentication is enabled: plain text authentication and MD5 authentication. The default authentication in every RIP Version 2 packet is plain text authentication.

ℹ Do not use plain text authentication in RIP packets for security purposes, because the unencrypted authentication key is sent in every RIP Version 2 packet.

In order to configure RIP authentication, use the following order of commands.

Command	Mode	Function
ip rip authentication string *LINE*	Interface	Specifies the authentication string or password used by a key. **LINE**: specifies authentication string or password used by a single key on an interface. The string must be shorter than 16 characters. Use the **no** parameter with this command to disable this feature.
ip rip authentication mode { text I md5 }	Interface	Specifies the type of authentication mode used for RIP v2 packets. **text**: clear text or simple password authentication. **md5**: uses the keyed MD5 authentication algorithm. Use the **no** parameter with this command to restore clear text authentication.

21.3.9 Checking of Router and Protocol Information

Display specific router statistics such as the contents of IP routing tables and databases to determine resource utilization and solve network problems. You can also discover the routing path your router’s packets are taking through the network.

Command	Mode	Function
show ip rip	Privileged/ Config	The command displays all RIP routes. For routes that are received through RIP, this command will display the time the packet was sent and the tag information. This command will also display this information for routes redistributed into RIP.
show ip protocols		Displays current RIP status. It includes RIP timer, filtering, version, RIP enabled interface, and RIP peer information.

21.4 IS-IS Routing

IS-IS (Intermediate System to Intermediate System) routing can be used inside the routing domain to form adjacencies between all Layer 3 nodes of the same domain. The implementation of IS-IS routing is dedicated to IP routing (Integrated IS-IS) according to RFC 1142 and RFC 1195.
Connectionless network routing and End System-IS discovery are not supported.

IS-IS routing makes use of a two-level hierachical:

- Level 1 (L1) routers know the topology inside their area, including all routers and hosts. They forward all traffic for destinations outside by using a Level 2 (L2) router within their area which knows the domain (level 2) topology. All L1 routers and hosts in an area must have a Network Service Access Point (NSAP) with the same area address.

  ℹ The GPON OLT itself is part of a single area. Therefore it performs the tasks of a L1 router only. The IS-IS routing can be established at the uplink ports only not at subscriber ports.
- Level 2 (L2) routers connect all areas within a routing domain. They advertise their own area addresses (NSAP) to the other L2 routers in the backbone.

L1 and L2 routers have two link-state databases: a level 1 link-state database for intra-area routing and a level 2 link-state database for inter-area routing. The routing tables are builded calculating the shortest path tree (SPT) by each IS.

An IS-IS area can consist of L1 routers only, L1/L2 routers or L2 only or a combination of all.

ℹ There is a limitation, only one IS-IS instance can run Level-2 routing (either Level-2 only IS or Level-1-2 IS).

IS-IS is used to intermittently send out link state information across the network, so that each router can maintain a current picture of network topology. For messages four packet types are used:

- Hello-packets are used for functions capability announcement and neighbor discovery
- LSP-packets (Link state PDU) are used to distribute routing information between the IS-IS notes, e.g. network topology information and IP addresses.
- CSNP-packets (Complete Sequence Number PDU) contains a list of all LSPs from the current link state database, using to be ensure that all routers of LSPs have the same information and are synchronized.
- PSNP-packets (Partial Sequence Number PDU) are used to request one or more LSPs and acknowledge their receiption.

The IS-IS configuration is described in the following sections:

- Basic Configuration of IS-IS Router
- Extended Router Configuration

- Configuring of Interface Parameters
- Redistribution of Reachability Information
- Checking the Configuration.

21.4.1 Basic Configuration of IS-IS Router

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

1. Enabling IS-IS Process on the Router
2. Configure Network Entity Titles (NET) for the Routing Process
3. Enabling IS-IS Routing on the Interface

Enabling IS-IS Process on the Router

Change to *Router configuration* mode and enable a IS-IS routing process.

Command	Mode	Function
router isis *WORD*	Config	Enables IS-IS routing and enters router configuration mode. **WORD**: router name excluding spaces) Remove IS-IS routing instance with the **no** command.

Configure Network Entity Titles (NET) for the Routing Process

Command	Mode	Function
net *NET*	Router	Adds a Network Entity Title (NET) for the instance. NET define the area addresses for the IS-IS area. XX. .. .XXXX.YYYY.YYYY.YYYY.00 XX. .. .XXXX Area Address YYYY.YYYY.YYYY System ID Use the **no** parameter to remove the NET.

ℹ Up to parameter **max-area-adresses** number of NETs can be specified.

Command	Mode	Function
max-area-addresses <3-254>	Router	Specifies the number of max area addresses. **3 - 254**: max. addresses range The **no** parameter set the number to the default value 3.

Enabling IS-IS Routing on the Interface

Enter into *Interface configuration* mode and specify the interfaces that should be actively routing IS-IS.

Command	Mode	Function
ip router isis [*WORD*]	Interface	Enables an IS-IS IPv4 routing process on the interface. This command is mandatory to IS-IS configuration! **WORD**: existing or new routing instance tag (e.g. symbolic router name) Disable IS-IS routing on the interface with the **no** command (To clear the database, unconfigure the IS-IS routing instance.)

21.4.2 Extended Router Configuration

- Level for the Routing Instance
- Dynamic Hostname Exchange

- LSP Parameter
- Summary Address
- Domain Password

Level for the Routing Instance

By default the first instance is Level 1 and Level 2 and the rest are Level 1.

Command	Mode	Function
is-type { level-1 I level-1-2 I level-2-only }	Router	Sets IS to specified level for the routing process. **level-1**: Act as a area router only **level-1-2**: Act as both a area router and an domain router **level-2-only**: Act as an domain router only

Dynamic Hostname Exchange

The following commands configures the Dynamic Hostname Exchange Mechanism (RFC2763) and System-ID-to-hostname translation.

Using this command to enable Dynamic Hostname Exchange Mechanism and System-ID to hostname translation is performed for the result of **show isis database** and some other CLI commands.

Command	Mode	Function
dynamic-hostname [area-tag]	Router	Enables the dynamic hostname exchange mechanism (RFC2763) and System-ID-to-hostname translation **area-tag**: Routing process tag The **no** parameter disables the mechanism.
hostname dynamic		

LSP Parameter

Command	Mode	Function
lsp-gen-interval { level-1 I level-2 } <1-120>	Router	Sets minimum interval before regenerating the same LSP **level-1**: sets interval for Level-1 IS. **level-2**: sets interval for Level-2 IS **1 - 120**: LSP generation interval in seconds. The smaller the interval the faster the convergence, but it might cause more frequent flooding. Use the **no** parameter with this command to set the interval to the default (10 s).
lsp-gen-interval <1-120>		
lsp-refresh-interval <1-65535>	Router	Sets the LSP refresh interval. **1 - 65535**: LSP refresh interval in seconds. Use the **no** parameter to set the interval to the default value of 900 seconds.
max-lsp-lifetime <1-65535>	Router	Sets the maximum LSP lifetime. **1 - 65535**: max. LSP lifetime in sec. The **no** paramater sets the default value 1200 Sec. for the LSP lifetime.
ignore-lsp-errors	Router	Uses to ignore LSPs' checksum error. By default LSP checksum is checked on receipt. The **no** parameter to turn off this function.

Command	Mode	Function
set-overload-bit [{ suppress { external | interlevel | external interlevel | interlevel external } | on-startup <5-86400>]	Router	Sets the overload-bit in self-LSPs. **Suppress**: The router suppresses the redistribution of specified types of reachability information during overload state. **suppress external**: suppress to redistribute external reachability **suppress interlevel**: suppress to redistribute interlevel reachability **on-startup**: The router sets overload bit at startup only , then clears the bit after specified interval has elapsed. **5 - 86400**: interval in seconds after which the overload state is exited. The **no** parameter clears the overload-bit from self-LSPs.

Normally the **set-overload-bit** command is allowed only when a router runs into problems.

Summary Address

The **summary-address** command aggregate addresses that are represented in the routing table. One summary address can include multiple groups of addresses for a given level. Routes learned from other routing protocols also can be summarized.

Command	Mode	Function
summary-address A.B.C.D/M [level-1 | level-1-2 | level-2]	Config/ Router	Configures summary address to summarize IPv4 reachability information. **A.B.C.D/M**: specifies the IP address prefix and length of this IP network. **level-1**: Summarize reachability information only for Level-1. **level-1-2**: Summarize reachability information for both Level-1 and Level-2. **level-2**: Summarize reachability information only for Level-2. Summary-address is applied to Level-2 IS if level parameter is omitted. The **no** parameter with this command is unconfigured the summary.

Domain Password

ℹ Configuring the domain password to enable authentication when receiving and sending **LSP** and Sequence Number PDU in Level-2 domain. Domain password must be the same in Level-2 domain.

Command	Mode	Function
domain-password *WORD*	Router	Sets the authentication password for Level-2 domain. **WORD**: routing domain password string (excluding spaces).

21.4.3 Configuring of Interface Parameters

Interface parameters must be consistent across all routers in an attached network. Therefore, be sure that if you do configure any of these parameters, the configurations for all routers on the network have compatible values.
The *Interfaces* configuration mode is entered with the **interface** *IFNAME* command in the configuration mode. The name of the interface to be configured must be specified.

- Circuit Type and Summary Address
- Message Intervals and Attributes
- Metrics
- Mesh Groups
- Authentication Password.

Circuit Type and Summary Address

The level of adjacencies formed on the interface can be specified with **circuit-type** command. The interface can be configured to form Level 1 and Level 2 adjacencies, if the routing instance supports both levels. By default the IS-IS circuit-type is the same as the **is-type** of the routing instance.

Command	Mode	Function
isis circuit-type { level-1 I level-1-2 I level-2-only }	Config/ Interface	Configures circuit type (type of adjacency desired for neighbors) on the specified interface. **level-1**: Level-1 only adjacencies are formed **level-1-2**: Level-1-2 adjacencies are formed (this is the default circuit typ) **level-2-only**: Level-2 only adjacencies are formed ℹ On the point-to point interface IS-IS Hello will be sent regardless of the circuit-type.

Message Intervals and Attributes

The average time between periodic PDU transmissions can be set and used in conjunction with a multiplier in order to control the actual value of holding time in the PDUs transmitted by the IS on the interface. If the PDUs are to be padded to the full MTU of the circuit, the command **isis hello padding** is specified. CSNPs are transmitted p eriodically on the circuit. The interval between periodic CSNP transmissions can be changed.

Command	Mode	Function
isis hello-interval { minimal I <1-65535> } [level-1 I level-2]	Config/ Interface	Specify the length of time, in seconds, between hello packets the router sends on the specified interface. The Hello interval is calculated by dividing by the hello-multiplier. **minimal**: Holdtime 1 second, interval depends on multiplier, **1 - 65535**: Hello interval value **level-1**: Specify hello-interval for level-1 IIHs **level-2**: Specify hello-interval for level-2 IIHs The **no** parameter with this command sets the default value 10 sec. for both level-1 and level-2.
isis hello-multiplier <3-1000> [level-1 I level-2]	Config/ Interface	Sets multiplier for Hello holding time. **3 - 1000**: Hello multiplier value **level-1**: Specify hello multiplier for level-1 IIHs **level-2**: Specify hello multiplier for level-2 IIHs The **no** parameter sets the default value 3 to both level-1 and level-2.
isis hello padding	Config/ Interface	Adds padding to IS-IS hello packets. IS-IS pads the Hello packet by default to notice neighbors the supported **MTU** size. The **no** parameter disable the padding.
isis csnp-interval <0-65535> [level-1 I level-2]	Config/ Interface	Sets CSNP interval. This parameter is only valid on broadcast interface. **0 - 65535**: CSNP interval in seconds **level-1**: Specify interval for level-1 CSNPs only **level-2**: Specify interval for level-2 CSNPs only The **no** paramater sets the default value 10 Sec. for the interval to both level-1 and level-2.
isis lsp-interval <1-4294967295>	Config/ Interface	Sets **LSP** transmission interval. **1 - 4294967295**: LSP interval in milliseconds The **no** parameter sets the default value 33 ms for the interval.

Command	Mode	Function
isis retransmit-interval <0-65535>	Config/ Interface	Sets per-LSP retransmission interval. **0 - 65535**: Interval between retransmissions of the same LSP in seconds The **no** paramater sets the default value 5 Sec. for the interval.

Metrics

Running integrated IS-IS, a default IP route will automatically be installed in the level 1 routers pointing toward the nearest L1/L2 router that originally set the attached bit in its level 1 **LSP**. If there are multiple level 2-capable routers in the area, the closest L1/L2 router is selected based on the cost.

The cost metric (narrow-metric) is used by default, measuring the cost of the complete link. The interface default metric is put into IP reachability information TLVs and IS reachability information TLVs in LSPs.
The default metric for the circuit can be set with the command **isis metric** and the priority for becoming IS with the command **isis priority**.

Command	Mode	Function
isis metric <1-63> [level-1 I level-2]	Interface	Configures the default metric (metric-style narrow) for the interface. **1 - 63**: Range of calculation **level-1**: metric to level-1 links **level-2**: metric to level-2 links The **no** parameter with this command sets default metric to the default value = 10 to both level-1 and level-2
isis priority <0-127> [level-1 I level-2]	Config/ Interface	Sets priority for designated router election. **0 - 127**: Priority value (default priority is 64 for both level-1 and level-2) **level-1**: Specify priority for level-1 routing **level-2**: Specify priority for level-2 routing

Mesh Groups

Mesh groups are a mechanism to reduce redundant packet transmissions for the IS-IS protocol.

ℹ If an interface is configured as "mesh group blocked", the standard **LSP** database synchronization process is applied if the interface receives CSNP (Complete Sequence Number PDU) or PSNP (Partial Sequence Number PDU).

Command	Mode	Function
isis mesh-group { blocked I <1-4294967295> }	Interface	Sets IS-IS mesh group ID on the specified interface. **1 - 4294967295**: Mesh-group *Number* **blocked**: blocks **LSP**s on the current interface. The **no** parameter disables / unblocked mesh group on the specified interface.

Authentication Password

IS-IS specifies an authentication mechanism to prevent unauthorized routers from forming adjacencies or injecting TLVs (Table-length-value). The authentication can only be activeted globally but can be configured independently for L1 and L2 Hello PDUs (Protocol Data Unit). By default no password is used.

ℹ On point-to-point interfaces for both L1 and L2 the same password must be configured.

Command	Mode	Function
isis password *WORD* [level-1 I level-2]	Interface	Configures the authentication password for interface. **WORD**: plain-text password (excluding spaces). **level-1**: Specify password for level-1 PDUs (Intra area) **level-2**: Specify password for level-2 PDUs (Domain) Use the **no** parameter to clear the password.

21.4.4 Redistribution of Reachability Information

- Redistribution of Information from other Routing Protocols
- Redistribution of Information between the Levels

Redistribution of Information from other Routing Protocols

Command	Mode	Function
redistribute { kernel I connected I static I rip I ospf I bgp } **metric** <0-4261412864> **metric-type** { internal I external } { level-1 I level-1-2 I level-2 }	Router	Redistributes reachability information from other routing protocols. **kernel**: kernel routes **connected**: connected routes **static**: static routes **rip**: **RIP** routes **ospf**: **OSPF** routes **bgp**: **BGP** routes. **0 - 4261412864**: metric value **internal**: internal metric **external**: external metric **level-1**: redistribute routes into level-1 **level-1-2**: redistribute routes into level-1 and level-2 **level-2**: redistribute routes into level-2 If metric is not specified: metric = 0 If metric type is not specified internal metric type is used. If level is not specified routes are redistributed into level-2. Use the **no** parameter with this command to stop redistribution.
redistribute { kernel I connected I static I rip I ospf I bgp }		
redistribute { kernel I connected I static I rip I ospf I bgp } { **metric** <0-4261412864> I **metric-type** { internal I external } I { level-1 I level-1-2 I level-2 } }		

Redistribution of Information between the Levels

The following commands redistributes reachability information from one level to the other level. If this commands are not used, IS-IS redistributes selected L1 routes into L2.

Command	Mode	Function
redistribute isis level-1 into level-2 [distribute-list *WORD*]	Router	Redistributes reachability information from one level to the other level. If an access-list name is given with this command for an access list that does not exist, the routes are still redistributed. Select routes: - Inter-area routes from level-1 - Inter-area routes into level-2 **WORD**: access-list name Use the **no** parameter with this command to stop redistribution.
redistribute isis level-2 into level-1 [distribute-list *WORD*]		

21.4.5 Checking the Configuration

In order to check the current configuration use the following commands:

Command	Mode	Function
show running-config router isis	Exec/ Config	Shows current IS-IS router information

Command	Mode	Function
show isis *WORD* **topology** [l1 | l2 | level-1 | level-2]	Privileged/ Exec	Displays data about IS-IS topology. **WORD**: routing area tag **l1**, **level-1**: path to all level-1 routers in the area (inter area topology) **l2**, **level-2**: path to all level-2 routers in the domain (intra area topology)
show isis topology [l1 | l2 | level-1 | level-2]		
show ip route [database] **isis**	Privileged/ Exec	Displays IS-IS routing table for IPv4. **database**: Link state database
show isis *WORD* **database** [detail | verbose] | [l1 | l 2 | level-1 | level-2]	Privileged/ Exec	Displays IS-IS link state database information. **detail**: detailed information **verbose**: detailed information **WORD**: routing area tag **l1**, **level-1**: for Level 1 only **l2**, **level-2**: for Level 2 only
show isis database [detail | verbose] | [l1 | l 2 | level-1 | level-2] | [*WORD*]		
show isis interface *IFNAME*	Privileged/ Exec	Displays detailed interface information. **IFNAME**: enter interface name
show memory isis	Config	Shows consumption ratio of IS-IS memory

22 Spanning Tree

If multiple paths exist on a network, the Spanning Tree Protocol (STP, 802.1D) configures the network so that a switch uses only the most efficient path. If that path fails, STP automatically sets up another active path on the network to sustain network operations. STP detects and eliminates logical loops by forcing the redundant data path into a blocked state.

Rapid Spanning Tree Protocol (RSTP, 802.1w) innovates to reduce the time of network convergence on STP. It is an easy and fast to configure protocol. Also, RSTP provides comparability with STP.

If the network contains more than one VLAN, the logical network configured by single (traditional) STP does not work. The Multiple Spanning Tree Protocol (MSTP, 802.1Q) configures a separate spanning tree for each VLAN and blocks the links which are redundant within each spanning tree. So several VLANs can be mapped to a single spanning tree instance.

Perform the following tasks in order to configure STP:

1. Decide STP mode using the **stp force-version** command
2. Activate MST daemon using the **stp mst enable** command
3. Configure detail options if specific commands are required.

22.1 Configuring the STP Operation Mode

Use the following command the configure the forced version.

Command	Mode	Function
stp force-version { stp | rstp | mstp }	Bridge	Sets the specified STP version. **stp**: Spanning Tree Protocol (STP) **rstp**: Rapid STP **mstp**: Multiple STP.
no stp force-version		Clears force-version configuration.

22.2 Activating STP/RSTP/MSTP

To enable/disable STP, RSTP, MSTP in the force-version, use the following commands.

Command	Mode	Function
stp mst { enable I disable }	Bridge	Enables/disables STP, RSTP or MSTP function.
stp mst reset-tccount *MSTID_RANGE*		Resets “bridge topology change” counts. **MSTID_RANGE**: instance number.

Even though STP function does not operated, loop event does not occur in a NE which belongs to the non-dual path LAN environment.

22.3 Adding STP Ports

This feature allows the operator to decide if the port can be managed by STP or not.

To set the port to be managed by STP, use the following command.

Command	Mode	Function
stp port { add I del } *PORTS*	Bridge	Sets port to be managed by STP. **add**: add port number to port-set (default: all ports are added) **del**: delete port number from port-set **PORTS**: select slot/port number (for STP slot number always 0)

After deleting a STP port, packets can be forwarded over it furthermore without STP function.

To check the ports managed by STP, use the following command.

Command	Mode	Function
show stp port	Privileged/ Config/ Bridge	Shows the port-set list to be managed by STP.

Example:

```
SWITCH(bridge)# show stp port
---------------------------------------------------------------
Port STP Portset-status MAC Admin-status MAC Oper-status
--------------------------------------------------------------
9/1    addedenabled On
 9/2 addedenabled On
 9/3 addedenabled On
 9/4 addedenabled On
 9/5 addedenabled Off
 9/6 addedenabled Off
--------------------------------------------------------------
Default portset bitmask:0x3f
Current portset bitmask:0x3f
SWITCH(bridge)# stp port del 9/3
SWITCH(bridge)# show stp port
---------------------------------------------------------------
Port STP Portset-status MAC Admin-status MAC Oper-status
---------------------------------------------------------------
9/1    addedenabled On
 9/2 addedenabled On
 9/4 addedenabled On
 9/5 addedenabled Off
 9/6 addedenabled Off
--------------------------------------------------------------
SWITCH(bridge)#
```

22.4 Configuring the STP

22.4.1 Deciding the Root Switch

To establish STP, RSTP, or MSTP function, first of all, the root switch (for MSTP the IST root switch) should be decided. Unless otherwise configured, the switch with the lowest bridge ID will be decided as the root switch. However, the operator can determine the root switch by configuring the priority. The switch with the lowest priority operates as root switch. Use the following command to change the switch priority.

Command	Mode	Function
stp mst priority *MSTID_RANGE* <0-61440>	Bridge	Configures the priority of the switch. **MSTID_RANGE**: instance number **0 - 61440**: priority value in steps of 4096 (default = 32768).
no stp mst priority *MSTID_RANGE*		Clears the Priority of the switch.

Example:

```
SWITCH(bridge)# stp mst priority 0 8192
SWITCH(bridge)# show stp mst 0 all
CST Root        2000.080006261d2fl
ST Root        2000.080006261d2f
max age 20(s) hello time 4(s) forward delay 15(s) max hops 20
-------------------- MST00 ---------------------
vlans : 51-4096
bridge id               2000.080006261d2f
designated root         2000.080006261d2f
root port 0/0 path cost 0
Port  id    AdminCost Cost      Role        State       Attribute
----------------------------------------------------------------
0/1 2001  0         20000     designated  forwarding  P2P
0/2 8002  0         20000     backup      blocking    P2P
0/3 8003  0         20000     designated  forwarding  P2P
0/4 8004  0         20000     backup      blocking    P2P
0/5 8005  0         -         disable     disabled    -
0/6 8006  0         -         disable     disabled
SWITCH(bridge)#
```

22.4.2 Deciding of Path-Cost

After deciding the root switch, there is the need to determine on which route packets has to be forwarded. The parameter to do this is the path-cost value.

Generally, the path cost depends on the transmission speed of the LAN interface. The following table shows path costs according to transmit rate of LAN interface.

Transmit Rate	Path-cost
4M	250
10M	100
100M	19
1G	4
10G	2

Table 24 STP Path Cost

Transmit Rate	Path-cost
4M	20,000,000
10M	2,000,000
100M	200,000
1G	20,000
10G	2,000

Table 25 RSTP Path Cost

If the route decided by path-cost gets overloading, another route should be taken. Considering these situations, there is the possibility for the operator to determine a route manually by configuring the path-cost of the root port.

In order to configure path cost, use following commands.

Command	Mode	Function
stp mst path-cost *MSTID_RANGE PORTS* <0-200000000>	Bridge	Configures path-cost to configure route. **MSTID_RANGE**: select instance number (0-32) **PORTS**: select the port number **0 - 200000000**: path cost value.
no stp mst path-cost *MSTID_RANGE* PORTS		Clears the configured path-cost.

22.4.3 Deciding the Port Priority

If all conditions of two routes are the same, the operator can decide the route by changing the port priority. To configure the port priority, use the following commands.

Command	Mode	Function
stp mst port-priority *MSTID_RANGE PORTS* <0-240>	Bridge	Configures port-priority. **MSTID_RANGE**: select instance number (0-64) **PORTS**: select the port number **0 - 240**: port priority value in steps of 16 (default: 128).
no stp mst port-priority *MSTID_RANGE PORTS*	Bridge	Clears the configured port-priority.

22.4.4 Deciding the MST Region

If MSTP is established, decide which MST region the switch is going to belong to by configuring the MST configuration ID. The configuration ID contains region name, revision, VLAN map. To set the configuration ID, use the following commands.

Command	Mode	Function
stp mst config-id name *NAME*	Bridge	Sets the name for the region. **NAME**: enter name to give the MST region.
no stp mst config-id name		Deletes the name of region.

Command	Mode	Function
stp mst config-id map <1-32> VLAN-RANGE	Bridge	Configures the range of VLAN that is going to be grouping as a region. **1 - 64**: select an instance ID number **VLAN-RANGE**: enter a number of the VLANs to be mapped to the specified instance.
no stp mst config-id map <1-32> *VLAN-RANGE*		Deletes entire VLAN-map or part of it.
no stp mst config-id map <1-32>		
stp mst config-id revision <0-65535>	Bridge	Configures the switches in the same MST boundary as same number. **0 - 65535**: set the MST configuration revision number.
no stp mst config-id revision		Deletes the configured revision number.

ℹ In case of STP or RSTP, the config- ID must not be set, otherwise, an error message will be displayed.

To delete the configuration ID, use following command.

Command	Mode	Function
no stp mst config-id	Bridge	Delete all of the configured configuration ID.

22.4.5 Applying the STP Configuration

ℹ After setting, changing, or deleting the configuration ID, the configuration must be applied to be injected.

To commit the configuration, use the following command.

Command	Mode	Function
stp mst config-id commit	Bridge	Commits the configuration of the region.

22.4.6 Configuring a Point-to-Point MAC

The internal sublayer service makes available a pair of parameters that permit inspection of, and control over, the administrative and operational state of the point-to-point status of the MAC entity by the MAC relay entity.

To configure the point-to-point status, use the following command.

Command	Mode	Function
stp point-to-point-mac *PORTS* {auto I force-true I force-false}	Bridge	Sets point-to-point MAC. **PORTS**: select the port number **auto**: auto detect **force-true**: force to point-to-point MAC **force-false**: force to shared MAC (not point-to point MAC)
no stp point-to-point-mac *PORTS*		Deletes point-to-point MAC configuration.

True means, the MAC is connected to a point-to-point LAN, i.e., there is at most one other system attached to the LAN.
False means, the MAC is connected to a non point-to-point LAN, i.e., there can be more than one other system attached to the LAN.

22.4.7 Configuring of Edge Ports

Edge ports are used to connect end devices. There are no switches or spanning-tree bridges after the edge port. To configure edge port mode, use the following command.

Command	Mode	Function
stp edge-port *PORTS*	Bridge	Sets port edge mode. **PORTS**: select the port number.
no stp edge-port *PORTS*		Deletes port edge mode.

22.4.8 Changing the STP Operation Mode

MSTP is backward compatible with STP and RSTP. If some other switches in the network send BDPUs of version STP or RSTP, a switch using MSTP will automatically change to the STP mode. However, the switch cannot change the STP mode to MSTP automatically. If the operator wants to change the network topology to MSTP mode, he has to clear the previous protocol on the ports manually. To clear the protocol and restart the protocol detected, use the following command.

Command	Mode	Function
stp clear-detected-protocol *PORTS*	Privileged / Config/ Bridge	Clears detected protocol. **PORTS**: select the port number.

22.4.9 Showing the Configuration

To check the xSTP configuration, use the following commands.

Command	Mode	Function
show stp	Privileged/ Config/ Bridge	Shows the configuration of STP/RSTP/MSTP.
show stp mst		Shows the configuration when it is configured as MSTP.
show stp mst *MSTID_RANGE*		Shows the configuration of specific Instance. **MSTID_RANGE**: MST instance number.
show stp mst *MSTID_RANGE* { all I *PORTS* } [detail]		Shows the configuration of the specific Instance for the ports. **all**: select all ports **PORTS**: select port number **detail**: show detail information (as option).

i With **show stp** command, it is possible to check the information about STP/ RSTP/MSTP. How to distinguish them is to check which one is marked on the mode.

i If STP or RSTP is configured, the *MSTID_RANGE* value should be `0`.

In case of configured MSTP, use the following command.

Command	Mode	Function
show stp mst config-id { current I pending }	Privileged/ Bridge	Shows the MSTP configuration identifier. **current**: shows the current configuration as it is used to run MST **pending**: shows the edited configuration.

For example, after setting the configuration ID and applying it with the **stp mst config-id commit** command, the configuration ID can be checked with the **show stp mst config-id** command.

Example:

```
SWITCH(bridge)# show stp mst 0,2 all
CST Root                8000.080006261d2fI
ST Root                8000.080006261d2f
max age 20(s)  hello time 4(s)  forward delay 15(s)  max hops 20
-------------------- MST00 --------------------
vlans : 51-4096
bridge id               8000.080006261d2f
designated root         8000.080006261d2f
root port 0/0 path cost 0
Port  id    AdminCost Cost      Role        State       Attribute
---------------------------------------------------------------
0/1 8001  0         20000     designated  forwarding  P2P
0/2 8002  0         20000     backup      blocking    P2P
0/3 8003  0         20000     designated  forwarding  P2P
0/4 8004  0         20000     backup      blocking    P2P
0/5 8005  0         -         disable     disabled    -
0/6 8006  0         -         disable     disabled
--------------------- MST02 --------------------
vlans : 1-50
bridge id               8002.080006261d2f
designated root         8002.080006261d2f
root port 0/0 path cost 0
Port  id    AdminCost Cost      Role        State       Attribute
---------------------------------------------------------------
0/1 8001  0         20000     designated  forwarding  P2P
0/2 8002  0         20000     backup      blocking    P2P
0/3 8003  0         20000     designated  forwarding  P2P
0/4 8004  0         20000     backup      blocking    P2P
0/5 8005  0         -         disable     disabled    -
0/6 8006  0         -         disable     disabled    -
SWITCH(bridge)#
```

```
SWITCH(bridge)# show stp mst 2 0/1 detail
CST Root                8000.080006261d2fI
ST Root                8000.080006261d2f
max age 20(s)  hello time 4(s)  forward delay 15(s)  max hops 20
-------------------- MST02 --------------------
vlans : 1-50
bridge id               8002.080006261d2f
designated root         8002.080006261d2f
root port 0/0
path cost 0port 0/1
port id                1001
state                  forwarding               role designated
designated root  8002.080006261d2f path cost 5000
designated bridge 8002.080006261d2 message age timer 0.0
designated port        1001 forward delay timer 0.00
designated cost           0
flags                  P2P
SWITCH(bridge)#
```

22.5 BPDU Configuration

BPDU is a transmission message used in order to configure and maintain the configuration of STP/RSTP/MSTP. Switches using STP exchange their information BDPU to find the best path. An MSTP BPDU is general an STP BPDU extended with additional MST data. The MSTP part of BPDU does not rest if it is out of the region.

- **Hello time**
  Hello time decides an interval time when a switch transmits BPDU. It can be configured from 1 to 10 seconds. The default is 2 seconds.
- **Max Age**
  Root switch transmits new information every time based on information from another switches. However, if there are many switches on network, it takes lots of time to transmit BDPUs. And, if the network status is changed while transmitting BDPU, this information is useless. To get rid of useless information, 'Max age' is identified in each information.
- **Forward Delay**
  Switches find location of another switches connected to LAN though received BDPU and transmit packets. Since it takes certain time to receive BDPU and find the location before transmitting packet, switches send packet at regular interval named forward delay.

ℹ The configuration for BPDU is applied as selected in force-version. The same commands are used for STP, RSTP, and MSTP.

22.5.1 Hello Time

Hello time decides an interval time when a switch transmits BPDU. To configure hello time, use the following command.

Command	Mode	Function
stp mst hello-time <1–10>	Bridge	Configures hello time to transmit the message in STP, RSTP, MSTP: **1 - 10**: set the hello time (default = 2 seconds).
no stp mst hello-time		Clears the time configuration that is set up to transmit route message.

22.5.2 Forward Delay

It is possible to configure forward delay, which means time to take port status from listening to forwarding. To configure forward delay, use the following command.

Command	Mode	Function
stp mst forward-delay <4–30>	Bridge	Designates Forward-delay in STP, RSTP or MSTP. **4 - 30**: delay time value. The default is 15 seconds
no stp mst forward-delay		Clears the configured forward-delay.

22.5.3 Max Age

Max age shows how long path message is valid. To configure max age to delete useless messages, use the following command.

Command	Mode	Function
stp mst max-age <6–40>	Bridge	Configures max age of route message in STP, RSTP or MSTP. **6 - 40**: max age time value (default: 20 sec.)
no stp mst max-age		Releases max age of configured route message.

ℹ It is recommended that max age is configured less than twice of forward delay and more than twice of hello time.

22.5.4 BPDU Hop

In MSTP, it is possible to configure the number of hop in order to prevent BPDU from wandering. BPDU passes the switches as the number of hop by this function. To configure the number of hop of BPDU in MSTP, use the following command.

Command	Mode	Function
stp mst max-hops <1-40>	Bridge	Configures the number of hop for BPDU **1 - 40**: set the number of possible hops in the region.
no stp mst max-hops		Deletes the number of hop for BPDU in MSTP.

22.5.5 Checking the BPDU Configuration

To check the configuration for BPDU, use the following command.

Command	Mode	Function
show stp mst	Privileged/ Config/ Bridge	Shows the configuration for BPDU.

22.6 Self Loop Detection

Although there is no double path in user's equipment, loop can be caused by network environment and cable condition connected to equipment. To prevent this, the hiX 5750 R2.0 has a self loop detection to perceive that an outgoing packet is got back. Through the self loop detection, it is possible to prevent packet, which comes back because it blocks the port. To enable/disable self loop detection, use the following command.

Command	Mode	Function
stp self-loop-detect { enable I disable }	Bridge	Enables/disables self loop detection function.

Use the following commands for detection of loops or to check the ports where a loop occurred.

Command	Mode	Function
show stp self-loop-detect	Bridge	Shows status of self loop detection and a port where loop is happed.
show stp self-loop-detect { all I *PORTS* }		Shows self loop detection status on specified ports. **all**: all the ports **PORTS**: selected port.

22.7 Sample of MSTP Configuration

```
SWITCH(bridge)# stp force-version mstp
SWITCH(bridge)# stp mst enable
SWITCH(bridge)# stp mst config-id map 2 1-50
SWITCH(bridge)# stp mst config-id name 1
SWITCH(bridge)# stp mst config-id revision 1
SWITCH(bridge)# stp mst config-id commit
SWITCH(bridge)# show stp mst
Status    enabled
bridge id    8000.00d0cb000183
designated root     8000.00d0cb000183
root port  0   path cost    0
max age      20.00     bridge max age    20.00
hello time   2.00       bridge hello time 2.00
forward delay    15.00 bridge forward delay    15.00
CIST regional root 8000.00d0cb000183  CIST path cost    0
max hops      20
name SWITCH
revision 1
instance vlans
---------------------------------------------------------------
CIST 51-4094
2 1-50
---------------------------------------------------------------
SWITCH(bridge)#
```

23 IP Anti-Spoofing

IP anti-spoofing can be used at the subscriber ports to control the IP traffic in the upstream direction. Only IP packets should be accepted which come in from valid IP source addresses. All other packets have to be discarded. IP anti-spoofing for incoming IP packets is enabled if it was set for both the VLAN and the port.

23.1 Global Enabling of IP Anti-Spoofing

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

Command	Mode	Function
ip antispoofing global [enable | disable]	Bridge	Sets the global antispoofing flag: **enable** or **disable**.

23.2 Enabling IP Anti-Spoofing for Port

Command	Mode	Function
bridgeport *PORTS* **antispoofing** { enable | disable }	Bridge	Bridge port IP anti-spoofing configuration, **PORTS**: slot/port/ONU ID/ONT slot/ONT port **enable**/**disables** IP anti-spoofing.

23.3 Checking the Status

Command	Mode	Function
show ip antispoofing global	Bridge	Displays global status of IP anti-spoofing.
show ip antispoofing bridgeport		Displays port status of IP anti-spoofing.

23.4 Configuring an IP Anti-Spoofing VLAN Profile

In VLANs which are entered into the IP anti-spoofing VLAN profile, packets with allowed IP addresses only will be accepted and forwarded. In the other VLANs, all packets are forwarded without verifying the IP source address.

i In the hiX 5750 R2.0, there is only one anti-spoofing VLAN profile.

Command	Mode	Function
ip antispoofing vlan-profile [<1-1>] **add** { <1-4094> | all }	Bridge	Adds specified VLAN or all VLANs to IP anti-spoofing VLAN profile. **1 - 1**: index VLAN profile **1 - 4094**: VLAN-ID **all**: all VLANs in system
ip antispoofing vlan-profile [<1-1>] **del** { <1-4094> | all }		Deletes specified VLAN or all VLANs from IP anti-spoofing VLAN profile.

Command	Mode	Function
show ip antispoofing vlan-profile	Bridge	Shows IP anti-spoofing VLAN profile,

24 Link Aggregation

LACP (link aggregation control protocol) complying with IEEE 802.3ad bundles several physical GPON ports together to one logical port providing enlarged bandwidth.

ℹ In the hiX 5750 R2.0 system, Link Aggregation Groups (LAG) 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 system supports two kinds of link aggregation groups - static groups as port trunk and dynamic groups using **LACP**. A static LAG balances the traffic load across the links in the LAG port. If a physical link within the static LAG fails, traffic previously carried over the failed link is moved to the remaining links.

24.1 Selecting Distribution Method

To choose the distribution method of aggregated CXU or IU_10x1GE ports, use the following commands.

Command	Mode	Function
trunk group distmode *AGGREGATORS* { srcmac I dstmac I srcdstmac I scrip I dstip I srcdstip }	Bridge	Manages distribution method of fixed trunk groups of CXUports. **AGGREGATORS**: trunk group ID (0-1) **srcmac**: set source MAC **dstmac**: set destination MAC **srcdstmac**: set source destination MAC(default) **srcip**: set source IP **dstip**: set destination IP **srcdstip**: set source destination IP.
no trunk group distmode *AGGREGATORS*		Deletes fixed trunk groups of CXU ports,
trunk iu *SLOT* **aggregator group distmode** *AGGREGATIONS* { srcmac | dstmac | srcdstmac | srcip | dstip | srcdstip }	Bridge	Manages distribution method of fixed trunk groups of IU ports. **AGGREGATORS**: trunk group ID (0 - 4) **SLOT**: IU slot number.
no trunk iu *SLOT* **aggregator group distmode** *AGGREGATIONS*		Deletes fixed trunk groups of IU ports.

ℹ Group-ID of port trunk cannot be configured repeatedly.

ℹ Source destination MAC address is basically used to decide the packet route.

24.2 Configuring a static Port Trunk

ℹ The port designated as member port of a trunk is automatically deleted from existing VLAN. Therefore, if member port and aggregated port exist in different VLAN, VLAN configuration should be changed for the aggregated port. If the operator deletes a member port from the logical port or releases the port trunk, ports will be automatically contained as default VLAN.

24.2.1 Forming a fixed Trunk Group of Ports

To form the port trunk, use the following command.

Command	Mode	Function
trunk port *AGGREGATOR PORTS*	Bridge	Manages fixed trunk of CXU ports. **AGGREGATOR**: trunk group ID (0-1) **PORTS**: port numbers that should be added (0/1 -0/4). Use the **no** parameter with this command to delete a fixed trunk of CXU ports.
trunk iu *SLOT* **port** *AGGREGATOR PORTS*	Bridge	Manage IU fixed trunk groups. **SLOT**: IU slot number **AGGREGATOR**: trunk group ID (0-4) **PORTS**: port numbers that should be added (Slot/Port). Use the **no** parameter with this command to delete a fixed trunk of IU ports.

ℹ Group-ID of port trunk cannot be configured repeatedly.

24.2.2 Checking Port Trunk Configuration

To check the configuration of port trunk, use the following command.

Command	Mode	Function
show trunk [all]	Privileged/ Config/ Bridge	Shows the configuration for trunk.
show trunk iu *SLOT*		Shows IU fixed trunk groups. **SLOT**: select IU slot number.

24.3 Configuring LACP

LACP provides a dynamically exchange of information in order to configure and maintain link aggregation groups automatically. Load sharing is automatically readjusted if a failure or recovery from failure occurs in any of the links that participate in a dynamic LAG.

ℹ Uplink ports which should be configured by LACP must be member of the same VLAN. The aggregated port is automatically added to the appropriate VLAN.

The following sections explain how to configure dynamic LAG:

- Enabling/Disabling LACP
- Configuring Packet Route
- Configuring the Member Ports
- Configuring Operating Mode of Member Port
- Configuring LACP Priority
- Deciding Member State of LACP Port
- Configuring LACPDU Transmission Rate
- Configuring Admin Key of Member Port and Aggregator
- Configuring Port Priority
- Checking LACP Configuration.

24.3.1 Enabling/Disabling LACP

To enable/disable the LACP function, use the following commands.

Command	Mode	Function
lacp aggregator *AGGREGATIONS*	Bridge	Enables LACP for CXU of designated Aggregator-number. **AGGREGATIONS**: aggregator ID that should be enabled for LACP (valid value from 0 to 1). Use the **no** parameter with this command to release LACP for CXU for designated aggregator-number,
lacp iu *SLOT* **aggregator** *AGGREGATIONS*	Bridge	Enables LACP for IU. **SLOT**: IU Slot number **AGGREGATIONS**: aggregator IDs that should be enabled for LACP (0-4). Use the **no** parameter with this command to disables LACP for IU.
lacp aggregator admin-key *AGGREGATIONS* <1-15>	Bridge	Enables admin-key of designated aggregator-number. **AGGREGATIONS**: aggregator IDs that should be enabled for LACP (valid value from 0 to 1). **0 - 15**: admin-key value (default 0)
no lacp aggregator admin-key *AGGREGATIONS*		Release admin-key of designated aggregator-number,
no lacp aggregator delay *AGGREGATIONS* <0-65535>	Bridge	Release collector max delay of designated aggregator-number, **AGGREGATIONS**: aggregator IDs that should be disabled for LACP **0 - 65535**: delay value.

The aggregator ID of an LAG cannot be configured repeatedly.

24.3.2 Configuring Packet Route

When packets enter to an LAG port and there is no process to decide the packet route, the packets could be gathered on particular member port. In this case, it is not possible to use the logical port effectively.

Therefore, the hiX 5750 R2.0 is configurable to route packets in order to distribute them on the member ports.The route is decided by source IP address, destination IP address, source MAC address, destination MAC address.

The hiX 5750 R2.0 uses source destination MAC address by default to choose the packet route.

Command	Mode	Function
lacp aggregator distmode *AGGREGETIONS* { srcmac I dstmacI srcdstmacI srcipI dstipI srcdstip }	Bridge	Manages distribution method of CXU ports to aggregator. **AGGREGATORS**: select the aggregator ID (0-1) **srcmac**: set source MAC **dstmac**: set destination MAC **srcdstmac**: set source destination MAC (default) **srcip**: set source IP **dstip**: set destination IP **srcdstip**: set source destination IP.
no lacp aggregator distmode *AGGREGETIONS*		Clears destination MAC address of CXU.
lacp iu *SLOT* **aggregator distmode** *AGGREGATIONS* { srcmac l dstmac l srcdstmac l srcip l dstip l srcdstip }	Bridge	Manages distribution method of IU ports to aggregator. **AGGREGATORS**: aggregator numbers (0-4) **SLOT**: select IU slot number.
no lacp iu *SLOT* **aggregator distmode** *AGGREGATIONS*		Deletes aggregator of IU ports.

The aggregator ID of an LAG cannot be configured repeatedly.

24.3.3 Configuring the Member Ports

After configuring the aggregator, choose the physical ports that should be member of the LAG port using the following commands in *Bridge configuration* mode.

Command	Mode	Function
lacp port *PORTS*	Bridge	Configures physical port that is member port of aggregator, **PORT**: port number(s) that should be enabled for LACP (slot/port, slot 0 is CXU slot) Use the **no** parameter with this command to release a member port of aggregator
lacp iu *SLOT* **port** *PORTS*	Bridge	Configures physical port that is member port of aggregator, **PORT**: port number(s) that should be enabled for LACP (Slot/Port) **SLOT**: select IU slot number. Use the **no** parameter with this command to release a member port of aggregator

ℹ It is possible to configure several ports by using the delimiter `,` or `-`.

24.3.4 Configuring Operating Mode of Member Port

After configuring the member ports, choose the port operation mode - *active* or *passive* mode. *Passive* mode starts LACP when the port of the opposite GPON is using *active* mode. Because the priority of *active* mode is higher than of *passive* mode, the *passive* port follows the *active* port.

ℹ If the uplink ports are set in *passive* mode, a link of member ports over two switches is impossible.

To configure the operation mode of member ports, use the following commands in *Bridge* mode.

Command	Mode	Function
lacp port activity *PORTS* { active I passive }	Bridge	Configures the mode of member port of CXU LAG (default is active), **PORT**: select the member port number.
no lacp port activity *PORTS*		Releases operation mode of configured member port of CXU LAG,
lacp iu *SLOT* **port activity** *PORTS* { active | passive }	Bridge	Configures the mode of member port of IU LAG (default is active), **PORT**: Select port number(s) (Slot/Port). **SLOT**: select IU slot number.
no lacp iu *SLOT* **port activity** *PORTS*		Releases operation mode of configured member port of IU LAG,

ℹ Member ports are set to active operation mode by default. After releasing the operating mode, the port is returned to default mode (active).

24.3.5 Configuring LACP Priority

In case of a configured *active* mode (LACP system enabled), it is required to choose the standard GPON port of the LAG and to configure the priority.

Command	Mode	Function
lacp system priority <1-65535>	Bridge	Sets the priority of the CXU switch in LACP function, **1 - 65535**: switch system priority.
no lacp system priority		Clears the priority of the configured CXU switch.

Command	Mode	Function
lacp iu *SLOT* **system priority** <1-65535>	Bridge	Sets switch system information needed by LACP (ex: SystemID) for IU. **SLOT**: select IU slot number. **1 - 65535**: switch system priority.
no lacp iu *SLOT* **system priority**		Clears the priority of the configured IU switch.

ℹ The priority of the system is set to “32768 (=0x8000)” by default. After clearing the operating mode, the priority of the member ports return to this default value.

24.3.6 Deciding Member State of LACP Port

By default, LACP ports are potentially member of a configured dynamic LAG. However, these ports could operate as well as independent ports without being aggregatable to an LAG. These independent ports cannot be used as trunk port by the system.

Use the following commands to configure if a member port is aggregatable or not.

Command	Mode	Function
lacp port aggregation *PORTS* { aggregatable I individual }	Bridge	Designate whether a member port of CXU is included in LACP or not, **PORT**: select the member port should be included. Default setting is aggregatable.
no lacp port aggregation *PORTS*		Clears the configured member port of CXU in LACP,
lacp iu *SLOT* **port aggregation** *PORTS* { aggregatable l individual }	Bridge	Designate whether a member port of IU is included in LACP or not, **PORT**: Select port number(s) (Slot/Port). Default setting is aggregatable. **SLOT**: Select port number(s).
no lacp iu *SLOT* **port aggregation** *PORTS*		Clears the configured member port of IU in LACP,

ℹ A member port is basically configured as aggregatable to LAG. After clearing the member state, the port returns to default configuration (aggregated).

24.3.7 Configuring LACPDU Transmission Rate

The member port transmits LACPDU (bridge protocol data unit) with its information. Configure the LACPDU transmission rate by using the following commands.

Command	Mode	Function
lacp port timeout *PORTS* { short I long }	Bridge	Configures LACPDU transmission rate for CXU LAG. **PORTS**: select the port number **short**: short timeout **long**: long timeout.
no lacp port timeout *PORTS*		Clears LACPDU transmission rate of configured member port of CXU LAG,
lacp iu *SLOT* **port timeout** PORTS { short l long }	Bridge	Configures LACPDU transmission rate for IU LAG: PORTS: Select port number(s) (Slot/Port) short: short timeout long: long timeout SLOT: select IU slot number.
no lacp iu *SLOT* **port timeout** *PORTS*		Clears LACPDU transmission rate of configured member port of IU LAG,

ℹ LACPDU transmission rate of member port is basically configured as `long`.

ℹ The values of transmission rate are: long = 30 sec and short = 1 sec.

24.3.8 Configuring Admin Key of Member Port and Aggregator

All member ports in one aggregator have the same key values. In order to make an aggregator consisted of specified member ports, configure a key value that is different from key values of other ports.

Command	Mode	Function
lacp port admin-key *PORTS* <1-15>	Bridge	Configures key value of member port on CXU. **PORTS**: port number **1- 15**: port key value.
no lacp port admin-key *PORTS*		Deletes key value of selected member port on CXU,
lacp iu *SLOT* **port admin-key** *PORTS* <1-15>	Bridge	Configures key value of member port on IU. **PORTS**: Select port number(s) (Slot/Port) **1- 15**: select the port key value **SLOT**: select IU slot number.
no lacp iu *SLOT* **port admin-key** *PORTS*		Deletes key value of selected member port on CXU.
lacp iu *SLOT* **aggregator admin-key** *AGGREGATIONS* <1-15>	Bridge	Configures the admin-key of IU aggregator. **SLOT**: IU slot number, **AGGREGATIONS**; aggregator numbers (0-4), **1 - 15**: admin-key value (default 1).
no lacp iu *SLOT* **aggregator admin-key** *AGGREGATIONS*		Deletes the admin-key of IU aggregator.

ℹ The key value of all ports is 1 by default. Executing the **no** commands returns the key value to 1.

24.3.9 Configuring Port Priority

To configure the priority of an LACP member port, use the following commands.

Command	Mode	Function
lacp port priority *PORTS* <1-65535>	Bridge	Sets the LACP priority of member port, **PORTS**: CXU port number. **1 - 65535**: port priority.
no lacp port priority *PORTS*		Clears port priority of selected member port of CXU.
lacp iu *SLOT* **port priority** *PORTS* <1-65535>	Bridge	Sets the LACP priority of member port, **SLOT**: IU slot number. **PORTS**: port number(s) (Slot/Port). **1 - 65535**: sets port priority.
no lacp iu *SLOT* **port priority** *PORTS*		Clears port priority of selected IU member ports.

ℹ The LACP priority of a member port is basically configured to 32768. After clearing the priority, the member port returns to this default configuration.

24.3.10 Checking LACP Configuration

To check the LACP configuration, use the following commands.

Command	Mode	Function
show lacp aggregator	Privileged/ Config Bridge	Shows aggregator information of CXU.
show lacp aggregator *AGGREGATIONS*		Shows aggregator information of the selected CXU aggregator. **AGGREGATORS**: Select aggregator number(s) (0-1)
show lacp port		Shows the information of member ports of CXU.
show lacp port *PORTS*		Shows the information of appropriated member port of CXU.
show lacp iu *SLOT* **aggregator**		Shows aggregator information of IU. **SLOT**: Select IU Slot Number.
show lacp iu *SLOT* **aggregator** *AGGREGATIONS*		Shows aggregator information of the selected IU aggregator. **SLOT**: Select IU Slot Number. **AGGREGATIONS**: Select aggregator number(s) (0-4)
show lacp iu *SLOT* **port**		Shows the information of IU member ports. **SLOT**: Select IU Slot Number.
show lacp iu *SLOT* **port** *PORT*		Shows the information of appropriated member port of IU. **SLOT**: Select IU Slot Number. **PORT**: Select port number(s) (Slot/Port)

25 Rules

The hiX 5750 R2.0 system provides rules for the traffic management. Using rules, packets will be operated as the user has configured. Rule functions analyze the incoming traffic by classifying dependent on designated policy in order to decide on packets which will be forwarded. For each rule, the rule type, rule priority, rule match, rule action, and action parameter(s) must be configured. The physical port and data fields within a packet such as the 802.1p priority (**CoS**), **VLAN ID**, and **DSCP** can be modified to configure a policy.

ℹ Note the following requirements and using hints:

- The rule name must be unique. Its size is limited to 63 characters.
- The sequence of entering the configuration commands is arbitrary.
- Rules can be modified (inclusive the rule type) only as long as the **apply** command is not executed. After that, the rule must be deleted and then created again with changed values.
- Some rule types will operate correctly only in single tagging mode, others only in double tagging mode. Nevertheless, it is possible and allowed to create and apply all rule types in both tagging modes. The hiX 5750 R2.0 system internally activates only rules that are fit for the tagging mode running currently.
- Use the **show rule-profile** command to display the configuration.

25.1 Creating a Rule

From the *Rule configuration* mode, use the following command to create a rule.

Command	Mode	Function
rule *NAME* **create**	Config	Begins *Rule Configuration* mode, **NAME**: enter an unique rule name.

After entering the **rule create** command, the prompt changes from `SWITCH(config)#` to `SWITCH(config-rule[name])#`.

25.2 Setting of the Rule Type

In general, the rule type classifies the rule and determines allowed rule matches, rule actions, and required action parameters.

Command	Mode	Function
type { cxu-generic | cxu-admin | iugpon-generic | iugpon-admin | iuuplink-generic | iuuplink-admin }	Rule	Configures rule of a certain rule type. **cxu-generic**: sets generic rule for CXU (rule 50, GenericRule) **cxu-admin**: sets admin access rule for CXU (rule 51, AdminRule) **iugpon-generic**: sets generic rule for IU-GPON **iuuplink-generic**: sets generic rule for IU-UPLINK **iuuplink-admin**: sets admin access rule for IU-UPLINK.

25.3 Setting of the Tagging Mode

Only for IU_GPON card set this parameter to specify if the rule expects double or single tags.

Command	Mode	Function
tagging { single I double }	Rule	Sets tagging mode of a rule. **single**: single tagged traffic **double**: double tagged traffic

25.4 Setting of Priority

To configure the priority of rule, use the following command. If multiple rules match the same packets, the rule with the higher priority will be processed first.

Command	Mode	Function
prio <0-7>	Rule	Configure the priority for the new rule, **0 - 7**: enter a priority value (default is 0).

25.5 Configuring of Matches and Actions

25.5.1 Matches

Configure the policy to adjust what properties should be analyzed within incoming packets. Some rule types support combinations of two or more rule matches. Such rules only match, if all of their matches are true.

Command	Mode	Function
iu-slot { *SLOT* I any }	Rule	Configures IU physical slot number: **SLOT**: enter slot number **any**: revokes this configuration
match { exact I exclude }	Rule	Configures the granulation of match action: **exact** (default): matches exactly the given value(s) **exclude**: matches all values except given value(s). (This command is optional because hiX 5750 R2.0 only supports `match exact` and uses this as default).
match port { *PORT* I cpu I any }	Rule	Matches a CXU (uplink or CXU) or IU (subscriber) port: **PORT**: enter the CXU or IU port number. **cpu**: CXU port **any**: revoke the PORT **classifier**.
match ingress slot { *PORT* I any I default }	Rule	Matches one IU slot number. **PORT**: enter logical IU slot number **any**: revoke the PORT classifier default: set all IU slots to default (=upstream).
match ingress port { *PORT* I any I default }	Rule	Matches one CXU uplink port. PORT: enter the uplink port number any: match any uplink port (ignore) default: set all IU slots to default (=upstream).
match ingress uport-map { *BITMASK* I any I default }	Rule	Matches user-port bit mask. **BITMASK**: bitmask value (max 32 bits) **any**: revoke the PORT classifier **default**: set all IU slots to default (=upstream).
match egress uport { *USERPORT* I any }	Rule	Matches the BCMX user port. **USERPORT**: user port number **any**: revoke this number.

Command	Mode	Function
match vlan { *VLAN* I any } [*MASK*]	Rule	Matches a VLAN. **VLAN**: enter a VLAN number. **any**: revoke the VLAN classifier **MASK**: VLAN mask.
match inner-vlan { *VLAN* I any } [*MASK*]	Rule	Matches an inner VLAN. **VLAN**: enter a VLAN number. **any**: revoke the VLAN classifier **MASK**: VLAN mask.
match dscp { *DSCP* I any }	Rule	Matches a DSCP value. **DSCP**: enter a DSCP value (0 to 63) **any**: revoke the DSCP classifier.
match cos { <0-7> I any }	Rule	Matches the IEEE 802.1p priority. **0 - 7**: enter a .1priority value. **any**: revoke the 1priority classifier.
match inner-cos { <0-7> I any }	Rule	Classifies a rule, matches the inner tag IEEE 801 .1p priority. **0 - 7**: enter a .1priority value. **any**: revoke the 1priority classifier
match tos { <0-255> I any }	Rule	Matches a rule. **0 - 255**: enter **TOS** value. **any**: revoke the TOS classifier.
match ip-prec { <0-7> I any }	Rule	Matches a rule (IP TOS precedence). **0 - 7**: enter IP TOS precedence value. **any**: revoke the IP TOS classifier
match mac { XX:XX:XX:XX:XX:XX I { XX:XX:XX:XX:XX:XX/M I any} { XX:XX:XX:XX:XX:XX I { XX:XX:XX:XX:XX:XX/M I any }	Rule	Matches layer2 address. source/destination MAC address, source/destination MAC address with mask **any**: revoke the destination MAC address classifier.
match ethtype { *TYPE-NUM* I arp I ip I ppp-disc I ppp-sess I any }	Rule	Matches the Ethernet type. **TYPE-NUM**: Ethernet type field (hex, e.g., 0800 for IPv4) **arp**: address resolution protocol **ip**: IP protocol **ppp-disc**: PPPoE discovery **ppp-sess**: PPPoE session **any**: revoke the Ethernet classifier.
match flow { upstream I downstream I bidirectional I default I any }	Rule	Matches the packet flow direction. **upstream**: only upstream packets **downstream**: only downstream packets **bidirectional**: upstream and downstream packets **default**: set all IU slots to default (=upstream) **any**: revoke packet flow direction classifier.
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any }	Rule	Matches the IP protocol. source/destination IP address, source/destination IP address with mask **any**: revoke the destination IP protocol classifier .
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any } **icmp**	Rule	Matches the IP protocol. source/destination IP address, source/destination IP address with mask **any** source/destination IP address **any**: revoke the destination IP protocol classifier.
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any } **icmp** <0-255>	Rule	Configures the IP protocol. source/destination IP address, source/destination IP address with mask any source/destination IP address **0 - 255**: ICMP message type number **any**: revoke the destination Ip address classifier.

Command	Mode	Function
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any } **icmp** <0-255> <0-255>	Rule	Configures the IP protocol. source/destination IP address, source/destination IP address with mask any source/destination IP address **0 - 255**: ICMP message type number **0 - 255**: ICMP message code number **any**: revoke the destination IP address classifier.
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any } { tcp I udp }	Rule	Configures the IP protocol. source/destination IP address, source/destination IP address with mask any source/destination IP address **tcp**: **TCP** **udp**: **UDP** **any**: revoke the destination IP address classifier.
match ip { A.B.C.D I A.B.C.D/M I any } { A.B.C.D I A.B.C.D/M I any } { tcp I udp} {<0-65535> I any } { <0-65535> I any }	Rule	Configures the IP protocol. source/destination IP address, source/destination IP address with mask any source/destination IP address **tcp**: TCP **udp**: UDP **0 - 65535**: TCP/UDP source/destination port number **any**: revoke the destination port classifier.
match ip { A.B.C.D I A.B.C.D/M I any} { A.B.C.D I A.B.C.D/M I any } { igmp I pim I <0-255> I any }	Rule	Configures the IP protocol. source/destination IP address, source/destination IP address with mask any source/destination IP address **igmp**: **IGMP** **pim**: **PIM** **0 - 255**: IP protocol number **any**: revoke the IP protocol classifier.

25.5.2 Actions

Configure the policy to adjust how to modify properties of transmitted packets. Use the **no** parameter with the command to delete the specified action.

Configuring of Match Actions

Command	Mode	Function
action deny	Rule	Rule action: deny access
no action deny		
action { allow I permit }	Rule	Rule action: permit access
no action { allow I permit }		
action redirect { *UPORT* I cpu }	Rule	Redirects to specified egress port. **PORT**: port number (e.g. 1/1) **cpu**: CXU port.
no action redirect		
action mirror	Rule	Sends a copy to mirror monitoring port.
no action mirror		
action dscp *DSCP*	Rule	Changes DiffServ field. **DSCP**: DSCP value (0 to 63).
no action dscp		

Command	Mode	Function
action cos <0-7>	Rule	Changes 802.1p class of service. **0 - 7**: enter **CoS** value.
action cos <0-7> **overwrite**		Overwrites 802.1p COS field in the packet.
action cos same-as-tos overwrite		Changes 802.1p class of service. **same-as-tos**: same as IP ToS precedence bits **overwrite**: overwrites 802.1p COS field in the packet.
no action cos		Deletes changes of 802.1p class of service.
action ip-prec <0-7>	Rule	Changes ToS precedence bits in the packet. **0 - 7**:ToS precedence value.
no action ip-prec		
action ip-precsame-as-cos	Rule	Changes P ToS precedence bits in the packet, same as 802.1p CoS value.
action bandwidth *BANDWIDTH*	Rule	Determines maximum allowed bandwidth. **BANDWIDTH**: value in Mbps.
no action bandwidth		
action vlan <1-4094>	Rule	Specifies matched-packet VLAN-ID. **1 - 4094**: VLAN-ID value.
no action vlan		
action copy-to-cpu	Rule	Copies to CXU.
no action copy-to-cpu		
action counter	Rule	Rule action: counter.
no action counter		
action untag	Rule	Rule action: untag.
no action untag		

Configuring of No-Match Actions

Command	Mode	Function
no-action deny	Rule	No deny access
no no-action deny		
no-action { allow I permit }	Rule	No permit access
no no-action { allow I permit }		
no-action redirect { *PORT* I cpu }	Rule	No redirect to specified egress port.
no no-action redirect		
no-action mirror	Rule	No sending a copy to mirror monitoring port.
no no-action mirror		
no-action dscp <0-63>	Rule	No change of Changes DiffServ field.
no no-action dscp		
no-action cos <0-7> **no-action cos** <0-7> **overwrite** **no-action cos same-as-tos-overwrite**	Rule	No changes of 802.1p class of service.
no no-action cos		
no-action ip-prec <0-7> **no-action ip-precsame-as-cos**	Rule	No change of IP ToS precedence bits in the packet.
no no-action ip-prec		

Command	Mode	Function
no-action bandwidth *BANDWITH*	Rule	No maximum allowed bandwidth
no no-action bandwidth		
no-action vlan <1-4094>	Rule	No specifying of matched-packet VLAN-ID.
no no-action vlan		
no-action copy-to-cpu	Rule	No copy to CPU
no no-action copy-to-cpu		
no-action counter	Rule	No rule action: counter
no no-action counter		
no-action untag	Rule	No rule action: untag
no no-action untag		

Configuring of Action Parameters

Use the following commands to specify the action parameters.

Command	Mode	Function
action-param vlan *VLAN*	Rule	Changes VLAN parameter. **VLAN**: VLAN-ID.
action-param cos <0-7>	Rule	Changes class of service (IEEE 802.1p priority). **0 - 7**: .1p priority value.
action-param tos <0-7>	Rule	Changes IP ToS precedence bits in the packet. **0 - 7**: ToS value.
action-param dscp <0-63>	Rule	Changes DiffServ. **0 - 63**: DiffServ value.

Example of Rule

A rule should be created that matches VLAN ID 100 (in downstream direction) and sets the .1p priority of VLAN tag (CoS value) to 4:

```
SWITCH(config)#rule Testrule1 create
SWITCH(config-rule[Testrule1])#type cxu-generic
SWITCH(config-rule[Testrule1])#prio 2
SWITCH(config-rule[Testrule1])#match vlan 100
SWITCH(config-rule[Testrule1])#action cos 4 overwrite
SWITCH(config-rule[Testrule1])#match flow downstream
SWITCH(config-rule[Testrule1])#apply
SWITCH(config-rule[Testrule1])#show rule-profile
rule Testrule1
type cxu-generic (Generic CXU rule)
prio 2
match vlan 100
match flow downstream
action cos 4 overwrite
SWITCH(config-rule[Testrule1])#
```

25.6 Saving a Rule

After configuring a rule, it must be applied to the GPON. Configured values will be checked and the rule will be activated within the system.

ℹ Without using the **apply** command, the rule configurations will be lost.

Command	Mode	Function
apply	Rule	Saves rule and applies it to the GPON.

ℹ Note the following information:

- The system performs a detailed plausibility check and rejects the rule if the configuration is incomplete, contains bad or unsupported values, or conflicts to other rules. In this case, the system informs about the reason and the operator may correct the values.
- It can be that the entered name interferes with the name of an internally managed rule (name will not be listed by command **show rule**). In this case the system rejects a rule with the message:
  `A rule having the same NAME already exists`
  Select another name for this rule (e.g. add a prefix).
- All previously entered values remain valid after successful (or unsuccessful) execution of command **apply**. If several rules being different only in one value should be created then only the one changed value needs to be entered again.

25.7 Displaying the Rules Configuration

The following commands can be used to show a certain rule by its name, all rules of a certain type, or all rules at once sorted by rule type.

Command	Mode	Function
show rule	Rule/ Privileged/ Config	Displays all rules sorted by type.
show rule all		Displays all rules sorted by type (alias to **show rule**)
show rule cxu		Displays all active user rules and admin rules at CXU in a condensed format.
show rule name *NAME*	Rule/ Privileged/ Config	Displays a rule, enter a rule name.
show rule type { cxu-generic I cxu-admin I iugpon-generic I iugpon-admin }	Rule/ Privileged/ Config	Displays rules of certain type. **cxu-generic**: generic rules for CXU (rule 50) **cxu admin**: admin access rules for CXU (rule 51) **iugpon-generic**: generic rules for IU_GPON **iugpon-admin**: admin access rules for IU_GPON.
show help	Rule	Displays help information of current rule context.
show rule-profile	Rule	Displays the profile currently being edited.

An example for using the **show rule** command:

```
SWITCH(config)#show rule
-----------------------------------------------------------
RULE TYPE 04: QosVlan (vlan-cos)
-----------------------------------------------------------
```

```
Prio : 2,
Name: "Testrule1"
Match: exact
vlan=100,
Action: Change inner .1p PRIO (set-iprio) cos=4
SWITCH(config)#
```

25.8 Deleting a Rule

To cancel an existing rule and remove it from the system, use one of the following commands.

Command	Mode	Function
no rule [*NAME*]	Config	Deletes all or specified rule, **NAME**: enter the rule name.
no rule-type { cxu-generic I cxu-admin I iugpon-generic I iugpon-admin }	Config	Deletes all rules of a certain type. **cxu-generic**: generic rules for CXU (rule 50, GenericRule) **cxu-admin**: admin access rules for CXU (rule 51, AdminRule) **iugpon-generic**: generic rules for IU_GPON **iugpon-admin**: admin access rules for IU_GPON.

An example for deleting a rule:

```
SWITCH(config)#no rule
```

```
1 rule(s) successfully deleted
SWITCH(config)# show rule
No rules configured.
SWITCH(config)#
```

26 Broadcast Storm Control

The hiX 5750 R2.0 system supports **BCSC**. A broadcast storm is the result of an overloading situation in which broadcast packets occupy the major part of network's bandwidth causing an unstable network. Such a broadcast storm may be occurred by hardware malfunctions or a wrong network configuration at which, for example, information of a routing protocol, regularly transmitted from the router, are wrong recognized by a system that does not support this protocol. BCSC operates with counting the broadcast packets per second and discarding packets which exceed the configured limit. Besides BCSC, the system can also control of **MC** or DLF (destination lookup fail) storms. The storm control configuration will be equally applied to all **VLAN**s.
To enable/disable storm control or to check its state, use the following commands.

<table>
<tr><th>Common</th><th>Mode</th><th>Function</th></tr>
<tr><td><b>storm-control</b> { broadcast | multicast | dlf } <i>RATE PORTS</i></td><td rowspan="2">Bridge</td><td>Enables broadcast, MC, or DLF storm control respectively in a port with a user defined rate.
<b>RATE</b>: values from the range (unit packet/s):
- <b>FE</b>: 1 - 262142
- <b>GE</b>: 1 - 2097150
<b>PORTS</b>: port number.</td></tr>
<tr><td><b>no storm-control</b> { broadcast | multicast | dlf } <i>PORTS</i></td><td>Disables specified storm control.</td></tr>
<tr><td><b>show storm-control</b> [<i>PORT</i>]</td><td>Exec/
Config/
Bridge</td><td>Displays a configuration of storm control,
<b>PORT</b>: port number.</td></tr>
</table>

ℹ By default, DLF storm control is enabled and MC storm control is disabled.

27 IRL - Input Rate Limitation

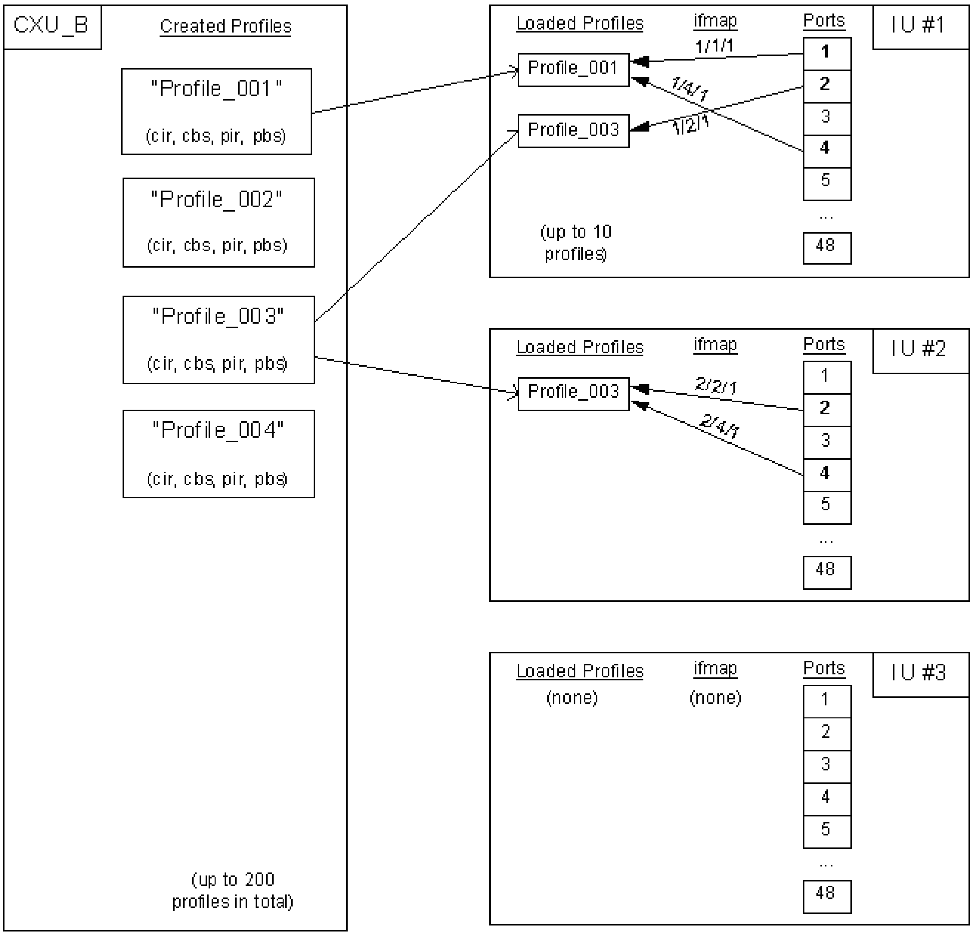
Input rate limiting (IRL) can be used to control the amount of incoming traffic at the subscriber's side. Many subscribers may share the same resources of the system and the network. IRL provides mechanisms to manage maximum and committed values of bandwidth (kbit/sec) and burst size (bytes).

IRL bases on profiles which are a kind of traffic policy. Each IRL profile determines a set of four values. The profile name must be unique.

Value	Unit	range
cir (committed information rate)	kbps	0-16000
pir (peak information rate)	kbps	0-16000
cbs (committed burst size)	bytes	96-10000
pbs (peak burst size)	bytes	96-15000

Table 26 IRL Values

A profile can be used to map one or more subscriber ports to it in order to activate IRL for these ports. Such ports can reside on the same or on different interface units (IUs). One profile can be referenced by any number of ports at the same time.



27.1 Creating a IRL Profile

Commands	Mode	Function
irl create profile *PROFILENAME*	Config	Creates a new IRL profile. **PROFILENAME**: enter a profile name.

Example of creating an IRL profile:

```
SWITCH(config)#irl create profileProfile_001
SWITCH(config)# irl set profile cir 1000
SWITCH(config)# irl set profile cbs 7500
SWITCH(config)# irl set profile pir 1000
SWITCH(config)# irl set profile pbs 10000
SWITCH(config)# irl apply profile
SWITCH(config)#show irl profile info Profile_001
------+-------+-------+-------+-------+----------------------
 CIR  |  CBS  |  PIR  |  PBS  | SNMP- | Profile Name
(kbps)|(bytes)| (kbps)|(bytes)| index |
------+-------+-------+-------+-------+----------------------
 1000 |  7500 |  1000 | 10000 |     1 | Profile_001
SWITCH(config)#
```

27.2 Modifying of IRL Profiles

Commands	Mode	Function
irl modify profile *PROFILENAME*	Config	Modifies an existing IRL profile. **PROFILENAME**: enter the profile name.
irl set profile { cir I cbs I pir I pbs } *VALUE*	Config	Sets IRL profile data, enter the profile name. **cir**: committed information rate <0-16000> **cbs**; committed burst size <96-10000> **pir**: peak information rate <0-16000> **pbs**: peak burst size <96-15000> **VALUE**: enter the value.

ℹ The order of **irl set profile** commands is arbitrary. Modifying of a profile is possible as long as **irl apply** command is not executed.

27.3 Saving a IRL Profile

A created or modified profile must be saved and applied to the system with the following command.

Commands	Mode	Function
irl apply profile	Config	Saves profile configuration.

ℹ If the IRL profile is not saved, all made settings will be lost.

Notes:

1. The **NE** manages up to 200 different profiles at the same time.
2. The name must be different. Otherwise the NE rejects the new profile or the modification.

3. The NE keeps the values of the last created or modified profile in a temporary memory. These values can be reused to create further profiles which only differ in e.g. the “cbs” value. That means, it is not necessary always to enter all four values if they are the same like in the previously created or modified profile.

27.4 Deleting a IRL Profile

Commands	Mode	Function
irl delete profile*PROFILENAME*	Privileged/ Config	Deletes an existing IRL profile. **PROFILENAME**: enter the profile name.

ℹ A currently used profile cannot be deleted. If this profile is referenced by one or more ports, the **show irl ifmap profile** command can be used to get a list of all ports which are mapped to it.

27.5 Mapping a Subscriber Port to IRL Profile

The mapping of a dedicated port to an existing IRL profile actives the input rate limiting for this port.

In order to map an IRL profile, use the following command.

Commands	Mode	Function
irl create ifmap *PORT PROFILNAME*	Config	Creates a new IRL port. **PORT**: subscriber port number **PROFILENAME**: enter profile name.

ℹ The port must be already exists and should be a subscriber port. The **NE** rejects not-created ports and ports which have a wrong type. However, offline configuration is of course possible (e.g. if the concerned IU is currently not plugged-in).

An example for creating IRL interface map.

```
SWITCH(config)#irl create ifmap1/1/1 Profile_001
SWITCH(config)#irl create ifmap1/4/1 Profile_001
SWITCH(config)#irl create ifmap2/2/1 Profile_003
SWITCH(config)#irl create ifmap2/4/1 Profile_003

SWITCH(config)#
```

The mapping can be deleted in order to stop IRL

Commands	Mode	Function
irl delete ifmap *PORT*	Config	Deletes an existing port from IRL profile. **PORT**: subscriber port name.

Notes:

1. The **irl create ifmap** command and the **irl delete ifmap** command are processed immediately. Afterwards, there is no need to execute the **irl apply** command.
2. One and the same IRL profile can be used for any number of ports residing on the same or different IUs
3. When an IRL profile is referenced the first time, it will be automatically loaded from CXU to that IU which owns the mapped port. It will be automatically unloaded if the

last port of this IU, that is mapped to this profile, is being unmapped. That means, unused (not referenced) profiles are not loaded on a IU in order to save profile memory on IUs.

4. This restriction (10 different profiles per IU) means that all IRL ports of one IU can be mapped to at most 10 different profiles. The NE rejects a port mapping command (**irl create ifmap**) for a further profile. In this case, an existing profile that fulfills the requirements as nearest as possible should be loaded.
5. The NE automatically deletes the port mapping if the concerned port is deleted and unloads the profile.

27.6 Checking the IRL Configuration

The system provides several ways to display IRL profiles, IRL port mapping, or both together.

To check an IRL profile and/or port mapping, use the following commands.

Commands	Mode	Function
show irl profile info	Privileged/ Config	Displays profile information of all existing profiles regardless used or unused.
show irl profile info *PROFILENAME*	Privileged/ Config	Displays profile values for a specified profile. **PROFILENAME**: enter the profile name.
show irl ifmap port *PORT*	Privileged/ Config	Displays IRL mapping information for a specified port. **PORT**: port number.
show irl profile editor	Privileged/ Config	Displays information of profile being created or modified.
show irl ifmap slot *SLOT*	Privileged/ Config	Displays all IRL mapping information for a specified slot together with their profile name. **SLOT**: slot number.
show irl ifmap profile *PROFILENAME*	Privileged/ Config	Displays all ports of the whole system (all slots), which are currently mapped to any given profile. **PROFILENAME**: enter the profile name.
show irl ifmap	Privileged/ Config	Displays IRL mapping information.

28 SNMP

An SNMP (simple network management protocol) system consists of three parts: SNMP manager, managed device, and SNMP agent. SNMP is an application-layer protocol that allows the SNMP manager and agent stations to communicate with each other. The SNMP manager and the agent use an SNMP Management Information Base (MIB) and a relatively small set of commands in order to exchange information. The SNMP MIB is organized in a tree structure with individual variables, such as point status or description, that are represented as leaves on the branches. An object identifier (OID) is used in order to distinguish each variable uniquely in the MIB and in SNMP messages. The SNMP configuration on the system determines the relationship between SNMP manager and agent. According to the community, different rights can be given - read only, write, or both read and write.The SNMP trap message allows the agent to spontaneously inform the SNMP manager about an important event and to alert the network status. It informs also about an improper user authentication, a reboot, the connection status (activate or deactivate), and closing of **TCP** connection to disconnect the neighboring system.

Following sections describe the SNMP configuration:

- Configuring an SNMP Community
- Configuring the SNMP Agentt
- Configuring an SNMP Group
- Configuring the SNMP MIB View
- Configuring the Access Policy for Group
- Configuring an SNMP Trap Host
- Checking the SNMP Configuration
- Disable SNMP.

28.1 Configuring an SNMP Community

According to the community, the access rights can be specified. A user is only authorized to access the SNMP agent of the system if a community has been configured for him. That means that the community name is usually the password to perform the identification for the remote SNMP management system. However, it is sent in clear text in the SNMP messages. As long as a community is configured, the NE is accessible full via SNMP v2c.
To configure a community in SNMP, use the following command.

Command	Mode	Function
snmp community { ro | rw } *COMMUNITY* [A.B.C.D] [*OID*]	Config	Creates a community and sets permission rights to allow authorized users the NE access over SNMP. **ro**: read only right to the MIB objects of NE **rw**: read-write right to the MIB objects of NE **COMMUNITY**: community name **A.B.C.D**: SNMP agent's IP address **OID**: only specified OID will be accessible.
no snmp community { ro | rw } *COMMUNITY*		Deletes specified community.

ℹ To access the NE, up to three SNMP communities for both reading right and writing right may be configured in the system.

To check configured communities, use the following command.

Command	Mode	Function
show snmp community	Privileged/ Config	Displays the communities.

Example:

The following example configures two communities: the first one with the password “public” and the access policy read/write and the other one as “private” with the access policy “read only”.

```
SWITCH(config)# snmp community rw public
SWITCH(config)# snmp community ro private
SWITCH(config)# show snmp community

Community List
         Community   Source         OID
-----------------------------------------------------
community  rw  public
community  ro private
SWITCH(config)#
```

28.2 Configuring the Security of SNMP Community

SNMP v2c authorizes the host to access the SNMP agent identified by both its IP address and the community name. The following command maps the identity of host and the community name to a security name. This mapping is needed to apply some access control settings also to the SNMP v1/v2 request with the specified community. The host IP address settings allows the SNMP agent to respond only to hosts with specified IP addresses. If the SNMP v1/v2c access support is needed not longer, the corresponding community settings have to be deleted.

Command	Mode	Function
snmp com2sec *SECURITY-NAME* { A.B.C.D I A.B.C.D/M } *COMMUNITY*	Config	Specifies the mapping from the identity of the host and community name to security name. **SECURITY-NAME**: security name **A.B.C.D**: host IP address **A.B.C.D/M**: host IP network **COMMUNITY**: community name.
no snmp com2sec *SECURITY-NAME*		Deletes the registered security name.

To check registered security name, use the following command.

Command	Mode	Function
show snmp com2sec	Privileged/ Config	Displays the registered security name.

An example of configuring com2sec and checking it.

```
SWITCH(config)# snmp com2sec switch 100.1.1.1 public
SWITCH(config)# show snmp com2sec
Com2Sec List
         SecName   Source     Community
```

```
----------------------------------------
 com2sec switch    100.1.1.1  public
SWITCH(config)#
```

28.3 Configuring the SNMP Agent

The SNMP agent and the MIB, which stores the information on system and network, reside on the NE. The SNMP agent uses MIB variables to reply on requests from SNMP administrator. The SNMP administrator can obtain data from the SNMP agent and on the other hand he can also save data in the SNMP agent.

Use the following commands to configure the identity of the agent accessing the NE over SNMP. This configuration is saved in the SNMP configuration file.

Command	Mode	Function
snmp agent-address A.B.C.D	Config	Configures the IP address of SNMP agent. **A.B.C.D**: IP address.
no snmp agent-address		Deletes IP address SNMP agent.
snmp location *NAME*		Configures the location name of SNMP agent. **NAME**: location name.
no snmp location		Deletes location of SNMP agent.
snmp contact *USER*		Configures name of user which can access the system. **USER**: user name.
no snmp contact		Deletes the name of accessed user.

Use the following commands to display information of the SNMP agent.

Command	Mode	Function
show snmp agent-address	Privileged/ Config	Shows SNMP agent IP address.
show snmp location		Shows location of SNMP agent.
show snmp contact		Shows the name of user with SNMP access.

Example:

```
SWITCH(config)# snmp contact manager
SWITCH(config)# snmp location ger_gwd
SWITCH(config)#
```

28.4 Configuring an SNMP Group

An SNMP group is a collection of SNMP users who share the same access permission. SNMP sets up the authentication strategy for a user and the group in which the user resides. In order to create/delete an group that can access the SNMP agent, use the following commands.

Command	Mode	Function
snmp group *GROUP* { v1 I v2c I v3 } *SECURITY-NAME*	Config	Creates an SNMP group **GROUP**: group name **v1**, **v2c**, **v3**: specify security level according to SNMP version **SECURITY-NAME**: security name (this is the name that is created with the **com2sec** command).
no snmp group *GROUP* { v1 I v2c I v3 }		Deletes specified SNMP group.

With the following command the SNMP groups can be verified.

Command	Mode	Function
show snmp group	Privileged/ Config	Checks the registered group.

28.5 Configuring the SNMP MIB View

Each object of MIB can be accessed by the SNMP manager over its unique ODI. Use the following command in order to create an SNMP view record that allows the SNMP agent, depending on the object identity (OID), to limit the user's access to MIB objects.

Command	Mode	Function
snmp view *VIEW* { included I excluded} *OID* [*MASK*]	Config	Configures OID which contains/does not contain a sub-tree. **VIEW**: MIB view record name **include**: includes MIB sub-tree **exclude**: excludes MIB sub-tree **OID**: OID number **MASK**: mask value (e.g. ff or ff.ff).
no snmp view *VIEW*		Deletes view of the specified name.

The following command displays the configured SNMP views.

Command	Mode	Function
show snmp view	Privileged/ Config	Shows configured view.

Example:

```
SWITCH(config)# show snmp view

View List
      ViewName   Type   SubTree   Mask
-------------------------------------------

SWITCH(config)#
```

28.6 Configuring the Access Policy for Group

To grant an SNMP group to access specific SNMP MIB view records, use the following command. SNMP v1/ v2c uses a community name for authentication without encryption.

Command	Mode	Function
snmp access *GROUP* { v1 | v2c } { *READ-VIEW* | *WRITE-VIEW* | *NOTIFY-VIEW* }	Config	Configures MIB view to permit for appropriate group in SNMP v1 or SNMP v2c. **GROUP**: group name **v1**, **v2c**: set the security level according to SNMP version **READ-VIEW**: set a read access view **WRITE-VIEW**: set a write access view **NOTIFY-VIEW**: set a notify access view.
no snmp access *GROUP*		Deletes the granted access of specified SNMP group to SNMP view records.

Use the following command to verify the permission of groups.

Command	Mode	Function
show snmp access	Privileged/ Config	Shows the granted access of SNMP group to a specific SNMP view record.

28.7 Configuring an SNMP Trap Host

An SNMP trap is a change-of-state message initiated by the SNMP agent. It alerts or notifies the SNMP manager about certain problems or important events of the SNMP agent. If SNMP trap was configured, the system transmits pertinent information to the network management program that is running on the so called trap-host.

ℹ The hiX 5750 R2.0 supports the configuration of up to 16 SNMP trap-hosts.

28.7.1 SNMP-V1/V2 Trap-Host

In order to configure a trap host receiving SNMP v1/v2c traps, use the following commands. The IP address of trap-host is always required. For example, if the SNMP manager is trap host then enter the IP address of SNMP manager.

Command	Mode	Function
snmp trap-host A.B.C.D [*COMMUNITY*]	Config	Configures SNMP v1 trap host. **A.B.C.D**: host IP address **COMMUNITY**: community name.
no snmp trap-host A.B.C.D		Deletes configured SNMP v1 trap host.
snmp trap2-host A.B.C.D [*COMMUNITY*]	Config	Configures SNMP v2 trap host.
no snmp trap2-host A.B.C.D		Deletes configured SNMP v 2 trap host.
snmp inform-trap-host A.B.C.D [*COMMUNITY*]	Config	Configures SNMP inform trap host.
no snmp inform-trap-host A.B.C.D		Deletes configured inform trap host.

Example:

An example of configuring the IP addresses 10.1.1.3, 20.1.1.5, and 30.1.1.2 as SNMP trap-host.

```
SWITCH(config)# snmp trap-host 10.1.1.3
SWITCH(config)# snmp trap-host 20.1.1.5
SWITCH(config)# snmp trap-host 30.1.1.2
SWITCH(config)#
```

An example of checking the above trap-host configuration.

```
SWITCH(config)# show snmp trap
Trap-Host List
HostCommunity
-------------------------------------------
trap-host 30.1.1.2
trap-host 20.1.1.5
trap-host 10.1.1.3
trap-host 210.0.0.100
SWITCH(config)#
```

28.7.2 Displaying the SNMP Trap Configuration

To show SNMP trap configuration, use the following command.

Command	Mode	Function
show snmp trap	Privileged/ Config	Shows SNMP trap configuration.

28.7.3 Displaying and Resetting the SNMP Trap Counter

Use the following commands to get information about number of counted traps.

Command	Mode	Function
snmp trap-counter reset	Config	Reset the SNMP trap counter.
show snmp trap-counter	Privileged/ Config	Shows the SNMP trap counter.

Example:

```
SWITCH(config)# show snmp trap-counter
snmp trap-counter 4662
SWITCH(config)# snmp trap-counter reset
SWITCH(config)# show snmp trap-counter
snmp trap-counter 1
SWITCH(config)#
```

28.8 Checking the SNMP Configuration

To check SNMP configuration, use the following command.

Command	Mode	Function
show snmp	Privileged/ Config	Shows the configuration of the switch.

28.9 Disable SNMP

SNMP is enabled by default. To disable SNMP on the system, use the following command.

Command	Mode	Function
no snmp	Config	Disables SNMP.

⚠ Using the above command, all configurations concerned with SNMP will be deleted.

29 System Logger (Syslog)

Syslog is a logging feature that gives administrators a way to centrally log and analyze configuration events and system error messages. This chapter describes the syslog configuration divided into the following sections:

- Configuring the Syslog Output Level
- Binding an IP Address
- Setting the local Facility Code
- Verifying and Clearing the local Syslog File
- Checking the Syslog Configuration
- Enabling/Disabling of Syslog Function.

29.1 Configuring the Syslog Output Level

The syslog function allows the **NE** to generate event notifications which can be forwarded to different event message collectors such as the console, the system memory, or a remote syslog server. The system logs errors depending on its importance with different severity levels. The highest level is “emergency” and the lowest one is “informational”. Only messages with an severity of at least the configured level and higher will be forwarded to the specified output, all other will be suppressed. That means, the “informational” level must be configured in order to receive all messages on the management system at last. It is possible, to configure the syslog output level with or without reference to the subsystem that generates the message.

29.1.1 Syslog Output Level without a Priority

Use the following commands, to configure the severity levels of syslog messages and to determine its output redirection. The output takes place regardless of a priority which part of system has generated the message.

Command	Mode	Function
syslog output { emerg | alert | crit | err | warning | notice | info | debug } **local** { volatile | non-volatile }	Config	Transmits syslog message of configured level to specified output. Severity levels: **emerg**: emergency(0) **alert**: alert(1) or more serious **crit**: critical(2) or more serious **err**: error(3) or more serious **warning**: warning(4) or more serious **notice**: notice(5) or more serious **info**: informational(6) or more serious **debug**: debug(7) or more serious System logger output redirection: Local output file (system memory), see also 29.4 Verifying and Clearing the local Syslog File **volatile**: deletes a syslog message after restart **non-volatile**: reserves a syslog message **A.B.C.D**: remote log host IP address Use the **no** parameter with this command to disable specified syslog output.
syslog output { emerg | alert | crit | err | warning | notice | info | debug } **remote** A.B.C.D		
syslog output { emerg | alert | crit | err | warning | notice | info | debug } **console**		

An example of configuring syslog to send all logs higher than “notice” to the remote log host IP address 10.1.1.1:

```
SWITCH(config)#syslog output notice remote 10.1.1.1
SWITCH(config)#
```

29.1.2 Syslog Output Level with a Priority

Use the following commands, to configure syslog messages depending on severity level, output redirection, and prioritized facility type generating the message.

Command	Mode	Function
syslog output priority { auth I authpriv I cron I daemon I kern I local1 I local2 I local3 I local4 I local5 I local6 I local7 I lpr I mail I news I syslog I user I uucp } { emerg I alert I crit I err I warning I notice I info } **local** { volatile I non-volatile }	Config	Transmits syslog message of configured level to specified output with chosen priority. Facility types: **auth**: security/authorization message **authpriv**: security/authorization message **cron**: clock daemon **daemon**: system daemons without separate facility value **kern**: kernel messages **local1... local7**: reserved for local use, see also 29.3 Setting the local Facility Code **lpr**: line printer subsystem **mail**: mail subsystem **news**: USENET news subsystem **syslog**: messages generated internally by syslog **user**: generic user-level messages **uucp**: UUCP subsystem Severity levels: **emerg**: emergency(0) **alert**: alert(1) or more serious **crit**: critical(2) or more serious **err**: error(3) or more serious **warning**: warning(4) or more serious **notice**: notice(5) or more serious **info**: informational(6) or more serious System logger output redirection: Local output file (system memory): **volatile**: deletes a syslog message after restart **non-volatile**: reserves a syslog message **A.B.C.D**: remote log host IP address Use the **no** parameter with this command to disable specified syslog output.
syslog output priority { auth I authpriv I cron I daemon I kern I local1 I local2 I local3 I local4 I local5 I local6 I local7 I lpr I mail I news I syslog I user I uucp } { emerg I alert I crit I err I warning I notice I info } **remote** A.B.C.D		
syslog output priority { auth I authpriv I cron I daemon I kern I local1 I local2 I local3 I local4 I local5 I local6 I local7 I lpr I mail I news I syslog I user I uucp } { emerg I alert I crit I err I warning I notice I info } **console**		

29.2 Binding an IP Address

Use the following command, to specify an IP address that is attached to the syslog message for its identity.

Command	Mode	Function
syslog bind-address A.B.C.D	Config	Specifies IP address for a syslog message identity. **A.B.C.D**: IP address.
no syslog bind-address		Deletes a specified binding IP address.

29.3 Setting the local Facility Code

Setting a facility code makes a generated syslog message distinguished from others, so that a network administrator can efficiently handle various syslog messages.
To set a facility code, use the following command.

Command	Mode	Function
syslog local-code <0-7>	Config	Sets local facility code for system use. **0 - 7**: from 0 (LOG_LOCAL0) to 7(LOG_LOCAL7).
no syslog local-code		Deletes a specified facility code.

29.4 Verifying and Clearing the local Syslog File

To check and delete the messages that are saved in the system memory, use the following commands.

Command	Mode	Function
show syslog local volatile [NUM]	Exec/ Config	Shows a received syslog message. **volatile**: memory to remove a syslog message after restart **NUM**: latest lines number.
clear syslog local volatile	Config	Deletes received syslog message from the system memory, **volatile**: deletes memory to remove a syslog message after restart.

29.5 Checking the Syslog Configuration

Use the following command to verify the syslog configuration.

ℹ The syslog configuration cannot be checked by using a **show running-config** command.

Command	Mode	Function
show syslog	Exec/ config	Shows a configuration of the syslog.

The following example shows a configuration that an emergency message sends to the console and all messages of level info and higher saves in the volatile file.

```
SWITCH(config)#show syslog
info local volatile
emerg console
SWITCH(config)#
```

29.6 Enabling/Disabling of Syslog Function

ℹ It is important that syslog is always running on the system. Therefore, syslog is enabled after the system start/reboot by default. Executing the **syslog start** command is only necessary when the function was manually disabled.

Use the following commands to enable/disable the syslog function.

Command	Mode	Function
syslog start	Config	Enables the syslog.
no syslog		Disables the syslog.

30 Remote Monitoring

Remote monitoring (RMON) is a function to observe the communication status of connected Ethernet devices. While **SNMP** can advertise only information about devices mounted via SNMP agent, RMON allows exchanging network monitoring data for devices overall segments. For Ethernet interfaces, RMON gathers cumulative statistics and tracks a history of statistics. The RMON standard defines objects that are suitable for an effectively management of Ethernet networks.

Because RMON processes lots of data, take care to prevent performance degradation caused by RMON. The hiX 5750 R2.0 supports the following RMON groups, as described in RFC 1757:

- Group 1: statistics (only for uplink ports)
- Group 2: history.

30.1 Configures Number of RMON History

RMON history is periodical sample inquiry of statistical data about each traffic occurred in Ethernet port. All ports are pre-configured, to monitor statistical data in an interval of 30-minute and to archive 50 statistical data. It is also possible to change the time interval taking the sample and the number of samples that should be saved.

The default configuration of history is displayed as result of the following command:

```
SWITCH(config)#show rmon-history config 1
RMON History configuration:
===========================
history index      : 1
data source        : 0/1 (1)
buckets requested  : 50
buckets granted    : 50
interval time (s)  : 1800
owner              : none
status             : under create
SWITCH(config)#
```

To configure RMON history, enter into *History configuration* mode first. The system prompt changes from `SWITCH(config)#` to `SWITCH(config-rmonhistory[n])#`. The variable “n” is the number to be configured to distinguish each different history.

Command	Mode	Function
rmon-history <1-65535>	Config	Configures a number to distinguish RMON History, enter the index number.

Example of entering into *History configuration* mode to configure history 5.

```
SWITCH(config)#rmon-history 5
SWITCH(config-rmonhistory [5])#
```

30.2 Assigning Source Port of statistical Data

To investigate statistical data from a specified port as sample inquiry, a source port has to be assigned by using the following command.

Command	Mode	Function
data-source *PORT*	RMON	Assigns a source port of statistical CXU uplink port. **PORT**: uplink port number (ex. slot/port for uplink port, slot/port/vcc for data port)

Example of assigning CXU uplink port 1 as source port.

```
SWITCH(config-rmonhistory [5])#data-source 9/1
SWITCH(config-rmonhistory [5])#
```

30.3 Identifying Subject of RMON History

To identify subject using the history, enter the following command.

Command	Mode	Function
owner *NAME*	RMON	Configures History and identifies subject using related data, enter the name (max. 127 characters).

Example of configuring a subject of history as “nokia”.

```
SWITCH(config-rmonhistory [5])#owner nokia
SWITCH(config-rmonhistory [5])#
```

30.4 Configuring Number of Sample Data

Configure the number of sample data in RMON history.

Command	Mode	Function
requested-buckets <1-65535>	RMON	Defines the bucket count for the interval, enter the number of buckets.

ℹ The max. number of granted buckets is 100.

Example of configuring the number of sample data as 25 in history.

```
SWITCH(config-rmonhistory [5])#requested-buckets 25
SWITCH(config-rmonhistory [5])#
```

30.5 Configuring Interval of Sample Inquiry

Command	Mode	Function
interval <1-3600>	RMON	Defines the time interval for the history (in seconds), enter the value.

ℹ The interval will be rounded up to a multiple of 30 seconds.

Example of configuring the interval of sample inquiry as 60 seconds.

```
SWITCH(config-rmonhistory [5])#interval 60
SWITCH(config-rmonhistory [5])#
```

30.6 Activating the RMON History

Finishing all configuration steps above, the RMON history must be activeded using the following command.

Command	Mode	Function
active	RMON	Activates RMON history.

ℹ Before activating RMON history, check if the configuration is correct. The configuration of an activated RMON history cannot be changed. If the configuration needs to be changed, delete the RMON history and configure it again.

30.7 Displaying RMON History

Command	Mode	Function
show rmon-history config [<1-65535>]	Privileged/ Rmon/Config	Shows the configuration of RMON history of specified number. **1 - 65535**: value for specifying.

Example of activating RMON history and viewing the configuration.

```
SWITCH(config-rmonhistory [5])#active
SWITCH(config)#show rmon-history config 5
---------------------------------------------------------------
history | data source | interval| buckets | status| owner
---------------------------------------------------------------
5       | 9/1         | 60 s    | 25/25   | valid | nokia
SWITCH(config)#
```

To show RMON ether history table, use the following command.

Command	Mode	Function
show rmon-history ether-history <1-65535> [1-100] **Note**: always the last n values will be displayed but no more than the number of the granted buckets.	Config	Shows the ether history entries (sampling values). **1 - 65535**: enter the history index for history table **1 - 100**: enter the number of samples should be displayed.

30.8 Deleting the RMON History

To change the history configuration, delete the history and then configure it again.

Command	Mode	Function
no rmon-history <1-65535>	Config	Deletes RMON history of specified number, **1 - 65535**: enter the history index for deleting.

Example of deleting RMON history 5.

```
SWITCH(config)#no rmon-history 5
SWITCH(config)#
```

31 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)