FURUKAWA

OLT EPON FK-C2-RADC

User´s Manual

Table of Contents

Caution

Circuit devices are sensitive to static electricity, which can damage their delicate electronics. Dry weather conditions or walking across a carpeted floor may cause you to acquire a static electrical charge.

To protect your device, always:
▪ Touch the metal chassis of your computer to ground the static electrical charge before you pick up the circuit device.
▪ Pick up the device by holding it on the left and right edges only.

Electronic Emission Notices

Federal Communications Commission (FCC) Statement

This equipment has been tested and found to comply with the limits for a class A computing device pursuant to Subpart J of part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment.

European Community (CE) Electromagnetic Compatibility Directive

This equipment has been tested and found to comply with the protection requirements of European Emission Standard EN55022/EN60555-2 and the Generic European Immunity Standard EN50082-1.

EMC:

EN55022(1988) /CISPR-22(1985)	class A
EN60555-2(1995)	class A
EN60555-3	
IEC1000-4-2(1995)	4k V CD, 8kV, AD
IEC1000-4-3(1995)	3V/m
IEC1000-4-4(1995)	1kV – (power line), 0.5kV – (signal line)

Introduction

Overview

The FK-C2-RADC manageable box is an OLT with cabinet height 1U. It is designed to accommodate 2-Port GEPON OLT fiber interface modules at a central location for PON (Passive Optical Network) application. Any combination of GEPON Fiber conversion solutions can be installed in a wiring closet for cable connection. The network management supports Web UI via browser, CLI via local console, Telnet/SSH interface and SNMP v1/v2c/v3. Supports IEEE 802.3ah OAM function for CO and CPE site “Remote Failure Indication”, “Remote Loopback” and “Link Monitoring”. Supports “Port Configuration” and “Bandwidth Configuration”.

The FK-C2-RADC includes a 2-Port of GEPON, providing ideal flexibility to design suitable network infrastructure for business requirements. It supports advanced security management capabilities and network features. Besides, it is easy to deploy and configure, providing stability and quality network services your business needs.

Overview of this user’s manual

Chapter 1 “Operation of Web-based Management”

Chapter 2 “System Configuration”

Chapter 3 “OLT Management”

Chapter 4 “ONU Management”

Chapter 5 “Configuration”

Chapter 6 “Security”

Chapter 7 “Maintenance”

Chapter 8 "CLI Management"

1 Operation of Web-based Management

1.1 Initial Configuration

This chapter instructs you how to configure and manage the FK-C2-RADC through the web user interface. With this functionality, you can easily access and monitor the equipment.
The default values of the FK-C2-RADC are shown in the table below:

IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Default Gateway	192.168.1.254
Username	admin
Password	

Type http://192.168.1.1 in the address row of the browser, it will show the following screen and ask you to input a username and password in order to login and access the interface.
The default username is “admin” and password is empty. On the first access please enter the default username and password, and then click the <OK> button. The login process now is completed. In this login menu, you have to input the complete username and password respectively, the FK-C2-RADC will not give you a tip about the username. This looks inconvenient, but safer.
The FK-C2-RADC supports a simple user management function allowing only one administrator to configure the system at the same time. If there are two or more users using administrator’s identity, it will only allow the one who logins first to configure the system. The rest of the users, even with administrator’s identity, can only monitor the system. The maximum number of users that are able to login simultaneously is 16.

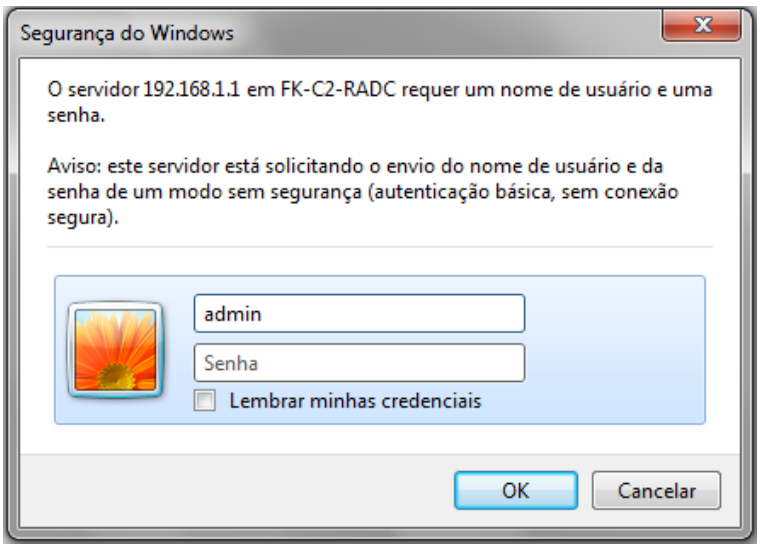


Figure 1-1: The login page

NOTE:
When you login FK-C2-RADC Web UI management, you can use either IPv4 or IPv6 login to manage.

To optimize the display effect, we recommend you to use Microsoft IE 6.0 or above, Netscape V7.1 or above, or FireFox V1.00 or above and have the resolution adjusted to 1024x768.

2 System Configuration

This chapter describes all the basic configuration tasks which includes the System Information and any manageable function of the FK-C2-RADC (e.g. Time, Account, IP, Syslog and SNMP).

2.1 System Information

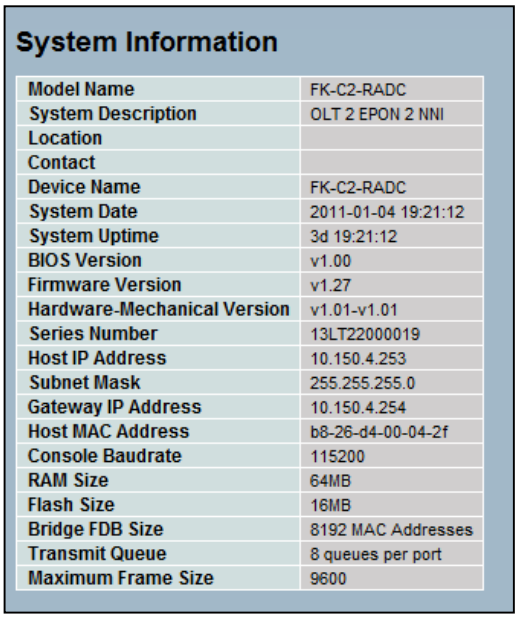
After you login, you can see and configure the system information.

It will display the FK-C2-RADC system information.

Web interface

To check the System Information in the web interface:

1. Click System, System Information and Information.



System Information

Model Name	FK-C2-RADC
System Description	OLT 2 EPON 2 NNI
Location	
Contact	
Device Name	FK-C2-RADC
System Date	2011-01-04 19:21:12
System Uptime	3d 19:21:12
BIOS Version	v1.00
Firmware Version	v1.27
Hardware-Mechanical Version	v1.01-v1.01
Series Number	13LT22000019
Host IP Address	10.150.4.253
Subnet Mask	255.255.255.0
Gateway IP Address	10.150.4.254
Host MAC Address	b8-26-d4-00-04-2f
Console Baudrate	115200
RAM Size	64MB
Flash Size	16MB
Bridge FDB Size	8192 MAC Addresses
Transmit Queue	8 queues per port
Maximum Frame Size	9600

Figure 2-1: System Information

Parameter description:

- **Model Name:** To display the device model name.
- **System Description:** To display the device description and product type.
- **Location:** To display device implement location (Configurable).
- **Contact:** To display the contact information (Configurable).
- **Device name:** To display the system name, the default value is the Model name (Configurable).
- **System Date:** The current (GMT) system time and date. The system time is obtained through the configured NTP Server or through synchronization with your PC.
- **System Uptime:** The period of time the device has been operational.
- **BIOS version:** To display the system BIOS current version.
- **Firmware version:** To display the system firmware current version.
- **Hardware-Mechanical version:** To display the system hardware-mechanical current version.
- **Series Number:** To display the system series number, that you can record the information and maintenance the device.
- **Host IP address:** To display the device's IP address
- **Subnet mask:** To display the device's subnet mask (Configurable).
- **Gateway IP address:** To display the device's gateway IP address (Configurable).
- **Host MAC address:** To display the device's MAC address.
- **Console Baudrate:** To display the device's console baudrate information to connect to the device's console port.

- **RAM Size:** To display the device's ram size information.
- **Flash Size:** To display the device's flash size information.
- **Bridge FDB size:** To display the bridge FDB size information.
- **Transmit Queue:** To display the device's transmit hardware priority queue information.
- **Maximum Frame size:** To display the device's maximum frame size information.

2.1.1 Configuration

This section will let you understand how to identify the system by configuring the contact information, name, and location of the OLT.

Web interface

To configure System Information in the web interface:

1. Click System, System Information, Configuration.
2. Write System Contact , System Name, System Location information in this page.
3. Click Save

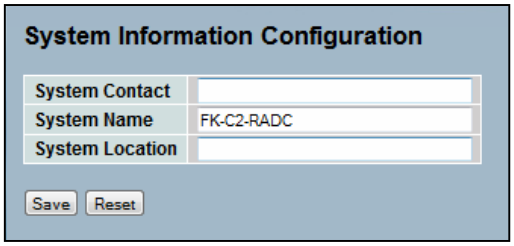


Figure 2-2: System Information Configuration

Parameter description:

- **System Contact:** The textual identification of the contact person for this managed node and the information on how to contact this person. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
- **System Name:** An administratively assigned name for this managed node. By convention, this is the node's fully-qualified domain name. A domain name is a text string drawn from the alphabet (A-Z, a-z), digits (0-9), minus sign (-). No space characters are permitted as part of a name. The first character must be an alpha character. And the first or last character must not be a minus sign. The allowed string length is 0 to 255.
- **System Location:** The physical location of this node (e.g., telephone closet, 3rd floor). The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
- Buttons:

Save: Click to apply the changes made.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.2 Time

This section will teach you how to configure the FK-C2-RADC host's time. Time configuration includes local Time Configuration and NTP Configuration.

2.2.1 Manual

Manual setting is simple and you just input "Year", "Month", "Day", "Hour", "Minute" and "Second" within the valid value range indicated for each item.

Web Interface

To configure Time in the web interface:

1. Click System, Time and Manual.
2. Specify the Time parameter in manual parameters.
3. Click Save.

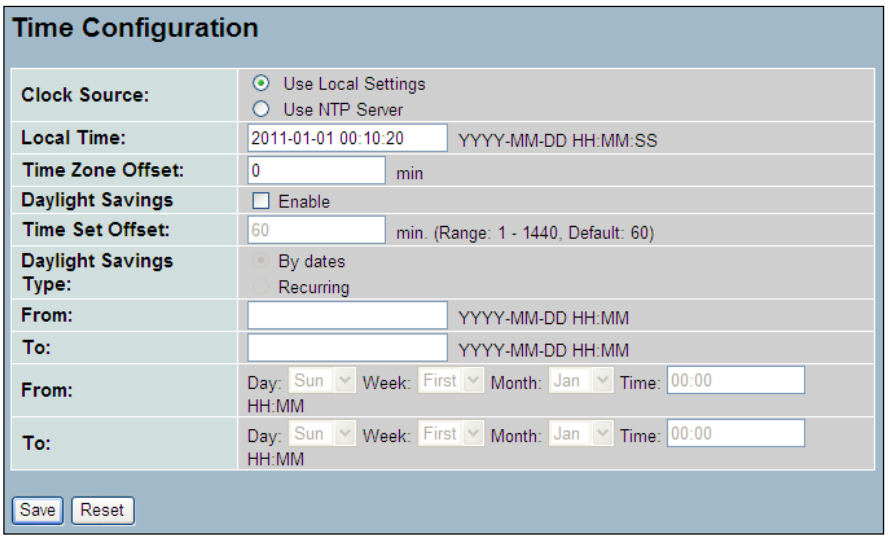


Figure 2-3: The time configuration

Parameter description

• **Clock Source:** To define the clock source for the FK-C2-RADC. You can select "Use local Settings" or "Use NTP Server" for FK-C2-RADC time clock source.

• **Local Time:** Show the current time of the system.

• **Time Zone Offset:** Provide the time zone offset relative to UTC/GMT. The offset is given in minutes east of GMT. The valid range is from -720 to 720 minutes

• **Daylight Saving:** Daylight saving is adopted in some countries. If set, it will adjust the time lag or in advance in unit of hours, according to the starting date and the ending date. For example, if you set the day light saving to be 1 hour. When the time passes over the starting time, the system time will be increased one hour after one minute at the time it passed over. And when the time passes over the ending time, the system time will be decreased one hour after one minute at the time it passed over.

The switch supports valid configurable day light saving time is –5 ~ +5 step one hour. The zero for this parameter means it doesn't need to adjust current time, equivalent to in-act daylight saving. You don't have to set the starting/ending date as well. If you set daylight saving to be non-zero, you have to set the starting/ending date as well; otherwise, the daylight saving function will not be activated.

• **Time Set Offset:** Provide the Daylight saving time set offset. The offset is given in minutes east of GMT. The valid range is from 1 to 1440 minutes. Default is 60 min.

• **Daylight Savings Type:** Provide the Daylight savings type selection. You can select "By Dates" or "Recurring" two types for Daylight saving type.

• **From:** To configure when Daylight saving start. The date and time format is "YYYY-MM-DD HH:MM".

• **To:** To configure when Daylight saving end. The date and time format is "YYYY-MM-DD HH:MM".

NOTE: The under "from" and "to" will display what you set on the "From" and "To" field information.

• **Buttons:**
Save: Click to apply the changes made.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.2.2 NTP (Network Time Protocol)

Web Interface

To configure NTP in the web interface:
1. Click System, Time and NTP.
2. Change mode to "Enabled".
3. Inform the server address.
4. Click Save.

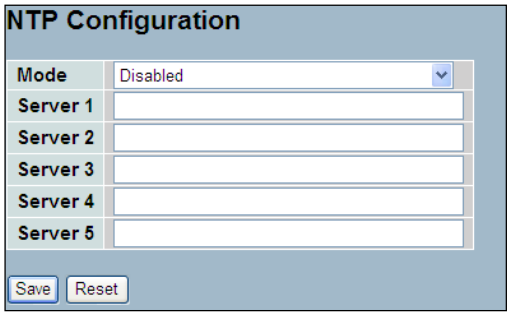


Figure 2-4: The NTP Server configuration

Parameter description
• **Mode:** Indicates the NTP mode operation. Possible modes are:
Enabled: Enable NTP mode operation. When NTP mode operation is enabled, the agent forwards NTP messages between the clients and the server when they are not on the same subnet domain.
Disabled: Disable NTP mode operation.
• **Server 1to 5:** Provide the NTP IPv4 or IPv6 address.
• **Buttons:**
Save – Click to save changes.
Reset – Click to undo any changes made locally and revert to previously saved values.

2.3 Account

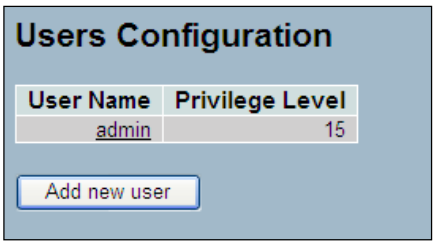
This section teaches you how to set the account and the rights to access the FK-C2-RADC. Only the administrator can create, modify or delete the username and password. Up to 20 accounts can be created.

2.3.1 Users

Web Interface

To configure Account in the web interface:

1. Click System, Account and Users.
2. Click Add new user



3. Specify the User Name parameter.

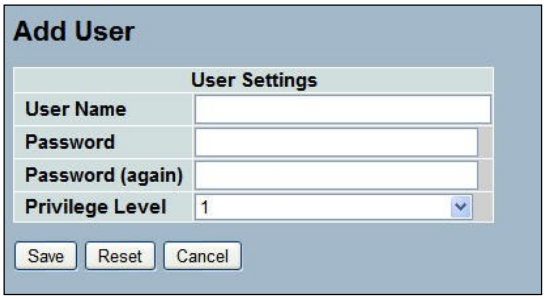


Figure 2-5: The Users Account configuration

4. Click Save.

Parameter description

- **User Name:** The name identifying the user. This is also a link to Add/Edit User.
- **Password:** To type the password. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 32 to 126.
- **Password (again):** To type the password again. You must type the same password again in the field.
- **Privilege Level:** The privilege level of the user. The allowed range is 1 to 15. If the privilege level value is 15, it can access all groups, i.e. that is granted the fully control of the device. But other values need to refer to each group privilege level. User's privilege should be the same or greater than the group privilege level to have access to that group. By default setting, groups with privilege level 5 have the read-only access and groups with privilege level 10 have the read-write access. And the system maintenance (software upload, factory defaults and etc.) need an user privilege level 15. Generally, the privilege level 15 can be used for an administrator account, privilege level 10 for a standard user account and privilege level 5 for a guest account.

2.3.2 Privilege Level

This section provides an overview of the privilege levels. The switch permits the user to set the Account, Diagnostics, IP, Maintenance, OLT, ONU, SMTP, SNMP, Security, System and Trap Privilege Levels from 1 to 15.

Web Interface

To configure Privilege Level in the web interface:

1. Click SYSTEM, Account, Privilege Level.

2. Specify the Privilege parameter.
3. Click Save.

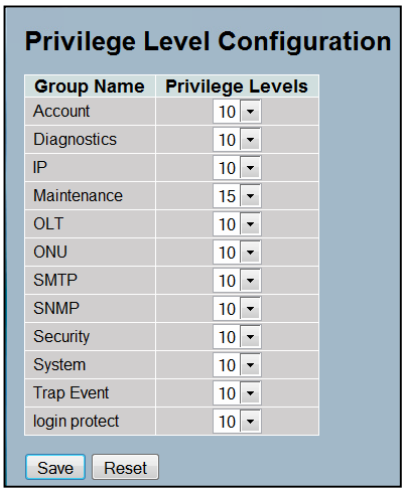


Figure 2-6: The Privilege Level configuration

Parameter description

• **Group Name:** The name identifying the privilege group. In most cases, a privilege level group consists of a single module, but some of them contain more than one. The following description defines these privilege level groups in details, for example:

System: Contact, Name, Location, Time zone, Log.

Security: Authentication, System Access Management, Port (contains Dot1x port, MAC based and the MAC Address Limit), ACL, HTTPS, SSH, ARP Inspection and IP source guard.

IP: Everything except 'ping'.

Port: Everything except 'VeriPHY'.

Diagnostics: 'ping' and 'VeriPHY'.

Maintenance: CLI- System Reboot, System Restore Default, System Password, Configuration Save, Configuration Load and Firmware Load. Web- Users, Privilege Levels and everything in Maintenance.

• **Privilege Levels:** Every group has an authorization Privilege level for the following sub groups: configuration read-only, configuration/execute read-write, status/statistics read-only, status/statistics read-write (e.g. for clearing of statistics). User Privilege should be the same or greater than the authorization Privilege level to have the access to that group.

2.4 IP

This section teaches you how to set the FK-C2-RADC's IP address. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing an excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

2.4.1 IPV4

It's possible to set the IP address manually or using a DHCP server. To manually configure an address, you need to change the switch's default settings to values that are compatible with your network. You may also need to establish a default gateway between the switch and management stations that exist on another network segment.

Configure the switch-managed IP information on this page.

The Configured column is used to view or change the IP configuration.

The Current column is used to show the active IP configuration.

Web Interface

To configure an IP address in the web interface:

1. Click System, IP and IPv4.
2. Specify the IPv4 settings, and enable DNS proxy service if required.
3. Click Save.

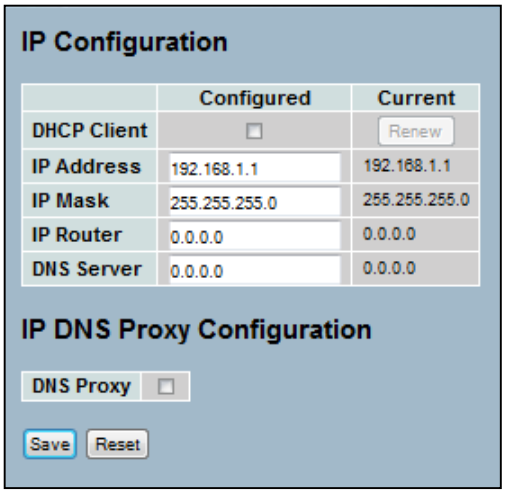


Figure 2-7: The IP address of IPv4 configuration

Parameter description

- **DHCP Client:** It enables the DHCP client by checking this box. If DHCP fails and the configured IP address is zero, DHCP will retry, but if the DHCP fails and the configured IP address is non-zero, DHCP will stop and the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup.
- **IP Address:** IP address of this switch is in dotted decimal notation.
- **IP Mask:** IP mask of this switch is in dotted decimal notation.
- **IP Router:** IP address of the router which FK-C2-RADC connects is in dotted decimal notation.

• **DNS Server:** IP address of the DNS Server is in dotted decimal notation.
• **DNS Proxy:** To enable or disable the DNS proxy. DUT will relay DNS requests to the current configured DNS server on DUT, and reply as a DNS resolver to the client devices on the network.
• **Buttons:**
Save: Click to apply the changes made.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.4.2 IPV6

This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. And the Current column is used to show the active IPv6 configuration.

Web Interface

To configure Management IPv6 of the switch in the web interface:
1. Click System, IP and IPv6.
2. Specify the IPv6 settings, and enable Auto Configuration service if required.
3. Click Save.

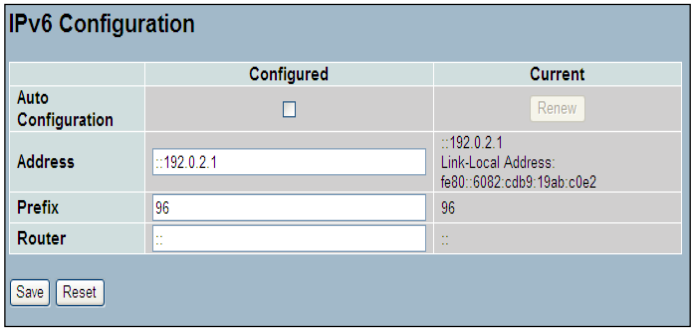


Figure 2-8: The IP address of IPv6 configuration

Parameter description
• **Auto Configuration:** To enable or disable IPv6 auto-configuration by checking this box.
• **Address:** IPv6 address of this switch.
Note: IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separating each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It can also represent a legally valid IPv4 address. For example, '::192.1.2.34'.
• **Prefix:** IPv6 Prefix of this switch. The allowed range is 1 to 128.
• **Router:** IPv6 gateway address of this switch.
• **Buttons:**
Save: Click to apply the changes made.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.5 Syslog

2.5.1 Configuration

This section describes how to configure the system log server.

Web Interface

To configure the Syslog Server in the web interface:

1. Click System, Syslog and Configuration.
2. Change the server mode to "Enabled".
3. Specify the syslog parameters including IP Address of Syslog server and the level from which the logs will be reported.
4. Click Save.

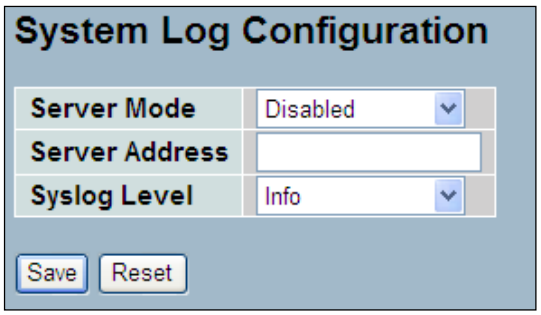


Figure 2-9: The System Log configuration

Parameter description

• **Server Mode:** Indicates the server mode operation. When the server mode operation is enabled, the syslog messages will be sent to a syslog server. The syslog protocol is based on UDP communication and received on UDP port 514, and the syslog server will not send acknowledgments back to the sender since UDP is a connectionless protocol and it does not provide acknowledgments. The syslog packet will always be sent even if the syslog server does not exist. Possible modes are:

Enabled: Enable server mode operation.

Disabled: Disable server mode operation.

• **Server Address:** Indicates the IPv4 host address of the syslog server.

• **Syslog Level:** Indicates what kind of message will be sent to the syslog server. Possible modes are:

Emerg: send Emerg

Alert: send Emerg, Alert

Crit: send Emerg, Alert, Crit

Error: send Emerg, Alert, Crit, Error

Warning: Send warnings

Notice: send Emerg, Alert, Crit, Error, Warning, Notice

Info: send Emerg, Alert, Crit, Error, Warning, Notice, Info

Debug : send everything, i.e. all

• **Buttons:**

Save: Click to apply the changes made.

Reset: Click to undo any changes made locally and revert to previously saved values.

2.5.2 Log

Web Interface

Display the log configuration in the web interface:

1. Click System, Syslog and Log.
2. To upload the logs using a TFTP Server, first configure the server then click on the Upload button.
3. To configure the auto upload function change the mode to "Enable". The auto upload will occur when the list reaches 200 entries.
4. Click Save.

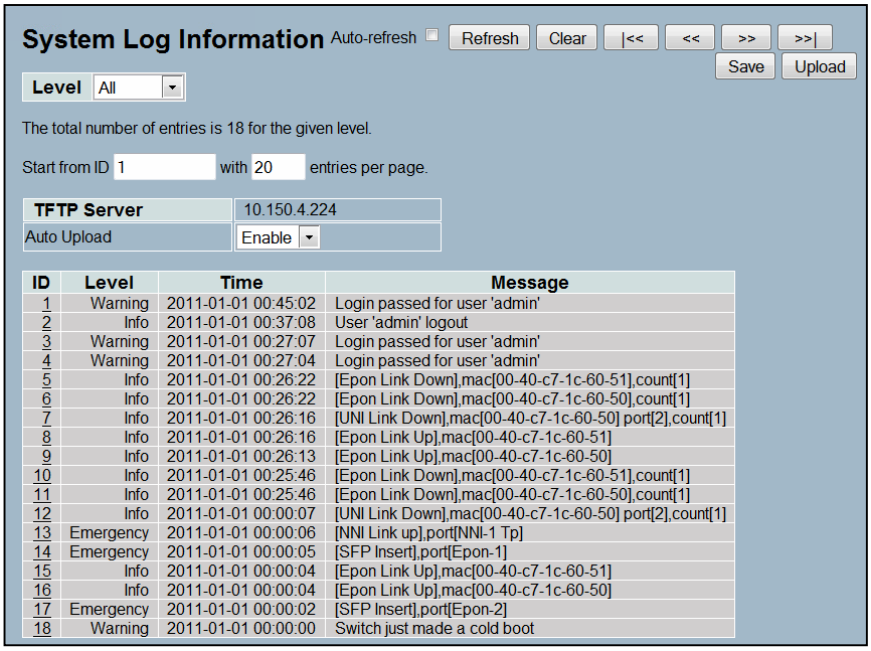


Figure 2-10: The System Log display

Parameter description

• **TFTP Sever:** TFTP server IP address for log data upload. To configure the server address click Maintenance - > TFTP Server.

• **Auto Upload:** enable/disable the auto upload function.

• **ID:** The ID (>= 1) of the system log entry.

• **Level:** The level of the system log entry. The following level types are supported:

<0> Emergency: System is unusable.

<1> Alert: Action must be taken immediately.

<2> Critical: Critical conditions.

<3> Error: Error conditions.

<4> Warning: Warning conditions.

<5> Notice: Normal, but significant conditions.

<6> Information: Information messages.

<7> Debug: Debug-level messages.

• **Time:** The time of the system log entry.

• **Message:** The message of the system log entry.

• **Buttons**

Auto-refresh: Check this box to refresh the page automatically. Automatic refresh occurs every 3 seconds.

Refresh: Click to refresh the page.

Clear: Flushes all system log entries.

Save: Save the configuration.

Upload: Upload the current logs to a file using the TFTP server.

2.5.3 Detailed Log

Web Interface

To display the detailed log configuration in the web interface:

1. Click System, Syslog and Detailed Log.

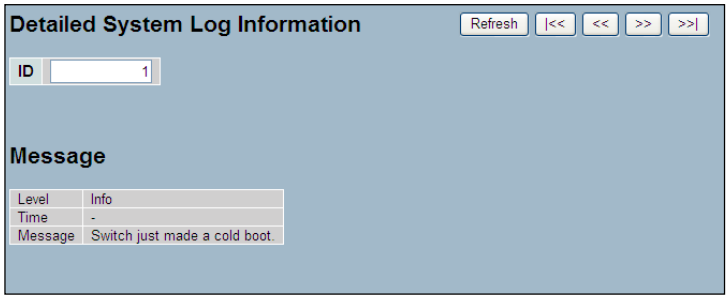


Figure 2-11: The System detail Log display

Parameter description

- **ID:** The ID (>= 1) of the system log entry.
- **Message:** The detailed message of the system log entry.
- **Refresh:** Click to refresh the page.

2.6 SNMP

This section will teach you how to use the SNMP protocol to manage the FK-C2-RADC. Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent once the right Management Information Base (MIB) is provided. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent must be running on the device to respond the request issued by SNMP manager.

2.6.1 System

Web Interface

To configure SNMP System in the web interface:

1. Click System, SNMP and System.
2. Enable or disable the SNMP function.
3. Specify the Engine ID
4. Click Apply.

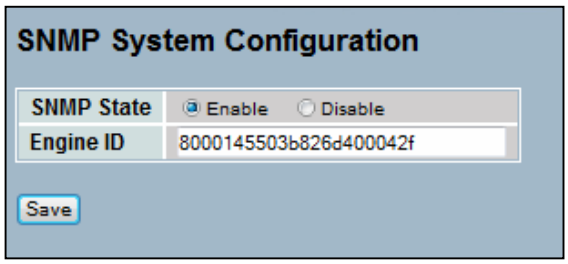


Figure 2-12: The SNMP system Configuration

Parameter description

• **SNMP State:** To activate or de-activate SNMP.
Enable: Enable SNMP operation.
Disable: Disable SNMP operation.
Default: Enable.
• **Engine ID:** SNMPv3 engine ID syntax: 0-9, a-f, A-F, min 5 octet, max 32 octet and the fifth octet can't be 00. If the Engine ID is changed, all original users will be cleared.

2.6.2 Communities

This function is used to configure SNMPv3 communities. The Community and UserName are unique. To create a new community account, please check <Add new community> button, and enter the account information then check <Save>. Max Group Number: 4.

Web Interface

To configure SNMP Communities in the web interface:

1. Click System, SNMP and Communities.
2. Click Add new community.
3. Specify the SNMP community parameters.
4. Click Save.

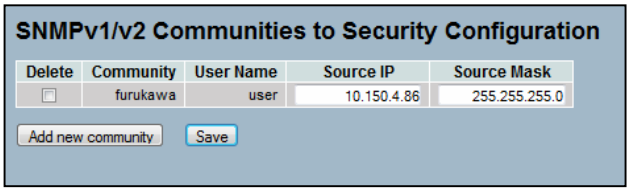


Figure 2-13: The SNMP communities Configuration

Parameter description

- **Delete:** Check to delete the entry. It will be deleted on next save.
- **Community:** Indicates the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126. The community string will be treated as security name and will map a SNMPv1 or SNMPv2c community string.
- **UserName:** The UserName access string to permit access to SNMPv3 agent. The length of the "UserName" string is restricted to 1-32.
- **Source IP:** Indicates the SNMP access source address. A specific range of source addresses can be used to restrict a source subnet when combined with source mask.
- **Source Mask:** Indicates the SNMP access source address mask.
- **Buttons:**

Add new community: Click to add a new community.
Save: Click to apply the changes made.

2.6.3 Users

This function is used to configure SNMPv3 user. The Entry index key is UserName. To create a new UserName account, please check <Add new user> button, and enter the user information then check <Save>. Max Group Number : 10.

Web Interface

To configure SNMP Users in the web interface:

1. Click System, SNMP and Users.
2. Click Add new user.
3. Specify the User name, security level, authentication protocol and passwords.
4. Click Save.

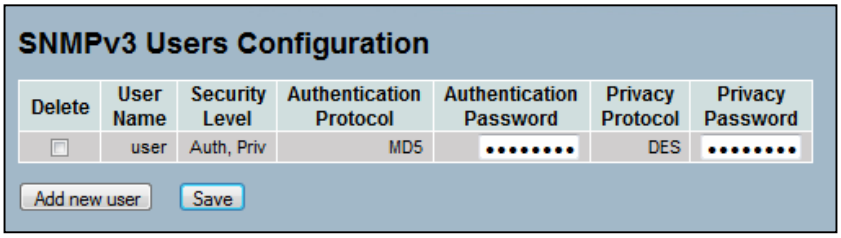


Figure 2-14: The SNMP Users Configuration

Parameter description

• **Delete:** Check to delete the entry. It will be deleted during the next save.

• **User Name:** A string identifying the user name. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

• **Security Level:** Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

Note: The value of the security level cannot be modified if the entry already exists.

• **Authentication Protocol:** Indicates the authentication protocol that this entry should belong to. Possible authentication protocols are:

None: No authentication protocol.

MD5: An optional flag to indicate that this user uses MD5 authentication protocol.

SHA: An optional flag to indicate that this user uses SHA authentication protocol. The value of security level cannot be modified if the entry already exists.

• **Authentication Password:** A string identifying the authentication password phrase. For MD5 authentication protocol, the allowed string length is 8 to 32. For SHA authentication protocol, the allowed string length is 8 to 40 and the allowed content is ASCII characters from 33 to 126.

• **Privacy Protocol:** Indicates the privacy protocol that this entry should belong to. Possible privacy protocols are:

None: No privacy protocol.

DES: An optional flag to indicate that this user uses DES authentication protocol.

Privacy Password: A string identifying the privacy password phrase. The allowed string length is 8 to 32 and the allowed content is ASCII characters from 33 to 126.

• **Buttons:**

Add new user: Click to add a new user.

Save: Click to apply the changes made.

2.6.4 Groups

This function is used to configure SNMPv3 group. The Entry index keys are Security Model and Security Name. To create a new group account, please check <Add new group> button and enter the group information, then check <Save>. Max Group Number : v1: 2, v2: 2, v3:10.

Web Interface

To configure SNMP Groups in the web interface:

1. Click System, SNMP and Groups.
2. Click Add new group
3. Specify the Security model, Security Name and Group Name.
4. Click Save.

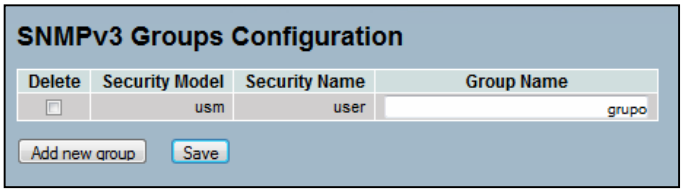


Figure 2-15: The SNMP Groups Configuration

Parameter description

• **Delete:** Check to delete the entry. It will be deleted on next save.

• **Security Model:** Indicates the security model that this entry should belong to. Possible security models are:

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

• **Security Name:** A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

• **Group Name:** A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

• **Buttons:**

Add new group: click to add a new group.

Save: Click to apply the changes made.

2.6.5 Views

This function is used to configure SNMPv3 view. The Entry index keys are OID Subtree and View Name. To create a new view account, please check <Add new view> button and enter the view information, then check <Save>. Max Group Number : 28.

Web Interface

To configure SNMP Views in the web interface:

1. Click System, SNMP and Views.
2. Click Add new View.
3. Specify the SNMP View parameters.
4. Click Save.

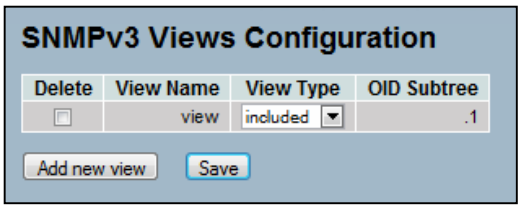


Figure 2-16: The SNMP Views Configuration

Parameter description

- **Delete:** Check to delete the entry. It will be deleted on next save.
- **View Name:** A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.
- **View Type:** Indicates the view type that this entry should belong to. Possible view types are:

included: An optional flag to indicate that this view subtree should be included.
excluded: An optional flag to indicate that this view subtree should be excluded.
In general, if a view entry's view type is 'excluded', there should be another view entry existing with view type as 'included' and its OID subtree should overstep the 'excluded' view entry.

- **OID Subtree:** The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*).
- **Buttons:**

Add new view: Click to add a new view.
Save: Click to apply the changes made.

2.6.6 Access

This function is used to configure SNMPv3 accesses. The Entry index keys are Group Name, Security Model and Security level. To create a new access account, please check <Add new access> button and enter the access information, then check <Save>. Max Group Number: 14

Web Interface

To display the configure SNMP Access in the web interface:

1. Click System, SNMP and Accesses.
2. Click Add new Access.
3. Specify the SNMP Access parameters.
4. Click Save.

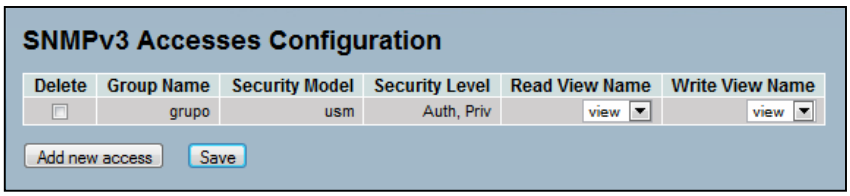


Figure 2-17: The SNMP Accesses Configuration

Parameter description

• **Delete :** Check to delete the entry. It will be deleted on next save.

• **Group Name:** A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is ASCII characters from 33 to 126.

• **Security Model:** Indicates the security model that this entry should belong to. Possible security models are:

any: Any security model accepted(v1|v2c|usm).

v1: Reserved for SNMPv1.

v2c: Reserved for SNMPv2c.

usm: User-based Security Model (USM).

• **Security Level :** Indicates the security model that this entry should belong to. Possible security models are:

NoAuth, NoPriv: No authentication and no privacy.

Auth, NoPriv: Authentication and no privacy.

Auth, Priv: Authentication and privacy.

• **Read View Name:** The name of the MIB view defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

• **Write View Name:** The name of the MIB view defining the MIB objects for which this request may potentially set new values. The allowed string length is 1 to 32 and the allowed content is ASCII characters from 33 to 126.

• **Buttons:**

Add new access: Click to add a new access.

Save: Click to save the changes.

2.6.7 Trap

This function is used to configure SNMP trap. To create a new trap account, please click the <No number> button and enter the trap information then check <Apply>. Max Group Number: 6.

Web Interface

To configure SNMP Trap setting:

1. Click System, SNMP and Trap. The trap Hosts Configuration table will be shown.

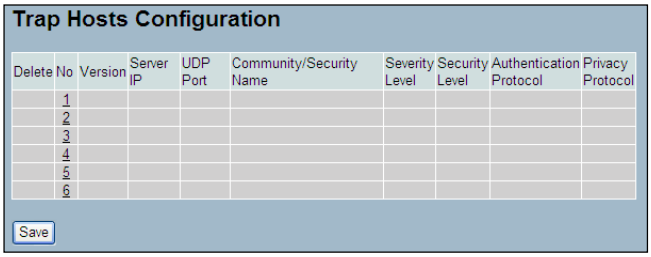


Figure 2-18: Trap Hosts Table

2. Choose an entry to display and modify the detail parameters or click the delete button to delete the trap hosts entry.
3. Specify the Trap Host Configuration Parameters.
4. Click Save.

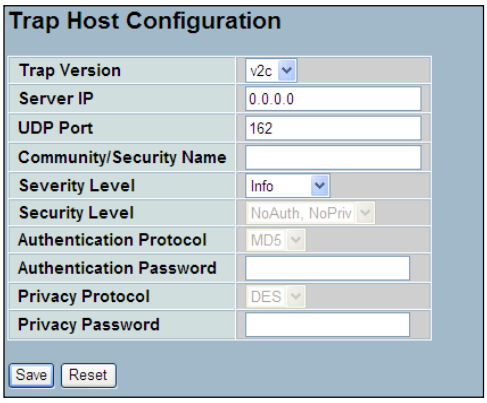


Figure 2-19: The SNMP Trap Host Configuration

Parameters description

- **Delete:** Check <Delete> entry then click the <Save> button, the entry will be deleted.
- **Trap Version:** You may choose v1, v2c or v3 trap.
- **Server IP:** To assign the SNMP Host IP address.
- **UDP Port:** To assign Port number. Default: 162.
- **Community / Security Name:** The length of “Community / Security Name” string is restricted to 1-32.
- **Severity Level:** Indicates what kind of message will be sent according to the Severity Level.
- **Security Level:** There are three kinds of choices.

NoAuth, NoPriv: No authentication and no privacy.
Auth, NoPriv: Authentication and no privacy.
Auth, Priv: Authentication and privacy.

- **Authentication Protocol:** You can choose MD5 or SHA for authentication.
- **Authentication Password:** The length of 'MD5 Authentication Password' is restricted to 8 – 32. The length of 'SHA Authentication Password' is restricted to 8 – 40.
- **Privacy Protocol:** You can set DES encryption for UserName.
- **Privacy Password:** The length of ' Privacy Password ' is restricted to 8 – 32.
- Buttons:

Save: Click to apply the changes made.
Reset: Click to undo any changes made locally and revert to previously saved values.

2.7 Login Protect

This function is used to block the access from an IP address after 3 wrong attempts.

Web Interface:

To configure the Login Protect in the WEB Interface:
1. Click System, Login Protect and Configuration.
2. Specify the Block time interval.
3. Click Save.

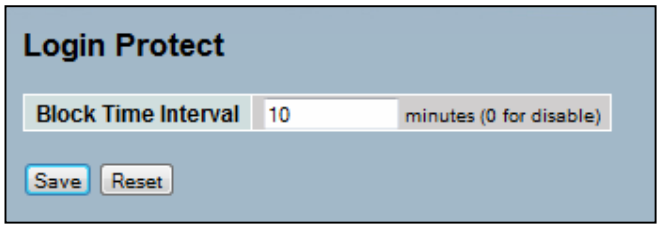


Figure 2-20: The Login Protect Configuration

Parameter description
- **Block time Interval:** determine how long the access will be blocked after 3 wrong login attempts.
- **Buttons:**
  Save: Click to apply changes.
  Reset: Click to undo any changes made locally and revert to previously saved values.

To check the Login Failed List, click System, Login Protect then Login-failed list.

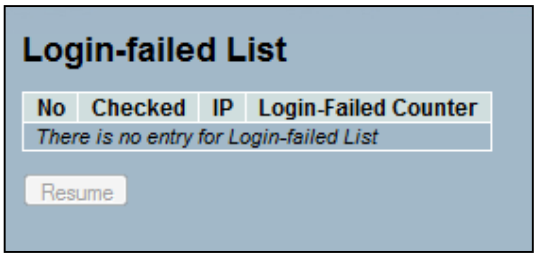


Figure 2-21: The Login-failed List

3 OLT Management

This chapter describes all of the EPON OLT Maintenance configuration tasks to enhance the performance of local network including Port, OLT Statistics, OLT DBA and OLT Operation.

3.1 OLT Management Mode

This function is used to define the in-band management interface. There are three possible configurations:
- Normal: it's possible to manage the interface from both uplink ports (NNI-1 and NNI-2).
- NN1: It's possible to manage the interface only from the NNI-1.
- NNI2: It's possible to manage the interface only from the NNI-2.

The default value is NNI-1.

Note: If both uplink ports are connected to the same switch and are part of the same VLAN group, it's necessary to define only one port as the management interface to avoid loops.

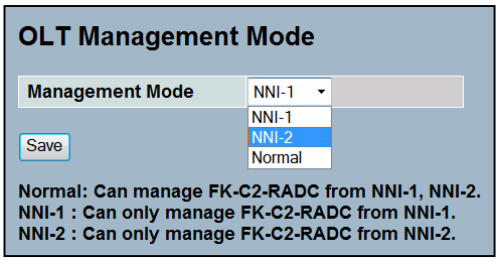


Figure 3-1: The OLT Management Mode configuration

3.2 OLT Provision Wizard

Allows the configuration of the main parameters of the OLT by creating a profile, loading a profile or by using the default parameters.

Web Interface To configure the OLT Provision Wizard in the web interface:

1. Click OLT Management, then OLT Provision Wizard.
2. To use a saved profile or the default settings, specify the chosen option on the field Select, click on the button Load, check the configured parameters and click on Next.

Note: It's possible to edit the parameters from the profile.

3. To set new parameters just make the necessary changes and click on Next.

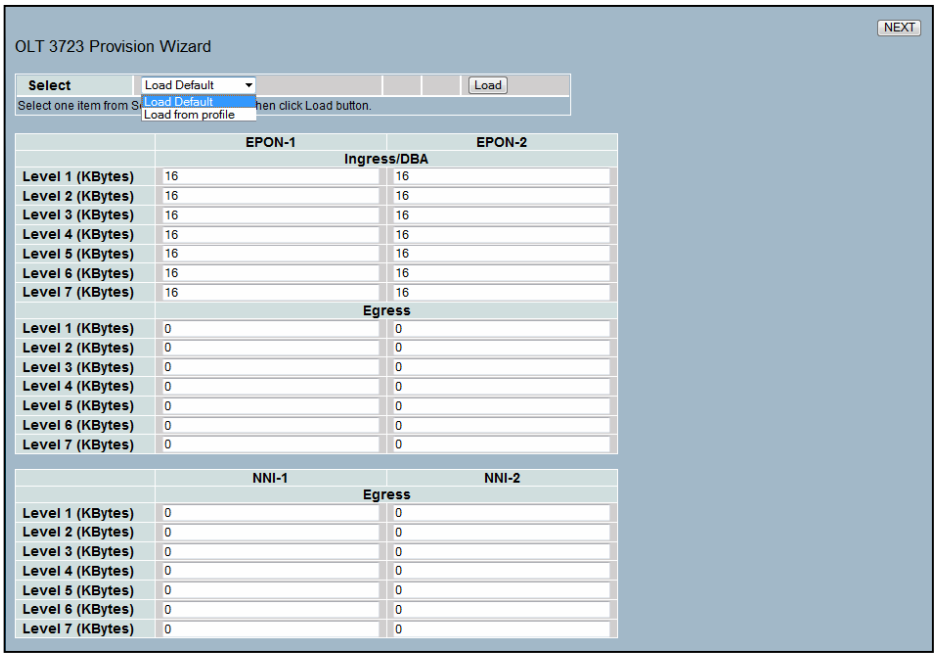


Figure 3-2: OLT Provision Wizard - DBA Drop Down Weights

4. On the next page, the rest of the parameters are shown. Check the values, make the necessary changes and click Next.

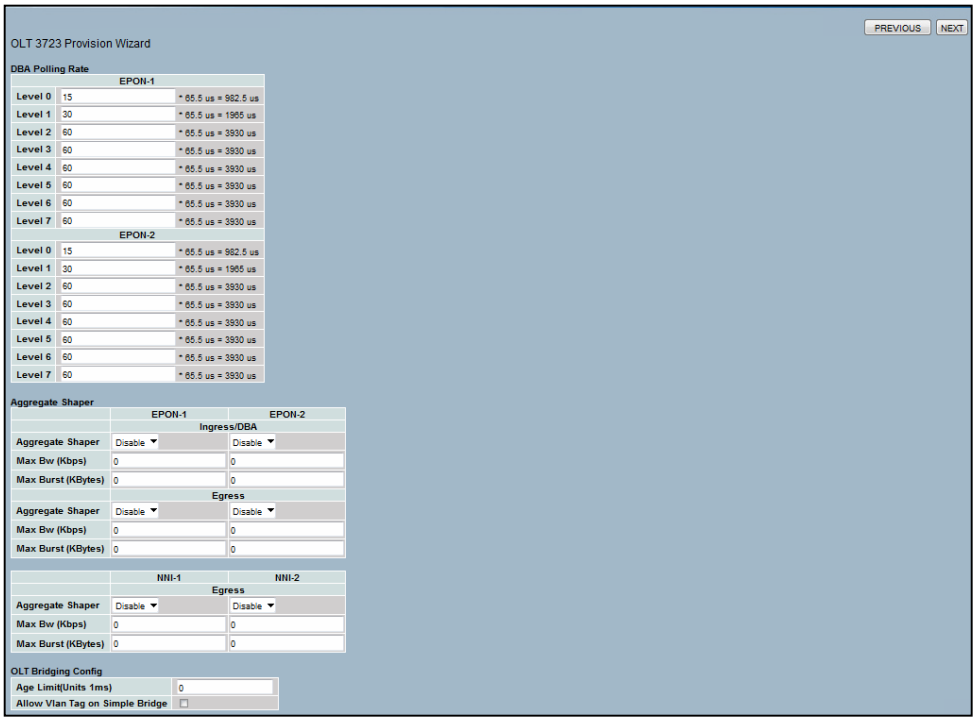


Figure 3-3: OLT Provision Wizard - DBA Pooling rate, Aggregate Shaper and Bridging Config.

5. On the next page, the configured TFTP Server address is shown. If there isn't a server configured, it won't be possible to save and use a profile. To configure the TFTP server address click Maintenance -> TFTP Server.

6. Choose the desired option and click on Finish.

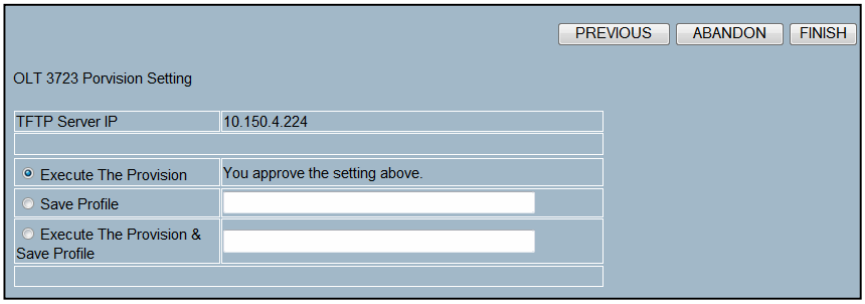


Figure 3-4: Applying the OLT Provision Wizard Configuration

7. A message indicating the status of the operation will appear.

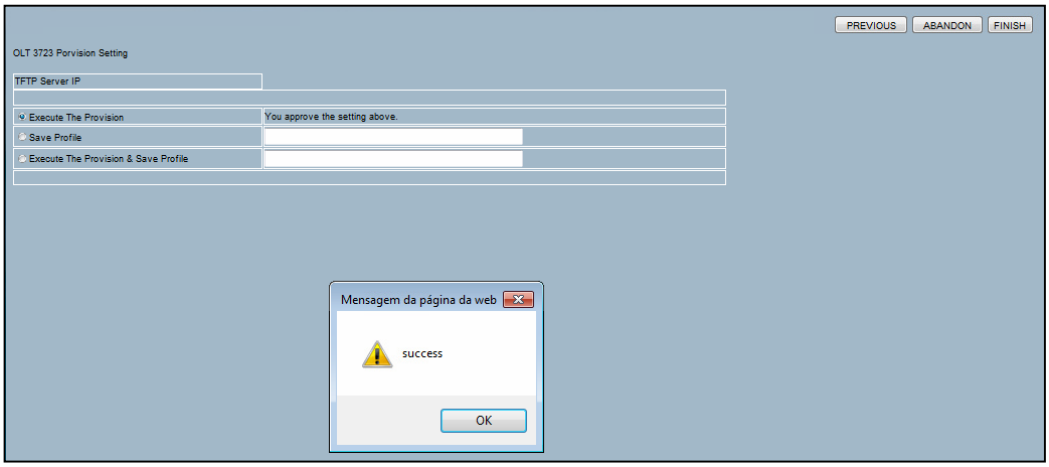


Figure 3-5: Status Message

3.3 Port Config

Configure port settings for both CNI and EPON ports on an OLT. Configuration values will not take effect until <Save> button is clicked.

Web Interface

To configure the OLT Port Configuration in the web interface:

1. Click OLT Management, then Port Configuration.
2. Specify the Auto Nego., Speed and Flow Control.
3. Click Save.

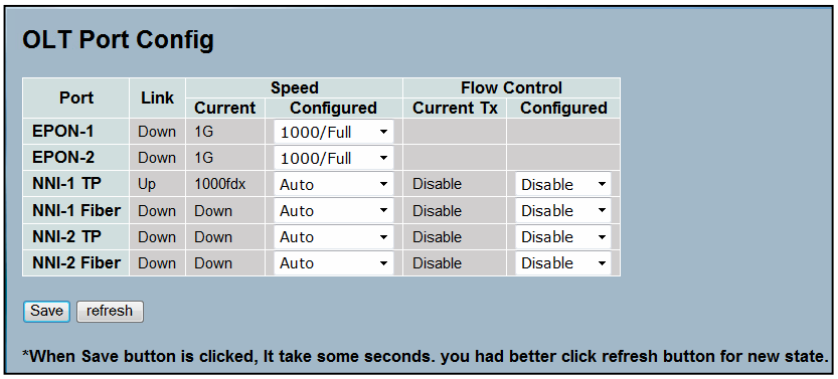


Figure 3-6: The OLT Port Configuration

Parameter description

• **State:** To configure the management status of both CNI (Combo Network Interface) and EPON ports on an OLT. Possible values are [Enable] and [Disable].
Default: [Enable].

• **Auto Nego:** To configure Auto Negotiation state of the CNI ports on an OLT. Possible values are [Enable] and [Disable]
Default: [Enable]

• **Speed/Duplex:** To configure line speed and duplex mode of the CNI ports on an OLT. Possible values are [1000/Full][100/Full and Half][10/Full and Half].
Default: [1000/Full]

• **Flow Control:** To configure flow control state of the CNI port of an OLT. Possible values are [Enable] and [Disable]
Default: [Disable]

• **Button:**
Save: Click to apply changes.

3.4 OLT Port Statistics

Present statistics related to the specified ports, including EPON ports and CNI ports. It supports both flow directions, upstream and downstream. If you click the Refresh button, the statistics information will be displayed. If the Clear button is clicked, the statistics information will be cleared. Upstream direction represents the traffic from EPON port to CNI port. Downstream direction represents the traffic from CNI port to EPON port.

Web Interface

To check the OLT Port Statistics in the web interface:

1. Click OLT Management, then OLT Statistics.
2. Specify the OLT Port. The options are: EPON Port 1, EPON Port 2, NNI Port 1 and NNI Port 2.
3. Specify the traffic direction. The options are:

EPON ports: OLT EPON LIF Transmit, OLT EPON LIF Receive, OLT EPON MAC Transmit and OLT EPON MAC Receive.
NNI ports: OLT NNI Transmit and OLT NNI Receive.

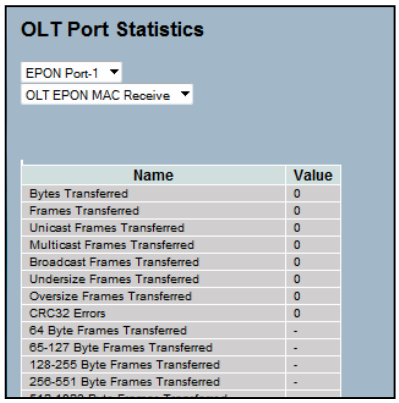


Figure 3-7: The OLT Port Statistics information

Parameter description

- **Auto-refresh:** To refresh the OLT Port Statistics information automatically.
- **Button:**

Refresh: Click to update the statistics information.
Clear: Click to clear the statistics information.

3.5 OLT Information

Web interface

To check the OLT Information in the web interface:

1. Click on OLT Management, then OLT Information.

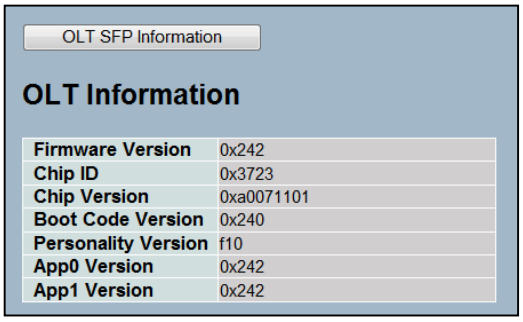


Figure 3-8: The OLT Information

2. To check the information about the SFP, click on the button OLT SFP Information.

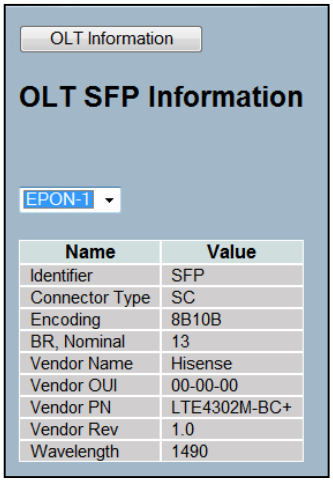


Figure 3-9: The SFP Information

Parameter description

- **Firmware version:** To display the device firmware version.
- **Chip ID:** To display the OLT chip vendor ID and model name.
- **Chip version:** To display the OLT chip version.
- **Boot Code version:** To display the OLT Boot code version.
- **Personality Version:** To display the OLT personality version reserved for specific application.
- **App0 Version:** To display the OLT App0 version.
- **App1 Version:** To display the OLT App1 version.

3.6 OLT Redundant

Web interface

To configure the OLT Redundancy in the web interface:

1. Click OLT Management, OLT Redundant.
2. Select the Enable option.
3. Specify the Master port.
4. Specify the Slave Port.
5. Click Save.

Note: For this function to work the OLT Personality version must be f10.

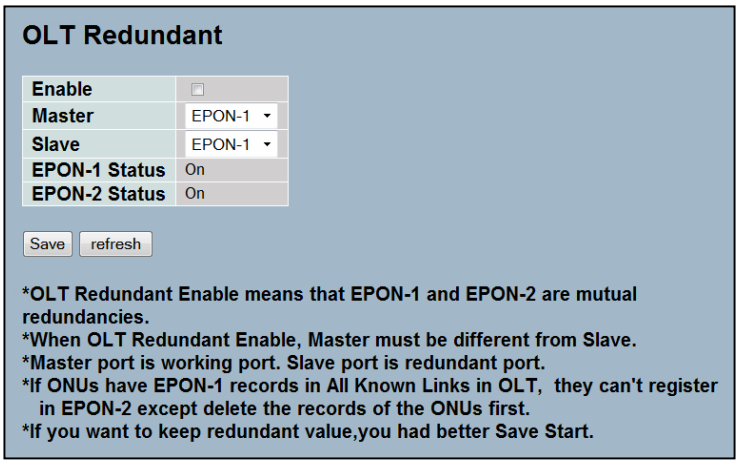


Figure 3-10: OLT Redundancy

3.7 OLT Green PON Config

This section teaches how to enable and monitor the Green PON function.

Web interface

To configure the Green PON in the web interface:

1. Click OLT Management, OLT Green Pon Config and then OLT Green PON.
2. Select the Optical port: EPON Port 1 or EPON Port 2.
3. Enable the Green Pon function.
4. Specify the Green Pon parameters.
5. Click Save.
6. Click Enable All ONUs Green Pon.

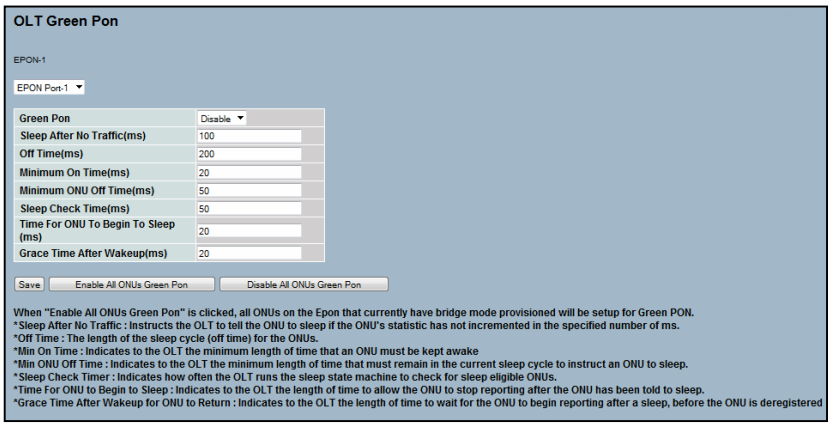


Figure 3-11: The Green PON Configuration

Parameter description:

• **Green Pon:** When configured as "Enable", it enables the green pon functionality for the PON port. To enable this function for the ONUs, it is necessary to click on the button "Enable All ONUs Green Pon".

• **Sleep After No Traffic (ms):** Instructs the OLT to put the ONU in the sleeping state if the ONU's statistics have not incremented in the specified number of ms.

• **Off Time (ms):** The length of the sleep cycle (off time) for the ONUs.

• **Minimum On Time (ms):** Indicates to the OLT the minimum time that an ONU must be kept awake.

• **Minimum ONU Off Time (ms):** Indicates to the OLT the minimum time that the ONU must remain in the current sleep cycle.

• **Sleep Check Time (ms):** Indicates how often the OLT runs the sleep state machine to check for sleep eligible ONUs.

• **Time For ONU To Begin To Sleep (ms):** Indicates to the OLT how much time the ONU will take to stop reporting after the ONU has been told to sleep.

• **Grace Time After Wakeup (ms):** Indicates to the OLT how much time to wait for the ONU to begin reporting after a sleep cycle, before the ONU is deregistered

• **Buttons**

Save: Click to Save changes.

Enable All ONUs Green Pon:

Click on this button to enable all ONUs power saving function.

Disable All ONUs Green Pon:

Click on this button to disable all ONUs power saving function.

The recommended configuration is the one showed below:

Sleep After No Traffic(ms)	100
Off Time(ms)	200
Minimum On Time(ms)	80
Minimum ONU Off Time(ms)	50
Sleep Check Time(ms)	50
Time For Onu To Begin To Sleep(ms)	20
Grace Time After Wakeup(ms)	60

To check the status of the ONUs with the Green Pon function enabled, click OLT Management, OLT Green PON Config and then ONU Power save report.

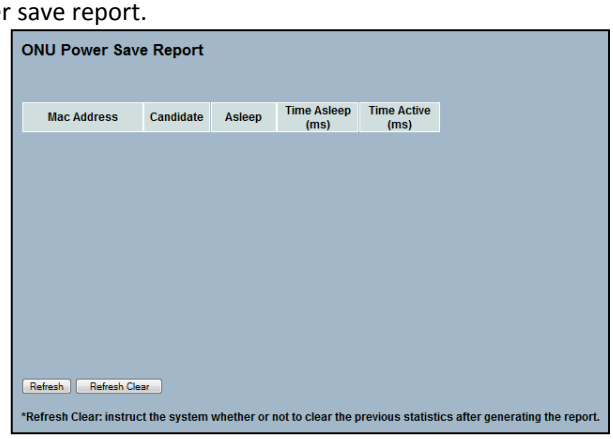


Figure 3-12: The ONU Power Save Report

Parameter description:

- **Mac Address:** Show all CPE site ONU's MAC address
- **Candidate:** Show if the ONU is eligible to sleep or not.
- **Asleep:** Show if the ONU is asleep or not.
- **Time Asleep (ms):** Show the amount of time that the ONU slept.
- **Time Active (ms):** Show the amount of time that the ONU was awake.
- **Buttons**

Refresh: Click to refresh the page.

Refresh Clear: instruct the system whether or not to clear the previous statistics after generating the report.

3.8 Optical Power Monitor Config

Web interface

To configure the Optical Power Monitor in the web interface:

1. Click OLT Management, OLT Optical Power Monitor and then Optical power Monitor Config.
2. Select the EPON port.
3. Change the Hardware Type for SFF-8472 Compliant.
4. Click Save.

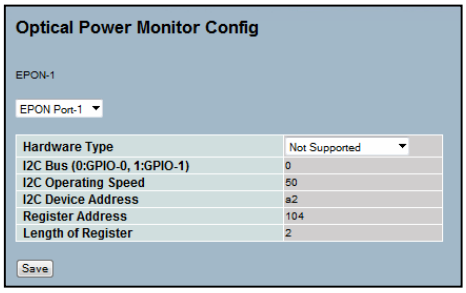


Figure 3-13: The Optical Power Monitor Configuration

Parameter description:

• **Hardware Type:** Must be selected to enable the function.
The option available is SFF-8472 Compliant.

• **Buttons**

Save: Click to Save changes.

5. To define in which links the power will be monitored, click OLT Management, OLT Optical Power Monitor, and then Optical Control.
6. Select the optical port.
7. Define the New Run Mode. Default value On (All Links).
8. Click Save.

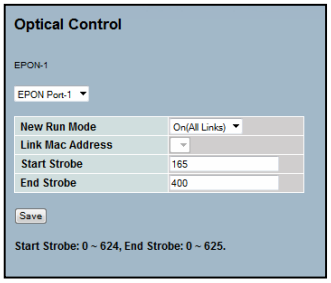


Figure 3-14: The Optical Control Configuration

3.9 OLT Traffic Management

3.9.1 OLT Port Filter Rule

This feature allows the user to filter the traffic based on the traffic direction, upstream (EPON) and downstream (NNI), and the destination output port.

Web interface

To configure the OLT Port Filter Rule in the web interface:

1. Click OLT Management, OLT Traffic Management and then OLT Port Filter Rule.
2. Select the port in which the rule will be applied, the options are EPON-1 and EPON-2 for the upstream direction, and NNI-1 and NNI-2 for the downstream direction.
3. Click on the button Add.

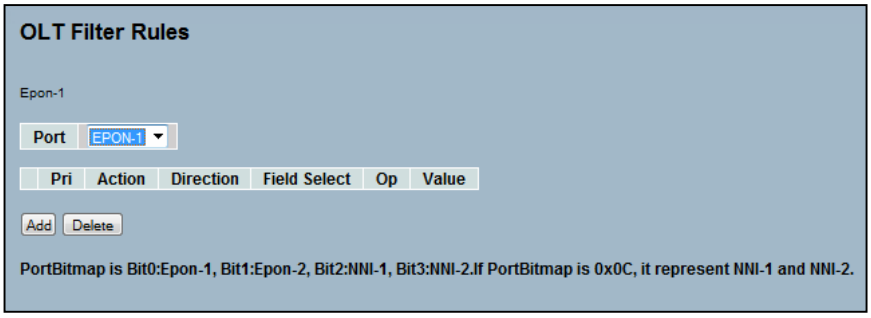


Figure 3-15: OLT Port Filter Rule

4. Define the Action to be taken if the received traffic complies with the rule. The options are: Set discard Flag, which means that the traffic will be discarded, and Clear Discard Flag, which means that the traffic will be forwarded.

Note: The default behavior of the OLT Port Filter rule is that all traffic is forwarded.

5. Define the rule Precedence from 0 to 7.
6. Define the Port Bitmap that represents the output destination of the traffic.

The options are:

Automatic: filter traffic based on the direct channel

Epon1--->NNI1 or Epon2 -----> NNI2

the traffic from the cross channel will not be filtered.

Epon1 -----> NNI2 or Epon2 ----> NNI1

NNI-1: filters traffic designated to the uplink NNI-1 from one of the EPON ports.

NNI-2: filters traffic designated to the uplink NNI-2 from one of the EPON ports.

NNI-1& NNI-2: filters traffic designated to the uplink NNI-1 or to the NNI-2 from one of the EPON ports.

EPON1: filters traffic designated to the EPON 1 from one of the uplink ports.

EPON2: filters traffic designated to the EPON 2 from one of the uplink ports.

EPON1&EPON2: filters traffic designated to the EPON 1 or EPON 2 from one of the uplink ports.

7. Add the desired clause. It's possible to add up to 8 different clauses per rule.
8. Click on the apply button.

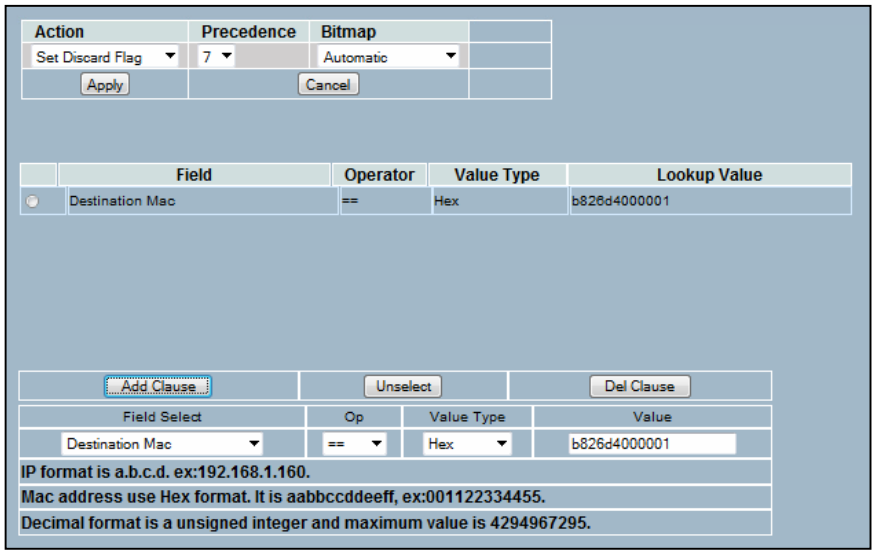


Figure 3-16: OLT Port Filter Rule - Add the Rule clauses

The configured rule will be shown on the main page of the OLT Port Filter rules.
To delete the rule, select it and click on the delete button.

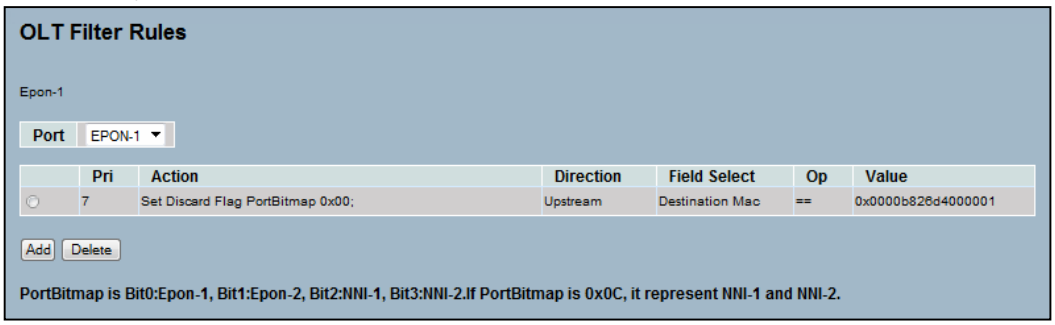


Figure 3-17: OLT Port Filter Rule main page.

3.9.2 OLT Link Filter Rule

This feature allows the user to filter the traffic based on a specific logical link.

Web interface

To configure the OLT Link Filter Rule in the web interface:

1. Click OLT Management, OLT Traffic Management and then OLT Link Filter Rule.
2. Select the link in which the rule will be applied.
3. Click on the button Add.

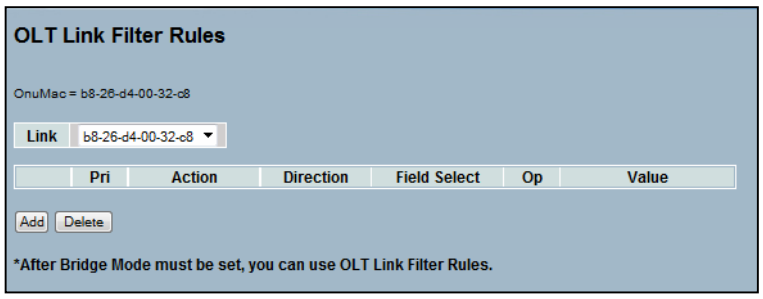


Figure 3-18: OLT Link Filter Rule

4. Define the Action which will be taken if the received traffic complies with the rule. The options are: Set discard Flag, which means that the traffic will be discarded, and Clear Discard Flag, which means that the traffic will be forwarded.

Note: The default behavior of the OLT Link Filter rule is that all traffic is forwarded.

5. Define the rule Precedence from 2 to 5.
6. Add the desired clause. It's possible to add up to 8 different clauses per rule.
7. Click on the apply button.

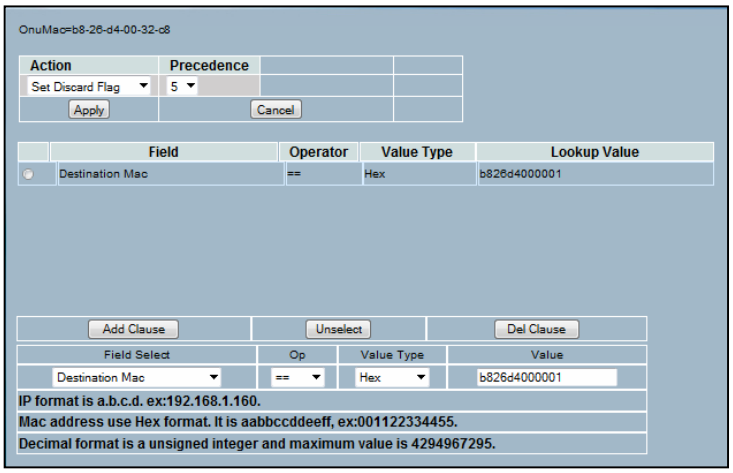


Figure 3-19: OLT Link Filter Rule - Add the Rule clauses

The configured rule will be shown on the main page of the OLT Link Filter rules.

To delete the rule, select it and click on the delete button.

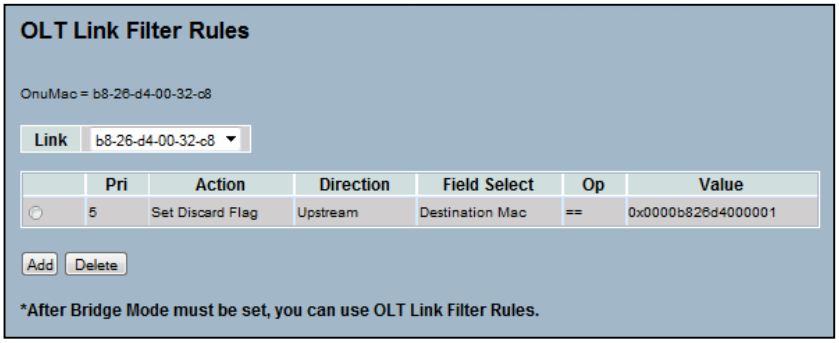


Figure 3-20: OLT Link Filter Rule main page

3.10 OLT Bridging Config

This section teaches you how to configure OLT advance Bridge function for OLT application.

Web Interface

To configure a General Setting in the web interface:

1. Click OLT Management, then OLT Bridging Config.
2. Set the parameters.
3. Click Save.

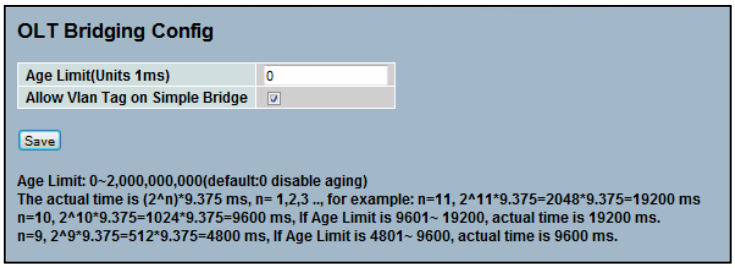


Figure 3-21: The OLT Adv. Bridging information

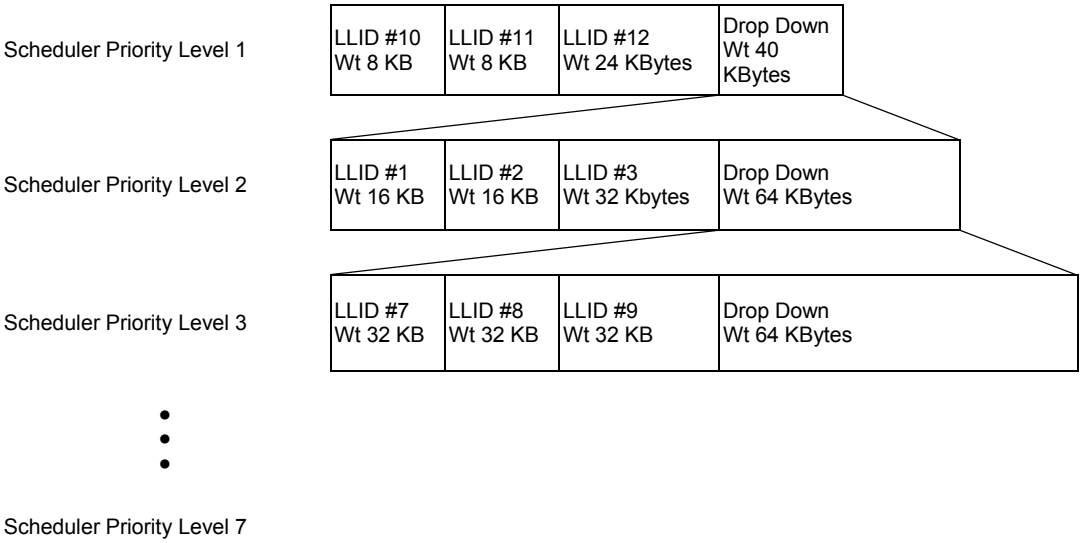
Parameter description

- **Age Limit:** defines how long a MAC address is going to be kept on the MAC Dynamic Table.
- **Allow Vlan Tag on Simple Bridge:** tagged packets are forwarded on simple bridge.

3.11 OLT DBA

Drop Down Weight, Broadcast SLA, Aggregate Shaper, and Polling Rate determine the operation of Dynamic Bandwidth Allocation (DBA). The DBA uses a Weighted Hierarchical Round Robin scheduler (WHRR). It allows the network operator to provision Service Level Agreements (SLAs) per Logical Link ID (LLID). Each SLA has four parameters: Minimum Guaranteed Bandwidth (Min Bw), Maximum Allowable Bandwidth (Max Bw), Burst Size and Delay Tolerance. The system implements the Aggregate Shaper, which ensures that the Maximum Allowable Bandwidth and Burst Size do not exceed what was determined on the SLA.
The DBA uses queue length status received from ONU Report messages, along with the SLA parameters, to calculate bandwidth allocation. There are up to 8 levels of hierarchy support. Each LLID can be mapped to a priority level and which is used by Round Robin Scheduling. The priority level of the LLID is determined by its SLA. The are 8 levels as shown below.

The DBA Scheduler depends on Drop Down weight to give next level total size.
For example:
LLIDs of Level 1: 10 ~ 12 < token size: 8K&24K / Drop Down Weight: 40K >
LLIDs of Level 2: 1 ~ 3 < token size: 16K&32K / Drop Down Weight: 64K >
LLIDs of Level 3: 7 ~ 9 < token size: 32K / Drop Down Weight: 64K >
The below diagram illustrates the DBA Scheduler.



3.11.1 DBA Aggregate Shaper

This functionality can control the overall bandwidth for user traffic on upstream and downstream. When this parameter is set to 0, it means that the Aggregate Shaper is disabled. This command is disabled by default. If the Maximum Allowed Bandwidth or Max Burst is 0, this function is disabled.
This functionality lets the Host restrict the bandwidth available to the OLT for user data traffic in both directions. This feature can be used to protect the core network from burst upstream flows and increase the accuracy of SLA enforcement. Aggregate bandwidth control can be disabled by setting the parameters to zero. This feature is disabled by default.

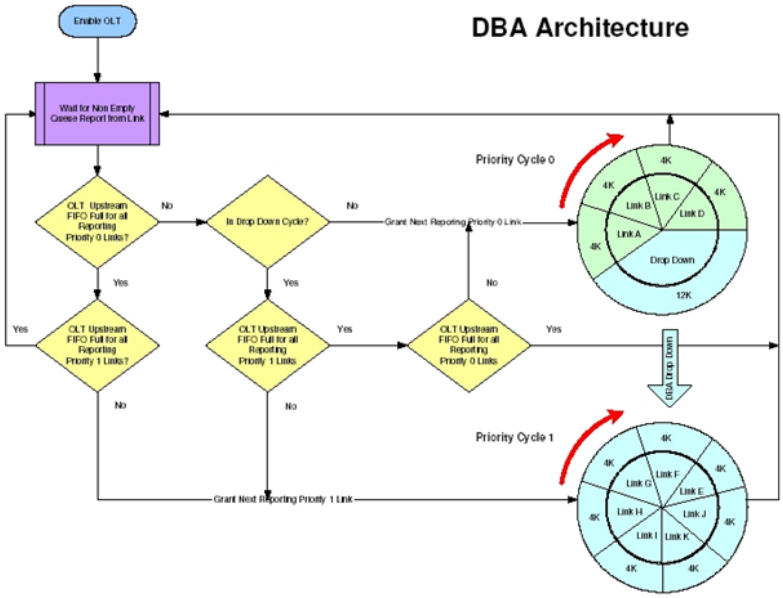


Figure 3-22: DBA Architecture

Web Interface

To configure a DBA Aggregate Shaper in the web interface:

1. Click OLT Management, OLT DBA and then DBA Aggregate Shaper.
2. Specify the detail Aggregate Shaper, Max Bw, Max Burst.
3. Click Save.

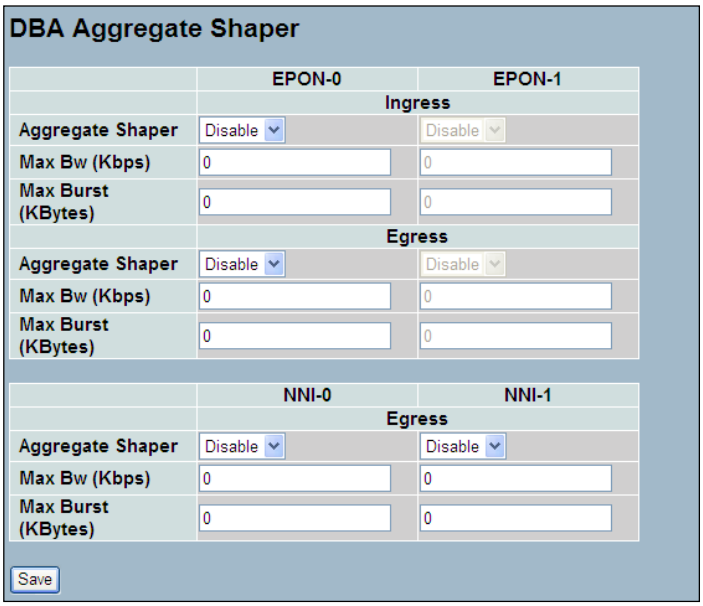


Figure 3-23: The OLT DBA Aggregate Shaper Configuration

Parameter description

- **Maximum Allowed Bandwidth (Max Bw)**

Range: 256~1000000
Default: 0

- **Max Burst**

Range: 1~256
Default: 0

- **Button:**

Save: Click to apply the changes.

3.11.2 DBA Drop Down Weights

This command configures the drop-down weights for the DBA priority levels. DBA for each EPON port operates independently. The DBA drop-downs are configured only in the upstream direction.
A zero value indicates strict priority. However, strict priority is not recommended at the OLT. Stopping all traffic from an LLID will cause the ONU to timeout and deregister. Bandwidth must be guaranteed to lower priorities by using a drop down or by limiting bandwidth.

Web Interface

To configure the DBA Drop Down Weights in the web interface:

1. Click OLT Management, OLT DBA and then DBA Drop Down Weights.

2. Specify the detail Level 1-7.

3. Click Save.

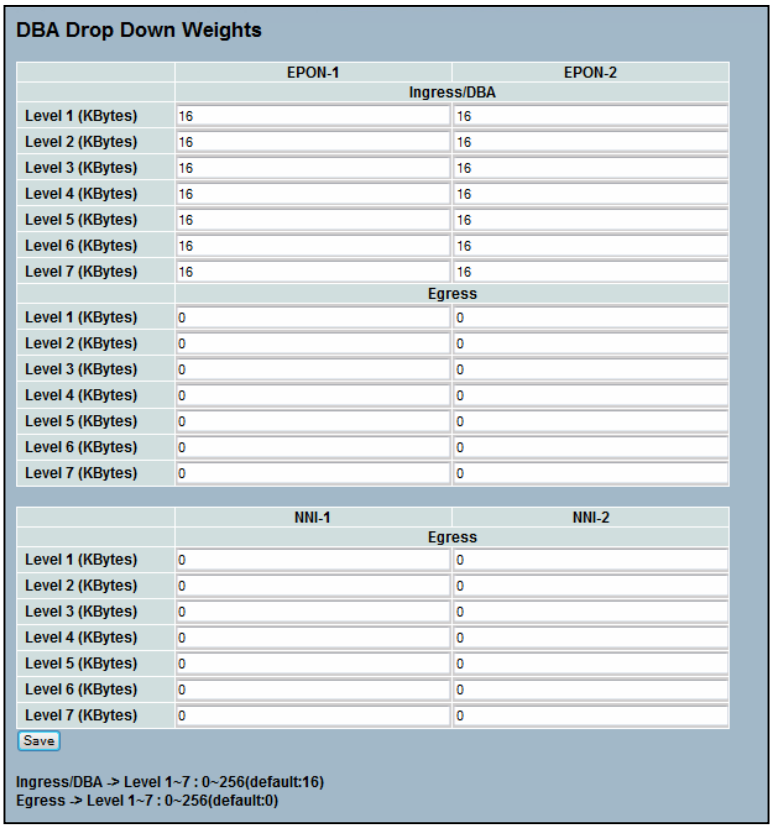


Figure 3-24: The OLT DBA Drop Down Weights Configuration

Parameter description

- **Ingress/DBA (LeveL1-7)**

Range: 0~256(Kbytes)

Default: 16

- **Egress:**

Range: 0~256

Default: 0

- **Button:** Save: Click to save the changes.

3.11.3 DBA Polling Rate

This functionality can set DBA Polling rates for the eight levels. Registered links in Active scheduler levels must be provisioned with a non-zero polling rate. If the parameter is set as zero, it means the scheduler level is disabled. This parameter can be set in multiples of 65.5 μsec.
The polling rate panel allows the operator to configure the rate at which each link will be asked to determine if it has any data to transmit. Smaller values result in lower latency and increased overhead. For priority 0, the scheduling latency is approximately equal to the larger of the polling rate and the cycle length.

Web Interface

To configure the DBA Polling Rate in the web interface:

1. Click OLT Management, OLT DBA and then DBA Polling Rate
2. Specify the detail Level 0-7
3. Click Save.

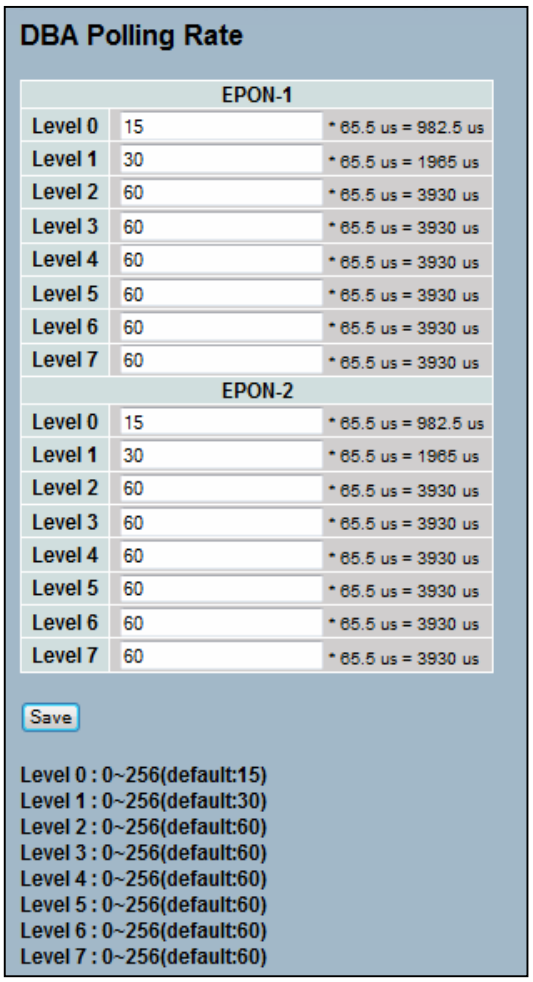


Figure 3-25: The OLT DBA Polling Rate Configuration

Parameter description

- **Level 0 - 7**

Range: 0~256

Default: 15

- **Button:**

Save: Click to save the changes.

3.11.4 Broadcast SLA

This session is identical to the functionality of the Link SLA Panel except that it is used to provision a SLA for the broadcast channel, as opposed to an unicast link. This unique feature of the OLT allows the OLT to use its large 64M buffer ram to serve the requirements of all ONUs.

Web Interface

To configure a Broadcast SLA in the web interface:

1. Click OLT Management, OLT DBA and then Broadcast SLA.
2. Set the parameters.
3. Click Save.

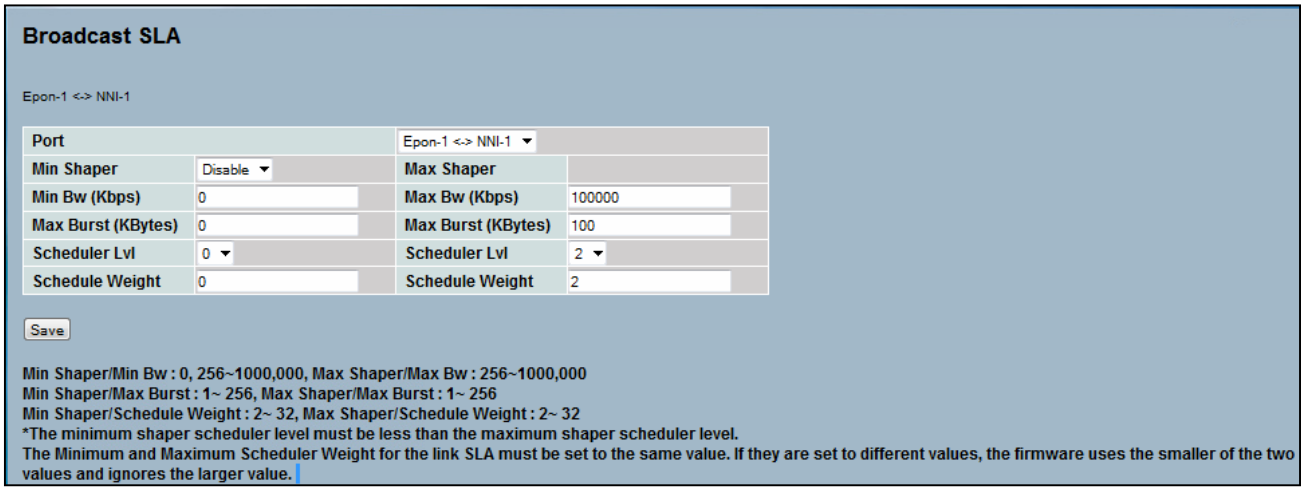


Figure 3-26: Broadcast SLA Configuration

Parameter description

Min Shaper/

- **Min Bw :**

Range:0, 256~1000,000,

- **Max Burst :**

Range:1~ 256

- **Schedule Weight :**

Range:2~ 32

Max Shaper/

- **Max Bw :**

Range:256~1000,000

- **Max Burst :**

Range:1~ 256

- **Schedule Weight :**

Range:2~ 32

3.12 OLT IGMP Proxy

3.12.1 IGMP Proxy

Web interface

To configure IGMP Proxy in the web interface:

1. Click OLT Management, OLT IGMP Proxy and then OLT IGMP Proxy
2. Set the parameters.
3. Click Save.

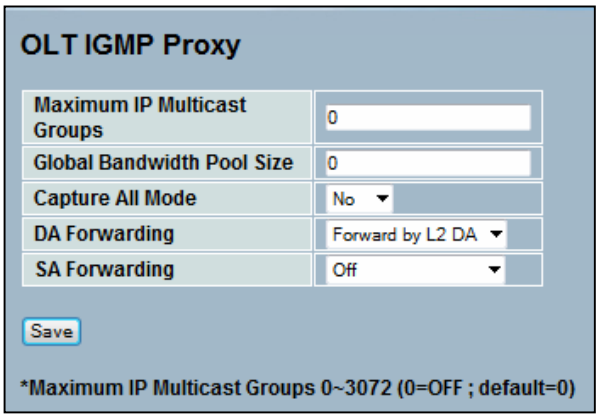


Figure 3-27: The OLT IGMP Proxy

Parameter description:

• **Maximum IP Multcast Groups:** This parameter means how many IGMP Groups can be supported. If this parameter is 0, the IGMP Proxy is disabled. When IGMP is disabled, all IP Multicast Frames are forwarded by the OLT. If the current number of groups is equal to the maximum IGMP Groups, no new groups will be added or forwarded by the OLT, and joins for new groups will be discarded.

Range: 0~3072 (0=OFF; default=0)

• **Global Bandwidth Pool Size:** This value applies to all Proxy Domain instances in the OLT. When it is set to zero, no groups can be joined on any proxy domain due to insufficient available bandwidth.

Range 0~2000000

• **Capture All Mode:** This bit applies to all Proxy Domains in the OLT. When it is set as Yes, the OLT Proxy software captures all IGMP protocol frames in both directions. When this bit is set as No, the OLT Proxy software only captures IGMP/MLD protocol frames that links to a provisioned proxy domain.

• **DA Forwarding /SA Forwarding:** Depending on the forwarding option and the group addresses in use, the maximum number of groups can be one fewer (4095). If groups are only forwarded by L2 DA, then the limit is always 4096. Other forwarding options can hit the 4095 limit instead.

Buttons

• **Save:** Click to Save changes.

3.12.2 OLT IGMP Parameters

Web interface

To configure IGMP Proxy Parameters in the web interface:

1. Click OLT Management, OLT IGMP Proxy and then OLT IGMP Param.
2. Set the parameters.
3. Click Save.

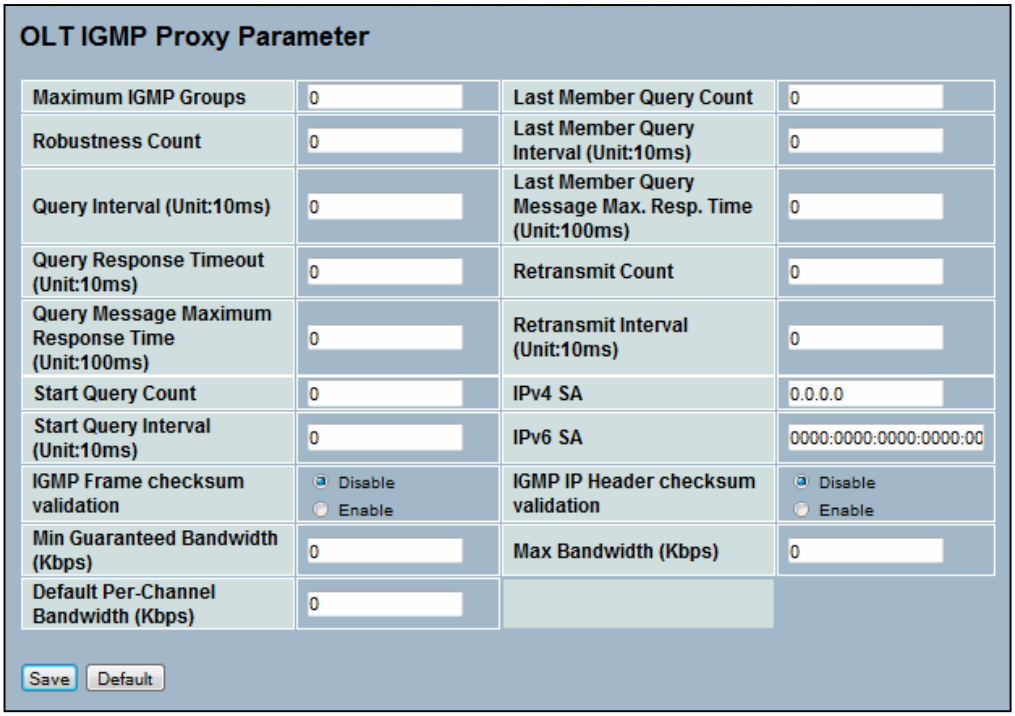


Figure 3-28: The OLT IGMP Proxy Parameters

Parameter description:

• **Maximum IGMP Groups:** This parameter determines how many IGMP Groups can be supported. If this parameter is 0, the IGMP Proxy is disabled. When IGMP is disabled, all IP Multicast Frames are forwarded by the OLT. If the current number of groups is equal to the maximum IGMP Groups, no new groups will be added or forwarded by the OLT, and joins for new groups will be discarded.

Range: 0~3072 (0=OFF; default=0)

• **Robustness Count:** This parameter represents the number of IGMP General Queries. The Robustness Count may pass with no corresponding IGMP Report reply before a Group is removed.

Range: 1~16 (default=2)

• **Query Interval :** This parameter is a time interval

Range: 1~65535 (Unit: 10ms; default=12500)

• **Query Response Timeout:** This parameter is the time that the OLT waits for IGMP Reports after sending a General IGMP Query. If the timer expires and the Group does not receive any report, then the Robustness counter is decremented.

Range: 1~2600 (Unit: 10ms; default=1001)

• **Query Message Maximum Response Time:** This parameter is the actual value set in the Maximum Response Time field of IGMP General Query messages sent downstream by the OLT. The Query Message Maximum Response Time must be lower than the Query Response Timeout.

Range: 1~255 (Unit: 100ms; default=100)

• **Start Query Count:** If IGMP is enabled or reset, the OLT uses Startup Queries initially. The Group memberships are quickly established after initialization.

Range: 0~16 (default=2)

• **Start Query Interval:** This interval must be lower than the regular IGMP General Query Interval.

Range: 1~65535 (Unit: 10ms; default=3125)

• **Last Member Query Count:** This parameter is the number of IGMP Group Specific Queries sent when an IGMP Leave message is received for a specific Group. If this count is 0 and Last Member Query Interval expires, the multicast group is removed and the multicast traffic forwarding for the group is stopped.

Range: 1~16 (default=2)

• **Last Member Query Interval:** This parameter is an interval, which IGMP Group Specific Queries are sent. The Last Member Query Interval must be higher than the Last Member Query Maximum Response Time.

Range: 1~2600 (Unit: 10ms; default=110)

• **Last Member Query Message Max. Resp. Time:** The Last Member Query Message Maximum Response time is set in the Maximum Response Time field of IGMP Group Specific Query messages sent downstream. This value must be lower than the Last Member Query Interval.

Range: 1~255 (Unit: 100ms; default=10)

• **Retransmit Count**
Range: 0~3 (default=0)

• **Retransmit Interval:** This is an interval, which represents the interval at which IGMP Reports (Joins) are retransmitted upstream.

Range: 1~2500 (Unit: 10ms; default=10)

• **IGMP Frame checksum validation:** This parameter can set IGMP Frame checksum validation. It has two modes, Enable and Disable.

(default=Disable)

• **IGMP IP Header checksum validation:** This parameter can set IGMP IP Header checksum validation. It has two modes, Enable and Disable.
(default=Disable)
• **Min Guaranteed Bandwidth(Kbps)**
Range**:** 0~2000000
• **Max Bandwidth(Kbps)**
Range: 0~2000000
• **Default Per-Channel Bandwidth(Kbps)**
Range: 0~1000000
• **Buttons**
Save: Click to Save changes.
Default: Click to restore the default configuration.

3.12.3 Group

Web interface

To check the IGMP Groups Joined in the web interface:

1. Click OLT Management, OLT IGMP Proxy and then OLT IGMP Group.
2. Click Refresh.

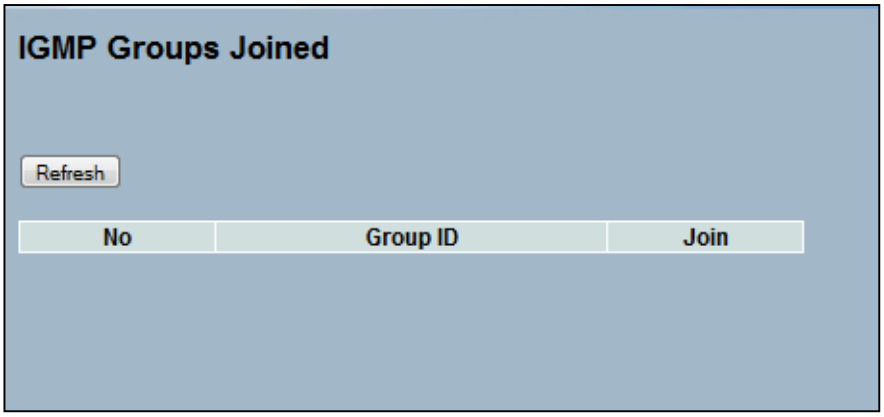


Figure 3-29: The OLT IGMP Groups Joined

3.13 Network Parameters

3.13.1 OAM Parameters

Web Interface

To configure the OAM Parameters in the web interface:

1. Click OLT Management, Network Parameters and then OAM Parameters.
2. Specify the detail Max OAM Rate, Min OAM Rate and LoopBack Timeout.
3. Click Save.

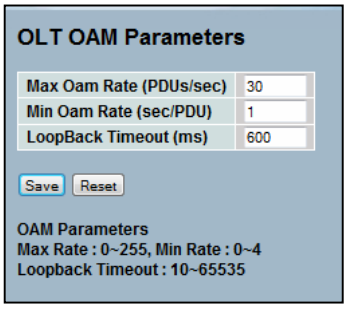


Figure 3-30: The OLT OAM Parameters Configuration

Parameter description

• **Max OAM Rate:** Total OAM PDU transmission per second per logical link is limited to the Max OAM Rate specified. A value of zero disables the limit and allows an unlimited number of OAM frames on a logical link.
Default: 30 (PDUs/sec)

• **Min Rate:** One OAM Information PDU is generated at Min OAM Rate, if no other OAM PDU is transmitted for the defined time. OAM link failure occurs when five minimum OAM intervals have passed with no OAM message received.
Default: 1 sec

• **Loopback Timeout:** The loopback timeout value. A port or a logical link on an ONU which is set to get into loopback mode will remain in this state until receiving the OAM “Loopback Disable” command, or until this timer expires.
Default: 600

• **Buttons**

Save: Click to Save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

3.13.2 VLAN Parameters

Web Interface

To configure the VLAN Parameters in the web interface:

1. Click OLT Management, Network Parameters and then VLAN Parameters.
2. Specify the detail VLAN Ether Type, Tag UP, Tag Down.
3. Click Save.

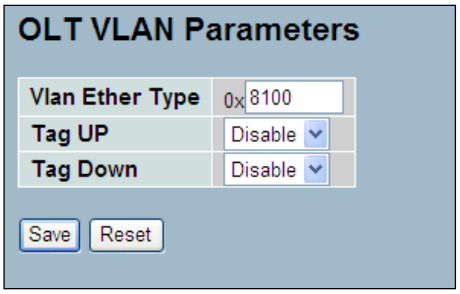


Figure 3-31: The OLT VLAN Parameters Configuration

Parameter description

• **Vlan Ether Type:** The firmware of the OLT uses the default Ether Type of 0x8100 to identify frames with VLAN tags. For the interoperability in some special application using VLAN, an additional Ether Type to identify VLAN frames may be defined here.

• **Tag UP :** Use the VLAN Ether Type Specified above to tag upstream

Default: [Disable]

• **Tag Down:** Use the VLAN Ether Type Specified above to tag downstream

Default: [Disable]

• **Buttons**

Save: Click to Save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

3.13.3 MPCP Parameters

Multi Point Control Protocol (MPCP) is used to arbitrate the channel between the ONU's so that no collisions will occur on the common fiber.

Web Interface

To configure the MPCP Parameters in the web interface:

1. Click OLT Management, Network Parameters and then MPCP Parameters.
2. Specify the detail Discovery Period, Discovery Window.
3. Click Save.

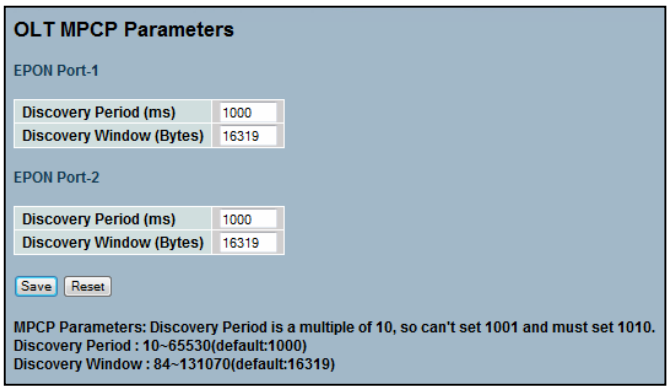


Figure 3-32: The OLT MPCP Parameters Configuration

Parameter description

• **Discovery Period (ms):** The period of time for the OLT to generate a discovery gate.
Default: 1000 (=1 Second)

• **Discovery Window (Bytes):** The size in bytes of the MPCP discovery window in a EPON system
Default: 16319

• **Buttons**

Save: Click to Save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

3.13.4 Loop Timing

Web Interface

To configure the Loop Timing in the web interface:

1. Click OLT Management, Network Parameters and then Loop Timing.
2. Specify the parameters.
3. Click Save.

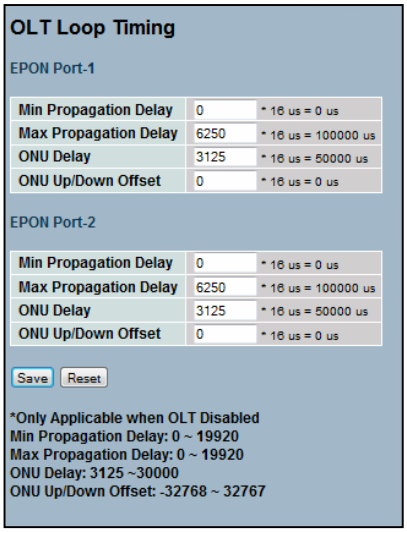


Figure 3-33: OLT Loop Timing Configuration

Parameter description

• **Min Propagation Delay:** the minimum delay generated by the transmission on the fiber.
Default: 0 - means there's 0 km of fiber.

• **Max Propagation Delay:** the maximum delay generated by the transmission on the fiber.
Default: 6250 - means there's 20 km of fiber between the OLT and the ONU.

• **ONU Delay:** the period that the ONU takes to process the data sent by the OLT and respond.

• **Buttons**

Save: Click to Save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

3.14 OLT Dynamic Table

Web interface

To check the OLT Dynamic Table in the web interface:

1. Click on OLT Management and then on OLT Dynamic Table.

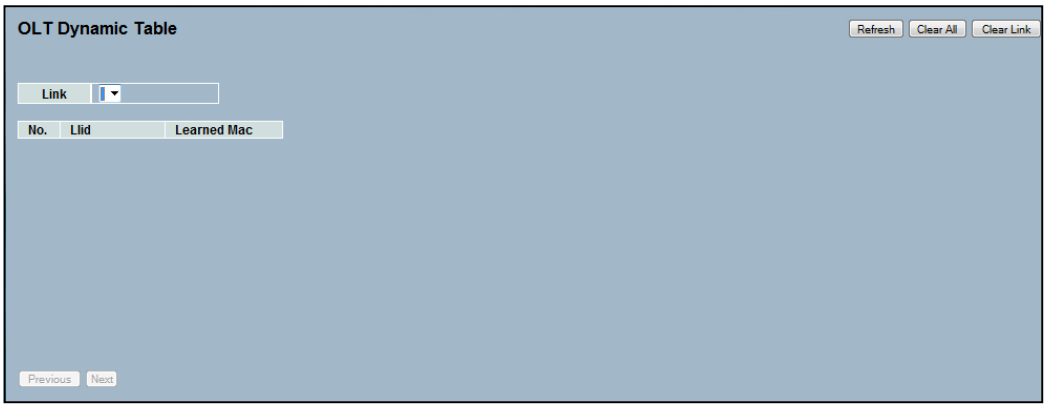


Figure 3-34: OLT Dynamic Table

Parameter description:

- **Link :** box to choose the llid address
- **Llid :** logical link address.
- **Learned Mac:** show the MAC addresses learned by the selected llid.
- **Buttons**

Previous: Go to the previous page.
Next: Go to the next page.
Refresh: Update the page
Clear All: Clear the entries for all the logical links.
Clear Link: Clear the entries for the selected logical link.

3.15 OLT Operation

3.15.1 Enable OLT

This section describes how to Enable the EPON configuration on the OLT.

Web Interface

To configure the Enable OLT function in the web interface:

1. Click OLT Management, OLT Operation and then Enable OLT.
2. Click Yes.

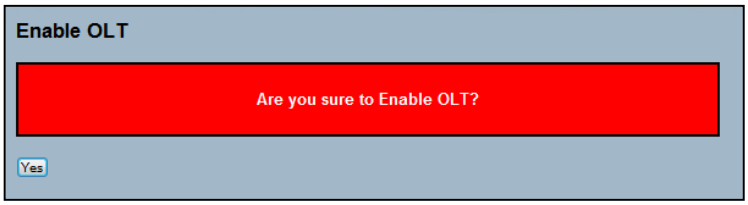


Figure 3-35: The Enable OLT Screen

3.15.2 Disable OLT

This section describes how to Disable the EPON configuration on the OLT.

Web Interface

To configure the Disable OLT function in the web interface:

1. Click OLT Management, OLT Operation and then Disable OLT.
2. Click Yes.

Figure 3-36: The Disable OLT Screen

3.15.3 Export OLT Config

This section describes how to export the OLT configuration.

Web Interface

To export the OLT configuration in the web interface:

1. Click OLT Management, OLT Operation and then Export OLT Config.
2. Click Save configuration.
3. Choose where to save the file.

Figure 3-37: OLT Configuration Export

3.15.4 Import OLT Config

This section describes how to import the OLT configuration.

Web Interface

To import the OLT configuration in the web interface:

1. Click OLT Management, OLT Operation and then Import OLT Config.
2. Select the configuration file.
3. Click Import.

Figure 3-38: OLT Configuration Import

3.16 Block Link List

This section describes how to check the Block link list.

Web Interface

To check the Block Link List in the web interface:

1. Click OLT Management then Block Link List

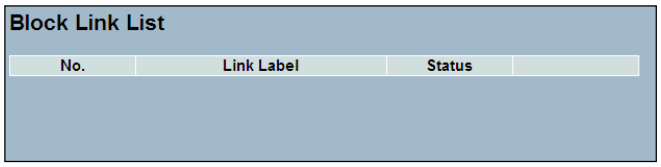


Figure 3-39: The Block Link List illustration

Parameter description

- **No.:** The OLT block Link list index.
- **Link Label:** indicate the MAC address of the logical link.
- **Status:** indicate the status of the link.
- **Buttons**

Unblock: click to unblock the link.

3.17 All Known Link Provision

3.17.1 In OLT

Web interface

To check all the links in the OLT in the web interface:

1. Click OLT Management, All Known Link Prov. and then In OLT.

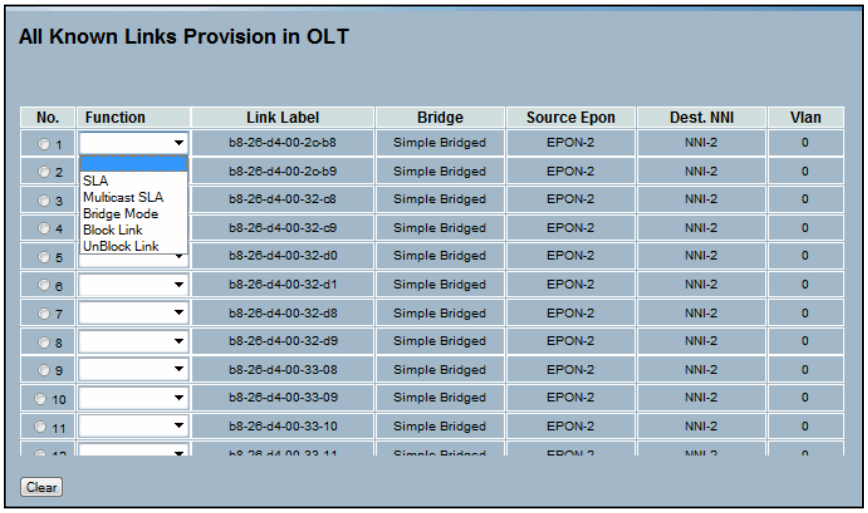


Figure 3-40: All Known Links Provision in OLT

Parameter description:

• **Function:** allow the user to configure the logical link from this menu. The following options are available:
SLA
Multicast SLA
Bridge Mode
Block Link
Unblock Link

• **Link Label:** show the logical link MAC address.

• **Bridge :** show the bridge mode configured for the llid.

• **Source Epon:** show the PON port the link belongs.

• **Dest. NNI:** show the destination uplink port the llid will use.

• **Vlan:** show the VLAN ID.

• **Buttons**

Clear: Click to delete the selected links.

3.17.2 In Host Memory

Web interface

To check the In host Memory in the web interface:

1. Click OLT Management All Known Link Provision and then In Host Memory.

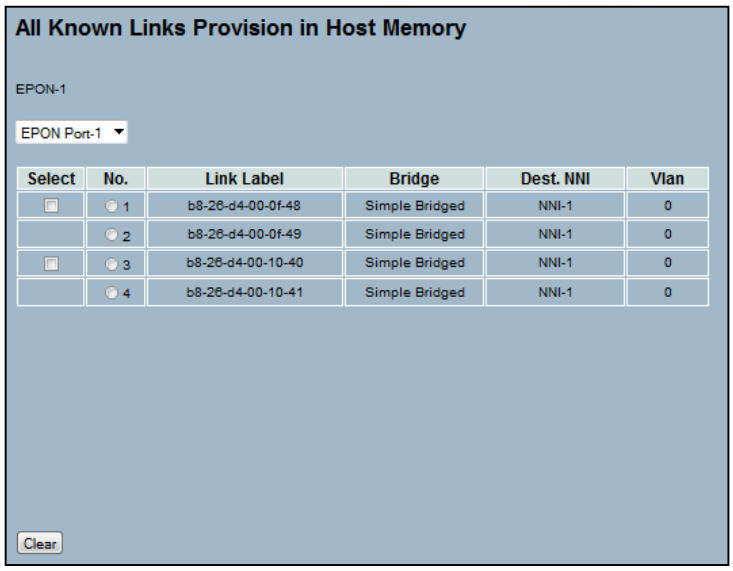


Figure 3-41: All Known Links Provision in Host Memory

The OLT Bridge mode setting is dynamic. When the OLT reboots, the All Known Links Provision list in OLT will be set as the Host setting.

Double click Select title field will select all entries. Click Select title field to unselect all entries.

Parameter description:

- **Link Label:** show the logical link MAC address.
- **Bridge:** show the bridge mode configured for the llid.
- **Dest. NNI:** show the destination uplink port the llid will use.
- **Vlan:** show the VLAN ID.
- **Buttons**

Clear: delete the selected links.

3.17.3 Switch ONU

Web interface

To Switch an ONU from EPON port in the web interface:

1. Click OLT Management, All Known Link Provision and then Switch ONU.

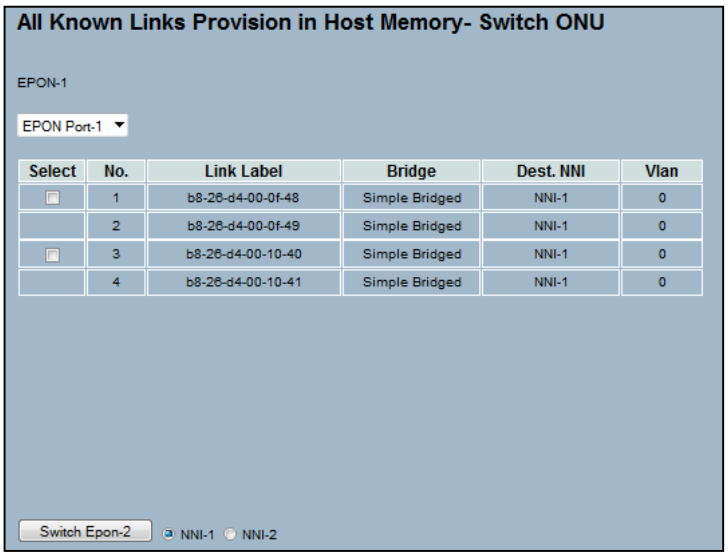


Figure 3-42: Switch ONU

Parameter description:

- **Link Label:** show the logical link MAC address.
- **Bridge:** show the bridge mode configured for the llid.
- **Dest. NNI:** show the destination uplink port the llid will use.
- **Button:**

Switch Epon-2: the selected ONU connected to the EPON 1 will be changed to the EPON 2. It's possible to change the Dest. NNI port or keep the same.

4 ONU Management

This chapter describes all of the EPON ONU Maintenance configuration tasks to enhance the performance of local network including ONU List, ONU Authorization.

4.1 ONU List

Web Interface

To check the ONU List in the web interface:

1. Click ONU Management.
2. Click ONU List EPON-1 or ONU List EPON-2.

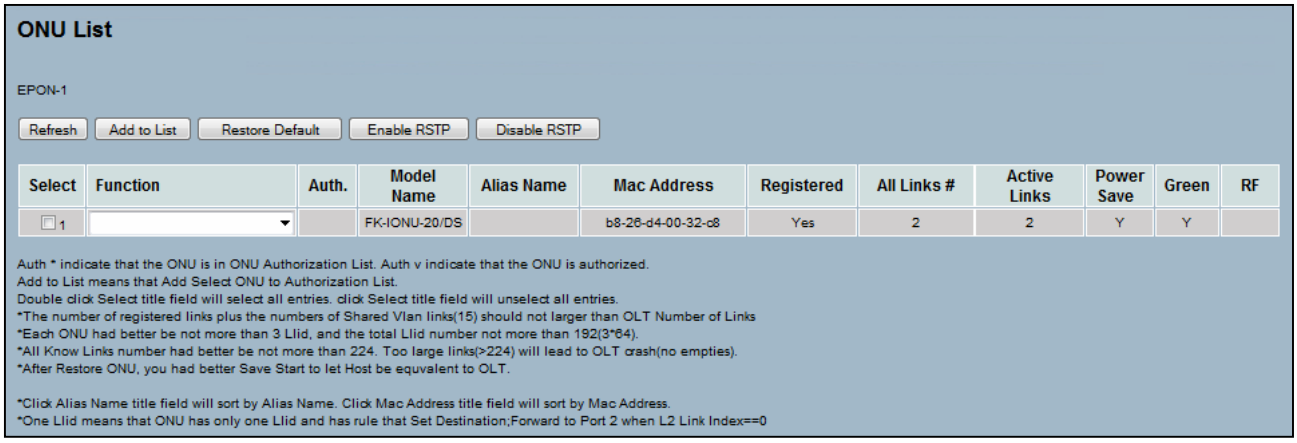


Figure 4-1: The ONU Management

Parameter description

- **Refresh:** Click the “Refresh” icon to clear or update the ONU connect table.
- **Add to List:** Click to add the selected ONUs to the Authorization List.
- **Restore Default:** Click to Restore to default the selected ONUs.
- **Enable RSTP:** Click to enable the passing of RSTP packets for the selected ONUs.
- **Disable RSTP:** Click to disable the passing of RSTP packets for the selected ONUs.
- **Select:** Click to select ONUs to Add to list, Restore or to enable the RSTP packets.
- **Function:** Shows the configuration menus available for the ONUs.

4.1.1 Alias Name

Web interface

To configure the Alias name in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Alias Name on the function combo box.

Note: This configuration is necessary for the ONU to appear on the Subscriber view list.

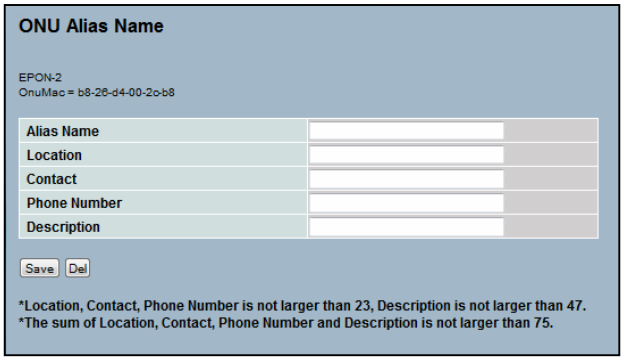


Figure 4-2: Alias Name Configuration

Parameter description:

- **Alias Name:** name to identify the ONU.
- **Location:** the location of the ONU.

Note: not larger than 23.

- **Contact:** contact of the responsible for the ONU.

Note: not larger than 23.

- **Phone Number:** phone number of the responsible for the ONU.

Note: not larger than 23.

- **Description:** description of the ONU.

Note: not larger than 47.

- **Buttons**

Save: Click to Save changes.
Del: Click to delete the configuration.

4.1.2 ONU Port Config

Web Interface

To configure the ONU Ports in the web interface:

1. Click ONU Management.
2. Click ONU List
3. For the selected ONU, choose the option ONU Port Config on the function combo box.
4. Set the parameters.
5. Click Save.

Note: Configuration values will take effect when <Save> button is clicked.

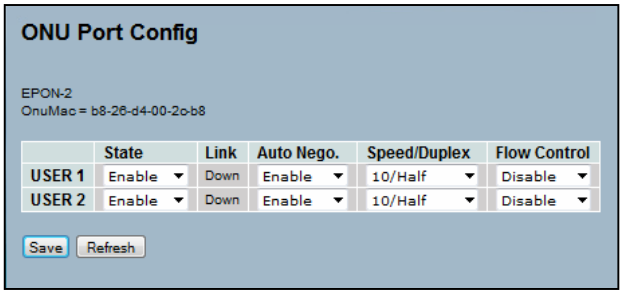


Figure 4-3: The ONU Port Config illustration

Parameter description

• **State:** The management status of the ONU's UNI ports. Possible values are [Enable] and [Disable].
Default: [Enable]

• **Link:** The physical link status of the ONU's UNI ports. Possible values are [Up] and [Down]. UNI is the abbreviation of "User Network Interface". It connects with the subscriber's network. This parameter cannot be configured.

• **Auto Nego:** Auto Negotiation status of the ONU's UNI ports. Possible values are [Enable] and [Disable]
Default: [Enable]

• **Speed/Duplex:** Line speed and duplex mode of the ONU's UNI ports. Possible values for UNI port 1 (USER 1 in the dialogue box) are [1000/Full] [100/Full] [100/Half] [10/Full] [10/Half]. Possible values for UNI port 2 (USER 2 in the dialogue box) are [100/Full] [100/Half] [10/Full] [10/Half].
Default: [1000/Full] for USER 1; [100/Full] for USER 2.

• **Flow Control:** IEEE802.3x Pause flow control state of the ONU's UNI ports. Possible values are [Enable] and [Disable]
Default: [Disable]

4.1.3 ONU Port Statistics

Web interface

To check the ONU Statistics in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Statistics on the function combo box.

On this Menu is possible to check the statistics for the EPON Port, UNI Port 1 (GbE) and UNI Port 2 (FE) on both directions upstream (Transmit) and downstream (Receive).

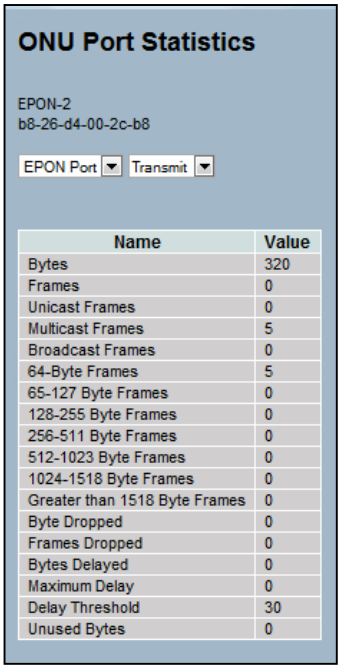


Figure 4-4: The ONU Port Statistics illustration

Parameter description

Auto-refresh: Click to update the ONU port statistics data automatically.

Refresh: Click to update the ONU Port statistics data manually.

Clear: Click to clear the ONU Port statistics data manually.

4.1.4 ONU Information

Web interface

To check the ONU Information in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Information on the function combo box.

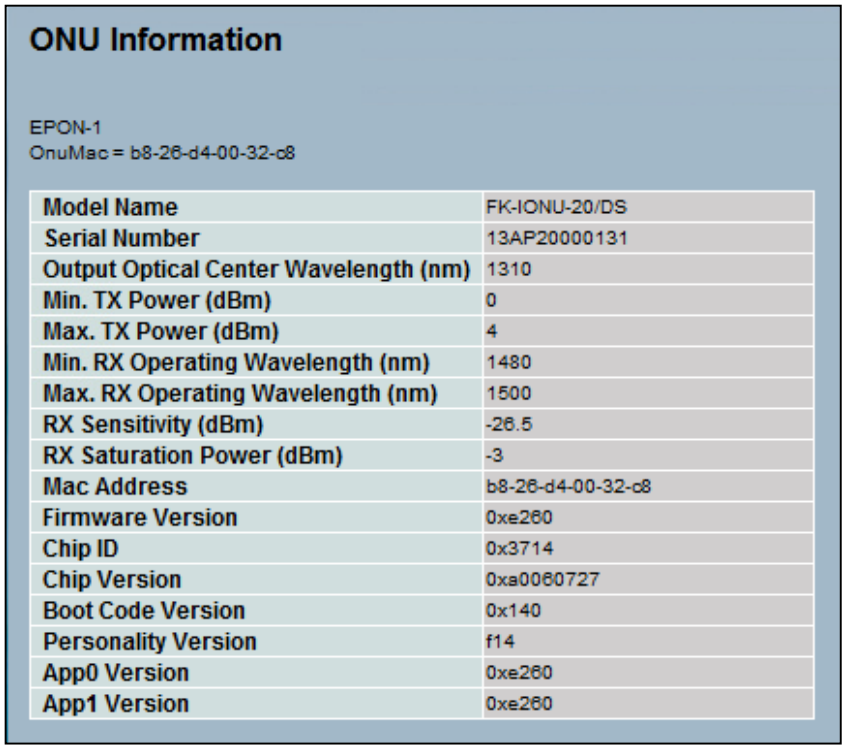


Figure 4-5: ONU Information

4.1.5 ONU Traffic Management

Rules Setting

The Rules Setting shows ONU traffic information that includes rule Priority, Action, Parameters, Field Select, Op, and Value. You can control the user data flow by configuring these rules. Classification is the process of deciding which frames are forwarded to particular queues and passed through the ONU. Filtering is the process of deciding which frames should be dropped and not passed through the ONU. An ONU has a Queue Configuration, which describes the number and sizes of queues in use, as well as their connectivity to user ports and EPON logical links. An ONU also has a classification scheme, which is a set of rules describing how traffic is forwarded to priority queues in either direction.

Web interface

To configure the ONU Rules in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Traffic Management on the function combo box.
4. Click on the "Add" button to create a new rule.

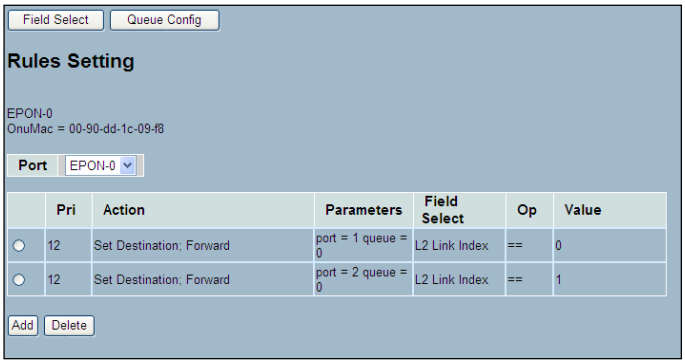


Figure 4-6: Adding a new rule

5. Create a clause, defining which Field of the packet will be analyzed, the operator, the Value type and the Value.
6. Click Add Clause.

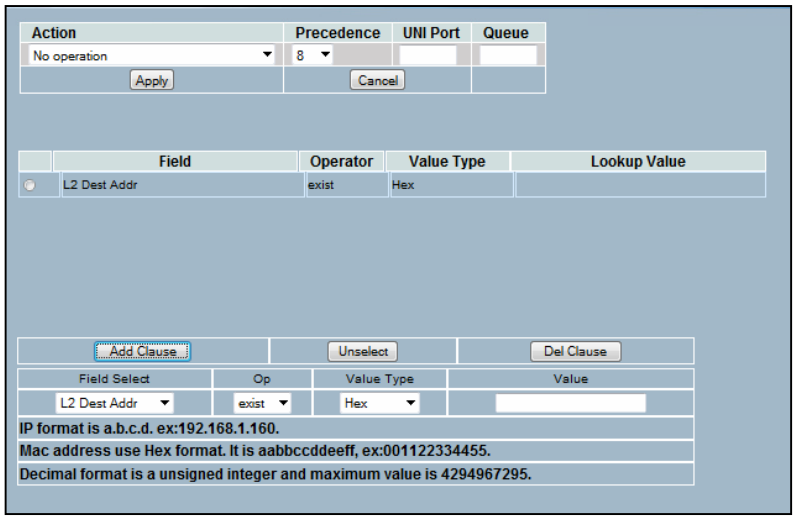


Figure 4-7: Configuring the rule clause

7. Define what action to take for each rule, its Precedence, to which UNI port will be applied and which queue to use.
8. Click Apply.

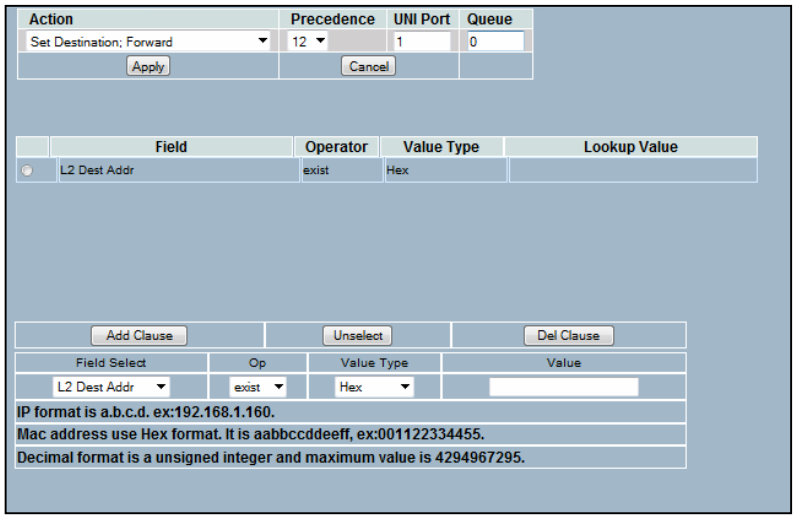


Figure 4-8: Configuration of the rule action

Parameter description

• **Action:** It's the action(s) taken upon the frame if all clauses of the rule are true. For example, rules may set the destination queue for a frame, add a VLAN tag or discard the frame.

• **Precedence:** Rule precedence.

• **Field Select:** Selects the field of the Ethernet frames that you desire to match.

• **Op:** Operator

value	symbol	description
0	False	Never match
1	==	Field Equal to value
2	!=	Field Not equal to value
3	<=	Field Less than or equal to value
4	>=	Field Greater than or equal to value
5	exists	True if field exists (value ignored)
6	!exist	True if field does not exist (value ignored)
7	True	Always match

• **Value Type:** It includes 3 types. Hex, Decimal and IP format. When field is IPv4 DA or IPv4 SA, you must select IP format type. When field is L2 Dest Addr, you must select Hex type. When field is Eth VID, you must select Decimal type.

• **Value:** Input the look-up value in the Ethernet frames that you desire to match.

4.1.6 ONU Queue Configuration

This functionality configures the upstream and downstream queues on the ONU. The upstream queues hold frames destined for the Logical Links and the downstream queues for the UNI Ethernet ports. Queue sizes are specified in the order of queue priority, where the first queue has the highest priority. Note that the Queue Configuration command causes any existing Classification rules on the ONU to be invalidated. Therefore a Queue configuration change should always be followed by Classification commands to re-install the required classification rules. The Filtering rules of the ONU will remain.

Web interface

To configure the ONU Queues in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Traffic Management on the function combo box and then click on the "Queue Config" button.
4. Click "Add new entry" to add new links
5. Select a link and click "Edit entry" to change the queue size or add new queues to the existing links.
6. Select a Port and click in "Edit" to change the queue size or add new queues.
7. Click Save and reboot the ONU to apply the changes.

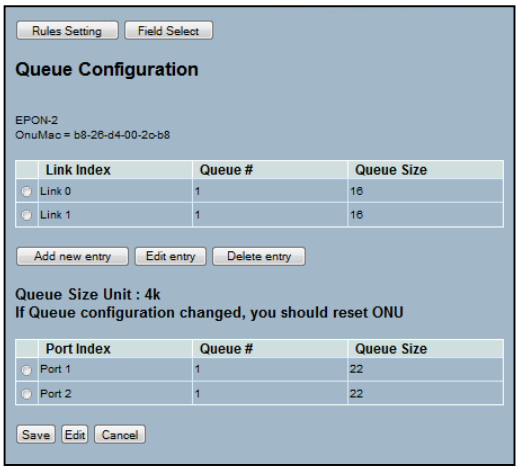


Figure 4-9: The ONU Queue configuration

4.1.7 Field Select Configuration

This functionality sets the fields parsed from each frame which are used in lookup engine rules to filter or classify frames. Each port on the ONU has a lookup engine (LUE) that processes frames received on that port. Each lookup engine has a number of field selectors supported in the hardware. Each field is programmed with a field code that describes the field parsed from the frame in terms of protocol layer, dword in the frame, bit start and bit width.
The Reference Count indicates the number of clauses in rules that are currently using this field. If the field is currently unused, the reference count will be zero, and the layer select, dword offset, bit offset, and bit width will contain the maximum possible values for that field on that ONU. Fields with a non-zero reference count cannot be reprogrammed with the Set message. All rules using a given field must be deleted before the meaning of that field can be changed. Note that hardware and firmware system rules will also use fields in the LUE. These rules cannot be deleted, and so it is possible that some reference counts will never go to zero.

Web interface

To configure the ONU Queues in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Traffic Management on the function combo box and then click on the "Field Select" button.
4. For the EPON port the entries 5, 6, 7, 8 and 9 are editable. Select the entry and click in the "Edit" button.
5. For the User port the entries 2, 5, 6, 7, 8, 9 and 10 are editable. Select the entry and click in the "Edit" button.
6. Click Save.

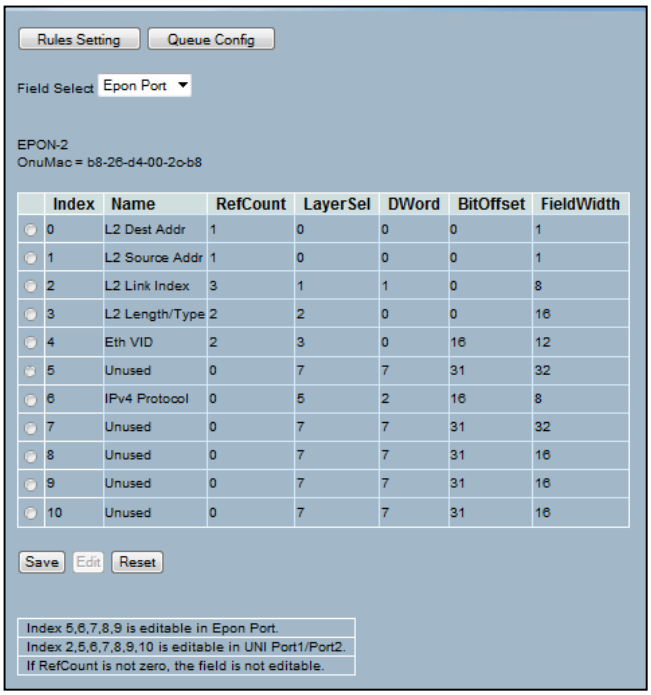


Figure 4-10: The Field Select configuration

Parameter description

- **Field Select:** Select EPON port, UNI Port0 or UNI Port1.
- **Edit:** Click to update the selected field entry.
- **Name:** Field Select description.
- **RefCount:** Display the reference count value.
- **LayerSel:** Layer 2 and 3 field selection.
- **DWord:** A 32-bit word. The Dword offset is such that the first 32 bits shown are dword offset =0, the next 32 bits are dword offset =1 and so on. The dword offset is a 4-bit field.

• **Bitoffset:** This value specifies the number of bits from the right after which the field select begins. It consists of 5 bits.
• **Fieldwidth:** This fieldwidth is one bit less than the actual width of the field. Since a field cannot be of width zero, this convention allows encoding widths up to 32 bits in only five bits. It consists of 5 bits.

4.1.8 ONU Green PON (Industrial ONUs)

Web interface

The Green PON feature is only available for industrial ONUs. To enable or disable it for an ONU individually in the Web Interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Green PON in the function combo box.
4. Select the ONU Green PON option.
5. Click Save.

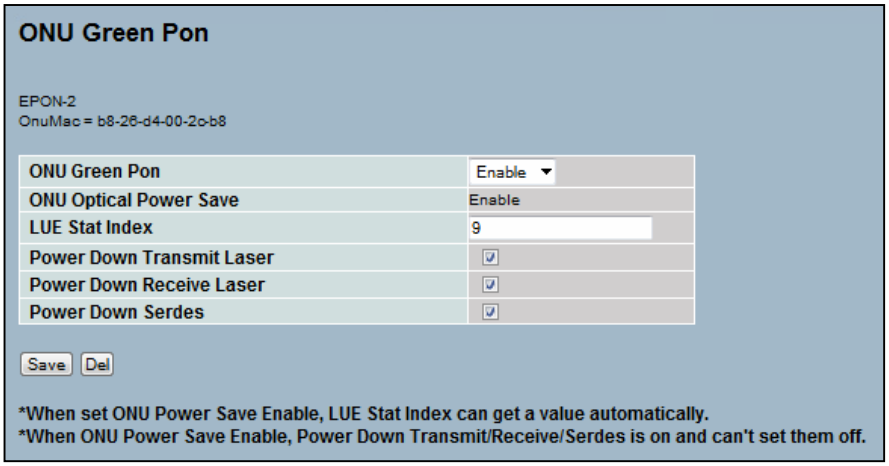


Figure 4-11: ONU Green PON Configuration

4.1.9 IGMP Snooping Parameters

This command is general IGMP Snooping configuration, which has four parameters Robustness Count, Last Member Query, Number of IGMP Groups and Queue for Classification. The ONU does not need to be explicitly provisioned, because the ONU obtains many values by snooping. The Query maximum response times are snooped from the query messages generated by the OLT. The ONU measures the interval between snooped General Queries to detect the General Query Interval of network Query.

Web interface

To configure the IGMP Snooping Parameters in the Web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option IGMP Snooping Parameters in the function combo box.
4. Set the parameters.
5. Click Save.

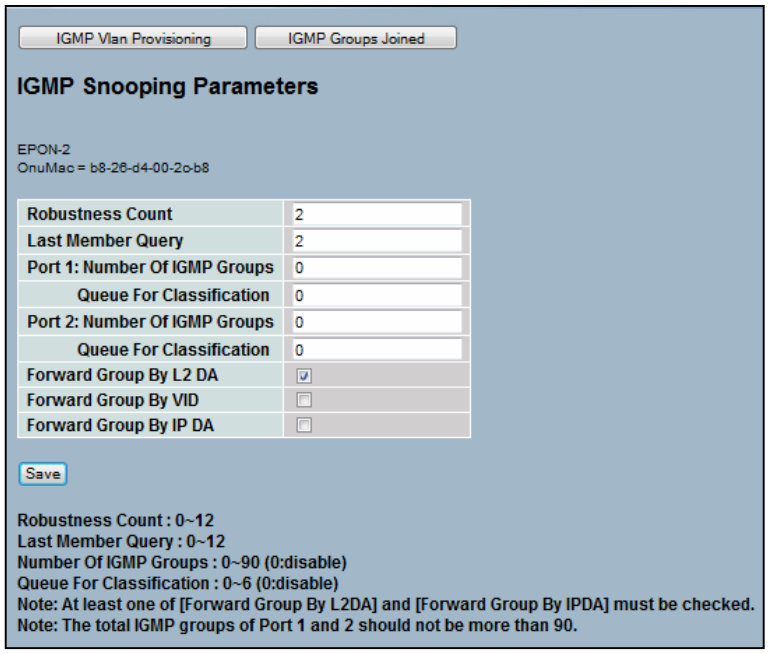


Figure 4-12: The IGMP Snooping Parameters configuration

Parameter description

• **Robustness Count:** The Robustness Count is the number of IGMP General Queries. The query may pass with no corresponding IGMP Report reply before a Group is removed. So if Robustness Count is set to 0, the group will be removed when it does not get any response.
Default: 2

• **Last Member Query:** If the Group exists, the Last Member Query represents the number of IGMP Group Specific Queries that may pass with no corresponding IGMP Report reply.
Default: 2

• **Number Of IGMP Groups:** This parameter is set per port. The number of IGMP Groups means how many Groups can be added to this port. If the number of IGMP Groups is set to 0, it means the IGMP snooping is disabled and all IGMP requests will be sent.
Default: 0

• **Queue For Classification:** This parameter decides how many Queues will be used for classification of downstream IP multicast traffic.
Default: 0

• **Forward Group By L2 DA:** Forwards the IGMP group via Layer 2 Destination Address (DA).

• **Forward Group By VID:** Forwards the IGMP group via VLAN ID (VID).

• **Forward Group By IP DA:** Forwards the IGMP group via IP Address (DA).

4.1.10 IGMP VLAN Provisioning

Web interface

To configure the IGMP Snooping Parameters in the Web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option IGMP Snooping Parameters in the function combo box and then click on "IGMP VLAN Provisioning" button.
4. Set the parameters.
5. Click Save to apply the changes.

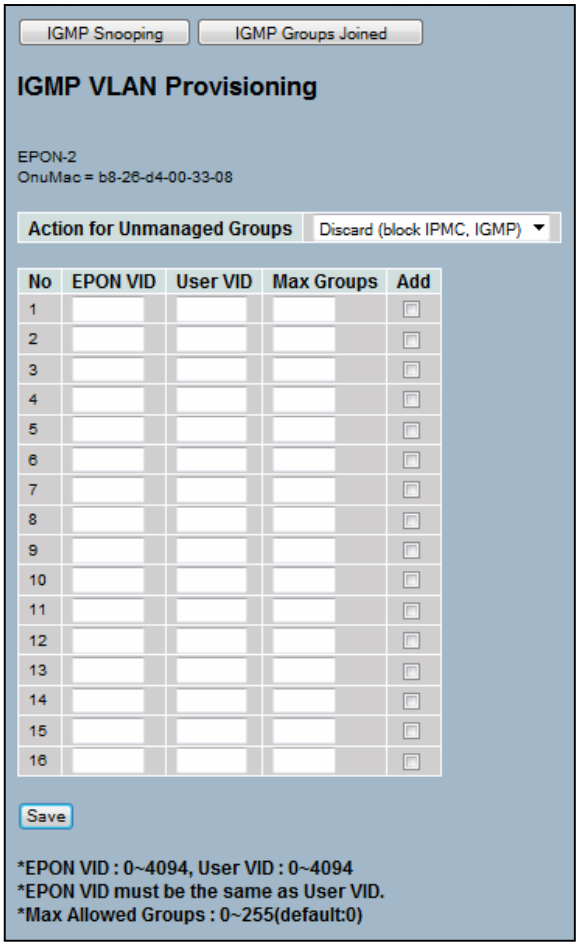


Figure 4-13: The IGMP VLAN Provisioning configuration

Parameter description

• **Action for Unmanaged Groups:** This parameter has two choices, Discard (block IPMC, IGMP) and Ignore (forward unchanged).

• **EPON VID:** IPMC will be sent to the OLT, the frame will use EPON VID.

• **User VID:** The User VID is the VID of the IPMC, it gets it from the ONU user port.

• **Allowed Groups:** This parameter limits IGMP VLAN groups. The Max Allowed Groups is the maximum number of groups that can be joined in each VLAN by this ONU. If the Max Allowed Groups is setting 0, the ONU will not join any groups and will discard all IGMP frames on this VLAN.

4.1.11 IGMP Groups Joined

This functionality will show the entries in the IGMP group table. It will list the number of ports and Group IP.

Web interface

To check the IGMP Groups Joined in the Web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option IGMP Snooping Parameters in the function combo box and then click on "IGMP Groups Joined" button.
4. Click Refresh.

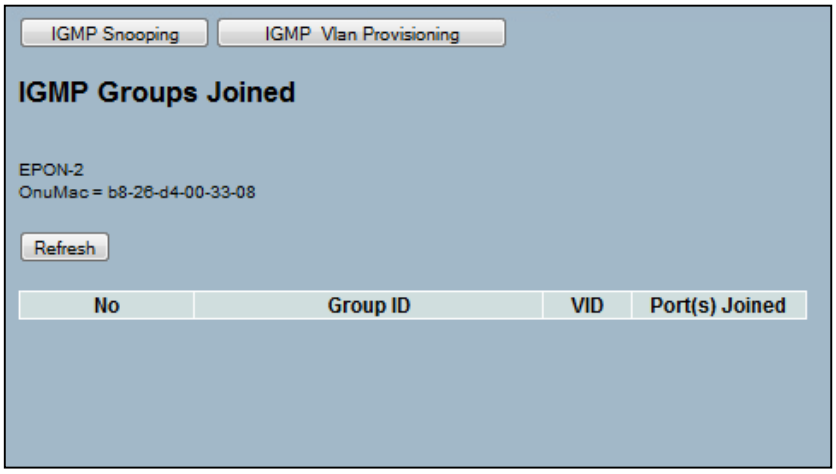


Figure 4-14: The IGMP Groups Joined illustration

Parameter description

Refresh: Click to update the IGMP Group table immediately.

4.1.12 ONU Bridge Config

This functionality configures the MAC address learning mode of the ports on the ONU. If the timeout is reached, the entries will be automatically removed from the table.
There are two kinds of Learning Modes, Forward (802.1d Learning) and Drop Until Learned (MAC Access Control). Forward mode will permit forwarding unlearned address, which is the default behavior. Drop Until Learned means the port learns by the allowed learning entry limit, and if the frames are discarded, the MAC address will not be learned.

Web interface

To configure the ONU Bridging in the Web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Bridging Config in the function combo box.
4. Set the parameters.
5. Click Save.

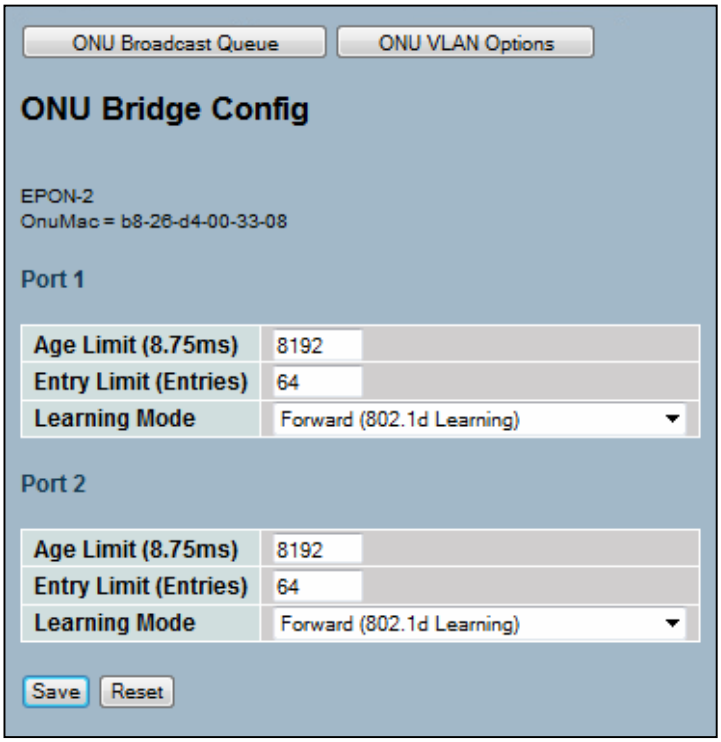


Figure 4-15: The ONU Bridge Config illustration

Parameter description

• **Age Limit:** how much time that the address will stay on the ONU Dynamic Table**.**

• **Entry Limit:** define the number of MAC addresses that the ONU can store locally on the ONU Dynamic table. The limit is 64.

• **Learning Mode:** There are two kinds of Learning Modes, Forward (802.1d Learning) and Drop Until Learned (MAC Access Control).

4.1.13 Downstream Multi/Broadcast Queue

Web interface

To configure the ONU Downstream Multi/Broadcast Queue in the Web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Bridging Config in the function combo box and then click on "ONU Broadcast Queue" button.
4. Select the port.
5. Define the Queue Idx.
6. Click Save.

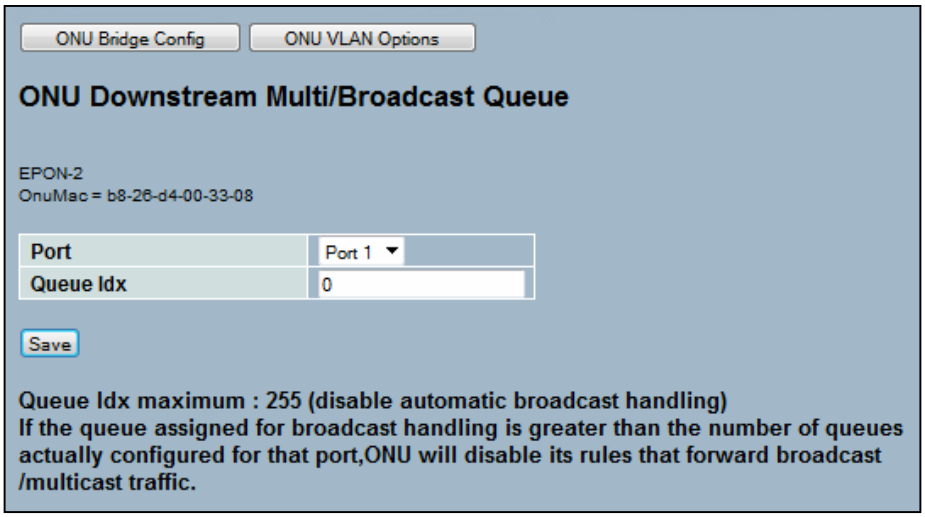


Figure 4-16: The Downstream Multi/Broadcast Configuration

Parameter description:

- **Queue Idx :** The broadcast/multicast queue index to be specified for a given port.
- **Buttons**

Save: Click to Save changes.

4.1.14 VLAN Options

Web interface

To configure ONU VLAN Options in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Bridging Config in the function combo box and then click on "ONU VLAN Option" button.
4. Set the parameters.
5. Click Save.

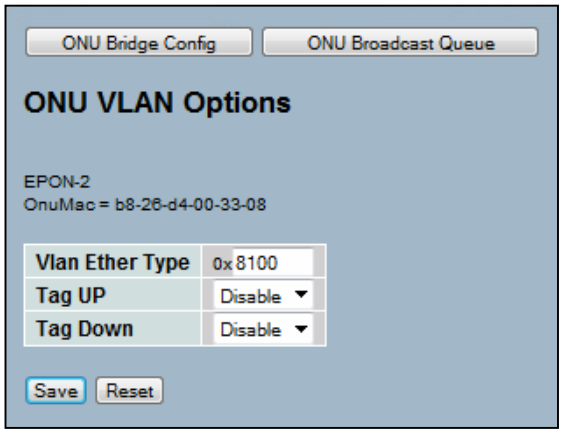


Figure 4-17: ONU VLAN Options Configuration

Parameter description:

- **VLAN Ether Type:** VLAN Ether Type uses hexadecimal format.
- **Tag UP:** This parameter can set as Enable or Disable.
- **Tag Down:** This parameter can set as Enable or Disable.
- **Buttons**

Save: Click to Save changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

4.1.15 ONU RSTP

Web interface

To enable RSTP packets for the ONU in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU RSTP in the function combo box.
4. Select the option Pass Through for Bridge mode.
5. Click Save.

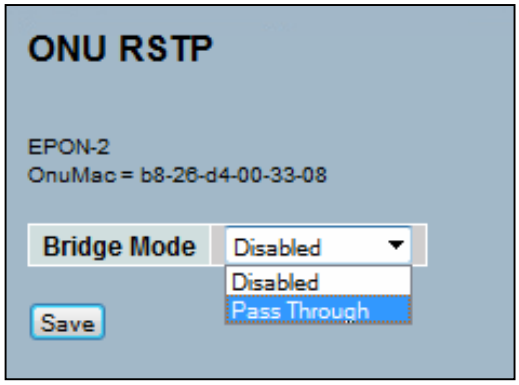


Figure 4-18: ONU RSTP Configuration

4.1.16 ONU Dynamic Table

The section will teach you how to display the automatically learned MAC addresses for the selected ONU.

Web interface

To check the ONU Dynamic Table in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Dynamic Table in the function combo box.
4. Click Refresh.

Figure 4-19: The ONU Dynamic Table illustration

Parameter description

- **Auto-refresh:** Select to enable the auto-refresh in the ONU Dynamic Table.
- **Refresh:** Click to refresh the ONU Dynamic Table immediately and manually.
- **Clear P1 and Clear P2:** Click to clear the dynamic MAC entries of the selected port.

4.1.17 ONU Operations

Web interface

To configure the ONU Operations in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option ONU Operations in the function combo box.
4. Click on the desired option.

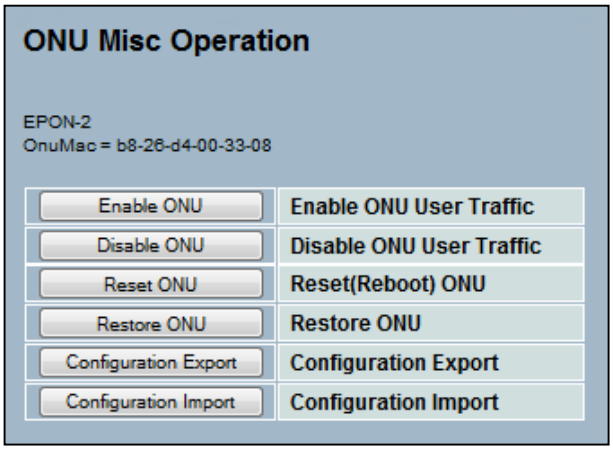


Figure 4-20: ONU Operations

Parameter description

- **Enable ONU:** Enable ONU User Traffic
- **Disable ONU:** Disable ONU User Traffic
- **Reset ONU:** Reset (Reboot) ONU
- **Restore ONU:** Restore ONU
- **Configuration Export:** Configuration Export
- **Configuration Import:** Configuration Import

4.1.18 Loopback Test

Function description:

This is an integrated OAM loopback test procedure. It commands the OLT to perform a connectivity and link quality test on a logical link. The test involves the following steps:

(1) The OLT asks the ONU to put either a link or a UNI port (MAC or PHY) in loopback.

(2) The OLT sends special frames downstream which will be looped back upstream by the target ONU.

(3) After the requested number of frames have been transmitted and received, the OLT commands the ONU to leave the OAM Loopback mode. The target logical link ends the user traffic service.

(4) Loopback is finished and the result would be reported.

Web interface

To perform the ONU Loopback Test in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Loopback Test in the function combo box.
4. Click Save.

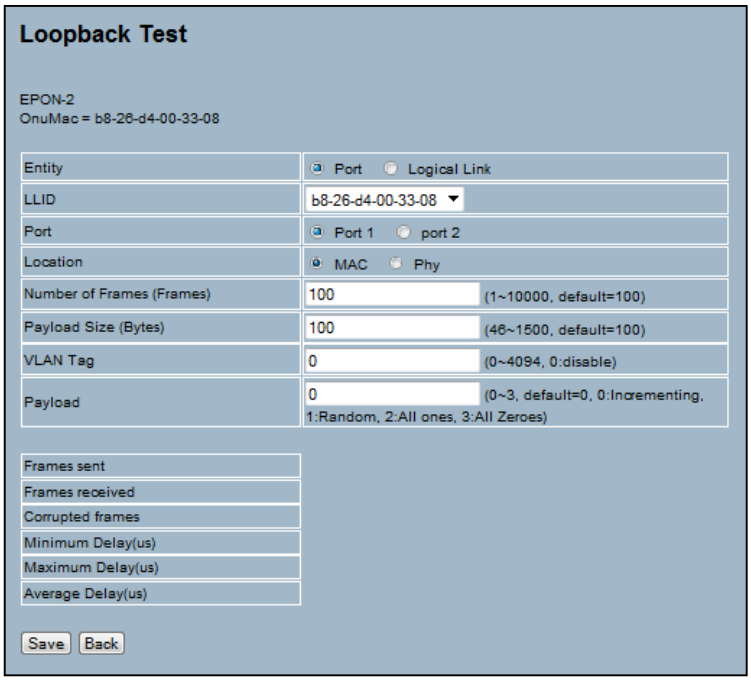


Figure 4-21: Loopback test

Parameter description:

- **Entity:** To specify the end point on the ONU in a loopback test. Possible Values are [Port] or [Logical Link].
- **LLID:** The Mac Address of the target logical link or Mac Address of a logical link which is connected to the target entity.
- **Port:** If the loopback entity is [Port], the target UNI port should be specified.
- **Location:** If the loopback entity is [Port], the target location ([Mac] or [Phy]) should be specified.
- **Payload Size (Bytes):** The size of the data portion of an Ethernet frame.
- **Number of Frames (Frames):** Number of frames to transmit in a loopback test.
- **VLAN Tag:** Specifies the VID of the loopback frames. The valid VID range is 1-4094. 0 disables frame tagging.
- **Test Result:**

Includes [Frames sent], [Frames received OK], [Corrupted frames received], [Minimum Delay (µs)], [Maximum Delay (µs)], [Average Delay (µs)].

A frame is presumed lost if it has not returned after 1 second. Delay stats are accumulated only for frames received OK. Five consecutively lost frames will cause the test to be aborted.

- **Buttons**

Save: Click to Save changes.

Back: Go back to the ONU List Page.

4.1.19 Logical Links

This section will teach you to display the “Logical Link” table. It displays all provisioned logical links belonging to an ONU.

Web interface

To configure the ONU Logical Links in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Links in the function combo box.

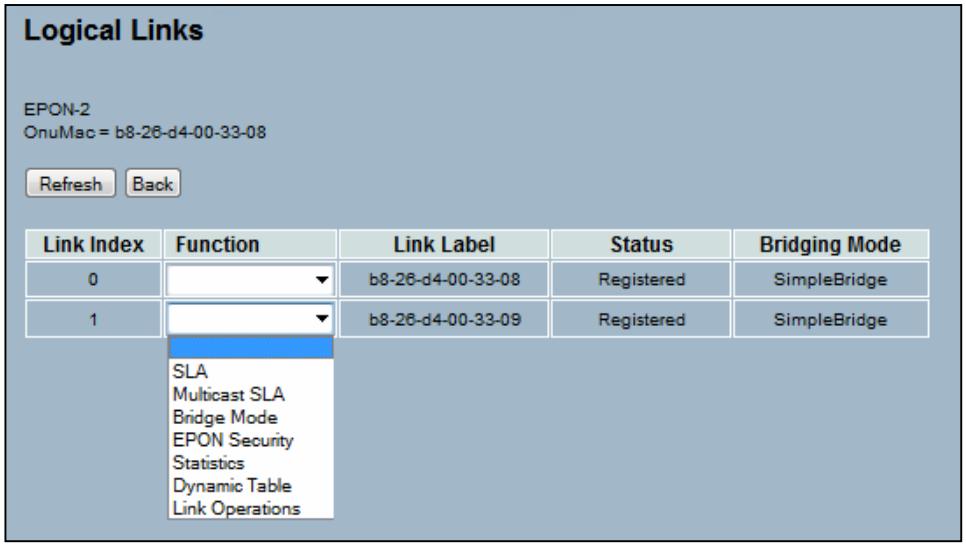


Figure 4-22: The Logical Links Table Screen

Parameter description

- **Link Index:** Sequential numbering from 1 to N (N <= 8).
- **Function:** Select the function type to display the logical links information, the available options are:

SLA
Multicast SLA
Bridge Mode
EPON Security
Statistics
Dynamic Table
Link Operations

- **Link Label:** It is the globally unique Mac Address assigned to a logical link. The Mac Address is used within an EPON system to identify the logical link. In IEEE802.3ah specification, one ONU supports one logical link. But our ONU support multiple logical links (up to 8) in a single physical device. Eight successive Mac Addresses are assigned for one ONU, each of them representing one logical link.
- **Status:** Possible values are [Registered] or [Blocked].
- **Bridging Mode:** The provisioned bridging mode of a logical link.
- **Refresh:** To update the logical links data immediately.
- **Back:** To return to previous logical links data immediately.

4.1.19.1 SLA

4.1.19.1.1 Upstream Ingress SLA

Web interface

To configure the Upstream Ingress SLA in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option SLA in the function combo box.
5. Set the parameters.
6. Click Save.

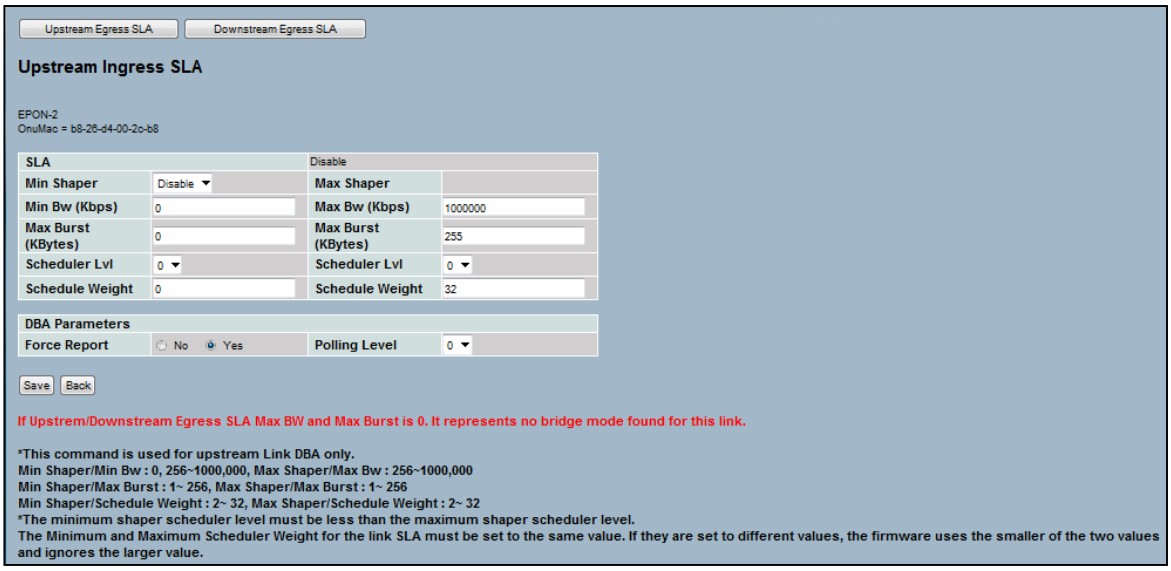


Figure 4-23: The Upstream Ingress SLA Configuration

Parameter description:

- **Min Shaper/Min Bw:**

This parameter will guarantee a minimum bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 0

- **Max Shaper/Max Bw:**

The maximum allowed use of Bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 100000

- **Min and Max Shaper/Max Burst:**

Range: 1~256 (Unit: KBytes)
Mix Default: 0
Max Default: 255

- **Min and Max Shaper/Schedule Weight:**

Range: 2~ 32. The minimum shaper/scheduler level must be less than the maximum shaper/scheduler level. The Minimum and Maximum Scheduler Weight for the link SLA must be set to the same value. If they are set to different values, the firmware will use the smaller of the two values and ignore the larger value.

- **Force Report**

YES = Force Report NO = No Auto OAM Bandwidth Padding

- **Polling level**

For priority 0, the scheduling latency is approximately equal to the larger value of the polling rate and the cycle length.

- **Upstream/downstream Queue SLA**

Dynamic bandwidth allocation (DBA) is used to adjust the uplink and downlink bandwidth of individual ONUs in real time, according to the traffic status of ONUs.

- **Buttons**

Save: Click to Save changes.
Back: Go back to the Logical Link page.

4.1.19.1.2 Upstream Egress SLA

Web interface

To configure the Upstream Egress SLA in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option SLA in the function combo box and then click on the button "Upstream Egress SLA".
5. Set the parameters.
6. Click Save.

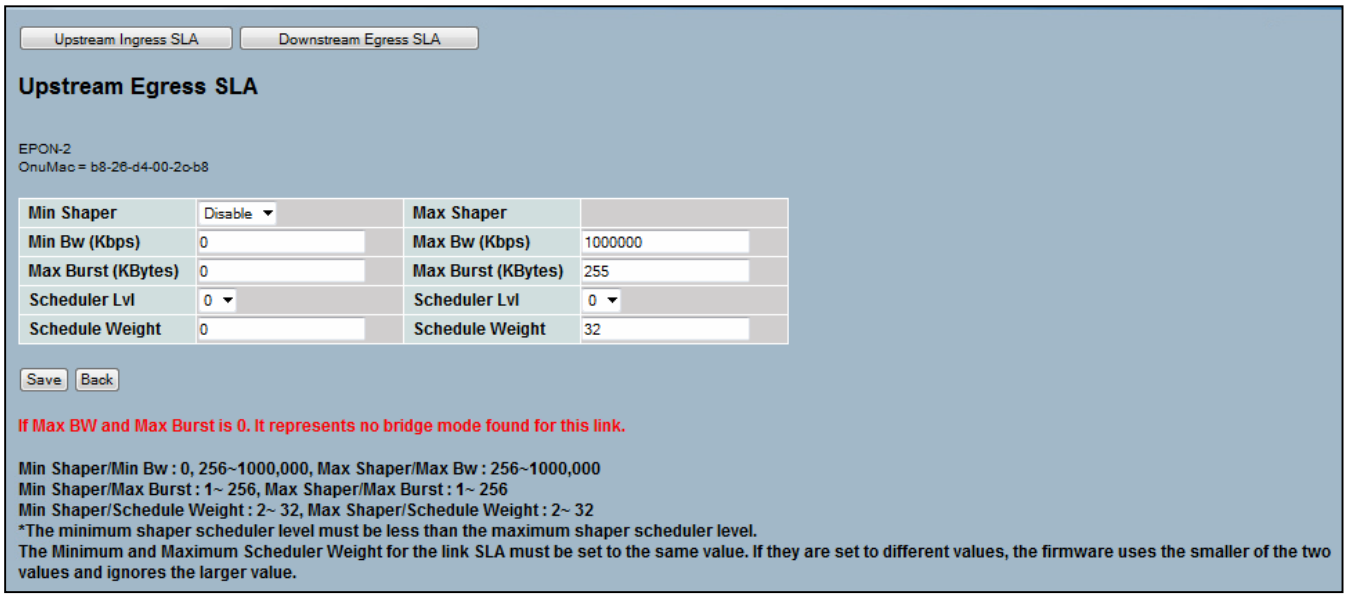


Figure 4-24: The Upstream Egress SLA Configuration

Parameter description:

- **Min Shaper/Min Bw:**

This parameter will guarantee a minimum bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 0

- **Max Shaper/Max Bw:**

The maximum allowed use Bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 100000

- **Min and Max Shaper/Max Burst:**

Range: 1~256 (Unit: KBytes)
Mix Default: 0
Max Default: 255

- **Min and Max Shaper/Schedule Weight:**

Range: 2~ 32.The minimum shaper/scheduler level must be less than the maximum shaper/scheduler level. The Minimum and Maximum Scheduler Weight for the link SLA must be set to the same value. If they are set to different values, the firmware will use the smaller of the two values and ignore the larger value.

- **Buttons**

Save: Click to Save changes.
Back: Go back to the Logical Link page.

4.1.19.1.3 Downstream Egress SLA

Web interface

To configure the Upstream Egress SLA in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option SLA in the function combo box and then click on the button "Downstream Egress SLA".
5. Set the parameters.
6. Click Save.

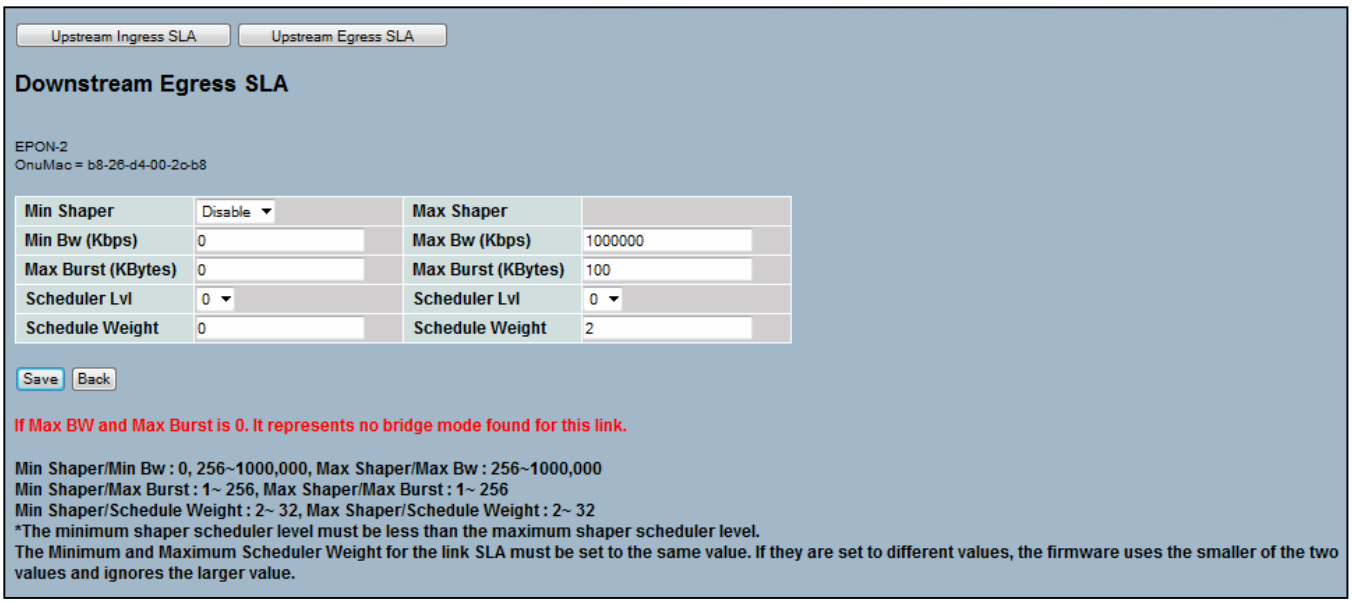


Figure 4-25: The Downstream Egress SLA Configuration

Parameter description:

- **Min Shaper/Min Bw :**

This parameter will guarantee a minimum bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 0

- **Max Shaper/Max Bw:**

The maximum allowed use Bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 100000

- **Min and Max Shaper/Max Burst:**

Range: 1~256 (Unit: KBytes)
Mix Default: 0
Max Default: 255

- **Min and Max Shaper/Schedule Weight:**

Range: 2~ 32.The minimum shaper/scheduler level must be less than the maximum shaper/scheduler level. The Minimum and Maximum Scheduler Weight for the link SLA must be set to the same value. If they are set to different values, the firmware will use the smaller of the two values and ignore the larger value.

- **Buttons**

Save: Click to Save changes.
Back: Go back to the Logical Link page.

4.1.19.2 Multicast SLA

Web interface

To configure the Multicast SLA in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Multicast SLA in the function combo box.
5. Set the parameters.
6. Click Save.

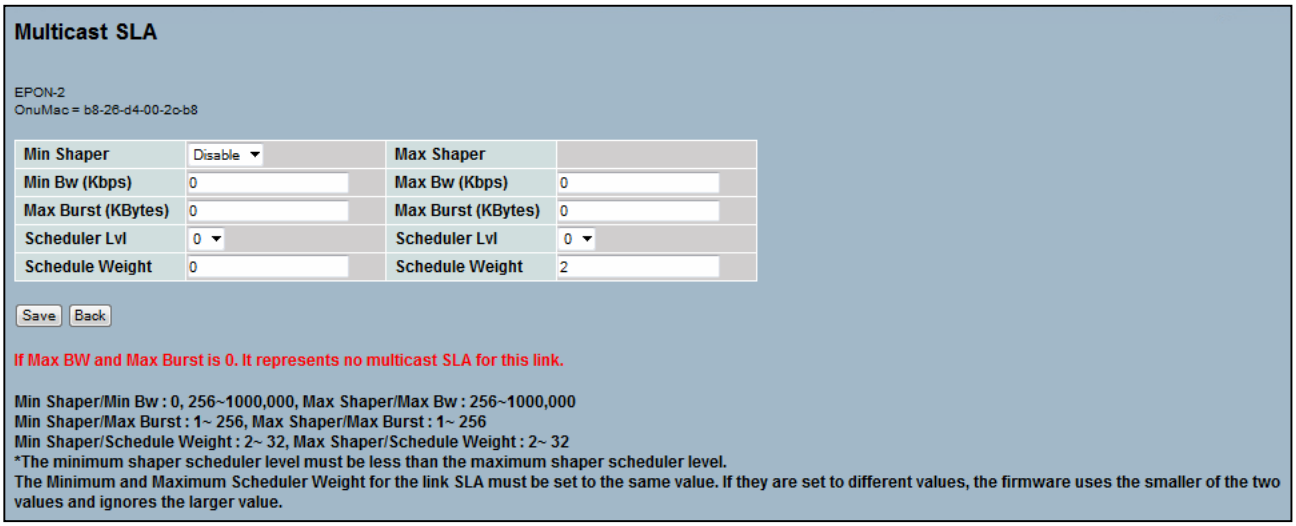


Figure 4-26: The Multicast SLA Configuration

Parameter description:

- **Min Shaper/Min Bw:**

This parameter will guarantee a minimum bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 0

- **Max Shaper/Max Bw:**

The maximum allowed use Bandwidth.
Range: 256~1000000 (Unit: Kbps)
Default: 100000

- **Min and Max Shaper/Max Burst:**

Range: 1~256 (Unit: KBytes)
Mix Default: 0
Max Default: 255

- **Min and Max Shaper/Schedule Weight:**

Range: 2~ 32. The minimum shaper/scheduler level must be less than the maximum shaper/scheduler level. The Minimum and Maximum Scheduler Weight for the link SLA must be set to the same value. If they are set to different values, the firmware will use the smaller of the two values and ignore the larger value.

- **Buttons**

Save: Click to Save changes.
Back: Go back to the Logical Link page.

4.1.19.3 Bridge Mode

This functionality configures the forwarding mode and learning table entry limit per-Logical Link. Logical links may be configured for simple 802.1d bridging or for various types of VLAN bridging.

The OLT maintains a single MAC table that may contain up to 3072 dynamically learned MAC addresses used for downstream bridging and other features. For bridging modes that use MAC table, the OLT learns the source address of upstream frame on a per LLID basis. An upper limit on the number of table entries that may be used is maintained for each LLID. When the sum of dynamically learned addresses reaches the per-LLID limit, additional MAC addresses will not be learned even if there is room in the table. The aggregate size of all per LLID MAC tables may exceed the available hardware table size (3072). In such a configuration, if the entire learning table is full, the oldest entry from all per LLID tables will be the target for replacement.

In the event that a per-LLID learning table becomes full, an attempt to learn another MAC address on that LLID will trigger a MAC Table Overflow alarm that will be issued to the host processor. In this case, the oldest entry on the table is subject to replacement by the source address of a frame received upstream (these are frames received by the EPON port).

Bridging modes that require a VLAN tag will not forward traffic until at least one VID has been set.

If a conflict exists between LLIDs configured in different bridging modes (destination address matches simple bridged, but VLAN tag matches an LLID configured in a VLAN mode) the packet will be dropped.

Web interface

To configure the Bridge Mode in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Bridge Mode in the function combo box.
5. Set the parameters.
6. Click Save.

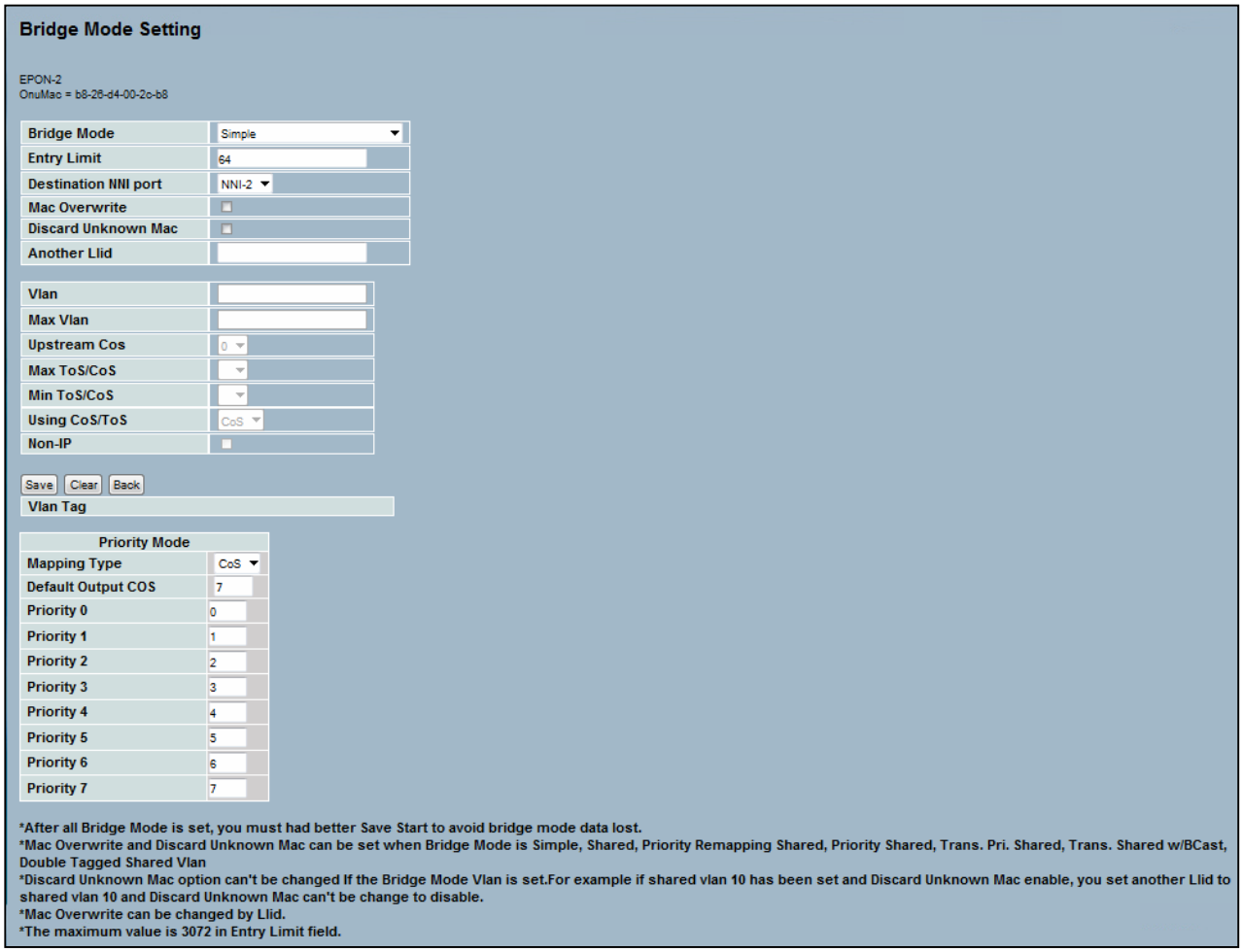


Figure 4-27: The Bridge Mode Configuration

Parameters description:

• **Bridge Mode:** Selects the type of data flow by choosing a Bridge Mode. Bridge Modes include 14 options.
Simple Bridged,
Dedicated Single VLAN,
Dedicated Double VLAN,
Shared VLAN,
Transparent VLAN,
Link Cross-Connect
Prioritized VLAN,
Priority Remapping Single VLAN,
Priority Remapping Double VLAN,
Priority Remapping Shared VLAN,
Priority Shared VLAN,
Transparent Priority Shared VLAN
Transparent Shared VLAN with Broadcast
Double Tagged Shared VLAN

• **Entry Limit:** An upper limit on the number of table entries that may be used for each LLID.
Range: 0~3072
Default: 64

• **Destination NNI Port:** defines the uplink port that will be used by the LLID.

• **Mac Overwrite:** when the number of entries on the table reaches the limit, it allows the entries to be overwritten.

• **Discard Unknown Mac:** it won't allow new entries on the table.

• **Another Llid:** the MAC address of the LLID on the other side of the link, used only when the bridge mode is Link Cross-connect.

• **Vlan:** VLAN ID

• **Max Vlan:** used to set a range of VLAN for the the Transparant Vlan Mode.

• **Upstream CoS:** defines the CoS value.

• **Max ToS/CoS:** defines the Max ToS/CoS value.

• **Min ToS/CoS:** defines the Min ToS/CoS value.

• **Using CoS/ToS:** defines which type of priority is going to be used.

• **Non-IP:** allows the passage of packets without IP header.

• **Mapping Type:** defines which type of priority is going to be used, necessary for the Remapping bridge modes.

• **Default Output CoS:** defines the output CoS.

• **Priority 0 ~ 7:** priority level.

• **Buttons:**

Save: Click to save the changes.
Clear: Click to clear the configuration.
Back: Click to Go back to the logical link page.

4.1.19.4 Epon Security

This command is used in encryption keys. This parameter is a timeout value. When the timer expires, a new key will be generated and exchanged. Setting 0 will disable it.

Web interface

To configure the Epon Security in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Epon Security in the function combo box.
5. Set the parameters.
6. Click Save.

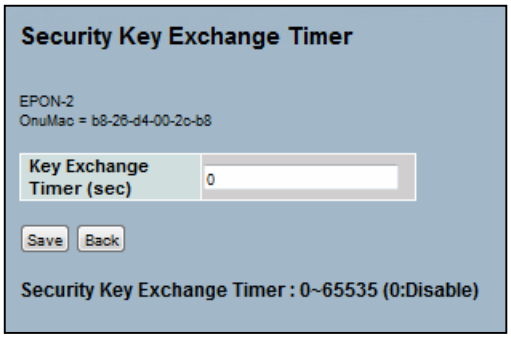


Figure 4-28: The Epon Security Configuration

Parameter description:

• **Key Exchange Timer (sec)**

0~65535 (0: Disable).

• **Buttons**

Save: Click to Save changes.

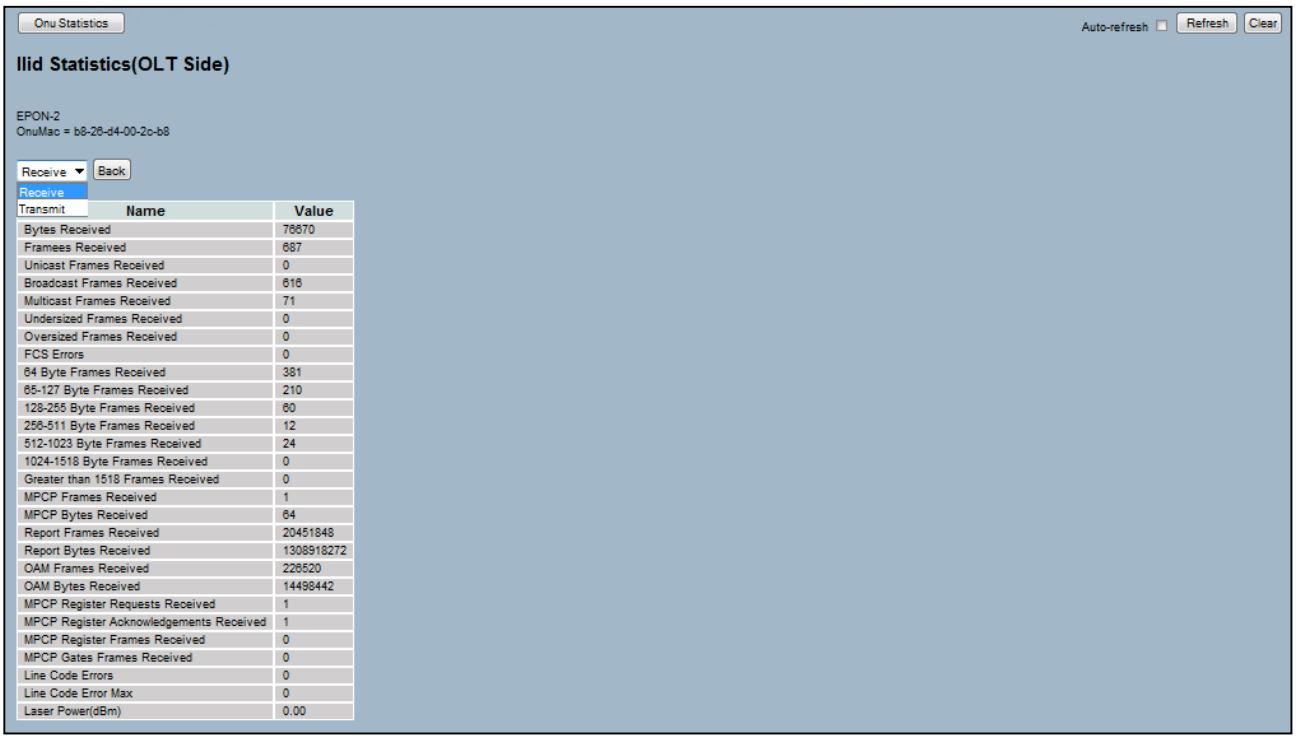
Back: Go back to the Logical Link Page.

4.1.19.5 Statistics

Web interface

To check the link statistics (OLT Side) in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Statistics in the function combo box.
5. Click Refresh.



Name	Value
Bytes Received	76670
Framees Received	687
Unicast Frames Received	0
Broadcast Frames Received	616
Multicast Frames Received	71
Undersized Frames Received	0
Oversized Frames Received	0
FCS Errors	0
64 Byte Frames Received	381
65-127 Byte Frames Received	210
128-255 Byte Frames Received	60
256-511 Byte Frames Received	12
512-1023 Byte Frames Received	24
1024-1518 Byte Frames Received	0
Greater than 1518 Frames Received	0
MPCP Frames Received	1
MPCP Bytes Received	64
Report Frames Received	20451848
Report Bytes Received	1308918272
OAM Frames Received	226520
OAM Bytes Received	14498442
MPCP Register Requests Received	1
MPCP Register Acknowledgements Received	1
MPCP Register Frames Received	0
MPCP Gates Frames Received	0
Line Code Errors	0
Line Code Error Max	0
Laser Power(dBm)	0.00

Figure 4-29: The Link Statistics (OLT Side)

Note: When the Power Monitor Function is enabled, the optical power received by the OLT can be checked on the last parameter (Laser Power) of the page above.

To check the link statistics (OLT Side) in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Statistics in the function combo box and then click on the button "Onu Statistics".
5. Click Refresh.

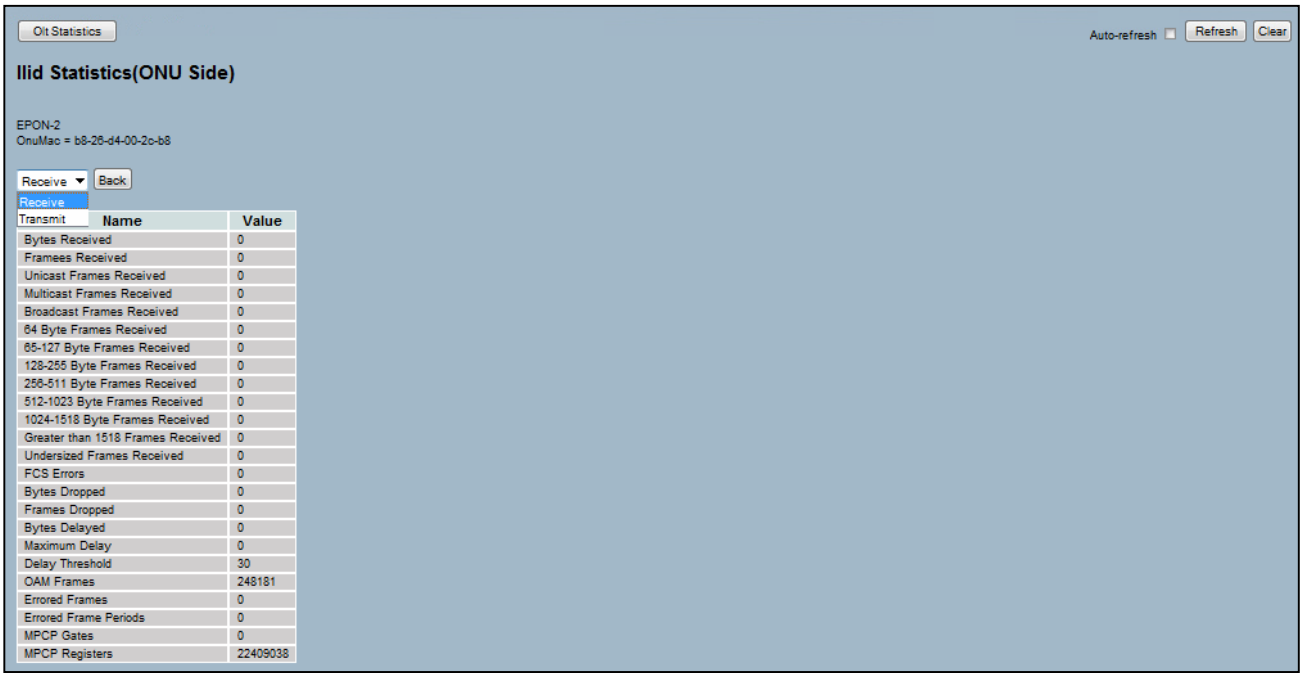


Figure 4-30: The Link Statistics (ONU Side)

4.1.19.6 Dynamic Table

Web interface

To check the ONU Dynamic Table in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Dynamic Table in the function combo box.
5. Click Refresh.

Figure 4-31: The ONU Dynamic Table

4.1.19.7 Link Operations

Web interface

To execute the ONU Operations in the web interface:

1. Click ONU Management.
2. Click ONU List.
3. For the selected ONU, choose the option Logical Link in the function combo box.
4. For the selected Logical Link, choose the option Operations in the function combo box.
5. Select the desired option.

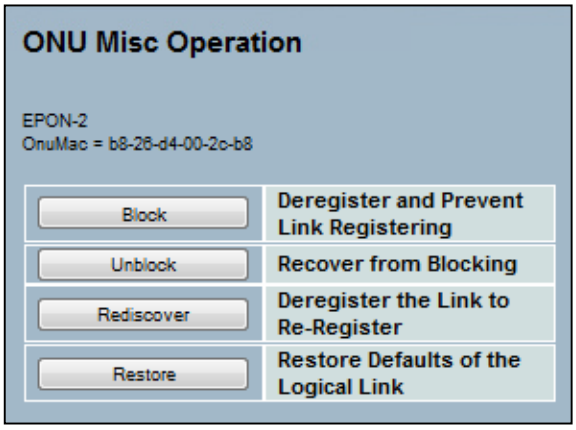


Figure 4-32: The ONU Operations

6. Click Save.

Parameter description:

- **Block:** Deregister and Prevent Link Registering
- **Unblock:** Recover from Blocking
- **Rediscover:** Deregister the Link to Re-Register
- **Restore:** Restore Defaults of the Logical Link

4.2 ONU Subscriber View

The ONU subscriber view allows to see all ONUs connected to both EPON ports of the OLT. For the ONU to appear on the subscriber view, it must have the Alias name configured.
When using the subscriber view, it's possible to access all menus related to the selected ONU.

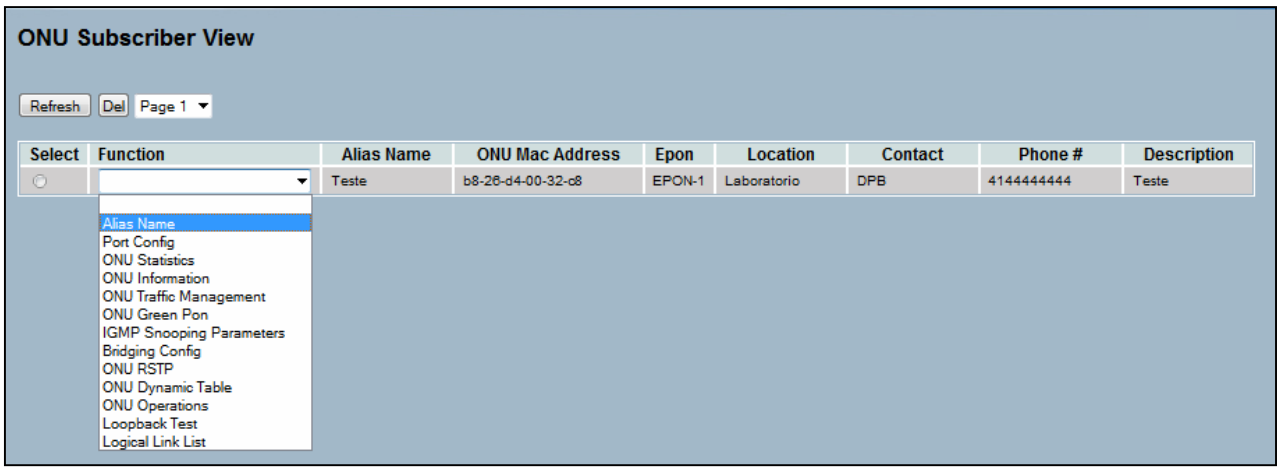


Figure 4-33: ONU Subscriber View

4.3 ONU Authorization

The “ONU Authorization” table displays Authorized/Unauthorized ONUs under an OLT. On the Select field in this table you may select the ONU to be authorized. If you want to authorize many ONUs at once, you may choose many ONUs on the Select field and click the Authorize button.

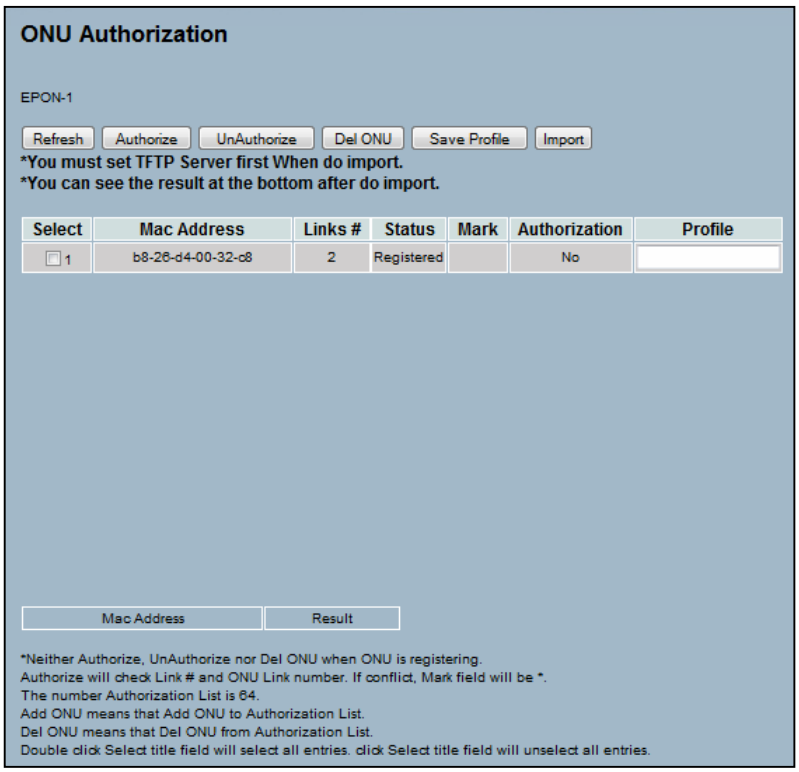


Figure 4-34: The ONU Authorization Screen

Parameter description

- **Mac Address:** The Mac Address is the unique identity of an ONU.
- **Link #:** Total number of logical links provisioned on an ONU.
- **Status:** The status displayed on the ONU. It include “Registered” and “ ”. “Registered” represent ONU on line. “ ” represent ONU not Registered.
- **Mark:** When clicking on Authorize, it will check Link # and ONU Link number. If there’s a conflict, Mark field will be *.
- **Authorization:** It can be Yes or No. After the ONU is authorized, ONU SLA can be enabled.
- **Profile:** The profile file name is informed on this field.
- **Buttons:**

Refresh: Click to update the ONU authorization entry immediately.
Authorize: Click to Authorize the selected ONUs.
UnAuthorize: Click to UnAuthorize the selected ONUs.
Del ONU: Click to remove the selected ONUs from the Authorization list.
Save Profile: Click to save the profile using the TFTP Server.
Import: Click to import the profile to the ONUs.

On the ONU Authorization page is also possible to apply profiles.

1. Save the ONU profile on the root directory of the TFTP Server.
   Note: To save the profile, go to ONU Operations -> Configuration Export.
2. On the ONU Authorization page, input the file name on the Profile field for all ONUs you want to apply the profile.

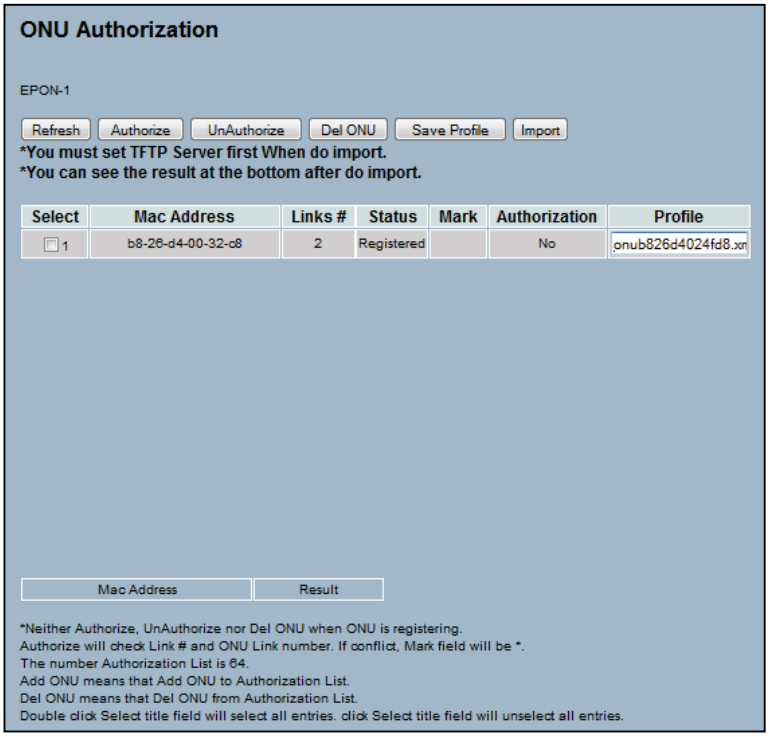


Figure 4-35: Setting the use of Profiles

3. Select the ONUs and then click on the button Save profile.
4. Select the ONUs again and then click on the Import button.
5. The status of the update will be shown on the table MAC Address/Result.

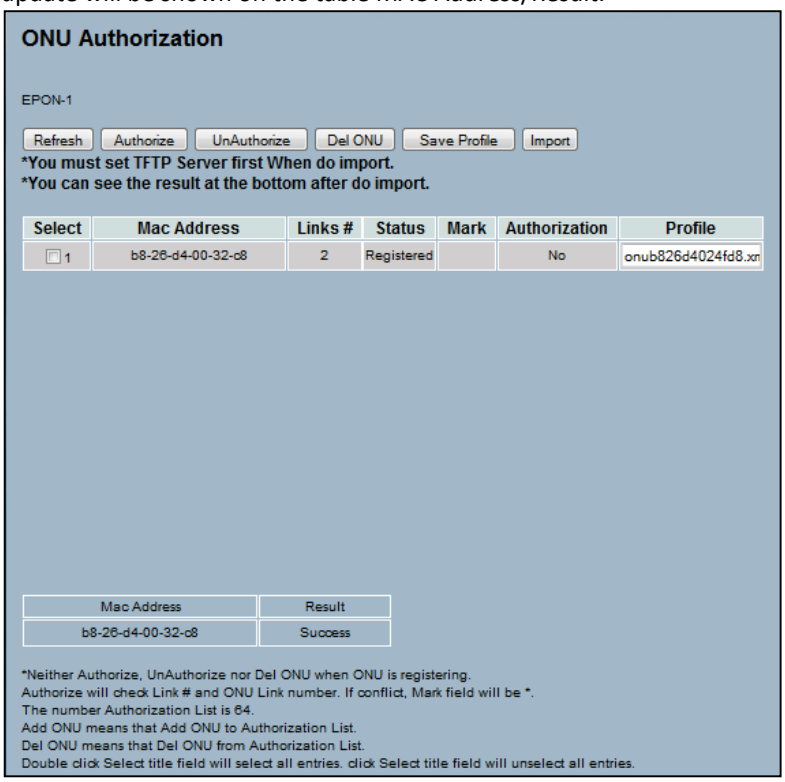


Figure 4-36: Applying Profiles

4.4 IONU Digital-IO

The IONU Digital-IO is a list that shows only the ONU model FK-IONU-DS connected to each of the EPON ports. This model of Industrial ONU has digital signal inputs and outputs to monitor devices connected to it, as Emergency Phones, for example.
The column DI-4, from the table below, shows the status of the device.
Hang Off: The device is in standby.
Pick up: The device is operational.
To send a signal to wake up the connected device, select the ONU and click on the button "DO-1 Send Wakeup".

Figure 4-37: IONU Digital IO

5 Configuration

5.1 Trap Event Severity

This function is used to set an Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the OLT to send out the trap information while pre-defined trap events occur.

Web Interface

To configure the Trap Event Severity in the web interface:

1. Click Configuration and then Trap Event Severity Configuration.
2. Scroll to select the Group name and Severity Level
3. Click the Save.

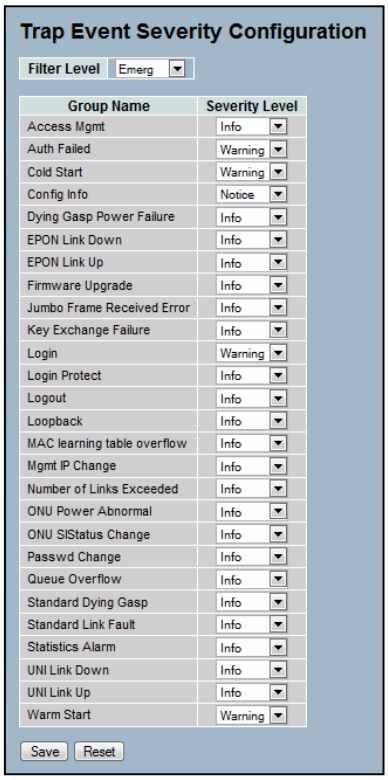


Figure 5-1: The Trap Event Severity Configuration Screen

Parameter description:

• **Group Name:** The name identifying the severity group.

• **Severity Level:** Every group has a severity level. The following level types are supported:

<0> Emergency: System is unusable.

<1> Alert: Action must be taken immediately.

<2> Critical: Critical conditions.

<3> Error: Error conditions.

<4> Warning: Warning conditions.

<5> Notice: Normal, but significant conditions.

<6> Information: Information messages.

<7> Debug: Debug-level messages.

• **Buttons**

Save: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

5.2 SMTP Configuration

Simple Mail Transfer Protocol is the message-exchange standard for the Internet. The OLT can be configured as a client of SMTP while the server is a remote device that will receive messages from the OLT about alarm events that occur.

Web Interface

To configure the in the web interface:

1. Click Configuration then SMTP Configuration
2. Specify the parameters.
3. Click Save.

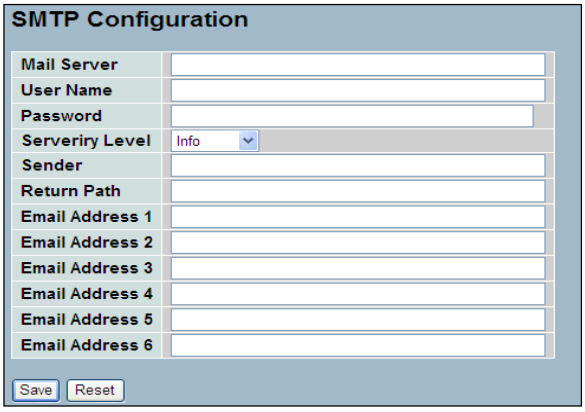


Figure 5-2: The SMTP Configuration Screen

Parameter description

- **Mail Server:** Specify the IP Address of the mail server.
- **Username:** Specify the username of the mail server.
- **Password:** Specify the password of the mail server.
- **Sender:** Sets the sender's mail name.
- **Return-Path:** Sets the mail return-path as the sender's mail address.
- **Email Address 1-6:** Email address that will receive the alarm message.
- **Buttons:**

Save: Click to apply changes.

Reset: Click to undo any changes made locally and revert to previously saved values.

6 Security

6.1 AAA

This section shows you how to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server.

6.1.1 Configuration

This section describes how to configure AAA settings of TACACS+ or RADIUS server.

Web Interface

To configure an AAA server in the web interface:
1. Click Security, AAA and then Configuration.
2. Set Timeout (Default is 15 seconds).
3. Set Dead Time (Default is 300 seconds).

To configure a TACACS+ Authorization and Accounting Configuration of AAA in the web interface:
1. Select “Enabled” in the Authorization.
2. Select “Enabled” in the Failback to Local Authorization.
3. Select “Enabled” in the Account.

To configure a RADIUS Authentication Server Configuration of AAA in the web interface:
1. Check “Enabled”.
2. Specify IP address or Hostname for Radius Server.
3. Specify Authentication Port for Radius Server (Default is 1812).
4. Specify the Secret with Radius Server.

To configure a RADIUS Accounting Server Configuration of AAA in the web interface:
1. Check “Enabled”.
2. Specify IP address or Hostname for Radius Server.
3. Specify Accounting Port for Radius Server (Default is 1813).
4. Specify the Secret with Radius Server.

To configure a TACACS+ Authentication Server Configuration of AAA in the web interface:
1. Check “Enabled”.
2. Specify IP address or Hostname for TACACS+ Server.
3. Specify Authentication Port for TACACS+ Server (Default is 49).
4. Specify the Secret with TACACS+ Server.

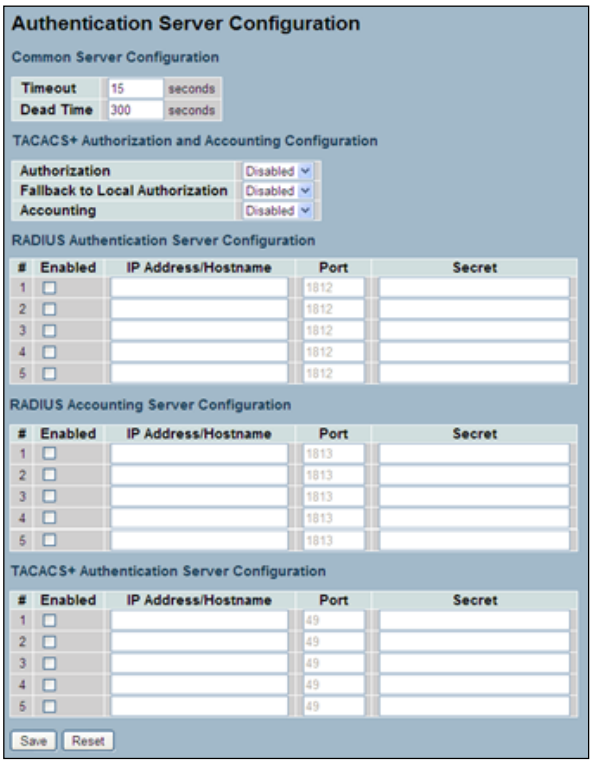


Figure 6-1: The Authentication Server Configuration Screen

Parameter description

• **Timeout:** The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum waiting time for a reply from the server.

If the server does not reply within this timeframe, it will be considered dead and try the next enabled server (if there is one).

RADIUS servers are using the UDP protocol, which is unreliable by design. In order to cope with lost frames, the timeout interval is divided into 3 subintervals of equal length. If a reply is not received within the subinterval, the request is transmitted again. This algorithm causes the RADIUS server to be queried up to 3 times before it is considered dead.

• **Dead Time:** The Dead Time, which can be set to a number between 0 and 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond a previous request. This will stop the switch from continually trying to contact a server that was already determined as dead.

Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured.

• **RADIUS Authentication Server Configuration:** The table has one row for each RADIUS Authentication Server and a number of columns, which are:

• **#:** The RADIUS Authentication Server number for which the configuration below applies.

• **Enabled:** Enables the RADIUS Authentication Server by checking this box.

• **IP Address/Hostname:** The IP address or hostname of the RADIUS Authentication Server. The IP address is expressed in dotted decimal notation.

• **Port:** The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server.

• **Secret:** The secret - up to 29 characters long - shared between the RADIUS Authentication Server and the switch stack.

• **RADIUS Accounting Server Configuration:** The table has one row for each RADIUS Accounting Server and a number of columns, which are:

• **#:** The RADIUS Accounting Server number for which the configuration below applies.

• **Enabled:** Enables the RADIUS Accounting Server by checking this box.

• **IP Address/Hostname:** The IP address or hostname of the RADIUS Accounting Server. The IP address is expressed in dotted decimal notation.

• **Port:** The UDP port to use on the RADIUS Accounting Server. If the port is set to 0 (zero), the default port (1813) is used on the RADIUS Accounting Server.
• **Secret:** The secret - up to 29 characters long - shared between the RADIUS Accounting Server and the switch stack.
• **TACACS+ Authentication Server Configuration:** The table has one row for each TACACS+ Authentication Server and a number of columns, which are:
• **#:** The TACACS+ Authentication Server number for which the configuration below applies.
• **Enabled**: Enables the TACACS+ Authentication Server by checking this box.
• **IP Address/Hostname:** The IP address or hostname of the TACACS+ Authentication Server. The IP address is expressed in dotted decimal notation.
• **Port:** The TCP port to use on the TACACS+ Authentication Server. If the port is set to 0 (zero), the default port (49) is used on the TACACS+ Authentication Server.
• **Secret:** The secret - up to 29 characters long - shared between the TACACS+ Authentication Server and the switch stack.

6.1.2 Radius Overview

This section shows you an overview of the RADIUS Authentication and Accounting server status to ensure the function is working.

Web Interface

To check the RADIUS Overview in the web interface:

1. Click Security, AAA and then Radius Overview.

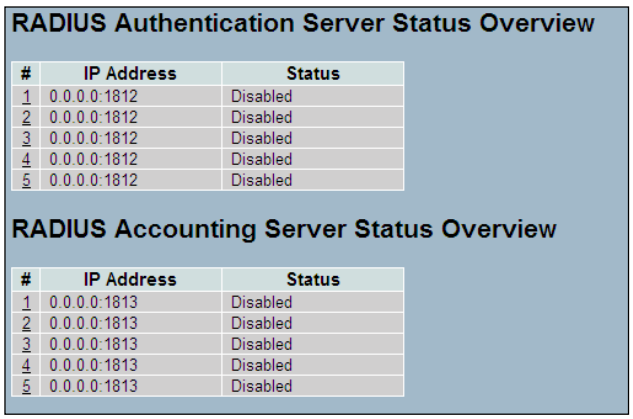


Figure 6-2: The Authentication Server Configuration illustration

Parameter description

- **#:** The RADIUS server number. Click to open the detailed statistics for this server.
- **IP Address:** The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server.
- **State:** The current state of the server. This field takes one of the following values:

Disabled: The server is disabled.
Not Ready: The server is enabled, but IP communication is not up and running.
Ready: The server is enabled, IP communication is up and running, and the RADIUS module is ready to accept accounting attempts.
Dead (X seconds left): Accounting attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled.

6.1.3 Radius Details

This section shows you detailed statistics of the RADIUS Authentication and Accounting servers. The statistics map is similar to those specified in RFC4668 - RADIUS Authentication Client MIB.

Web Interface

To check the RADIUS Detail in the web interface:

1. Click Security, AAA and then Radius Details.
2. Specify the Server which you want to check.

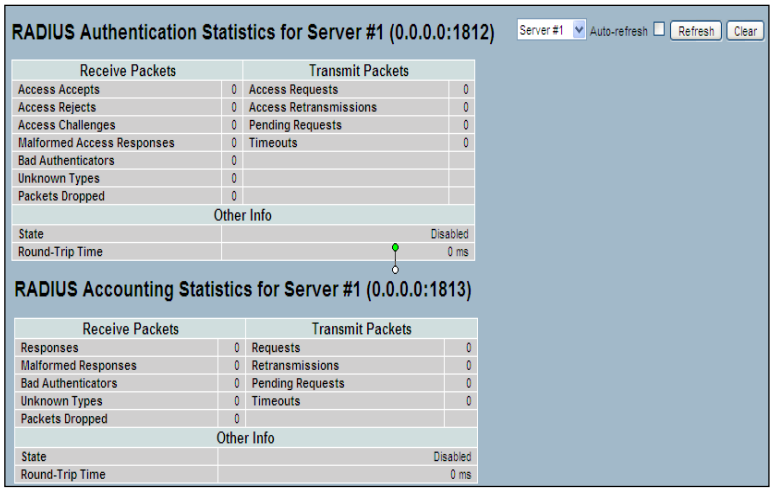


Figure 6-3: The RADIUS Server Statistics illustration

Parameter description

- **Auto-refresh:** It will update the table detail information automatically.
- **Refresh:** Updates the RADIUS Server detail statistics immediately and manually.
- **Clear:** Cleans the RADIUS Server detail statistics immediately and manually.

6.2 Access Management

6.2.1 Configuration

This section shows you how to configure the access management table of the OLT. The maximum entry number is 16. If the application's type matches any of the access management entries, it will allow access to the OLT.

Web Interface

To configure the Access Management in the web interface:

1. Click Security, Access Management and then Configuration.
2. Select “Enabled” in the Mode of Access Management Configuration.
3. Click “Add new entry”.
4. Specify the Start IP Address and End IP Address.
5. Check the Access Management method (HTTP/HTTPS, SNMP, and TELNET/SSH) in the entry.
6. Click Save.

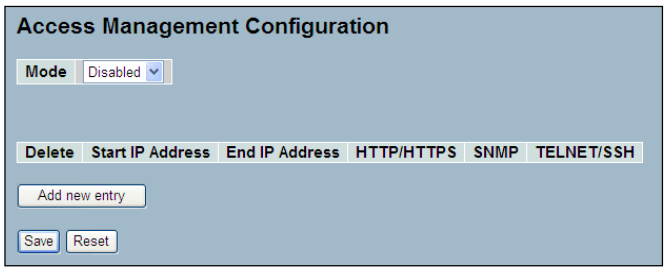


Figure 6-4: The Access Management Configuration

Parameter description

• **Mode:** Indicates the access management mode operation. Possible modes are:
Enabled: Enables access management mode operation.
Disabled: Disables access management mode operation.
• **Delete:** Check to delete the entry. It will be deleted during next save.
• **Start IP address:** Indicates the start IP address for the access management entry.
• **End IP address:** Indicates the end IP address for the access management entry.
• **HTTP/HTTPS:** Indicates that the host can access the switch from a HTTP/HTTPS interface, if the host IP address matches the IP address range provided in the entry.
• **SNMP:** Indicates that the host can access the switch from a SNMP interface, if the host IP address matches the IP address range provided in the entry.
• **TELNET/SSH:** Indicates that the host can access the switch from a TELNET/SSH interface, if the host IP address matches the IP address range provided in the entry.

6.2.2 Statistics

This section shows you a detailed statistics of the Access Management including HTTP, HTTPS, TELNET and SSH.

Web Interface

To check the Access Management Statistics in the web interface:

1. Click Security, Access Management and then Statistics.

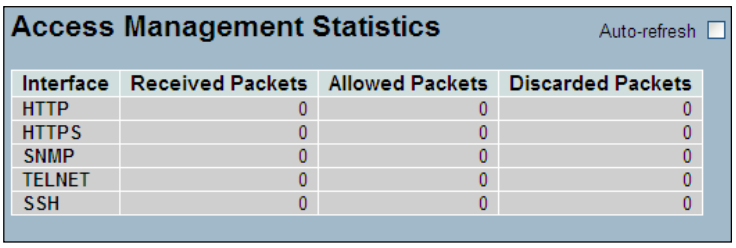


Figure 6-5: The Access Management Statistics

Parameter description

- **Interface:** The interface type through which the remote host can access the switch.
- **Received Packets:** Number of received packets from the interface when access management mode is enabled.
- **Allowed Packets:** Number of allowed packets from the interface when access management mode is enabled.
- **Discarded Packets:** Number of discarded packets from the interface when access management mode is enabled.

6.3 SSH

This section shows you how to use SSH (Secure Shell) to securely access the Device. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

Web Interface

To configure SSH in the web interface:

1. Click Security then SSH.
2. Select “Enabled” in the Mode of SSH Configuration.
3. Click Save.

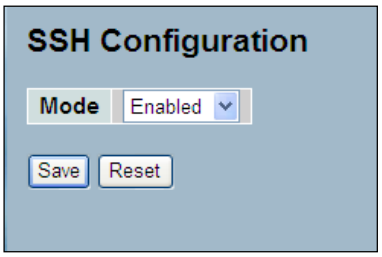


Figure 6-6: The SSH Configuration Screen

Parameter description

• **Mode:** Indicates the SSH mode operation. Possible modes are:
Enabled: Enables SSH mode operation.
Disabled: Disables SSH mode operation.
• **Buttons:**
Save: Click to apply changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.4 HTTPS

This section shows you how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via browser.

Web Interface

To configure HTTPS in the web interface:

1. Click Security then HTTPS.
2. Select “Enabled” in the Mode of HTTPS Configuration.
3. Select “Enabled” in the Automatic Redirect of HTTPS Configuration.
4. Click Save.

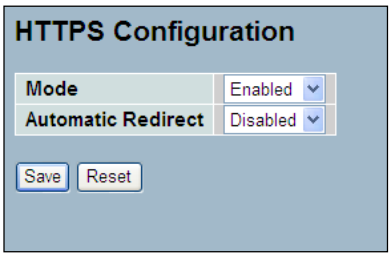


Figure 6-7: The HTTPs Configuration

Parameter description

• **Mode:** Indicates the HTTPS mode operation. Possible modes are:
Enabled: Enables HTTPS mode operation.
Disabled: Disables HTTPS mode operation.
• **Automatic Redirect:** Indicates the HTTPS redirects the mode operation. Automatically redirects the web browser to HTTPS when HTTPS mode is enabled. Possible modes are:
Enabled: Enables HTTPS redirect mode operation.
Disabled: Disables HTTPS redirect mode operation.
• **Buttons:**
Save: Click to apply changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

6.5 Auth Method

Web Interface

To configure an Authentication Method in the web interface:

1. Specify the Client (console, telnet, ssh, web) which you want to monitor.
2. Specify the Authentication Method (none, local, radius, tacacs+)
3. Checked Fallback.
4. Click Save.

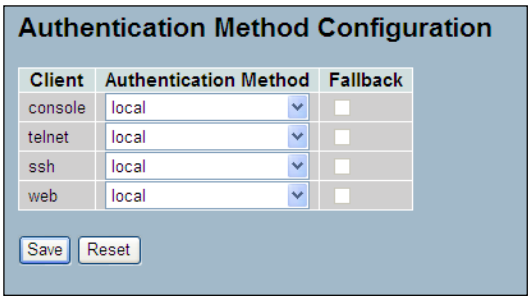


Figure 6-8: The HTTPs Configuration

Parameter description

- **Client:** The management client for which the configuration below applies.
- **Authentication Method:** Authentication Method can be set to one of the following values:
- **none**: authentication is disabled and login is not possible.
- **local**: use the local user database on the switch stack for authentication.
- **radius**: use a remote RADIUS server for authentication.
- **tacacs+**: use a remote TACACS+ server for authentication.
- **Fallback:** Enable fallback to local authentication by checking this box.

If none of the configured authentication servers are alive, the local user database is used for authentication.

Note: This is only possible if the Authentication Method is set to a value other than 'none' or 'local'.

- **Buttons:**

Save: Click to apply changes.
Reset: Click to undo any changes made locally and revert to previously saved values.

7 Maintenance

7.1 Restart Device

This section describes how to restart the OLT for any maintenance needs. Any configuration files or scripts that you saved in the device should still be available afterwards.

Web Interface

To Restart the device in the web interface:

1. Chick Maintenance then Restart Device.
2. Click Yes.

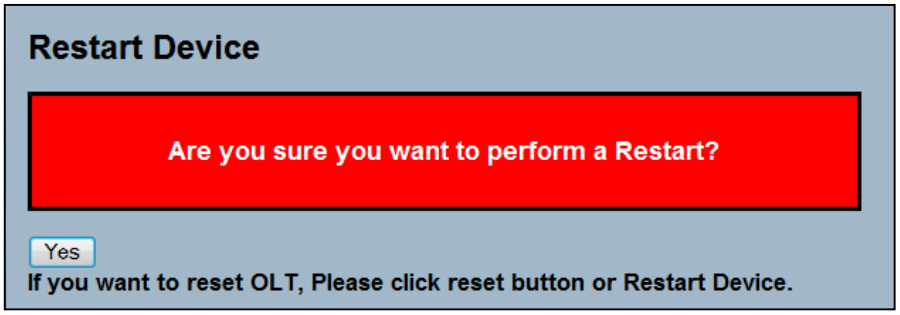


Figure 7-1: The Restart Device Screen

Parameter description

• **Yes :** Click the “Yes” button to immediately reboot the device.

7.2 Save and Restart Device

This section allows you to first save the configurations made before restarting the device.

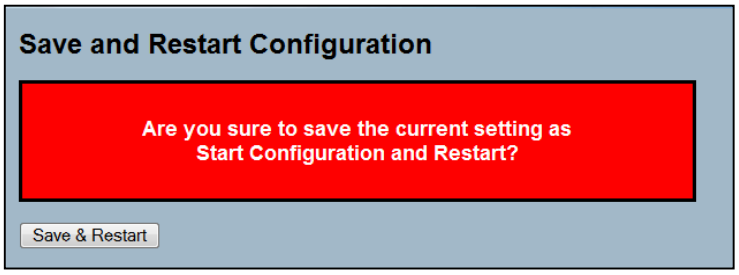


Figure 7-2: Save and Restart Device Screen

7.3 TFTP Server

This section allows you to configure the IP address of the TFTP Server.

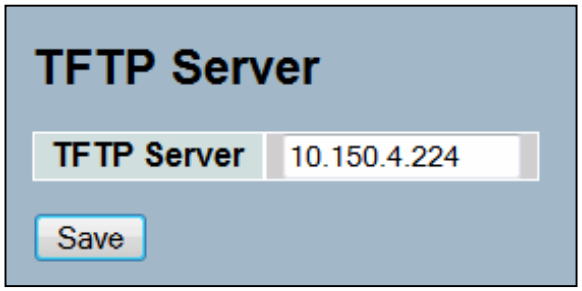


Figure 7-3: TFTP Server IP Configuration

7.4 Firmware

7.4.1 Firmware Upgrade

This section describes how to upgrade the device firmware.

Web Interface

To upgrade the firmware in the web interface:

1. Click Maintenance then Firmware Upgrade.
2. Click "Procurar" to select the firmware file.
3. Click Upload.

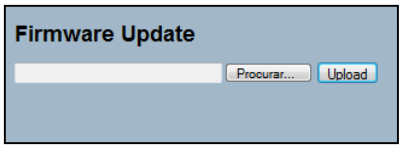


Figure 7-4: The Device Firmware update Screen

7.4.2 GEPON Firmware Upgrade

To upgrade the EPON chipset software in the web interface:

1. Click Maintenance then Firmware OLT Upgrade (EPON Firmware Upgrade).
2. Click "Procurar" to select the firmware file.
3. Click Upload.
4. Click Reboot.

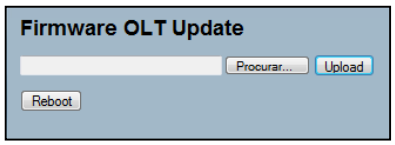


Figure 7-5: Chipset Firmware update Screen

7.4.3 Firmware ONU Upgrade

To upgrade the ONU firmware in the web interface:

1. Click Maintenance then Firmware ONU Upgrade.
2. Select the EPON port.
3. Select the ONUs that will be upgraded.
4. Click "Procurar" to select the firmware file.
5. Click Upload.
6. After the upgrade is finished, it's necessary to reboot the ONUs.

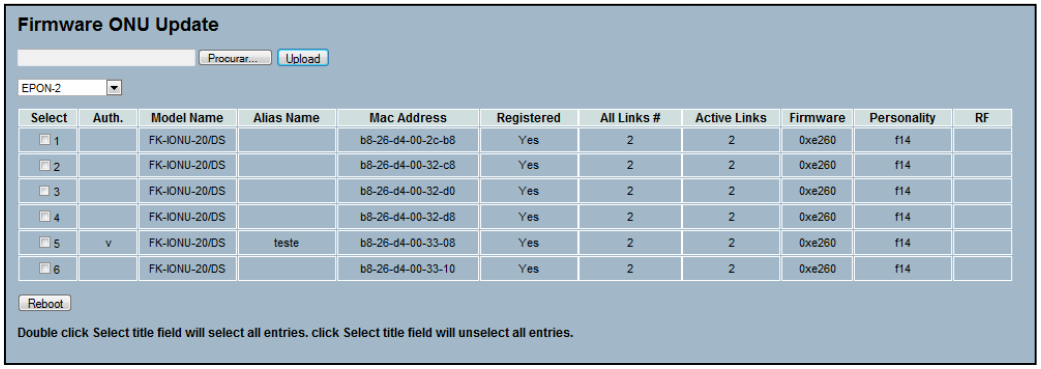


Figure 7-6: ONU Firmware Upgrade Screen

Note: This page is very useful to check the current firmware of the ONUs.

7.5 Save / Restore

This section describes how to save and restore the OLT configuration, including reset to Factory Defaults, Save Start, Save Users and Restore Users for any maintenance needs.

7.5.1 Factory Defaults

This section describes how to reset the OLT configuration to Factory Defaults. Any configuration files or scripts will recover to factory default values.

Web Interface

To reset the OLT to the Factory Default Configuration in the web interface:

1. Click Maintenance, Save/Restore and then Factory Defaults.
2. Click Yes.

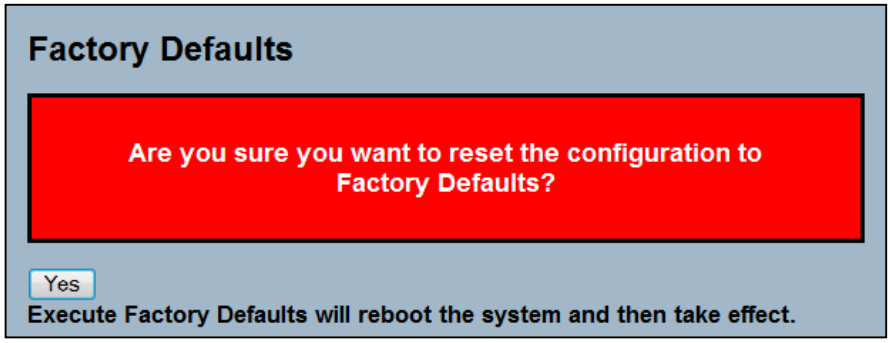


Figure 7-7: The Reset the device to Factory Defaults Screen

Parameter description

Yes: Click the “Yes” button to reset the OLT to the factory default configuration.
No: Click the “No” button to cancel the command.

7.5.2 Save Start

This section describes how to save the OLT Start configuration. Any current configuration files will be saved as XML format.

Web Interface

To save the current configuration as the startup configuration in the web interface:

1. Click Maintenance, Save/Restore and then Save Start.
2. Click Save.

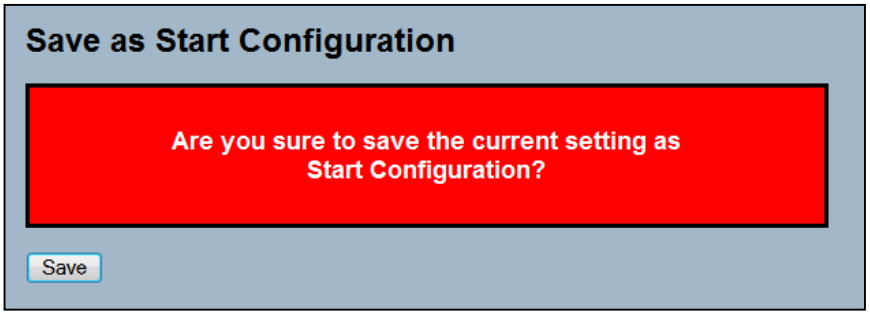


Figure 7-8: The save as start configuration Screen

Parameter description

Buttons:

- **Save:** Click to the current setting to become device start configuration.

7.5.3 Save User

Web interface

To save the current configuration as backup configuration in the web interface:

1. Click Maintenance, Save/Restore and then Save User.

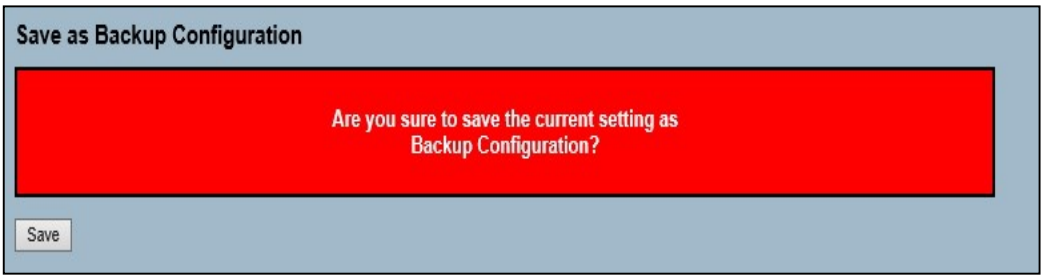


Figure 7-9: The save as back up configuration Screen

Parameter description:

• **Buttons**

Save: Click to save the configuration.

7.5.4 Restore User

Web interface

To apply the backup configuration to the equipment in the web interface:

1. Click Maintenance, Save/Restore and Restore User.

Figure 7-10: The Restore backup configuration Screen

Parameter description:

• **Buttons**

Save: Click to save the configuration.

7.6 Export/Import

7.6.1 Export Config

Web interface

To Export the current configuration via web interface:

1. Click Maintenance, Export/Import and then Export Config.
2. Click on Save Configuration
3. A window will appear in which the user will define where to save the file.

Figure 7-11: The Export Configuration Screen

Parameter description:

• **Buttons**

Save configuration: Click to save the configuration.

7.6.2 Import Config

Web interface

To import a configuration file in the web interface:

1. Click Maintenance, Export/Import and Import Config.
2. Select the file clicking on the button "Procurar".
3. Click on Upload.

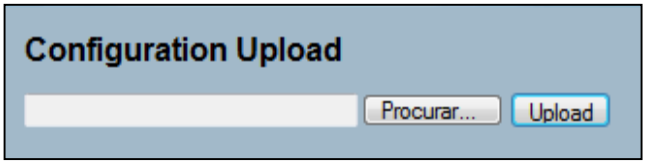


Figure 7-12: The Import Configuration Screen

7.6.3 Host/OLT/ONU Config Backup

Web interface

To configure the Host/OLT/ONU Config Backup in the web interface:

1. Click Maintenance, Export/Import and Host/OLT/ONU Config Backup.
2. Defines the TFTP Server IP address.
3. Defines the backup interval in days.
4. Defines the hour to make the backup.
5. Defines if the backup will be done just this one time, by selecting the One time option, or if it is going to be a periodic action.

If the One time is set, the Day must be 0 or 1. Day =0, Hour must >= current time hour. Day=1, Hour must < current time hour, which means that it is the next day backup.

If Periodic is set, the Day can’t be equal to 0.

If the One time is set and Periodic is not set, the backup is disabled.

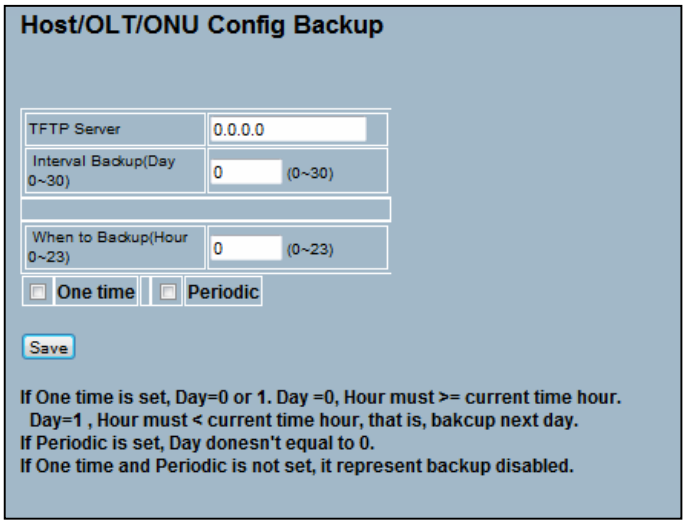


Figure 7-13: The Host/OLT/ONU Configuration Backup Screen

7.7 Diagnostics

This section provides a set of basic system diagnosis. It let users know whether the system is healthy or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

7.7.1 Ping

This section allows you to issue ICMP PING packets to troubleshoot IPv4 connectivity issues.
Web Interface

To perform an ICMP PING test in the web interface:
1. Click Maintenance, Diagnostics and then Ping.
2. Specify ICMP PING IP Address.
3. Specify ICMP PING Size.
4. Click Start.

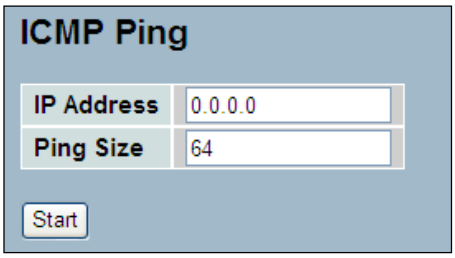


Figure 7-14: The ICMP Ping Screen

Parameter description
- **IP Address:** The destination IP Address.
- **Ping Size:** The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

NOTE: After you press Start, 5 ICMP packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

7.7.2 Ping6

This section allows you to issue ICMPv6 PING packets to troubleshoot IPv6 connectivity issues.
Web Interface

To perform an ICMPv6 PING test in the web interface:
1. Click Maintenance, Diagnostics and then Ping6.
2. Specify ICMPv6 PING IP Address.
3. Specify ICMPv6 PING Size.
4. Click Start.

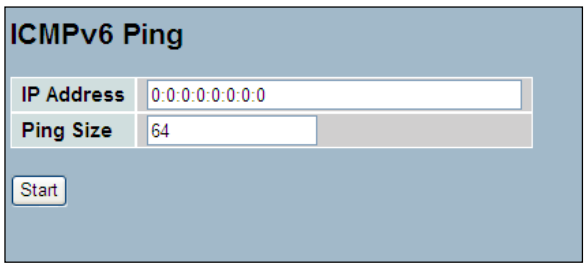


Figure 7-15: The ICMPv6 Ping Screen

Parameter description

- **IP Address:** The destination IP Address.
- **Ping Size:** The payload size of the ICMP packet. Values range from 8 bytes to 1400 bytes.

NOTE: After you press Start, 5 ICMPv6 packets are transmitted, and the sequence number and roundtrip time are displayed upon reception of a reply. The page refreshes automatically until responses to all packets are received, or until a timeout occurs.

7.7.3 Diag

Web interface

To use the Diag toll in the web interface:

1. Click Maintenance, Diagnostics and then Diagnostic.
2. Click on Start.

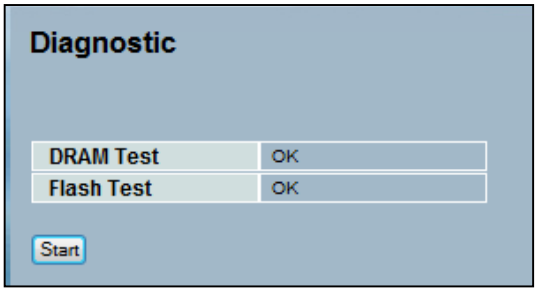


Figure 7-16: The Dignostic Screen

8 CLI Management

8.1 Initial Configuration

This chapter instructs you how to configure and manage the GEPON OLT through the CLI interface.
The RJ-45 serial port on the front panel is used to connect to device for out-of-band console configuration.

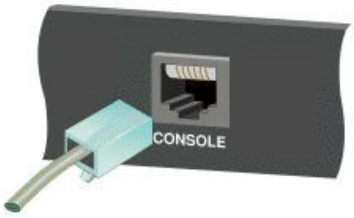


Figure 8-1: Plug in the Console Port

The command –line -driven configuration program can be accessed from a terminal or a PC running a terminal emulation program. The pin assignments used to connect to it are provided in the following table.

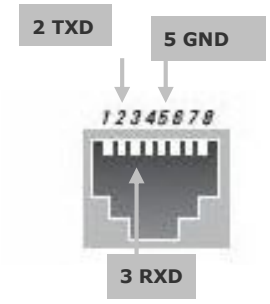


Figure 8-2: Serial Port (RJ-45) Pin-Out

Serial Cable Wiring

FK-C2-RADC's 8-Pin Serial Port	Null Modem	PC's 9-Pin DTE Port
2 RXD (receive data)	←----------	3 TXD (transmit data)
3 RXD (receive data)	----------→	2 RXD (receive data)
5 SGND (Signal ground)	----------	5 SGND (Signal ground)

NOTE: No other pins are used.

The serial port's configuration requirements are as follows:

- Default Baud rate—115,200 bps
- Character Size—8 Characters
- Parity—None
- Stop bit—One
- Data bits—8
- Flow control—none

The default username is **"admin"** and password is empty. For the first time to use, please enter the default username and password, and then click the **Enter** button. The login process now is completed.

8.2 AAA Commands of CLI

AAA

This section shows you to use an AAA (Authentication, Authorization, Accounting) server to provide access control to your network. The AAA server can be a TACACS+ or RADIUS server to create and manage objects that contain settings for using AAA servers.

AAA Commands in CLI

Command	Function
acc-radius	Configure RADIUS accounting Server
accounting	Configure Accounting mode
authorization	Configure Authorization mode
deadtime	Configure server dead time
fallback-author	Configure Authorization mode
radius	Configure RADIUS authentication server
show	Show AAA information
tacacs+	Configure TACACS+ authentication server
timeout	Configure server response timeout

acc-radius:

The command lets you configure the RADIUS accounting server parameter.

acc-radius <index> <enable/disable> <ip-hostname> <0-65535> <Line>

<index> The RADIUS accounting Server index. The available value is from 1 to 5

<disable/enable> To enable or disable the RADIUS accounting service.

<ip-hostname> The RADIUS accounting server IP address or hostname.

<0-65535> The RADIUS accounting server UDP port. If the port is set to 0 (zero), then the default port (1813) is used.

<LINE> Secret shared with external accounting server. The Available value is up to 29 characters long.

EXAMPLE:

```
Switch(aaa)# acc-radius 1 enable 192.168.2.22 65535 radius
Switch(aaa)# show config

Server Timeout    : 15 seconds
Server Dead Time : 300 seconds
TACACS+ Authorization and Accounting Configuration:
Authorization                  : Disable
Fallback to Local Authorization: Disable
Accounting                     : Disable
```

```
RADIUS Authentication Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ------------------------------
RADIUS Authentication Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ------------------------------

1      Disabled                           1812
2      Disabled                           1812
3      Disabled                           1812
4      Disabled                           1812
5      Disabled                           1812

RADIUS Accounting Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ------------------------------

1      Enabled  192.168.2.22               65535 radius
2      Disabled                           1813
3      Disabled                           1813
4      Disabled                           1813
5      Disabled                           1813

TACACS+ Authentication Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ------------------------------

1      Disabled                          49
2      Disabled                          49
3      Disabled                          49
4      Disabled                          49
```

accounting :

The command lets you enable or disable the RADIUS accounting operation mode.

Syntax: **accounting** <enable/disable>

Parameter :

<disable> Globally disable Accounting operation mode.

<enable> Globally enable Accounting operation mode.

EXAMPLE:

```
Switch(aaa)# accounting enable
Server disconnect!
Switch(aaa)# accounting disable
Switch(aaa)#
```

NOTE: If you didn't connect the RADIUS Server already then the switch will show "Server disconnect".

authorization:

To configure (enable/disable) RADIUS Authorization mode.

Syntax: **authorization** <enable/disable>

Parameter: **<disable>** Globally disable Authorization operation mode.

<enable> Globally enable Authorization operation mode.

EXAMPLE:

```
Switch(aaa)# authorization enable
Switch(aaa)#
```

deadtime:

The command lets you configure the RADIUS server deadtime.

Syntax: **deadtime** <0-3600>

Parameter: **<0-3600>** Time that a server is considered dead if it doesn't answer a request. The available value is from 0 to 3600 second

Default Setting: **None**

EXAMPLE:

```
Switch(aaa)# deadtime 3600
Server disconnect!
Switch(aaa)#
```

NOTE: If you didn't connect the RADIUS Server already then the switch will show "Server disconnect".

fallback-author:

The command lets you configure the fallback function of RADIUS authorization with enable/disable if remote authorization fails.

Syntax: **fallback-author** <disable/ enable>.

Parameter: **<disable>** Disable fallback function.

<enable> Enable fallback function if remote authorization fails.

EXAMPLE:

```
Switch(aaa)# fallback-author enable
Server disconnect!
```

NOTE: If you didn't connect the RADIUS Server already then the switch will show "Server disconnect".

radius:

The command lets you configure the RADIUS Server detail parameter.

Syntax: **radius** <index> <enable/disable> <ip-hostname> <0-65535> <Line> .

Parameter: **<index>** The RADIUS accounting Server index. The available value is from 1 to 5

<disable/enable> To enable or disable the RADIUS accounting service.

<ip-hostname> The RADIUS accounting server IP address or hostname.

<0-65535> The RADIUS accounting server UDP port. If the port is set to 0 (zero), then the default port (1813) is used.

<LINE> Secret shared with external accounting server. The Available value is up to 29 characters long.

EXAMPLE:

```
Switch(aaa)# radius 1 enable 192.168.2.22 0 radius
Server disconnect!
```

NOTE: If you didn't connect the RADIUS Server already then the switch will show "Server disconnect".

Show:

The command lets you display the RADIUS AAA information.

Syntax:	**Show** <config>
	Show <statistics> <1-5>
Parameter:	**<config>** To show AAA configuration
	<statistics> To show RADIUS statistics
	<1-5> The RADIUS Server Index

EXAMPLE:

```
Switch(aaa)# show config

Server Timeout    : 15 seconds
Server Dead Time : 300 seconds

TACACS+ Authorization and Accounting Configuration:
Authorization                  : Disable
Fallback to Local Authorization: Disable
Accounting                     : Disable

RADIUS Authentication Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ----------------------------
--

1      Disabled                           1812
2      Disabled                           1812
3      Disabled                           1812
4      Disabled                           1812
5      Disabled                           1812

RADIUS Accounting Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ----------------------------
--

1      Disabled                           1813
2      Disabled                           1813
3      Disabled                           1813
4      Disabled                           1813
5      Disabled                           1813

TACACS+ Authentication Server Configuration:
Server Mode     IP Address or Host Name     Port  Secret
------ -------- -------------------------- ----- ----------------------------
--

1      Disabled                         49
2      Disabled                         49
3      Disabled                         49
4      Disabled                         49
5      Disabled                         49
```

```
Switch(aaa)#  show statistics 1

Server #1 (0.0.0.0:1812) RADIUS Authentication Statistics:
Rx Access Accepts                    0  Tx Access Requests                  0
Rx Access Rejects                    0  Tx Access Retransmissions           0
Rx Access Challenges                 0  Tx Pending Requests                 0
Rx Malformed Acc. Responses          0  Tx Timeouts                         0
Rx Bad Authenticators                0
Rx Unknown Types                     0
Rx Packets Dropped                   0
State:                         Disabled
Round-Trip Time:                     0 ms

Server #1 (0.0.0.0:1813) RADIUS Accounting Statistics:
Rx Responses                         0  Tx Requests                         0
Rx Malformed Responses               0  Tx Retransmissions                  0
Rx Bad Authenticators                0  Tx Pending Requests                 0
Rx Unknown Types                     0  Tx Timeouts                         0
Rx Packets Dropped                   0
State:                         Disabled
Round-Trip Time:                     0 ms
Switch(aaa)#
```

tacacs+ :

The command lets you configure the TACACS+ authentication server detail parameter

Syntax: **tacacs+** <index> <enable/disable> <ip-hostname> <0-65535> <Line>

Parameter:

<index> The TACACS+ authentication Server index. The available value is from 1 to 5

<disable/enable> To enable or disable the TACACS+ authentication service.

<ip-hostname> The TACACS+ authentication server IP address or hostname.

<0-65535> The TACACS+ authentication server UDP port. If the port is set to 0 (zero), then the default port (1813) is used.

<LINE> Secret shared with external accounting server. The Available value is up to 29 characters long.

EXAMPLE:

```
Switch(aaa)# tacas+ 1 enable 192.168.2.22 0 tacacs
Server disconnect!
```

NOTE: If you didn't connect the RADIUS Server already then the switch will show "Server disconnect".

timeout :

The command lets you configure server response timeout

Syntax: **timeout** <3-3600>

Parameter: **<3-3600>** The Timeout, which can be set to a number between 3 and 3600 seconds, is the maximum time to wait for a reply from a server.

EXAMPLE:

```
Switch(aaa)# timeout 360
Switch(aaa)#
```

8.3 Access Commands of CLI

Access

This section shows you to configure access management table of the Switch including HTTP/HTTPS, SNMP, and TELNET/SSH. You can manage the Switch over an Ethernet LAN, or over the Internet.

Access Commands in CLI

Command	Function
add	Add or modify access management entry
clear	Clear access management statistics
delete	Delete access management entry
mode	Configure the access management mode
show	Show access management information

add:

The command lets you add or modify access management entry.

Syntax: **add** <1-16> <ipv4/ipv6> <ip-address> <ip-address> <all> <snmp> <telnet> <web>

Parameter:

<1-16> To set the entry index

<ipv4> IPv4 format address

<ipv6> IPv6 format address

<ip-address> Start IP address

<ip-address> End IP address

<all> All interfaces what the switch physical ports

<snmp> To set the SNMP interface

<telnet> To set up the TELNET/SSH interface

<web> To set the HTTP/HTTPS interface

EXAMPLE:

```
Switch(access)# add 1 ipv4 192.168.1.1  192.168.1.241 all
Switch(access)# show config
Access Management Mode : Disabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH
Index Start IP Address                End IP Address                W S T
----- ------------------------------ ------------------------------ - - -
1     192.168.1.1                     192.168.1.241                 Y Y Y
Switch(access)#
```

clear:

The command lets you clear access management statistics

Syntax: **Clear** < statistics>

Parameter: **<None>** Clear access management statistics

EXAMPLE:

```
Switch(access)# clear statistics
Switch(access)#
```

delete:

The command lets you delete access management entry.

Syntax: **Delete** <1-16>

Parameter: **<1-16>** Entry index

EXAMPLE:

```
Switch(access)# delete  1
Switch(access)# show config
Access Management Mode : Disabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH
Index Start IP Address                End IP Address                W S T
----- ------------------------------- ------------------------------ - - -
Switch(access)#
```

mode:

The command lets you configure the access management mode.

Syntax: **mode** <disable> <enable>

Parameter: **<disable>** Disable access management mode operation

<enable> Enable access management mode operation

EXAMPLE:

```
Switch(access)# mode enable
Switch(access)#
Switch(access)# show config
Access Management Mode : Enabled
W: WEB/HTTPS
S: SNMP
T: TELNET/SSH
Index Start IP Address                End IP Address                W S T
----- ------------------------------- ------------------------------ - - -
1     192.168.2.22                    192.168.2.250                 Y Y Y
Switch(access)#
```

show:

The command lets you display access setting information

Syntax: **show** < config> / < statistics>

Parameter: **<config>** Show access management configuration

<statistics> Show access management statistics

EXAMPLE:

```
Switch(access)# show config

Access Management Mode : Enabled

W: WEB/HTTPS
S: SNMP
T: TELNET/SSH
 Index Start IP Address               End IP Address                W S T
----- ------------------------------- ------------------------------
```

```
Switch(access)# show statistics
Client  Receive     Allow       Discard
------  ----------  ----------  ----------
HTTP    0           0           0
HTTPS   0           0           0
SNMP    0           0           0
TELNET  0           0           0
SSH     0           0           0
```

8.4 Account Commands of CLI

Account

In this function, only administrator can create, modify or delete the username and password. Administrator can modify other guest identities' password without confirming the password but it is necessary to modify the administrator-equivalent identity. Guest-equivalent identity can modify his password only. Please note that you must confirm administrator/guest identity in the field of Authorization in advance before configuring the username and password. Only one administrator is allowed to exist and unable to be deleted. In addition, up to 4 guest accounts can be created.

Account Commands

Command	Function
add	Add or modify user account
delete	Delete user account
show	Show user account information

add:

This command lets you add or modify user account.

Syntax: **add** <1-15> <word> <word>

Parameter: **<1-15>** User privilege level

<WORD> Up to 32 characters to identify the user name

<WORD>: The password for this user name

EXAMPLE:

```
Switch(account)# add 10 david david
Switch(account)# show
User Name                       Privilege Level
------------------------------- ---------------
admin                                        15
david                                        10
```

delete:

This command lets you delete a new operator user or you add one in the switch.

Syntax: **delete** <WORD>

Parameter: **<WORD>** Up to 32 characters to identify the user name

EXAMPLE:

```
Switch(account)# delete 12
Switch(account)# show
User Name                       Privilege Level
------------------------------- ---------------
admin                                        15
Switch(account)#
```

show :

The command lets you display user account information what you set in the switch.

Syntax: **Show** <name>

Parameter: **<name>** Up to 32 characters to identify the user name

EXAMPLE:

```
Switch(account)# show
User Name                      Privilege Level
------------------------------ ---------------
admin                                       15
Switch(account)#
```

8.5 Auth Commands of CLI

Auth

This page shows how to configure a user with authenticated when he logs into the switch via one of the management client interfaces.

Auth Method Commands

Command	Function
fallback	Configure local authentication fallback
method	Configure authentication method
show	Show Authentication configuration

fallback:

The command lets you configure the local authentication fallback function.

Syntax: **fallback** < console>/< ssh >/ < telnet >/ < web >, disable/enable

Parameter:

<console> Settings the authenticate method fallback via console

<ssh> Settings the authenticate method fallback via ssh

<telnet> Settings the authenticate method fallback via telnet

<web> Settings the authenticate method fallback via web

disable Disable local authentication if remote authentication fails

enable Enable local authentication if remote authentication fails

EXAMPLE:

```
Switch(auth)# fallback ssh disable
Switch(auth)#
```

method :

The command lets you configure Authentication method function

Syntax: **method** < console>/< ssh >/ < telnet >/ < web >, local / none / radius / tacats+

Parameter:

<console> Settings the authenticate method via console

<ssh> Settings the authenticate method via ssh

<telnet> Settings the authenticate method via telnet

<web> Settings the authenticate method via web

local Use local authentication

none Authentication disabled

telnet Use remote RADIUS authentication

tacacs+ Use remote TACACS+ authentication

EXAMPLE:

```
Switch(auth)# method ssh local
Switch(auth)#
```

show:

The command lets you display the ARP inspection configuration information.

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(auth)# show
Client   Authentication Method  Local Authentication Fallback
-------  ---------------------  ------------------------------
console  local                  Disabled
telnet   local                  Disabled
ssh      local                  Disabled
web      local                  Disabled10B   Disabled
```

8.6 Config-file Commands of CLI

Config-file

This section describes how to export and import the GEPON configuration. Any current configuration files will be exported as XML format.

Config-file Commands

Command	Function
export	Export configuration file to TFTP server
export-olt	Export OLT configuration file to TFTP server
export-onu	Export configuration file to TFTP server
import	Import configuration file from TFTP server
import-olt	Import OLT configuration file from TFTP server
import-onu	Import configuration file from TFTP server

export:

The command lets you run the export function to export the switch configuration to TFTP server.**Syntax:** **export** < ip-address> <WORD>

Parameter : **<ip-address>:** The TFTP server ip address

<WORD>: Configuration file name

EXAMPLE:

```
Switch(config-file)# export 192.168.1.100  testfile
Switch(config-file)#
```

export-olt:

The command lets you Export OLT configuration file to TFTP server.

Syntax: **export-olt** < ip-address> <WORD>

Parameter: **<ip-address>:** The TFTP server ip address

<WORD>: Configuration file name

EXAMPLE:

```
Switch(config-file)# export-olt 192.168.0.1 bbb
Switch(config-file)#
```

export-onu:

The command lets you Export configuration file to TFTP server

Syntax: **export-onu** < ip-address> <mac-address> <WORD>

Parameter: **<ip-address>:** The TFTP server ip address

<mac-address>: ONU

<WORD>: Configuration file name

EXAMPLE:

```
Switch(config-file)# export-onu 192.168.1.1 12-21-12-12-22-12 ccc
```

import:

The command lets you Import configuration file from TFTP server.

Syntax: **import** < ip-address> <WORD>

Parameter: **<ip-address>:** The TFTP server ip address

<WORD>: Configuration file name

EXAMPLE:

```
Switch(config-file)# import 192.168.1.100  testfile
Switch(config-file)#
```

import-olt:

The command lets you Import OLT configuration file from TFTP server.

Syntax: **import-olt** < ip-address> <WORD> check/ <cr>

Parameter: **<ip-address>:** The TFTP server ip address

<WORD>: Configuration file name

check: Check configuration file only

EXAMPLE:

```
Switch(config-file)# import-olt 192.168.1.1 ddd check
```

import-onu:

The command lets you Import configuration file from TFTP server.

Syntax: **import-onu** < ip-address> <mac-address> <WORD> check/ <cr>

Parameter: **<ip-address>:** The TFTP server ip address

<mac-address>: ONU

<WORD>: Configuration file name

check: Check configuration file only

EXAMPLE:

```
Switch(config-file)# import-onu 192.168.1.1 22-22-22-22-22-22 nnn check
```

8.7 Diagnostic Commands of CLI

Diagnostic

This section provides a set of basic system diagnosis. It let users know that whether the system is health or needs to be fixed. The basic system check includes ICMP Ping, ICMPv6, and VeriPHY Cable Diagnostics.

Diagnostic Commands

Command	Function
diag	Diagnostic Ram, Flash if OK
ping	Uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.
ping6	Uses the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway

diag:

The command lets you test the RAM and the FLASH status.

Syntax: **diag**

EXAMPLE:

```
Switch(diagnostic)# diag
DRAM Test: OK
Flash Test: OK
```

ping:

The command lets you to use the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway.

Syntax: **ping** <ip-hostname> <60-1400>

Parameter: **<ip-hostname>:** Hostname or IP address

<60-1400>: Size of ICMP echo packet

EXAMPLE:

```
Switch(diagnostic)# ping 192.168.6.127 1400
PING server 192.168.6.127
1400 bytes from 192.168.6.127: icmp_seq=0, time=10ms
1400 bytes from 192.168.6.127: icmp_seq=1, time=0ms
1400 bytes from 192.168.6.127: icmp_seq=2, time=0ms
1400 bytes from 192.168.6.127: icmp_seq=3, time=0ms
1400 bytes from 192.168.6.127: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
```

ping6:

The command lets you to use the ICMP protocol's mandatory ECHO_REQUEST datagram to elicit an ICMP ECHO_RESPONSE from a host or gateway

Syntax: **ping6** <ipv6-address> <60-1400>

Parameter: **<ipv6-address>** The parameter you need to type IPv6 address

<60-1400> Size of ICMP echo packet

EXAMPLE:

```
Switch(diagnostic)# ping6 ff06:0:0:0:0:0:0:c3 80
PING6 server ff06::c3, 80 bytes of data.
88 bytes from 192.168.6.200: icmp_seq=0, time=0ms
88 bytes from 192.168.6.200: icmp_seq=1, time=0ms
88 bytes from 192.168.6.200: icmp_seq=2, time=0ms
88 bytes from 192.168.6.200: icmp_seq=3, time=0ms
88 bytes from 192.168.6.200: icmp_seq=4, time=0ms
Sent 5 packets, received 5 OK, 0 bad
Switch(diagnostic)#
```

8.8 Event Commands of CLI

Event

The function is used to set an Alarm trap and get the Event log. The Trap Events Configuration function is used to enable the switch to send out the trap information while pre-defined trap events occurred.

Event Commands

Command	Function
filter-lvl	Set trap event severity level filter level
group	Configure trap event severity level
show	Show trap event configuration

filter-lvl:

The command lets you Set trap event severity level filter level.

Syntax: **filter-lvl** <0-8>

Parameter: **<0-8>:** Severity level; 0: Emergency,1: Alert,2: Critical,3: Error,4: Warning,5: Notice,6: Informational,7: Debug,8: No Filter

EXAMPLE:

```
Switch(event)# filter-lvl 0
Switch(event)# show
Filter Level : Emergency
Group Name                      Severity Level
------------------------------  ----------------
Access_Mgmt                     Info
Auth_Failed                     Warning
Cold_Start                      Warning


Switch(event)# filter-lvl 5
Switch(event)# show
Filter Level : Notice
Group Name                      Severity Level
------------------------------  ----------------
Access_Mgmt                     Info
Auth_Failed                     Warning
Cold_Start                      Warning


Switch(event)# filter-lvl 8
Switch(event)# show
Filter Level :
Group Name                      Severity Level
------------------------------  ----------------
Access_Mgmt                     Info
Auth_Failed                     Warning
Cold_Start                      Warning
```

group:

The command lets you to configure trap event severity level.

Syntax: **Group** <group-name> <port-list>

Parameter:

<group-name> Trap event group name
<0-7> Severity level
- **<0>** Emergency: system is unusable
- **<1>** Alert: action must be taken immediately
- **<2>** Critical: critical conditions
- **<3>** Error: error conditions
- **<4>** Warning: warning conditions
- **<5>** Notice: normal but significant condition
- **<6>** Informational: informational messages
- **<7>** Debug: debug-level messages

EXAMPLE:

```
Switch(event)# group acl 5
Switch(event)# show
Group Name                      Severity Level
------------------------------  ---------------
ACL                             Notice
ACL_Log                         Debug
Access_Mgmt                     Info
Auth_Failed                     Warning
Cold_Start                      Warning
Config_Info                     Info
Firmware_Upgrade                Info
Import_Export                   Info
LACP                            Info
Passwd_Change                   Info
Port_Security                   Info
Thermal_Protect                 Info
VLAN                            Info
Warm_Start                      Warning
Switch(event)#
```

Show:

The command lets you display trap event configuration what you set on the switch.

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(event)# show
Filter Level :
Group Name                       Severity Level
-------------------------------  ---------------
Access_Mgmt                      Info
Auth_Failed                      Warning
Cold_Start                       Warning
Config_Info                      Notice
Dying_Gasp_Power_Failure         Info
EPON_Link_Down                   Info
EPON_Link_Up                     Info
Firmware_Upgrade                 Info
Jumbo_Frame_Received_Error       Info
Key_Exchange_Failure             Info
Login                            Warning
Login Protect                    Info
Logout                           Info
Loopback                         Info
MAC_learning_table_overflow      Info
Mgmt_IP_Change                   Info
Number_of_Links_Exceeded         Info
OLT_Bad                          Info
ONU_Power_Abnormal               Info
Passwd_Change                    Info
Queue_Overflow                   Info
Standard_Dying_Gasp              Info
Standard_Link_Fault              Info
Statistics_Alarm                 Info
UNI_Link_Down                    Info
UNI_Link_Up                      Info
Warm_Start                       Warning
```

8.9 Firmware Commands of CLI

firmware

This section describes how to upgrade Firmware. The GEPON can be enhanced with more value-added functions by installing firmware upgrades.

firmware Commands

Command	Function
oltreboot	Reset(Reboot) OLT
oltupgrade	Upgrade OLT firmware
onureboot	reset ONUs
onuupgrade	Upgrade ONUs firmware
show	Show information about active and alternate firmware images
upgrade	Upgrade system firmware

oltreboot:

The command lets you Reset(Reboot) OLT.

Syntax: **oltreboot** <cr>

Parameter: **<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(firmware)# oltreboot
Switch(firmware)# +M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7424 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12-Vitesse - built 19:19:16, Apr 18 2011

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x84000000 [0x80021198-0x83fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x806c04b8
RedBoot> go

Username:
```

oltupgrade:

The command lets you Upgrade OLT firmware.

Syntax: **oltupgrade** <ip-hostname> <WORD>

Parameter: **<ip-hostname>:** TFTP server ip address or hostname

<WORD>: Firmware image file name

EXAMPLE:

```
Switch(firmware)# oltupgrade 192.168.20.20 FK-C2-RADC_v1.11
Upgrading firmware ...
```

onureboot:

The command lets you reset ONUs.

Syntax: **onureboot** epon-0/epon-1 <onu-list>

Parameter: **epon-0:** Port: epon-0

epon-1: Port: epon-1

<onu-list>: ONUs range : available from 1 to 64.

EXAMPLE:

```
Switch(firmware)# onureboot epon-0 1
Switch(firmware)#
```

onuupgrade:

The command lets you Upgrade ONUs firmware.

Syntax: **onuupgrade** <ip-hostname> <WORD> epon-0/ epon-1 <onu-list>

Parameter: **<ip-hostname>:** TFTP server ip address or hostname

<WORD>: Firmware image file name

epon-0: Port: epon-0

epon-1: Port: epon-1

<onu-list>: ONUs range : available from 1 to 64.

EXAMPLE:

```
Switch(firmware)# onuupgrade 192.168.20.20 aaa_v1.11.dat epon-0 1
Upgrading firmware ...
```

show:

The command lets you Show ONUs Information command.

Syntax: **show** epon-0/ epon-1

Parameter: **epon-0:** Port: epon-0

epon-1: Port: epon-1

EXAMPLE:

```
Switch(firmware)# show epon-0
Show ONUs in epon-0 Information
No model name       onu mac address
-- ---------------- -----------------
 1 FK-IONU-20       b8-26-d4-00-21-d8

Switch(firmware)# show epon-1
No active onu to upgrade.
Switch(firmware)#
```

upgrade :

The command lets you upgrade the system firmware to active or alternate division

Syntax: **upgrade** <ipv6-address>/ <ip-hostname> <word>

Parameter:

<ipv6-address>: TFTP server ipv6 address. IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separate each field (:).For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'.

<ip-hostname>: TFTP server ip address or hostname

<word>: Firmware image file name

EXAMPLE:

```
Switch(firmware)# upgrade 192.168.1.100 bbb.bk
Switch(firmware)# show epon-0
Show ONUs in epon-0 Information
No model name       onu mac address
-- ---------------- -----------------
 1 FK-IONU-20       b8-26-d4-00-21-d8
```

8.10 HTTPs Commands of CLI

Https

This section shows you how to use HTTPS to securely access the Switch. HTTPS is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication via the browser.

HTTPs Commands

Command	Function
mode	Configure the HTTPS mode
redirect	Configure the HTTPS redirect mode
show	Show the HTTPs configuration

mode:

The command lets you configure the HTTPs enable or disable.

Syntax: **mode** disable/enable

Parameter: **disable:** The parameter lets you to disable HTTPS mode operation

enable: The parameter lets you to enable HTTPS mode operation

EXAMPLE:

```
Switch(https)# mode enable
Switch(https)# show
HTTPS Mode          : Enabled
HTTPS Redirect Mode : Disabled
```

redirect:

The command lets you to configure the HTTPs redirect mode enable or disable.

Syntax: **redirect** disable/enable

Parameter: **disable:** The parameter lets you to disable HTTPS redirect mode operation

enable: The parameter lets you to enable HTTPS redirect mode operation

EXAMPLE:

```
Switch(https)# redirect enable
ERROR! Can not enable HTTPS redirect function when the HTTPS operation mode
is disabled.

Switch(https)# mode enable
Switch(https)# redirect enable
Switch(https)# show
HTTPS Mode          : Enabled
HTTPS Redirect Mode : Enabled
```

show:

The command lets you to display the HTTPs all setting or status information.

Syntax: **show** <cr>

Parameter: **<cr>:** means no parameter needed to type..

EXAMPLE:

```
Switch(https)# show
HTTPS Mode          : Enabled
HTTPS Redirect Mode : Enabled
Switch(https)#
```

8.11 IP Commands of CLI

IP

IP is an acronym for Internet Protocol. It is a protocol used for communicating data across an internet network. IP is a "best effort" system, which means that no packet of information sent over is assured to reach its destination in the same condition it was sent. Each device connected to a Local Area Network (LAN) or Wide Area Network (WAN) is given an Internet Protocol address, and this IP address is used to identify the device uniquely among all other devices connected to the extended network.

The current version of the Internet protocol is IPv4, which has 32-bits Internet Protocol addresses allowing for in excess of four billion unique addresses. This number is reduced drastically by the practice of webmasters taking addresses in large blocks, the bulk of which remain unused. There is a rather substantial movement to adopt a new version of the Internet Protocol, IPv6, which would have 128-bits Internet Protocol addresses. This number can be represented roughly by a three with thirty-nine zeroes after it. However, IPv4 is still the protocol of choice for most of the Internet.

IP Commands

Command	Function
dhcp	Enable/Disable DHCP client
name-server	Set DNS IP address
setup	Set the IP address
show	Show ip information

dhcp:

The command lets you to configure the DHCP client.

Syntax: **dhcp** disable/ enable

Parameter: **disable:** Disable DHCP client

enable: Enable DHCP client

renew: Force DHCP client to renew IP address

EXAMPLE:

```
Switch(ip)# dhcp enable
Switch(ip)# show
DHCP Client          : Enabled
Active Configuration : Static
IP Address           : 0.0.0.0
Subnet Mask          : 0.0.0.0
Gateway              : 0.0.0.0
DNS Server           : 0.0.0.0
SNTP Server          :
```

name-server:

The command lets you to set DNS IP address.

Syntax: **name-server** <ip-address>

Parameter: **<ip-address>:** DNS IP address

EXAMPLE:

```
Switch(ip)# name-server 192.168.5.5
Switch(ip)#
```

setup:

The command lets you to configure the IP address.

Syntax:	**setup** <ip-address> <ip-mask>/<cr> <ip-address>/ <cr>
Parameter:	**<ip-address>:** IP address
	<ip-mask>: IP subnet mask
	<ip-address>: Gateway IP address

EXAMPLE:

```
Switch(ip)# setup 192.168.1.2 255.255.255.0 192.168.1.250
Switch(ip)# show
DHCP Client          : Enabled
Active Configuration : Static
IP Address           : 192.168.1.2
Subnet Mask          : 255.255.255.0
Gateway              : 192.168.1.250
DNS Server           : 192.168.5.5
SNTP Server          :
```

NOTE: The IP address and the router must be on the same subnet.

show:

The command lets you to show IP information.

Syntax:	**show** <cr>
Parameter:	**<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(ip)# show
DHCP Client          : Enabled
Active Configuration : Static
IP Address           : 192.168.6.127
Subnet Mask          : 255.255.255.0
Gateway              : 0.0.0.0
DNS Server           : 0.0.0.0
SNTP Server          :
```

8.12 IPv6 Commands of CLI

IPv6

This section describes how to configure the switch-managed IPv6 information. The Configured column is used to view or change the IPv6 configuration. And the Current column is used to show the active IPv6 configuration.
Configure the switch-managed IPv6 information on this page.
The Configured column is used to view or change the IPv6 configuration.
The Current column is used to show the active IPv6 configuration.

IPv6 Commands

Command	Function
autoconfig	Configure IPv6 autoconfig mode
setup	Set the IPv6 address
show	Show IPv6 information

autoconfig:

The command lets you configure IPv6 autoconfig mode.

Syntax: **autoconfig** disable/ enable

Parameter: **disable:** Disable autoconfig mode

enable: Enable autoconfig mode

EXAMPLE:

```
Switch(ipv6)# autoconfig enable
Switch(ipv6)# show config
Auto Configuration : Enabled
Address            : ::192.168.1.1
Prefix             : 96
Gateway            : ::
```

setup:

The command lets you set the IPv6 address.

Syntax: **setup** <ipv6-address> <deny> <permit>.

Parameter: **<ipv6-address>:** IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:).

For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'

<1-128>: IPv6 prefix

<ipv6-address>: Gateway IPv6 address IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:).

For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'

<1-4094>: VLAN ID, available value is from 1 to 4094

EXAMPLE:

```
Switch(ipv6)# setup ::192.168.6.1 1 ::192.168.0.0 20
Switch(ipv6)# show
IPv6 Autoconfig Mode     : Disabled
IPv6 Link-Local Address  : fe80::240:c7ff:fe1c:6c13
IPv6 Address             : ::192.168.6.1
IPv6 Prefix              : 1
IPv6 Router              : ::192.168.0.0
IPv6 SNTP Server         : ::
IPv6 VLAN ID             : 20
```

show:

This command show IPv6 information on the switch.

Syntax: **show**

Parameter: **<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(ipv6)# show
IPv6 Autoconfig Mode     : Disabled
IPv6 Link-Local Address  : fe80::240:c7ff:fe1c:6c13
IPv6 Address             : ::192.168.1.1
IPv6 Prefix              : 96
IPv6 Router              : ::
IPv6 SNTP Server         : ::
IPv6 VLAN ID             : 0
```

8.13 Link Commands of CLI

Link

The section will teach you to configure the “Logical Link ” table. You can configure all provisioned logical links belonging to an ONU.

Link Commands

Command	Function
bm	Enter into Link Bridge Mode
link-block	Deregister and Prevent Link Registering
link-rediscover	Deregister and Link Registering
link-unblock	Recover from Blocking
show	Show Logical Link Information command
sla	Enter into Link SLA
sta	Enter into Link Statistic Information Management

bm:

This command lets you Enter into Link Bridge Mode

.**Syntax:** **bm**

apply brdgmode <0-4> <0-1> <mac-address>

del brdgmode <0-1> <mac-address>

editmp brdgmode <0-4> <0-15> <0-1>

editmp brdgoption <0-4> <0-999> <0-1>

editmp privlan <0-4> <1-4095> <0-7> <0-7> <0-7> <0-1> <0-1>

editmp vlan <0-4> <1-4095> <0-4095>

hint brdgmode

show brdgmode <0-1> <mac-address>

showtmp brdgmode <0-4>

Parameter: **apply:** Apply Bridge Mode Template

brdgmode: Apply Bridge Mode template

<0-4>: template no: 0~ 4

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: Bridge Mode Value

del: Del Link Bridge Mode command

brdgmode: Apply Bridge Mode template

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: Bridge Mode Value

editmp: Edit function

brdgmode: Edit Bridge Mode in Bridge Mode template

<0-4>: template no: 0~ 4

<0-15> Bridge Mode Value:

0:Simple Bridged,

1:Dedicated Single VLAN,

2:Dedicated Double VLAN,

3:Shared VLAN,

4:Transparent VLAN,

7:Priority VLAN,

8:Priority Remapping Single VLAN,

9:Priority Remapping Double VLAN,

10:Priority Remapping Shared VLAN,

11:Priority Shared VLAN,

13:Transparent Priority Shared VLAN,

14:Trans. Shared VLAN w/Bcast,

15:Double Tagged Shared VLAN

<0-1>: 0: Epon-0, 1: Epon-1

brdgoption: Edit Bridge Option in Bridge Mode template

<0-4>: template no: 0~ 4

<0-999>: Entry Limit

<0-1>: mac overwrite, it is used in simple, shared, double tagged shared vlan. 0: disable, 1: enable

privlan: Edit priority vlan in Bridge Mode template

<0-4>: template no: 0~ 4

<1-4095>: Vlan Tag

<0-7>: Upstream Cos

<0-7>: Max Tos/Cos

<0-7>: Min Tos/Cos

<0-1>: Using Cos/Tos

<0-1>: Non-IP

vlan: Edit vlan in Bridge Mode template

<0-4>: template no: 0~ 4

<1-4095>: Vlan Tag

<0-4095>: upcos|max vlan tag: if transparent vlan then using max vlan tag. if others then using upcos.

hint: Hint command

brdgmode: Hint Bridge Mode

show: Show Link command

brdgmode: Apply Bridge Mode template

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: Bridge Mode Value

showtmp: Show function

brdgmode: Show Bridge Mode template

<0-4>: template no: 0~ 4

EXAMPLE:

```
Switch(bm)# apply Brdgmode 4 0 08:00:69:02:01:FC
The Mac not exist
Switch(bm)#

Switch(bm)# del brdgmode 0 08:00:69:02:01:FC
Out Of Range
Switch(bm)#

Switch(bm)# editmp brdgmode 0 15 0
Switch(bm)#

Switch(bm)# editmp brdgoption 4 999 1
Switch(bm)#

Switch(bm)# editmp privlan 4 4095 7 7 7 1 1
must be used for priority vlan, priority shared vlan, transparent pri. shared
vl
an
Switch(bm)#

Switch(bm)# editmp vlan 4 4095 4095
Vlan can't be set in simple bridge
Switch(bm)#

Switch(bm)# hint brdgmode
     Action                                Value
-----------------------------------------------
Simple Bridged                          :     0
Dedicated Single VLAN                   :     1
Dedicated Double VLAN                   :     2
Shared VLAN                             :     3
Transparent VLAN                        :     4
Priority VLAN                           :     7
Priority Remapping Single VLAN          :     8
Priority Remapping Double VLAN          :     9
Priority Remapping Shared VLAN          :    10
Priority Shared VLAN                    :    11
Transparent Priority Shared VLAN        :    13
Transparent Shared VLAN with Broadcast  :    14
Double Tagged Shared VLAN               :    15


Switch(bm)# show brdgmode 1 08:00:69:02:01:FC
Bridge Mode is not set.
Switch(bm)#

Switch(bm)# showtmp brdgmode 4
mode           : Simple Bridged
entry limit    : 64
Dest. NNI      : NNI-0
Mac Overwrite  : disable
Mac Overwrite can be set when Bridge Mode is Simple, Shared, Double Tagged
Share
d Vlan
Switch(bm)#
```

link-block:

This command lets you Deregister and Prevent Link Registering.

Syntax: **link-block** <mac-address>

Parameter: **<mac-address>:** LINK

EXAMPLE:

```
Switch(link)# link-block 08:00:69:02:01:FC
08-00-69-02-01-fc don't exist
```

link-unblock:

The command lets you Recover from Blocking.

Syntax: **link-unblock** <mac-address>

Parameter: **<mac-address>:** LINK

EXAMPLE:

```
Switch(link)# link-unblock 00-15-F2-4E-CC-B1
00-15-f2-4e-cc-b1 isn't blocked
```

show:

This command lets you Show Logical Link Information command.

Syntax: **show** block-links

Parameter: **block-links:** Show Block Links Of An OLT

EXAMPLE:

```
Switch(link)# show block-links

No.  Link Label
==== ====================

Switch(link)#
```

sla:

This command let you Enter into Link SLA.

Syntax: **sla**

set dbaparam <0-1> <mac-address> <0-1> <0-7>

set downqsla <0-1> <mac-address> <0-1> <0-1000000> <1-256> <0-7> <2-32>

set mcastsla <0-1> <mac-address> <0-1000000> <1-256> <0-7> <2-32>

set sla <0-1> <mac-address> <0-1> <0-1000000> <1-256> <0-7> <2-32>

set upqsla <0-1> <mac-address> <0-1> <0-1000000> <1-256> <0-7> <2-32>

show downqsla/ mcastsla/ sla/ upqsla <0-1> <mac-address>

Parameter: **dbaparam:** Set Link SLA DBA Parameter

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

<0-1>: 0: do not force report, 1: force report

<0-7>: polling level

downqsla: Set Downstream Queue SLA command

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

<0-1>: 0: Min Shaper, 1: Max Shaper

<0-1000000>: Banswidth value, 0(not including Max Bw), 256~ 1000,000

<1-256>: Burst value

<0-7>: Scheduler Level

<2-32>: Schedule Weight

mcastsla: Set Multicast SLA command

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

<0-1000000>: Banswidth value, 0(not including Max Bw), 256~ 1000,000

<1-256>: Burst value

<0-7>: Scheduler Level

<2-32>: Schedule Weight

sla: Set Link SLA command

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

<0-1>: 0: Min Shaper, 1: Max Shaper

<0-1000000>: Banswidth value, 0(not including Max Bw), 256~ 1000,000

<1-256>: Burst value

<0-7>: Scheduler Level

<2-32>: Schedule Weight

upqsla: Set Upstream Queue SLA command

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

<0-1>: 0: Min Shaper, 1: Max Shaper

<0-1000000>: Banswidth value, 0(not including Max Bw), 256~ 1000,000

<1-256>: Burst value

<0-7>: Scheduler Level

<2-32>: Schedule Weight

EXAMPLE:

```
Switch(sla)# set dbaparam 1 00-15-F2-4E-CC-B1 1 7
Out Of Range
Switch(sla)#
Switch(sla)# set downqsla 1 00-15-F2-4E-CC-B1 1 1000000 256 7 32
Out Of Range
Switch(sla)#
Switch(sla)# set mcastsla 1 00-15-F2-4E-CC-B1 1000000 256 7 32
Out Of Range
Switch(sla)#
Switch(sla)# set sla 1 00-15-F2-4E-CC-B1 1 1000000 256 7 32
Out Of Range
Switch(sla)#
Switch(sla)# set upqsla 0 00-15-F2-4E-CC-B1 1 100000 256 7 32
Out Of Range
Switch(sla)#

Switch(sla)# show downqsla 0 00-15-F2-4E-CC-B1
Min Shaper          : Enable
Min Bw(kbps)        : 0
Min Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0

Max Bw(kbps)        : 0
Max Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0
Switch(sla)#

Switch(sla)# show mcastsla 0 00-15-F2-4E-CC-B1
Min Shaper          : Disable
Min Bw(kbps)        : 0
Min Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 2

Max Bw(kbps)        : 0
Max Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 2

Switch(sla)# show sla 0 00-15-F2-4E-CC-B1
SLA                 : Enable
Min Shaper          : Enable
Min Bw(kbps)        : 0
Max Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0

Max Bw(kbps)        : 0
Max Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0

Force Report        : No
Polling Level       : 0
Switch(sla)#

Switch(sla)# show upqsla 0 00-15-F2-4E-CC-B1
Min Shaper          : Enable
Min Bw(kbps)        : 0
Min Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0

Max Bw(kbps)        : 0
Max Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0
Switch(sla)#
```

sta:

The command lets you Enter into Link Statistic Information Management.

Syntax:	**sta**
	clear/ show <mac-address> <0-3>
Parameter:	**clear:** Clear EPON Link Statistics
	show: Show Link Statistic
	<mac-address>: LINK Address
	<0-3>: 0:Link Receive(OLT Side), 1:Link Transmit(OLT Side), 2:Link Receive(ONU Side), 3:Link Transmit(ONU Side)

EXAMPLE:

```
Switch(sta)# clear 00-15-f2-4e-cc-b1 3

Switch(sta)# show 00-15-F2-4E-CC-B1 3
Link Statistics(ONU Side) 00-15-f2-4e-cc-b1
Group  :  ONU Link Transmit
-------------------------------------------------
Bytes Transmitted:                      0
Frames Transmitted:                     0
Unicast Frames Transmitted:             0
Multicast Frames Transmitted:           0
Broadcast Frames Transmitted:           0
64 Byte Frames Transmitted:             0
65-127 Byte Frames Transmitted:         0
128-255 Byte Frames Transmitted:        0
256-511 Byte Frames Transmitted:        0
512-1023 Byte Frames Transmitted:       0
1024-1518 Byte Frames Transmitted:      0
Greater than 1518 Frames Transmitted:   0
Bytes Dropped:                          0
Frames Dropped:                         0
Bytes Delayed:                          0
Maximun Delayed:                        0
Delay Threshold:                        0
Unused Bytes:                           0
OAM Frames:                             0
MPCP Reports:                           0
MPCP Requests:                          0
MPCP Register ACKs:                     0
Switch(sta)#
```

8.14 Login Protect Commands of CLI

Login-protect

The unit supports the Login Protect function. It is a security function to protect the unit from any illegal access. When the login information is incorrect, the unit will block the access for a period configured. Login Protect is able to stop too many unauthorized login action, and re-open the login after a period of time.

Login-protect Commands

Command	Function
block-time	Set block time interval
resume	resume login-failed IP Address
show	Show Login Protect information

Block-time:

This command lets you Set block time interval.

Syntax: **block-time** <0-60>

Parameter: **<0-60>:** available from 0 to 60 (minutes), set 0 as disabled

EXAMPLE:

```
Switch(login-protect)# block-time 60
Switch(login-protect)# show config
Lock-Minutes : 60 minutes
Switch(login-protect)#
```

resume:

This command lets you resume login-failed IP Address.

Syntax: **resume <ip-hostname>**

Parameter: **<ip-hostname>:** IP address

EXAMPLE:

```
Switch(login-protect)# resume 192.168.6.127
IP:192.168.6.127 not in login-failed list!
Switch(login-protect)#
```

show:

The command Show Login Protect information.

Syntax: **show** config/ login-failed

Parameter: **config:** Show Login Protect configuration

login-failed: Show login-failed list

EXAMPLE:

```
Switch(login-protect)# show config
Lock-Minutes : 10 minutes
Switch(login-protect)#

Switch(login-protect)# show login-failed
No. IP               Login-Failed Counter
--- ---------------- --------------------
There is no entry for Login-failed List
Switch(login-protect)#
```

8.15 OLT Commands of CLI

OLT

This chapter describes all of the EPON OLT Maintenance configuration tasks to enhance the performance of local network including Port, OLT Statistics, OLT DBA, OLT Operation.

OLT Media Commands

Command	Function
brdgcfg	Set OLT bridge config
dba	Enter into DBA Information
flow-control	set Port Flow Control
green	Enter into OLT Green Pon
igmp	Enter into OLT IGMP Proxy Config
management-mode	set management mode
network	Enter into Network Parameters Management
olt-control	GUI Control EPON OLT. Warning: for debug
olt-disable	Disable EPON OLT
olt-enable	Enable EPON OLT
olt-reset	Reset EPON OLT
optcalctrl	set Optical Control
optcalmon	set Optical Power Monitor Config
show	Show OLT command
speed	set Port Speed Duplex
sta	Enter into Statistic Information Management
state	set Port State
tm	Enter into TM Information

dba:

The command lets you Enter into DBA Information.

Syntax: **dba**

broadcast-sla <0-3> <0-1> <0-1000000> <1-256> <0-7> <2-32>

egress-ddw <0-3> <1-7> <0-256>

egress-shaper <0-1000000> <0-256>

ingress-dba <0-1> <0-1000000> <0-256>

ingress-ddw <0-1> <1-7> <0-256>

polling-rate <0-1> <0-7> <0-256>

show <cr>

Parameter: **broadcast-sla:** Set Broadcast SLA command

<0-3>: 0: epon-0 <-> nni-0, 1: epon-1 <-> nni-0, 2: epon-0 <-> nni-1, 3: epon-1 <-> nni-1

<0-1>: 0: Min Shaper, 1: Max Shaper

<0-1000000>: Banswidth value, 0(not including Max Bw), 256~ 1000,000

<1-256>: Burst value

<0-7>: Scheduler Level

<2-32>: Schedule Weight

egress-ddw: set Egress DBA Drop-Down Weight

<0-3>: 0: epon-0 <-> nni-0, 1: epon-1 <-> nni-0, 2: epon-0 <-> nni-1, 3: epon-1 <-> nni-1

<1-7>: level 1~7

<0-256>: level 1~7 value

egress-shaper: set Aggregate Shaper Egress

<0-1000000>: MaxBw: available from 256 to 1000000, (0 : disable aggregate bandwidth).

<0-256>: MaxBurst: available from 0 to 256, 0 : disable aggreg ate bandwidth.

ingress-dba: set Aggregate Shaper Ingress/DBA

<0-1>: direction: 0: epon-0, 1: epon-1.

<0-1000000>: MaxBw: available from 256 to 1000000, (0 : disable aggregate bandwidth).

<0-256>: MaxBurst: available from 0 to 256, 0 : disable aggreg ate bandwidth.

ingress-ddw: set Ingress/DBA Drop-Down Weight

<0-1>: Port: 0: epon-0, 1: epon-1

<1-7>: level 1~7

<0-256>: level 1~7 value

polling-rate: Set Polling Rate

<0-1>: Port: 0: epon-0, 1: epon-1

<0-7>: level 0~7 (Unit: 65.5 us).

<0-256>: level rate (Unit: 65.5 us).

show: Show Aggregate Shaper Information command

EXAMPLE:

```
Switch(dba)# broadcast-sla 3 1 100000 256 7 32
Switch(dba)# show broadcast-sla 3
Epon-1 <-> NNI-1 Broadcast SLA
Min Shaper          : Disable
Min Bw(kbps)        : 0
Min Burst(kbps)     : 0
Scheduler Lvl       : 0
Schedule Weight     : 0

Max Shaper          : Enable
Max Bw(kbps)        : 100000
Max Burst(kbps)     : 256
Scheduler Lvl       : 7
Schedule Weight     : 32
Switch(dba)#

Switch(dba)# egress-ddw 3 7 256
Switch(dba)# show egress-ddw

NNI-1 Egress DBA Drop Down Weights
============================
Level 1 : 0   KBytes
Leval 2 : 0   KBytes
Leval 3 : 0   KBytes
Leval 4 : 0   KBytes
Leval 5 : 0   KBytes
Leval 6 : 0   KBytes
Leval 7 : 256 Kbytes


Switch(dba)# egress-shaper 3 999 200
Switch(dba)# show egress-shaper
Epon-0 Egress
Epon-0 Aggregate Shaper Egress : Disable

Epon-1 Egress
Epon-1 Aggregate Shaper Egress : Disable

NNI-0 Egress
NNI-0 Aggregate Shaper Egress : Disable

NNI-1 Egress
NNI-1 Aggregate Shaper Egress : Enable
============================
Max Bw    : 999     Kbps
Max Burst : 200     Kbytes


Switch(dba)# ingress-dba 1 100000 256
Switch(dba)# show ingress-dba

Epon-0 Aggregate Shaper Ingress : Disable

Epon-1 Aggregate Shaper Ingress  : Enable
============================
Max Bw    : 100000  Kbps
Max Burst : 256     Kbytes
```

```
Switch(dba)# ingress-ddw 1 7 222
Switch(dba)# show ingress-ddw

Epon-0 Ingress/DBA Drop Down Weights
============================
Level 1 : 16  KBytes
Leval 2 : 16  KBytes
Leval 3 : 16  KBytes
Leval 4 : 16  KBytes
Leval 5 : 16  KBytes
Leval 6 : 16  KBytes
Leval 7 : 16  KBytes

Epon-1 Ingress/DBA Drop Down Weights
============================
Level 1 : 16  KBytes
Leval 2 : 16  KBytes
Leval 3 : 16  KBytes
Leval 4 : 16  KBytes
Leval 5 : 16  KBytes
Leval 6 : 16  KBytes
Leval 7 : 222 Kbytes

Switch(dba)# polling-rate 1 7 256
Switch(dba)# show polling-rate

EPON-0
DBA Polling Rate
=====================================
Level 0 : 15   ( 65.5 us * 15 = 982.5 us )
Level 1 : 30   ( 65.5 us * 30 = 1965 us )
Level 2 : 60   ( 65.5 us * 60 = 3930 us )
Level 3 : 60   ( 65.5 us * 60 = 3930 us )
Level 4 : 60   ( 65.5 us * 60 = 3930 us )
Level 5 : 60   ( 65.5 us * 60 = 3930 us )
Level 6 : 60   ( 65.5 us * 60 = 3930 us )
Level 7 : 60   ( 65.5 us * 60 = 3930 us )


EPON-1
DBA Polling Rate
============================
Level 0 : 15   ( 65.5 us * 15 = 982.5 us )
Level 1 : 30   ( 65.5 us * 30 = 1965 us )
Level 2 : 60   ( 65.5 us * 60 = 3930 us )
Level 3 : 60   ( 65.5 us * 60 = 3930 us )
Level 4 : 60   ( 65.5 us * 60 = 3930 us )
Level 5 : 60   ( 65.5 us * 60 = 3930 us )
Level 6 : 60   ( 65.5 us * 60 = 3930 us )
Level 7 : 256   ( 65.5 us * 256 = 16768 us )
```

flow-control:

The command lets you set Port Flow Control

.**Syntax:** **flow-control** <2-5> <0-1>

Parameter: **<2-5>:** 2:nni-0 tp,3:nni-0 fiber,4:nni-1 tp,5:nni-1 fiber

<0-1>: Flow Control. 1:Enable, 0:Disable

EXAMPLE:

```
Switch(olt)# flow-control 5 1
```

green:

The command lets you Enter into OLT Green Pon

Syntax: **green**

disonugn/ enblonugn <0-1>

green <0-1> <0-1>

greenparam <0-1> <0-999> <0-999> <0-999> <0-999> <0-999> <0-999> <0-999>

show green/ onupwsvrep

Parameter:

disonugn: Del many ONUs green pon for an OLT

<0-1>: 0: epon-0, 1: epon-1

enblonugn: Set many ONUs green pon for an OLT

green: Set green pon for an OLT

<0-1>: 0: disable, 1: enable, other value is not changed.

greenparam: Set green pon parameters for an OLT

<0-999>: Sleep After No Traffic

<0-999>: Off Time

<0-999>: Min On Time

<0-999>: Min ONU Off Time

<0-999>: Sleep Check Timer

<0-999>: Time For ONU to Begin to Sleep

<0-999>: Grace Time After Wakeup for ONU to Return

show: Show OLT Green Pon command

green: Show OLT Green Pon

onupwsvrep: Show ONU Power Save Report

EXAMPLE:

```
Switch(green)# enblonugn 0
Switch(green)# show onupwsvrep 0
index  onu mac            Candidate  Asleep  Time Asleep  Time Active
================================================================================
====
    1  b8-26-d4-00-21-d8  No         No      0            0

Switch(green)# disonugn 0
Switch(green)# show onupwsvrep 0
index  onu mac            Candidate  Asleep  Time Asleep  Time Active

Switch(green)# green 0 1
Switch(green)# show green 0
OLT Green Pon - Epon-0
-----------------------
Green Pon                                 : enable
Sleep After No Traffic(ms)                : 100
Off Time(ms)                              : 200
Minimum On Time(ms)                       : 20
Minimum ONU Off Time(ms)                  : 50
Sleep Check Time                          : 50
Time For ONU To Begin To Sleep(ms)        : 20
Grace Time After Wakeup(ms)               : 20

Switch(green)# greenparam 0 10 20 30 40 50 60 70
Switch(green)# show green 0
OLT Green Pon - Epon-0
-----------------------
Green Pon                                 : enable
Sleep After No Traffic(ms)                : 10
Off Time(ms)                              : 20
Minimum On Time(ms)                       : 30
Minimum ONU Off Time(ms)                  : 40
Sleep Check Time                          : 50
Time For ONU To Begin To Sleep(ms)        : 60
Grace Time After Wakeup(ms)               : 70
```

igmp:

The command lets you configure LLDP-MED Emergency Call Service.

Syntax: **igmp**

proxy <0-4095> <0-2000000> <0-1> <0-1> <0-1>

show proxy

Parameter: **proxy:** Set OLT IGMP Proxy Config

<0-4095>: Maximum IP Multicast Group

<0-2000000>: Global Bandwidth Poll Size

<0-1>: Capture All Mode

<0-1>: DA Fprwarding

<0-1>: SA Forwarding

show: Show OLT IGMP Proxy Command

EXAMPLE:

```
Switch(igmp)# proxy 4095 200000 0 1 1
Switch(igmp)# show proxy
            Proxy Configuration
=========================================
Maximum IP Multicast Groups             : 4095
Global Bandwidth Pool Size              : 200000
Capture All Mode                        : No
DA Forwarding                           : Forward by L2 DA
SA Forwarding                           : Forward by L3 SA
Switch(igmp)#
```

management-mode:

The command lets you set management mode.

Syntax: **management-mode** <0-2>

Parameter: **<0-2>:** 0: normal, 1: nni-0, 2: nni-1

EXAMPLE:

```
Switch(olt)# management-mode 0
Switch(olt)# show management-mode
Management Mode : Normal
Switch(olt)#
```

network:

The command lets you Enter into Network Parameters Management.

Syntax: **network**

loop_timing maxpgdelay/ minpgdelay <0-1> <0-19920>

loop_timing onudelay <0-1> <3125-30000>

loop_timing updndelayoff <0-1> <-32768-32767>

mpcp_param period <0-1> <10-65530>

mpcp_param period <0-1> <84-131070>

oam_param loopBack <10-65535>

oam_param max_rate <0-255>

oam_param min_rate <0-4>

show loop_timing/ mpcp_param/ oam_param/ vlan_param

vlan_param ether_type <WORD>

vlan_param tag_down/ tag_up disable/ enable

Parameter: **loop_timing:** Set EPON OLT Loop Timing

maxpgdelay: Set EPON OLT Max Propagation Delay

<0-1>: Set EPON OLT Max Propagation Delay, 0:EPON Port-0, 1:EPON Port-1

<0-19920>: Default:0, Range:0~19920

minpgdelay: Set EPON OLT Min Propagation Delay

<0-1>: Set EPON OLT Min Propagation Delay, 0:EPON Port-0, 1:EPON Port-1

<0-19920>: Default:0, Range:0~19920

onudelay: Set EPON ONU Delay

<0-1>: Set EPON ONU Delay, 0:EPON Port-0, 1:EPON Port-1

<3125-30000>: Default:3125, Range:3125~30000

updndelayoff: Set EPON OLT Up/Down Delay Offset

<-32768-32767>: Default:0, Range:-32768~32767

mpcp_param: Set EPON OLT MPCP Parameters

period: Set EPON OLT MPCP Discovery Period

<0-1>: Set EPON OLT MPCP Discovery Period, 0:EPON Port-0, 1:EPON Port-1

<10-65530>: Default:100, Range:1~6553(10ms)

window: Set EPON OLT MPCP Discovery Window

<0-1>: Set EPON OLT MPCP Discovery Period, 0:EPON Port-0, 1:EPON Port-1

<84-131070>: Default:16319, Range:84~131070(Bytes)

oam_param: Set EPON OLT OAM Parameters

loopBack: Set EPON OLT LoopBack Timeout

<10-65535>: Default:600, Range:10~65535(100ms)

max_rate: Set EPON OLT Max OAM Rate

<0-255>: Default:30, Range:0~255(PDUs/sec)

min_rate: Set EPON OLT Min OAM Rate

<0-4>: Default:1, Range:0~4(sec/PDU)

show: Show OLT EPON Network Parameters

loop_timing: Show EPON Loop Timing

mpcp_param: Show EPON MPCP Parameters

oam_param: Show EPON OAM Parameters

vlan_param: Show EPON VLAN Parameters

vlan_param: Set EPON OLT VLAN Parameters

ether_type: Set EPON OLT Vlan Ether Type

<WORD>: Default:8100

tag_down: Set EPON OLT VLAN Tag Up Mode

disable: Disable EPON OLT VLAN Tag Down

enable: Enable EPON OLT VLAN Tag Down

tag_up: Set EPON OLT VLAN Tag Up Mode

disable: Disable EPON OLT VLAN Tag Up

enable: Enable EPON OLT VLAN Tag Up

EXAMPLE:

```
Switch(network)# loop_timing maxpgdelay 0 19920
Wrong Mode

Switch(network)# loop_timing minpgdelay 0 19920
Wrong Mode

Switch(network)# loop_timing onudelay 0 30000
Wrong Mode

Switch(network)# loop_timing updndelayoff 0 -27768
Wrong Mode

Switch(network)# show loop_timing
OLT Loop Timing  :

EPON Port-0  :
Minimum Propagation Delay      : 0
Maximum Propagation Delay      : 6250
Onu Delay                      : 3125
Onu Up/Donw Offset             : 0

EPON Port-1  :
Minimum Propagation Delay      : 0
Maximum Propagation Delay      : 6250
Onu Delay                      : 3125
Onu Up/Donw Offset             : 0
Switch(network)#

Switch(network)# mpcp_param period 0 65530
Switch(network)# mpcp_param window 0 131070
SSwitch(network)# show mpcp_param
OLT MPCP Parameters  :

EPON Port-0  :
Discovery Period (10ms)  :    6550
Discovery Window (Bytes)  :    131070

EPON Port-1  :
Discovery Period (10ms)  :    1000
Discovery Window (Bytes)  :    16319
Switch(network)#

Switch(network)# oam_param loopBack 65535
Switch(network)# oam_param max_rate 255
Switch(network)# oam_param min_rate 4
Switch(network)# show oam_param
OLT OAM Parameters  :

Max Oam Rate (PDUs/sec)  :    255
Min Oam Rate (sec/PDU)  :    4
LoopBack Timeout (100ms)  :    65535

Switch(network)# vlan_param ether_type 8100
Switch(network)# vlan_param tag_down enable
Switch(network)# vlan_param tag_up enable
Switch(network)# show vlan_param
OLT VLAN Parameters  :

Vlan Ether Type  :    0x8100
Tag UP  :    Enable
Tag Down  :    Enable
Switch(network)#
```

olt-control:

The command lets you GUI Control EPON OLT. Warning: for debug.

Syntax: **olt-control** <0-1>

Parameter: **<0-1>:** 0: Tk GUI not control, 1: Tk GUI can control

EXAMPLE:

```
Switch(olt)# olt-control 1
Switch(olt)#
```

olt-disable:

The command lets you Disable EPON OLT.

Syntax: **olt-disable** <cr>

Parameter: **<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(olt)# olt-disable
Switch(olt)#
```

olt-enable:

The command lets you Enable EPON OLT.

Syntax: **olt-enable** <cr>

Parameter: **<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(olt)# olt-enable
Switch(olt)#
```

olt-reset:

The command lets you Reset EPON OLT.

Syntax: **olt-reset** <cr>

Parameter: **<cr>:** means no parameter needed to type.

EXAMPLE:

```
Switch(olt)# olt-reset
Switch(olt)# +M25PXX : Init device with JEDEC ID 0xC22018.
Luton10 board detected (VSC7424 Rev. B).

RedBoot(tm) bootstrap and debug environment [ROMRAM]
Non-certified release, version 1_12-Vitesse - built 19:19:16, Apr 18 2011

Copyright (C) 2000, 2001, 2002, 2003, 2004, 2005, 2006, 2007, 2008, 2009
Free Software Foundation, Inc.
RedBoot is free software, covered by the eCos license, derived from the
GNU General Public License. You are welcome to change it and/or distribute
copies of it under certain conditions. Under the license terms, RedBoot's
source code and full license terms must have been made available to you.
Redboot comes with ABSOLUTELY NO WARRANTY.

Platform: VCore-III (MIPS32 24KEc) LUTON26
RAM: 0x80000000-0x84000000 [0x80021198-0x83fe1000 available]
FLASH: 0x40000000-0x40ffffff, 256 x 0x10000 blocks
== Executing boot script in 3.000 seconds - enter ^C to abort
RedBoot> fis load -d managed
Image loaded from 0x80040000-0x806c04b8
RedBoot> go

Username:
```

optcalctrl:

The command lets you set Optical Power Monitor Config.

Syntax: **optcalctrl** <0-1> <0-4> <mac-address> <0-624> <0-625>

Parameter:

<0-1>: 0: epon-0, 1: epon-1

<0-4>: New Run Mode, 0: Off,1: On(All Links),2: No Idle,3: Idle Only,4: Single Link

<mac-address>: Link Mac Address, If New Run Mode is 4, you must set Link Mac Address. If others, Set Link Mac Address 00-00-00-00-00-00.

<0-624>: Start Strobe

<0-625>: End Strobe

EXAMPLE:

```
Switch(olt)# optcalctrl 0 3 00-00-00-00-00-00 624 625
Switch(olt)# show optcalctrl 0
Optical Monitor Control
==========================
New Run Mode         : Idle Only
Link Mac Address     : 00-00-00-00-00-00
Start Strobe         : 624
End Strobe           : 625
```

optcalmon:

The command lets you set Optical Power Monitor Config.

Syntax: **optcalmon** <0-1> <0-1>

Parameter:

<0-1>: 0: epon-0, 1: epon-1

<0-1>: Hardware Type, 0:Not Supported, 1:SFF-8472 Compliant

EXAMPLE:

```
Switch(olt)# optcalmon 0 1
Switch(olt)# show optcalmon 0
Optical Power Monitor
=====================
Hardware Type        : SFF-8472 Compliant
I2C Bus              : GPIO-0
I2C Operating Speed  : 50
I2C Device Address   : a2
Register Address     : 104
Length of Register   : 2
```

show:

The command lets you Show OLT command

Syntax: **show** oltInfo/ port-config/ port-status/ provinolt

show optcalctrl/ provinhost <0-1>

Parameter:

management-mode: Show OLT management-mode, if normal, can manage OLT-E202 from nni-0, nni-1

if nni-0, can manage OLT-E202 from nni-0. if nni-1, can manage OLT-E202 from nni-1.

oltInfo: Show General Information Of An OLT

optcalctrl: Show OLT Optical Power Control

<0-1>: 0: epon-0, 1: epon-1

optcalmon: Show OLT Optical Power Monitor Config

port-config: Show OLT Port Configuration

port-status: Show OLT Port Information

provinhost: Show OLT Provision in Host

provinolt: Show OLT Provision in OLT

EXAMPLE:

```
Switch(olt)# show management-mode
Management Mode : Normal

Switch(olt)# show oltInfo
                                          Attribute
                                        ====================
Output Optical Center Wavelength (nm)   1490
Min. TX Power (dBm)                     3.5
Max. TX Power (dBm)                     7
Min. RX Operating Wavelength (nm)       1260
Max. RX Operating Wavelength (nm)       1360
RX Sensitivity (dBm)                    -27
RX Saturation Power (dBm)               -6
Firmware Version                        0x242
Chip ID                                 0x3723
Chip Version                            0xa0071101
Boot Code Version                       0x240
Personality Version                     f9
App0 Version                            0x242
App1 Version                            0x242

Switch(olt)# show optcalctrl 0
Optical Monitor Control
===========================
New Run Mode         : On(All Links)
Link Mac Address     : 00-00-00-00-00-00
Start Strobe         : 165
End Strobe           : 400

Switch(olt)# show optcalmon 0
Optical Power Monitor
=======================
Hardware Type        : Not Supported
I2C Bus              : GPIO-0
I2C Operating Speed  : 50
I2C Device Address   : a2
Register Address     : 104
Length of Register   : 2
```

```
Switch(olt)# show port-config
Port              State    Speed/Duplex  Flow Control
----------------  -------  ------------  ------------
NNI-0 TP          Enabled   Auto          Disabled
NNI-0 Fiber       Enabled   Auto          Disabled
NNI-1 TP          Enabled   Auto          Disabled
NNI-1 Fiber       Enabled   Auto          Disabled

Switch(olt)# show port-status ?
  <cr>
Switch(olt)# show port-status
Port             Link State   Auto Nego Speed/Duplex Flow Control
---------------- ---- ------- --------- ------------ ------------
Epon-0           Up   Enable            1000/Full
Epon-1           Down Enable            1000/Full
NNI-0 TP         Down Enable  Enable                 Disable
NNI-0 Fiber      Down Enable  Enable                 Disable
NNI-1 TP         Down Enable  Enable                 Disable
NNI-1 Fiber      Down Enable  Enable                 Disable

Switch(olt)# show provinhost 0
No.   Link Label         Bridge                            Dest. NNI Vlan
===== ================= ================================= ========= =====
1     b8-26-d4-00-21-d8  Simple Bridged                    NNI-0     0
2     b8-26-d4-00-21-d9  Simple Bridged                    NNI-0     0
Switch(olt)#

Switch(olt)# show provinolt
No. Link Label         Bridge                            Src Epon Dest. NNI Vl
an
=== ================= ================================= ======== ========= ==
===
1   b8-26-d4-00-21-d8  Simple Bridged                    EPON-0   NNI-0     0
```

speed:

The command lets you set Port Speed Duplex.

Syntax: **speed** <2-5> <WORD>

Parameter: **<2-5>:** 2:nni-0 tp,3:nni-0 fiber,4:nni-1 tp,5:nni-1 fiber

<WORD>: 1:Auto Nego. Enable,

10:Force 10M half duplex,

11:Force 10M full duplex,

100:Force 100M half duplex,

101:Force 100M full duplex,

1001:Force 1G full duplex

EXAMPLE:

```
Switch(olt)# speed 5 1001
Switch(olt)# show port-config
Port              State    Speed/Duplex  Flow Control
----------------  -------  ------------  ------------
NNI-0 TP          Enabled   Auto          Disabled
NNI-0 Fiber       Enabled   Auto          Disabled
NNI-1 TP          Enabled   Auto          Disabled
NNI-1 Fiber       Enabled   1G Full       Disabled
```

sta:

The command lets you Enter into Statistic Information Management.

Syntax: **sta**

clear/ show <0-3> <0-5>

Parameter: **clear:** Clear EPON OLT Port Statistics

show: Show EPON OLT Statistic

<0-3>: 0:EPON Port-0, 1:EPON Port-1, 2:NNI Port-0, 3:NNI Port-1

<0-5>: 0:OLT EPON LIF Transmit, 1:OLT EPON LIF Receive, 2:OLT EPON MAC Transmit, 3:OLT EPON MAC Receive, 4:OLT NNI Transmit, 5:OLT NNI Receive

EXAMPLE:

```
Switch(sta)# show 0 0
EPON Port-0 Statistics
Group  :  OLT EPON LIF Transmit
================================
Bytes Transmitted  :190432735
Frames Transmitted  :2975199
FEC Blocks Transmitted  :0
Laser Power  :31550
Laser VCC  :32754
Laser Bias  :4320
Laser Temperature  :10494
Switch(sta)#

Switch(sta)# clear 0 0
Switch(sta)# show 0 0
EPON Port-0 Statistics
Group  :  OLT EPON LIF Transmit
================================
Bytes Transmitted  :162505
Frames Transmitted  :2539
FEC Blocks Transmitted  :0
Laser Power  :31618
Laser VCC  :32754
Laser Bias  :4456
Laser Temperature  :10494
Switch(sta)#
```

state:

The command lets you set Port State.

Syntax: **state** <0-5> <0-1>

Parameter: **<0-5>:** 0: epon-0 port, 1: epon-1 port

2,3: nni-0 tp,fiber, 4,5: nni-1 tp,fiber

<0-1>: 0: Disable, 1:Enable

EXAMPLE:

```
Switch(olt)# state 0 0
Switch(olt)# show port-status
Port             Link State   Auto Nego Speed/Duplex Flow Control
---------------- ---- ------- --------- ------------ ------------
Epon-0           Down Disable           1000/Full
Epon-1           Down Enable            1000/Full
NNI-0 TP         Down Enable  Enable                 Disable
NNI-0 Fiber      Down Enable  Enable                 Disable
NNI-1 TP         Down Enable  Enable                 Disable
NNI-1 Fiber      Down Enable  Disable                Disable
```

tm:

The command lets you Enter into TM Information.

Syntax: **tm**

apply filter-rule <0-3> <0-19>

brdgcfg <0-2000000000>

del filter-rule <0-3> <1-30>

editmp clause <0-19> <1-17> <0-7> <0-3> <WORD>

editmp rule <0-19> <0-7> <0-1> <0-12> <WORD>

show brdgcfg

show dynamactbl <0-1> <mac-address>

show filter-rule <0-3>

showtmp clause/rule <0-19>

Parameter:

apply: Apply function

filter-rule: OLT filter rule

<0-3>: 0: Epon-0, 1: Epon-1, 2: NNI-0, 3: NNI-1

<0-19>: rule no: rule index(0~19)

brdgcfg: Set OLT bridge config

<0-2000000000>: age limit

del: Del Traffic Rule command

filter-rule: Del OLT filter rule

<0-3>: 0: Epon-0, 1: Epon-1, 2: NNI-0, 3: NNI-1

<1-30>: rule no: Before del filter-rule, you must display filter-rule

editmp: Edit function

clause: Edit clause template

<0-19>: clause no: clause index(0~19)

<1-17>: Field select value:

1:Destination Mac,

2:Source Mac,

3:Ether Type,

4:Svlan0,

5:Svlan1,

6:Cvlan0,

7:Cvlan1,

8:Ip Priority,

9:IpV6 NextHeader,

10:Ip Ttl,

11:Ip Protocol

, 12:Ip Source,

13:Ipv6 SourceUpper,

14:Ip Destination,

15:Ipv6 DestinationUpper

16:Source Port

17:Destination Port

<0-7>: Operation value:

0:Fail,

1:==,

2:!=,

3:<=,

4:>=,

5:exists,

6:!exist,

7:True,

<0-3>: Type: value type , 0:Hex , 1:Decimal , 2:IP format, 3:automatic. When field is User, can't select type automatically

<WORD>: Vaule: operation value.

rule: Edit rule template

<0-19>: Rule no: rule index(0~19)

<0-7>: Priority: rule template rule priority(0~7)

<0-1>: Action no: 0:set discard flag, 1:clear discard flag

<0-12>: Bitmap: 0:Automatic, 1:Epon-0, 2:Epon-1, 3:Epon-0& Epon-1, 4:NNI-0, 8:NNI-1, 12:NNI-0& NNI-1

<WORD>: Each clause separated by commas

Clause no: clause index(0~19)

show: Show Traffic Rule command

brdgcfg: Show OLT bridge config

dynamactbl: Show Link Dynamic Table

<0-1>: 0: Epon-0, 1: Epon-1

<mac-address>: link mac address

filter-rule: Show OLT filter rule

<0-3>: 0: Epon-0, 1: Epon-1, 2: NNI-0, 3: NNI-1

showtmp: Show function

clause: Show clause template

<0-19>: Show clause template index

rule: Show rule template

<0-19>: Show rule template index

EXAMPLE:

```
Switch(tm)# apply filter-rule 0 19
Cmd Failed
Switch(tm)#

Switch(tm)# brdgcfg 20000000
Switch(tm)# show brdgcfg
Learned entry age limit(unit=9.375ms)    : 11520

The actual time is (2^n)*9.375 ms, n= 1,2,3 ..,
for example: n=11, 2^11*9.375=2048*9.375=19200 ms
n=10, 2^10*9.375=1024*9.375=9600 ms.
If Age Limit is 9601~19200, actual time is 19200 ms.
n=9, 2^9*9.375=512*9.375=4800 ms.
If Age Limit is 4801~9600, actual time is 9600 ms.

Switch(tm)# del filter-rule 0 30
Switch(tm)#

Switch(tm)# editmp clause 19 17 7 3 11
Switch(tm)# showtmp clause 19
no field-select         op         type      value
== ==================== ========== ========= ==================
19 Destination Port     True       Hex        0x0000000000000000

Switch(tm)# editmp rule 19 7 1 12 10
Switch(tm)# showtmp rule 19
rule template no     : 19
priority             : 7
action               : Clear Discard Flag;PortBitmap 0x00
field-select         : Reserved,
operation            : Fail
value                :  0x0000000000000000
------------------------------------------------------------
```

8.16 ONU Commands of CLI

ONU

This chapter describes all of the EPON ONU Maintenance configuration tasks to enhance the performance of local network including ONU List, ONU Authorization.

Table 15: ONU Commands

Command	Function
auth	Enter into Auth Information Management
bc	Enter into Bridging Config Information Management
dt	Enter dynamic table
flow-control	set Port Flow Control
green	Enter into ONU Green Pon
igmp	Enter Igmp Snooping Information
ionus-wakeup	Wake up Many ONUs
lblink	Loopback Test on A Logical Link
lbport	Loopback Test Through Logical Link and ONU UNI Port
onu-reset	Reset EPON ONU
onu-restore	Restore EPON ONU
onus-restore	Restore EPON Many ONUs
rstp	Enter into RSTP command
show	Show ONU command
si	Enter into ONU Subscriber Information Management
speed-duplex	set Port Speed and Duplex
sta	Enter into Statistic Information Management
state	set Port State
tm	Enter into Traffic Management Information

auth:

The command lets you Enter into Auth Information Management.

Syntax: **auth**

add <0-1> <mac-address> <0-8>

authorize <0-1> <WORD>

del <0-1> <WORD>

show <0-1>

unauthorized <0-1> <WORD>

Parameter: **<0-1>:** 0:EPON-0, 1:EPON-1

<WORD>: Index: the index of the onu-auth. e.g. 2,5-7,9,11

Before del-onus , you must first show onu-auth

Neither authorize, unauthorize nor del-onu when onu is registering

add: Add one ONU to authorization list

<mac-address>: ONU

<0-8>: Linknum: link number

authorize: Authorize onu in the olt

del: Del many ONUs from authorization list

show: Show onu authorization

unauthorized: Unauthorize onu in the olt

EXAMPLE:

```
Switch(auth)# add 0 00-0a-c2-2e-01-00 8
Switch(auth)# show 0
Idx ONU-MAC            Link #  Status        Mark  Authorized
=== =================  ======  ============  ====  ==========
1   00-0a-c2-2e-01-00  8                           No

Switch(auth)# authorize 0 8

Switch(auth)# del 0 16
Switch(auth)# show 0
Idx ONU-MAC            Link #  Status        Mark  Authorized
=== =================  ======  ============  ====  ==========
Switch(auth)#

Switch(auth)# unauthorize 0 9
```

bc:

The command lets you Enter into Bridging Config Information Management.

Syntax: **bc**

age_limit <mac-address> <1-2> <0-32768>

broadcast-que <mac-address> <1-2> <0-255>

entry_limit <mac-address> <1-2> <0-64>

eth <mac-address> <WORD>

learning_mode <mac-address> <1-2> <0-1>

show <mac-address>

tag_down <mac-address> disable/ enable

tag_up <mac-address> disable/ enable

Parameter: **age_limit:** EPON ONU Bridging Config Age Limit.

<mac-address>: ONU

<1-2>: 1:Port 1, 2:Port 2.

<0-32768>: (Unit:8.75ms), available from 0 to 32768.

broadcast-que: Set onu Broadcast Queue

<0-255>: Queue index: Queue Idx maximum : 255 (disable automaticbroadcast handling)

entry_limit: EPON ONU Bridging Config Entry Limit.

<0-64>: Entry Limit, available from 0 to 64.

eth: EPON ONU VLAN Option Ethertype.

<WORD>: (hexadecimal)

learning_mode: EPON ONU Bridging Config Learning Mode.

<0-1>: Learning mode, 0: Forward (802.1d Learning), 1: Drop Until Learned (MAC Access Control)

show: Show EPON ONU Bridging Config Information

tag_down: Set EPON ONU VLAN Tag Up Mode

disable: Disable EPON ONU VLAN Tag Down

enable: Enable EPON ONU VLAN Tag Down

tag_up: Set EPON ONU VLAN Tag Up Mode

EXAMPLE:

```
Switch(bc)# age_limit b8-26-d4-00-21-d8 1 32768
Switch(bc)# broadcast-que b8-26-d4-00-21-d8 2 255
Switch(bc)# entry_limit b8-26-d4-00-21-d8 1 64
Switch(bc)# eth b8-26-d4-00-21-d8 a
Switch(bc)# learning_mode b8-26-d4-00-21-d8 1 1
Switch(bc)# tag_down b8-26-d4-00-21-d8 enable
Switch(bc)# tag_up b8-26-d4-00-21-d8 enable

Switch(bc)# show b8-26-d4-00-21-d8
ONU Bridging Config :
=====================
Port 1 :
  Age Limit (8.75ms) :    32768
  Entry Limit (Entries) :    64
  Learning Mode :    1: Drop Until Learned (MAC Access Control)
Port 2  :
  Age Limit (8.75ms) :    8192
  Entry Limit (Entries) :    64
  Learning Mode :    0: Forward (802.1d Learning)

ONU VLAN Option :
=================
Vlan Ether Type :    0x a
Tag UP :    Enable
Tag Down :    Enable

ONU Broadcast Queue :
=====================
Port : 1, Queue index : 255
Port : 2, Queue index : 0
```

dt:

The command lets you check the OLT Dynamic table.

Syntax: **dt**

show: show dynamic table

dynamactbl <mac address>

clear: Clear onu dynamic table

.... **dynamactbl** <mac address> <1-2>

Parameter: **<mac-address>:** ONU Mac Address

<1-2> UNI Port 1 or 2

EXAMPLE:

```
Switch(dt)# show dynamactbl b8-26-d4-00-33-08
onu = b8-26-d4-00-33-08
no.    port  mac
=====  ====  =================
No Response
Switch(dt)# clear dynamactbl b8-26-d4-00-33-08
% Incomplete command
Switch(dt)# clear dynamactbl b8-26-d4-00-33-08 ?
  <1-2>                ONU
Switch(dt)# clear dynamactbl b8-26-d4-00-33-08 1
No Response
Switch(dt)# clear dynamactbl b8-26-d4-00-33-08 2
No Response
```

flow-control:

The command lets you set Port Flow Control.

Syntax: **flow-control** <mac-address> <1-2> disable/ enable

Parameter: **<mac-address>:** ONU Mac Address

<1-2>: UNI Port 1 or 2

disable: Disable Port Flow Control

enable: Enable Port Flow Control

EXAMPLE:

```
Switch(onu)# flow-control b8-26-d4-00-21-d8 1 enable
```

green:

The command lets you Enter into ONU Green Pon.

Syntax: **green**

green <mac-address> <0-1>

show green <mac-address>

Parameter: **green:** Set ONU Green Pon.

<mac-address>: ONU Mac Address

<0-1>: 0: disable, 1: enable

show: Show ONU command

green: Show ONU Green Pon

EXAMPLE:

```
Switch(green)# green b8-26-d4-00-21-d8 1
Switch(green)# show green b8-26-d4-00-21-d8
ONU Green Pon                    :enable
ONU Optical Power Save           :enable
LUE Stat Index                   :2
Power Down Transmit Laser        :on
Power Down Receive Laser         :on
Power Down Serdes                :on
Switch(green)#
```

igmp:

The command lets you Enter Igmp Snooping Information.

Syntax: **igmp**

action <mac-address> <0-1>

add vlan <mac-address> <0-4094> <0-4094> <0-255>

del vlan <mac-address> <1-16>

edit vlan <mac-address> <0-4094> <0-4094> <0-255>

show joined/ snooping/ vlan <mac-address>

snooping <mac-address> <0-12> <0-12> <0-90> <0-6> <0-90> <0-6> <0-1> <0-1> <0-1>

Parameter:

action: Set Action for Unmanaged Groups

<mac-address>: ONU

<0-1>: act: Action for Unmanaged Groups

0: Discard (block IPMC, IGMP)

1: Ignore (forward unchanged)

add: Add ONU IGMP Snooping Parameters

vlan: Add ONU IGMP VLAN

<0-4094>: EPON VID

<0-4094>: User VID

<0-255>: MaxGroups: available from 0 to 255.

EPON VID must be the same as User VID.

If you add onu IGMP Vlan Provisioning entry when action is ignore, you must disable onu IGMP snooping first.

del: Delete ONU IGMP Snooping Parameters

<1-16>: vlan group number

If you add onu IGMP Vlan Provisioning entry when action is ignore, you must disable onu IGMP snooping first.

edit: Edit ONU IGMP VLAN Provisioning

show: Show Igmp Snooping Information command

joined: Show IGMP Groups Joined

snooping: Show Igmp Snooping

vlan: Show IGMP VLAN Provisioning

snooping: Set Igmp Snooping

<0-12>: RC: Robustness Count

<0-12>: LMQ: Last Member Query

<0-90>: NG1: Number Of IGMP Groups (Port 1)

<0-6>: QC1: Queue For Classification (Port 1)

<0-90>: NG2: Number Of IGMP Groups (Port 2)

<0-6>: QC2: Queue For Classification (Port 2)

<0-1>: FWbyL2DA: Forward Group by L2 DA. Available Values are '1' = (yes) or '0' = (no).

<0-1>: FWbyVID: Forward Group by VID. Available Values are '1' = (yes) or '0' = (no).

<0-1>: FWbyIPDA: Forward Group by IP DA. Available values are '1' = (yes) or '0' = (no).

Note: At least one of <FWbyL2DA> and <FWbyIPDA> must be (yes).

Note: The total IGMP groups of Port 1 and 2 should not be more than 90.

EXAMPLE:

```
Switch(igmp)# action b8-26-d4-00-21-d8 1
Switch(igmp)# add vlan b8-26-d4-00-21-d8 4094 4094 255
Switch(igmp)# del vLan b8-26-d4-00-21-d8 16
Switch(igmp)# show vlan b8-26-d4-00-21-d8

Action for Unmanaged Groups: Ignore (forward unchanged)
 No    EPON VID    User VID    Max Groups
==== ========== ========== ============
  1     4094        4094         255

Switch(igmp)# edit vlan b8-26-d4-00-21-d8 4094 4094 100
Switch(igmp)# show vlan b8-26-d4-00-21-d8

Action for Unmanaged Groups: Ignore (forward unchanged)
 No    EPON VID    User VID    Max Groups
==== ========== ========== ============
  1     4094        4094         100

Switch(igmp)# snooping b8-26-d4-00-21-d8 12 12 90 6 90 6 1 1 1
Switch(igmp)# show snooping b8-26-d4-00-21-d8

Robustness Count              : 12
Last Member Query             : 12
Port 1 Number Of IGMP Groups   : 90
       Queue For Classification: 6
Port 2 Number Of IGMP Groups   : 90
       Queue For Classification: 6
Forward Group by L2 DA: yes
Forward Group by VID: yes
Forward Group by IP DA: yes
```

ionus-wakeup:

The command allow to wake up Many ONUs.

Syntax: **ionus-wakeup** <0-1> <onu-list>

Parameter: **<0-1> : 0:** epon-1, 1: epon-2

<onu-list> : ONUs range : available from 1 to 64. refer to onulist command

EXAMPLE:

```
Switch(onu)# ionus-wakeup 0 1
Invalid onu number list.The onu list num is 0.
```

lblink:

The command performs the Loopback Test on A Logical Link.

Syntax: **lblink** <mac-address> <1-1000> <46-1500> <0-4094>

Parameter: **<mac-address>:** ONU MAC Address, format : xx-xx-xx-xx-xx-xx

<1-1000>: Number of Frames, available from 1 to 10000, default:100

<46-1500>: Payload Size, available from 46 to 1500, default:100

<0-4094>: VLAN Tag, available from 0 to 4094, disable:0

EXAMPLE:

```
Switch(onu)# lblink b8-26-d4-00-2c-b9 100 100 0
  Description     Value
================ =======
Frames sent         100
Frames received     100
Corrupted frames      0
Minimum Delay      3103
Maximum Delay      8066
Average Delay      4231
```

lbport:

The command performs the Loopback Test on a UNI port.

Syntax: **lbport** <mac-address> <1-2> <1-2> <1-1000> <46-1500> <0-4094>

Parameter:

<mac-address>: ONU MAC Address, format : xx-xx-xx-xx-xx-xx

<1-2>: Port number

<1-2>: Location 1:Mac, 2:Phy

<1-1000>: Number of Frames, available from 1 to 10000, default:100

<46-1500>: Payload Size, available from 46 to 1500, default:100

<0-4094>: VLAN Tag, available from 0 to 4094, disable:0

EXAMPLE:

```
Switch(onu)# lbport b8-26-d4-00-2c-b8 1 1 100 100 0
  Description     Value
================ =======
Frames sent         100
Frames received     100
Corrupted frames      0
Minimum Delay       486
Maximum Delay      5032
Average Delay      4078
```

onu-reset:

The command display Reset EPON ONU.

Syntax: **onu-reset** <mac-address>

Parameter: **<mac-address>:** ONU MAC Address, format : xx-xx-xx-xx-xx-xx

EXAMPLE:

```
Switch(onu)# onu-reset b8-26-d4-00-21-d8
Switch(onu)#
```

onu-restore:

The command lets you Restore EPON ONU

Syntax: **onu-restore** <mac-address>

Parameter: **<mac-address>:** ONU MAC Address, format : xx-xx-xx-xx-xx-xx

EXAMPLE:

```
Switch(onu)# onu-restore b8-26-d4-00-21-d8
Switch(onu)#
```

onus-restore:

The command lets you Restore EPON Many ONUs.

Syntax: **onus-restore** <0-1> <onu-list>

Parameter: **<0-1>:** 0: epon-0, 1: epon-1

<onu-list>: ONUs range : available from 1 to 64. refer to onulist command

EXAMPLE:

```
Switch(onu)# onus-restore 1 10
```

rstp:

The command allow to enable/disable rstp traffic.

Syntax: **rstp**

rstp <mac-address> <0-1>

show rstp <mac-address>

Parameter: **rstp:** Set rstp control config

<mac-address>: ONU MAC Address, format : xx-xx-xx-xx-xx-xx

<0-1>: 0: disabled, 1: pass Through

show: Show onu rstp config

rstp: Show ONU RSTP

<mac-address>: ONU MAC Address, format : xx-xx-xx-xx-xx-xx

EXAMPLE:

```
Switch(rstp)# rstp b8-26-d4-00-2c-b8 1
Switch(rstp)# show rstp b8-26-d4-00-2c-b8
onu = b8-26-d4-00-2c-b8
RSTP Bridge Mode      : Pass Through
```

show:

The command lets you Show ONU command.

Syntax: **show** onuinfo/ onus <mac-address>

Parameter: **onuInfo:** Show General Information Of An ONU

<mac-address>: ONU

onus: Show Registered ONUs

EXAMPLE:

```
Switch(onu)# show onuinfo b8-26-d4-00-21-d8
mac=b8-26-d4-00-21-d8

                                        Attribute
                                      ==================
Model Name                             FK-IONU-20
Serial Number                          12IU20000209
Output Optical Center Wavelength (nm)  1310
Min. TX Power (dBm)                    0
Max. TX Power (dBm)                    4
Min. RX Operating Wavelength (nm)      1480
Max. RX Operating Wavelength (nm)      1500
RX Sensitivity (dBm)                   -26.5
RX Saturation Power (dBm)              -3
Mac Address                            b8-26-d4-00-21-d8
Firmware Version                       0x240
Chip ID                                0x3714
Chip Version                           0xa0060727
Boot Code Version                      0x140
Personality Version                    f10
App0 Version                           0x240
App1 Version                           0x240

Switch(onu)#
Switch(onu)# show onus b8-26-d4-00-21-d8
Port Link State   Auto Nego. Speed/Duplex Flow Control|
---- ---- -------- ---------- ------------ ------------| [b8-26-d4-00-21-d8]
1    Down Enable   Enable     10/Half      Disable
2    Up   Enable   Enable     100/Full     Disable
```

si:

The command lets you Enter into ONU Subscriber Information Management.

Syntax: **si**

alias <mac-address> <WORD>

del alias <mac-address>

descrip <mac-address> <WORD>

show alias <mac-address>

Parameter: **alias:** Set ONU Alias Name.

<mac-address>: ONU

<WORD>: ONU alias name

del: Delete ONU Alias Name

alias: Delete ONU Alias Name

descrip: Set ONU Description.

show: Show ONU command

alias: Show ONU Alias

EXAMPLE:

```
Switch(si)# alias b8-26-d4-00-21-d8 ccc
Switch(si)# descrip b8-26-d4-00-21-d8 ggg
Switch(si)# show alias b8-26-d4-00-21-d8
Alias Name        :ccc
Description       :ggg
Switch(si)#

switch(si)# del alias b8-26-d4-00-21-d8
Switch(si)# show alias b8-26-d4-00-21-d8
Alias Name        :
Description       :
Switch(si)#
```

speed-duplex:

The command lets you set Port Speed and Duplex.

Syntax: **speed-duplex** <mac-address> <1-2> 10/ 100/ 1000/ auto

Parameter:

<mac-address>: ONU

<1-2>: UNI Port 1 or 2

10: Speed

100: Speed

1000: Speed

auto: Auto Nego.

EXAMPLE:

```
Switch(onu)# speed-duplex b8-26-d4-00-21-d8 2 1000 1
Switch(onu)#
```

sta:

The command lets you Enter into Statistic Information Management.

Syntax: **sta**

clear/ show <mac-address> <0-2> <0-1>

Parameter:

clear: Clear EPON ONU Port Statistics

show: Show EPON ONU Statistic

<mac-address>: ONU

<0-2>: 0:EPON Port, 1:UNI Port 1, 2:UNI Port 2

<0-1>: 0:Transmit, 1:Receive

EXAMPLE:

```
Switch(sta)# show b8-26-d4-00-21-d8 2 1
UNI Port 2 Statistics
Direction   :  Receive

Bytes   :552558
Frames   :4520
Unicast Frames   :1480
Multicast Frames   :1074
Broadcast Frames   :1966
64-Byte Frames   :2626
65-127 Byte Frames   :919
128-255 Byte Frames   :626
256-511 Byte Frames   :154
512-1023 Byte Frames   :177
1024-1518 Byte Frames   :18
Greater than 1518 Byte Frames   :0
Undersized Frames   :0
Oversized Frames   :0
Pause Frames   :0
LLength Errors   :0
Aligment Errors   :0
CRC-32 Errors   :0
Switch(sta)#
```

state:

The command lets you set Port State.

Syntax: **state** <mac-address> <1-2> disable/ enable

Parameter:

<mac-address>: ONU

<1-2>: UNI Port 1 or 2

disable: Disable Port state

enable: Enable Port state

EXAMPLE:

```
Switch(onu)# state b8-26-d4-00-21-d8 2 disable
```

tm:

The command lets you Enter into Traffic Management Information.

Syntax: **tm**

apply field <0-4> <mac-address> <0-2>

apply queue <0-4> <mac-address>

apply rule <0-19> <0-2>

deltmp **Delete function**

editmp action <0-19> <0-29> <1-4094> <0-8>

editmp clause <0-19> <0-1> <0-10> <0-7> <0-3> <WORD>

editmp downq <0-4> <1-2> <WORD>

editmp field <0-4> <0-10> <0-6> <0-9> <0-31> <1-32>

editmp field_index <0-4> <0-10> <0-37>

editmp rule <0-19> <8-13> <0-19> <WORD>

editmp upq <0-4> <0-7> <WORD>

hint action/ clause

loadtmp field <0-2> <0-4>

loadtmp queue <mac-address> <0-4>

show field <mac-address> <0-2>

show quecfg <mac-address>

show rule <mac-address> <0-2>

show target

showtmp action/ clause/ rule <0-19>

showtmp field/ queue <0-4>

target <mac-address>

Parameter: **apply:** Apply function

field: Apply field select template

<0-4>: template no : 0~4

<mac-address>: ONU, up max queue # is 10, down max queue # is 16 up queue max size is 236,down queue max size is 55

<0-2>: ONU port no, 0-epon port, 1,2-user port

queue: Apply queue template

rule: Apply rule template

<0-19>: Rule template no : 0~19

<0-2>: Source port: ONU port. 0-epon port(downstream), 1,2-user port(upstream)

deltmp: Delete function

editmp: Edit function

action: Edit action template

<0-19>: Action template index(0~19)

<0-29>: Action value (using "hint action" value)

<1-4094>: Action param 1: action needed parameter

Action param 2: action needed parameter

Action value 2, 18 need 2 params

Action value 5,6,8,21,22,24 need only 1 param

Others need no param

<0-8>: Action param 1: action needed parameter

Action param 2: action needed parameter

Action value 2, 18 need 2 params

Action value 5,6,8,21,22,24 need only 1 param

Others need no param

clause: Edit clause template

<0-19>: Clause no: clause index(0~19)

<0-1>: Direction: 1-upstream, 0-downstream

<0-10>: Field select value: (using "hint clause" field selects-value)

<0-7>: Op: operation (using "hint clause" operation-value). if op=0, 5,6,7, it doesn't need type and value

<0-3>: Type: value type , 0:Hex , 1:Decimal , 2:IP format, 3:automatic. When field is User, can't select type automatically

<WORD>: Vaule: operation value. Show help using "hint clause"

downq: Edit down queue template

<0-4>: Down stream queue template no(0~4)

<1-2>: Port no: down stream port no, 1: port 1, 2: port 2; 0 is invalid, each port queue # Maximum is 8

down queue max queue # is 16

<WORD>: Each queue separated by commas

Queue Size Minimum is 2, queue Size Maximum is 100

field: Edit down queue template

<0-4>: Field select template no(0~4)

<0-10>: Field select template index

<0-6>: Layer select: 1:Ethernet Header, 2:Ether Type, 3:VLAN/L2-Frame, 5:Ipv4-Header, 6:Ipv4-Msc

<0-9>: Dword: dword offset, depend on layer select. refer to field-pattern

<0-31>: Bit offset: point to particular areas of interest in a frame. refer to field-pattern

<1-32>: Field width: point to particular areas of interest in a frame

field_index: Edit down queue template

<0-4>: Field select template no(0~4)

<0-10>: Field select template index

<0-37>: Field patterns index: represent the index using field-pattern command

rule: Edit rule template

<0-19>: Rule no: rule index(0~19)

<8-13>: Priority: rule template rule priority(8~13)

<0-19>: Action no: action template index(0~19)

<WORD>: Each clause separated by commas

Clause no: clause index(0~19)

upq: Edit up queue template

<0-4>: Up stream queue template no(0~4)

<0-7>: Up stream queue llid index,each queue # max is 8 up queue max queue # is 10

up queue max queue # is 10

<WORD>: Each queue separated by commas

Queue Size Minimum is 2, queue Size Maximum is 100

hint: Hint function

action: Hint action

clause: Hint clause

loadtmp: Load function

field: Show field select and load to field select template

<0-2>: ONU port no, 0-epon port, 1,2-user port

<0-4>: Field select template no(0~4)

queue: Show queue config and load to queue template

<0-4>: Queue template no(0~4)

show: Show EPON ONU Traffic Management Information

field: Show ONU Field Selects

<0-2>: ONU port no, 0-epon port, 1,2-user port

quecfg: Show ONU Queue Config

rule: Show ONU Rule Table

<0-2>: 0:EPON Port, 1:UNI Port 1, 2:UNI Port 2

target: Show target onu

showtmp: Show function

action: Show action template

<0-19>: Show action template index

clause: Show clause template

field: Show field template

<0-4>: template no : 0~4

queue: Show queue template

rule: Show rule template

target: Set target onu

EXAMPLE:

```
Switch(tm)# apply field 1 b8-26-d4-00-21-d8 2
Switch(tm)# apply queue 4 b8-26-d4-00-21-d8
Switch(tm)# apply rule 19 2
Switch(tm)# target b8-26-d4-00-21-d8
onu mac = b8-26-d4-00-21-d8
Down stream
value Field Selects             Type
===== ======================== ===============
0     L2 Dest Addr              Hex
1     L2 Source Addr            Hex
2     L2 Link Index             Decimal
3     L2 Length/Type            Hex
4     Eth VID                   Decimal
5     Unused                    Hex
6     IPv4 Protocol             Decimal
7     Unused                    Hex
8     Unused                    Hex
9     Unused                    Hex
10    Unused                    Hex
-------------------------------------------------------
Up stream
value Field Selects             Type
===== ======================== ===============
0     L2 Dest Addr              Hex
1     L2 Source Addr            Hex
2     Unused                    Hex
3     L2 Length/Type            Hex
4     Eth VID                   Decimal
5     Unused                    Hex
6     IPv4 Protocol             Decimal
7     Unused                    Hex
8     Unused                    Hex
9     Unused                    Hex
10    Unused                    Hex
-------------------------------------------------------
value Operator
===== ============
0     Fail
1     ==
2     !=
3     <=
4     >=
5     exists
6     !exist
7     True
Switch(tm)#
Switch(tm)# editmp action 0 29
Switch(tm)#
Switch(tm)# editmp clause 19 1 10 1 0 rrr
Switch(tm)# editmp downq 4 1 yyy
Switch(tm)#
Switch(tm)# editmp field 4 10 6 9 31 32
index Name                LayerSel DWord BitOffset FieldWidth
===== ================== ======== ===== ========== ==========
10    User                6        9     31         32
Switch(tm)#
```

```
Switch(tm)# loadtmp field 2 4
Switch(tm)#

Switch(tm)# loadtmp queue b8-26-d4-00-21-d8 4
Up-stream queue config :
link-index  queue set
================================================
0            <16 >
1            <16 >

Down-stream queue config :
port-no     queue set
================================================
1            <22 >
2            <22 >
Switch(tm)#

Switch(tm)# show field b8-26-d4-00-21-d8 2
EPON ONU Field Selects

Index     Name      RefCount     LayerSel     DWord BitOffset FieldWidth
-----  ------------ ----  ------------------ ---  -------   ----------
1    L2 Dest Addr     1       0              0       0           1
2    L2 Source Addr   1       0              0       0           1
3    Unused           0       7              7       31          32
4    L2 Length/Type   8       2              0       0           16
5    Eth VID          4       3              0       16          12
6    Unused           0       7              7       31          32
7    IPv4 Protocol    0       5              2       16          8
8    Unused           0       7              7       31          32
9    Unused           0       7              7       31          16
10   Unused           0       7              7       31          16
11   Unused           0       7              7       31          16

Switch(tm)# show quecfg b8-26-d4-00-21-d8
Up-stream queue config :
link-index  queue set
================================================
0            <16 >
1            <16 >

Down-stream queue config :
port-no     queue set
================================================
1            <22 >
2            <22 >

Switch(tm)# show rule b8-26-d4-00-21-d8 0
onu mac = b8-26-d4-00-21-d8
 (downstream)
================================================
no.                  : 1
priority             : 12
action               : Set Destination; Forward
param                : port-no = 1 ; queue-index = 0
field-selects        : L2 Link Index
operation            : ==
value                : 0
------------------------------------------------------------
no.                  : 2
priority             : 12
action               : Set Destination; Forward
param                : port-no = 2 ; queue-index = 0
field-selects        : L2 Link Index
operation            : ==
value                : 1
------------------------------------------------------------
Switch(tm)#
Switch(tm)# show target
onu mac = b8-26-d4-00-21-d8
Switch(tm)#
```

8.17 Privilege level Commands of CLI

privilege

This page provides an overview of the privilege levels.

privilege Commands

Command	Function
group	Configure a privilege level group
show	Show privilege configuration

group:

The command lets you configure a privilege level group

Syntax: **group** <group-name> <1-15>

Parameter: **<group-name>:** Privilege group name

<1-15>: Privilege level

EXAMPLE:

```
Switch(privilege)# group account 13
Switch(privilege)# show
Privilege Current Level: 15

Group Name                      Privilege Level
------------------------------  ----------------
Account                         13
Aggregation                     10
Diagnostics                     10
```

show:

The command lets you show privilege configuration

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(privilege)# show
Privilege Current Level: 15

Group Name                      Privilege Level
------------------------------  ----------------
Account                         10
Diagnostics                     10
IP                              10
Maintenance                     15
OLT                             10
ONU                             10
SMTP                            10
SNMP                            10
Security                        10
System                          10
Trap_Event                      10
login protect                   10
```

8.18 Reboot Commands of CLI

Reboot

This section describes how to restart switch for any maintenance needs. Any configuration files or scripts that you saved in the switch should still be available afterwards.

Table 17: Reboot Commands

Command	Function
reboot	Reboot the system

reboot:

The command lets you reboot the system

Syntax: **Reboot** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch# reboot
```

8.19 SMTP Commands of CLI

SMTP

The function, is used to set a Alarm trap when the switch alarm then you could set the SMTP server to send you the alarm mail.

SMTP Commands

Command	Function
delete	Delete command
level	Configure Severity level
mail-address	Configure email user name
return-path	Configure email sender
sender	Configure email sender
server	Configure email server
show	Show email configuration
username	Show DHCP snooping information

delete:

The command lets you delete command

Syntax: **delete** mail-address <1-6>
return-path/ sender/ server/ username

Parameter: **mail-address:** Delete email address
<1-6>: Delete email address id
return-path: Delete return path
sender: Delete sender
server: Delete email server
username: Delete username and password

EXAMPLE:

```
Switch(smtp)# delete mail-address 2
Switch(smtp)# show
Mail Server     :
User Name       :
Password        :
Severity level  : Info
Sender          :
Return Path     :
Email Adress 1  :
Email Adress 2  :
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  :
```

level:

The command lets you configure Severity level

Syntax: **level** <0-7>

Parameter: **<0-7>:** Severity level <0> Emergency: system is unusable
<1> Alert: action must be taken immediately
<2> Critical: critical conditions
<3> Error: error conditions
<4> Warning: warning conditions
<5> Notice: normal but significant condition
<6> Informational: informational messages
<7> Debug: debug-level messages

EXAMPLE:

```
Switch(smtp)# level 7
Switch(smtp)# show
Mail Server     :
User Name       :
Password        :
Severity level  : Debug
Sender          :
Return Path     :
Email Adress 1  :
Email Adress 2  :
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  :
```

mail-address:

The command lets you configure email user name.

Syntax: **mail-address** <1-6> <mail-address>

Parameter: **<1-6>:** Email address index

<mail-address>: Up to 47 characters describing mail address

EXAMPLE:

```
Switch(smtp)# mail-address 6 david@tech.com.tw
Switch(smtp)# show
Mail Server     :
User Name       :
Password        :
Severity level  : Debug
Sender          :
Return Path     :
Email Adress 1  :
Email Adress 2  :
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  : david@tech.com.tw
```

return-path:

The command lets you configure the address of email sender

Syntax: **return-path** <return-path>

Parameter: **<return-path>:** Up to 47 characters describing return path

EXAMPLE:

```
Switch(smtp)# return-path david@tech.com.tw
Switch(smtp)# show
Mail Server      :
User Name        :
Password         :
Severity level   : Debug
Sender           :
Return Path      : david@tech.com.tw
Email Adress 1   :
Email Adress 2   :
Email Adress 3   :
Email Adress 4   :
Email Adress 5   :
Email Adress 6   : david@tech.com.tw
```

sender:

The command lets you configure email sender

Syntax: **sender** <sender>

Parameter: **<sender>:** Up to 47 characters describing sender

EXAMPLE:

```
Switch(smtp)# sender tech
Switch(smtp)# show
Mail Server      :
User Name        :
Password         :
Severity level   : Debug
Sender           : david
Return Path      : david@mail. tech.com.tw
Email Adress 1   :
Email Adress 2   :
Email Adress 3   :
Email Adress 4   :
Email Adress 5   :
Email Adress 6   : david@tech.com.tw
```

server:

The command lets you configure email server

Syntax: **server <**server>

Parameter: **<server>:** Up to 47 characters describing email server

EXAMPLE:

```
Switch(smtp)# server davidserver
Switch(smtp)# show
Mail Server      : davidserver
User Name        :
Password         :
Severity level   : Debug
Sender           : davidtech
Return Path      : david@mail.davidtech.com.tw
Email Adress 1   :
Email Adress 2   :
Email Adress 3   :
Email Adress 4   :
Email Adress 5   :
Email Adress 6   : jack@davidtech.com.tw
```

show:

The command lets you show email configuration

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

NOTE: When enable DHCP snooping mode operation, the request DHCP messages will be forwarded to trusted ports and only allowed reply packets from trusted ports.

EXAMPLE:

```
Switch(smtp)# show
Mail Server     :
User Name       :
Password        :
Severity level  : Info
Sender          :
Return Path     :
Email Adress 1  :
Email Adress 2  :
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  :
```

username:

The command lets you configure email user name

Syntax: **mode** username password

Parameter: **<username>:** Up to 47 characters describing user name

<password>: Up to 47 characters describing password

EXAMPLE:

```
Switch(smtp)# username david 1111
Switch(smtp)# show
Mail Server     : davidserver
User Name       : david
Password        : ********
Severity level  : Debug
Sender          : davidtech
Return Path     : david@mail.davidtech.com.tw
Email Adress 1  :
Email Adress 2  :
Email Adress 3  :
Email Adress 4  :
Email Adress 5  :
Email Adress 6  : rose@davidtech.com.tw
```

8.20 SNMP Commands of CLI

SNMP

Any Network Management System (NMS) running the Simple Network Management Protocol (SNMP) can manage the Managed devices equipped with SNMP agent, provided that the Management Information Base (MIB) is installed correctly on the managed devices. The SNMP is a protocol that is used to govern the transfer of information between SNMP manager and agent and traverses the Object Identity (OID) of the management Information Base (MIB), described in the form of SMI syntax. SNMP agent is running on the switch to response the request issued by SNMP manager.

Basically, it is passive except issuing the trap information. The switch supports a switch to turn on or off the SNMP agent. If you set the field SNMP "Enable", SNMP agent will be started up. All supported MIB OIDs, including RMON MIB, can be accessed via SNMP manager. If the field SNMP is set "Disable", SNMP agent will be de-activated, the related Community Name, Trap Host IP Address, Trap and all MIB counters will be ignored.

SNMP Commands

Command	Function
access	Configure SNMP access
community	Configure SNMP community
delete	Delete command
engine-id	Set SNMP Engine ID
group	Configure SNMP groups
mode	Enable/Disable SNMP mode
show	Show SNMP command
trap	Configure SNMP trap
user	Configure SNMP users
view	Configure SNMP views

access:

The command lets you configure SNMP access

Syntax:

access any/ usm AuthNoPriv/ AuthPriv/ NoAuthNoPriv <WORD> <WORD>

access v1/ v2c AuthNoPriv <WORD> <WORD>

Parameter:

<WORD>: group name: max 32 chars

any: Security Model

usm: Security Model

AuthNoPriv: Security Level. If security_model is not usm, the security_level value must be NoAuthNoPriv

AuthPriv: Security Level. If security_model is not usm, the security_level value must be NoAuthNoPriv

NoAuthNoPriv: Security Level. If security_model is not usm, the security_level value must be NoAuthNoPriv

<WORD>: read_view_name: The scope for a specified instance can read, None is reserved for Empty.

<WORD>: write_view_name: The scope for a specified instance can write,None is reserved for Empty.

v1: Security Model

v2c: Security Model

AuthNoPriv: Security Level. If security_model is not usm, the security_level value must be NoAuthNoPriv

EXAMPLE:

```
Switch(snmp)# access g usm noAuthNoPriv v v
Switch(snmp)# show access

SNMPv3 Accesses Table:
Idx    Group Name     Model SecurityLevel   Read View Name  Write View Name
--- ---------------- ----- -------------- ---------------- ----------------
1   g                usm   NoAuth, NoPriv v                v
```

comminity:

The command lets you configure SNMP community

Syntax: **community** <WORD> <WORD> <ip-address> <ip-mask>

Parameter: **<WORD>**: community: max 32 chars<60-1400> Size of ICMP echo packet

<WORD>: user name: max 32 chars

<ip-address>: SNMP access source ip

<ip-mask>: SNMP access source address mask

EXAMPLE:

```
Switch(snmp)# community david pm 192.168.6.127 255.255.255.0
Switch(snmp)# show community

SNMP Community Table:
Idx Community        UserName         Source IP       Source Mask
--- ---------------- ---------------- --------------- ---------------
1   david             pm               192.168.6.127   255.255.255.0

Number of entries: 1
```

delete:

The command lets you delete command

Syntax: **delete** access/ community/ group/ trap/ user/ view <1-14>/<1-4>/<1-6>/<1-10>/<1-48>

Parameter: **access:** Delete snmpv3 access entry

<1-14>: table index

community: Delete community entry

<1-4>: table index

group: Delete snmpv3 groups entry

<1-14>: table index

trap: Delete trap entry

<1-6>: table index

user: Delete snmpv3 users entry

<1-10>: table index

view: Delete snmpv3 views entry

<1-48>: table index

EXAMPLE:

```
Switch(snmp)# delete access 14
```

engine-id:

The command lets you set SNMP Engine ID.

Syntax: **engine-id** <HEX>

Parameter: **<HEX>**: the format may not be all zeros or all 'ff'H,and is restricted to 5 - 32 octet string

EXAMPLE:

```
Switch(snmp)# engine-id ffffffffffffffff
```

group:

The command lets you configure SNMP groups.

Syntax: **group** <WORD> usm/ v1/ v2c

Parameter: **<WORD>**:user name: max 32 chars

usm: Security Model

v1: Security Model

v2c: Security Model

EXAMPLE:

```
Switch(snmp)# group pm v1 ccc
Switch(snmp)# show group

SNMPv3 Groups Table:
Idx Model Security Name                     Group Name
--- ----- --------------------------------- --------------------------------
1   v1    pm                                ccc

Number of entries: 1


Switch(snmp)# group pm v2c aaa
Switch(snmp)# show group

SNMPv3 Groups Table:
Idx Model Security Name                     Group Name
--- ----- --------------------------------- --------------------------------
1   v2c   pm                                aaa
```

mode:

The command lets you Enable/Disable SNMP mode.

Syntax: **mode** disable/ enable

Parameter: **disable:** Disable SNMP mode

enable: Enable SNMP mode

EXAMPLE:

```
Switch(snmp)# mode enable
Switch(snmp)# show mode

SNMPv3 State Show
SNMP State           : Enabled
SNMPv3 Engine ID     : 80001455030040c7232600
```

show:

The command lets you show SNMP command.

Syntax: **show** access/ community/ group/ mode/ snmp/ trap/ user/ view

Parameter:

access: Show snmpv3 access entry

community: Show snmpv3 community entry

group: Show snmpv3 groups entry

mode: Show snmp configuration

snmp: Show snmp community configuration

trap: Show snmp trap entry

user: Show snmpv3 users entry

view: Show snmpv3 views entry

EXAMPLE:

```
Switch(snmp)# show access

SNMPv3 Accesses Table:
Idx    Group Name    Model SecurityLevel   Read View Name  Write View Name
--- ---------------- ----- -------------- ---------------- ----------------

Number of entries: 0

Switch(snmp)# show community

SNMP Community Table:
Idx Community        UserName         Source IP       Source Mask
--- ---------------- ---------------- --------------- ---------------
1   david             pm               192.168.6.127   255.255.255.0

Number of entries: 1
```

trap:

The command lets you configure SNMP trap

Syntax: **trap** <1-6> v2/ v3 ipv4/ ipv6 <ip-address> <1-65535> <0-7>

Parameter:

<1-6>: trap index : 1 - 6

v2: version

v3: version

ipv4: Trap host IP type

ipv6: Trap host IP type

<ip-address>: Trap host IPv4 address

<1-65535>: trap port

<0-7> Severity level

- **<0>** Emergency: system is unusable
- **<1>** Alert: action must be taken immediately
- **<2>** Critical: critical conditions
- **<3>** Error: error conditions
- **<4>** Warning: warning conditions
- **<5>** Notice: normal but significant condition
- **<6>** Informational: informational messages
- **<7>** Debug: debug-level messages

EXAMPLE:

```
Switch(snmp)# trap 2 v2 ipv4 192.168.6.127 65535 7 aaa
Switch(snmp)# show trap
SNMPv3 Trap Host Configuration:

                                Community                    Severity     Auth.
Priv.
No Ver Server IP       Port Security Name          Level     Protocol  Protocol
-- --- --------------- ---- ---------------------- --------- --------- -------
-
1
2  v2c 192.168.6.127   65535 aaa                     Debug
3
4
```

user:

The command lets you configure SNMP users

Syntax: **user** <WORD> AuthNoPriv/ AuthPriv/ NoAuthNoPriv MD5/ SHA <WORD>

Parameter:

<WORD>: user name: max 32 chars

AuthNoPriv: Security_Level

AuthPriv: Security_Level

NoAuthNoPriv: Security_Level

MD5: Authentication Protocol

SHA: Authentication Protocol

<WORD>: MD5 Authentication Password is restricted to 8 - 32

EXAMPLE:

```
Switch(snmp)# user wade authnoPriv md5 12345678
Switch(snmp)# show user

SNMPv3 Users Table:
Index User Name                       Security Level Auth Priv
----- ------------------------------- -------------- ---- ----
1     wade                            AuthNoPriv     MD5  None

Number of entries: 1
```

view:

The command lets you configure SNMP views

Syntax: **view** <WORD> excluded/ included <WORD>

Parameter:

<WORD>: view name: max 32 chars

excluded: view_type

included: view_type

<WORD>: oid_subtree: The OID defining the root of the subtree.

EXAMPLE:

```
Switch(snmp)# view viewdavid included .1.3.6.1.2
Switch(snmp)# show view

SNMPv3 Views Table:
Idx View Name                       View Type OID Subtree
--- ------------------------------- --------- --------------------------------
1   viewdavid                       included  .1.3.6.1.2
```

8.21 SSH Commands of CLI

SSH

This section shows you to use SSH (Secure SHell) to securely access the Switch. SSH is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication.

SSH Commands

Command	Function
mode	Configure the SSH mode
show	Show SSH configuration

mode:

The command lets you configure the SSH mode

Syntax: **mode** disable/ enable

Parameter: **disable:** Disable SSH mode operation

enable: Enable SSH mode operation

EXAMPLE:

```
Switch(ssh)# mode enable
Switch(ssh)# show
SSH Mode : Enabled
```

show:

The command lets you show SSH configuration

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(ssh)# show
SSH Mode : Enabled
```

8.22 Syslog Commands of CLI

Syslog

The Syslog is a standard for logging program messages . It allows separation of the software that generates messages from the system that stores them and the software that reports and analyzes them. It can be used as well a generalized informational, analysis and debugging messages. It is supported by a wide variety of devices and receivers across multiple platforms.

Syslog Commands

Command	Function
clear	Clear syslog entry
level	Configure syslog level
mode	Configure syslog mode
server	Configure syslog server IP address
show	Show syslog information

clear:

The command lets you Clear syslog entry

Syntax: **clear** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(syslog)# clear
Switch(syslog)# show log
<0> Emergency: 0
<1> Alert    : 0
<2> Critical : 0
<3> Error    : 0
<4> Warning  : 0
<5> Notice   : 0
<6> Info     : 0
<7> Debug    : 0
    All      : 0

ID   Level     Time                Message
---- --------- ------------------- ---------------------------------------
<none>
```

level:

The command lets you Configure syslog lev

el**Syntax:** **level** <0-7>

Parameter: **<0-7>:** Severity level

- **<0>** Emergency: system is unusable
- **<1>** Alert: action must be taken immediately
- **<2>** Critical: critical conditions
- **<3>** Error: error conditions
- **<4>** Warning: warning conditions
- **<5>** Notice: normal but significant condition
- **<6>** Informational: informational messages
- **<7>** Debug: debug-level messages

EXAMPLE:

```
Switch(syslog)# level 7
Switch(syslog)# show config
Server Mode      : Disabled
Server Address 1 :
Server Address 2 :
Syslog Level     : Debug
```

mode:

The command lets you Configure syslog mode

Syntax: **mode** disable/ enable

Parameter: **disable:** Disable syslog mode

enable: Enable syslog mode

EXAMPLE:

```
Switch(syslog)# mode enable
Switch(syslog)# show config
Server Mode      : Enabled
Server Address 1 :
Server Address 2 :
Syslog Level     : Debug
```

server:

The command lets you Configure syslog server IP address

Syntax: **server** <1-2> <ip-hostname>

Parameter: **<1-2>:** Syslog Server No.

<ip-hostname>: Syslog server IP address or host name

EXAMPLE:

```
Switch(syslog)# server 2 192.168.6.1
Switch(syslog)# show config
Server Mode      : Enabled
Server Address 1 :
Server Address 2 : 192.168.6.1
Syslog Level     : Debug
```

show:

The command lets you Show syslog information

Syntax: **show** config

show detail-log <log-id>

show log <0-7>

Parameter: **config:** Show syslog configuration

detail-log: Show detailed syslog information

<log-id>: Log ID

log: Show syslog entry

<0-7> : Show syslog entry that match the level

EXAMPLE:

```
witch(syslog)# show config
Server Mode      : Disabled
Server Address 1 :
Server Address 2 :
Syslog Level     : Info


Switch(syslog)# show detail-log 2
ID      : 2
Level   : Warning
Time    : 2011-01-01 01:00:27
Message:

Link up on port 2


Switch(syslog)# show log 2
<0> Emergency: 0
<1> Alert    : 0
<2> Critical : 0
<3> Error    : 0
<4> Warning  : 8
<5> Notice   : 0
<6> Info     : 12
<7> Debug    : 0
    All      : 20

ID   Level     Time                Message
---- --------- ------------------- ------------------------------------
<none>
```

8.23 System Commands of CLI

System

System Commands

Command	Function
contact	Configure system contact
location	Configure system location
name	Configure device name
show	Show system information

contact:

The command lets you Configure system contact

Syntax: **contact** <LINE>

Parameter **<LINE>:** Up to 255 characters describing system contact information

EXAMPLE:

```
Switch(system)# contact david +55413333333
Switch(system)# show
Model Name                      : FK-C2-RADC
System Description              : OLT 2 EPON 2 NNI
Location                        :
Contact                         : david +55413333333
Device Name                     : FK-C2-RADC
System Uptime                   : 15:53:42
Current Time                    : 2011-01-01 15:53:42
BIOS Version                    : v1.00
Firmware Version                : v1.27
Hardware-Mechanical Version     : v1.01-v1.01
Series Number                   : 12LT22000036
Host IP Address                 : 10.150.4.253
Subnet Mask                     : 255.255.255.0
Gateway IP Address              : 10.150.4.254
Host MAC Address                : b8-26-d4-1c-6c-37
Console Baudrate                : 115200
RAM Size                        : 64
Flash Size                      : 16
CPU Load (100ms, 1s, 10s)       : 0%, 0%, 0%
Bridge FDB Size                 : 8192 MAC addresses
Transmit Queue                  : 8 queues per port
Maximum Frame Size              : 9600
```

location:

The command lets you Configure system location

Syntax: **location** <LINE>

Parameter **<LINE>:** Up to 255 characters describing system location

EXAMPLE:

```
Switch(system)# location Curitiba
Switch(system)# show
Model Name                    : FK-C2-RADC
System Description            : OLT 2 EPON 2 NNI
Location                      : Curitiba
Contact                       : david +55413333333
Device Name                   : FK-C2-RADC
System Uptime                 : 15:54:48
Current Time                  : 2011-01-01 15:54:48
BIOS Version                  : v1.00
Firmware Version              : v1.27
Hardware-Mechanical Version   : v1.01-v1.01
Series Number                 : 12LT22000036
Host IP Address               : 10.150.4.253
Subnet Mask                   : 255.255.255.0
Gateway IP Address            : 10.150.4.254
Host MAC Address              : b8-26-d4-1c-6c-37
Console Baudrate              : 115200
RAM Size                      : 64
Flash Size                    : 16
CPU Load (100ms, 1s, 10s)     : 0%, 0%, 0%
Bridge FDB Size               : 8192 MAC addresses
Transmit Queue                : 8 queues per port
Maximum Frame Size            : 9600
```

name:

The command lets you Configure device name

Syntax: **name** <WORD>

Parameter : **<WORD>:** Up to 255 characters describing device name

EXAMPLE:

```
Switch(system)# name eponolt
Switch(system)# show
Model Name                    : FK-C2-RADC
System Description            : OLT 2 EPON 2 NNI
Location                      : Curitiba
Contact                       : david +55413333333
Device Name                   : eponolt
System Uptime                 : 15:57:52
Current Time                  : 2011-01-01 15:57:52
BIOS Version                  : v1.00
Firmware Version              : v1.27
Hardware-Mechanical Version   : v1.01-v1.01
Series Number                 : 12LT22000036
Host IP Address               : 10.150.4.253
Subnet Mask                   : 255.255.255.0
Gateway IP Address            : 10.150.4.254
Host MAC Address              : b8-26-d4-1c-6c-37
Console Baudrate              : 115200
RAM Size                      : 64
Flash Size                    : 16
CPU Load (100ms, 1s, 10s)     : 0%, 0%, 0%
Bridge FDB Size               : 8192 MAC addresses
Transmit Queue                : 8 queues per port
Maximum Frame Size            : 9600
```

show:

The command lets you Show system information

Syntax: **show** <cr>

Parameter: **<cr>** means it without any parameter needs to type.

EXAMPLE:

```
Switch(system)# show
Model Name                      : FK-C2-RADC
System Description              : OLT 2 EPON 2 NNI
Location                        : Curitiba
Contact                         : david +55413333333
Device Name                     : eponolt
System Uptime                   : 15:58:33
Current Time                    : 2011-01-01 15:58:33
BIOS Version                    : v1.00
Firmware Version                : v1.27
Hardware-Mechanical Version     : v1.01-v1.01
Series Number                   : 12LT22000036
Host IP Address                 : 10.150.4.253
Subnet Mask                     : 255.255.255.0
Gateway IP Address              : 10.150.4.254
Host MAC Address                : 00-40-c7-1c-6c-37
Console Baudrate                : 115200
RAM Size                        : 64
Flash Size                      : 16
CPU Load (100ms, 1s, 10s)       : 0%, 0%, 0%
Bridge FDB Size                 : 8192 MAC addresses
Transmit Queue                  : 8 queues per port
Maximum Frame Size              : 9600
```

8.24 System time Commands of CLI

Time

This page configure the switch Time. Time configure is including Time Configuration and NTP Configuration
The switch provides manual and automatic ways to set the system time via NTP. Manual setting is simple and you just input “Year”, “Month”, “Day”, “Hour”, “Minute” and “Second” within the valid value range indicated in each item.

Time Commands

Command	Function
clock-source	Enable/Diable applicant administrative control
daylight	Set the GARP join timer configuration
delete	Set the GARP leave all timer configuration
manual	Set the GARP leave timer configuration
ntp	Configure NTP server
show	Show the GARP configuration
time-zone	Configure system time zone

clock-source:

The command lets you configure the clock source

Syntax: **clock-source** local/ ntp

Parameter :
local: Local settings
ntp: Use NTP to synchronize system clock

EXAMPLE:

```
Switch(time)# clock-source ntp
Switch(time)# show daylight
Clock Source          : NTP Server
Local Time            : 2011-01-01 07:19:44 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 0 (min)
Daylight Savings      : Disabled
```

daylight:

The command lets you indicates the Daylight Savings operation

Syntax: **daylight** disable

enable <1-1440> By-dates <YYYY:MM:DD> <HH:MM> <YYYY:MM:DD> <HH:MM>

enable <1-1440> Recurring <DAY> <WORD> <MONTH> <HH:MM> <DAY> <WORD> <MONTH> <HH:MM>

Parameter: **disable**: Disable Daylight Savings operation

enable: Enable Daylight Savings operation

<1-1440>: Minute. Time Set Offset.

By-dates: Manually enter day and time that DST starts and ends

<YYYY:MM:DD>: Day that DST starts

<HH:MM>: Time that DST starts

<YYYY:MM:DD>: Day that DST ends

<HH:MM>: Time that DST ends

Recurring: DST occurs on the same date every year

<DAY>: Sun, Mon, Tue, Wed, Thu, Fri, Sat at which DST begins every year

<WORD>: first, 2, 3, 4, last at which DST begins every year

<MONTH>: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec at which DST begins every year

<HH:MM>: The time at which DST begins every year

<DAY>: Sun, Mon, Tue, Wed, Thu, Fri, Sat at which DST ends every year

<WORD>: first, 2, 3, 4, last at which DST ends every year

<MONTH>: Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, Dec at which DST ends every year

<HH:MM>: The time at which DST ends every year

EXAMPLE:

```
Switch(time)# daylight enable 1440 by-dates 2012:03:01 10:00 2012:04:01 09:00
Switch(time)# show daylight
Clock Source          : NTP Server
Local Time            : 2011-01-01 07:23:21 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 0 (min)
Daylight Savings      : Enabled
Time Set Offset       : 1440 (min)
Daylight Savings Type : By dates
From                  : 2012-03-01 10:00 (YYYY-MM-DD HH:MM)
To                    : 2012-04-01 09:00 (YYYY-MM-DD HH:MM)


Switch(time)# daylight enable 1000 recurring wed 2 jan 11:00 sun 3 may 12:00
Switch(time)# show daylight
Clock Source          : NTP Server
Local Time            : 2011-01-01 07:28:43 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 0 (min)
Daylight Savings      : Enabled
Time Set Offset       : 1000 (min)
Daylight Savings Type : Recurring
From                  : Day:Wed Week:2     Month:Jan Time:11:00
To                    : Day:Sun Week:3     Month:May Time:12:00
```

delete:

The command lets you delete NTP server

Syntax: **delete** <1-5>

Parameter: **<1-5>:** NTP server index

EXAMPLE:

```
Switch(time)# delete 1
```

manual:

The command lets you configure system time manually

Syntax: **manual** <YYYY:MM:DD> <HH:MM:SS>

Parameter: **<YYYY:MM:DD>**: Date of system, example: 2011:06:25

<HH:MM:SS>: Time, example: 23:10:55

EXAMPLE:

```
Switch(time)# manual 2011:12:12 10:00:00
Switch(time)# show daylight
Clock Source          : Local Settings
Local Time            : 2011-12-12 10:00:07 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 0 (min)
Daylight Savings      : Enabled
Time Set Offset       : 1000 (min)
Daylight Savings Type : Recurring
From                  : Day:Wed Week:2     Month:Jan Time:11:00
To                    : Day:Sun Week:3     Month:May Time:12:00
```

ntp:

The command lets you configure NTP server

Syntax: **ntp** <1-5> <ipv6-address>/<ip-hostname>

Parameter: **<1-5>:** NTP server index

<ipv6-address>: NTP server IPv6 address

IPv6 address is in 128-bit records represented as eight fields of up to four hexadecimal digits with a colon separates each field (:). For example, 'fe80::215:c5ff:fe03:4dc7'. The symbol '::' is a special syntax that can be used as a shorthand way of representing multiple 16-bit groups of contiguous zeros; but it can only appear once. It also used a following legally IPv4 address. For example, '::192.1.2.34'

<ip-hostname>: NTP server IP address or hostname

EXAMPLE:

```
Switch(time)# ntp 1 64.90.182.55
Switch(time)# show ntp
Index    Server IP host address or a host name string
-----    ----------------------------------------------------
1        64.90.182.55
```

show:

The command lets you show time information

Syntax: **show** daylight/ ntp

Parameter: **daylight**: Show time information

ntp: Show NTP information

EXAMPLE:

```
Switch(time)# show daylight
Clock Source          : Local Settings
Local Time            : 2011-01-01 07:17:29 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 0 (min)
Daylight Savings      : Disabled


Switch(time)# show ntp
Index    Server IP host address or a host name string
-----    ----------------------------------------------------
1
2
3
4
5
```

time-zone:

The command lets you configure system time zone

Syntax: **time-zone** <HH:MM>

Parameter: **<HH:MM>:** The time difference between GMT and local time, the possible value is from GMT-12:00 to GMT+12:00

EXAMPLE:

```
Switch(time)# time-zone 01:00
Switch(time)# show daylight
Clock Source          : NTP Server
Local Time            : 2011-12-12 11:14:24 (YYYY-MM-DD HH:MM:SS)
Time Zone Offset      : 60 (min)
Daylight Savings      : Enabled
Time Set Offset       : 1000 (min)
Daylight Savings Type : Recurring
From                  : Day:Wed Week:2     Month:Jan Time:11:00
To                    : Day:Sun Week:3     Month:May Time:12:00
```

8.25 Global Commands of CLI

global

The Global commands is probably the most commonly used in the CLI console. It is used for global configuration at any level of command.

Global Commands

Command	Function
auto-logout	Configure time of inactivity before automatic logout
exit	Exit from current mode
help	Show available commands
history	Show a list of previously run commands
ionudilist	Show ionu digital-io config list Of an OLT
logout	Disconnect
onulist	Show onu list Of an OLT
quit	Disconnect
restore	Restore running configuration
save	Save running configuration

auto-logout:

The command lets you Configure time of inactivity before automatic logout

Syntax: **auto-logout** <10-3600>

Parameter: **<10-3600>:** Time in seconds of inactivity before automatic logout

EXAMPLE:

```
Switch# auto-logout 3600
```

exit:

The command lets you Exit from current mode

Syntax: **exit**

Parameter: **<cr>:** means it without any parameter needs to type.

EXAMPLE:

```
Switch(aaa)# exit
Switch#
```

help:

This command lets you Show available commands

Syntax: **help**

Parameter: **<cr>:** means it without any parameter needs to type.

EXAMPLE:

```
Switch# help

Commands available:
  aaa                   Authentication, Authorization, Accounting
  access                Access management
  account               User account management
  auth                  Authentication method
  config-file           Export/Import configuration file from/to TFTP Server
  diagnostic            Diagnostic tools
  event                 Trap event severity level
  firmware              Firmware upgrade
  https                 Hypertext Transfer Protocol over Secure Socket Layer
  ip                    System internet protocol
  ipv6                  System IPv6 address
  link                  Enter into Logical Link Management
  login-protect         Login Protect method
  olt                   Enter into OLT Management
  onu                   Enter into ONU Management
  privilege             Privilege level
  reboot                Reboot the system
  smtp                  Email information
  snmp                  Simple Network Managemant Protocol
  ssh                   Secure Shell
  syslog                Syslog configuration
 --More--, q to quit
```

history:

This command lets you Show a list of previously run commands

Syntax: **history**

Parameter: **<cr>:** means it without any parameter needs to type.

EXAMPLE:

```
Switch# history

Command history:
  0. help
  1. history
  2. 0
  3. history
  4. 3
  5. history
```

ionudilist:

This command lets you check the ionu digital-io config list of an OLT

Syntax: **ionulist <0-1> <0-1>**

Parameter: **<0-1>: 0:EPON-1, 1:EPON-2**

<0-1>: 0:sort by mac 1:sort by alias

EXAMPLE:

```
Switch# ionudilist 1 0
index   onu mac            model name              DI-4      DO-1 Count
                           alias name
================================================================================
    1   b8-26-d4-00-2c-b8  FK-IONU-20/DS            Pick Up   0

    2   b8-26-d4-00-33-08  FK-IONU-20/DS            Pick Up   0
```

logout:

This command lets you Disconnect

Syntax: **logout**

Parameter: **<cr>:** means it without any parameter needs to type.

EXAMPLE:

```
Switch# logout
Username:
```

onulist:

This command lets you check the onu list of an OLT.

Syntax: **onulist <0-1>**

Parameter: **<0-1> : 0:EPON-1, 1:EPON-2**

EXAMPLE:

```
Switch# onulist 1
index  onu mac           Register  All Links#  Active Link  Power Save  Green
                         alias name               model name
=============================================================================
==
    1  b8-26-d4-00-2c-b8  Yes       2           2            Y           Y
                                                 FK-IONU-20/DS
    2  b8-26-d4-00-33-08  Yes       2           2            Y           Y
                                                 FK-IONU-20/DS
```

quit:

This command lets you Disconnect

Syntax: **quit**

Parameter : **<cr>:** means it without any parameter needs to type.

EXAMPLE:

```
Switch# quit
Username:
```

restore:

This command lets you Restore running configuration

Syntax:

restore default keep-ip/ <cr>

restore user

Parameter:

default: Restore configuration as factory default

user: Restore configuration as user configuration

keep-ip: Restore configuration as factory default unless ip address

<cr>

EXAMPLE:

```
Switch# restore default keep-ip
Switch# restore user
```

save:

This command lets you Save running configuration

Syntax: **save** start/ user

Parameter

start: Save running configuration as start configuration

user: Save running configuration as user configuration

EXAMPLE:

```
Switch# save start

Switch# save user
```

FURUKAWA

PRODUCTION CENTERS

BRAZIL

HEAD OFFICE
CURITIBA - PR
R. Hasdrubal Bellegard, 820
Cidade Industrial
CEP: 81460-120
Tel.: (41) 3341-4200
Fax: (41) 3341-4141
E-mail: fisa@furukawa.com.br

ARGENTINA
Ruta Nacional 2, km 37,5
Centro Industrial Ruta 2
Berazategui
Província de Buenos Aires
Tel.: (54 22) 2949-1930

COLOMBIA
Kilometro 6 via Yumbo-Aeropuerto,
Zona Franca del Pacifico
Lotes 1-2-3 Manzana J, Bodega 2
Palmira - Valle del Cauca

OFFICE

BRAZIL

SÃO PAULO - SP
Av. das Nações Unidas, 11.633
14º andar - Ed. Brasilinterpart
CEP: 04578-901
Tel.: (11) 5501-5711
Fax: (11) 5501-5757
E-mail: mercosur@furukawa.com.br

CURITIBA - PR
Tel.: (41) 3341-4275
E-mail: latinoamerica@furukawa.com.br

ARGENTINA
OFFICE - BUENOS AIRES
Moreno, 850 - Piso 15B
Cód. Postal C1091AAR
Ciudad Autónoma de Buenos Aires
Tel.: (54 11) 4331-2572
E-mail: argentina@furukawa.com.br

DISTRIBUTION CENTERS

BRAZIL

CURITIBA - PR
R. Hasdrubal Bellegard, 820
Cidade Industrial
CEP: 81460-120
Curitiba - PR

ARGENTINA
BUENOS AIRES
Ruta Nacional 2, km 37,5
Centro Industrial Ruta 2
Berazategui
Província de Buenos Aires
Tel.: (54 22) 2949-1930

www.furukawa.com.br