



DPN-6608

User Manual

The information contained in this document is subject to change without prior notice.

The information in this manual has been carefully checked and is believed to be accurate at the time of publication. D-Link Inc. assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. D-Link reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time without prior notice and is not obligated to update this documentation to reflect such changes.

D-Link makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does D-Link assume any liability arising out of the application or the use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

The products of D-Link are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use an D-Link product for any such unintended or unauthorized application, the Buyer shall indemnify and hold D-Link and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that D-Link was negligent regarding the design or manufacture of said product.

WARNING

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the administrator will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressly approved by the party responsible for compliance could void the administrator's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

The DPN-6608 device and components are sensitive to static:

	<p>ESD Alert Follow strict ESD (electrostatic discharge) precautions when handling or working on the DPN-6608 or related equipment.</p>
---	--

Revision History

Date	Page	Revision history	Editor	Revision
2014/3		The Usage of CLI Commands Static MAC Spoofing Table Connectivity Fault Management	Kirk	1.31.00

Table of Contents

Chapter 1 Device Introduction	8
1.1 Key Features	8
1.2 Specification	9
1.2.1 Hardware Specification	9
1.2.2 Software Specification	10
1.3 Front View of DPN-6608	11
1.3.1 LED Indicators.....	12
1.3.2 Console	14
1.3.3 GPON OLT Ports.....	15
1.3.4 NNI (Uplink) Interface.....	16
1.3.5 SFP(Small Form Factor Pluggable) Installation.....	17
1.4 Rear View of DPN-6608	19
1.5 Application.....	22
1.6 Login DPN-6608	23
1.6.1 Web Server Login	23
1.6.2 Command Line Interface (CLI) Login.....	24
1.6.3 First Screen - Version Information	27
Chapter 2. GPON Configuration.....	28
2.1 OLT Configuration	28
2.1.1 Edit OLT in GUI.....	28
2.1.2 Edit OLT in CLI	30
2.2 OLT Information	31
2.2.1 OLT Resource Report.....	31
2.2.2 OLT SFP Information	32
2.2.3 OLT Alarm List.....	34
2.3 Service VLAN	35
2.3.1 Edit Service VLAN in GUI	35
2.3.2 Edit Service VLAN in CLI.....	37
2.4 Bandwidth Profile.....	38
2.4.1 Edit Bandwidth Profile in GUI	39
2.4.2 Edit Bandwidth Profile in CLI	40
2.5 ONT Image Profile	41
2.5.1 Edit ONT Image in GUI	41
2.5.2 Automatic ONT Upgrade	41
2.5.3 Edit ONT Image in CLI.....	42
2.6 ONT Config Profile.....	43
2.6.1 Edit ONT Config Profile in GUI	43
2.6.2 Edit ONT Config Profile in CLI.....	44
2.7 SIP Server Profile	45
2.7.1 Edit SIP Server Profile in GUI	45
2.7.2 Edit SIP Server Profile in CLI.....	46
2.8 Server List for Proxy Agent	47
2.8.1 Edit Server List in GUI.....	47
2.8.2 Edit Server List in CLI	48
2.9 Service Profiles.....	49
2.9.1 Data Service Profile	49
2.9.2 IPTV Service Profile.....	50
2.9.3 VoIP Service Profile.....	50
2.9.4 Ethernet UNI Service Profile.....	51

2.9.5 CATV Service Profile.....	51
2.9.6 Misc Service Profile	52
2.10 Auto-Provision Profile	54
2.10.1 Edit Auto-Provision Profile in GUI	54
2.10.2 Edit Auto-Provision Profile in CLI	55
2.11 ONT Registration.....	56
2.11.1 ONT Registration in GUI.....	56
2.11.2 ONT Discovery in GUI.....	57
2.11.3 ONT Registration in CLI	58
2.11.4 ONT Alarm List	59
2.11.5 ONT State.....	61
2.11.6 Managed ONT.....	62
2.11.7 Manual Operation on ONT	64
2.12 ONT Service Binding.....	65
2.12.1 Specify ONT Service in GUI	65
2.12.2 Specify ONT Service in CLI.....	65
2.13 ONT Service Batch	66
2.13.1 ONT Service batch in GUI	66
2.13.2 ONT Service batch in CLI	67
2.14 ONT POTS Data	68
2.14.1 Edit ONT POTS in GUI.....	68
2.14.2 Edit ONT POTS in GUI.....	69
2.15 ONT Authentication Data.....	70
2.15.1 Edit ONT Authentication in GUI	70
2.15.2 Edit ONT Authentication in CLI.....	71
2.16 GPON Redundancy	72
2.16.1 OLT Duplex Feed.....	72
2.16.2 Full Duplex Redundancy.....	73
2.16.3 Full Duplex Redundancy with dual chassis OLT	73
2.16.4 Manual Redundancy in GUI	74
2.16.5 Manual Redundancy in CLI	74
Chapter 3 Ethernet Configuration	75
3.1 NNI Configuration	75
3.1.1 Specify NNI Configuration in GUI	75
3.1.2 Specify NNI (Uplink) Configuration in CLI.....	76
3.1.3 NNI SFP information	77
3.2 Global Configuration.....	79
3.2.1 ONT Isolation Case	81
3.2.2 Knowledge of IGMP.....	82
3.2.3 View IGMP Snooping in GUI	84
3.2.4 View IGMP Snooping in CLI.....	85
3.3 Link Aggregation	86
3.3.1 Static LACP Aggregation	87
3.3.2 Dynamic LACP Aggregation Group	88
3.3.3 Hash Code Contributors in GUI.....	89
3.3.4 Port Trunking in GUI.....	90
3.3.5 LACP Configuration in GUI	91
3.3.6 LACP Status in GUI	92
3.3.7 Link Aggregation in CLI	94
3.4 Port Based VLAN.....	96
3.4.1 Specify Port Based VLAN in GUI.....	96
3.4.2 Specify Port Based VLAN in CLI	96

3.5 Rate Strom Control	97
3.5.1 Specify Rate Strom Control in GUI	97
3.5.2 Specify Rate Strom Control in CLI	97
3.6 Quality of Service (QoS)	98
3.6.1 Specify QoS in GUI	99
3.6.2 Specify QoS in CLI	99
3.7 Access Control List (ACL)	100
3.7.1 ACL Overview	100
3.7.2 ACL Configuration in GUI	100
3.7.3 ACL configuration in CLI	101
3.8 Relay Agent Information	102
3.8.1 Knowledge of DHCP Option 82	102
3.8.2 Specify Relay Agent Information in GUI	104
3.8.3 Specify Relay Agent Information in CLI	104
3.9 ARP Proxy Table	105
3.9.1 Dynamic ARP Proxy in GUI	105
3.9.2 Dynamic ARP Proxy in CLI	105
3.9.3 Static ARP Proxy in GUI	106
3.9.4 Static ARP Proxy in CLI	106
3.10 Static MAC Spoofing Table	107
3.10.1 Specify Static MAC Spoofing Address in GUI	107
3.10.2 Specify Static MAC Spoofing Address in CLI	107
3.11 Spanning Tree Protocol (STP)	108
3.11.1 Rapid Spanning Tree Protocol	109
3.11.2 STP Configuration in GUI	111
3.11.3 MSTP Configuration in GUI	112
3.11.4 STP Status in GUI	113
3.11.5 STP configuration and Status in CLI	114
3.12 Connectivity Fault Management (CFM)	115
3.12.1 Specify Connectivity Fault Management in GUI	115
3.12.2 Specify MEP/MIP/RMEP in CLI	116
3.12.3 Specify Loopback test in CLI	117
3.12.4 Specify Linktrace test CLI	118
3.13 Port Mirroring	119
Chapter 4 Status Monitoring	120
4.1 Alarm/Event	120
4.1.1 View Alarm/Event in GUI	120
4.1.2 Alarm/Event in CLI	120
4.2 Performance Data	122
4.2.1 Ethernet RMON in GUI	122
4.2.2 Ethernet RMON in CLI	123
4.2.3 GPON OLT Counters in GUI	125
4.2.4 GPON OLT Counters in CLI	126
4.2.5 ONT Counters in GUI	127
4.2.6 ONT Counters in CLI	129
4.3 MAC Table	130
4.3.1 MAC Table of Layer-2 Switch in GUI	130
4.3.2 MAC Table of GPON OLT in GUI	130
4.3.3 MAC Table in CLI	131
Chapter 5 System Configuration	132
5.1 Network Setting	132
5.1.1 Network Setting in GUI	132

5.1.2 Network Setting in CLI	132
5.2 SNMP Settings.....	133
5.2.1 SNMP Overview	133
5.2.2 SNMP v1/v2c Configuration in GUI	134
5.2.3 SNMP v3 Configuration in GUI	135
5.2.4 SNMP Configuration in CLI	136
5.3 Device Clock	137
5.3.1 Set Device Clock in GUI.....	137
5.3.2 Set Device Clock in CLI	137
5.4 Alarm Cut Off.....	138
5.5 Device Description	139
5.5.1 Device Description in GUI	139
5.5.2 Device Description in CLI.....	139
5.6 Reboot	140
5.6.1 Reboot in GUI	140
5.6.2 Reboot in CLI	140
5.7 Upgrade Device	141
5.7.1 Upgrade through Local Disk in GUI	141
5.7.2 Upgrade in GUI	141
5.7.3 Upgrade in CLI	142
5.8 Backup/Restore the Configuration.....	143
5.8.1 Backup Configuration in GUI	143
5.8.2 Restore Configuration in GUI.....	143
5.8.3 Backup/Restore Configuration in CLI	144
5.9 Account Management.....	145
5.9.1 Create new Account in GUI	145
5.9.2 Create new Account in CLI	145
5.9.3 Change Password in GUI.....	146
5.9.4 Change Password in CLI	146
5.10 License Control.....	147
5.10.1 License Control through Local Disk in GUI	147
5.10.2 License Control in GUI	147
5.10.3 License Control in CLI.....	148
5.11 Log File.....	149
Chapter 6 Application Examples.....	150
6.1 Provision Data Service.....	151
6.1.1 Provision Data Service in GUI.....	151
6.1.2 Provision Data Service in CLI	154
6.2 Cascaded OLTs	157
APPENDIX A.Abbreviations	158
APPENDIX B.Maximum Numbers of Resources	160
APPENDIX C.Supported Transceivers.....	161
APPENDIX D.CLI Command Help.....	162
APPENDIX E.GPON Encapsulation Method (GEM).....	180

Chapter 1 Device Introduction

1.1 Key Features

- 8x GPON OLT
 - Compliant with ITU-T G.984.1, 984.2, 984.3, 984.4
 - 512 / 1024 subscribers
- Various NNI (Network-to-Network Interfaces)
 - 2 x 10GbE (SFP+)
 - 4 x 1GbE (SFP)
 - 2 x 10/100/1000 BASE-T (Optional)
- Robust Traffic Management
 - Per-flow QoS / Bandwidth control
 - IGMP Snooping and proxy for multicasting network
 - Up to 10K jumbo frame supported
 - 8 strict and weighted scheduling queues
 - IEEE 802.3ad link aggregation
 - High capacity packet switching with 32K MAC address table.
 - 4K VLAN and Q-in-Q
 - Ingress policing per service
- Excellent Operation and Management
 - CLI command
 - In-band / Out-of-band Ethernet web-based HTTP
 - In-band / Out-of-band Ethernet telnet
 - SNMP for NMS
- Easy Expansion and Maintenance
 - SFP type fiber module for both GPON OLT and NNI offers the flexibility of subscriber expansion and maintenance.
 - Hot-swappable AC / DC power modules with load-sharing and redundancy
- Miscellaneous
 - 3 alarm outputs (optional)
 - 1 external clock input (optional)
 - 2 external clock outputs (optional)
 - ACO and Reset buttons
 - LED indicators for each link / alarm / power

1.2 Specification

1.2.1 Hardware Specification

Hardware Capacity	
Switching Capacity	64G(simplesx)/128G(duplex) Ethernet Switching
GPON	
Standard	ITU-T G.984.1.2.3.4
Capacity	8 OLT Ports X 2.5Gbps
Split Rate	Up to 1:128
Downstream	2.5Gbps, 1490nm, Class B+
Upstream	1.25Gbps, 1310nm, Class B+
NNI	
Capacity	2 x 10GbE (SFP+) 4 x 1GbE (SFP) 2 x 10/100/1000 BASE-T
Mechanism	
Dimension	440(W) x 44.45(H) x 270(D) mm
Weight	3.1Kg
Operation Environment	
Input Power	DC -36V ~ -72V, Normal -48V DC or 90~264VAC @47~63Hz
Power consumption	Max. 45W
FAN	2 x 12V Fans - left and right side, 40x40x10mm, Noise 30dBA
Operation Temp.	-10 ~ 60 °C
Humidity	From 10% up to 85%
EMI	FCC part 15 sub B/ CISPR 22 class A EN 55022 : 2010 / EN 55024 : 2010 EN 61000-3-2 / EN 61000-3-3 IEC 61000-4 SERIES ANSI C63.4 Canadian ICES-003 ETSI EN 300 386 V1.5.1 (2010-10)
Operation and Management	
Alarm	Critical, Major, Minor relay contacts (optional)
Management Interface	1 x Ethernet Port (NMS) 1 x Console RS232 (RJ45 type)
Upgrade	Remote s/w upgrade via TFTP/FTP/HTTP
LED	PWR1/2, CRT, MJR, MNR, RDI, MNT, ACO GPON 1~8, NNI 1~8

1.2.2 Software Specification

GPON	<p>OLT enable/disable ONT Auto/Manual Registration ONT Activation/Deactivation ONT Auto Discovery Auto-Learn ONT password Standard OMCI OMCI encryption FEC (Forward Error Correction) AES security Service Provisioning Link and Alarm Management Performance Monitoring Digital Diagnosis Monitoring of OLT/ONT GPON QoS Type B Protection</p>
Layer 2	<p>IEEE 802.1p QoS IEEE 802.3ad/Link Aggregation IEEE 802.1d STP IEEE 802.1q VLAN Jumbo Frame IGMP Snooping(v2,v3)/proxy(v2) PPPoE Intermediate Agent</p>
DHCP	DHCP Relay, DHCP Option 82
QoS	<p>8 priorities queues per port 802.1p Traffic Control Priority based on 802.1p, ToS, DSCP SPQ, WRR, DRR Scheduling</p>
Flow Control	802.3x
Security	<p>128 Bit- AES encryption MAC limit per port Packet limit by type of traffic (Broadcast/Multicast/DLF) Packet block by traffic type (Broadcast/Multicast/ DLF) MAC Flood Guard Port Flood Guard Packet filtering (L1 –L4) RADIUS Proxy / IEEE 802.1x MAC Spoofing Detection ACL</p>
Management	CLI, HTTP, Telnet/SSH, SNMP(v1,v2c,v3)

1.3 Front View of DPN-6608

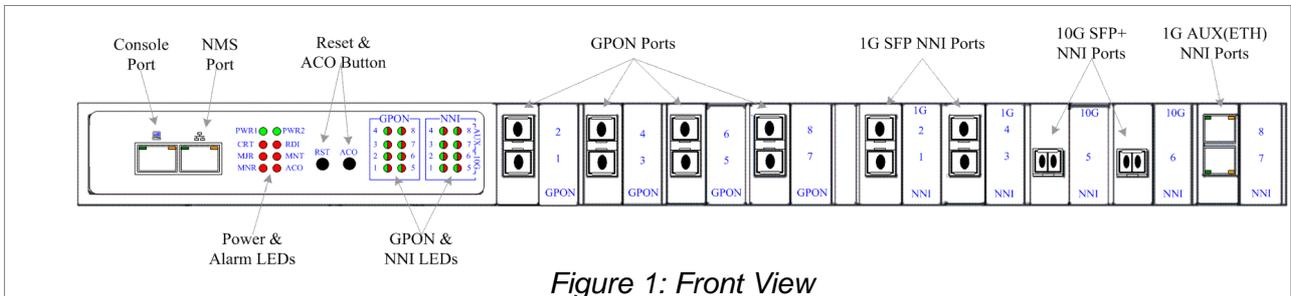


Figure 1: Front View

The above figure shows the front view of DPN-6608. The left RJ45 connector at the left side of device is RS232 console for CLI , and the right one is 10/100/1000 BASE-T Ethernet port for NMS via SNMP / web-based GUI and Telnet.

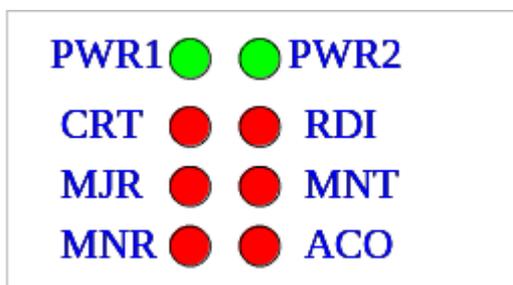
Reset button is for device hardware reset, and ACO is the 『Alarm cut-off』 button to cut off all audible / visible alarms.

The following section will describe LED indicators in detail.

DPN-6608 uses 45 degree bevel angle design for all GPON OLT ports and Ethernet ports under the consideration of optical safety.

1.3.1 LED Indicators

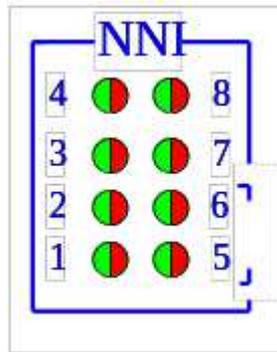
The following LED indicators show the definition of power cards and alarms.



LED	Description
PWR1 PWR2	Power indicator for power module slot 1/2 Off: not available Green: power module works normal Flash Green: detect error reported by power module
CRT	Critical alarm indicator Off : no critical alarm detected Red : critical alarm detected
MJR	Major alarm indicator Off : no major alarm detected Red : major alarm detected
MNR	Minor alarm indicator Off : no minor alarm detected Red : minor alarm detected
RDI	Remote defect/alarm indicator Off: no Error Bit detected Red: RDI(remote defect (alarm) indicator of ONT) or Error Bit Detected in upstream path
MNT	Maintenance status indicator Off: device is idle Flash: device upgrade is processing
ACO	ACO status indicator Off: the alarm cut off disabled or new Alarm detected Red: the alarm cut off is executed



GPON 1~8	Description
off	Port disabled.
red	Port enabled, but LOS is detected.
green	Port enabled, and no LOS detected.
flash green	Port is working (Data transferring.)



NNI 1~8	Indication
off	Port disabled.
red	Port enabled, but link is down.
green	Normal.
flash green	Port is working (Data transferring.)

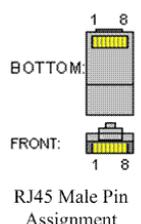
1.3.2 Console

The administrator can manage the device locally by connecting the operating terminal to the console port with the provided console cable (RJ45-to-DB9). The setting of console terminal is as shown below.

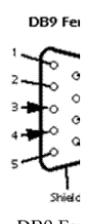
Items	Setting
Data Rate	115200 bps
Parity	None Parity
Data Bits	8 bits
Stop Bits	1 stop bit
Flow Control	No Flow Control

RJ-45 type connector of the console cable is connected to DPN-6608 and DB-9 type connector of the console cable is connected to console terminal (PC or Laptop). Pin assignment of the console port is shown as below table.

Signal Name/ Function	RJ-45 Pin	RJ-45	DB-9 Pin	Signal Name/ Function
TXD	6	Yellow	2	RXD
RXD	3	Black	3	TXD
DSR	2	Orange	4	DTR
GND	5	Green	5	GND
DTR	7	Brown	6	DSR
RTS	1	Blue	7	CTS
CTS	8	Slate/Grey	8	RTS
GND	4	Red	—	GND
—	—	White	—	—
—	—	Purple	—	—



RJ45 Male Pin
Assignment



DB9 Fe
Assignr

Figure 2: Pin Definition of RJ45-to-DB9 Connector

1.3.3 GPON OLT Ports

GPON technology provides one of the most cost effective ways for service providers to deploy fiber based services to the residential subscribers, businesses or other types of node.

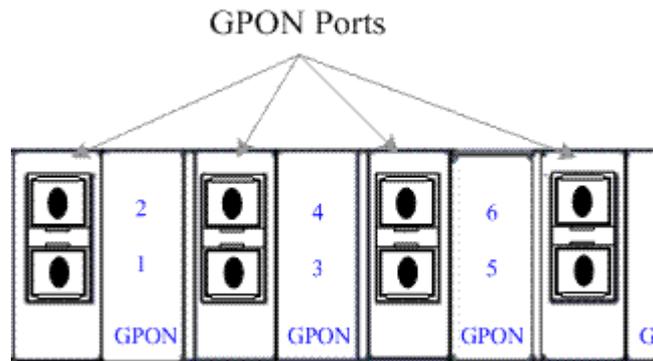


Figure 3: GPON Ports

Each GPON OLT port supports 2.488Gbps downstream bandwidth and up to 1.244Gbps upstream bandwidth as mentioned in the G.984.1-4 specifications.

GPON OLT ports are designed in SFP type for plugging in hot-swappable GPON OLT transceiver modules. Sometimes, optical attenuator may be needed to make sure the receiver power levels in both OLT and ONT sides are within -8dBm ~ -28dBm range. The following OLT physical features are supported:

- ✓ Class B+ Optics with -28dB link budget
- ✓ 64 (up to 128) subscribers per OLT interface
- ✓ RSSI support

The OLT transceiver module used in the GPON ports is the ODEM-PB1S-OLT . For details, please refer to DEM-PB1S-OLT datasheet.

1.3.4 NNI (Uplink) Interface

Three types (1GbE SFP, 10GbE SFP+, 10/100/1000 BASE-T Ethernet) of NNI Interfaces are provided in DPN-6608.

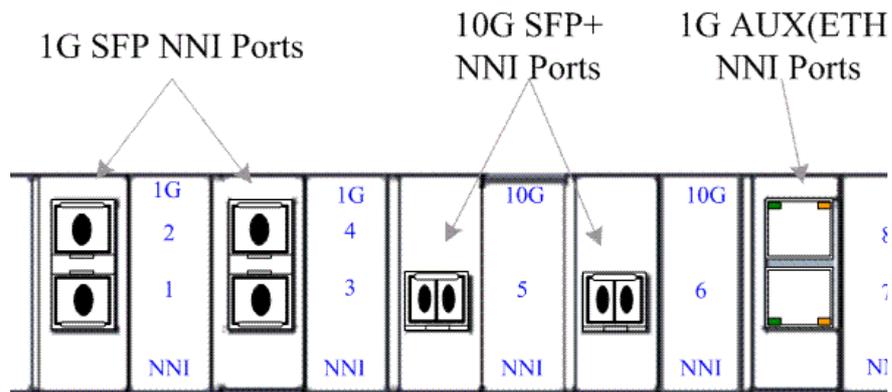


Figure 4: NNI Ports

Port 1~4 are 1GbE SFP slots.

Port 5~6 are 10GbE SFP+.

Optional Port 7~8 are 10/100/1000 BASE-T.

When more than one NNI port are used, the system offers a redundant connection to the network that can also be used for load-sharing traffic, and thereby provide abundant bandwidth for today's demanding triple play applications.

The transceiver module used in the 10GbE SFP+ slot is listed below.

- DEM-431XT-DD
- DEM-432XT-DD
- DEM-433XT-DD
- DEM-435XT-DD
- DEM-431XT
- DEM-432XT
- DEM-433XT
- DEM-435XT
- DEM-436XT-BX

. For details, please refer to datasheet accordingly.

1.3.5 SFP(Small Form Factor Pluggable) Installation

OLT/NNI fiber connections use SFP or SFP+ connectors. These connectors may be used with 10 Gigabit Ethernet, Gigabit Ethernet and GPON.

Inserting an SFP module and a fiber connection:

1. Push the handle of SFP module inward.
2. Slide SFP module into the slot. You should hear or feel a slight 'click' sound. Without it, SFP module is not installed properly.
3. Insert the fiber connector into the SFP module.

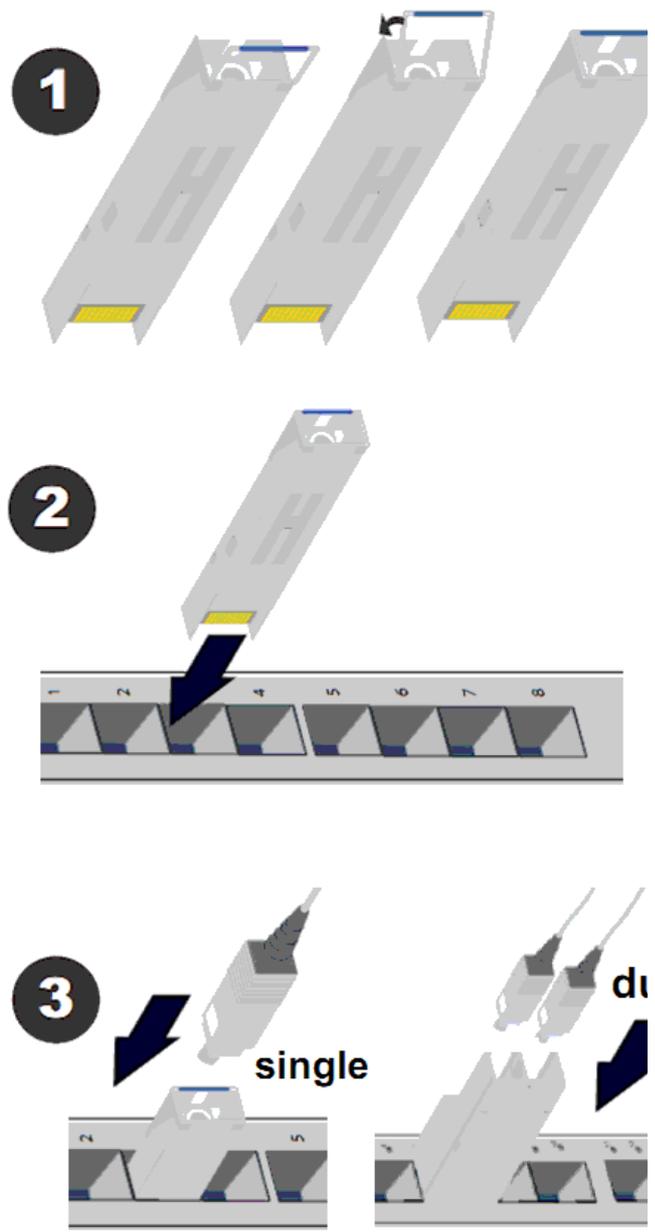


Figure 5: Instruction of SFP plug-in

Removing a fiber connection and an SFP:

Removing an SFP connector is just like doing the installation in reverse.

1. Remove the fiber connector from the SFP module.
2. Pull the handle o SFP module outward.
3. Pull out the SFP module from the slot.

1.4 Rear View of DPN-6608

The following figure shows the rear view of DPN-6608.

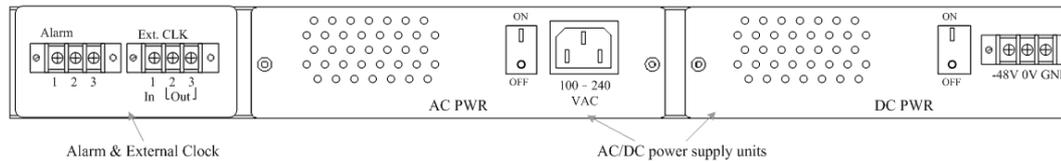


Figure 6: Rear View

Alarm output & external clock interfaces are provided by optional pluggable modules.

DPN-6608 power module can be supplied by 110/220 AC or -48V DC power. The device works stably with either power supply provided individually. (Please make sure the current of your power supply system is stable.) When both of AC and DC modules are applied, they share the power load of device. When one of DC/AC module is down or the voltage or current is not stable, the device will switch the load to another DC/AC module totally. This switching will interrupt services and the traffic won't be influenced.

Either AC or DC modules can be powered off manually by the switch button on the module panel. After power is applied properly, DPN-6608 starts the POST (Power-On Self Test) and then initializes the device with the data in the non-volatile backup memory.

After the completion of lightning surge immunity test for AC power, a temporary degradation of transmission performance or temporary loss of function might be acceptable, but the equipment and the protection device must be self-recoverable. To fulfil surge protection in an easy-installation manner, the DPN-6608 incorporates with chassis grounding mechanism on the surface of the device.



Figure 7: AC Power Module



Figure 8: DC Power Module

Power Supply Specification:

- ✓ Dimension: 156(L) x 100(W) x 44.5(H) mm
- ✓ Connector type:
 - ◆ AC module: Standard 3 holes AC Socket
 - ◆ DC module: Terminal Block with Screws
 - ◆ Internal DC +12V Output with Golden Finger Connector
- ✓ Input Voltage:
 - ◆ AC module: 90~264VAC, 47~63Hz
 - ◆ DC module: -36 ~ -72V, Normal =48Vdc
- ✓ Output Voltage: DC +12.0V
- ✓ Output Current(Max): 6.6A(80W)
- ✓ Load reg.: 5%
- ✓ Line reg.: 1%
- ✓ Ripple: 1%
- ✓ Noise: 2%
- ✓ Efficiency: 82% @F.L
- ✓ Operation Temperature: -15 ~ +65 Degree
- ✓ Storage Temperature: -25 ~ +85 Degree
- ✓ Operation Humidity: 5% - 90%
- ✓ Cooling: Fan cooling
- ✓ Load Sharing
- ✓ Redundant mechanisms
- ✓ Hot-swappable
- ✓ Short protection
- ✓ Overload protection
- ✓ Over Voltage protection

Frame Ground:

The “GND” is connected to the Frame Ground when power is applied for case protection. It is located on DC power module marked “GND” with screw type connection. If AC power is applied, it resides in the AC jack ground pin.



Figure 9: Side View

Ventilation holes are located at the left/right/rear side panel of DPN-6608 for proper heat dissipation, and two fans are located at the left/right sides inside the case.

1.5 Application

DPN-6608 GPON OLT (Optical Line Terminal) device provides GPON interfaces for connecting to ONTs via splitters (normal splitter ratio is 1:64) and NNI interfaces for connecting to service networks like SIP servers, Internet cloud and IPTV streaming servers to offer triple play services as shown in the diagram below to achieve FTTH application.

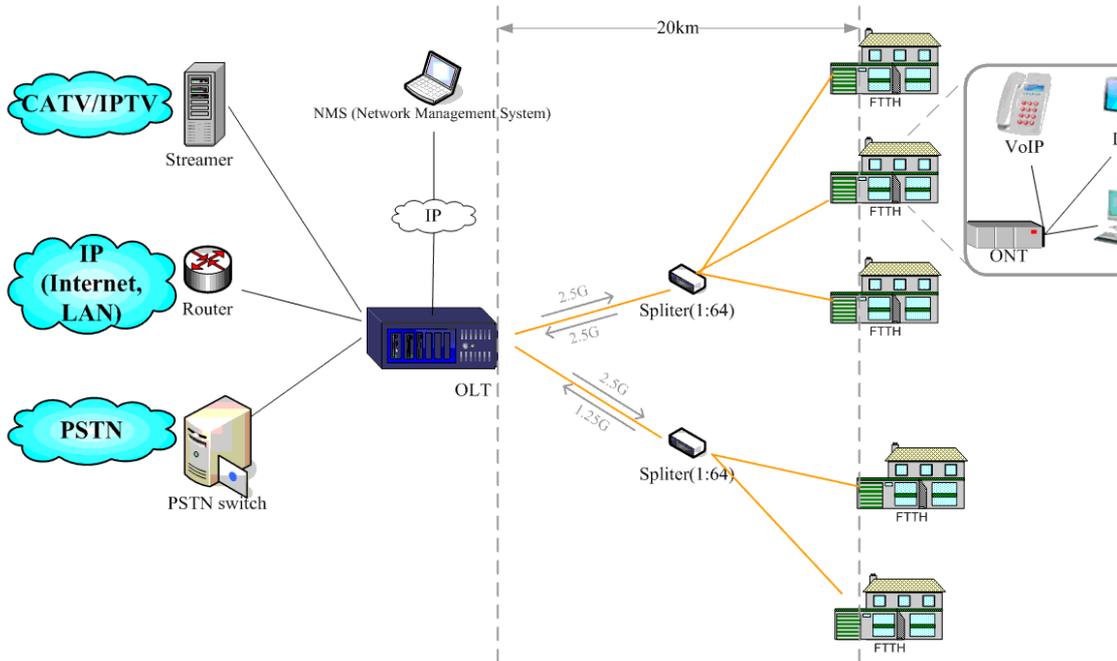


Figure 10: GPON Application

1.6 Login DPN-6608

1.6.1 Web Server Login

Web Server is a simple and embedded Network Management System for maintenance. There is no functionality difference from Console CLI. The administrator can access the performance, alarm and configuration of OLT/ONT easily with web browser, like IE or Firefox.



The default administrator account user name is **admin**, and the default password is **admin**. The default device IP address is **192.168.1.150**

Note: Remember to Save configuration (CLI command 'save' or click button 'Save Config into Flash' in GUI) after changes are confirmed. Otherwise, those changes will be discarded after device reboot.

1.6.2 Command Line Interface (CLI) Login

Set Up Console Connection:

1. Configure the baud rate and character format of the PC serial port (please refer to Section 1.3.2).
2. Connect the provided RJ45-to-DB9 cable to the RJ45 jack of DPN-6608 console port.
3. Connect the provided RJ45-to-DB9 cable to the RJ45 jack of DPN-6608 console port.
4. Connect the DB9 of the provided RJ45-to-DB9 cable to a RS232 serial port of PC.
5. Run a terminal emulation program in your PC.
6. Power on DPN-6608.
7. Click the “Enter” to start login when DPN-6608 booting is done. Then you will get the message shown as below.

```
- init -  
  
Please press Enter to activate this console.  
GPON-OLT login: admin  
Password:  
  
Enter 'help' for a list of built-in commands.  
  
admin@192.168.1.150:>
```

Default Login Account is “**admin**”, and default password is “**admin**”

Basic Command Operations:

Requirement	Command
Recall last command	up arrow or <Ctrl-P>
Recall next command	down arrow or <Ctrl-N>
Complete Command	TAB
Delete entire line.	Ctrl-U

Help for CLI Commands:

Issue the command “**help**”, and you can get a list of supported commands.

```
admin@192.168.1.150:> help

Command      Description
-----
account      - Account Management
acl          - Access Control List
aco          - Alarm Cut Off
aggregation  - Aggregation Mode/Group
arp-dynamic  - Dynamic ARP Proxy Table
arp-static   - Static ARP Proxy Table
auto-profile - Auto Provision Profile
bw_dba      - Bandwidth Profile
configuration - Configuration Backup/Restore
debug        - Internal Debug Tool
dbg          - alias of Debug
device       - Device Description
diagnosis    - Diagnosis Function
event        - Alarm and Event
global       - Global Configuration
help         - This Help
?           - alias of help
host         - Host Network Setting
igmp         - IGMP Protocol Status
information  - Display Device Information
license      - License Information
logfile      - Log File Control
logout       - Logout
mac-table    - Display MAC Table
nni          - UP-Link Interface
ntp          - Network Tool - ntp
olt          - OLT Configuration
ont          - ONT Configuration
ont-auth     - ONT Authentication Profile
ont-batch    - ONT Service Batch Script
ont-cfg      - ONT Configuration Profile
ont-image    - ONT Image Profile
ont-pots     - ONT POTS Configuration
ont-svc      - ONT Service Configuration
passwd       - Change Login Password
pbvlan       - Port-Based VLAN
performance  - Display Performance Data
ping         - Network Tool - ping
```

ps	- Show Processes
qos	- Quality of Service
rate-control	- Rate Storm Control
reboot	- Reboot Device
relay-agent	- Relay Agent Information
save	- Save Config into Flash
server-list	- Server List for Agent
shell	- Exit to Shell
show	- Display Configuration
sip-server	- SIP Server Profile
snmp	- SNMP Configuration
spoofing-mac	- Static MAC Spoofing Table
stp	- Spanning Tree Protocol
svc-catv	- CATV Service Profile
svc-data	- Data Service Profile
svc-eth	- Ethernet Service Profile
svc-misc	- Misc Service Profile
svc-iptv	- IPTV Service Profile
svc-voip	- VOIP Service Profile
time	- Device Date and Time
traceroute	- Network Tool - traceroute
upgrade	- Device Upgrade
version	- alias of Information
vlan	- Service VLAN

help <command> to display command help

If you want to know the usage of a particular command like "**host**", type "**help host**" or "**? host**" to get description of command "**host**"

Usage:

```
show host
host [dhcp <on|off>] [vlan <VID>] [ip <ADDR>] [mask <ADDR>]
    [gate <ADDR>] [dns-1 <ADDR>] [dns-2 <ADDR>]
```

Note: It's not advised to use Management VLAN ID for service traffic at ONTs. If that's the case, two current limitations are encountered in the Management VLAN:
 Clients at ONT are able to access and manage OLT,
 and PPPoE and DHCP relay functions don't work.
 Other service traffic VLANs would work normal.

1.6.3 First Screen - Version Information

After login succeed, the first page will show you the device information like model name / software version / hardware rev. / MAC address....etc. as below.

Model Name	GPON-OLT
OS Version	Linux 2.6.32.27 (2014-03-05)
Serial Number	
Current SW Version	1.31.00 rc-1 03/06/2014 14:08
Backup SW Version	none
GPON Driver	PJ 2.6.05.00
OMCI Version	OCS R3.1 V0.3
HW Version	0.b
EPLD Version	0.7
Device MAC	
Device Uptime	1:25:04
Database in Flash	2014-03-04 13:20:39
Core Temperature	48 °C

The administrator also can get OLT information by CLI command "**information**".

```
admin@192.168.1.150:> information

Version information:
Model name..... OLT
OS Version..... Linux 2.6.32.27 (2014-03-05)
Serial Number.....
Current SW..... 1.31.00 rc-1 03/06/2014 14:08
Backup SW..... none
GPON driver..... PJ 2.6.05.00
OMCI version..... OCS R3.1 V0.3
HW version..... 0.d
EPLD version..... 0.7
MAC address..... xx:xx:xx:xx:xx:xx
IP address..... 192.168.1.159
Device uptime..... 1:17:40
Database in Flash... 2014-03-04 13:20:39
Core Temperature.... 47 C
```

Chapter 2. GPON Configuration

2.1 OLT Configuration

In order to activate GPON OLT ports correctly, the administrator should plug in GPON OLT SFP modules and change the state of the specified OLT ports from default value “OOS” (Out-of-Service) to “IS” (In Service).

2.1.1 Edit OLT in GUI

Before enabling a OLT, please verify all parameters match real scenario and ONTs on field. Transceiver Type / Pwd-Auth / DS FEC / AES Key Exchange can't be changed if OLT is in “IS” state.

GUI Path: **>GPON>OLT>PonLink**

OLT	Transceiver	AES Key Exchange	DS FEC	Protection	Description	ONTs	DG	Busy	Current State	In Service	
	Pwd-Auth	SN Scan Period									
1	(21)DELTA Auto-Provision	- scan per 10 sec	-	OLF-2	PonLink-1	0/2/0	0	2	IS	Yes (working)	
2		Same as OLT-1		OLF-1	PonLink-2				IS	(standby)	
3	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-3	0/0/0	0	0	OOS-MA	no	
4	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-4	0/0/0	0	0	OOS-MA	no	
5	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-5	0/0/0	0	0	OOS-MA	no	
6	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-6	0/0/0	0	0	OOS-MA	no	
7	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-7	0/0/0	0	0	OOS-MA	no	
8	(21)DELTA No-Pwd	- scan per 10 sec	-	-	PonLink-8	0/0/0	0	0	OOS-MA	no	

Note: GPON protection port can not have any ONT registered.
Info: There are 1 activated ONT.

Transceiver

The administrator has to select correct transceiver type to match GPON OLT SFP transceiver, the default transceiver type is “(21) Delta”. Refer to APPENDIX C for the supported transceiver type.

Pwd-Auth

This option define how discovered ONTs are to be registered and to be activated by OLT:

No-Pwd: OLT activates the registered ONTs with option 'In-Service' enabled

Pwd-Verify: OLT activates the registered ONTs with option 'In-Service' enabled and ONT password matched.

Auto-Provision: OLT activates all discovered ONTs. If discovered ONT's password is found in Auto-Provision Profile, ONT configuration will be replaced with the one defined in Section 2.10 and the ONT will be re-activated with new configuration.

AES Key Exchange

To enable AES encryption, “AES Key Exchange mode” option should be checked and “Key Exchange Interval” determines how often the exchange operation is activated.

SN Scan Period

In order to discover ONT automatically, this option should be checked and “Scan Period” determines how often the scan operation is activated. Lower bound of scan period is 10 seconds.

DS FEC

Enable/disable Downstream Forward Error Correction. If ONT doesn't support FEC but this option is checked, the communication channel to ONT will not be able to be established.

Protection

Select the redundancy partner when the redundant function is needed.

ONTs

Display how many ONTs are registered in GPON OLT port.

DG

Display how many ONTs down due to Dying-Gasp Event.

Busy

Display how many ONTs are busy on activation or deactivation.

The administrator can also specify the name for each GPON OLT ports. For example, the administrator can specify it as the name of building, company, community, etc.

The check box of “In service” is to switch this OLT port to in-service (IS) or out of service (OOS).

Once all settings are done, please click symbol “S” to save the configuration and start initialization process. A few seconds(around 2) later, the specified OLT Port will be switched to “IS” (In Service).

2.1.2 Edit OLT in CLI

```
Usage:
show olt <all|oltid>
olt config <oltid> [is|oos] [xcvr <XCVR>]
                    [pwd-auth <none|verify|auto>]
                    [aes-mode <off|normal|enhanced>]
                    [aes-period <VALUE>]
                    [ds-fec <on|off>]
                    [partner <none|oltid>]
                    [sn-scan <on|off>] [sn-period <VALUE>]
                    [descr <"TEXT">]

olt resource
olt sfp <oltid>
olt sfp <oltid> <temp|volt|bias|txp|rxp>
                    <alarm|warning> <high|low>
                    <SEVERITY>

XCVR: (6)SOURCE (21)DELTA
SEVERITY: (0)None (1)Event (2)Minor (3)Major (4)Critical
```

Activate GPON OLT 1

```
admin@192.168.1.150:> olt edit 1 is
```

```
Info: update successfully.
```

Inquire the configuration and status of GPON OLT ports

```
admin@192.168.1.150:> show olt all

olt-1, descr="Gpon-1", is, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=olt-2, status=IS, working, ont=2/2/0
olt-2, descr="Gpon-2", partner=olt-1, status=IS, alarm=Los(128), standby
olt-3, descr="Gpon-3", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
olt-4, descr="Gpon-4", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
olt-5, descr="Gpon-5", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
olt-6, descr="Gpon-6", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
olt-7, descr="Gpon-7", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
olt-8, descr="Gpon-8", oos, ds-fec=off, pwd-auth=none, sn-scan=on,
    sn-period=10 sec, aes-mode=off, aes-period=3600 sec, xcvr=DELTA(21),
    partner=none, status=OOS-MA
```

2.2 OLT Information

2.2.1 OLT Resource Report

The administrator can check how many resources and bandwidth are being used in each OLT port.

GUI Path: >GPON>OLT>Resource

Path: > GPON > OLT > Resource

OLT Resource Report

OLT	Used Dynamic Alloc ID	Used Static Alloc ID	Total Bandwidth (kbps)	CBR Bandwidth (kbps)
1	12 / 384	0 / 384	1,125,712	450,912
2	0 / 384	0 / 384	0	0
3	0 / 384	0 / 384	0	0
4	0 / 384	0 / 384	0	0
5	0 / 384	0 / 384	0	0
6	0 / 384	0 / 384	0	0
7	0 / 384	0 / 384	0	0
8	0 / 384	0 / 384	0	0

Used Dynamic Alloc ID

Display how many services with Max bandwidth profile are being used.

Used Static Alloc ID

Display how many services with Fix bandwidth profile are being used.

Total Bandwidth (kbps)

Display the totally bandwidth can be used including CBR bandwidth.

CBR Bandwidth (kbps)

Display the Constant Bit Rate (CBR). If CBR bandwidth runs out, individual port setting needs to be checked and readjusted.

The CLI command as below:

```
admin@192.168.1.150:> olt resource
```

OLT Resource Report:

olt-1, dynamic=0/384, static=0/384, total=1126768 kbps, cbr=450912 kbps

olt-2, dynamic=0/384, static=0/384, total=1126768 kbps, cbr=450912 kbps

olt-3, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

olt-4, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

olt-5, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

olt-6, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

olt-7, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

olt-8, dynamic=0/384, static=0/384, total=0 kbps, cbr=0 kbps

2.2.2 OLT SFP Information

The administrator can check the detail SFP module information including the vendor name / part number / SN / Date code. If Digital Diagnostic Monitoring is available in SFP module, the administrator can also specify the Threshold Crossing indicators for Low/High threshold of parameters.

GUI Path: **>GPON>OLT>SFP Information**

Module Information		Digital Diagnostic Monitoring (DDM)									
Vendor Name	SOURCEPHOTONICS	Module Temperature	Alarm	-----▲▼	-48.0	38.8	High	95.0	-----▲▼	°C	
Part Number	SPS4348HHPCDESD		Warning	-----▲▼	-43.0		90.0	-----▲▼			
Revision	1		Module Voltage	Alarm	-----▲▼	2.80	3.13	High	3.80	-----▲▼	V
Serial Number	B7U2007261			Warning	-----▲▼	3.00		3.60	-----▲▼		
Date Code	2011/06/29	Laser Bias	Alarm	-----▲▼	2.00	17.43	High	110.20	-----▲▼	mA	
Parameter Information			Warning	-----▲▼	3.00		100.18	-----▲▼			
Transceiver	SFP	Laser Output	Alarm	-----▲▼	1.1214	0.0030 (-25.23 dbm)	High	3.5463	-----▲▼	mW	
Connector	SC		Warning	-----▲▼	1.2584		3.1607	-----▲▼			
Link Length	20 km	Laser Rx	Alarm	-----▲▼	0.0000	0.0000 (-inf dbm)	High	0.1310	-----▲▼	mW	
Laser Wavelength	1490 nm		Warning	-----▲▼	0.0000		0.1310	-----▲▼			
Encoding	NRZ										
Nominal Bit Rate	2500 Mbps										
Upper Rate Margin	0%										
Lower Rate Margin	0%										
Compatibility	00-00-00-00-00-00-00										
<input type="button" value="Apply"/> <input type="button" value="Undo"/>											

The CLI command is shown in the following:

```
admin@192.168.1.150:> olt sfp 1

Module Information:
Vendor Name..... D-Link
Part Number..... OPGP-43-B3B1RS
Revision..... A
Serial Number..... DE122000000250
Date Code..... 2012/05/29

Parameter Information:
Transceiver..... SFP
Connector..... SC
Link Length..... 20 km
Laser Wavelength..... 1490 nm
Encoding..... NRZ
Nominal Bit Rate..... 2500 Mbps
Upper Rate Margin..... 0%
Lower Rate Margin..... 0%
Compatibility..... 00-00-00-00-00-00-00-00

Digital Diagnostic Monitoring: (ALM-LO/WARN-LO/WARN-HI/ALM-HI)
Module Temperature..... 44.7 C (-20.0/ -10.0/ 85.0/ 95.0)
Module Voltage..... 3.34 V ( 3.00/ 3.13/ 3.46/ 3.60)
Laser Bias Current..... 9.29 mA ( 1.00/ 1.00/ 60.00/ 70.00)
Laser Output Power..... 2.1136 mW (1.2589/1.4125/3.1623/3.5481)
                        3.25 dBm
Laser Rx Power..... 0.0010 mW (6.5535/6.5535/6.5535/6.5535)
                        -30.00 dBm

Threshold Crossing Indicators:  ALM-LO  WARN-LO  WARN-HI  ALM-HI
Module Temperature.....         -         -         -         -
Module Voltage.....             -         -         -         -
Laser Bias Current.....         -         -         -         -
Laser Output Power.....         -         -         -         -
Laser Rx Power.....             -         -         -         -
```

2.2.3 OLT Alarm List

Alarm list when OLT command is processed successfully or unsuccessfully:

Current state type	Description
OltDatabase	Failed to load OLT database
OltXcvrPwr	Failed to power on OLT Transceiver module
OltXcvrType	Failed to configure OLT Transceiver type
OltDsFEC	Failed to configure Downstream FEC
OltAddOnt	Failed to add ONTs into OLT Link
OltLinkInit	Failed to initialize OLT Link
OltLinkMode	Failed to configure OLT Protection Mode
OltProtocol	Failed to configure OLT Protocol
OltRssiCfg	Failed to configure RSSI
OltGemMap	Failed to configure Gem Port mapping
OltMacMode	Failed to configure OLT MAC mode
OltMacFlush	Failed to flush OLT MAC table
OltAct	Failed to activate OLT Link
OltResource	Failed to initialize OLT Resource
OltOntEna	Failed to enable ONTs
OltOntAct	Failed to activate ONTs
OltMonitor	Failed to activate OLT Link Monitoring
OltKeyMode	Failed to set Key Exchange Mode
OltKeyExchange	Failed to start Key Exchange Process
OltSnAcq	Failed to start Serial-Number Acquisition
OltPswSucceed	Automatic Protection switching succeed
OltPswFailure	Failed to do Automatic Protection switching
OltPswPartial	Automatic Protection switching does not work properly
UsrPswSucceed	Manual Protection switching succeed
UsrPswFailure	Failed to do Manual Protection switching
UsrPswPartial	Manual Protection switching does not work properly

2.3 Service VLAN

The administrator should plan the service models based on VLANs.

2.3.1 Edit Service VLAN in GUI

GUI Path: **>GPON>S-VLAN**

S-VLAN	C-VLAN	U-VLAN	DHCP	PPPoE	ARP Proxy	NNI (UpLink)								GPON OLT								Description	Services						
VLAN Mode			Security	IGMP	Broadcast	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8								
10 / - Single VLAN		100	Relay	-	-	-	-	-	-	-	-	V	V	V	V	-	-	-	-	-	-	-	-	-	-	s 10, u100	0		
20 / - Single VLAN		200	Forward	-	ARP	-	-	-	-	-	-	V	V	V	V	-	-	-	-	-	-	-	-	-	-	s 20, u 200	0		
2011 / - Single VLAN		2011	-	-	ARP	-	-	-	-	-	-	V	V	V	V	-	-	-	-	-	-	-	-	-	-	s 2011, u 2011	0		

VLAN Mode

- 'Single VLAN'
- 'QinQ per U-VLAN'
- 'QinQ per Customer'
- 'TLS VLAN'

DHCP

None / Forward / DHCP relay / DHCP relay with option 82 supported. Refer to Section 2.8.

Note: if one of VLAN requires DHCP relay feature, all DHCP frames in all VLANs will be forwarded to CPU for process according to the desired action.

PPPoE

Checked to enable PPPoE Intermediate Agent.

Note: if one of VLAN has PPPoE enabled, all PPPoEd frames in all VLANs will be forwarded to CPU for process according to the desired action.

ARP Proxy

Checked to enable ARP Proxy.

Note: if one of VLAN has ARP-Proxy enabled, all ARP/DHCP frames in all VLANs will be forwarded to CPU for process according to the desired action.

Security

None / MAC Spoofing / IEEE 802.1x & RADIUS proxy.

Refer to Section 2.8.

Note: if one of VLAN require Security feature, all related frames in all VLANs will be forwarded to CPU for process according to the desired action.

IGMP

Checked to enable IGMP Snooping.

Note 1: To enable IGMP Proxy support in each S-VLAN, the administrator should enable IGMP mode in Section 3.2 first.

Note 2: if one of VLAN has IGMP enabled, all IGMP frames in all VLANs will be forwarded to CPU for process according to the desired action.

Broadcast

Checked to create VLAN with Broadcast support.

Note: this option is used for requiring broadcast traffic in 2.9.1 which option 'only broadcast' is checked.

NNI (Uplink)

Involved NNI ports.

GPON OLT

Involved GPON OLT ports.

2.3.2 Edit Service VLAN in CLI

Usage:

```
show vlan <all|uvid>
vlan create <uvid> <svid> <single|double <CVID>|custom|tls>
vlan remove <uvid>
vlan config <uvid> [single|double <CVID>|custom|tls]
                    [dhcp <none|relay|option82|forward>]
                    [pppoe-relay <on|off>]
                    [arp-proxy <on|off>]
                    [secure <none|spoofing|radius>]
                    [igmp <on|off>] [with-bc <on|off>]
                    [nni <none|LIST>] [olt <none|LIST>]
                    [descr <"TEXT">]
```

Create VLAN with single tagged

```
admin@192.168.1.150:> vlan create 10 20 single
```

Info: create successfully.

Specify NNI 7/8 and GPON OLT 1/2 as members of VLAN and enable ARP proxy

```
admin@192.168.1.150:> vlan config 10 arp-proxy on nni 7,8 olt 1,2
```

Info: update successfully.

View the configuration of VLAN 10

```
admin@192.168.1.150:> show vlan 10
```

```
uvid-10, svid-20, descr="s 20, u 10", single, dhcp=none, pppoe-relay=off,
igmp=off, secure=none, arp-proxy=on, with-bc=off, nni=7,8, olt=1,2
```

2.4 Bandwidth Profile

Bandwidth Profile is typically used when a service provider needs to provide customer services with limited bandwidth. In other words, a service provider may need to ensure that video traffic gets to the user at the expense of data or voice traffic.

In GPON there are two forms of DBA, status-reporting (SR) and non-status reporting (NSR).

About **NSR DBA**, the OLT continuously allocates a small amount of extra bandwidth to each ONU. If the ONU has no traffic to send, it transmits idle frames during its excess allocation. If the OLT observes that a given ONU is not sending idle frames, it increases the bandwidth allocation to that ONU. Once the ONU's burst has been transferred, the OLT observes a large number of idle frames from the given ONU, and reduces its allocation accordingly. NSR DBA has the advantage of imposing no requirements on the ONU, but the disadvantage of no way of OLT knowing how to best assign bandwidth across several ONUs that need more.

About **SR DBA**, the OLT polls ONTs for their backlogs. A given ONU may have several so-called transmission containers (T-CONTs), each with its own priority or traffic class. The ONU reports each T-CONT separately to the OLT. The report message contains a logarithmic measure of the backlog in the T-CONT queue. Through the knowledge of the [service level agreement](#) for each T-CONT across the entire PON, as well as the size of each T-CONT's backlog, the OLT can optimize allocation of the spare bandwidth on the PON.

DBA functionalities are categorized into 5 parts:

- Detection of congestion status by OLT and/or ONU
- Report of congestion status to OLT
- Update of assigned bandwidth by OLT
- Issues of grants by OLT according to updated bandwidth and T-CONT types
- Management issues for DBA operations

T-CONT Types – Upstream QoS

There are 5 types of The T-CONT upstream traffic descriptor as listed below:

	Type 1	Type 2	Type 3	Type 4	Type 5
Fixed	R_F				R_F
Assured		R_A	R_A		R_A
Maximum	$R_M=R_F$	$R_M=R_A$	$R_M>R_A$	R_M	$R_M>R_F+R_A$

2.4.1 Edit Bandwidth Profile in GUI

In order to provide different QoS for different level subscribers, the The administrator should define the Bandwidth Profile. The Bandwidth Profile is used by Data, IPTV and VoIP Service Profiles.

Note: Any profile change will not affect the activated services in ONTs. It only takes effect after those services are re-activated.

GUI Path: **>GPON>Configuration-Profiles>Bandwidth**

Index	Fix	Assure	Max	DBA	Method	Description	Services	
1	0 kbps	0 kbps	51,200 kbps	Type-4	NSR-DBA	default 50M	3	 
2	0 kbps	0 kbps	75,000 kbps	Type-4	NSR-DBA	dba 75M	1	 
3	0 kbps	0 kbps	60,000 kbps	Type-4	NSR-DBA	dba 60M	1	 
4	0 kbps	0 kbps	80,000 kbps	Type-4	NSR-DBA	dba 80M	1	 

Note: any change only takes effect after corresponding ONT service reactivated
 Note: Downstream Rate Limit only uses Fix/Max Rates

Bandwidth

The Max value can't be set to zero, it should be the same or more than Fix/Assure value. The Fix/Assure default setting is zero and Max default setting is 512 kbps.

DBA

This field indicates the type of current traffic descriptor.

Note: Downstream Rate Limit does not use 'Assure'.

Method

Two type of DBA, status-reporting (SR) and non-status reporting (NSR).

Services

Display how many services referred to this profile. If the profile has been associated to particular services, it can't be deleted.

2.4.2 Edit Bandwidth Profile in CLI

Usage:

```
show bw_dba <all|idx>
bw_dba create <idx>
bw_dba remove <idx>
bw_dba config <idx> [fix <VALUE>] [assure <VALUE>]
                    [max <VALUE>] [sr|nsr]
                    [descr <"TEXT">]
```

Note: fix/assure/max: multiples of 8 kbps
Downstream Rate Limit only uses fix/max Rates

Add a new bandwidth profile (index=2)

```
admin@192.168.1.150:> bw_dba create 2
```

Info: create successfully.

Edit bandwidth profile (index=2), fix/assure/max=10/10/20M, NSR.

```
admin@192.168.1.150:> bw_dba config 2 fix 10000 assure 10000 max 20000 nsr descr "20M"
```

Info: create successfully.

Add a new bandwidth profile (index=3)

```
admin@192.168.1.150:> bw_dba create 3
```

Info: create successfully.

Edit bandwidth profile (index=3), fix/assure/max=0/0/512M, NSR.

```
admin@192.168.1.150:> bw_dba config 3 fix 0 assure 0 max 512 nsr descr "voip"
```

Info: create successfully.

Inquire bandwidth profiles

```
admin@192.168.1.150:> show bw_dba all
```

```
bw-1, "default", fix=0 kbps, assure=0 kbps, max=512 kbps, nsr
bw-2, "20M", fix= 10000 kbps, assure= 10000 kbps, max= 20000 kbps, nsr
bw-3, "voip", fix=0 kbps, assure=0 kbps, max=512 kbps, nsr
```

2.5 ONT Image Profile

The administrator can assign the ONT software image with version number and download path by either GUI or CLI commands. This profile is used by ONT configuration. The administrator can also upgrade ONT with this profile manually.

2.5.1 Edit ONT Image in GUI

GUI Path: >GPON>Configuration-Profiles>ONT-Images

Index	Version	Protocol	File Link	Description	ONTs	
1	ve1.0.7	TFTP	192.168.1.123:img_ve107	ont image 1	0/0/idle	  

ftp ex: [user[:password]@]server_address/file_path/file_name
tftp ex: server_address:file_name
Note: any change only takes effect after corresponding ONT reactivated

The administrator should specify the location link of ONT image with protocol option (FTP or TFTP).

2.5.2 Automatic ONT Upgrade

The administrator can specify the ONT Image profile to registered ONT in Section 2.11. When OLT activates the ONT, the version information from ONT will be compared with the version string of ONT Image Profile. If they do not match, OLT will ask the ONT to upgrade.

2.5.3 Edit ONT Image in CLI

Usage:

```
show ont-image <all|idx>
ont-image create <idx> <"Version TEXT">
ont-image remove <idx>
ont-image config <idx> [version <"TEXT">] [descr <"TEXT">]
                        [<ftp|tftp> <PARAM>]
```

PARAM example:

```
ftp: [user[:password]@]server_address/file_path/file_name
tftp: server_address:file_name
```

Add an new ONT Image Profile with version string 've1.0.7'

```
admin@192.168.1.150:> ont-image create 1 "ve1.0.7"
```

Info: create successfully.

Assign file link and protocol type to ONT Image Profile

```
admin@192.168.1.150:> ont-image config 1 tftp 192.168.1.123:img_ve107
```

Info: update successfully.

Specify the ONT Image Profile to ONT 1-3

```
admin@192.168.1.150:> ont config 1 3 img 1
```

Info: update successfully.

2.6 ONT Config Profile

This profile is used by ONT configuration update. The administrator can update ONT configuration with this profile manually.

Note: *This feature requires ONT support.*

2.6.1 Edit ONT Config Profile in GUI

Here is an example to create a ONT Config profile and upload it onto ONT.

GUI Path: >GPON> Configuration-Profiles>ONT-Cfg

Index	Protocol	File Name	Description	ONTs	
1	TFTP	192.168.1.10:mgmt_db	mgmt_db	0	  
ftp example: server_address:file_name ftp example: server address:file name					
Note: any change only takes effect after corresponding ONT reactivated					

1. Create ONT Config profile
select protocol: TFTP or FTP
assign filename: 192.168.1.10:mgmt_db

GUI Path: >GPON>ONT>Managed

Status	IS	
ONT Index	ONT-1-2	
Vendor ID	ONTL (4F4E544C)	
Version	407-2200	
Equipment ID	ON-608	
Serial Number/Password	4F4E544C-23000676	4D25000001
SW Image 0/1	null	3.04.584B, Valid, Committed, Active
Number of Interface	T:CONT/UNI/POTS: 8/6/2	EqD = 265385, (0.071 km)
DS Signal Level	OLT_TX(3.33 dBm) - ONT_RX(-20.96 dBm) = 24.29 dBm	
US Signal Level	ONT_TX(3.14 dBm) - OLT_RX(-22.37 dBm) = 25.51 dBm	
Transceiver Parameters	Temperature: 0.0 °C, Voltage: 0.00 V, Laser Bias: 0.00 mA	
IP Host/CFG File	IP Address: 0.0.0.0, Netmask: 0.0.0.0, Gateway: 0.0.0.0 MAC Address: 00:16:52:F0:6A:44	
ONT Image	1. ont image 1	Manual Upgrade
ONT Config	Select ONT CFG	Manual Config
ONT Control	Reboot	Measure ONT Signal Level
		Last measure time: 2013/12/10-14:14:18

2. Upload the ONT configuration profile by manual
Select profile: 1.mgmt_db and click button 'Manual Config' to upload configuration file onto ONT manually.

2.6.2 Edit ONT Config Profile in CLI

Usage:

```
show ont-cfg <all|idx>
ont-cfg create <idx>
ont-cfg remove <idx>
ont-cfg config <idx> [<ftp|tftp> <PARAM>]
                    [descr <"TEXT">]
```

PARAM example:

```
ftp: [user[:password]@]server_address/file_path/file_name
tftp: server_address:file_name
```

Create a new ONT Config profile

```
admin@192.168.1.150:> ont-cfg create 1
```

Info: create successfully.

Specify file link and protocol type to ONT Config profile

```
admin@192.168.1.150:> ont-cfg config 1 tftp 192.168.1.10:mgmt_db
```

Info: update successfully.

Info: any change only takes effect after corresponding ONT reactivated.

*Note. If you select FTP mode, it is restricted to log in FTP site with anonymous.
The path and filename of Config profile is predefined and fixed.*

Ex: ftp://server_address/tmp/Configure.xml

Specify the ONT Config Profile to ONT 1-3

```
admin@192.168.1.150:> ont config 1 3  cfg 1
```

Info: update successfully.

Upload ONT configuration onto ONT 1-1 manually

```
admin@192.168.1.150:> ont managed 1 1  cfg 1
```

Info: action successfully.

2.7 SIP Server Profile

The SIP Server profile is used when VoIP service is activating in ONT. All parameters in SIP Server profile will be sent to ONT by OMCI.

Note: Any profile change will not affect the activated services in ONTs. It only takes effect after VoIP service is re-activated.

2.7.1 Edit SIP Server Profile in GUI

GUI Path: **>GPON> Configuration-Profiles>SIP Server**

Index	SIP Servers	User Agent Domain	Register Expire	Description	Services	
1	Proxy: 192.168.1.231:5060 Registrar: 192.168.1.232:5060 Outbound: :5060	test.domain	3600	sip server 1	0	 

Note: any change only takes effect after corresponding VoIP service reactivated

Proxy

The SIP Proxy server address.

Registrar

The Registrar server address.

Outbound

The Outbound proxy server address.

User Agent Domain

User agent's domain name.

Register Expire

the expire time for SIP register.

2.7.2 Edit SIP Server Profile in CLI

Usage:

```
show sip-server <all|idx>
sip-server create <idx>
sip-server remove <idx>
sip-server config <idx> [proxy <"TEXT">] [sip-port <VALUE>]
                        [regist <"TEXT">] [reg-port <VALUE>]
                        [outbound <"TEXT">] [out-port <VALUE>]
                        [agent <"TEXT">] [expire <VALUE>]
                        [descr <"TEXT">]
```

Create a new SIP Server profile

```
admin@192.168.1.150:> sip-server create 1
```

Info: create successfully.

Edit SIP Server profile

```
admin@192.168.1.150:> sip-server config 1 proxy "192.168.1.230"
```

Info: update successfully.

Info: any change only takes effect after corresponding VoIP service reactivated.

2.8 Server List for Proxy Agent

The Server List for Proxy Agent is used when DHCP proxy is required or option 'Security' is set to 'RADIUS' in Section 2.3.

2.8.1 Edit Server List in GUI

GUI Path: >GPON> Configuration-Profiles>Server List

Index	Server Type	Server IP	Virtual IP	U-VLAN List	Description	Status	
		S-VLAN	Gateway	Shared Secret			
1	DHCP RADIUS	192.168.1.11 20	192.168.1.157 0.0.0.0	VID: 10,20,2011 < *** hidden password *** >	server 1	checking  	

Server Type

The features that Remote Server supports. DHCP / RADIUS.

Server IP

The IP address of Remote Server.

S-VLAN

The VLAN ID in NNI (Uplink) for accessing remote server.

Virtual IP

The virtual IP address for proxy agent. It should be unique in the sub-network.

Gateway

If the proxy agent is not in the same sub-network of Remote Server, the administrator should specify the gateway address.

U-VLAN List

Only the packets in VLAN list from ONT side will be processed.

Shared Secret

If remote server supports RADIUS, this is the shared secret key for it.

2.8.2 Edit Server List in CLI

Usage:

```
show server-list <all|idx>
server-list create <idx> <server-addr>
server-list remove <idx>
server-list config <idx> [dhcp-relay <on|off>]
                        [radius <on|off>]
                        [vlan <VID>]
                        [vip <ADDR>]
                        [gate <ADDR>]
                        [list <none|LIST>]
                        [secret <"TEXT">]
                        [descr <"TEXT">]
```

Create a new Server profile. Remote server address is 192.168.1.254

```
admin@192.168.1.150:> server-list create 1 192.168.1.254
```

Info: create successfully.

Edit Server profile.

The remote server supports DHCP and is in VLAN 30 domain.

We assign Virtual IP 192.168.1.153(same subnetwork as remote server) to this device(Proxy Agent) and this device will handle DHCP with VLAN 10/20 packets from ONT and forward them to remote server.

```
admin@192.168.1.150:> server-list config 1 dhcp-relay on vlan 30 vip 192.168.1.153 list 10,20
```

Info: update successfully.

2.9 Service Profiles

For more flexible and convenient usage, DPN-6608 utilizes service profiles for Triple-Service. The administrator can specify parameters like DATA / IPTV / VoIP / ETH / CATV / MISC in the service profiles, and then go to Section 2.12 for the proper setting.

Note: any profile change will not affect the activated services in ONTs. It only takes effect after those services are re-activated.

2.9.1 Data Service Profile

GUI Path: >GPON>Service-Profiles/Data

Index	VLAN ID	DS Encryption	Bridge Mode	Only Broadcast	Upstream BW	Downstream BW	Description	Services	
1	s 10, u100	no	Yes	no	1. default	0. not used	data 1	0	 
2	s 20, u 200	no	no	no	1. default	0. not used	data 2	0	 

Note: any change only takes effect after corresponding ONT service reactivated

DS Encryption

Checked to enable the encryption on DS GEM port.

Bridge Mode

Checked to enable the bridge mode of ONT. It requires ONT support.

Only Broadcast

Checked to create Broadcast GEM Port only.

Note: this option is used for requiring broadcast traffic in data stream path and the associated VLAN should also enable option 'with broadcast'.

Upstream BW

Upstream Bandwidth Association.
Refer to Section 2.4.

Downstream BW

Downstream Bandwidth Association.
Refer to Section 2.4.

2.9.2 IPTV Service Profile

GUI Path: **>GPON>Service-Profiles/IPTV**

Index	VLAN ID	DS Encryption	Only Multicast	Upstream BW	Downstream BW	Description	Services	
1	s_2011_u_2011	no	Yes	1.default	0. not used	iptv 1	0	  

Note: any change only takes effect after corresponding ONT service reactivated

DS Encryption

Checked to enable the encryption on DS GEM port.

Only Multicast

Checked to create Multicast GEM Port only.

Note: this option is used for supporting multiple multicast streams in different VLANs. In the case, option 'multi-VLAN IPTV' in 3.2 should be enabled.

Upstream BW

Upstream Bandwidth Association.
Refer to Section 2.4.

Downstream BW

Downstream Bandwidth Association.
Refer to Section 2.4.

2.9.3 VoIP Service Profile

GUI Path: **>GPON>Service-Profiles/VoIP**

Index	VLAN ID	DS Encryption	SIP Server	Upstream BW	Downstream BW	Description	Services	
1	s_20_u_200	no	1.sip server 1	1.default	0. not used	voip 1	0	  

Note: any change only takes effect after corresponding ONT service reactivated

DS Encryption

Checked to enable the encryption on DS GEM port.

SIP Server

SIP Server Association.
Refer to Section 2.7.

Upstream BW

Upstream Bandwidth Association.
Refer to Section 2.4.

Downstream BW

Downstream Bandwidth Association.
Refer to Section 2.4.

2.9.4 Ethernet UNI Service Profile

GUI Path: **>GPON>Service-Profiles/ETH**

Index	UNI	VLAN	P-Bits	UNI Mode	IP Host	IPcam	Description	Services		
1	1	10	0	Untagged	no	no	vid 10 uni 1	0		
2	3	2011	0	Untagged	no	no	vid 2011 uni 3	2		
3	4	30	0	Untagged	no	no	vid 30 uni 4	2		

Note: any change only takes effect after corresponding ONT service reactivated

UNI

The index of Ethernet UNI port in ONT.

VLAN

The expected VLAN ID for UNI port.

P-Bits

Priority bit for this UNI port.

UNI Mode

Tagging mode of this UNI port.

Untagged: packets to this UNI port should be untagged.

Tagged: packets to this UNI port should be tagged as **VLAN**.

Transparent: packets from/to this UNI should be tagged and the tag will not be modified by UNI.

IPHost

Checked to enable IP-Host in ONT. It requires ONT support.

IPCam

Checked to enable IP Camera in ONT. It requires ONT support.

2.9.5 CATV Service Profile

GUI Path: **>GPON>Service-Profiles/CATV**

Index	Enable	Description	Services	
0		<input type="text"/>		
no profile found				

Note: any change only takes effect after corresponding ONT service reactivated

Enable

Checked to turn on CATV in ONT. Unchecked to turn off CATV in ONT. It requires ONT support.

2.9.6 Misc Service Profile

GUI Path: **>GPON>Service-Profiles/MISC**

Index	Authentication	Description	Services
0	<input checked="" type="checkbox"/>		
no profile found			
Note: any change only takes effect after corresponding ONT service reactivated			

Authentication

Checked to enable the authentication on ONT. Also see Section 2.15.

CLI command for all service profiles:

```
admin@192.168.1.150:> help svc-data

Usage:
  show svc-data <svcid|all>
  svc-data create <svcid> <none|vlan>
  svc-data remove <svcid>
  svc-data config <svcid> [vlan <none|VID>] [encrypt <on|off>]
                        [ubw <VALUE>] [dbw <VALUE>]
                        [bridge <on|off>] [only-bc <on|off>]
                        [descr <"TEXT">]

admin@192.168.1.150:> help svc-iptv

Usage:
  show svc-iptv <svcid|all>
  svc-iptv create <svcid> <none|vlan>
  svc-iptv remove <svcid>
  svc-iptv config <svcid> [vlan <none|VID>] [encrypt <on|off>]
                        [ubw <VALUE>] [dbw <VALUE>]
                        [only-mc <on|off>]
                        [descr <"TEXT">]

admin@192.168.1.150:> help svc-voip

Usage:
  show svc-voip <svcid|all>
  svc-voip create <svcid> <none|vlan>
  svc-voip remove <svcid>
  svc-voip config <svcid> [vlan <none|VID>] [encrypt <on|off>]
                        [ubw <VALUE>] [dbw <VALUE>]
                        [sip <VALUE>] [descr <"TEXT">]
```

```
admin@192.168.1.150:> help svc-eth
```

Usage:

```
show svc-eth <svcid|all>
svc-eth create <svcid> <uniid> <none|vlan>
svc-eth remove <svcid>
svc-eth config <svcid> [uniid <ID>] [vlan <VID>]
                        [untag|tagged|transparent]
                        [iphost <on|off>] [ipcam <on|off>]
                        [pbits <VALUE>] [descr <"TEXT">]
```

Note:

```
transparent mode: vlan = none
untag/tagged mode: vlan = 1 to 4095
```

```
admin@192.168.1.150:> help svc-catv
```

Usage:

```
show svc-catv <svcid|all>
svc-catv create <svcid>
svc-catv remove <svcid>
svc-catv config <svcid> <on|off> [descr <"TEXT">]
```

```
admin@192.168.1.150:> help svc-misc
```

Usage:

```
show svc-misc <svcid|all>
svc-misc create <svcid>
svc-misc remove <svcid>
svc-misc config <svcid> [auth <on|off>] [descr <"TEXT">]
```

2.10 Auto-Provision Profile

The Auto-Provision profile is used for updating ONT configuration automatically when new discovered ONT is activating. To enable this feature in each OLT, the option 'Pwd-Auth' in Section 2.1 should be set to 'Auto-Provision'.

2.10.1 Edit Auto-Provision Profile in GUI

GUI Path: **GPON>Service-Profiles>Auto-Provision**

Index	Password	SW Version	Encryption	US FEC	Locked	ONT-Service Slot	Description	
		ONT CFG	Auto Learn	Mib Upload				
1	0000000000	0. not used 0. not used	- Auto-Learn	-	-	1. Data-1 . vid 100 2. IPTV-1 . vid 2011 3. 4. 5.	6. ETH-1 . vid 100 uni 4 7. 8. 9. 10.	 
auto provision 1								
<i>Note: any change only takes effect to new discovered ONTs</i>								

Password

During ONT activation, ONT Password will be compared with this field. If they are matched, the configuration of the matched Auto-Provision Profile will replace that ONT configuration and that ONT will be re-activated with new configuration.

SW Version

During ONT activation, OLT will check ONT software version is matched with this assignment or not. If not, OLT will try to upgrade ONT. Refer to Section 2.5.

ONT CFG

During ONT activation, OLT will check ONT configuration is matched with this assignment or not. If not, OLT will try to upload configuration file onto ONT. (**optional. It requires ONT support**) Refer to Section 2.6.

Encryption

Checked to encrypt the OMCI channel.

Auto Learn

Checked to allow OLT learn ONT's password automatically.

US FEC

Checked to enable Upstream Forward Error Correction.

MIB Upload

When this option is checked, OLT configures ONT resource according to the MIB data uploaded from ONT. If unchecked, OLT uses predetermined values for ONT configuration.

Locked

If unchecked, this ONT will be removed from database after device reboot.

ONT-Service Slots

These fields define what services will be assigned to ONT-Service. The maximum number of slot assignments is up to 10 currently. Refer to Section 2.9 and 2.12.

2.10.2 Edit Auto-Provision Profile in CLI

```
admin@192.168.1.150:> help auto-profile

Usage:
show auto-profile <all|idx>
auto-profile create <idx> <Password>
auto-profile remove <idx>
auto-profile config <idx> [pwd <Password>] [locked <on|off>]
                        [img <VALUE>] [cfg <VALUE>]
                        [encrypt <on|off>] [auto-learn <on|off>]
                        [us-fec <on|off>] [mib-load <on|off>]
                        [svc <svcid> <none|<stype> <index> <CVID>>]
                        [descr <"TEXT">]

stype: data iptv voip eth catv misc
```

Create an new Auto-Provision Profile

```
admin@192.168.1.150:> auto-profile create 1 abcde12345

Info: create successfully.
```

Edit the Auto-Provision Profile

```
admin@192.168.1.150:> auto-profile config 1 img 1 cfg 1

Info: update successfully.
Info: any change only takes effect to new discovered ONTs.
```

2.11 ONT Registration

2.11.1 ONT Registration in GUI

This page shows ONTs registered in DPN-6608 and their information, including Serial Number, Password, SW version, ONT CFG, Encryption, Auto Learn, US FEC, Locked State, Services and POTS.

The administrator can also register a new ONT here manually in advance without ONT connected. The administrator MUST specify a unique Serial number for each ONT in a OLT. If “Auto Learn” option is checked, password field of ONT will be ignored during ONT activation. If it is unchecked, password field should match the password configured in that ONT. Password is a 10 ASCII character field.

For security, it is recommended to enable OMCI encryption.

GUI Path: **GPON>ONT**

OLT	ONT	Serial Number	SW Version	Encryption	US FEC	Locked	Description	Services	POTS	Current State	In Service	+
		Password	ONT CFG	Auto Learn	Mib-Upload							
1	1	54434F4D-25000002 0000000000	0. not used 0. not used	- Auto-Learn	- -	-	ont 1-1	0/0/0	0	IS	Yes	 
1	2	4F4E544C-23000676 0000000000	0. not used 0. not used	- Auto-Learn	- -	-	ont 1-2	0/0/0	0	IS	Yes	 

Password

Password for ONT registration. If auto learn is enabled, this password is ignored.

SW Version

During ONT activation, OLT will check ONT software version is matched with this assignment or not. If not, OLT will try to upgrade ONT. Refer to Section 2.5.

ONT CFG

During ONT activation, OLT will check ONT configuration is matched with this assignment or not. If not, OLT will try to upload configuration file onto ONT. (optional. It requires ONT support) Refer to Section 2.6.

Encryption

Checked to encrypt the OMCI channel.

Auto Learn

Checked to allow OLT learn ONT's password automatically.

US FEC

Checked to enable Upstream Forward Error Correction.

MIB Upload

When this option is checked, OLT configures ONT resource according to the MIB data uploaded from ONT. If unchecked, OLT uses predetermined values for ONT configuration.

Locked

If unchecked, this ONT will be removed from database after device reboot.

Services

Display how many services are associated to and how many are being used in this ONT. Also see Section 2.9 and 2.12.

POTS

Display how many POTS data are associated to this ONT. Refer to Section 2.14.

2.11.2 ONT Discovery in GUI

When a new ONT is discovered by a specific OLT like OLT 1 as illustrated in the following example, the administrator can go to “>GPON” menu, then click “>ONT” sub-menu, then click “>Discovered” to take a look at which ONT has been discovered by OLT. In this example, you can see OLT:1(2), and it means there are 2 discovered ONTs in OLT 1.

GUI Path: >GPON>ONT>Discovered

Discovered ONT			OLT: 1(2) 2(0) 3(0) 4(0) 5(0) 6(0) 7(0) 8(0)								Auto-Refresh <input type="checkbox"/>	
<input type="checkbox"/>	Serial Number	Discovered Time	ONT Parameters									
<input type="checkbox"/>	4F4E544C-23000676	2013/11/21 15:21:50	<input checked="" type="checkbox"/> In Service									
<input type="checkbox"/>	54434F4D-25000002	2013/11/21 15:21:50	<input type="checkbox"/> OMCI Encryption									
<i>Note: aged Serial Number will be removed automatically. (5 minutes)</i>			<input type="checkbox"/> US FEC									
			<input checked="" type="checkbox"/> Auto Learn									
			<input type="checkbox"/> Mib Upload									
			<input checked="" type="checkbox"/> Locked									
<input type="button" value="Add selected ONT(s) into Registered Table"/>												

The administrator can click “Add selected ONT(s) into Registered Table” to register discovered ONT into device.

2.11.3 ONT Registration in CLI

Usage:

```
show ont <all|oltid [all|ontid]>
ont create <oltid> <ontid> <Serial Number>
ont remove <oltid> <ontid>
ont config <oltid> <ontid> [is|oos] [sn <Serial Number>]
                               [no-pwd|pwd <Password>]
                               [img <VALUE>] [cfg <VALUE>]
                               [encrypt <on|off>]
                               [us-fec <on|off>]
                               [auto-learn <on|off>]
                               [mib-load <on|off>]
                               [locked <on|off>]
                               [descr <"TEXT">]

ont managed <oltid> <ontid>
ont managed <oltid> <ontid> <img <VALUE>|cfg <VALUE>>
ont managed <oltid> <ontid> <reboot|measure>
ont discover <all|oltid>
ont counter <oltid> <ontid>
ont statistics <oltid> <ontid>
```

Serial Number: 16 digital numbers in hex format
example 00112233aabbccdd

List ONTs discovered by GPON OLT 1

```
admin@192.168.1.150:> ont discover 1

ont-1-1, sn=AABBCCDDEEFF0740
```

Add a new ONT with Index=1 and serial 'AABBCCDDEEFF0740'

```
admin@192.168.1.150:> ont create 1 1 AABBCCDDEEFF0740

Info: create successfully.
```

Activate ONT 1-1

```
admin@192.168.1.150:> ont config 1 1 is

Info: update successfully.

admin@192.168.1.150:> show ont 1 1

ont-1-1, descr="ont 1-1", is, encrypt=off, auto-learn=on, us-fec=off, mib-load=off,
locked=off, img=0, cfg=0, sn=AABBCCDDEEFF0740, pwd=0000000000,
status=IS, svc=0/0
```

2.11.4 ONT Alarm List

Alarm list when ONT registration is processed successfully or unsuccessfully:

Current state type	Description
Ranging	The ranging process had failed
Pwd-inconsistency	The password authentication failed; received 3 different passwords
Pwd-mismatch	The password authentication failed; received password does not match registered one
Auth-Timeout	The password authentication timeout
Onu-alarm	Activation failed because of ONT alarm
Onu-disabled	Activation failed because of disable ONT
Onu-los	Activation failed because of LOS
Los	Loss-Of-Signal
Losi	Loss-Of-Signal Indication of ONT
Lofi	Loss-Of-Frame Indication of ONT
DriftOfWindow	Drift-Of-Window of ONT
SignalFailure	Signal-Fail of ONT
SignalDegrade	Signal-Degrade of ONT
LossOfGemCh	Loss-Of-Gem-Channel-Delineation of ONT
RemoteDefect	Remote-Defect-Indication of ONT
StartUpFailure	Start-Up-Failure of ONT
LossOfAck	Loss-Of-Acknowledge from ONT
Dying-Gasp	Received Dying-Gasp message from ONT
DFi	DFi indication
PLOAMcellLoss	PLOAM-Loss of ONT
MessageError	Message-Error-Message from ONT
PhysicalEquError	Physical-Equipment-Error from ONT
PST	PST PLOAM message
TiWi	Transmission-Interference-Alarm of ONT
LOKi	Loss-Of-Key sync with ONT
ONT-BIP	OLT detects Upstream Bit Error (BIP)
ONT-REI	ONT detects Downstream Bit Error (REI)
ONT-DOW	OLT detects Drift-of-Window
ONT-Rogue	Rogue ONT - energy detected

Alarm list when ONT registration is not successful due to an OMCI failure:

Current state type	Description
OntOmciID	Failed to configure OMCI Port ID for ONT
OntDslIPTV	Failed to configure Gem Port ID for IPTV
OntUsFEC	Failed to configure Upstream FEC
OntAct	Failed to activate ONT
OntCfgLoad	Failed to load ONT configuration
OntOmciAct	Failed to activate OMCI Protocol
OntSvcCheck	Failed to deactivate Services
OntSvcAct	Failed to activate Services
OntLicense	License rejects this ONT
OntFinish	Failed to finish ONT Activation
OntOmciLink	Failed to establish OMCI Link
OntOmciRst	Failed to reset OMCI Mib reset
OntOmciMib	Failed to upload OMCI Mib
OntStaticMib	Failed to configure Static Mib file
OntResource	Failed to initialize ONT Resource
OntOmciSwVer	Failed to retrieve OMCI SwImageMe
OntOmciOntgGet	Failed to retrieve OMCI OntGMe
OntOmciOnt2gGet	Failed to retrieve OMCI Ont2GMe
OntOmciAniGet	Failed to retrieve OMCI AniGMe
OntOmciImgCmp	Failed to compare ONT SW version
OntOmciGalEth	Failed to create GalEthProfMe
OntOmciBrSvc	Failed to create MacBridgeSvcProfMe
OntOmciBrPort	Failed to create MacBridgePortConfigDataMe for UNI
OntOmciIpBrPort	Failed to create MacBridgePortConfigDataMe for POTS
OntOmciCfgGet	Failed to retrieve ONT CFG filename
OntOmciCfgAddr	Failed to create LargeStrMe for ONT CFG address
OntOmciCfgFile	Failed to create LargeStrMe for ONT CFG filename
OntOmciCfgCtrl	Failed to create NetAddrMe for ONT CFG control
OntOmciIPHostGet	Failed to retrieve IPHost Config
OntOmciReboot	Failed to reboot ONT Reboot
OntOmciImgReady	ONT SW Image Profile is not active
OntOmciImgGet	Failed to retrieve ONT SW Image
OntOmciSwUpdate	Failed to update ONT SW
OntOmciSwVerify	Failed to verify ONT SW Image
OntOmciSwCommit	Failed to commit ONT SW
OntOmciSwActive	Failed to activate ONT SW
OntOmciSetAddr	Failed to set LargeStrMe for ONT CFG address
OntOmciSetFile	Failed to set LargeStrMe for ONT CFG filename

OntOmciSetCtrl

Failed to set ONT CFG controller

2.11.5 ONT State

The current state of ONT is used to monitor ONT, and it is not accessible from OLT. As shown below, there are 5 Operation States for the ONT REGISTER. If ONT is in service state, then it should be in Operation State (O5)

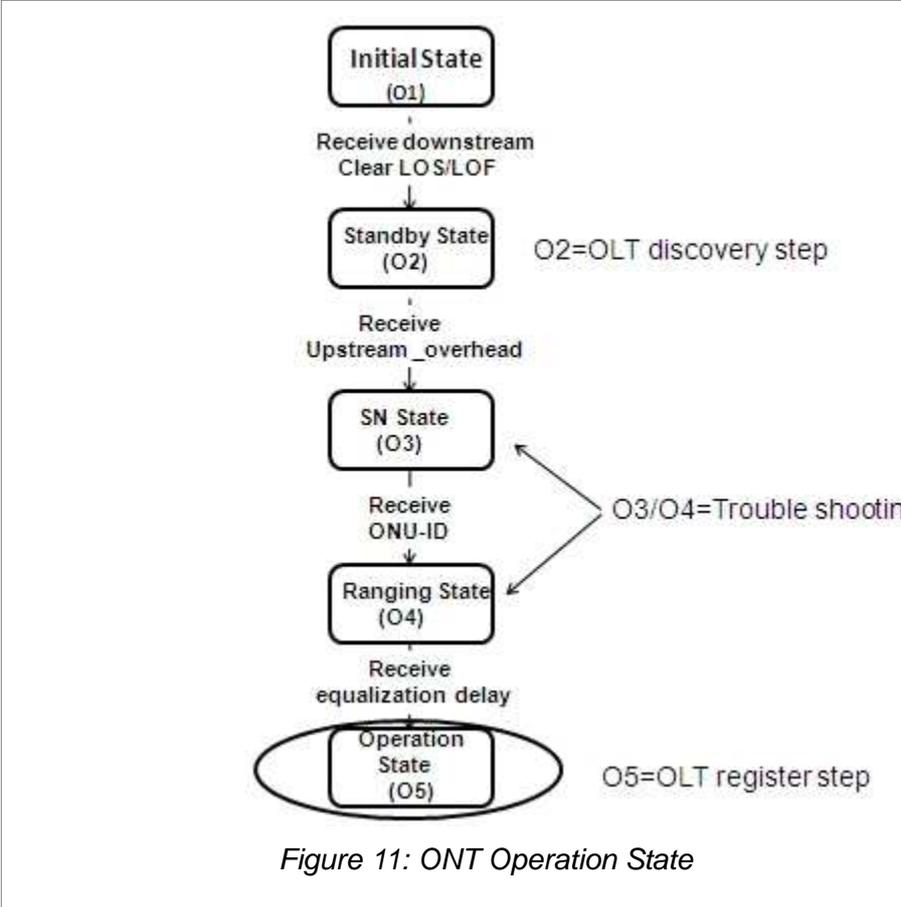


Figure 11: ONT Operation State

2.11.6 Managed ONT

The page shows the information of a specific and managed ONT. The administrator also can upgrade ONT image, upload ONT config or reboot ONT manually here.

GUI Path: **>GPON>ONT>Managed**

Status	IS	
ONT Index	ONT-1-2	
Vendor ID	DLNK(444C4E4B)	
Version	407-2200	
Equipment ID	DPN-R5402	
Serial Number/Password	444C4E4B-00000125	4D25000001
SW Image 0/1	null	3.04.584B, Valid, Committed , Active
Number of Interface	T-CONT/UNI/POTS: 8/6/2	EqD = 265385, (0.071 km)
DS Signal Level	OLT_TX(3.33 dBm) - ONT_RX(-20.96 dBm) = 24.29 dBm	
US Signal Level	ONT_TX(3.14 dBm) - OLT_RX(-22.37 dBm) = 25.51 dBm	
Transceiver Parameters	Temperature: 0.0 °C, Voltage: 0.00 V, Laser Bias: 0.00 mA	
IP Host/CFG File	IP Address: 0.0.0.0, Netmask: 0.0.0.0, Gateway: 0.0.0.0 MAC Address: 00:16:52:F0:6A:44	
ONT Image	1. ont image 1	Manual Upgrade
ONT Config	Select ONT CFG	Manual Config
ONT Control	Reboot	Measure ONT Signal Level
		Last measure time: 2013/12/10-14:14:18

1. ONT Status.
2. Reboot ONT manually.
3. Measure DS/US Signal Level and DDM information manually.
4. Manual ONT upgrade. Refer to Section 2.5.
5. Manual ONT config upload. Refer to Section 2.6.
6. Estimate the real distance between OLT and ONT.

CLI command "**ont managed**" also can get the same result as shown below:

```
admin@192.168.1.150:> ont managed 1 1
```

```
ont-1-1: IS
Vendor ID..... xxxx
Version..... xxxxxxxx
Equipment ID..... xxxxxx
Serial Number..... xxxxxxxx-23000xxx
Password..... xxxxxx0001
Number of Interface. 8/6/2 (T-CONT/UNI/POTS)
EqD..... 265383, (0.071 km)
SW Image 0..... null
SW Image 1..... xxxxxxxx, Valid, Committed, Active
DS Signal Level..... OLT_TX(3.32 dBm) - ONT_RX(-21.05 dBm) = 24.37 dBm
US Signal Level..... ONT_TX(3.15 dBm) - OLT_RX(-22.84 dBm) = 25.99 dBm
Temperature..... 73.0 C
Supply Voltage..... 3.30 V
Laser Bias Current.. 27.44 mA
Last Measure Time... 2013/11/14-17:00:44
IPHost IP Address... 0.0.0.0
IPHost Netmask..... 0.0.0.0
IPHost Gateway..... 0.0.0.0
IPHost MAC Address.. 00:xx:xx:xx:xx:xx
Configuration File..
```

2.11.7 Manual Operation on ONT

Usage:

```
show ont <all|oltid [all|ontid]>
ont create <oltid> <ontid> <Serial Number>
ont remove <oltid> <ontid>
ont config <oltid> <ontid> [is|oos] [sn <Serial Number>]
                               [no-pwd|pwd <Password>]
                               [img <VALUE>] [cfg <VALUE>]
                               [encrypt <on|off>]
                               [us-fec <on|off>]
                               [auto-learn <on|off>]
                               [mib-load <on|off>]
                               [locked <on|off>]
                               [descr <"TEXT">]

ont managed <oltid> <ontid>
ont managed <oltid> <ontid> <img <VALUE>|cfg <VALUE>>
ont managed <oltid> <ontid> <reboot|measure>
ont discover <all|oltid>
ont counter <oltid> <ontid>
ont statistics <oltid> <ontid>
```

Serial Number: 16 digital numbers in hex format
example 00112233aabbccdd

Specify ONT Image profile (index=1) to ONT 1-1

```
admin@192.168.1.150:> ont managed 1 1 img 1
```

Info: action successfully.

Specify ONT Config profile (index=1) to ONT 1-1

```
admin@192.168.1.150:> ont managed 1 1 cfg 1
```

Info: action successfully.

Reboot ONT 1-1 manually

```
admin@192.168.1.150:> ont managed 1 1 reboot
```

Info: action successfully.

Measure the signal level and DDM information of ONT 1-1 manually

```
admin@192.168.1.150:> ont managed 1 1 measure
```

Info: action successfully.

2.12 ONT Service Binding

Each ONT may provide several different services according to ONT model. Here the administrator can assign what and how many services(Data, IPTV, VoIP, ..., etc.) a ONT should have.

2.12.1 Specify ONT Service in GUI

GUI Path: **>GPON>ONT>Service-Binding**

ONT	SVC	Service Profile	C-VLAN	Custom GEM	Description	Alloc ID	GEM Port	Current State	In Service	
0		Service Profile								
1	1	Data-1. data 1	-	-	ont-1-1 svc-1	256	256	IS	Yes	 
1	2	IPTV-1. iptv 1	-	-	ont-1-1 svc-2	257	257	IS	Yes	 

Service Profile

Specify the service defined in Section 2.9 to this ONT.

2.12.2 Specify ONT Service in CLI

Usage:

```
show ont-svc <all|oltid [all|ontid [all|svcid]]>
ont-svc create <oltid> <ontid> <svcid> <stype> <index> <is|oos>
ont-svc remove <oltid> <ontid> <svcid>
ont-svc config <oltid> <ontid> <svcid> [is|oos]
                                     [svc <none|<stype> <index>>]
                                     [gem <VALUE>] [cvid <VID>]
                                     [descr <"TEXT">]

stype: data iptv voip eth catv misc
```

Specify ETH-UNI service(Index = 3) to ONT 1-4 SVC 4

```
admin@192.168.1.150:> ont-svc create 1 1 4 eth 3 is
```

Info: create successfully.

2.13 ONT Service Batch

ONT Service Batch is a simple tool for creating, overwriting or removing service profile assignments in multiple ONTs at the same time.

2.13.1 ONT Service batch in GUI

The administrator should make sure the necessary service profiles are created first before executing the batch.

1. Assign the DATA service(Index = 1) to OLT 1, ONT 4,5

GUI Path: **>GPON>ONT>Batch**

OLT	ONT	SVC	In Service	Service Profile	Description	Action
OLT-1	4 -5		<input checked="" type="checkbox"/>	Data-1. vid 30 U50 D75		Add

Note: ONT Service Index = 0 means assigned automatically

Service Profile

Specify the service defined in Section 2.9 to this ONT.

Select OLT-1
 ONT range: 4-5
 SVC: Data Service index = 1
 In Service: YES
 Service Profile: Data-1
 Action: Add

2. Process Result

OLT	ONT	SVC	In Service	Service Profile	Description	Action
OLT-1	4 -5	0	<input checked="" type="checkbox"/>	Data-1. vid 30 U50 D75		Add

Note: ONT Service Index = 0 means assigned automatically

Result of Batch: 2013-10-22 16:20:49

Action: Add new ONT-SVC
 Service: Data-1. vid 30 U50 D75

0 ONT-SVC processed.

2.13.2 ONT Service batch in CLI

```
Usage:
show ont-batch
ont-batch create <oltid> <ontid-a> <ontid-b> <svcid>
                    <is|oos> <stype> <index>
                    <cvid> [descr <"TEXT">]
ont-batch remove <oltid> <ontid-a> <ontid-b> <svcid>
ont-batch config <oltid> <ontid-a> <ontid-b> <svcid>
                    <is|oos> <stype> <index>
                    <cvid> [descr <"TEXT">]

ontid-a: begin of ontid
ontid-b: end of ontid
stype   : data iptv voip eth catv misc
```

Assign the DATA service (Index = 1) to OLT 1, ONT 4,5

Select the OLT-1
ONT range: 4-5
SVC: 1
In Service: YES
Service Profile: Data-1

```
admin@192.168.1.150:> ont-batch create 1 4 5 1 is data 1 0
```

```
Result of Batch:
Action : Add new ONT-SVC
Target : SVC-1
Service: data-1

0 ONT-SVC processed.
```

2.14 ONT POTS Data

The POTS data is used when ONT activates VoIP service. Each ONT may have multiple POTS data and all parameters of POTS data which has option 'Enable' checked will be passed to ONT one by one through OMCI channel during activating VoIP service.

Refer to VoIP Service defined in Section 2.9.

Note: any data change will not affect the activated VoIP service in ONTs. It only takes effect after those VoIP services are re-activated.

2.14.1 Edit ONT POTS in GUI

GUI Path: >GPON>ONT>POTS

OLT	ONT	UNI	Enable	Display Name	User Name	Description	+
				Phone Number	Password		
1	2. ont 1-2	1	Yes	test	2151	ont-1-2 pots-1	 
<p>Note: any change only takes effect after corresponding VoIP service reactivated</p>							

Create an new POTS data for ONT 1-2:

```

ONT> ont 1-2
UNI> 1
Enable> Yes
Display Name> "test"
User Name > "2151"
Phone Number > "2151"
Password > "2151"
  
```

2.14.2 Edit ONT POTS in GUI

Usage:

```
show ont-pots <all|oltid> [all|ontid [all|uniid]>
ont-pots create <oltid> <ontid> <uniid>
ont-pots remove <oltid> <ontid> <uniid>
ont-pots config <oltid> <ontid> <uniid>
                                [on|off]
                                [display <"TEXT">]
                                [phone <"TEXT">]
                                [user <"TEXT">]
                                [pass <"TEXT">]
                                [descr <"TEXT">]
```

Create a new POTS data for ONT 1-2

```
admin@192.168.1.150:> ont-pots create 1 2 1
```

Info: create successfully.

Info: any change only takes effect after corresponding VoIP service reactivated.

Edit the POTS data of ONT 1-2

```
admin@192.168.1.150:> ont- pots config 1 2 1 on display test phone 2151 user 2151 pass 2151
```

Info: update successfully.

Info: any change only takes effect after corresponding VoIP service reactivated.

2.15 ONT Authentication Data

The Authentication data is used when ONT activates Misc service with option 'Authentication' enabled. The method of authentication may be DHCP, PPPoE or Static IP. The options 'Parameters' in authentication data are valid when PPPoE or Static IP mode is selected.

Refer to Misc Service defined in Section 2.9.

Note: any data change will not affect the activated Misc service in ONTs. It only takes effect after those Misc services are re-activated.

2.15.1 Edit ONT Authentication in GUI

GUI Path: **>GPON>ONT>Auth**

OLT	ONT	IDX	Enable	Mode	VLAN	Parameters	Description	
1	1. ont 1-1	1	Yes	PPPoE	10	Param-1: root Param-2: root123 Param-3: Param-4:	ont-1-1 auth-1	 

Note: any change only takes effect after corresponding Misc service with Auth option enabled is reactivated

Mode = PPPoE
 Param-1: PPPoE User Name
 Param-2: PPPoE Password
 Param-3: PPPoE Access Concentrator
 Param-4: PPPoE Service Name

Mode = Static IP
 Param-1: Static IP address
 Param-2: Netmask
 Param-3: Gateway Address
 Param-4: DNS Server Address

Create an new authentication data with PPPoE mode for ONT 1-1:

ONT> ont 1-1

IDX> 1

Enable> Yes

Mode > PPPoE

VLAN > 10

Parameter 1 > "root"

Parameter 2 > "root123"

2.15.2 Edit ONT Authentication in CLI

Usage:

```
show ont-auth <all|oltid [all|ontid [all|numid]>
ont-auth create <oltid> <ontid> <numid>
ont-auth remove <oltid> <ontid> <numid>
ont-auth config <oltid> <ontid> <numid>
                [on|off] [vlan <VID>]
                [mode <pppoe|dhcp|static>]
                [param1 <"TEXT">]
                [param2 <"TEXT">]
                [param3 <"TEXT">]
                [param4 <"TEXT">]
                [descr <"TEXT">]
mode= pppoe, param1 is 'User Name'
                param2 is 'Password'
                param3 is 'Wan Access Concentrator'
                param4 is 'Service Name'
mode=static, param1 is 'Static IP address'
                param2 is 'Netmask'
                param3 is 'Gateway Address'
                param4 is 'DNS Server'
```

Create an new authentication data with PPPoE mode for ONT 1-1

```
admin@192.168.1.150:> ont-auth create 1 1 1
```

Info: create successfully.

Info: any change only takes effect after corresponding Misc service reactivated.

Edit the authentication data of ONT 1-1

```
admin@192.168.1.150:> ont-auth config 1 1 1 on mode pppoe vid 10 param1 "root" param2
"root123"
```

Info: update successfully.

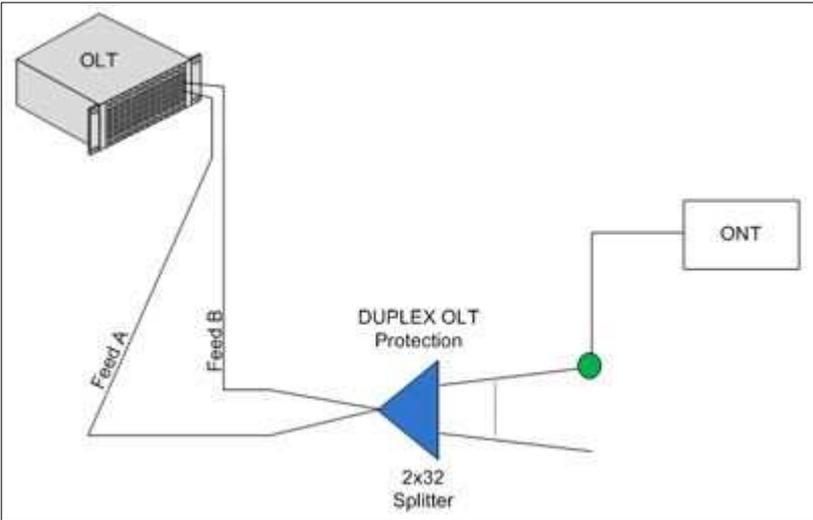
Info: any change only takes effect after corresponding Misc service reactivated.

2.16 GPON Redundancy

To enable OLT Redundancy feature, the administrator should specify the partner of GPON OLT in Section 2.1.

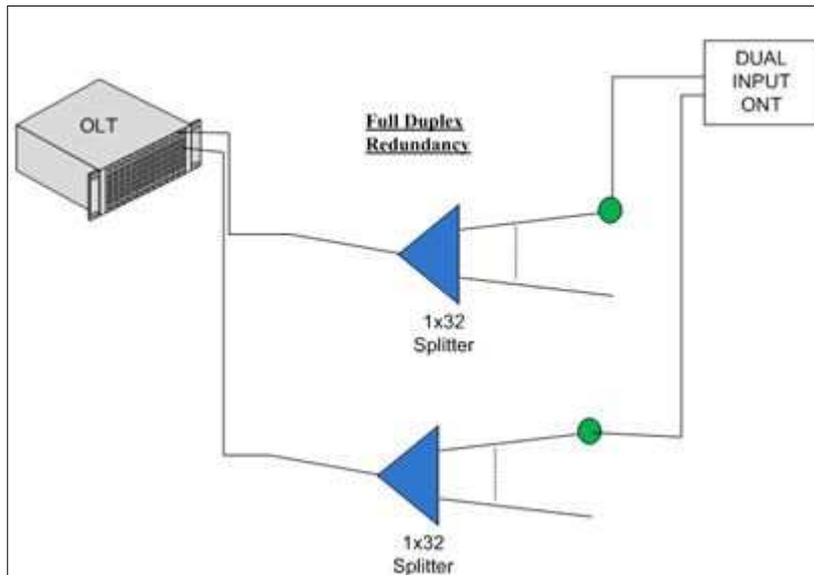
2.16.1 OLT Duplex Feed

The OLT duplex feed method relies on two separate GPON feeds from the OLT. Each of these feeds can take a diverse route to the customer splitter distribution location (Distribution Point). The traditional 1x32 Splitter is replaced by a 2x32 splitter and each input is fed with a separate OLT feed. This provides fallback should one OLT feed become damaged, enabling a software switch on the OLT to a separate line card enabling uninterrupted data transmission. The major benefit with this method is that the ONT and customer drop can remain as standard items and ensure that costs are not too high.



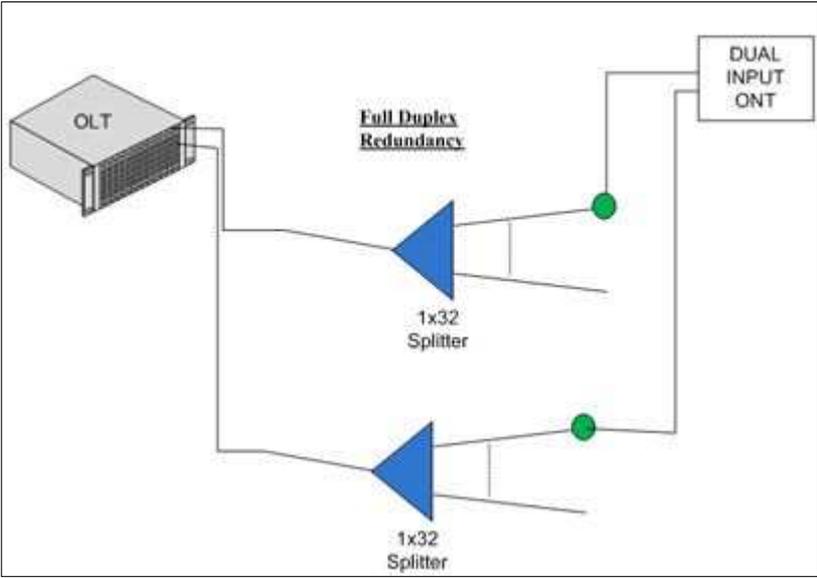
2.16.2 Full Duplex Redundancy

Full duplex redundancy requires two separate distribution nodes, coupled with two separate customer drops. This method provides a very effective redundancy method, however, the element with the highest cost of GPON deployment needs to be duplicated. A second disadvantage is the requirement for a Dual input ONT, a costly product for the customers.



2.16.3 Full Duplex Redundancy with dual chassis OLT

It is possible to add a second OLT at the head end. This method of resilience will provide the ultimate redundancy but essentially the administrator will be duplicating the GPON feed. So the customer will receive two separate GPON circuits which can be fed into a Dual input ONT.



2.16.4 Manual Redundancy in GUI

GUI Path: **>Monitoring>Diagnosis>Protection Switching**

OLT	Transceiver Type	Description	ONTs	DG	Busy	Current State	In Service	
1	(21)DELTA	PonLink-1	0/2	0	2	IS	working	
2		PonLink-2				IS (Los)	standby	

Click 'Save' icon to exchange service status of working/standby OLT ports.

2.16.5 Manual Redundancy in CLI

Usage:

diagnosis gpon switch <oltid>

diagnosis prbs [on]

diagnosis prbs <oltid> [clr]

Warn: the only way let OLT goes back normal state is to
reboot device after prbs is on

Switch the working path to GPON OLT 2 manually

```
admin@192.168.1.150:> diagnosis gpon switch 2
```

Chapter 3 Ethernet Configuration

3.1 NNI Configuration

NNI stands for network-to-network interface and it determines the Ethernet ports facing the network side of the OLT, also called uplink ports. DPN-6608 has 4x 1G SFP, and 2x 10G SFP+ ports (and optional 2x 10/100/1000 base-T). The administrator can specify the link speed as fixed rate or AutoNeg.

3.1.1 Specify NNI Configuration in GUI

GUI Path: >Configuration/NNI

Port	Flow Control	Configured Speed	Egress Tag	Port VLAN ID	Current Speed	Status	
1	no	AutoNeg	Tagged	1	Down		
2	no	AutoNeg	Tagged	1	Down		
3	no	AutoNeg	Tagged	1	Down		
4	no	AutoNeg	Tagged	1	Down		
5	no	10Gbps FDX	Tagged	1	Down		
6	no	10Gbps FDX	Tagged	1	Down		
7	no	AutoNeg	Untagged	1102	Down		
8	no	AutoNeg	Tagged	1	Down		

Flow Control

Checked to enable flow control.

Configured Speed

Link speed of NNI port. AutoNeg/100M/1G/10Gbps

Egress Tag

Tagged Mode: All packets from/to this port should be tagged. Untagged packets to this port will be discarded.

Untagged Mode: All packets from/to this port should be untagged. The default VLAN ID will be added into untagged packets to this port.

Current Speed

The detected link speed.

Status

Reports the service status of the NNI port: green=IS/red=OOS.

3.1.2 Specify NNI (Uplink) Configuration in CLI

Usage:

```
show nni <all|nniid>
nni config <nniid> [flow <on|off>]
                    [speed <none|auto|100M|1G|10G>]
                    [untag|tagged] [vlan <VID>]

nni sfp <nniid>
nni sfp <nniid> <temp|volt|bias|txp|rxp>
          <alarm|warning> <high|low>
          <SEVERITY>
```

SEVERITY: (0)None (1)Event (2)Minor (3)Major (4)Critical

Inquire the status of NNI ports

```
admin@192.168.1.150:> show nni all
```

```
nni-1, descr="NNI-1", flow=off, speed=auto, untagged, VLAN=1, status=1Gfdx
nni-2, descr="NNI-2", flow=off, speed=auto, untagged, VLAN=1, status=down
nni-3, descr="NNI-3", flow=off, speed=auto, tagged, VLAN=1, status=down
nni-4, descr="NNI-4", flow=off, speed=auto, tagged, VLAN=1, status=down
nni-5, descr="NNI-5", flow=off, speed=10G, tagged, VLAN=1, status=down
nni-6, descr="NNI-6", flow=off, speed=10G, tagged, VLAN=1, status=down
nni-7, descr="NNI-7", flow=off, speed=auto, untagged, VLAN=1102, status=down
nni-8, descr="NNI-8", flow=off, speed=auto, tagged, VLAN=1, status=down
```

Specify the default VLAN ID if NNI 1 to VLAN 1101

```
admin@192.168.1.150:> nni config 1 vlan 1101
```

Info: update successfully.

3.1.3 NNI SFP information

The administrator can check the detail SFP module information including the vendor name / part number / SN / Date code. If Digital Diagnostic Monitoring is available in SFP module, the administrator can also specify the Threshold Crossing indicators for Low/High threshold of parameters.

GUI Path: **> Configuration>NNI>SFP Information**

Module Information		Digital Diagnostic Monitoring (DDM)							
Vendor Name	CCC	Module Temperature	Alarm	Indicator	Low	Real-Time	High	Indicator	°C
Part Number	LC-DFB-S13-40D		Warning	Indicator	Low	Real-Time	High	Indicator	
Revision	A	Module Voltage	Alarm	Indicator	Low	Real-Time	High	Indicator	V
Serial Number	FC1308070093		Warning	Indicator	Low	Real-Time	High	Indicator	
Date Code	2013/08/13	Laser Bias	Alarm	Indicator	Low	Real-Time	High	Indicator	mA
Parameter Information			Warning	Indicator	Low	Real-Time	High	Indicator	
Transceiver	SFP	Laser Output	Alarm	Indicator	Low	Real-Time	High	Indicator	mW
Connector	LC		Warning	Indicator	Low	Real-Time	High	Indicator	
Link Length	40 km	Laser Rx	Alarm	Indicator	Low	Real-Time	High	Indicator	mW
Laser Wavelength	1310 nm		Warning	Indicator	Low	Real-Time	High	Indicator	
Encoding	SONET Scrambled								
Nominal Bit Rate	1200 Mbps								
Upper Rate Margin	0%								
Lower Rate Margin	0%								
Compatibility	00-00-00-00-00-00-00-00								

The CLI commands are shown below:

```
admin@192.168.1.150:> nni sfp 2
```

Module Information:

```
Vendor Name..... xxxxx  
Part Number..... LC-DFB-S13-40D  
Revision..... A  
Serial Number..... FC1308070093  
Date Code..... 2013/08/13
```

Parameter Information:

```
Transceiver..... SFP  
Connector..... LC  
Link Length..... 40 km  
Laser Wavelength..... 1310 nm  
Encoding..... SONET Scrambled  
Nominal Bit Rate..... 1200 Mbps  
Upper Rate Margin..... 0%  
Lower Rate Margin..... 0%  
Compatibility..... 00-00-00-00-00-00-00-00
```

Digital Diagnostic Monitoring: (ALM-LO/WARN-LO/WARN-HI/ALM-HI)

```
Module Temperature..... 39.1 C (-10.0/ -5.0/ 75.0/ 80.0)  
Module Voltage..... 3.20 V ( 3.00/ 3.10/ 3.50/ 3.60)  
Laser Bias Current..... 0.00 mA ( 1.00/ 6.00/ 70.00/ 80.00) **  
Laser Output Power..... 0.0000 mW (0.5623/0.7943/2.2387/3.1623) **  
-inf dbm  
Laser Rx Power..... 0.0000 mW (0.0019/0.0031/0.5012/0.7943) **  
-inf dbm
```

Threshold Crossing Indicators:

	ALM-LO	WARN-LO	WARN-HI	ALM-HI
Module Temperature.....	-	-	-	-
Module Voltage.....	-	-	-	-
Laser Bias Current.....	-	-	-	-
Laser Output Power.....	-	-	-	-
Laser Rx Power.....	-	-	-	-

3.2 Global Configuration

GUI Path: **> Configuration > Global**

General Configuration								
<input checked="" type="checkbox"/>	ONT Isolation Enable							
<input type="checkbox"/>	Multi-VLAN IPTV Enable							
<input checked="" type="radio"/>	IGMP Snooping mode: Disabled ▲▼							
IGMP parameters:								
	Query Interval(1-900 sec, def=125): 125			Max Response Time(1-25 sec, def=10): 10				
	Robustness Value(1-255, def=2): 2			Last Member Query Interval(1-25 sec, def=1): 1				
Connectivity Fault Management(CFM)								
<input type="checkbox"/>	Connectivity Fault Management Enable							
Maintenance Domain	Level							
	0	1	2	3	4	5	6	7
Customer	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>
Provider	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Operator	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
MAC Ageing Time								
<input checked="" type="radio"/>	15 minutes ▲▼		GPON MAC Ageing Time. change takes effect after OLT re-activation !!					
<input checked="" type="radio"/>	5 minutes ▲▼		Switch MAC Ageing Time.					

ONT Isolation

Checked to isolate the traffic between ONTs.

Multi-VLAN IPTV

Checked to support multiple IPTV streams.

IGMP Snooping mode

The global switch to control the IGMP snooping support. Option 'IGMP proxy' in S-VLAN is useless if this option is set to 'Disabled'.

Connectivity Fault Manage

The global switch to control the CFM support. There are 3 available Maintenance Domains with customized level.

MAC Aging Time

Define how long the learned MAC address will be expired and removed from device.

CLI command list:

Usage:

show global

global config [isolation <on|off>]

[multi IPTV <on|off>]

[igmp <none|snoop|proxy>]

[igmp_qi <VALUE>] [igmp_qri <VALUE>]

[igmp_rv <VALUE>] [igmp_llqi <VALUE>]

[cfm <on|off>] [customer <Level>]

[provider <Level>] [operator <Level>]

[bl_mac_age <VALUE>] [sw_mac_age <VALUE>]

3.2.1 ONT Isolation Case

To isolate the traffic between ONT 1 and ONT 2, the administrator should enable option 'ONT Isolation' in Global Configuration page.

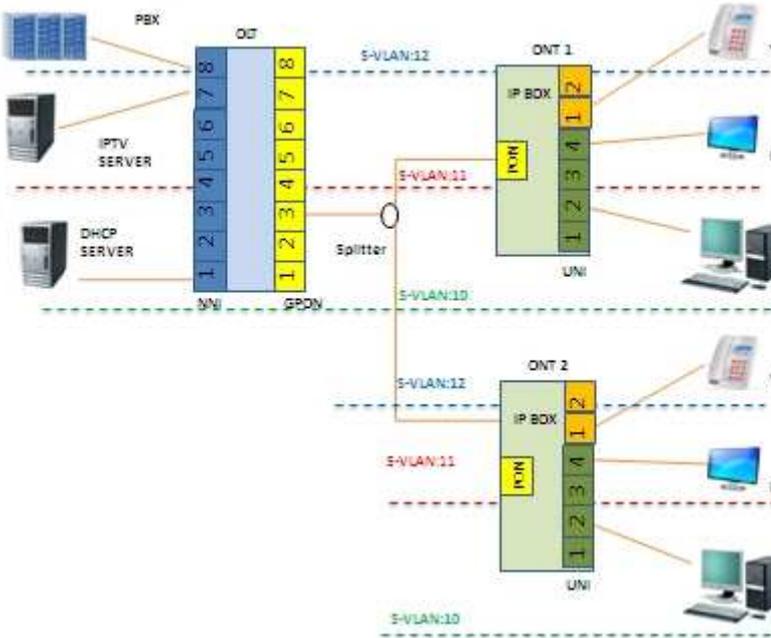


Figure 12: ONT Isolation Test Environment

Option 'ONT Isolation' is unchecked, ONT 1 UNI ports can receive packets from ONT 2 UNI ports, and ONT 2 UNI ports also can receive packets from ONT 1 UNI ports.

Option 'ONT Isolation' is checked, there is no traffic allowed between ONT 1 UNI ports and ONT 2 UNI ports.

3.2.2 Knowledge of IGMP

IGMP (Internet Group Management Protocol)

IGMP v1: Hosts can join multicast groups, but there were no leave messages. Routers were using a time-out based mechanism to discover the groups that are of no interest to the members.

Bits 0-3	4-7	8-15	16-31
version	Type	Max Resp Time	Check sum
32	Group address		

IGMP v2: Leave messages were added to the protocol. Allow group membership termination to be quickly reported to the routing protocol, which is important for high-bandwidth multicast groups and/or subnets with highly volatile group membership.

IGMP v3: Major revision of the protocol. It allows hosts to specify the list of hosts from which they want to receive traffic from. Traffic from other hosts is blocked inside the network. It also allows hosts to block inside the network packets that come from sources that sent unwanted traffic.

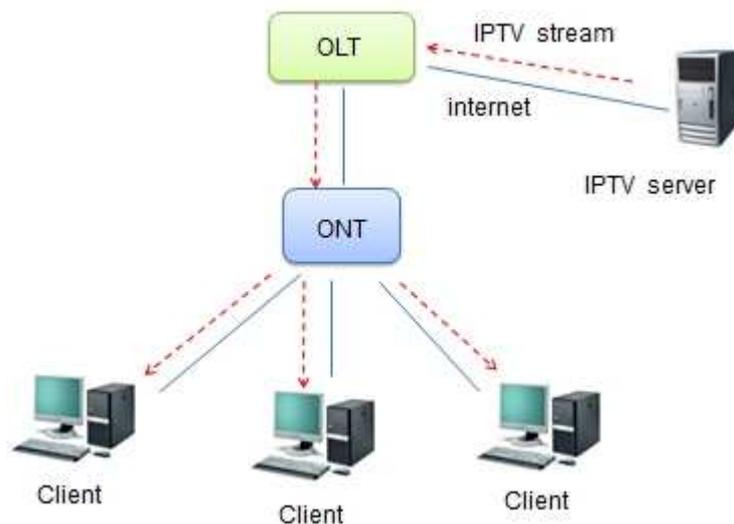
bit offset	0-3	4	5-7	8-15	16-31
0	Type = 0x11			Max Resp Code	Checksum
32	Group Address				
64	Resv	S	QRV	QQIC	Number of Sources (N)
96	Source Address [1]				
128	Source Address [2]				
	...				
	Source Address [N]				

IGMP Snooping

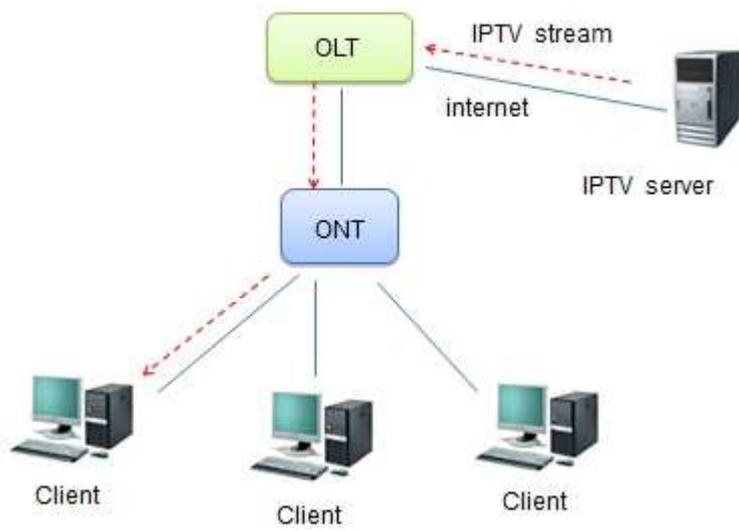
A layer-2 switch supports IGMP snooping can passively snoop on IGMP Query, Report and Leave (IGMP version 2) packets transferred between IP Multicast Routers/Switches and IP Multicast hosts to learn the IP Multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly.

Without IGMP snooping, multicast traffic is treated in the same manner as broadcast traffic, that is, it is forwarded to all ports. With IGMP snooping, multicast traffic of a group is only forwarded to ports that are members of that group. IGMP Snooping generates no additional network traffic, allowing you to significantly reduce multicast traffic passing through your switch. .

When not running IGMP snooping, multicast packet will broadcast the layer-2. As shown below:



After IGMP snooping is applied, packet is not broadcast in layer 2, it multicast in layer 2 as shown below:



The Multicast source only sends out the message once, Multicast Routing Protocol sets up tree-routing for Multicast data packet, and then the transferred packet just starts to be duplicated and distributed in the bifurcate crossing as far as possible. Thus the packet can be sent to users who need it accurately and efficiently.

Through IGMP snooping does not need to be manually set and the packet will not be sent to the other does not belong to the multicast group of the port, thus achieving fast L2 multicast packet forwarding.

IGMP Proxy

IGMP proxy enables the OLT to issue IGMP host messages on behalf of hosts that the OLT discovered through standard IGMP interfaces. The OLT acts as a proxy for its hosts.

Both IGMP Proxy and IGMP Snooping can build the same functionality but the principle is different : IGMP snooping only listens to get the IGMP messages, but IGMP Proxy intercepts the IGMP requests of end administrators and associated processing, then forwards it to the top router.

3.2.3 View IGMP Snooping in GUI

GUI Path: >Monitoring>IGMP>Snooping Status

VLAN ID	Querier Version	Host Version	Queries Transmitted	Queries Received	V1 Reports Received	V2 Reports Received	V3 Reports Received	V2 Leaves Received
1102	v3	v3	6	0	0	12	4	0

GUI Path: >Monitoring>IGMP>Groups Information

VLAN ID	Groups	NNI (UpLink)								GPON OLT							
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8
1102	239.255.12.42	-	-	-	-	-	-	-	-	V	-	-	-	-	-	-	-
1102	239.255.255.250	-	-	-	-	-	-	-	-	V	-	-	-	-	-	-	-

Querier Version

Current working querier version.

Host Version

Current working host version.

Querier Status

Show the Querier status is 'Active' or 'Idle'. 'Disable' denotes the specific interface is administratively disabled.

Querier Transmitted

The number of Transmitted Queries.

Querier Received

The number of Received Queries.

V1 Reports Received

The number of Received V1 Reports.

V2 Reports Received

The number of Received V2 Reports.

V3 Reports Received

The number of Received V3 Reports.

V2 Leaves Received

The number of Received V2 Leaves.

3.2.4 View IGMP Snooping in CLI

```
Usage:
  igmp status
  igmp group
```

Inquire the IGMP snooping status

```
admin@192.168.1.150:> igmp status

IGMP Snooping Status:
  VLAN  Querier/Host  Q-Transmit  V1-Reports  V3-Reports
        Q-Received  V2-Reports  V2-Leaves
  1102   v3/v3        6           0           4
        0           12          0
```

Inquire the IGMP group information

```
admin@192.168.1.150:> igmp group

IGMP Snooping Groups Information:
  VLAN  Groups          Member
  1102  239.255.12.42   olt=1
  1102  239.255.255.250 olt=1
```

3.3 Link Aggregation

DPN-6608 supports the Link Aggregation by either LACP or port trunking. Link aggregation can provide the benefits of load sharing and redundancy for NNI ports. Load sharing algorithm will be based on your hash code setting.

Link Aggregation Control Protocol (LACP) is part of an IEEE specification (802.3ad) that allows you to bundle several physical ports together to form a single logical channel. LACP allows a switch to negotiate an automatic bundle by sending LACP packets to the peer. LACP can be configured in one of two modes:

Link aggregation control protocol (LACP) is designed to implement dynamic link aggregation and de-aggregation. It is based on IEEE802.3ad and uses link aggregation control protocol data units (LACPDUs) to interact with its peers.

With LACP enabled on a port, LACP notifies the following information of the port to its peers by sending LACPDUs: priority and MAC address of this system, priority, number and operation key of the port. Upon receiving the information, the peer compares the information with the information of other ports on the peer device to determine the ports that can be aggregated. In this way, the two parties can reach an agreement in adding/removing the port to/from a dynamic aggregation group.

Operation key is generated by the system, and is determined by port settings such as port speed, duplex mode, and basic configurations.

The management key of an LACP-enabled dynamic aggregation port is 0 by default. The management key of an LACP-enabled static aggregation port is the same as the aggregation group ID. In a dynamic aggregation group, the member ports have the same operation key. In manual and static aggregation groups, the selected ports have the same operation key.

Link aggregation aggregates multiple physical Ethernet ports into one logical link, also called an aggregation group. It allows you to increase bandwidth by distributing traffic across the member ports in the aggregation group. In addition, it provides reliable connectivity because these member ports can dynamically back up each other.

3.3.1 Static LACP Aggregation

A static LACP aggregation group is also manually created. All its member ports are manually added and can be manually removed (it inhibits the system from automatically adding/removing ports to/from it). Each static aggregation group must contain at least one port. When a static aggregation group contains only one port, the port can only be removed when the whole aggregation group is removed.

LACP is enabled on the member ports of static aggregation groups, and you cannot disable LACP on such a port. When you remove a static aggregation group, the system will maintain the member ports of the group in LACP-enabled state and re-aggregate the ports to form one or more dynamic LACP aggregation groups.

Port status of static aggregation group

A port in a static aggregation group can be in one of the two states: selected or standby. Both the selected and the standby ports can transceive LACP protocol packets however, the standby ports cannot forward user packets.

In a static aggregation group, the system sets the ports to selected or standby state according to the following rules:

The system sets the "most preferred" ports (that is, the ports take most precedence over other ports) to selected state, and others to standby state. Port precedence descends in the following order: full duplex/high speed, full duplex/low speed, half duplex/high speed, half duplex/low speed. The system sets the state of the following ports to "standby": port connected to a peer device different from the one the master port is connected to; port connected to the same peer device as the master port but to a peer port that is not in the same aggregation group as the peer port of the master port.

The system sets the ports unable to aggregate with the master port (due to some hardware limit, for example, cross-board aggregation unavailability) to standby state. The system sets the ports with basic port configuration different from that of the master port to standby state.

Passive:

Sets a link to receive LACP messages, and responds with LACP when receiving a far-end LACP initiation.

3.3.2 Dynamic LACP Aggregation Group

Introduction to dynamic LACP aggregation group

A dynamic LACP aggregation group is automatically created and removed by the system. Users cannot add/remove ports to/from it. Ports can be aggregated into a dynamic aggregation group only when they are connected to the same peer device and have the same basic configuration, and the same rate and duplex mode. Besides multiple-port aggregation groups, the system is also able to create single-port aggregation groups, each of which contains only one port. LACP is enabled on the member ports of dynamic aggregation groups.

Port status of dynamic aggregation group

A port in a dynamic aggregation group can be in one of the two states: selected or standby. In a dynamic aggregation group, both the selected and the standby ports can transmit LACP protocol packets; however, the standby ports cannot forward user packets.

There is a limit on the number of selected ports in an aggregation group. Therefore, if the number of the member ports in an aggregation group exceeds the maximum number supported by the device, the system will negotiate with its peer end, to determine the states of the member ports according to the IDs of ports of the preferred device (that is, the device with smaller system ID). The following is the negotiation procedure:

Compare device IDs (system priority + system MAC address) between the two parties. First compare the system priority of the two devices. If the system priorities are equal, compare the MAC address of the two systems. The device with smaller device ID will be considered as the preferred one.

Compare port IDs (port priority + port number) on the preferred device. The comparison between two port IDs is as follows: First compare the two port priorities, then the two port numbers if the two port priorities are equal; the port with smaller port ID is the selected port and the other port is a standby port.

In an aggregation group, the selected port with the minimum port number serves as the master port of the group, and other selected ports serve as member ports of the group.

Active:

Enables the Ethernet link to send and receive LACP messages and automatically link aggregates when the remote system responds with the appropriate LACP messages.

3.3.3 Hash Code Contributors in GUI

GUI Path: >Configuration>L2-SW>Aggregation

Hash Code Contributors	
<input checked="" type="checkbox"/>	Source MAC Address
<input checked="" type="checkbox"/>	Destination MAC Address
<input type="checkbox"/>	IP Address
<input checked="" type="checkbox"/>	TCP/UDP Port Number

Source MAC Address

The Source MAC address can be used to calculate the destination port for the frame, and checked to enable the use of the Source MAC address, or unchecked to disable it. By default, Source MAC Address is enabled.

Destination MAC Address

The Destination MAC Address can be used to calculate the destination port for the frame, and checked to enable the use of the Destination MAC Address, or unchecked to disable it. By default, Destination MAC Address is disabled.

IP Address

The IP address can be used to calculate the destination port for the frame, and checked to enable the use of the IP Address, or unchecked to disable it. By default, IP Address is enabled.

TCP/UDP Port Number

The TCP/UDP port number can be used to calculate the destination port for the frame, and checked to enable the use of the TCP/UDP Port Number, or unchecked to disable it. By default, TCP/UDP Port Number is enabled.

3.3.4 Port Trunking in GUI

GUI Path: >Configuration>L2-SW>Aggregation

Group ID	Port Members							
	1	2	3	4	5	6	7	8
Normal	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input checked="" type="radio"/>
1	<input checked="" type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2	<input type="radio"/>							
3	<input type="radio"/>							
4	<input type="radio"/>							

Group ID for Port Trunking

Indicates the group ID for the settings contained in the same row. Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port.

Port Members for Port Trunking

Each switch port is listed for each group ID. Select a radio button to include a port in an aggregation, or clear the radio button to remove the port from the aggregation. By default, no ports belong to any aggregation group. Only full duplex ports can join an aggregation and ports must be in the same speed in each group.

3.3.5 LACP Configuration in GUI

GUI Path: >Configuration>L2-SW>Aggregation

Port	LACP Enable	Key			Role
1	<input checked="" type="checkbox"/>	Auto		(1-65535)	Active
2	<input checked="" type="checkbox"/>	Auto		(1-65535)	Active
3	<input type="checkbox"/>	Auto		(1-65535)	Active
4	<input type="checkbox"/>	Auto		(1-65535)	Active
5	<input type="checkbox"/>	Auto		(1-65535)	Active
6	<input type="checkbox"/>	Auto		(1-65535)	Active
7	<input type="checkbox"/>	Auto		(1-65535)	Active
8	<input type="checkbox"/>	Auto		(1-65535)	Active

LACP Enable

Check the box “LACP Enable” to enable LACP on this specified switch port. LACP will form an aggregation when 2 or more ports are connected to the same partner. LACP can form max 12 LLAGs per switch and 2 GLAGs per stack.

Key

The Key value incurred by the port, range 1-65535. The Auto setting will set the key appropriately by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3. Using the specific setting, a administrator-defined value can be entered. Ports with the same Key value can participate in the same aggregation group, while ports with different Keys cannot.

Role

The Role shows the LACP activity status. The Active will transmit LACP packets every second; while Passive will wait for a LACP packet from a partner (speak if spoken to).

3.3.6 LACP Status in GUI

GUI Path: >Monitoring>LACP>System Status

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
1	02:03:04:05:07:21	3	0d 00:00:32	1,2

Aggr ID

The Aggregation ID associated with this aggregation instance.

Partner System ID

The system ID (MAC address) of the aggregation partner.

Partner Key

The Key that is assigned to this aggregation ID.

Last changed

The timestamp since this aggregation changed.

Local Ports

Shows which ports are the members of this aggregation for this switch.

GUI Path: >Monitoring>LACP>Port Status

Port	LACP	Key	Aggr ID	Partner System ID	Partner Port	LACP Received	LACP Transmitted	Discarded	
								Unknown	Illegal
1	Yes	3	1	02:03:04:05:07:21	1	475	483	0	0
2	Yes	3	1	02:03:04:05:07:21	2	467	474	0	0
3	no	-	-	-	-	0	0	0	0
4	no	-	-	-	-	0	0	0	0
5	no	-	-	-	-	0	0	0	0
6	no	-	-	-	-	0	0	0	0
7	no	-	-	-	-	0	0	0	0
8	no	-	-	-	-	0	0	0	0

LACP

“Yes” means that LACP is enabled and the port link is up. “No” means that LACP is not enabled or the port link is down. “Backup” means that the port could not join the aggregation group but will join if other port leaves, and its LACP status is disabled.

Key

The key assigned to this port. Only ports with the same key can be aggregated together.

Aggr ID

The Aggregation ID assigned to this aggregation group

Partner System ID

The partner's System ID (MAC address).

Partner Port

The partner's port number connected to this port.

LACP Received

Shows how many LACP frames have been received at each port.

LACP Transmitted

Shows how many LACP frames have been sent from each port.

Discarded

Shows how many unknown or illegal LACP frames have been discarded at each port.

3.3.7 Link Aggregation in CLI

Usage:

```
show aggregation
aggregation hash [smac <on|off>] [dmac <on|off>]
                 [ip <on|off>] [port <on|off>]
aggregation port
aggregation port <nniid> [lACP <on|off>] [key <auto|1-65535>]
                    [group <VALUE>] [role <active|passive>]
aggregation port-status <nniid>
aggregation lACP-status
```

Inquire all aggregation configuration

```
admin@192.168.1.150:> show aggregation
Hash Code Contributors:
Source MAC Address..... on
Destination MAC Address..... on
IP Address..... off
TCP/UDP Port Number..... on

LACP Port Configuration:
nni-1, lACP=off, key=auto, role=active, group=0
nni-2, lACP=off, key=auto, role=active, group=0
nni-3, lACP=off, key=auto, role=active, group=0
nni-4, lACP=off, key=auto, role=active, group=0
nni-5, lACP=off, key=auto, role=active, group=0
nni-6, lACP=off, key=auto, role=active, group=0
nni-7, lACP=off, key=auto, role=active, group=0
nni-8, lACP=off, key=auto, role=active, group=0

Aggregation Static Group:
Normal(0)..... nni="1,2,3,4,5,6,7,8"
Group-1..... nni="none"
Group-2..... nni="none"
Group-3..... nni="none"
Group-4..... nni="none"
```

Inquire LACP system status

```
admin@192.168.1.150:> aggregation lacp-status 1
```

Aggr ID	Partner System ID	Partner Key	Last Changed	Local Ports
1	02:03:04:05:07:21	3	0d 00:00:32	1,2

Inquire LACP status and statistics.

```
admin@192.168.1.150:> aggregation port-status 1
```

NNI 1 Status/Statistics

```
LACP support      : on
Port Key          : 3
Aggr ID           : 1
Partner System ID : 02:03:04:05:07:21
Partner Port      : 1
LACP Received     : 475
LACP Transmitted  : 483
Unknown Discarded : 0
Illegal Discarded : 0
```

```
admin@192.168.1.150:> aggregation port-status 2
```

NNI 2 Status/Statistics

```
LACP support      : on
Port Key          : 3
Aggr ID           : 1
Partner System ID : 02:03:04:05:07:21
Partner Port      : 2
LACP Received     : 467
LACP Transmitted  : 474
Unknown Discarded : 0
Illegal Discarded : 0
```

3.4 Port Based VLAN

The DPN-6608 can store the Port Base VLAN up to 15 rules in the device, and won't accept anything more than that.

3.4.1 Specify Port Based VLAN in GUI

GUI Path: >Configuration>L2-SW>Port Based VLAN

Port based VLAN Rule	NNI (UpLink)								GPON OLT								+	
	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8		
1	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	S												
	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	e	X

Check the box to be the same port based VLAN group.

3.4.2 Specify Port Based VLAN in CLI

Usage:

```
show pbvlan <all|idx>
pbvlan create <idx>
pbvlan remove <idx>
pbvlan config <idx> [nni <none|LIST>] [olt <none|LIST>]
```

Add a new Port Based VLAN rule (index=2)

```
admin@192.168.1.150:> pbvlan create 2
```

Info: create successfully.

Specify NNI 1/2 and GPON OLT 1/2 to this rule

```
admin@192.168.1.150:> pbvlan config 2 nni 1,2 olt 1,2
```

Info: update successfully.

Inquire this rule

```
admin@192.168.1.150:> show pbvlan 2
```

```
rule-2, nni="1,2", olt="1,2"
```

3.5 Rate Storm Control

To prevent the system from the impact of Rate Storm, different data rate can be set for different packet. Once the rate storm of the packet goes over the limit, the system can filter the packets for system stability.

3.5.1 Specify Rate Storm Control in GUI

GUI Path: **>Configuration>L2-SW>Rate Control**

Port	Unknown Unicast	Broadcast	Multicast	CPU Traffic
NNI-1	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-2	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-3	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-4	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-5	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-6	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-7	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NNI-8	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-1	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-2	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-3	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-4	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-5	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-6	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-7	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
OLT-8	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps
NMS	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] kbps	<input type="checkbox"/> [] fps

Note: Maximum Rate is 15,000,000 kbps.

3.5.2 Specify Rate Storm Control in CLI

Rate storm control by CLI:

Usage:

```
show rate-control
rate-control <nni <nniid>|olt <oltid>|nms>
           [unknown <off|VALUE>] [broadcast <off|VALUE>]
           [multicast <off|VALUE>] [cpu_port <off|VALUE>]
```

NOTE:

VALUE is in kbps. Maximum value is 15000000.

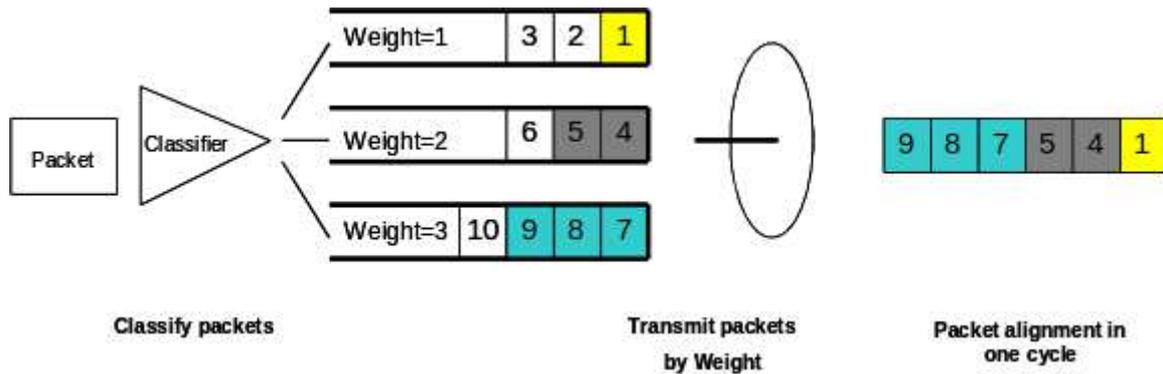
For cpu_port is recommended values higher than 50000.

3.6 Quality of Service (QoS)

OLT supports "Weighted Round-Robin" & "Strict Priority" method traffic scheduling:

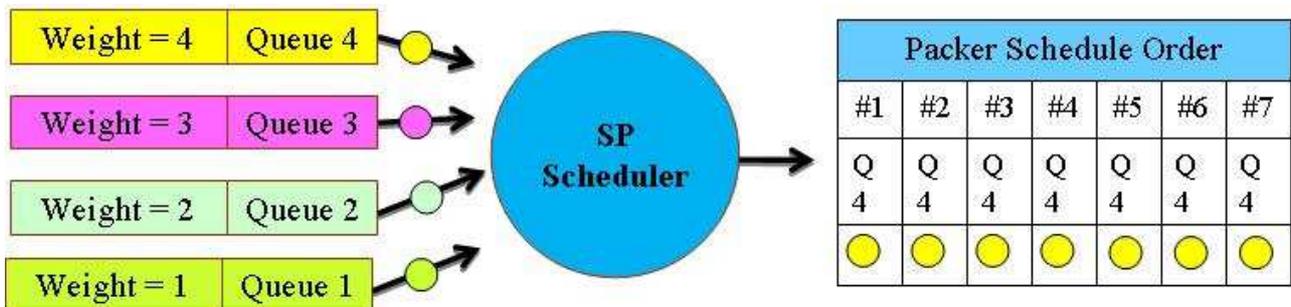
Weighted Round-Robin (WRR):

The Queue 0~5 is belong WRR



Strict Priority (SP):

The Queue 6~7 is belong SP



3.6.1 Specify QoS in GUI

GUI Path: **>Configuration>L2-SW>QoS**

Port	Port Scheduling	DWRR Queue 0	DWRR Queue 1	DWRR Queue 2	DWRR Queue 3	DWRR Queue 4	DWRR Queue 5
NNI-1	Strict Priority	17	17	17	17	17	17
NNI-2	Strict Priority	17	17	17	17	17	17
NNI-3	Strict Priority	17	17	17	17	17	17
NNI-4	Strict Priority	17	17	17	17	17	17
NNI-5	Strict Priority	17	17	17	17	17	17
NNI-6	Strict Priority	17	17	17	17	17	17
NNI-7	Strict Priority	17	17	17	17	17	17
NNI-8	Strict Priority	17	17	17	17	17	17
OLT-1	Strict Priority	17	17	17	17	17	17
OLT-2	Strict Priority	17	17	17	17	17	17
OLT-3	Strict Priority	17	17	17	17	17	17
OLT-4	Strict Priority	17	17	17	17	17	17
OLT-5	Strict Priority	17	17	17	17	17	17
OLT-6	Strict Priority	17	17	17	17	17	17
OLT-7	Strict Priority	17	17	17	17	17	17
OLT-8	Strict Priority	17	17	17	17	17	17

Note: the value of Queue Weight is between 1 to 100.

3.6.2 Specify QoS in CLI

Usage:

```
show qos
qos <nni <nniid>|olt <oltid>> [strict|dwrr]
    [qw0 <VALUE>] [qw1 <VALUE>] [qw2 <VALUE>]
    [qw3 <VALUE>] [qw4 <VALUE>] [qw5 <VALUE>]
```

NOTE:

VALUE is between 1 to 100.

3.7 Access Control List (ACL)

3.7.1 ACL Overview

Access Control List (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to the objects, as well as what operations are allowed on the given objects. Each entry in a typical ACL specifies a subject and an operation. For instance, if a file has an ACL that contains (Alice, delete), this would give Alice permission to delete the file.

3.7.2 ACL Configuration in GUI

The DPN-6608 can store the ACL with up to 99 rules in the device.

GUI Path: >Configuration/L2-SW/ACL

Rule	Type	Multicast	NNI (UpLink)								GPON OLT								NMS	Extra Options	Description
	Forward	Broadcast	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8			
	Any	Any	<input type="checkbox"/>																		
	Deny	Any																			

no configuration found

Note 1: For MASK cleared bits are wildcards.
 Note 2: For Ethernet Type, it applies for frames with Etype from 0x6000 - 0xffff but excluding 0x0800(IPv4), 0x0806(ARP) and 0x86dd(IPv6)
 Note 3: For IPv4 Type, sport/dport only work for frames which protocol is 0x06(TCP) or 0x11(UDP)

Type

- Any:** no extra option.
- Etype:** extra options – Ethernet Type and Source/Destination MAC.
- IPv4:** extra options – Protocol Type and Source/Destination IP/Port.

Forward

Deny or Permit.

Multicast

Check Destination MAC address is Multicast or not. Any, No or Yes.

Broadcast

Check Destination MAC address is Broadcast or not. Any, No or Yes.

NNI (Uplink)

Involved NNI ports.

GPON OLT

Involved GPON OLT ports.

3.7.3 ACL configuration in CLI

Usage:

```
show acl <all|idx>
acl create <idx> <any|etype|ipv4> <permit|deny>
acl config <idx> [dmac_mc <any|no|yes>] [dmac_bc <any|no|yes>]
                [nni <none|LIST>] [olt <none|LIST>]
                [nms <no|yes>] [Extra OPTIONS]
                [descr <"TEXT">]

acl remove <idx>
acl counter <all|idx>
acl clr-cnt <all|idx>
```

Extra OPTIONS

```
any : no option
etype: [etype <HEX> <MASK>]
      [dmac <MAC> <MASK>] [smac <MAC> <MASK>]
ipv4 : [proto <HEX> <MASK>]
      [sip <ADDR> <MASK>] [dip <ADDR> <MASK>]
      [sport <START> <END>] [dport <START> <END>]
```

Note:

For MASK cleared bits are wildcards.
Etype: It applies for frames with Etype from 0x6000 - 0xffff
but excluding 0x0800(IPv4)/0x0806(ARP)/0x86dd(IPv6)
IPv4 : sport/dport only work for frames which protocol is
0x06(TCP) or 0x11(UDP)

Add an new ACL rule

```
admin@192.168.1.150:> acl create 1 etype deny
```

```
Info: create successfully.
```

Specify MAC/Mask 001915b9d1e8/ffffffff to this rule

```
admin@192.168.1.150:> acl config 1 dmac 001915b9d1e8 ffffffff
```

3.8 Relay Agent Information

3.8.1 Knowledge of DHCP Option 82

Option 82 message structure:

CODE	LEN	Agent Information field					
82	N	i1	i2	i3	i4		iN

Code: represents the sequence number of the relay agent information option, the option 82 is called because RFC3046 is defined as 82.

Len: the number of bytes in Agent Information Field, not including the two bytes in Code segment and Len segment.

Option 82 can have several sub-options, and needs at least one sub-option. RFC3046 defines the following two sub-options, whose formats are showed below.

sub0bt	LEN	Sub-option value					
1	N	s1	s2	s3	s4		sN

sub0bt	LEN	Sub-option value					
2	N	i1	i2	i3	i4		iN

SubOpt: the sequence number of sub-option, the sequence number of Circuit ID sub-option is 1, the sequence number of Remote ID sub-option is 2.

Len: the number of bytes in Sub-option Value, not including the two bytes in SubOpt segment and Len segment

option82 sub-option 1: represents the agent circuit ID, namely Circuit ID. It holds the port number and VLAN-ID of the switch port connected to the DHCP client, and is usually configured on the DHCP relay agent.

option82 sub-option 2: represents the remote agent ID, namely Remote ID. It holds the MAC address of the DHCP relay agent, and is usually configured on the DHCP relay agent.

Generally, sub-option 1 and sub-option 2 must be used together to identify information about a DHCP source.

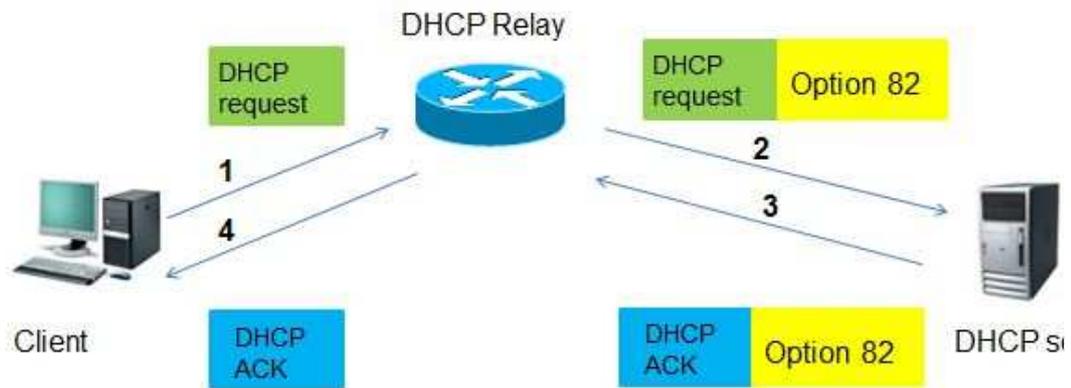


Figure 13: DHCP OPTION 82 principles

1. DHCP client sends a request in the initialization broadcast packets, but the message does not contain option 82.
2. DHCP relay agent will add option 82 at the end of relay packets to the DHCP server
3. DHCP server receives the DHCP request packet from DHCP relay. According to the message carried in the option, option is intended for information and strategies to assign IP addresses and other information to the client, and then reply with DHCP option 82 configuration information embedded in response packet to the DHCP relay agent.
4. DHCP relay agent receives the response message packet and will strip off the option 82 information, and then forward the DHCP packet to the DHCP client

3.8.2 Specify Relay Agent Information in GUI

The administrator can define the Relay Agent Information this page.

GUI Path: **> Configuration > L2-SW > Relay Agent**

DHCP Relay Agent	
Circuit ID:	Access-Node-Identifier eth 1/%l/%n/0/0:%v Preview: Access-Node-Identifier eth 1/<OLT ID>/<ONT ID>/0/0:<VLAN ID>
Remote ID:	%m Preview: 00:11:52:00:ae:11
PPPoE Agent Information	
Circuit ID:	Access-Node-Identifier eth 1/%l/%n/0/0:%v Preview: Access-Node-Identifier eth 1/<OLT ID>/<ONT ID>/0/0:<VLAN ID>
Remote ID:	%m Preview: 00:11:52:00:ae:11
Available Symbols	
	%h: OLT Device Name %m: OLT MAC Address (lower case) %M: OLT MAC Address (upper case) %p: OLT IP Address %v: VLAN ID %l: OLT ID %n: ONT ID %: Percentage Symbol

3.8.3 Specify Relay Agent Information in CLI

```

Usage:
show relay-agent
relay-agent status [clr]
relay-agent config [dhcp-circuit <"TEXT">]
                    [dhcp-remote <"TEXT">]
                    [pppoe-circuit <"TEXT">]
                    [pppoe-remote <"TEXT">]

%h: OLT Device Name
%m: OLT MAC Address (lower case)
%M: OLT MAC Address (upper case)
%p: OLT IP Address
%v: VLAN ID
%l: OLT ID
%n: ONT ID
%: Percentage Symbol
%l: OLT ID
%n: ONT ID
%: Percentage Symbol

```

3.9 ARP Proxy Table

3.9.1 Dynamic ARP Proxy in GUI

The administrator can view the MAC address learned according to DHCP packet monitoring.

GUI Path: **> Monitoring > ARP Proxy**

Start from VLAN and IP address with entries per page.

No.	VID	IP Address	MAC Address	GPON OLT								ONT ID	Flow ID	Last Change	Action
				1	2	3	4	5	6	7	8				
no address found															

3.9.2 Dynamic ARP Proxy in CLI

Usage:

```
arp-dynamic table
arp-dynamic remove <VID> <ADDR>
```

Enable the ARP Proxy in S-VLAN

```
admin@192.168.1.150:> vlan config 10 arp-proxy on
```

Info: update successfully.

Check the Dynamic ARP Proxy Table

```
admin@192.168.1.150:> arp-dynamic table
```

VID	IP Address	MAC Address	Last Change	Member
10	192.168.1.15	xx-xx-xx-xx-xx-xx	2012/06/01-10:53:45	olt=1

3.9.3 Static ARP Proxy in GUI

Broadcast traffic in downstream path is always blocked by GPON. In case of special application, like Server in ONT side, the administrator can specify the reply information (IP address/MAC address) for ARP inquire from NNI (Uplink).

GUI Path: **> Configuration > L2-SW > ARP Proxy**

Index	U-VLAN ID	IP Address	MAC Address	Description	
1	12	172.12.0.33	00-16-52-F0-AA-11	arp entry 1	  
2	100	172.12.0.34	00-16-52-F0-AA-12	arp entry 2	 

3.9.4 Static ARP Proxy in CLI

Usage:

```
show arp-static <all|idx>
arp-static create <idx> <VID> <ADDR> <MAC-ADDR>
arp-static remove <idx>
arp-static config <idx> [vlan <VID>] [addr <ADDR>]
                        [mac <MAC-ADDR>]
                        [descr <"TEXT">]
```

Assign the static ARP -proxy

```
admin@192.168.1.150:> arp-static create 1 12 172.12.0.33 00-16-52-F0-AA-11
```

Info: create successfully.

```
admin@192.168.1.150:> arp-static create 2 100 172.12.0.34 00-16-52-F0-AA-12
```

Info: create successfully.

3.10 Static MAC Spoofing Table

Static MAC Spoofing Table list a sets of VLAN/MAC Address which are allowed to forward traffic from GPON OLT port to NNI Ports. The VLAN/ MAC Address pair are valid and checked while MAC address learning if the security option of VLAN (Refer to Section 2.3) is selected as 'MAC Spoofing' or 'RADIUS'.

3.10.1 Specify Static MAC Spoofing Address in GUI

GUI Path: >Configuration>L2-SW>MAC Spoofing

Index	U-VLAN ID	MAC Address	GPON OLT								Description
			1	2	3	4	5	6	7	8	
0			<input type="checkbox"/>								
no entry found											

3.10.2 Specify Static MAC Spoofing Address in CLI

Usage:

```
show spoofing-mac <all|idx>
spoofing-mac create <idx> <VID> <MAC-ADDR>
spoofing-mac remove <idx>
spoofing-mac config <idx> [vlan <VID>] [mac <MAC-ADDR>]
                             [olt <none|LIST>]
                             [descr <"TEXT">]
```

Add a new MAC Spoofing address

```
admin@192.168.1.150:> spoofing-mac create 1 10 00-11-22-33-44-55
```

Info: create successfully.

Specify GPON OLT 1/2 to this address

```
admin@192.168.1.150:> spoofing-mac config 1 olt 1,2
```

Info: update successfully.

Inquire this address

```
admin@192.168.1.150:> show spoofing-mac 1
```

```
index-1, descr="entry 1", vlan=10, mac=00-11-22-33-44-55, olt=1,2
```

3.11 Spanning Tree Protocol (STP)

The Spanning Tree Protocol (STP) is a network protocol that ensures a loop-free topology for any bridged Ethernet local area network. The basic function of STP is to prevent bridge loops and the broadcast radiation that results from them. Spanning tree also allows a network design to include spare (redundant) links to provide automatic backup paths if an active link fails, without the danger of bridge loops, or the need for manual enabling/disabling of these backup links.

Spanning Tree Protocol (STP) is standardized as IEEE 802.1D. As the name suggests, it creates a spanning tree within a mesh network of connected layer-2 bridges (typically Ethernet switches), and disables those links that are not part of the spanning tree, leaving a single active path between any two network nodes. Each port on a switch using STP is in one of the following five states: blocking, listening, learning, forwarding, disable.

Blocking: A port in the blocking state does not participate in frame forwarding, and after initialization, a BPDU is sent to each port in the switch. A switch assumes it is the root until it exchanges BPDUs with other switches in the network. This BPDU exchange establishes which switch in the network is the root switch. If only one switch resides in the network, no exchange occurs, and after the forward delay timer expires, the ports move to the listening state.

Listening: The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.

Learning: While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.

Forwarding: A port receiving and sending data, normal operation. STP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

Disable: Not strictly part of STP, a administrator can manually disable a port. To prevent the delay when connecting hosts to a switch and during some topology changes, Rapid STP was developed and standardized by IEEE 802.1w, which allows a switch port to rapidly transition into the forwarding state during these situations.

3.11.1 Rapid Spanning Tree Protocol

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP.

While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within $3 \times$ Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds. Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard.

There are only three port states left in RSTP that correspond to the three possible operational states. The 802.1D disabled, blocking, and listening states are merged into a unique 802.1w discarding state.

The role is now a variable assigned to a given port. The root port and designated port roles remain, while the blocking port role is split into the backup and alternate port roles. The Spanning Tree Algorithm (STA) determines the role of a port based on Bridge Protocol Data Units (BPDUs). In order to simplify matters, the thing to remember about a BPDU is there is always a method to compare any two of them and decide whether one is more useful than the other. This is based on the value stored in the BPDU and occasionally on the port on which they are received. The information in this section explains practical approaches to port roles.

Root

The port that receives the best BPDU on a bridge is the root port. This is the port closest to the root bridge in terms of path cost. The STA elects a single root bridge in the whole bridged network (per-VLAN). The root bridge sends BPDUs that are more useful than the ones sent by any other bridges. The root bridge is the only bridge in the network that does not have a root port. All other bridges receive BPDUs from at least one port.

Designate

A port is designated if it can send the best BPDU on the segment to which it is connected. 802.1D bridges link together different segments, such as Ethernet segments, to create a bridged domain. On a given segment, there can only be one path toward the root bridge. If there are two, there is a bridging loop in the network. All bridges connected to a given segment listen to the BPDUs of each and agree on the bridge that sends the best BPDU as the designated bridge for the segment. The port on that bridge that corresponds is the designated port for that segment.

Alternate

An alternate port is a port that is in a blocking state and receives superior (better) BPDU frames from another switch.

Backup

A backup port is a port in the blocking state that receives superior BPDU frames from the same switch. This port provides a redundant path (but less desirable) to a segment to which another switch port already connects. (They can only exist when there are two ports connected between the switches.)

Disabled

A disabled port does not participate in the active topology.

3.11.2 STP Configuration in GUI

GUI Path: >Configuration>Spanning Tree> Bridge Settings

Basic Settings	
Protocol Version:	RSTP ▲▼
Forward Delay:	15, default is 15
Max Age:	20, default is 20
Maximum Hop Count:	20, default is 20
Transmit Hold Count:	6, default is 6
Advanced Settings	
Edge Port BPDU Filtering:	<input type="checkbox"/>
Edge Port BPDU Guard:	<input type="checkbox"/>
Port Error Recovery:	<input type="checkbox"/>
Port Error Recovery Timeout:	
Configuration Identification	
Configuration Name:	00-10-10-10-10-10
Configuration Revision:	0

Protocol Version

STP: Spanning Tree Protocol

RSTP: Rapid Spanning Tree Protocol

MSTP: Multiple Spanning Tree Protocol

GUI Path: >Configuration>Spanning Tree> CIST/MSTI Ports

Port	STP Enabled	Path Cost	Priority	Admin Edge	Auto Edge	Restricted		BPDU Guard	Point-to-Point
						Role	TCN		
Aggregated	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Forced False ▲▼
NNI-1	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-2	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-3	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-4	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-5	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-6	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-7	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼
NNI-8	<input type="checkbox"/>	Auto ▲▼	128 ▲▼	Non-Edge ▲▼	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Auto ▲▼

3.11.3 MSTP Configuration in GUI

GUI Path: >Configuration>Spanning Tree> MSTI Mapping

MSTI	Priority	VLANs Mapped
CIST:	128 ▲▼	Unmapped VLANs are mapped to the CIST. (The default bridge instance).
MSTI1:	128 ▲▼	
MSTI2:	128 ▲▼	
MSTI3:	128 ▲▼	
MSTI4:	128 ▲▼	
MSTI5:	128 ▲▼	
MSTI6:	128 ▲▼	
MSTI7:	128 ▲▼	

GUI Path: >Configuration>Spanning Tree> CIST/MSTI Ports

Port	Path Cost	Priority
Aggregated	Auto ▲▼	128 ▲▼
NNI-1	Auto ▲▼	128 ▲▼
NNI-2	Auto ▲▼	128 ▲▼
NNI-3	Auto ▲▼	128 ▲▼
NNI-4	Auto ▲▼	128 ▲▼
NNI-5	Auto ▲▼	128 ▲▼
NNI-6	Auto ▲▼	128 ▲▼
NNI-7	Auto ▲▼	128 ▲▼
NNI-8	Auto ▲▼	128 ▲▼

3.11.4 STP Status in GUI

GUI Path: > Monitoring>Spanning Tree>Bridge Status

STP Bridge Status	
Bridge Instance	CIST
Bridge ID	80:00-00:16:52:f0:12:34
Root ID	80:00-00:16:52:f0:12:34
Root Cost	0
Root Port	-
Regional Root	80:00-00:16:52:f0:12:34
Internal Root Cost	0
Topology Flag	Steady
Topology Change Count	0
Topology Change Last	Never

Ports & Aggregations State

Port	Port ID	Role	State	Path Cost	Edge	Point2Point	Uptime
No ports or aggregations active							

GUI Path: > Monitoring>Spanning Tree>Port Status

Port	CIST Role	CIST State	Uptime
NNI-1	Non-STP	Forwarding	-
NNI-2	Non-STP	Forwarding	-
NNI-3	Non-STP	Forwarding	-
NNI-4	Non-STP	Forwarding	-
NNI-5	Non-STP	Forwarding	-
NNI-6	Non-STP	Forwarding	-
NNI-7	Non-STP	Forwarding	-
NNI-8	Non-STP	Forwarding	-

GUI Path: > Monitoring>Spanning Tree>Port Statistics

Port	Transmitted				Received				Discarded	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
No ports enabled										

3.11.5 STP configuration and Status in CLI

Usage:

```
stp bridge [stp|rstp|mstp] [forward <VALUE>]
           [max-age <VALUE>] [hop-cnt <VALUE>]
           [tx-hold <VALUE>] [filter <on|off>]
           [guard <on|off>] [recover <VALUE>]
           [name <"TEXT">] [revision <VALUE>]

stp map
stp map    <cist|msti <1-7>> [priority <VALUE>]
           [vlan <none|LIST>]

stp cist
stp cist   <aggr|nni <nniid>> [stp <on|off>]
           [path-cost <auto|VALUE>]
           [priority <VALUE>]
           [admin-edge <on|off>]
           [guard <on|off>]
           [auto-edge <on|off>]
           [rst-role <on|off>]
           [rst-tcn <on|off>]
           [p2p <false|true|auto>]

stp msti   <1-7>
stp msti   <1-7> <aggr|nni <nniid>> [path-cost <auto|VALUE>]
           [priority <VALUE>]

stp status <cist|msti <1-7>>
stp port   <status|statistics>
```

3.12 Connectivity Fault Management (CFM)

DPN-6608 provides the support of IEEE 802.1ag. The administrator can assign up to 256 MEPs/MIPs with different VLAN/MD/MEPID to NNI ports. CFM feature is globally disabled in default. Refer to Section 3.2 for enabling CFM feature.

3.12.1 Specify Connectivity Fault Management in GUI

GUI Path: >Diagnosis/CFM/MEP/MIP

Index	Port	Mode	Domain	MEPID	MD Name	Peer RMEP	XCON CCM	Config Error	RMEP Error	MAC Status	RMEP RDI	+
	S-VLAN	Direction	CCM Rate	Priority	Short MA							
1	NNI-2 10	MEP Outward	Provider(3) 6 t/min	11 3	test test ma name	1	●	●	●	●	●	⊖ ⊗

GUI Path: >Diagnosis/CFM/Remote MEPs

Index	Peer MEPID	Peer MAC Address	Detect Time	CCM	Port	Interface	Last SN	RDI	Interval	Priority	+	
1	22	00-01-02-03-04-02	2014/03/11-14:33:05	OK	Up	-	1988	Yes	OK	OK	⊗	
				CCM	LBR	LBM	LTR	LTM	Dropped			
				Transmitted	1138	0	0	0	0			
				Received	1138	0	0	0	0			
				CCM			LBR			LTR		
				Cross Connect	Config Error	Out of Sequence	In-Order LBR	Out-of-Order	Unexpected			
				0	0	0	0	0	0			

MIP CCM Database

Index	Source	MEPID	MAC Address	Detect Time
1	NNI-2	22	00-01-02-03-04-02	2014/03/11-14:33:05

GUI Path: >Diagnosis/CFM/Loopback

Enable	Priority	Mode	Peer MAC Address	Size	To Send		
<input type="checkbox"/>	0	Unicast	00-01-02-03-04-02	64	4		
Send LBM(s)					Undo		
Transmitted LBM		In-Order LBR		Out-of-Order LBR		Mismatch LBR	
4		4		0		0	
Index	TransID	Reply MAC Address			Bytes	Response Time	
1	8	00-01-02-03-04-02			64	1 ms	
2	9	00-01-02-03-04-02			64	4 ms	
3	10	00-01-02-03-04-02			64	5 ms	
4	11	00-01-02-03-04-02			64	4 ms	
4 transmitted, 4 received, 0% loss							

GUI Path: >Diagnosis/CFM/Linktrace

Enable	Peer MAC Address	Time to Live	To Send
	00-01-02-03-04-02	64	3
<input type="button" value="Send LTM"/> <input type="button" value="Undo"/>			

TransID	Hop	Mode	MEPID	Direction	Forwarded	Relay	Ingress MAC	Egress MAC	Last Time
0	1	MEP	22	Outward	no	Hit	01-00-01-02-03-04	-	2014/03/11-16:27:46
1	1	MEP	22	Outward	no	Hit	01-00-01-02-03-04	-	2014/03/11-16:27:51
2	1	MEP	22	Outward	no	Hit	01-00-01-02-03-04	-	2014/03/11-16:27:56

3.12.2 Specify MEP/MIP/RMEP in CLI

Usage:

```
show cfm <all|idx>
cfm create <idx> <nniid> <VID> <mip|mep <in|out> <mepid>>
cfm remove <idx>
cfm config <idx> [nni <nniid>] [vlan <VID>]
                    [mip|mep <in|out> <mepid>]
                    [customer|provider|operator]
                    [ccm <VALUE>] [prio <VALUE>]
                    [md-name <"TEXT">] [ma-name <"TEXT">]

cfm status <idx>
cfm mip-db <idx>
```

ccm: (0)none (1)300f/s (2)100f/s (3)10f/s (4)1f/s
(5)6f/m (6)1f/m (7)1f/h

Usage:

```
show cfm-rmep <mp idx> [rmep id]
cfm-rmep create <mp idx> <rmep id>
cfm-rmep remove <mp idx> <rmep id>
```

Add a new MEP with NNI 2, VLAN 10, Outward and MEPID 11

```
admin@192.168.1.150:> cfm create 1 2 10 mep out 11
```

Info: create successfully.

Assign Maintenance Domain, CCM frame rate, priority and MD/MA name

```
admin@192.168.1.150:> cfm config 1 provider ccm 5 prio 3 md-name "test" ma-name
"test_ma_name"
```

Info: update successfully.

Inquire this MEP

```
admin@192.168.1.150:> show cfm 1
```

```
cfm mp-1, nniid=2, vlan=10, provider, mep, out, mepid=11, ccm=6f/m(5),
prio=3, md-name="test", ma-name="test_ma_name"
```

Add a new RMEP with MEPID 22 to this MEP

```
admin@192.168.1.150:> cfm-rmep create 1 22
```

```
Info: create successfully.
```

Inquire this RMEP

```
admin@192.168.1.150:> show cfm-rmep 1 22
```

```
mp-1, rmep-22:
  CCM State..... OK
  RDI..... Yes
  Interval Match..... OK
  Priority Match..... OK
  Peer MAC Address..... 00-01-02-03-04-02
  Detected Time..... 2014/03/11-16:17:35
  Port Status..... Up
  Interface Status..... -
  Last Serial Number..... 2615
```

3.12.3 Specify Loopback test in CLI

Usage:

```
show cfm-lpbk <mp idx>
cfm-lpbk send <mp idx> <mcast|ucast <MAC-ADDR>>
               <size> <count> <priority>
cfm-lpbk result <mp idx>
```

Activate loopback test

```
admin@192.168.1.150:> cfm-lpbk send 1 mcast 97 3 3
```

```
Info: action successfully.
```

Inquire the result

```
admin@192.168.1.150:> cfm-lpbk result 1
```

```
mp-1, Loopback Test Result:
  transid 0, 97 bytes from 00-01-02-03-04-02, time 1 ms
  transid 1, 97 bytes from 00-01-02-03-04-02, time 5 ms
  transid 2, 97 bytes from 00-01-02-03-04-02, time 5 ms
```

3.12.4 Specify Linktrace test CLI

Usage:

```
show cfm-trace    <mp idx>
cfm-trace send   <mp idx> <MAC-ADDR> <ttl> <count>
cfm-trace result <mp idx>
```

Activate linktrace test

```
admin@192.168.1.150:> cfm-trace send 1 00-01-02-03-04-02 64 3
```

```
Info: action successfully.
```

Inquire the result

```
admin@192.168.1.150:> cfm-trace result 1
```

```
mp-1, Linktrace Test Result:
```

```
trandid 0:
```

```
hop 1, mep, out, id 22, Hit, ingress 01-00-01-02-03-04, 2014/03/11-14:41:12
```

```
trandid 1:
```

```
hop 1, mep, out, id 22, Hit, ingress 01-00-01-02-03-04, 2014/03/11-14:41:17
```

3.13 Port Mirroring

This function is used for trouble shooting. The administrator can use it to mirror the traffic of a port to another one in order to check the transmitting and receiving status of the port. This feature is only available in CLI.

Usage:

```
debug mirror <none|nni <nniid>>  
          [nni_ingress <none|LIST>] [nni_egress <none|LIST>]  
          [olt_ingress <none|LIST>] [olt_egress <none|LIST>]
```

Mirror the Egress traffic of NNI 1 to NNI 3

```
admin@192.168.1.150:> debug mirror nni 3 nni_egress 1
```

Info: update successfully.

Chapter 4 Status Monitoring

4.1 Alarm/Event

The DPN-6608 can keep up to 10,000 Alarms/Events. If more Alarms/Events arrival, the earliest and cleaned Alarms/Events will be removed from list.

4.1.1 View Alarm/Event in GUI

GUI Path: **>Alarm/Event**

View Alarm/Event with Severity >= , from Page and

EventID	Class	Interface	Severity	Message	Description	Event Time
3	PWR	dev-1	Event	(9) PwrRe	er module is ready	2013/01/09-09:23:54
2	NNI	nni-6	Critical	(34) LinkD	face Link down	2013/01/09-09:23:54
1	SYS	-	Event	(1) DevUp	e Up	2013/01/09-09:23:54

The administrator can view the Alarm/Event list by filter.

1. Current or History
2. Severity level: Event, Minor, Major, Critical
3. Number of items in a page.
4. Event class: SYS, DEV, NNI, OLT, ONT, SVC, PWR

Click Button 'Clean' to clean outdated Alarm/Event.

4.1.2 Alarm/Event in CLI

Usage:
event <curr|hist> [clean]

Inquire current alarm/event

```
admin@192.168.1.150:> event curr

evnet-9, class=NNI, intf=nni-8, Critical, msg=(31) LinkDown
time=02/17/2012-15:52:49
descr="Interface Link down"
evnet-7, class=NNI, intf=nni-6, Critical, msg=(31) LinkDown
time=02/17/2012-15:52:49
descr="Interface Link down"
evnet-6, class=NNI, intf=nni-5, Critical, msg=(31) LinkDown
time=02/17/2012-15:52:49
descr="Interface Link down"
evnet-5, class=NNI, intf=nni-4, Critical, msg=(30) MissMod
time=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-4, class=NNI, intf=nni-3, Critical, msg=(30) MissMod
time=02/17/2012-15:52:49
descr="Missing transceiver module"
```

```
evnet-3, class=NNI, intf=nni-2, Critical, msg=(30) MissMod
time=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-2, class=NNI, intf=nni-1, Critical, msg=(30) MissMod
time=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-1, class=SYS, Event, msg=(1) SysUp
time=02/17/2012-15:52:49
descr="System up"
```

Inquire history alarm/event

```
admin@192.168.1.150:> event hist
```

```
evnet-10, class=NNI, intf=nni-7, Critical, msg=(31) LinkDown
raise=02/17/2012-15:55:04,
descr="Interface Link down"
evnet-9, class=NNI, intf=nni-8, Critical, msg=(31) LinkDown
raise=02/17/2012-15:52:49
descr="Interface Link down"
evnet-8, class=NNI, intf=nni-7, Critical, msg=(31) LinkDown
raise=02/17/2012-15:52:49,
descr="Interface Link down"
evnet-7, class=NNI, intf=nni-6, Critical, msg=(31) LinkDown
raise=02/17/2012-15:52:49
descr="Interface Link down"
evnet-6, class=NNI, intf=nni-5, Critical, msg=(31) LinkDown
raise=02/17/2012-15:52:49
descr="Interface Link down"
evnet-5, class=NNI, intf=nni-4, Critical, msg=(30) MissMod
raise=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-4, class=NNI, intf=nni-3, Critical, msg=(30) MissMod
raise=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-3, class=NNI, intf=nni-2, Critical, msg=(30) MissMod
raise=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-2, class=NNI, intf=nni-1, Critical, msg=(30) MissMod
raise=02/17/2012-15:52:49
descr="Missing transceiver module"
evnet-1, class=SYS, Event, msg=(1) SysUp
raise=02/17/2012-15:52:49
descr="System up"
```

Clean current alarm/event

```
admin@192.168.1.150:> event curr clean
```

```
Info: clean current alarm/event.
```

Clean history alarm/event

```
admin@192.168.1.150:> event hist clean
```

```
Info: clean history alarm/event.
```

4.2 Performance Data

The administrator can view performance counters of all Ethernet ports including the NNI /GPON OLT/NMS and GPON-layer related status counters.

4.2.1 Ethernet RMON in GUI

The RMON Counters show the transferred and received traffic including Receive total/Receive Size Counters/Receive Queue/Receive Error/Receive Error/Transmit Total/Transmit Size Counters/Transmit Queue/Transmit Error.

The administrator can clean counters of an individual port by clicking that particular port or clean all counters by clicking "Clean All".

GUI Path: **>Monitoring>Performance>RMON**

	NNI (UpLink)								GPON OLT								NMS	
	Clean All	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7		8
Receive Total																		
Rx Packets	0	0	0	0	0	0	0	50541	0	163	0	0	0	0	0	0	0	20707
Rx Octets	0	0	0	0	0	0	0	068853929	0	15474	0	0	0	0	0	0	0	027116962
Rx Unicast	0	0	0	0	0	0	0	0	0	148	0	0	0	0	0	0	0	930
Rx Multicast	0	0	0	0	0	0	0	50436	0	10	0	0	0	0	0	0	0	19716
Rx Broadcast	0	0	0	0	0	0	0	105	0	5	0	0	0	0	0	0	0	61
Rx Pause	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Receive Size Counters																		
Rx 64 Byte	0	0	0	0	0	0	0	24	0	0	0	0	0	0	0	0	0	667
Rx 65-127 Byte	0	0	0	0	0	0	0	218	0	159	0	0	0	0	0	0	0	131
Rx 128-255 Byte	0	0	0	0	0	0	0	143	0	2	0	0	0	0	0	0	0	59
Rx 256-511 Byte	0	0	0	0	0	0	0	43	0	1	0	0	0	0	0	0	0	27
Rx 512-1023 Byte	0	0	0	0	0	0	0	81	0	1	0	0	0	0	0	0	0	267
Rx 1024-1518 Byte	0	0	0	0	0	0	0	50032	0	0	0	0	0	0	0	0	0	19556
Rx 1519- Byte	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Receive Queue																		
Rx Q0	0	0	0	0	0	0	0	20046	0	162	0	0	0	0	0	0	0	1036
Rx Q1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Q7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Receive Error																		
Rx Drops	0	0	0	0	0	0	0	30495	0	1	0	0	0	0	0	0	0	19673
Rx CRC/Alignment	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Undersize	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Oversize	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Fragments	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Jabber	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Rx Filtered	0	0	0	0	0	0	0	30495	0	1	0	0	0	0	0	0	0	19673
Transmit Total																		
Tx Packets	0	0	0	0	0	0	0	15	0	20165	0	0	0	0	0	0	0	1399
Tx Octets	0	0	0	0	0	0	0	1993	0	27344650	0	0	0	0	0	0	0	1121465
Tx Unicast	0	0	0	0	0	0	0	1	0	145	0	0	0	0	0	0	0	1392
Tx Multicast	0	0	0	0	0	0	0	10	0	19963	0	0	0	0	0	0	0	0
Tx Broadcast	0	0	0	0	0	0	0	4	0	57	0	0	0	0	0	0	0	7
Tx Pause	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transmit Size Counters																		
Tx 64 Byte	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	514
Tx 65-127 Byte	0	0	0	0	0	0	0	12	0	253	0	0	0	0	0	0	0	87
Tx 128-255 Byte	0	0	0	0	0	0	0	1	0	51	0	0	0	0	0	0	0	28
Tx 256-511 Byte	0	0	0	0	0	0	0	1	0	21	0	0	0	0	0	0	0	12
Tx 512-1023 Byte	0	0	0	0	0	0	0	1	0	39	0	0	0	0	0	0	0	21
Tx 1024-1518 Byte	0	0	0	0	0	0	0	0	0	19800	0	0	0	0	0	0	0	737
Tx 1519- Byte	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transmit Queue																		
Tx Q0	0	0	0	0	0	0	0	15	0	20165	0	0	0	0	0	0	0	1399
Tx Q1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Q7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Transmit Error																		
Tx Drops	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Tx Late/Exc. Coll.	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

4.2.2 Ethernet RMON in CLI

Usage:

```
performance rmon <nni <nniid>|olt <oltid>|nms> [clr]
performance pon <oltid> [clr]
```

Inquire RMON of NNI 1

```
admin@192.168.1.150:> performance rmon nni 1
```

NNI 1 RMON Counters

Rx Packets	: 0	Tx Packets	: 0
Rx Octets	: 0	Tx Octets	: 0
Rx Unicast	: 0	Tx Unicast	: 0
Rx Multicast	: 0	Tx Multicast	: 0
Rx Broadcast	: 0	Tx Broadcast	: 0
Rx Pause	: 0	Tx Pause	: 0
Rx 64 Byte	: 0	Tx 64 Byte	: 0
Rx 65-127 Byte	: 0	Tx 65-127 Byte	: 0
Rx 128-255 Byte	: 0	Tx 128-255 Byte	: 0
Rx 256-511 Byte	: 0	Tx 256-511 Byte	: 0
Rx 512-1023 Byte	: 0	Tx 512-1023 Byte	: 0
Rx 1024-1518 Byte	: 0	Tx 1024-1518 Byte	: 0
Rx 1519- Byte	: 0	Tx 1519- Byte	: 0
Rx Q0	: 0	Tx Q0	: 0
Rx Q1	: 0	Tx Q1	: 0
Rx Q2	: 0	Tx Q2	: 0
Rx Q3	: 0	Tx Q3	: 0
Rx Q4	: 0	Tx Q4	: 0
Rx Q5	: 0	Tx Q5	: 0
Rx Q6	: 0	Tx Q6	: 0
Rx Q7	: 0	Tx Q7	: 0
Rx Drops	: 0	Tx Drops	: 0
Rx CRC/Alignment	: 0	Tx Late/Exc. Coll.	: 0
Rx Undersize	: 0		
Rx Oversize	: 0		
Rx Fragments	: 0		
Rx Jabber	: 0		
Rx Filtered	: 0		

Inquire RMON of GPON OLT 1

```
admin@192.168.1.150:> performance rmon olt 1
```

OLT 1 RMON Counters

Rx Packets	: 172	Tx Packets	: 20171
Rx Octets	: 16460	Tx Octets	: 27345166
Rx Unicast	: 156	Tx Unicast	: 151
Rx Multicast	: 10	Tx Multicast	: 19963
Rx Broadcast	: 6	Tx Broadcast	: 57
Rx Pause	: 0	Tx Pause	: 0
Rx 64 Byte	: 0	Tx 64 Byte	: 1
Rx 65-127 Byte	: 167	Tx 65-127 Byte	: 259
Rx 128-255 Byte	: 2	Tx 128-255 Byte	: 51

Rx 256-511 Byte	: 2	Tx 256-511 Byte	: 21
Rx 512-1023 Byte	: 1	Tx 512-1023 Byte	: 39
Rx 1024-1518 Byte	: 0	Tx 1024-1518 Byte	: 19800
Rx 1519- Byte	: 0	Tx 1519- Byte	: 0
Rx Q0	: 170	Tx Q0	: 20171
Rx Q1	: 0	Tx Q1	: 0
Rx Q2	: 0	Tx Q2	: 0
Rx Q3	: 0	Tx Q3	: 0
Rx Q4	: 0	Tx Q4	: 0
Rx Q5	: 0	Tx Q5	: 0
Rx Q6	: 0	Tx Q6	: 0
Rx Q7	: 0	Tx Q7	: 0
Rx Drops	: 2	Tx Drops	: 0
Rx CRC/Alignment	: 0	Tx Late/Exc. Coll.	: 0
Rx Undersize	: 0		
Rx Oversize	: 0		
Rx Fragments	: 0		
Rx Jabber	: 0		
Rx Filtered	: 2		

Inquire the RMON of NMS

```
admin@192.168.1.150:> performance rmon nms
```

NMS RMON Counters

Rx Packets	: 21438	Tx Packets	: 2609
Rx Octets	: 27185120	Tx Octets	: 2617705
Rx Unicast	: 1647	Tx Unicast	: 2602
Rx Multicast	: 19724	Tx Multicast	: 0
Rx Broadcast	: 67	Tx Broadcast	: 7
Rx Pause	: 0	Tx Pause	: 0
Rx 64 Byte	: 1351	Tx 64 Byte	: 549
Rx 65-127 Byte	: 138	Tx 65-127 Byte	: 225
Rx 128-255 Byte	: 67	Tx 128-255 Byte	: 50
Rx 256-511 Byte	: 27	Tx 256-511 Byte	: 15
Rx 512-1023 Byte	: 299	Tx 512-1023 Byte	: 26
Rx 1024-1518 Byte	: 19556	Tx 1024-1518 Byte	: 1744
Rx 1519- Byte	: 0	Tx 1519- Byte	: 0
Rx Q0	: 1759	Tx Q0	: 2609
Rx Q1	: 0	Tx Q1	: 0
Rx Q2	: 0	Tx Q2	: 0
Rx Q3	: 0	Tx Q3	: 0
Rx Q4	: 0	Tx Q4	: 0
Rx Q5	: 0	Tx Q5	: 0
Rx Q6	: 0	Tx Q6	: 0
Rx Q7	: 0	Tx Q7	: 0
Rx Drops	: 19679	Tx Drops	: 0
Rx CRC/Alignment	: 0	Tx Late/Exc. Coll.	: 0
Rx Undersize	: 0		
Rx Oversize	: 0		
Rx Fragments	: 0		
Rx Jabber	: 0		
Rx Filtered	: 19679		

Clean RMON of NNI 1

```
admin@192.168.1.150:> performance rmon nni 1 clr
```

Info: Switch RMON Counters are clean.

Clean RMON of GPON OLT 1

```
admin@192.168.1.150:> performance rmon olt 1 clr
```

Info: OLT 1 RMON Counters are clean.

Clean RMON of NMS

```
admin@192.168.1.150:> performance rmon nms clr
```

Info: Switch RMON Counters are clean.

4.2.3 GPON OLT Counters in GUI

The administrator can monitor the GPON upstream/downstream counters for all GPON links. The administrator can clean counters of an individual port by clicking that particular port or clean all counters by clicking “clean All”.

GUI Path: **>Monitoring>Performance>OLT**

	GPON OLT							
	1	2	3	4	5	6	7	8
<input type="button" value="Clean All"/>								
Upstream	IS	IS	IS	IS	IS	IS	IS	IS
US PON received packets	0	0	0	0	0	0	0	0
US valid ploam include idle ploams	0	0	0	0	0	0	0	0
US valid ploam excluding idle ploams	0	0	0	0	0	0	0	0
US error ploams	0	0	0	0	0	0	0	0
US dropped ploams due to fifo full	0	0	0	0	0	0	0	0
US discarded packets due to invalid length	0	0	0	0	0	0	0	0
US dropped packets due to not configure GEM port	0	0	0	0	0	0	0	0
US received CPU packets	0	0	0	0	0	0	0	0
US TM egress queue forward packets	0	0	0	0	0	0	0	0
US TM egress queue congestion dropped packets	0	0	0	0	0	0	0	0
US TM CPU forward packet	0	0	0	0	0	0	0	0
US TM dropped packets due to crc error	0	0	0	0	0	0	0	0
US TM dropped packets due to security rule	0	0	0	0	0	0	0	0
US MAC learning failuers due to fifo full	0	0	0	0	0	0	0	0
Downstream								
DS packet counter	0	0	0	0	0	0	0	0
DS CPU packet counter	0	0	0	0	0	0	0	0
DS Ploam packet	1401	1401	1401	1401	1401	1401	1401	1401
DS transmitted byte counter	0	0	0	0	0	0	0	0
DS TM RX valid packets counter	0	0	0	0	0	0	0	0
DS TM RX crc error packets counter	0	0	0	0	0	0	0	0
DS TM CPU valid counter	0	0	0	0	0	0	0	0
DS TM CPU dropped packet	0	0	0	0	0	0	0	0
DS TM MAC lookup miss counter	0	0	0	0	0	0	0	0
DS TM HM forward counter	0	0	0	0	0	0	0	0
DS TM HM dropped counter	0	0	0	0	0	0	0	0
DS TM Egress queue forward counter	0	0	0	0	0	0	0	0
DS TM Egress queue congestion dropped counter	0	0	0	0	0	0	0	0

4.2.4 GPON OLT Counters in CLI

Inquire the counters of GPON OLT 1

```
admin@192.168.1.150:> performance pon 1
```

OLT 1 Counters

```
US PON received packets           : 0
US valid ploam include idle ploams : 0
US valid ploam excluding idle ploams : 0
US error ploams                   : 0
US dropped ploams due to fifo full  : 0
US discarded packets due to invalid length : 0
US dropped packets due to not configure GEM port : 0
US received CPU packets            : 0
US TM egress queue forward packets : 0
US TM egress queue congestion dropped packets : 0
US TM CPU forward packet           : 0
US TM dropped packets due to crc error : 0
US TM dropped packets due to security rule : 0
US MAC learning failuers due to fifo full : 0

DS packet counter                  : 0
DS CPU packet counter              : 0
DS Ploam packet                    : 345
DS transmitted byte counter        : 0
DS TM RX valid packets counter     : 0
DS TM RX crc error packets counter : 0
DS TM CPU valid counter            : 0
DS TM CPU dropped packet           : 0
DS TM MAC lookup miss counter      : 0
DS TM HM forward counter           : 0
DS TM HM dropped counter           : 0
DS TM Egress queue forward counter : 0
DS TM Egress queue congestion dropped counter : 0
```

Clean the counters of GPON OLT 1

```
admin@192.168.1.150:> performance pon 1 clr
```

```
Info: OLT 1 RMON Counters are clean.
```

4.2.5 ONT Counters in GUI

The administrator can check the ONT Counters in GPON OLT.

GUI Path: **>Monitoring>Performance>ONT**

ONT ID, Serial Number, State	Registered Page, Managed Page, Service Page	
8-1, 5277234-00000101, IS	Status IS	
8-2, 5277234-00000125, OOS	ONT Index ONT-8-1	
8-3, 5277234-00035392, IS	Unreceived Bursts 0	
8-4, 5277234-00035394, IS	Positive Drift in bits 0	
8-5, 5277234-00004393, OOS	Negative Drift in bits 0	
8-6, 45475410-104A000D, IS	Corrected Bytes 0	
8-7, 5277234-00050615, OOS	Corrected Codewords 0	
8-8, 5277234-02123588, OOS	Uncorrectable Codewords 0	
8-9, 5277234-00001951, OOS	Total received Codewords 0	
8-10, 5277234-00001968, OOS	ONT Error Counters	
8-11, 5277234-00050607, OOS	Upstream Bit Error (BIP8) 0	
8-12, 47120410-23000156, OOS	Downstream Bit Error (REI) 0	
8-13, 5277234-25000001, OOS	ONT Performance Counters (Bytes)	
8-14, 47120410-71F8A000, OOS	OMCC (Alloc-0) 2256	
8-15, unassigned	SVC-1 (Alloc-256) 0	
8-16, unassigned		
8-17, unassigned		
8-18, unassigned		
8-19, unassigned		

Unreceived Bursts Number of Unreceived Bursts

Positive Drift Accumulated positive drift in bits

Negative Drift Accumulated negative drift in bits

Corrected Bytes Number of corrected bytes.

Corrected Codewords
Number of corrected codewords.

Uncorrectable Codewords:
Number of un-corrected codewords

Total received Codewords
Number of total received codewords

Upstream Bit Error (BIP8)
Number of Upstream BIP8 errors

Downstream Bit Error (REI)

Downstream Bit Error Ratio (number of BER reported by the ONU)

OMCC (Alloc-x)

The total bytes of received data in OMCC which is assigned to this ONT

SVC-x (Alloc-x)

The total bytes if received data in Alloc-ID which is assigned to this ONT.

4.2.6 ONT Counters in CLI

Usage:

```
show ont <all|oltid [all|ontid]>
ont create <oltid> <ontid> <Serial Number>
ont remove <oltid> <ontid>
ont config <oltid> <ontid> [is|oos] [sn <Serial Number>]
                               [no-pwd|pwd <Password>]
                               [img <VALUE>] [cfg <VALUE>]
                               [encrypt <on|off>]
                               [us-fec <on|off>]
                               [auto-learn <on|off>]
                               [mib-load <on|off>]
                               [locked <on|off>]
                               [descr <"TEXT">]
ont managed <oltid> <ontid>
ont managed <oltid> <ontid> <img <VALUE>|cfg <VALUE>>
ont managed <oltid> <ontid> <reboot|measure>
ont discover <all|oltid>
ont counter <oltid> <ontid>
ont statistics <oltid> <ontid>
```

Serial Number: 16 digital numbers in hex format
example 00112233aabbccdd

Inquire the counters of ONT 8-1

```
admin@192.168.1.150:> ont counters 8 1
```

ALL counters for ONT-8-1:

```
Unreceived Bursts      : 0
Positive Drift         : 0
Negative Drift         : 0
Corrected Bytes       : 0
Corrected Codewords   : 0
Uncorrctable Codewords : 0
Total received Codewords : 0
```

```
Upstream Bit Error(BIP8) : 0
Downstream Bit Error(REI): 0
```

```
OMCC   Alloc-0      : 3744
SVC-1  Alloc-256   : 34656
```

4.3 MAC Table

Frame destination detection is based upon the DMAC address contained in the frame. The switch builds up a table that maps DMAC addresses to switch ports for the knowledge of which port the frames should go to (based upon the MAC address in the frame).

The frames also contain a MAC address (SMAC address), which shows the MAC address of the equipment sending the frame. The SMAC address is used by the switch to automatically update the MAC Table with these dynamic MAC addresses. Dynamic entries are removed from the MAC table if no frames with the corresponding SMAC address have been seen after a configurable age time.

4.3.1 MAC Table of Layer-2 Switch in GUI

GUI Path: >Monitoring>MAC Table>L2-SW

VID	Source MAC Address	NNI (UpLink)								GPON OLT								NMS	Flush
		1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8		
100	00-1D-60-6B-94-22	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	
100	48-5B-39-82-5F-40	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	V	
100	FF-FF-FF-FF-FF-FF	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	v	V	
1102	00-1D-60-6B-94-22	-	-	-	-	-	-	-	v	-	-	-	-	-	-	-	-	-	
1102	01-00-5E-7F-0C-2A	v	v	v	v	-	-	v	v	v	-	-	-	-	-	-	-	-	
1102	01-00-5E-7F-FF-FA	v	v	v	v	-	-	v	v	v	-	-	-	-	-	-	-	-	
1102	48-5B-39-82-5F-40	-	-	-	-	-	-	v	-	-	-	-	-	-	-	-	-	-	
4094	00-50-56-66-01-00	-	-	-	-	-	-	-	v	-	-	-	-	-	-	-	-	-	

4.3.2 MAC Table of GPON OLT in GUI

Not only L2-SW but also GPON OLT contains the MAC address table.

GUI Path: >Monitoring>MAC Table>GPON

Index	MAC Address	VLAN ID	Gem Port ID	Flush
1	00-1D-60-6B-94-22	1102	1	

4.3.3 MAC Table in CLI

Usage:

```
mac-tab sw [clr]
```

```
mac-tab pon <oltid> [clr]
```

Inquire the MAC Table of Layer-2 Switch

```
admin@192.168.1.150:> mac-tab sw
```

VID	MAC address	Member
100	00-1D-60-6B-94-22	NMS
100	48-5B-39-82-5F-40	NMS
100	FF-FF-FF-FF-FF-FF	nni=1,2,3,4,5,6,7,8 olt=1,2,3,4,5,6,7,8 NMS
1102	00-1D-60-6B-94-22	olt=1
1102	01-00-5E-7F-0C-2A	nni=1,2,3,4,7,8 olt=1
1102	01-00-5E-7F-FF-FA	nni=1,2,3,4,7,8 olt=1
1102	48-5B-39-82-5F-40	nni=7
4094	00-50-56-66-01-00	olt=1

Clean the MAC Table of Layer-2 Switch

```
admin@192.168.1.150:> mac-tab sw clr
```

Info: Switch MAC table is flushed.

Inquire the MAC Table of GPON OLT 1

```
admin@192.168.1.150:> mac-tab pon 1
```

MAC address	VID	Gem Port ID
00-1D-60-6B-94-22	1102	1

Clean the MAC Table of GPON OLT 1

```
admin@192.168.1.150:> mac-tab pon 1 clr
```

Info: MAC table of GPON OLT 1 is flushed.

Chapter 5 System Configuration

5.1 Network Setting

5.1.1 Network Setting in GUI

The administrator can specify the network settings of device here.

GUI Path: **>System>Network Setting>Host**

NMS Port Status	 (Speed = 100M FDX)
DHCP Client	<input type="checkbox"/>
Host Address	<input type="text" value="192.168.1.159"/> , 192.168.1.150
Netmask	<input type="text" value="255.255.255.0"/> , 255.255.255.0
Gateway	<input type="text" value="192.168.1.254"/> , 192.168.1.254
VLAN ID	<input type="text" value="4011"/>
DNS Server	<input type="text" value="192.168.1.254"/> , <input type="text" value="0.0.0.0"/>
Current DNS Server	192.168.1.254 0.0.0.0
Note	It's not advised to use Management VLAN ID for service traffic at ONTs. If that's the case, two current limitations are encountered in the Management VLAN: Clients at ONT are able to access and manage OLT, and PPPoE and DHCP relay functions don't work. Other service traffic VLANs would work normal.

DHCP Client Enable/disable DHCP client to obtain IP address from DHCP server.

VLAN ID The VLAN ID for in-band management.

5.1.2 Network Setting in CLI

Usage:

```
show host
host [dhcp <on|off>] [vlan <VID>] [ip <ADDR>] [mask <ADDR>]
    [gate <ADDR>] [dns-1 <ADDR>] [dns-2 <ADDR>]
```

Note: It's not advised to use Management VLAN ID for service traffic at ONTs. If that's the case, two current limitations are encountered in the Management VLAN: Clients at ONT are able to access and manage OLT, and PPPoE and DHCP relay functions don't work. Other service traffic VLANs would work normal.

5.2 SNMP Settings

5.2.1 SNMP Overview

The Simple Network Management Protocol (SNMP) is by far the dominant protocol in network management. This Protocol (SNMP) was designed to be an easily implementable, basic network management tool that could be used to meet network management needs.

It is named Simple Network Management Protocol as it is really easy to understand. A key reason for its widespread acceptance, besides being the chief Internet standard for network management, is its relative simplicity. There are different versions of SNMP, such as SNMP V1, SNMP V2c, and SNMP V3.

Implementing SNMP management in a networked device is far more straightforward than most other standard or non-standard approaches to network management. Despite that, SNMP application development has not been as simple as one would like it to be. It has required significant effort to develop management applications to manage a variety of networked devices to be managed. This situation is now changing for the better, as more SNMP tools become available. With improved tools, SNMP is poised to deliver end-to-end management for all areas of the growing inter-networking industry.

Thus SNMP has become the dominant standardized network management scheme in use today. The SNMP set of standards provides a framework for the definition of management information along with a protocol for the exchange of that information. The SNMP model assumes the existence of Managers and Agents.

5.2.2 SNMP v1/v2c Configuration in GUI

GUI Path: **>System>Network Setting>SNMP**

SNMP v1/v2c Settings

Save Undo

Agent UDP Port	Get Community	Set Community
161 <small>take effect after reboot</small>	public	private

SNMP v1/v2c Trap Settings

	Address	Protocol	Community
Trap 1	192.168.1.97	SNMP v1 Trap	public
Trap 2	0.0.0.0	SNMP v1 Trap	
Trap 3	0.0.0.0	SNMP v1 Trap	

Agent UDP Port: Specify the UDP port used for SNMP Agent

Get Community: The community string for the read operation of SNMP agent

Set Community: The community string for the write operation of SNMP agent

Trap Address: The remote address for SNMP agent sending a trap to.

Trap Protocol: The type of trap. Trap v1 Trap v2c or Inform v2c.

Trap Community: The community string for the trap sending of SNMP agent

5.2.3 SNMP v3 Configuration in GUI

GUI Path: >System>Network Setting>SNMP

	USM Name	Permission	Security Level	
1	<input type="text"/>	read-only ▾	noAuthNoPriv ▾	Auth MD5 ▾ <input type="text"/>
				Privacy DES ▾ <input type="text"/>
				Trap Trap ▾ 0.0.0.0 <input type="text"/>
2	<input type="text"/>	read-only ▾	noAuthNoPriv ▾	Auth MD5 ▾ <input type="text"/>
				Privacy DES ▾ <input type="text"/>
				Trap Trap ▾ 0.0.0.0 <input type="text"/>
3	<input type="text"/>	read-only ▾	noAuthNoPriv ▾	Auth MD5 ▾ <input type="text"/>
				Privacy DES ▾ <input type="text"/>
				Trap Trap ▾ 0.0.0.0 <input type="text"/>

USM Name: Account name for SNMP v3

Permission: Permission for USM name is only-read or read-write

Security Level: Security Level. NoAuthNoPriv / AuthNoPriv / AuthPriv

Auth: Authentication algorithm. Password is encrypted by MD5 or SHA. At least 8 characters.

Privacy: Privacy algorithm. Password is encrypted by DES or AES. At least 8 characters.

Trap: Trap or Inform in SNMP v3

Remote Address: The remote address for SNMP agent sending a trap to.

5.2.4 SNMP Configuration in CLI

Usage:

```
show snmp
snmp [udp <VALUE>] [getcomm <"TEXT">] [setcomm <"TEXT">]
snmp trap <id> [addr <ADDR>] [v1-trap|v2c-trap|v2c-info]
      [community <"TEXT">]
snmp usm <id> <ro|rw> <USER> none [<trap|info> <ADDR>]
snmp usm <id> <ro|rw> <USER> auth <md5|sha> <"VALUE">
      [<trap|info> <ADDR>]
snmp usm <id> <ro|rw> <USER> priv <md5|sha> <"VALUE">
      <des|aes> <"VALUE">
      [<trap|info> <ADDR>]

snmp usm <id> delete
```

5.3 Device Clock

5.3.1 Set Device Clock in GUI

GUI Path: >System>System Clock

System Clock

RTC Date/Time	2011/8/17 02:20:32 
NTP Server	<input type="text" value="192.168.1.254"/> <input type="button" value="UTC"/> <input type="button" value="NTP"/>

NTP Server Remote NTP Server IP address

UTC Time offset from UTC

NTP Button Click button to update device time by remote NTP server

5.3.2 Set Device Clock in CLI

Usage:

```
show time  
time <yyy/mm/dd> [HH:MM:SS]
```

Usage:

```
ntp <time offset> <addr>
```

```
ex: ntp +8 192.168.1.254
```

Time offset Time offset from UTC

addr Remote NTP Server IP address

5.4 Alarm Cut Off

ACO is used to turn off the audible of the office alarm and stop the audio warning. The system will activate the relay contact closures of the office alarm when there are alarms detected by system. It can inform the people on duty by enable the visible LED on the alarm panel. The manager can push this button to deactivate it. The ACO LED will light on at the same time to indicate this cut off action and last until the alarm status is cleared. If there is new alarm occurs again before existing one is cleared, the ACO LED will automatically be turned off and audio warning will be sent out.

GUI Path: >System>Alarm Cut off

Setting	Disabled ▼
---------	------------

Enable: enable the ACO function

Disable: disable the ACO function

Cut Off: enable ACO function and cut off alarm immediately

Alarm Cut Off in CLI

```
Usage:
show aco
aco <on|off|cut>
```

```
admin@192.168.1.150:> aco off
```

```
Info: update alarm cut off successfully.
```

5.5 Device Description

Default device description is “DPN-6608”. The Administrator may the description at any time.

5.5.1 Device Description in GUI

GUI Path: >System>Device Description



The screenshot shows a web-based interface for configuring a device description. At the top, the title "Device Description" is displayed in a blue font, followed by "Save" and "Undo" buttons. Below this, there is a label "Description" in a grey box, and a text input field containing the text "DPN-6608".

5.5.2 Device Description in CLI

```
Usage:  
show device  
device <"TEXT">
```

5.6 Reboot

There are 4 reboot modes:

1. **Normal:** Normal mode works as power cycling.
2. **Default:** Remove interface configuration files and then reboot device.
3. **Factory:** Remove all configuration files(includes Network/Account/SNMP) and then reboot device.
4. **Forcely:** In case of system damaged seriously, this mode can force device reboot immediately. The configuration may be lost !! Use it only when you know what you are doing !

5.6.1 Reboot in GUI

GUI Path: >System>Admin>Reboot

Reboot Mode	
<input type="radio"/>	Normal : reboot device normally.
<input type="radio"/>	Default: reboot device and reset to Default settings.
<input type="radio"/>	Factory: reboot device and reset to Factory settings.
<input type="radio"/>	Forcely: force to reboot device. Configuration may be lost !!

5.6.2 Reboot in CLI

Usage:

```
reboot <normal|default|factory|force>
```

normal : reboot device normally

default: reboot device and reset to Default settings

factory: reboot device and reset to Factory settings

force : force to reboot device. Configuration may be lost !!

5.7 Upgrade Device

There are several ways to upgrade device: FTP, TFTP, HTTP, Local Disk.

Note: DO NOT turn off device power during upgrade.

5.7.1 Upgrade through Local Disk in GUI

GUI Path: >System>Admin>Upgrade

Upload Upgrade Image	
Local Disk ▾	C:\Users\stev\Desktop\test 瀏覽... Upgrade

Select Local Disk

Select file through file explorer and then click 'Upgrade' button

5.7.2 Upgrade in GUI

GUI Path: >System>Admin>Upgrade

Version Information	
Current	1.00.00 11/14/2013 16:52
Upload Upgrade Image	
TFTP ▾	Server: 192.168.1.69 Upgrade Filename: x_v1.24.04.tar.gz
Software Image Restore	
Backup	1.00.00 11/14/2013 16:44 Restore
Factory	1.00.00 10/16/2013 19:58 Factory

Select TFTP for example. Upgrade by FTP/HTTP are similar.

Assign Server address and filename

Click "Upgrade" button to start upgrade.

The upgrading status would be shown in the "Status" field. After upgrade is finished, "Status" will show "Succeed". The administrator can reboot the device normally or with default settings.

Version Information	
Current	1.00.00 11/14/2013 11:46
Status	Succeed (Reboot, Reboot with default settings)
Upload Upgrade Image	
Local Disk ▾	瀏覽...

5.7.3 Upgrade in CLI

Usage:

```
show upgrade
upgrade file <ftp|tftp|http> <PARAM>
upgrade start
upgrade factory
upgrade restore
```

PARAM example:

```
ftp: [user[:password]@]server_address/file_path/file_name
tftp: server_address:file_name
http: server_address/file_path/file_name
```

Example:

```
TFTP server address: 192.168.1.69
file name: x_v1.24.04.tar.gz
```

```
admin@192.168.1.150:> upgrade start tftp 192.168.1.69:x_v1.24.04.tar.gz
```

```
Info: update successfully.
```

```
Info: system upgrade thread is being processed.
```

```
Info: please wait a moment.....
```

When upgrade is starting, you may use “***show upgrade***” command to check the upgrading status.

5.8 Backup/Restore the Configuration

The Administrator can backup the whole configuration file by backup command, and restore the configuration by restore command.

5.8.1 Backup Configuration in GUI

GUI Path: >System>Admin> Backup

Download Configuration File		
<input checked="" type="radio"/> Saved Configuration		
<input type="radio"/> Current Configuration		
<input type="checkbox"/> Include Account/Network/SNMP settings		
TFTP	Server: 192.168.1.254	Download
	Filename:	

File Transfer Mode may be 'FTP', TFTP' or 'Local Disk'.

The backup configuration files doesn't include Account / Network / SNMP settings. The administrator can request to include them by checking the option 'Include Account/Network/SNMP settings'.

5.8.2 Restore Configuration in GUI

GUI Path: >System>Admin> Restore

Upload Configuration File		
FTP	Server:	Upload
	Username:	
	Password:	
	Filename:	

File Transfer Mode may be 'FTP', TFTP', 'HTTP' or 'Local Disk'.

Note: Restore Configuration will cause device reboot !

5.8.3 Backup/Restore Configuration in CLI

Usage:

```
show config
config file <ftp|tftp|http> <PARAM>
config backup <saved|curr> [whole]
config restore
```

PARAM example:

```
ftp: [user[:password]@]server_address/file_path/file_name
```

```
tftp: server_address:file_name
```

```
http: server_address/file_path/file_name
```

Note: config backup doesn't support HTTP mode

Warning: device will reboot immediately after config restore

5.9 Account Management

There are 3 available roles in DPN-6608:

admin
user
guest

admin has full permission to control/read/write all settings in device.
user can do all things as admin role, except account management.
guest can only view setting/performance/information in device.

5.9.1 Create new Account in GUI

GUI Path: **>System>Admin>Account**

Index	Username	Group	Password	
	user	user	user	
	admin	admin		
				

Username > "user"
Select Group > user
Password > "user"

click "Save" to create new account.

5.9.2 Create new Account in CLI

Usage:

```
show account
account create <username> <group> <nopwd|pwd <Password>>
account remove <username>
account config <username> <group> <nopwd|pwd <Password>>
```

Group: admin user guest

Create new account in CLI

```
admin@192.168.150:> account create "new_user_name" user pwd "new_passwd"
```

Info: operation successfully.

5.9.3 Change Password in GUI

The User is allowed to change the login password by himself.

GUI Path: **>System>Admin>Account**

Path: > System > Admin > Account

Change Login Password		<input type="button" value="Reset Password"/>	<input type="button" value="Change Password"/>
New Password	<input type="text"/>		
Confirm Password	<input type="text"/>		

5.9.4 Change Password in CLI

Usage:

```
passwd reset  
passwd <new_pwd> <new_pwd>
```

Ex: change password to 123

```
admin@192.168.1.150:> passwd 123 123
```

Info: operation successfully.

5.10 License Control

DPN-6608 import a license system to control which vendor of ONT are allowed to service. Without a license file, the device can only manage up to **64** activated ONTs.

5.10.1 License Control through Local Disk in GUI

GUI Path: **>System>Admin>License**

New License File		
Local Disk ▾	<input type="text"/>	瀏覽...
Uploading new license file will overwrite original license.		Upload

Select Local Disk

Select file through file explorer and then click 'Upload' button

5.10.2 License Control in GUI

GUI Path: **>System>Admin>License**

Index	Vendor ID	Start of Serial Number	End of Serial Number
Trial License. Only 64 ONTs allowed. There are 2 activated ONT.			
New License File			
HTTP ▾	<input type="text"/>		Upload
http example: server_address/file_path/file_name			
Uploading new license file will overwrite original license.			

File Transfer Mode may be 'TFTP', 'FTP' or 'HTTP'.

Select File Transfer Mode

Assign Server address and filename

e.g. [192.168.1.66: license_for_ont_20120608.dat](#)

Click 'Upload' to load new license

5.10.3 License Control in CLI

Usage:

```
show license
license remove license
license <ftp|tftp|http> <PARAM>
```

PARAM example:

```
ftp: [user[:password]@]server_address:/file_path/file_name
tftp: server_address:file_name
http: server_address/file_path/file_name
```

Example:

```
admin@192.168.1.150:> license tftp 192.168.1.66:license_for_ont_20120608.dat
```

```
Info: prepare to retrieve license file ...
```

5.11 Log File

The log file is for trouble shooting in case of abnormal device behavior detected. The administrator can turn on more options here in order to get more detail messages for problem tracing.

GUI Path: **>System>Admin>Logs**

Download Log File	
Local Disk 	Download Log File through Browser. 
Log Configuration	
<input checked="" type="checkbox"/>	enable GPON Process Log Messages
<input checked="" type="checkbox"/>	enable Task Process Log Messages
<input type="checkbox"/>	enable ONT Discover Log Messages
<input checked="" type="checkbox"/>	enable Internal Event Log Messages
<input checked="" type="checkbox"/>	enable Layer-2 Switch Log Messages
<input type="checkbox"/>	enable Packet Process Log Messages
<input type="checkbox"/>	enable IGMP Frame Log Messages
<input type="checkbox"/>	enable IPTV Frame Log Messages
<input type="checkbox"/>	enable DHCP Relay Agent Log Messages
<input type="checkbox"/>	enable PPPoE Intermediate Agent Log Messages
<input type="checkbox"/>	enable Radius & 802.1x Security Log Messages
<input type="checkbox"/>	enable Link Aggregation Log Messages
<input type="checkbox"/>	enable Spanning Tree Protocol Log Messages
<input type="checkbox"/>	enable ARP Proxy Log Messages
<input type="checkbox"/>	enable MAC Learning Log Messages
<input type="checkbox"/>	enable Data Rate Control Log Messages
<input type="checkbox"/>	enable User Command Log Messages
 	

Log File in CLI

Usage:

```
show logfile
logfile <on|off> [all] [pon] [msg] [disc] [event] [vtss]
                [pkt] [igmp] [iptv] [dhcp] [pppoe] [auth]
                [aggr] [mstp] [arp] [mac] [rate] [cmd]
logfile <ftp|tftp> <PARAM>
```

PARAM example:

```
ftp: [user[:password]@]server_address/file_path/file_name
tftp: server_address:file_name
```

Chapter 6 Application Examples

In order to explain how to set up the end-to-end triple play services in DPN-6608, let's consider the service model below as an example in the following sections. In this network plan, all ONTs are connected in physical OLT port #1. NNI port #1 connects to Internet cloud for its service
NNI port #2 connects to IPTV server for IPTV service
NNI port #3 connects to SIP server for VOIP service
S-VLAN=1103 for VOIP SIP service through ONT POTS
S-VLAN=1101 for HSI data service for Ethernet UNI #1 of each ONT.
S-VLAN=1102 for IPTV video service for Ethernet UNI #2 of each ONT.

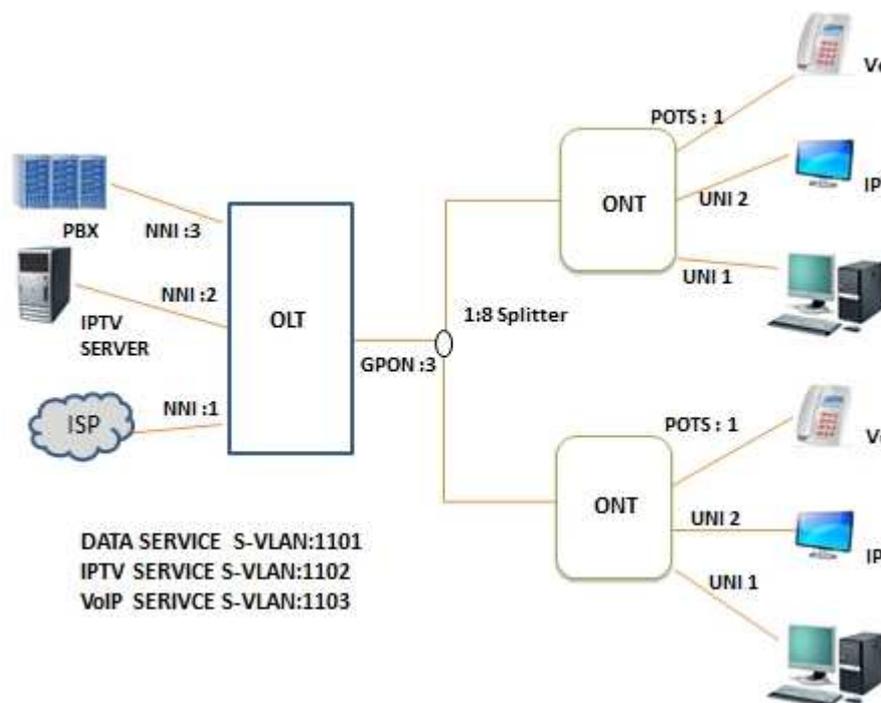


Figure 14: Triple-Play Test Environment

6.1 Provision Data Service

6.1.1 Provision Data Service in GUI

The administrator should follow the 6 steps illustrated below to create Data service:

1. Create Bandwidth profile

Upstream bandwidth profiles will be created according to the price plans telecom service operators provided to subscribers.

GUI Path: >GPON>Profiles>Bandwidth

Index	Fix	Assure	Max	DBA	Method	Description	Services	
1	0 kbps	0 kbps	512 kbps	Type-4	NSR-DBA	default	0	 
2	10,000 kbps	10,000 kbps	20,000 kbps	Type-5	NSR-DBA	dba profile 2	0	 

Note: any change only takes effect after corresponding ONT service reactivated
 Note: Downstream Rate Limit only uses Fix/Max Rates

For example, we can create an upstream bandwidth profile as Index 2
 Fix=10,000Kbps , Assure=10,000Kbps ,Max=20,000Kbps

2. Specify S-VLAN

According to this example, we should define S-VLAN=1101 as Data service in:

GUI Path: >GPON>S-VLAN

S-VLAN	VLAN Type	DHCP	PPPoE	ARP	NNI (UpLink)								GPON OLT								Description	Services	
	NNI Tagging	Security	IGMP	Proxy	1	2	3	4	5	6	7	8	1	2	3	4	5	6	7	8			
10	N:1 - Residential Single	-	-	ARP	V	V	-	-	-	-	-	-	V	-	-	-	-	-	-	-	vid 10	0	 
1101	N:1 - Residential Single	-	-	-	V	-	-	-	-	-	-	-	V	-	-	-	-	-	-	-	vid 1101	0	 

- Select N: 1 Residential and select only "Single Tagged" in NNI Tagging,
- SVLAN: 1101
- VLAN Type: N: 1 Residential
- NNI Tagging: Single Tagged
- NNI (Uplink): 1
- GPON OLT: 1

3. create Data service

The administrator should cross connect particular ONTs with “data” S-VLAN using the pre-defined bandwidth profile to allocate right GPON bandwidth to achieve pre-arranged QoS.

The above settings can be found in:

GUI Path: **>GPON>Service-Profiles>Data**

Index	S-VLAN	DS Encryption	Bridge Mode	Upstream BW	Downstream BW	Description	Services	
1	10. vid 10	no	no	2. dba profile 2	0. not used	data 1	0	 
2	1101. vid 1101	no	no	2. dba profile 2	0. not used	data 2	0	 

Note: any change only takes effect after corresponding ONT service reactivated

S-VLAN: 1101.data

Upstream BW: 2. 20M

Bridge mode: For some ONTs, you also need to enable the Bridge mode there, for other ONTs once Bridge mode is set here, the setting is done, and nothing else is needed.

4. create Ethernet UNI service .

Several UNIs of Ethernet in an ONT may share the same VLAN, and multiple VLANs can be assigned to a single ONT. The administrator should do some settings for UNI traffic and add p-bit here based on the particular service model.

GUI Path: **>GPON>Services>UNI-ETH**

Index	UNI	VLAN	P-Bits	UNI Mode	IP Host	IPcam	Description	Services	
1	1	10	0	Untagged	no	no	eth 1	0	 
2	2	1101	0	Untagged	no	no	eth 2	0	 

Note: any change only takes effect after corresponding ONT service reactivated

P-Bits: This is the value used for priority bit in the VLAN tag upstream information. All traffic from this port should be assigned the same priority bit.

IPHost: OLT managed the ONT if this option enabled

5. Configure NNI

After finishing all the settings for ONT UNI / S-VLAN / Profile, the administrator still has to configure speed for uplink ports. The default setting is disable

GUI Path: **>Configuration>NNI>Up-Link**

Port	Flow Control	Configured Speed	Egress Tag	Port VLAN ID	Current Speed
1	no	AutoNeg	Tagged	1	Down
2	no	Disabled	Tagged	1	Down
3	no	AutoNeg	Tagged	1	Down
4	no	Disabled	Tagged	1	Down
5	no	Disabled	Tagged	1	Down
6	no	Disabled	Tagged	1	Down
7	no	AutoNeg	Tagged	1	100Mfdx

Port: 1 >AutoNeg

6. Assign ONT Service

GUI Path: **>GPON>ONT>Service-Binding**

ONT Service in OLT-1 1 2 3 4 5 6 7 8 Auto-Refresh

ONT ID, Serial Number, State Register

Index	Service Profile	Description	GEM Port ID	Alloc ID
1	Data-2.	ont-1-1 svc-1	---	---
2	ETH-2.	ont-1-1 svc-2	---	---

1. Select the OLT: 1
2. Select the ONT ID: 1-1
3. Assign the service profile
 - index 1: Data-2 , data 2
 - index 4: ETH-2 , 2

6.1.2 Provision Data Service in CLI

1. Create Bandwidth profiles

Add a bandwidth profile 2

```
admin@192.168.1.150:> bw_dba create 2
```

```
Info: create successfully.
```

Edit a bandwidth profile Fix=10M , Assure=10M , Max=20M.

```
admin@192.168.1.150:> bw_dba config 2 fix 10000 assure 10000 max 20000 nsr
```

```
Info: create successfully.
```

2. Specify Service VLAN

Add a VLAN with Single Tagged mode.

```
admin@192.168.1.150:> vlan create 100 10 single
```

```
Info: create successfully.
```

Bind VLAN in OLT NNI port 1 with OLT GPON port 1 and description.

```
admin@192.168.1.150:> vlan config 100 nni 1 olt 1 descr data
```

```
Info: update successfully.
```

Inquire the status of VLAN.

```
admin@192.168.1.150:> show vlan 100
```

```
uvid-100, svid-10, descr="data", single, dhcp=none, pppoe-relay=off,  
igmp=off, secure=none, arp-proxy=off, with-bc=off, nni=1, olt=1
```

3. Create Data service

create a data service with VLAN

```
admin@192.168.1.150:> svc-data create 2 100
```

Info: create successfully.

configure the Data service.

```
admin@192.168.1.150:> svc-data config 2 vlan 100 ubw 2 descr "data"
```

Info: update successfully.

Info: any change only takes effect after corresponding ONT service reactivated.

Inquire the Data Service configuration.

```
admin@192.168.1.150:> show svc-data 2
```

```
data-2, descr="data", vlan=100, encrypt=off, bridge=off, ubw=2, dbw=0
```

4. Configure UNI port of Ethernet service for ONT

create a Ethernet service for UNI 1.

```
admin@192.168.1.150:> svc-eth create 2 2 100
```

Info: create successfully.

configure this Ethernet UNI service

```
admin@192.168.1.150:> svc-eth config 2 uniid 2 vid 100
```

Info: update successfully.

Inquire the status of UNI.

```
admin@192.168.1.150:> show svc-eth 2
```

```
uni-eth-2, descr="eth 2", uniid=2, vlan=100, pbits=0, untagged, iphost=off,  
ipcam=off
```

5. Configure NNI

Specify a NNI port for this data service S-VLAN.

```
admin@192.168.1.150:> nni config 1 tagged speed auto
```

```
Info: update successfully.
```

6. Specify services to ONT

Assign Data service to ONT 1-1

```
admin@192.168.1.150:> ont-svc create 1 1 1 data 2 is
```

```
Info: create successfully.
```

Assign Ethernet UNI service to ONT 1-1

```
admin@192.168.1.150:> ont-svc create 1 1 2 eth 2 is
```

```
Info: create successfully.
```

6.2 Cascaded OLTs

In order to expand the capacity of GPON Links, it is allowed to cascade several OLT devices into a single-IP-management system with high density of OTL links supported.

To realize this feature, some configurations must be assigned in advance.

1. Cascade Option

All OLT devices must enable the option 'Cascade' in order to support this feature. Only 10G ports can support cascade feature.

2. Management VLAN

All OLT devices must have the same Management VLAN assigned. The Management VLAN should include the NNI ports(10G ports) which is connected to other OLT device.

3. Traffic Redirection

The data traffic of OLT devices in cascaded chain must be redirected to the first OLT device which is connected to management network for single-IP-management.

After configuration is done and OLT device detected cascaded OLT devices automatically, the administrator can access those OLT devices in cascaded chain by selecting device in management list in GUI.

APPENDIX A. Abbreviations

Abbreviation	Description
ACL	Access Control List
ACO	Alarm Cut Off
AES	Advanced Encryption Standard
ARP	Address Resolution Protocol
CLI	Command Line Interface
DBA	Dynamic Bandwidth Allocation
DG	Dying-Gasp
DHCP	Dynamic Host Configuration Protocol
DS	Downstream path
FEC	Forward Error Correction
GUI	Graphical User Interface
IGMP	Internet Group Management Protocol
IPTV	Internet Protocol Television
IS / is	In Service
LACP	Link Aggregation Control Protocol
NNI	Network-to-Network Interface
NSR	Non-Status Reporting
OLT	Optical Line Terminal
ONT	Optical Network Terminal
OOS / oos	Out Of Service
OOS-MA	Out-of-Service and Management
POTS	Plain Old Telephone Service
PPPoE	Point-to-Point over Ethernet
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
SFP	Small Form-factor Pluggable
SNMP	Simple Network Management Protocol
SR	Status Reporting
STP	Spanning Tree Protocol
US	Upstream path
VoIP	Voice over Internet Protocol
dbw	Downstream Bandwidth
descr	Description
ds-fec	Downstream Forward Error Correction
nniid	NNI Port number
oltid	OLT ID number

ontid	ONT ID number
res	N:1 Residential
s-vid / s-vlan	Service VLAN ID
sn-period	Serial Number Scan Period
sn-scan	Serial Number Scan
svcid	Service ID number
ubw	Upstream Bandwidth
uniid	ETH UNI number
us-fec	Upstream Forward Error Correction
xcon	N:1 - Cross-Connect
xcvr	Transceiver

APPENDIX B. Maximum Numbers of Resources

The following table shows the maximum numbers/valid ranges of available resources in device.

Resource Name	Maximum
ONT per OLT	128
Service Slot per ONT	64
ETH UNI per ONT	16
POTS Data per ONT	4
Authentication Data per ONT	8
MAC Learn per OLT	4096
Resource Name	Valid Range
Service VLAN	2 - 4095
Data Service Profile	1 - 4095
IPTV Service Profile	1 - 4095
VoIP Service Profile	1 - 4095
ETH UNI Service Profile	1 - 4095
CATV Service Profile	1 - 4095
Misc Service Profile	1 - 4095
Auto-Provision Profile	1 - 255
Bandwidth Profile	1 - 255
ONT Image Profile	1 - 63
ONT Config Profile	1 - 255
SIP Server Profile	1 - 255
Server List for Proxy Agent	1 - 255
Static ARP Proxy Table	1 - 1023
Port Based VLAN Rule	1 - 15
ACL Rule	1 - 99

APPENDIX C. Supported Transceivers

XCVR Type	Part Number	Comments
(0)HISENSE	Hisense-Ligent LTB3677 LTB3678 LTB3678M LTB3678P	Tested (no squelch), uses 144 bits for preamble in data mode, and 1024 bits for ranging preamble Uses TRX-energy detection. Guard time = 48bit minimum.
(4)HISENSE_A	Hisense-Ligent LTB3677 LTB3678 LTB3678M LTB3678P	8 bytes guard time, 13 bytes preamble in data, 108 bytes in Ranging, target for 1.1Gbps upstream capability . TRX Based energy detection.
(5)HISENSE_B	Hisense-Ligent LTB3677 LTB3678 LTB3678M LTB3678P	US-FEC optimized, 8bytes guard time, 19 bytes preamble in Data, 107 bytes preamble in Ranging, 1.1 Gbps upstream capable. TRX-Based energy detection.
(6)SOURCE	Source SPS4348HHPCDESD	
	Luminent SPS-4348HP	US-FEC Optimized, 8 bytes guard, 16 bytes preamble in data, 24 bytes preamble in Ranging, delayed /Trx-RESET, 1.1 Gbps upstream capabilities. BCDR-Based energy detection.
(12)HISENSE_C	Hisense-Ligent LTE3680M LTE3680P	8 bytes guard time, 11 bytes preamble in data BCDR-Based energy detection
(21)DELTA	Delta OPGP-43-B3B1RS	

APPENDIX D. CLI Command Help

OLT Command

command	description
show olt <all oltid>	Show OLT configuration and status
olt config <oltid>	Edit this OLT configuration
is oos	Enable/disable this OLT
xcvr <VALUE>	Select Transceiver Type
pwd-auth <none verify auto>	Select ONT Password Authentication mode None / Verify / Auto-Provision
aes-mode <off normal enhanced>	Select the AES mode Off / Normal / Enhanced
aes-period <VALUE>	The interval of AES Key Exchange
ds-fec <on off>	Enable/disable Downstream Forward Error Correction
partner <none oltid>	Select the partner for Redundant
sn-scan <on off>	Enable/disable auto ONT S/N discover
sn-period <VALUE>	The period of auto ONT S/N discover
descr <"TEXT">	Description
olt resource	Show resource utilization of OLT
olt sfp <oltid>	Show SFP module information of OLT
<temp volt bias txp rxp> <alarm warning> <high low> <SEVERITY>	Specify the threshold crossing indicators for parameters in SFP module.

ONT Command

command	description
show ont <all oltid [all ontid]>	Show ONT configuration and status
ont create <oltid> <ontid> <Serial Number>	Add new ONT into OLT by S/N
ont remove <oltid> <ontid>	Remove ONT from OLT
ont config <oltid> <ontid>	Edit ONT configuration
is oos	Enable/Disable this ONT
sn <Serial Number>	Edit ONT S/N
no-pwd	ONT with empty password
pwd <Password>	Assign ONT password
img <VALUE>	ONT Image profile association
cfg <VALUE>	ONT Config profile association
encrypt <on off>	Enable/disable OMCI encryption
us-fec <on off>	Upstream Forward Error Correction
auto-learn <on off>	Learn password from ONT automatically
mib-load <on off>	Enable/disable ONT MIB Upload
locked <on off>	Store this ONT into flash memory or not
descr <"TEXT">	Description
ont managed <oltid> <ontid>	Display the detail information of ONT

img <VALUE>	Upgrade ONT firmware by manual
cfg <VALUE>	Update ONT configuration by manual
reboot	reboot ONT by manual
measure	Get ONT DDM information.
ont discover <all oltid>	Show discovered ONTs
ont counter <oltid> <ontid>	Performance counters of ONT
ont statistics <oltid> <ontid>	Optical statistics of ONT

ONT Service Command

command	description
show ont-svc <all oltid [all ontid [all svcid]]>	Show ONT service configuration
ont-svc create <oltid> <ontid> <svcid> <stype> <index> <is oos>	Assign new service to ONT
ont-svc remove <oltid> <ontid> <svcid>	Remove the ONT service assignment
ont-svc config <oltid> <ontid> <svcid>	Edit ONT service assignment
is oos	Enable/Disable this service
svc <none <stype> <index>>	Assign service to ONT or remove it stype: data iptv voip eth catv misc
gem <VALUE>	Assign gem port id manually
cvid <VID>	Assign Customer VLAN ID
descr <"TEXT">	Description

ONT-batch Command

command	description
show ont-batch	Show the ont-batch command
ont-batch create <oltid> <ontid-a> <ontid-b> <svcid> <is oos> <stype> <idx> <cvid>	Assign or overwrite the service assignment in multiple ONTs
descr <"TEXT">	Description
ont-batch remove <oltid> <ontid-a> <ontid-b> <svcid>	Remove the service assignment in multiple ONTs
ont-batch config <oltid> <ontid-a> <ontid-b> <svcid> <is oos> <stype> <idx>> <cvid>	Overwrite the service assignment in multiple ONTs
descr <"TEXT">	Description

ONT POTS Command

command	description
show ont-pots <all oltid [all ontid [all uniid]>	Show ONT POTS configuration
ont-pots create <oltid> <ontid> <uniid>	Add new ONT POTS data
ont-pots remove <oltid> <ontid> <uniid>	Delete ONT POTS data
ont-pots config <oltid> <ontid> <uniid>	Edit ONT POTS data
on off	Enable/disable this data
display <"TEXT">	Assign Display Name
phone <"TEXT">	Assign Phone Number
user <"TEXT">	Assign User Name
pass <"TEXT">	Assign Password
descr <"TEXT">	Description

ONT Authentication Command

command	description
show ont-auth <all oltid [all ontid [all numid]>	Show ONT authentication configuration
ont-auth create <oltid> <ontid> <numid>	Add new ONT authentication data
ont-auth remove <oltid> <ontid> <numid>	Delete ONT authentication data
ont-auth config <oltid> <ontid> <numid>	Edit ONT authentication data
on off	Enable/disable this data
mode <pppoe dhcp static>	Select authentication mode PPPoE / DHCP / Static
vid <VID>	Assign Service-VLAN
param1 <"TEXT"> param2 <"TEXT"> param3 <"TEXT"> param4 <"TEXT">	PPPoE: param1 - User Name param2 - Password param3 - Wan Access Concentrator param4 - Service Name DHCP: param1 - Static IP address param2 - Netmask param3 - Gateway Address param4 - DNS Server
descr <"TEXT">	Description

VLAN Command

command	description
show vlan <all uvid>	Show VLAN configuration
vlan create <uvid> <svid> <single qinq-u <CVID> qinq-c tls>	Add new VLAN ID with selected mode single: single tagged qinq-u: QinQ per U-VLAN qinq-c: QinQ per Customer tls: TLS
vlan remove <uvid>	Delete VLAN
vlan config <uvid>	Edit VLAN configuration
single qinq-u <CVID> qinq-c tls	single: single tagged qinq-u: QinQ per U-VLAN qinq-c: QinQ per Customer tls: TLS
dhcp <none forward relay option82>	Enable/disable DHCP Relay Agent None/Forward/Relay only/Option82
pppoe-relay <on off>	Enable/disable PPPoE Intermediate Agent
arp-proxy <on off>	Enable/disable ARP proxy
secure <none spoofing radius>	Enable MAC Spoofing or IEEE.802.1/RADIUS proxy
igmp <on off>	Enable/disable IGMP proxy
with-bc <on off>	Enable/disable Broadcast support
nni <none LIST>	Involved NNI ports
olt <none LIST>	Involved OLT ports
descr <"TEXT">	Description

Data-Service Command

command	description
show svc-data <svcid all>	Show data-service profile
svc-data create <svcid> <none vlan>	Add new data-service profile with VLAN
svc-data remove <svcid>	Delete data-service profile
svc-data config <svcid>	Edit data-service profile
vlan <none VID>	Specify VLAN ID
encrypt <on off>	Enable/disable DS Encryption
ubw <VALUE>	Bandwidth Profile association for US
dbw <VALUE>	Bandwidth Profile association for DS
bridge <on off>	Enable/disable ONT bridge mode
only-bc <on off>	Enable/disable Only Broadcast GEM Port creation
descr <"TEXT">	Description

IPTV-Service Command

command	description
show svc-iptv <svcid all>	Show iptv-service profile
svc-iptv create <svcid> <none vlan>	Add new iptv-service profile with VLAN
svc-iptv remove <svcid>	Delete iptv-service profile
svc-iptv config <svcid>	Edit iptv-service profile
vlan <none VID>	Specify VLAN ID
ubw <VALUE>	Bandwidth Profile association for US
dbw <VALUE>	Bandwidth Profile association for DS
encrypt <on off>	Enable/disable DS Encryption
only-mc <on off>	Enable/disable Only Multicast GEM Port creation
descr <"TEXT">	Description

VoIP-Service Command

command	description
show svc-voip <svcid all>	Show voip-service profile
svc-voip create <svcid> <none vlan>	Add new voip-service profile with VLAN
svc-voip remove <svcid>	Delete voip-service profile
svc-voip config <svcid>	Edit voip-service profile
vlan <none VID>	Specify VLAN ID
encrypt <on off>	Enable/disable DS Encryption
ubw <VALUE>	Bandwidth Profile association for US
dbw <VALUE>	Bandwidth Profile association for DS
sip <VALUE>	SIP Server Profile association
descr <"TEXT">	Description

ETH-Service Command

command	description
show svc-eth <svcid all>	Show Ethernet-service profile
svc-eth create <svcid> <uniid> <none vlan>	Add new Ethernet-service profile
svc-eth remove <svcid>	Delete Ethernet-service profile
svc-eth config <svcid>	Edit Ethernet-service profile
uniid <ID>	The index of UNI
vlan <VID>	The VALN ID of UNI
untag tagged transparent	The VLAN tagged mode of UNI
iphost <on off>	Enable/disable IPHost feature
ipcam <on off>	Enable/disable IPCAM feature
pbits <VALUE>	Assign Priority bit of UNI
descr <"TEXT">	Description

CATV-Service Command

command	description
show svc-catv <svcid all>	Show catv-service profile
svc-catv create <svcid>	Add new catv-service profile
svc-catv remove <svcid>	Delete catv-service profile
svc-catv config <svcid>	Edit catv-service profile
on off	Enable/disable CATV feature
descr <"TEXT">	Description

MISC-Service Command

command	description
show svc-misc <svcid all>	Show misc-service profile
svc-misc create <svcid>	Add new misc-service profile
svc-misc remove <svcid>	Delete misc-service profile
svc-misc config <svcid>	Edit misc-service profile
auth <on off>	Enable/disable ONT Authentication
descr <"TEXT">	Description

Auto Provision Command

command	description
show auto-profile <all idx>	Show Auto Provision Profile
auto-profile create <idx> <Password>	Add new Auto Provision Profile
auto-profile remove <idx>	Delete Auto Provision Profile
auto-profile cofig <idx>	Edit Auto Provision Profile
pwd <Password>	Specify ONT password
locked <on off>	Enable to store this ONT into flash memory
img <VALUE>	ONT Image profile association
cfg <VALUE>	ONT Config profile association
encrypt <on off>	Enable/disable OMCI encryption
auto-learn <on off>	Learn ONT password automatically
us-fec <on off>	Upstream Forward Error Correction
mib-load <on off>	Enable/disable auto ONT MIB-Upload
svc <svcid> <none <stype> <index>>	Service Profile association stype: data iptv voip eth catv misc
descr <"TEXT">	Description

Bandwidth Profile Command

command	description
show bw_dba <all idx>	Show Bandwidth profile
bw_dba create <idx>	Add new Bandwidth profile
bw_dba remove <idx>	Delete Bandwidth profile
bw_dba config <idx>	Edit Bandwidth profile
fix <VALUE>	Committed Information Rate
assure <VALUE>	Assure Information Rate
max <VALUE>	Peak Information Rate
sr nsr	sr – Status Reporting nsr – Non Status Reporting
descr <"TEXT">	Description

ONT Image Profile Command

command	description
show ont-image <all idx>	Show ONT Image profile
ont-image create <idx>	Add new ONT Image profile
ont-image remove <idx>	Delete ONT Image profile
ont-image config <idx>	Edit the ONT Image profile
version <"TEXT">	Assign version string
ftp <FileLink>	File located by ftp username and password are optional
tftp <FileLink>	File located by tftp
descr <"TEXT">	Description

ONT Configuration Profile Command

command	description
show ont-cfg <all idx>	Show ONT Config profile
ont-cfg create <idx>	Add new ONT Config profile
ont-cfg remove <idx>	Delete ONT Config profile
ont-cfg config <idx>	Edit ONT Config profile
ftp <FileLink>	File located by ftp username and password are optional
tftp <FileLink>	File located by tftp
descr <"TEXT">	Description

SIP Server Profile Command

command	description
show sip-server <all idx>	Show SIP-Server profile
sip-server create <idx>	Add new SIP-Server profile
sip-server remove <idx>	Delete SIP-Server profile
sip-server config <idx>	Edit SIP-Server profile
proxy <"TEXT">	Assign Proxy Server address
sip-port <VALUE>	The port number of Proxy Server
regist <"TEXT">	Assign Registrar Server address
reg-port <VALUE>	The port number of Registrar Server
outbound <"TEXT">	Assign Outbound Server address
out-port <VALUE>	The port number of Outbound Server
agent <"TEXT">	Assign User Agent Domain
expire <VALUE>	The Expire time of Register
descr <"TEXT">	Description

Server-List Command

command	description
show server-list <all idx>	Show Server List configuration
server-list create <idx> <server-addr>	Add new Server-List profile
server-list remove <idx>	Delete Server-List profile
server-list config <idx>	Enable Server-List profile
dhcp-relay <on off>	Server support DHCP Server or not
radius <on off>	Server support RADIUS or not
vlan <VID>	The VLAN ID used at NNI side
vip <ADDR>	Virtual IP address for Proxy Agent
gate <ADDR>	Gateway address if needed
list <none LIST>	Service VLAN list
secret <"TEXT">	Shared Secret for RADIUS server
descr <"TEXT">	Description

Global Command

command	description
show global	Show Global configuration
global config	Edit Global configuration
isolation <on off>	Enable/disable ONT Isolation
multi_iptv <on off>	Enable/disable Multi-VLAN for IPTV
igmp <none snoop proxy>	Select IGMP mode
igmp_qi <VALUE>	Query Interval second (1-900,def=125)
igmp_qri <VALUE>	Max Response Time (1-25,def=10)
igmp_rv <VALUE>	Robustness Value (1-255,def=2)
igmp_llqi <VALUE>	Last Member Query Interval (1-25, def=1)
cfm <on off>	Enable CFM support globally
customer <Level>	Assign the MD level of 'Customer'
provider <Level>	Assign the MD level of 'Provider'
operator <Level>	Assign the MD level of 'Operator'
bl_mac_age <VALUE>	Assign the Aging time for GPON MAC
sw_mac_age <VALUE>	Assign the Aging time for Ethernet Switch

NNI Command

command	description
show nni <all nniid>	Show NNI configuration and status
nni config <nniid>	Edit NNI configuration
is oos	Enable/Disable this NNI
speed <none auto 100M 1G 10G>	Configure the link speed
flow <on off>	Enable/disable flow control
untag tagged	Configure Egress Tag mode
vlan <VID>	Assign the default VLAN ID
nni sfp <nniid>	Display SFP module information of NNI
<temp volt bias txp rxp> <alarm warning> <high low> <SEVERITY>	Specify the threshold crossing indicators for 5 parameters in SFP module.

Port Based VLAN Command

command	description
show pbvlan <all idx>	Show Port Based VLAN configuration
pbvlan create <idx>	Add new Port Based VLAN rule
pbvlan remove <idx>	Delete Port Based VLAN rule
pbvlan config <idx>	Edit Port Based VLAN rule
nni <none LIST>	Involved NNI port
olt <none LIST>	Involved GPON OLT port

Aggregation Mode/Group Command

command	description
show aggregation	Show all aggregation configuration
aggregation hash	Show or edit Hash Code Contributors
smac <on off>	Include Source MAC Address
dmac <on off>	Include Destination MAC Address
ip <on off>	Include IP Address
port <on off>	Include TCP/UDP Port Number
aggregation port	View aggregation configuration
aggregation port <nniid>	Edit aggregation configuration
lACP <on off>	Enable/disabled LACP support
key <auto 1-65535>	Assign LACP KEY
role <active passive>	Select LACP role active / passive
group <VALUE>	Assign member of group for static aggregation
aggregation port-status <nniid>	show aggregation port status
aggregation lACP-status	show aggregation lACP status

ACL Command

command	description
show aCL <all idx>	Show ACL configuration
aCL create <idx> <any etype ipv4> <permit deny>	Create new ACL rule with type permit / deny
aCL remove <idx>	Delete ACL rule
aCL config <idx>	Edit ACL rule
dmac_mc <any no yes>	Test Multicast Destination MAC
dmac_bc <any no yes>	Test Broadcast Destination MAC
[nni <none LIST>]	Involved NNI port
[olt <none LIST>]	Involved GPON OLT port
[nms <no yes>]	Involved NMS port
Extra OPTIONS for etype	
etype <HEX> <MASK>	Ethernet Type and Mask
dmac <MAC> <MASK>	Destination MAC address and Mask
smac <MAC> <MASK>	Source MAC address and Mask
Extra OPTIONS for ipv4	
proto <HEX> <MASK>	Protocol and Mask (hex)
sip <ADDR> <MASK>	Source IP address and Mask
dip <ADDR> <MASK>	Destination IP address and Mask
sport <START> <END>	Range of Source port
dport <START> <END>	Range of Destination port
descr <"TEXT">	Description
aCL cnt <all idx>	View ACL counters
aCL clr-cnt <all idx>	Clear ACL counter

Rate Storm Control Command

command	description
show rate-control	Show Rate Storm Control configuration
rate-control <nni <nniid> olt <oltid> nms>	Edit Rate Storm Control configuration
unknown <off VALUE>	Rate of Unknown Unicast frame (kbps)
broadcast <off VALUE>	Rate of Broadcast frame (kbps)
multicast <off VALUE>	Rate of Multicast frame (kbps)
cpu_port <off VALUE>	Rate of CPU traffic (fps)

Quality of Service Command

command	description
show qos	Show QoS configuration
qos <nni <nniid> olt <oltid>>	Edit QoS configuration for OLT or NNI
strict	Assign Strict Priority
dwrr	Assign Weighted Round Robin
[qw0 <VALUE>] [qw1 <VALUE>] [qw2 <VALUE>] [qw3 <VALUE>] [qw4 <VALUE>] [qw5 <VALUE>]	Assign the percentage of queue VALUE – 1 to 100

Relay Agent Information Command

command	description
show relay-agent	Show Relay Agent information
relay-agent status [clr]	Show or clean relay-agent counters
relay-agent edit	Edit Relay Agent information
dhcp-circuit <"TEXT">	Circuit ID for DHCP
dhcp-remote <"TEXT">	Remote ID for DHCP
pppoe-circuit <"TEXT">	Circuit ID for PPPoE
pppoe-remote <"TEXT">	Remote ID for PPPoE

Relay Agent Information Command

command	description
show relay-agent	Show Relay Agent information
relay-agent status [clr]	Show or clean relay-agent counters
relay-agent edit	Edit Relay Agent information
dhcp-circuit <"TEXT">	Circuit ID for DHCP
dhcp-remote <"TEXT">	Remote ID for DHCP
pppoe-circuit <"TEXT">	Circuit ID for PPPoE
pppoe-remote <"TEXT">	Remote ID for PPPoE

Static ARP Proxy Table Command

command	description
show arp-static <all idx>	Show Static ARP Proxy Table
arp-static create <idx> <VID> <ADDR> <MAC-ADDR>	Add new Static ARP Proxy entry
arp-static remove <idx>	Delete Static ARP Proxy entry
arp-static config <idx>	Edit Static ARP Proxy entry
vlan <VID>	Assign VLAN ID
addr <ADDR>	IP address
mac <MAC-ADDR>	MAC address
descr <"TEXT">	Description

Static MAC Spoofing Table Command

command	description
show spoofing-mac <all idx>	Show Static MAC Spoofing Table
spoofing-mac create <idx> <VID> <MAC-ADDR>	Add new Static MAC Spoofing entry
spoofing-mac remove <idx>	Delete Static MAC Spoofing entry
spoofing-mac config <idx>	Edit Static MAC Spoofing entry
vlan <VID>	Assign VLAN ID
mac <MAC-ADDR>	MAC address
olt <none LIST>	Involved GPON OLT port
descr <"TEXT">	Description

Connectivity Fault Management Command

command	description
show cfm <all idx>	Show MEP/MIP
cfm create <idx> <nniid> <VID> <mip mep <in out> <mepid>>	Add new MEP or MIP
cfm remove <idx>	Delete a MEP/MIP
cfm config <idx>	Edit Static MAC Spoofing entry
nni <nniid>	Assign NNI ID
vlan <VID>	Assign VLAN ID
mip mep <in out> <mepid>	MIP mode or MEP mode with direction and MEPID
customer provider operator	Assign the Maintenance Domain
ccm <VALUE>	Assign CCM frame rate
prio <VALUE>	Assign the priority level
md-name <"TEXT">	Assign Maintenance Domain name
ma-name <"TEXT">	Assign Short Maintenance Associate name

Connectivity Fault Management - RMEP Command

command	description
show cfm-rmep <mp idx> [rmep id]	Show the status of RMEP
cfm-rmep create <mp idx> <rmep id>	Add new Remote MEP
cfm remove <mp idx> <rmep id>	Delete a Remote MEP

Connectivity Fault Management - Loopback Command

command	description
show cfm-lpbk <mp idx>	Show the configuration of loopback
cfm-lpbk send <mp idx> <mcast ucast <MAC-ADDR>> <size> <count> <priority>	Activate the CFM loopback test
cfm-lpbk result <mp idx>	Show the result of loopback test

Connectivity Fault Management - Linktrace Command

command	description
show cfm-trace <mp idx>	Show the configuration of linktrace
cfm-trace send <mp idx> <MAC-ADDR> <ttl> <count>	Activate the CFM linktrace test
cfm-trace result <mp idx>	Show the result of linktrace test

Spanning Tree Command

command	description
stp bridge	View or edit STP Bridge Configuration
stp rstp mstp	Select STP mode
forward <VALUE>	Forward Delay (def=15)
max-age <VALUE>	Max Age (def=20)
hop-cnt <VALUE>	Maximum Hop Count (def=20)
tx-hold <VALUE>	Transmit Hold Count (def=6)
filter <on off>	Enable/disable Edge Port BPDU Filtering
guard <on off>	Enable/disable Edge Port BPDU Guard
recover <VALUE>	Port Error Recovery Timeout (0=disable)
name <"TEXT">	Configuration Name for Identification
revision <VALUE>	Configuration Revision for Identification
stp map	View CIST/MSTI Mapping
stp map <cist msti <1-7>>	Edit CIST/MSTI Mapping
priority <VALUE>	Priority
vlan <none LIST>	Involved VLAN list for MSTI-x
stp cist	View CIST Port Configuration
stp cist <aggr nni <nniid>>	Edit CIST Port Configuration
stp <on off>	Enable/disable STP
path-cost <auto VALUE>	Specify the Path Cost
priority <VALUE>	Specify the Priority
admin-edge <on off>	Specify Admin Edge type
guard <on off>	Enable/disable BPDU guard
auto-edge <on off>	Enable/disable Auto Edge
rst-role <on off>	Enable/disable Restricted role
rst-tcn <on off>	Enable/disable Restricted TCN
p2p <false true auto>	Specify Point to Point type
stp msti <1-7>	View MSTI Port Configuration
stp msti <1-7> <aggr nni <nniid>>	Edit MSTI Port Configuration
path-cost <auto VALUE>	Specify the Path Cost
priority <VALUE>	Specify the Priority
stp status <cist msti <1-7>>	View CIST/MSTI status
stp port <status statistics>	View STP port status or statistics

Alarm and Event Command

command	description
event <curr hist> [clean]	View or clean current / history event and alarm

Performance Data Command

command	description
performance rmon <nri <nriid> olt <oltid> nms> [clr]	View or clean ROMN counters
performance pon <oltid> [clr]	View or clean GPON counters

IGMP Status Command

command	description
igmp status	View IGMP Snooping status
igmp group	View IGMP Snooping Group information

Dynamic ARP Proxy Table Command

command	description
arp-dynamic table	Show dynamic ARP Proxy
arp-dynamic remove <VID> <ADDR>	Remove one entry from ARP Proxy table

MAC Table Command

command	description
mac-table sw [clr]	View or clean the MAC table of Ethernet Switch
mac-table pon <oltid> [clr]	View or clean the MAC table of GPON OLT

Protection Switching Command

command	description
diagnosis gpon switch <oltid>	do Protection Switching Manually

Host Network Setting Command

command	description
show host	Show Host network configuration
host	Edit Host network configuration
dhcp <on off>	Enable/disable DHCP client
vlan <VID>	Specify VLAN ID for in-band management
ip <ADDR>	Static IP address for Host
mask <ADDR>	Netmask for Host
gate <ADDR>	Gateway for Host
dns-1 <ADDR>	Specify DNS Server 1 for Host
dns-2 <ADDR>	Specify DNS Server 2 for Host

SNMP Configuration Command

command	description
show snmp	Show SNMP configuration
snmp	Edit SNMP configuration
udp <VALUE>	Specify UDP port of SNMP
getcomm <"TEXT">	Specify Get Community
setcomm <"TEXT">	Specify Set Community
snmp trap <id>	Edit SNMP Trap
addr <ADDR>	Specify SNMP Trap address
v1-trap v2c-trap v2c-info	Specify Trap Version
community <"TEXT">	Specify Trap Community
snmp usm <id> <ro rw> <USER> none	Edit SNMP v3 account without security
<trap info> <ADDR>	Specify SNMPv3 Trap/Info address
snmp usm <id> <ro rw> <USER> auth	Edit SNMP v3 account with Auth security
<md5 sha> <"VALUE">	Specify authentication method
<trap info> <ADDR>	Specify SNMPv3 Trap/Info address
snmp usm <id> <ro rw> <USER> priv	Edit SNMP v3 account with privacy security
<md5 sha> <"VALUE">	Specify authentication password
<des aes> <"VALUE">	Specify privacy password
<trap info> <ADDR>	Specify SNMPv3 Trap/Info address
snmp usm <id> delete	Remove account of SNMP USM

Time Command

command	description
show time	Show current time
time <yyyy/mm/dd> [HH:MM:SS]	Update the current time
ntp <time offset> <addr>	Update time with NTP server

Alarm Cut Off Command

command	description
show aco	Show Alarm Cut Off configuration
aco <on off cut>	Edit Alarm Cut Off configuration or do Cut-Off action

Device Description Command

command	description
show device	Show device description
device <"TEXT">	Edit device description

Reboot command

command	description
reboot <normal default factory force>	Reboot according to mode

Device Upgrade Command

command	description
show upgrade	Show the upgrade configuration and status
upgrade file	Edit file location
ftp <FileLink>	File located by ftp username and password are optional
tftp <FileLink>	File is located by tftp
http <HyperLink>	File is located by http
upgrade start	Start to upgrade device
upgrade factory	Restore the factory firmware version
upgrade restore	Restore the previous firmware version

Configuration Backup/restore Command

command	description
show config	Show Backup/Restore configuration and status
config file	Edit file location
ftp <FileLink>	File located by ftp username and password are optional
tftp <FileLink>	File is located by tftp
http <HyperLink>	File is located by http
config backup <saved curr>	Backup Saved/Current Configuration file and put it onto remote server
config backup <saved curr> whole	Backup configuration including account/network/SNMP settings and put it onto remote server
config restore <tftp tftp http>	Restore configuration file.

Account Management Command

command	description
show account	Show accounts in device
account create <username> <group> <nopwd pwd <Password>>	Create an new account
account remove account	Delete account
account config <username> <group> <nopwd pwd <Password>>	Edit account

License Command

command	description
show license	Show the license information
license remove license	Remove current license
license	Upload License
ftp <FileLink>	File located by ftp username and password are optional
tftp <FileLink>	File is located by tftp
http <HyperLink>	File is located by http

Log File Control Command

command	description
show logfile	Show the log file status
logfile <on off>	Edit options for logfile
all	Enable all logs
pon	Enable GPON Process Log
msg	Enable Task Process Log
disc	Enable ONT Discover Log
event	Enable Internal Event Log
vtss	Enable Layer-2 Switch Log
pkt	Enable Packet Process Log
igmp	Enable IGMP Frame Log
iptv	Enable IPTV Frame Log
dhcp	Enable DHCP Relay Agent Log
pppoe	Enable PPPoE Intermediate Agent Log
auth	Enable RADIUS & IEEE 802.1x Log
aggr	Enable Link Aggregation Log
mstp	Enable Spanning Tree Protocol Log
arp	Enable ARP Proxy Log
mac	Enable MAC Learning Log
rate	Enable Data Rate Control Log
cmd	Enable User Command Log
logfile <ftp tftp> <FileLink>	Upload log file to remote server by

Others Command

Command	Description
help	List the command
?	alias of help
information	Display Device Information
logout	Logout from CLI
ping	Network tool - ping
ps	Show the Processes in device
save	Save configuration into Flash memory
show	Display Configuration
traceroute <addr>	Network tool - traceroute
version	alias of Information

APPENDIX E. GPON Encapsulation Method (GEM)

The previous generation of FSAN PON standard used ATM to encapsulate data for transmission within PON frames. ATM is extremely flexible with all the adaptations already defined. The primary drawbacks to ATM, however, are its inefficient bandwidth utilization, the derived protocol translation, and the cost involved in implementing a high bandwidth switching PON chassis that can switch up to 160Gbit/s. Achieving this in ATM is more costly than with Ethernet. ATM uses 5 overhead bytes for every 48 payload bytes. In addition, since ATM cells must always be 53-byte long, there is typically some wasted padding at the end of the ATM cell that contains the end of an encapsulated packet. While this degree of bandwidth inefficiency is acceptable in a core network with its ample bandwidth available, it is unacceptable in the access network where bandwidth is very expensive. For this reason, GPON looked to the new ITU-T G.7041 Generic Framing Procedure (GFP) as the model for its encapsulation method. GFP allows direct encapsulation of variable length packets without repeating the encapsulation overhead on a regular basis.

	PLI (Payload Length Indicator)	Port ID	PTI	HEC - BCH(39, 12, 2) + P	Fragment Payl
#bits	12	12	3	13	L(bytes)

code Meaning
 000 User data fragment - Not end of frame (No Congestion)
 001 User data fragment - End of frame (No Congestion)
 010 User data fragment - Not end of frame (Congestion has occurred)*
 011 User data fragment - End of frame (Congestion has occurred)
 100 GEM OAM
 101-111 Reserved
 * For further study

Figure 15: GEM Frame Header

The GFP frame overhead, however, was optimized for point-to-point NE-to-NE links rather type of encapsulated payload frame, whether a frame check sequence (FCS) is used over the payload, and what type of Extension header (if any) is used. Applications using GFP were typically expected to rely on higher layer protocols for packet/frame multiplexing, so G.7041 defines a second, optional payload header (i.e., the Extension header) for communicating channel/port number information in applications where it's needed. In contrast, since the ONTs and OLT of a PON system can be logically considered as a

single NE with the PON fiber functioning as a backplane extension, much of this information is already known through provisioning. Since the PON uplink multiplexes multiple client streams, it typically needs a port identifier for each GEM frame. Due to provisioning, the port identifier gives the OLT and ONT adequate knowledge about the type of encapsulated frame. Consequently, the GPON standard re-used the basic concepts of GFP but redefined the overhead fields so that their information and bandwidth are optimized for the PON application.

The Payload Length Indicator (PLI) is the primary mechanism for delineating GEM frames and is functionally equivalent to the GFP PLI. The value of the PLI, L , is the number of bytes in the fragment payload area of the GEM frame. The PLI of the first GEM frame in the downstream GTC frame or upstream burst is located at the beginning of the payload area. The next GEM frame will begin L bytes after the header of the current GEM frame. This GEM frame also contains a PLI, and its value can likewise be used to find the beginning of the next GEM frame, and so forth through the remainder of the GPON payload area.

Note that since each GEM partition or payload begins with a GEM header, GEM frames can be delineated immediately at the start of each partition or payload. This feature is especially valuable for the OLT, since the OLT does not need to keep track of the delineation alignment between upstream frames of each ONT separately.

The Port ID field allows multiplexing up to 4096 traffic streams per PON.

In contrast to GFP, the GEM payload type indicator (PTI) does not identify the type of client data frame encapsulated into the fragment payload area. It only indicates whether this fragment contains the end of the client data frame or if this GEM frame is carrying a GEM OAM message.

The header error check (HEC) comprises a 12-bit BCH-2 code followed by a parity bit that allows detection and correction of transmission errors within the GEM header. The BCH code is a double error correcting BCH (39, 12, 2) code that covers all the header bits except the parity bit. The BCH generator polynomial is $x^{12}+x^{10}+x^8+x^5+x^4+x^3+1$. The parity bit is set to provide an even number of 1s within the header.

In order to provide good transition density to correctly delineate a series of idle frames, the 40-bit header is exclusive ORed with the pattern 0x0xB6AB31E055 prior to transmitting the frame.

Definitions:**GEM Encapsulation**

G-PON Encapsulation Method (GEM): A data frame transport scheme used in GPON systems that is connection-oriented and that supports fragmentation of the administrator data frames into variable sized transmission fragments.

T-CONT:

A traffic bearing object within an ONT that represents a group of logical connections, and is treated as a single entity for the purpose of upstream bandwidth assignment on the PON. In the upstream direction, it is used to bear the service traffic. Each T-CONT corresponds to service traffic of one bandwidth type. Each bandwidth type has its own QoS feature.

ALLOC_ID:

Each T-CONT is identified by the ALLOC_ID uniquely. The ALLOC_ID ranges from 0 to 4095. It is allocated by OLT i.e. a T-CONT, and can only be used by one ONT per PON interface on the OLT.

GEM Port:

A GPON Encapsulation Method (GEM) port is a virtual port for performing GEM encapsulation for transmitting frames between the OLT and the ONT. Each different traffic-class (TC) per UNI is assigned a different GEM Port. Each T-CONT consists of one or more GEM Ports. Each GEM port bears one kind of service traffic i.e. a T-CONT type.

GEM Port ID:

Each GEM Port is identified by a port ID uniquely. The Port ID ranges from 0 to 4095. It is allocated by the OLT, i.e. a GEM port, and can only be used by a single ONT per PON interface on the OLT.