

SIXPON GPON ONU

FX Series

User's Manual

Version 1.0



SIXPON
SMART • EFFICIENT • SYNC

All Rights Reserved ©2016



TABLE OF CONTENTS

FX SERIES Overview	4
ONU FX Series components	4
To reset the ONU	5
Management	5
Register OLT	5
Using SN in ONU to register OLT.	6
To set ONU SN	6
Web login	6
Factory mode	7
Network configure	8
WAN connection.....	8
Bridged	9
Router	11
WLAN Configure	14
Introduce	14
Creating WLAN connection	15
TR69.....	15
Introduce	15
ITMS server.....	15
IP address	15
Port	15
Set ITMS server configure	16
QOS config.....	16
QOS.....	16
Set QOS configure	17
Security	17
URL filter	17
Config URL filter.....	17
Firewall	18
Configure firewall	18
MAC filter	19
Configure MAC filter	19
IP filter	19

Configure IP filter.....	20
Application	21
VOIP	21
Basic Setup	21
Log Plot Setup.....	22
Voice Media	22
SIP Application	23
IGMP	23
IGMP Settings	23
Enable IGMP Snooping.....	23
Diagnosis	24
Line Diagnosis	24
Ethernet connection Test	24
Ping Test.....	24
Inform Test.....	25

FX SERIES Overview

- The ONU FX Series (SIXPON TECHNOLOGIES Network Interface Device) is a family of indoor, full-featured gateways for residential installations. These next generation ONUs support GPON or Active Ethernet termination to meet the demands of multi-service network deployments to the user. With either GPON or Active Ethernet uplinks, the FX Series ONUs deliver data, voice, or video (IPTV) over fiber.
- Compliant to The ONUs is a full-featured gateway supporting services such as DHCP server, rate limiting, filtering, comprehensive logging, and more. The ONU product line implements a very flexible QoS allowing the service provider to guarantee that services are being prioritized correctly and the end-user receives the Quality of Experience that is expected.
- The ONU FX Series may be managed by
 - TR069
 - Web (HTTP)
 - Command Line Interface (CLI/Telnet)
 - ONT Management Control Interface (OMCI) *for GPON only*

ONU FX Series components

Depending upon the model selected, the interfaces include:

- two, or four Gigabit Ethernet ports
- Two Phone Ports (POTS)
- four wireless ports
- USB port

To reset the ONU

Press a pin into the reset button and hold it down until all LEDs are on together.

- Release the reset button.

Management

- CLI

The FX products can be managed using a command line interface.

- Web

The FX products can also be fully managed through the web (HTTP)

interface. The web pages are very intuitive and they include a context sensitive help button for additional information. The web interface will be used for the configuration examples used in this document.

- TR069

The FX products can also be managed through tr069. The FX family is compatible with any industry standard tr069.

- OMCI

ONU Management Control Interface (OMCI) provides policy based configuration and management capabilities for GPON. OMCI management is intergrated into the OLT command set, so configuration of the ONU with OMCI is done from the OLT, not directly as with the Web UI or CLI interfaces.

Register OLT

- Access on the GPON interface requires a Registration ID. This value must match the value programmed in the OLT. The system administrator should have programmed this value. Changing the value will disable communications with the network. The unit will reset once the Reg ID has been changed and the GPON link will not communicate with the OLT until the same password is entered in the OLT.

Using SN in ONU to register OLT.

To set ONU SN

- telnet ONU ;such as telnet 192.168.1.1, username and password are admin/admin or twmanu/twmanu
- set sn or password.

FX601 :

```
T&W#
T&W# man
T&W# manufactory
manufactory#
manufactory# set sn
<string> format:CCCCXXXXXXXX
manufactory# set sn ALCLf9c1fbde
.set sn success!
manufactory# write password hex f201300055902600
.Write password success!
```

FX660 :

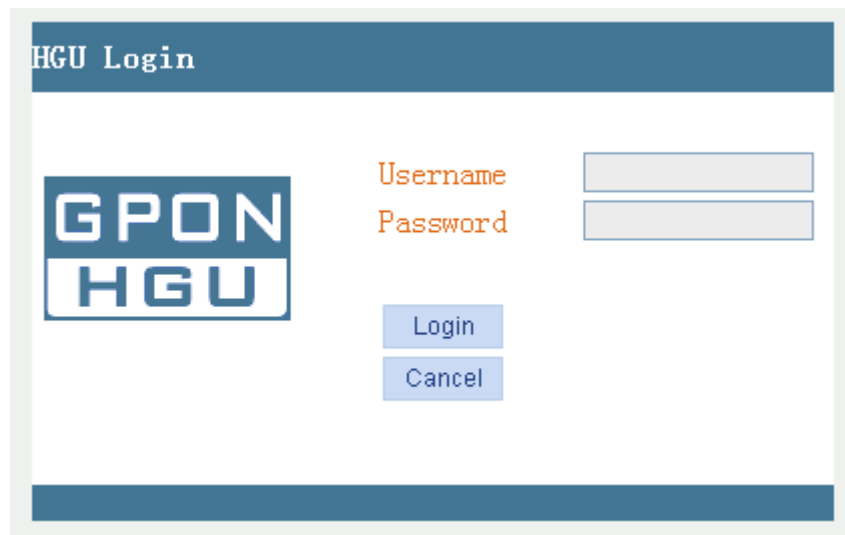
```
BCM99999 Broadband Router
VosLogin: admin
Password:
S304# man
S304# manufactory
MANUFACTORY# write sn
<string> format:CCCCXXXXXXXX
MANUFACTORY# write sn aaaaaaaaaaaaaaa //16 HEX char
SN formate: 4 vendor ID, 8 serial ID sample: TWSH01020304

MANUFACTORY# write oltpassword hex 1111122222333334444455555 //20 HEX char
Password formate: 20 hex value; sample: 00112233445566778899
```

- restart onu, the new SN will take effect.

Web login

- The default IP address of device is 192.168.1.1. we need configure ONT on the web (<http://192.168.1.1/login.html>). The default Username is 'admin', and password is 'admin'

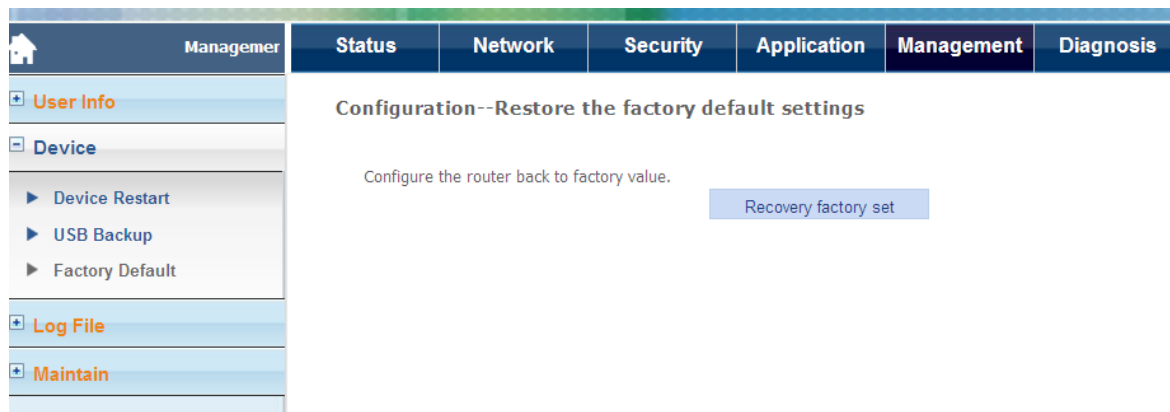


The image shows a web browser window displaying the 'HGU Login' page. At the top, there is a blue header bar with the text 'HGU Login'. Below the header, on the left, is a logo consisting of a blue square with the text 'GPON' in white, and a white square with the text 'HGU' in blue. To the right of the logo, there are two input fields. The first is labeled 'Username' in orange text, and the second is labeled 'Password' in orange text. Below these input fields are two buttons: 'Login' and 'Cancel', both in blue. The entire login form is enclosed in a light gray border.

Factory mode

- The factory default screen allows you to recover factory configuration. Clicking recovery factory set button on the Management | factory default page will recover configuration of ONU to factory configuration

Figure 2: The factory mode



Network configure

- The network pages define and configure wan connection by the ONU, such as WAN, LAN , WLAN and QOS. The System pages also provide options for binding, by port or vLan.

Figure 3: The network menu

The screenshot displays a web interface for network configuration. On the left, a sidebar menu shows a hierarchy: 'work' > 'WAN' > 'Wan Connection'. Below this, a list of network-related items is shown: 'WAN', 'Wan Connection', 'Bind', 'LAN', 'WLAN', 'TR69', 'Qos', 'SNTP', and 'Route'. The main content area is titled 'Internet(WAN)Connection setting' and contains several configuration fields: 'Upstream method' (GPON), 'Connected Name' (1_INTERNET_B_VID_46), 'Mode' (Bridge), 'IP Mode' (IPv4), 'MTU' (1400), 'Enable Vlan' (checked), 'Vlan ID' (46), and '802.1p' (0).

This section describes the following network pages:

- Wan connection
- Bind
- LAN
- WLAN
- TR069
- Qos
- SNTP
- Route

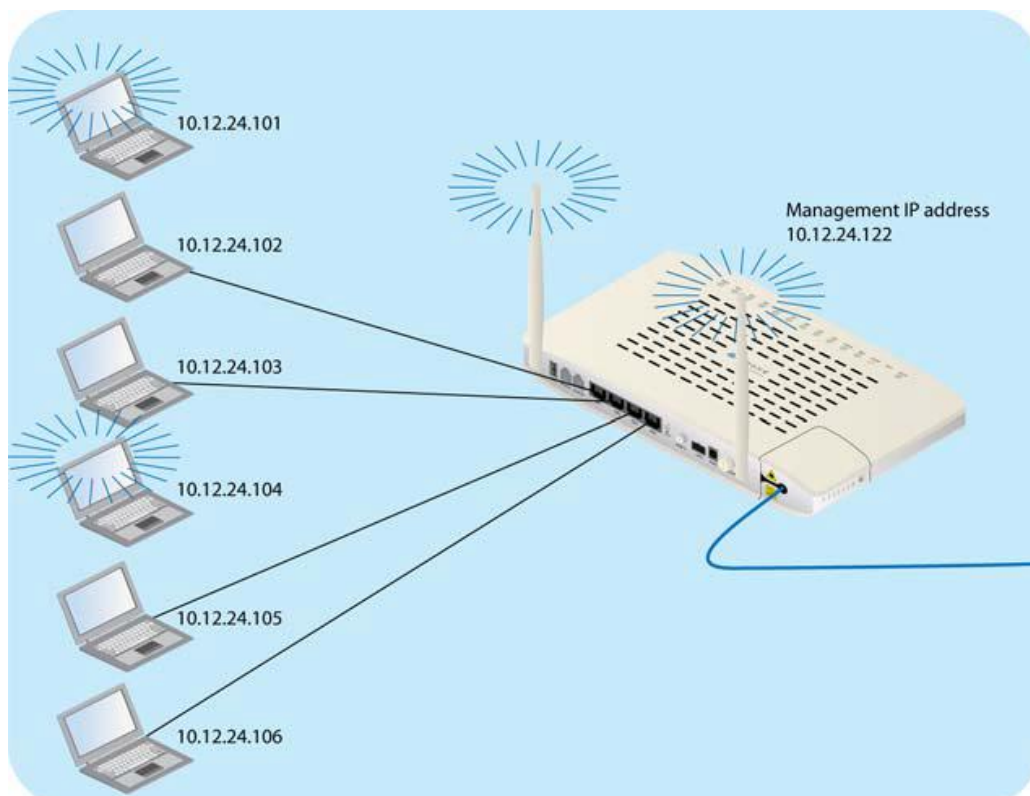
WAN connection

- The Deployment scenarios section is a task based section which describes how to create data, video and voice connections.

Bridged

- For bridged VLANs, an IP Address can be assigned if the ONU will be a host in a particular IP subnet. IP addresses for LAN-side client devices can be statically assigned or assigned by an upstream DHCP server. Any number of Ethernet ports or WiFi SSIDs can be members of the Bridged VLAN. All clients in a bridged VLAN will be in the same IP subnet, and the FX Series will enable direct local peer-to-peer communications between all clients unless the Secure Forwarding option has been enabled. If Secure Forwarding is enabled, all broadcast traffic is forwarded upstream and not flooded out the other local ports in the VLAN. This prevents local peer-to-peer communications, and is equivalent to the ONU operating mode Bridged with CPU or CPU-Bridged must be selected for using bridged VLANs in Dual Managed mode with VEIP.

Figure 4: For bridged connections all the interfaces are in the same subnet



To create a bridged connection

Figure 5: wan bridge connection page

Network>>WAN>>V

Status Network Security Application

WAN

WAN Connection

Bind

LAN

WLAN

TR069

QoS

SNTP

Route

WAN Connection Settings

Upstream Method: GPON

Connected Name: 1_OTHER_B_VID_10

Mode: Bridge

IP Mode: IPv4

MTU: 1500

Enable VLAN: ☒

Vlan ID: 10

802.1p: 0

Service Mode: OTHER

Bind Port:

☒ Port_1 ☒ Port_2

- On the | wan connection page, click Add New VLAN in drop down box of connection name.
- In the mode text box select the bridge
- In the IP mode text box select the IP protocol.
- In the VLAN ID text box enter a VLAN ID(1 - 4095)
- From the service mode dropdown select service type.
- From the service mode dropdown select the bind port
- Click Apply/Save

Notes:

In bridge mode,'OTHER'should be checked in Service mode box. So user'PCs get IP address from PPPOE(dail-up internet mode) or other DHCP server .

Besides,you can check wireless Box in Bind Port. After wireless cards access to ONU's SSID, PC can dail-up internet by PPPOE

Check bridge connect status

Figure 6: check bridge connect status

The screenshot shows a network management interface. On the left is a sidebar with a tree view containing: 'IPv4 Info' (selected), 'Device Info', 'WAN Info' (expanded), 'IPv4 Info', 'IPv6 Info', 'GPON Info', 'LAN Info', 'Voice Info', and 'Remote Info'. The main content area has a top navigation bar with tabs: 'Status', 'Network', 'Security', 'Application', 'Management', and 'Diagn'. Below the tabs, the 'WAN IPv4 Info' section contains a table with the following data:

Interface Name	Interface Description	Type	VlanMuxId	IGMP	NAT	Firewall	State
veip0.1	1_OTHER_B_VID_10	Bridge	10	Disable	Disable	Disable	Connected

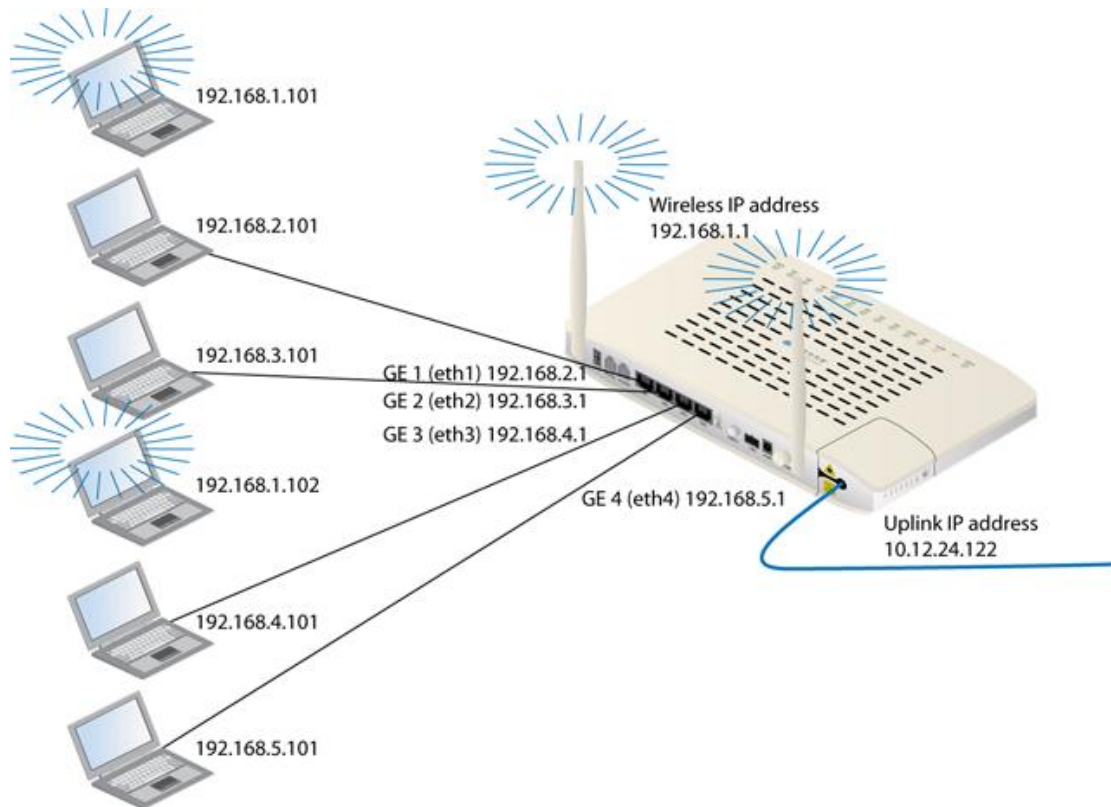
The 'State' column in the table is circled in red. Below this, the 'Network Information' section contains a table with the following data:

Default Gateway	
Subnet Mask	
Primary DNS Server	
Secondary DNS Server	

Router

- For Router VLANs, an IP Address will be assigned per physical port that is assigned to the VLAN. The minimum configuration will have the uplink interface and at least one LAN-side interface. When there are multiple LAN ports in the same Router VLAN, each one must be assigned its own IP subnet
 - In the illustration below, a NAT Router VLAN has been configured that contains three LAN ports and one SSID. A total of six IP addresses are assigned to the 2426 for this configuration. A WAN IP address is assigned the uplink, and four LAN-side IP addresses must be assigned, each in a separate subnet, plus an IP subnet for the WiFi interface.
 - All Wi-Fi connected client devices will be in the same subnet. An RG configuration item called “Isolate Clients” in the Wireless / Basic menu determines if these devices will be able to communicate locally with each other, or if all traffic will be forwarded upstream. When Isolate Clients is enabled, all traffic is forwarded upstream, blocking local peer-to-peer communications.
 - The example below shows a Router VLAN with NAT. When NAT is enabled, the Router performs Network Address Translation, mapping each LAN side IP address and source port to a unique protocol port used with the WAN IP Address for communications across the network

Figure 7: For router connections each interface is in its own subnet



Creating router connections

Figure 8: Creating a router

Network>>>	Status	Network	Security	Application	Man
WAN					
Wan Connection					
Bind					
LAN					
WLAN					
TR69					
Qos					
SNTP					
Route					

Internet(WAN)Connection setting

Upstream method: GPON

Connected Name: 1_INTERNET_B_VID_11

Mode: Route

IP Mode: IPv4

☒ DHCP Get a Ip address from ISP
☐ Static Config a static Ip address by ISP
☐ PPPoE Please select this item if ISP use PPPOE

MTU: 1500

NAT: ☒

Enable Vlan: ☒

Vlan ID: 11

802.1p: 0

Service mode: VOIP_INTERNET

Bind port: ☐ Port 1 ☐ Port 2

- On the Configuration| wan connection , click Add New VLAN in drop down box of connection name.
- In the mode text box select the Route.
- In the IP mode text box select the IP protocol.
- In the VLAN ID text box enter a VLAN ID(1-4095)
- From the service mode dropdown select service type.
- From the service mode dropdown select the bind port ‘
- Click Apply/Save

Check router connections

Figure 9: router connection status

>>WAN Info>>IPv4 Info

+ Device Info

- WAN Info

▶ IPv4 Info

▶ IPv6 Info

▶ GPON Info

+ LAN Info

+ Voice Info

+ Remote Info

StatusNetworkSecurityApplicationManagementDiagnosisHelp

WAN IPv4 Info

Interface Name	Interface Description	Type	VlanMuxId	IGMP	NAT	Firewall	State	IP Address
veip0.1	1_TR069_VOICE_INTERNET_R_VID_10	IPoE	10	Enable	Enable	Enable	Connected	219.141.136.10
veip0.2	2_OTHER_B_VID_10	Bridge	10	Disable	Disable	Disable	Connected	

Network Information

Default Gateway	192.168.0.1
Subnet Mask	255.255.255.0
Primary DNS Server	219.141.136.10
Secondary DNS Server	219.141.140.10

WLAN Configure

Introduce

- Open Wireless:

If you want to make wireless effective, you have to put this check box selected, otherwise hidden Access Point SSID, Country, Enable Wireless Guest Network, and Guest SSID option will not be displayed.

- Hidden Access Point

If you want to hide the access point to your router, you must put on the marquee. In this case, the configuration will not be able to get through the passive scan SSID.

- SSID

SSID (Service Set Identification) is a unique name shared in the wireless network, The SSID for all devices in the network must be the same.

UI	Status	Network	Security	Application	Management	Diagnosis
WAN						
Bind						
LAN						
WLAN						
▶ WLAN						
TR69						
Qos						
SNTP						
Route						

Wireless -- Basic

This page allows you to configure basic features of the wireless LAN interface. You can enable or disable the wireless interface, hide the network from active scans, set the wireless network name (also known as SSID) and restrict the c based on country requirements. Click "Apply/Save" to configure the basic wireless options

☒ Enable Wireless
☐ Hide Access Point
☐ Clients Isolation
☐ Disable WMM Advertise
☒ Enable WMM

SSID:
 BSSID: 02:10:18:01:00:02

BAND:
 Channel: Current Channel1
 802.11n/EVC:
 Bandwidth: Current Bandwidth:40 Mt
 Control Sideband: Current Control Sideband

Creating WLAN connection

1. enable wireless
2. set ssid name in ssid text box.
3. set the channel ,bandwidth and so on. if you not set ,it will be valued as default.
4. Click Apply/Save

TR69

Introduce

ITMS server

Remote management allows you to make configuration settings from WAN (Wide Area Network) client by Web browser. Access browser interface still requires a user name and password to login.

IP address

Access Internet router IP address. If the specified IP address is 0.0.0.0, then all the hosts can be connected to the DI-624 + A for configuration settings.

Port

Access to the router port number. Example:http://x.x.x.x:8080 ???x.x.x.x is the router's WAN IP address, 8080 is the Web-management interface port.

Set ITMS server configure

letwork>>TR69>>ITMS serv

WAN
Bind
LAN
WLAN
TR69
ITMS server
OLT Auth
Qos
SNTP
Route

Status Network Security Application Management Diagnosis

TR-069 Client-Configuration

WAN Management Protocol (TR-069) allows a Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device

Select the desired values and click "Apply/Save" to configure the TR-069 client options.

Inform ☐ Disable ☒ Enable

Safety Link:

Inform Interval:

ACS URL:

ACS Username:

ACS password:

☐ Connection Request Authentication:

1. Enable inform.
2. set ITMS address int ACS URL.such as
<http://80.80.80.80:9090/ACS-server/ACS> 80.80.80.80 is itms server ip, 8080
is connect port
3. set itms server name and pass.
4. Click Apply/Save

QOS config

QOS

- QoS is a network security mechanism is used to solve issues such as network latency and blocking a technology, QoS refers to the messaging throughput, delay, delay jitter, loss rate performance.

Qos Setup

Rule templates: INTERNET, TR069

Enable QoS: ☒

US bandwidth: 0 kbps

Policy: ☒ PQ ☐ WRR ☐ CAR

DSCP Mark: ☐ TC Mark: ☐ 802-1_P Mark: 0 Mark

Queue	Priority	Enable
Q1	Highest	<input checked="" type="checkbox"/>
Q2	High	<input checked="" type="checkbox"/>
Q3	Middle	<input checked="" type="checkbox"/>
Q4	Low	<input checked="" type="checkbox"/>

Group ID	Queue	Classification	IP Version	Maximum	Minimum	Protocol	DSCP	TC	802.1	Delete	Edit
<div>add class</div> <div>del class</div>											

Traffic Class Edit:

☒ App Class Edit ☐ Traffic Class Edit

App Name: TR069

queue: 1

Confirm

Set QOS configure

1. Set one Rule template in rule template drop down box.
2. Enable QOS in group box.
3. Set the policy for queues.

Security

URL filter

- Use URL refused to the LAN to access a particular Web client computer side. URL is a specific schedule for the regional network and a string. If any section of characters in the URL included in the block will not be accessed. If any section of the URL contains the word in the block, the page will not be displayed.

Config URL filter

Security >> URL Filter >> URL Filter	Status	Network	Security	Application	Management	Diagnosis
<ul style="list-style-type: none"> URL Filter URL Filter Firewall Mac Filter IP Filter 	<p>URL Filter -- Please select the list type first then configure the list entries. Maximum 100 entries can be configured</p> <p>URL Addresss Filter: <input type="radio"/> Enable <input checked="" type="radio"/> Disable</p> <p>URL List Type: <input checked="" type="radio"/> Blacklist <input type="radio"/> Whitelist</p>					

1. Select the group box to enable URL filter.
2. Select the filter type: blacklist or whitelist.
3. Click Apply/Save

Firewall

- A firewall is used to allow or deny packet data through the machine. It works as well as settings and IP filters.

Configure firewall

Configure firewall level on the firewall level page.

Firewall >> Firewall Level	Status	Network	Security	Application	Management	Diagnosis
<ul style="list-style-type: none"> URL Filter Firewall <ul style="list-style-type: none"> Firewall Level DDOS Setup Mac Filter IP Filter 	<p>Choose the fireware level and do corresponding setting.</p> <p>Firewall Level: Middle</p> <p><input type="button" value="Save/Apply"/></p>					

Enable dos attack to set the DOS protection or prevent port scanning on the DDOS Setup page.

> DDOS Setup	Status	Network	Security	Application	Management	Diagnosis
<ul style="list-style-type: none"> URL Filter Firewall <ul style="list-style-type: none"> Firewall Level DDOS Setup 	<p>Attack Protect</p> <p>If you want to set the DOS protection or prevent port scanning ,you must set this item</p> <p><input checked="" type="radio"/> Disable <input type="radio"/> Enable <input type="button" value="Save/Apply"/></p>					

MAC filter

- MAC (Media Access Control) address filtering Based on the user computer's MAC address to allow or deny access to LAN and the Internet. We can filter by MAC Filter to connect to the LAN port users and wireless users.

Configure MAC filter

The screenshot shows the 'Add MAC Filter Rule' configuration page. The left sidebar has a navigation menu with 'Mac Filter' selected. The main content area has a title bar with tabs: Status, Network, Security, Application, Management, and Diagnosis. The 'Security' tab is active. The configuration fields are as follows:

- MAC Filter: ☒ Enable ☐ Disable
- Filter Mode: ☒ Blacklist ☐ Whitelist
- Protocol Type:
- MAC Address: (xx:xx:xx:xx:xx:xx)

Below the fields is an 'Add' button. At the bottom, there is a table with the following structure:

MAC Address	Protocol Type	Delete
-------------	---------------	--------

Below the table is a 'Delete' button.

1. enable MAC filter.
2. select the filter mode :blacklist or white list.
3. select protocol type.
4. set the MAC in the text box.
5. click add to set up one MAC filter or delete to release . one filter.

IP filter

- IP Filter

Use the IP address filter refused to specific IP addresses access to information on the Internet. You can deny specific ports or specific IP address of all ports. The screen will show the defined ports. Want to use them, you can choose edit item. You only need to enter the LAN IP address of the computer to access the Internet can be defined.

- IP

IP address of the client computer in the LAN to access Internet information. You can add an IP range or an IP address.

- Port

use a single port or a port range to define the Internet access. If you do not define a specific port, then all ports will be denied access.

Click the "Security" -> "IP filtering", in default, the firewall is enabled. Firewall is used to prevent files transmission between the Internet and the PC, . Certification of documents can only transfer to LAN side.

- Note

If the modem configuration bridge approach pvc, IP filtering is disabled. IP filtering interface is not displayed. If the modem is not configured to bridge mode pvc, MAC filtering is disabled, MAC filtering interface is not displayed.

Filter Name:	IP Version:	Protocol:	Source IP Address(Range)/Mask:	Source Port:	Destination IP Address(Range)/
--------------	-------------	-----------	--------------------------------	--------------	--------------------------------

Configure IP filter

1. enable IP filter.
2. select filter type:blacklist or whitelist.
3. click add to add one filter.

Application

VOIP

- You can have a call over internet after doing some configuration in this part.

Basic Setup

Figure 8: basic setup about voice interface

on>>VOIP>>Basic Setup

DDNS

Advance NAT

UPnP

VOIP

Basic Setup

Status **Network** **Security** **Application** **Management** **Diagnosis**

Voice -- SIP Basic Configure

Please input SIP parameter, then click "apply" to save.

voice binding interface name: LAN

SIP local port[range:0-65535]: 5058

- In the voice binding interface name, the choose one you have configured for voice

Figure 9: basic setup about voice

Application>>VOIP

DDNS

Advance NAT

UPnP

VOIP

Basic Setup

Log Plot Setup

Voice Media

SIP App

IMS App

Debug Setup

IGMP

MLD

Status **Network** **Security** **Application** **Management** **Diagnosis**

☒ enable primary sip proxy

IP Address 172.24.242.251

Port 5060

☐ enable primary sip external proxy

☒ enable primary SIP registration

IP Address 172.24.242.251

Port 5060

☐ enable second SIP proxy

☐ enable second SIP external proxy

☐ enable second SIP registration

SIP Account	enable account	User Number	authentication user name	authentication password
1	<input checked="" type="checkbox"/>	02164958305	02164958305	*****
2	<input checked="" type="checkbox"/>	02164958306	02164958306	*****

- Check enable primary sip proxy and input the proxy server address to the IP Address option, such as 172.24.242.251,
- Check enable primary sip registration and input the registration address to the IP Address option, for

example 172.24.242.251.

- Check the enable account for both line1 and line2, and then Input the user number to the User Number table respectively
- For the authentication user name and authentication password,input the information which is used for authentication in register or Invite.

Log Plot Setup

Figure 10: digitmap setup

basic digitmap configure

enable basic

digitmap:
basic digitmap(length 1024 character):

[*#]x[0-9*].#|**xx|*x[0-9*].#|*x[0-9*].#|#300#|#500#|[*#]
96#xx.t|[*#]95#xx.t|*99*xx.#xx.t|*66*x[0-9*].#x[0-
9*].t|##|010xxxxxxxx|02xxxxxxxx|0[3-9]xxxxxxxx|0311xxxxxxxx|037

digitmap match mode:

inter-digit long timer: [Unit:S]

first digit timer: [range:5~20, unit: sec]

terminal character trigger mode:

☐ dial out in matching

- input the digitmap you will use to the basic digitmap table

Voice Media

Figure 11: voice media

Voice -- SIP voice media setup

codec and ptime negotiation mode

voice codec--line 1	ptime [unit:ms]	codec priority	enable
G722	20	1 (1-4)	<input checked="" type="checkbox"/>
G711A	20	2 (1-4)	<input checked="" type="checkbox"/>
G711U	20	3 (1-4)	<input checked="" type="checkbox"/>
G729	20	4 (1-4)	<input checked="" type="checkbox"/>

voice codec--line 2	ptime [unit:ms]	codec priority	enable
G722	20	1 (1-4)	<input checked="" type="checkbox"/>
G711A	20	2 (1-4)	<input checked="" type="checkbox"/>
G711U	20	3 (1-4)	<input checked="" type="checkbox"/>
G729	20	4 (1-4)	<input checked="" type="checkbox"/>

- You can choose the ptime and codec priority for the two line

SIP Application

Figure 12: Sip Application

line	1	2
call waiting	<input type="checkbox"/>	<input type="checkbox"/>
call forwarding number	<input type="text"/>	<input type="text"/>
unconditional call forwarding	<input type="checkbox"/>	<input type="checkbox"/>
busy call forwarding	<input type="checkbox"/>	<input type="checkbox"/>
No answer call forwarding	<input type="checkbox"/>	<input type="checkbox"/>
MWI voicemail message	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous call blocking	<input type="checkbox"/>	<input type="checkbox"/>
Anonymous call	<input type="checkbox"/>	<input type="checkbox"/>
Do Not Disturb	<input type="checkbox"/>	<input type="checkbox"/>
Call Transfer	<input type="checkbox"/>	<input type="checkbox"/>
Conference Call	<input type="checkbox"/>	<input type="checkbox"/>
call waiting tone play count	5000	5000

- You can enable the corresponding table when you need a supplementary service

IGMP

IGMP Settings

- You can make the user can watch IPTV through the router program by set the IGMP Snooping, IGMP Proxy function.

IGMP Snooping Configuration

This page allows you to enable or disable IGMP Snooping function.

☒ Enable IGMP Snooping

[Save/Apply](#)

Enable IGMP Snooping

- Select the group box to enable or disable IGMP Snooping.

Diagnosis

Line Diagnosis

sis>>Network diagnosis>>L

Network diagnosis

- Line Diagnosis
 - Ping Test
 - Tracert Test
 - Inform Test

StatusNetworkSecurityApplicationManagement**Diagnosis**

Diagnostic Tests

Your ONU is capable of testing your Line connection. The individual tests are listed below. If a test displays a fail stat "Rerun Diagnostic Tests" at the bottom of this page to make sure the fail status is consistent.

Test the connection to your local network

Test eth0 connection:	Fail	Help
Test eth1 connection:	Fail	Help
Test eth2 connection:	Pass	Help
Test eth3 connection:	Fail	Help
Test wireless connection:	Pass	Help

Rerun Diagnostic Tests

Ethernet connection Test

Pass	Show that your computer's Ethernet port is connected to the LAN port of the ONU. ONU on the LAN indicator lights or flashes indicates that the Ethernet connection, the test was successful.
Failure	That ONU does not detect the computer's Ethernet interface.

Ping Test

The Ping test sends an IP ping to an IP address. The ping can be used to determine if another device can be accessed from the ONU.

gnosis>>Network diagnosis

Network diagnosis

- Line Diagnosis
- Ping Test**
- Tracert Test
- Inform Test

StatusNetworkSecurityApplicationManagement**Diagnosis**

Ping Diagnosis

This page is used for ping test

Interface: LAN/br0


Destination Ip address or host name:: 192.168.1.5

Start

The result info:

ping to 192.168.1.5 [192.168.1.5]
PING 192.168.1.5 (192.168.1.5): 56 data bytes
--- 192.168.1.5 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
Network is unreachable!

Inform Test

 >>Network diagnosis>>Info

Network diagnosis

- Line Diagnosis
- Ping Test
- Tracert Test
- Inform Test

StatusNetworkSecurityApplicationManagement**Diagnosis**

Manual Inform:

Manual report Inform Test, need to wait for 12s.

Test

- Click on the "test " to test the CPE to the ACS of the reported situation.