OT-4020VW GEPON ONU User Manual

Version: V1.2

CONTENT

1. Product Description

2. Network Configuration and Management Introduction

3. Status

4. INTERNET

5. Security

6. Application

7. Management

8. Diagnosis – Network Diagnosis

9. Help

1. Product Description

The OT-4020VW is a Telecom grade GEPON Optical Network Unit (ONU) based on IEEE802.3ah Gigabit EPON Standard. It comes with GEPON WAN interface, 4 Port IEEE802.11n Wireless Router and 2 FXS Port Analog Telephone adaptor for Fiber To The Home Networking and VoIP applications.

1.1. Product Application

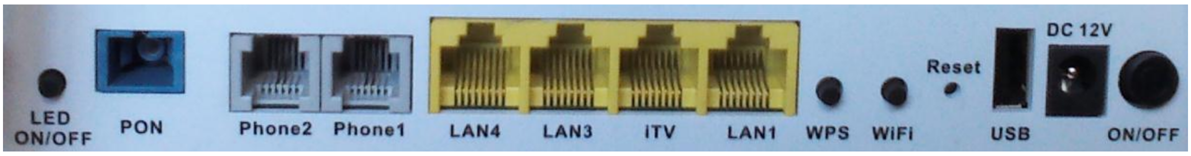
Fiber To The Home
Home Gateway
SOHO Gateway
IPTV Application
High Speed Broadband Sharing
Voice, Video Stream and Data Transmission
Voice Over IP application
Fax Over IP application

1.2. Product Features

- ✧ Fully Compatible with IEEE802.3ah Gigabit Epon Standard
- ✧ Offers 1 Gepon SC port for uplinking, 1.25Gbps
- ✧ Sensibility of Gepon Optical port: -2dBm to -27dBm
- ✧ Fiber Ratio: Different Fiber Ratio applies to different transmission distance, 1:64 MAX.
- ✧ Support 1.8Gbps Backplane bandwidth
- ✧ Offers 4 10/100Base-Tx LAN port for downlinking to User PC, VoIP Phone, IPTV Setup box
- ✧ Built-in 2 FXS Port VoIP Phone Adaptor
- ✧ Support SIP protocol, two SIP accounts can be registered simultaneously
- ✧ Two calls can be made/received simultaneously
- ✧ Support auto-provisioning

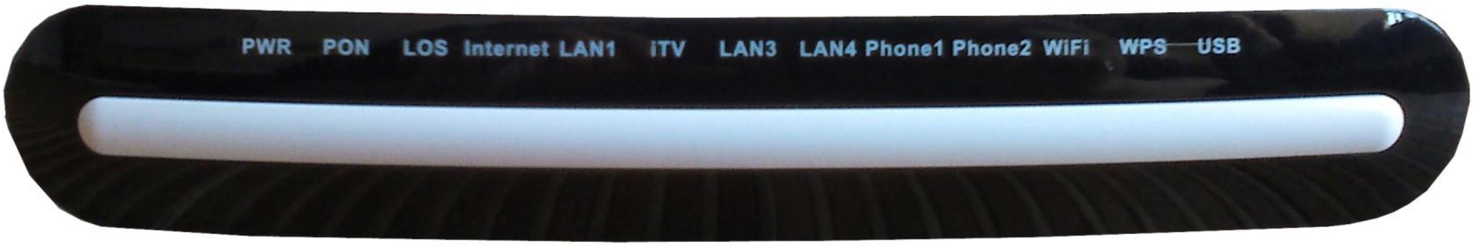
- Support G.711,G.723.1,G.729A–8 kbps,G.726,G.722, ILBC voice codecs
- Support DTMF Tone Detection, DTMF Tone Relay, Multiple Calling Tone, FSK Caller ID
- Support Calling line Identification Presentation and Calling line Identification Restriction
- Support call forwarding, call hold features
- Support QOS and TOS to ensure voice packets pass through in priority
- Support RFC62 Echo protocol
- Support SIP V1, V2 (RFC3261, RFC3262, RFC3264, RFC3265)
- Built-in IEEE802.11n Wireless Router,
- support wireless transmission rate of 150Mbps, 2.4GHz
- Comes with 4 10/100Base-Tx LAN ports
- Offers 1 USB host port
- Comes with 2 external Antenna of 5db
- Wireless Range support: Outdoor: 150m, Indoor: 100m
- Support DHCP, Static IP and PPPOE
- Support DHCP Server, DHCP Relay, DHCP Client
- Support Static Routing from source IP to destination IP
- Support firewall, NAT, NAPT, UPnP
- Support DDNS, DMZ Host, Port Forwarding
- Support 64/128 bit WEP, IEEE802.1x, WPA and WPA2 authentications
- Support Multiple SSID broadcasting, Hidden SSID and Wifi Protocol Setup (WPS),
- Support Automatically choose the best signal channel
- Support STA mutual isolation and ACL table based on MAC Accesses
- Support Wifi Multimedia (WMM), enhanced QOS for multimedia packets
- Support TR069 management for large Internet Service Providers deploy remote management and maintenance.
- Support FTP/TFTP/HTTP Auto Provision for small and medium ISP deploying remote management and maintenance.
- Support SNTP Simple Network Time Protocol
- Support Loop Detection to prevent Loop of network.
- Comes with live LED Indicators for working status, standby status, power, Wifi connectivity, fiber Link, etc
- Desktop design, Plastic housing,
- External Power Supply,
- Impulse Power Supply, AC 96 – 260V, DC 12V, 2A
- Support Asia, Europe, U.S, U.K, AU standard power plugs

1.3. Rear View & Rear Interface Description



Port	Description
LED ON/OFF	Turn on/Turn off LED Indicators
PON	1.25G GEPON SC Port
Phone1, Phone2	Standard RJ11 ports for VoIP
LAN1, iTV, LAN 3, LAN 4	10/100Base-Tx Ethernet LAN Ports
iTV	10/100Base-Tx Ethernet Port, can be specified for IPTV
WPS	Enable/Disable WPS
WiFi	Enable/Disable Wireless AP
Reset	Restore to factory default settings
USB	USB 2.0 Host Port
DC 12V	12V, 1.5A DC Power input, connecting to Power Adaptor
ON/OFF	Switch for Power ON/OFF

1.4. LED Description:



LED	Color	Status	Description
PWR	Green	Light	ONU is powered
		Extinguished	ONU is not powered
LOS	RED	Extinguished	ONU receives good GEPON Signals
		Flashing	ONU receives poor GEPON Signals
PON	GREEN	Light	ONU logic link is established successful
		Extinguished	ONU logic link is not established
		Flashing	ONU is trying to establish a link with OLT
WiFi	GREEN	Light	Wireless LAN is activated
		Extinguished	Wireless LAN is not activated or disabled
		Flashing	Data Transmission over Wireless LAN interface
WPS	Multi Color	Extinguished	WPS is not activated or disabled
		Yellow LED Flashing	Light for 2s, Extinguished for 1s, accepting wireless LAN registration after pressing the WPS button
		RED LED Flashing	Light or Extinguished in an time interval of 1s, fail to accept Wireless LAN registration
		RED LED Flashing	Flashing 5 times with time interval of 1s, Extinguished for 0.5s, accepting two or multiple Wireless LAN registration
		GREEN LED Light	Lights for more than 5 minutes, accepting Wireless LAN registration successful
USB	GREEN	Light	USB is connected and working on Host mode
		Extinguished	USB is not connected
		Flashing	Data Transmission over USB port
Internet	Green	Light	Successfully connected to Internet
		Extinguished	Not connected to Internet
Phone1, 2	GREEN	Light	Analog phone connected is in use
		Extinguished	Analog phone connected is not in use
		Flashing	Incoming call
LAN1/3/4/ITV	GREEN	Light	Connected to Ethernet LAN devices
		Extinguished	Not connected to any Ethernet LAN devices
		Flashing	Data Transmission over Ethernet LAN Interfaces

1.5. Wireless Description

Built-in IEEE802.11n Wireless Router,
Support wireless transmission rate of 150Mbps, 2.4GHz
Comes with 2 external Antenna of 5db
Wireless Range support: Outdoor: 150m, Indoor: 100m
Support 64/128 bit WEP Open & Shared, IEEE802.1x, WPA and WPA2 wireless authentications
Support TKIP, AES or TKIP + AES wireless encryption
Support Multiple SSID broadcasting, Hidden SSID and Wifi Protected Setup (WPS),
Support Automatically choose the best signal channel
Support Wifi Multimedia (WMM), enhanced QOS for multimedia packets
Support Wireless Transmission Power control

1.6. Compliance

FCC Class B
CE Mark
Rohs

1.7. Product Standards

Support IEEE802.3ah standard GEPON
Support OAM based on IEEE802.3ah standard, support CTC2.1, 2.2
Support FEC coding
Support 128bit AES Encryption over logic link

RFC2516 PPP Over Ethernet（ PPPoE ）

RFC1332 PPP Internet Protocol Control Protocol
RFC894 A Standard for the Transmission of IP Datagrams over Ethernet Networks
RFC1042 A Standard for the Transmission of IP Datagrams over IEEE 802 Networks
ALG
IEEE802.3
IEEE802.3u
IEEE 802.11b
IEEE 802.11g
RFC 2327, SDP: Session Description Protocol
RFC 3261, SIP: Session Initiation Protocol
RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)
RFC 3264, An Offer-Answer Model with the Session Description Protocol (SDP)
RFC 3311, The Session Initiation Protocol (SIP) UPDATE Method
RFC 3515, The Session Initiation Protocol (SIP) Refer Method
RFC 3550, RTP: A Transport Protocol for Real-Time Applications
RFC 2617, HTTP Authentication: Basic and Digest Access Authentication
RFC 2833, RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals
RFC 3842, A Message Summary and Message Waiting Indication Event Package for the Session Initiation Protocol (SIP)

1.8. Working environment

Operation Temperature: 0℃ - 45℃
Operation Humidity: 10% - 90%
Standby Temperature: -40℃ - 70℃
Standby Humidity: 5% - 90% RH

1.9. Recommended Operation System

Processor: Pentium 233MHz

Memory：64MB

LAN: 10/100Base-Tx LAN Card
Windows 9x, Windows2000, Windows XP, Windows ME, Windows NT, Windows 7

1.10. Safety Notice

Please read the following safety notices before installing or using this ONU. They are crucial for the safe and reliable operation of the device.

- ✓ Please use the external power supply that is included in the package. Other powers supplies may cause damage to the device, affect the behavior or induce noise.
- ✓ Before using the external power supply in the package, please check with home power voltage. Inaccurate power voltage may cause fire and damage.
- ✓ Please do not damage the power cord. If power cord or plug is impaired, do not use it, it may cause fire or electric shock.
- ✓ The plug-socket combination must be accessible at all times because it serves as the main disconnecting device.
- ✓ Do not drop, knock or shake it. Rough handling can break internal circuit boards.
- ✓ Do not install the device in places where there is direct sunlight. Also do not put the device on carpets or cushions. It may cause fire or breakdown.
- ✓ Avoid exposure the ONU to high temperature, below 0℃ or high humidity. Avoid wetting the unit with any liquid.
- ✓ Do not attempt to open it. Non-expert handling of the device could damage it. Consult your authorized dealer for help, or else it may cause fire, electric shock and breakdown.
- ✓ Do not use harsh chemicals, cleaning solvents, or strong detergents to clean it. Wipe it with a soft cloth that has been slightly dampened in a mild soap and water solution.
- ✓ When lightning, do not touch power plug or device line, it may cause an electric shock.
- ✓ Do not install this device in an ill-ventilated place.
- ✓ You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

2. Network Configuration and Management Introduction

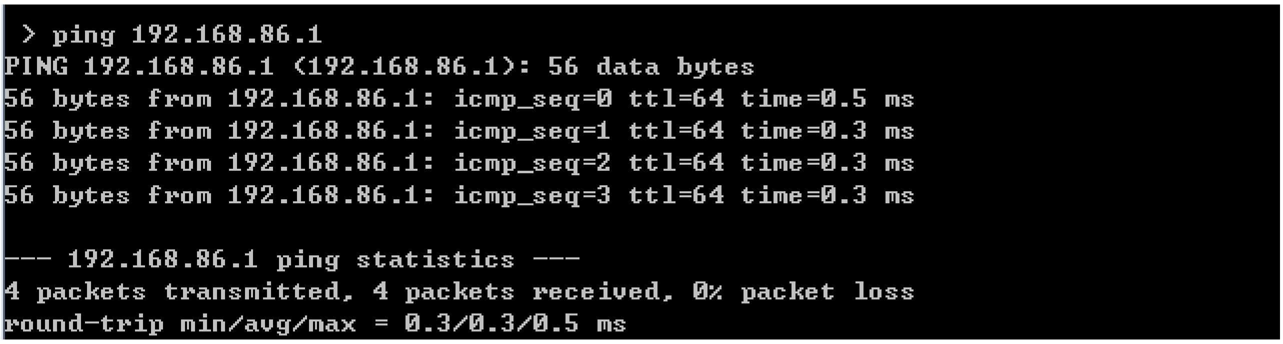
2.1. Prepare to log in OT-4020VW ONU

Before to log in the OT-4020VW ONU, please make sure the connections in between the ONU and the PC is correct.

2.1.1. Configure the IP address of your Manage PC to **192.168.86.x** (2-254), subnet **255.255.255.0**, Gateway: **198.168.86.1**

2.1.2. Connect your Manage PC to the OT-4020VW ONU's Ethernet LAN interface

2.1.3. Ping 192.168.86.1 (192.168.86.1 is the default manage IP of the OT-4020VW ONU)



```
 > ping 192.168.86.1
PING 192.168.86.1 (192.168.86.1): 56 data bytes
56 bytes from 192.168.86.1: icmp_seq=0 ttl=64 time=0.5 ms
56 bytes from 192.168.86.1: icmp_seq=1 ttl=64 time=0.3 ms
56 bytes from 192.168.86.1: icmp_seq=2 ttl=64 time=0.3 ms
56 bytes from 192.168.86.1: icmp_seq=3 ttl=64 time=0.3 ms

--- 192.168.86.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.3/0.3/0.5 ms
```

Notice: Do not power off the ONU when configuring the ONU through WEB interface. Any termination of power could cause damage to the OT-4020VW ONU.

2.2. Default Logon Information

Default Management IP address: 192.168.86.1

The OT-4020VW has two main user rights,

'**admin**' is the super administrator that has all authorities to configure the ONU.

'**user**' is the user for subscribers, which is only authorized to view the status of ONU and configure DHCP server.

Please use Super Admin to log in and configure the OT-4020VW ONU.

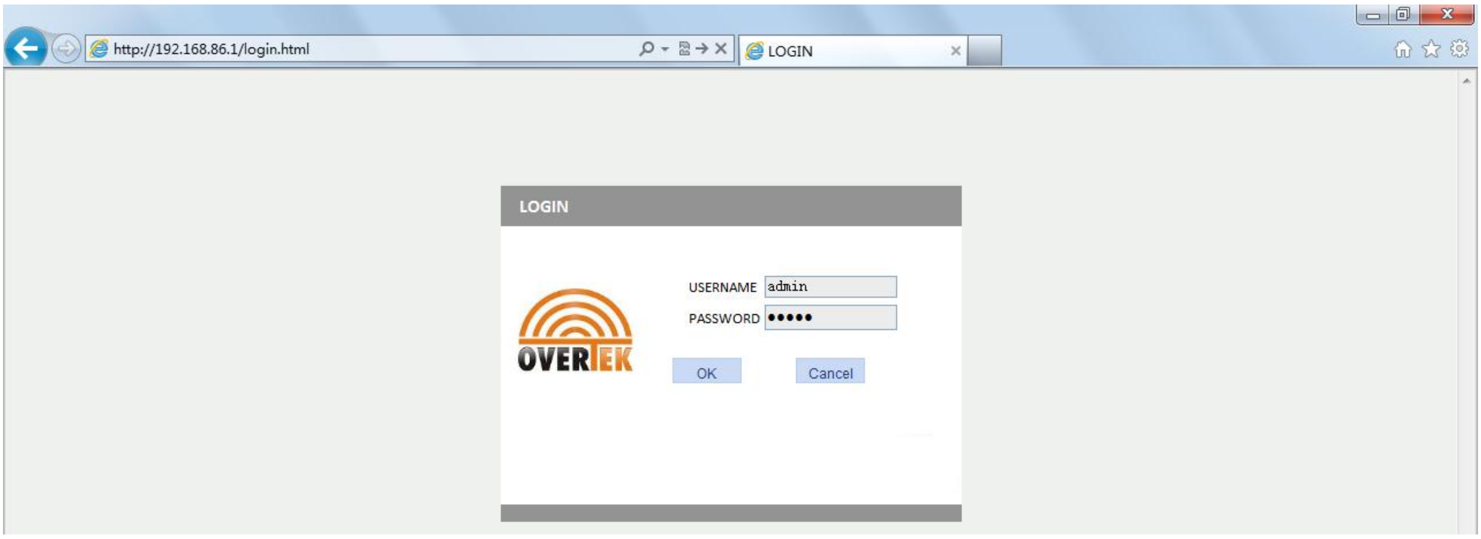
Super Administrator: admin
Password: admin

Subscriber Administrator: user
Password: user

2.3. log in the OT-4020VW GEPON ONU:

2.3.1. Open a browser, input ' 192.168.86.1 ', press ' Enter '

2.3.2. Input ' admin ' as the user name, and ' admin ' as the password, press ' Enter '



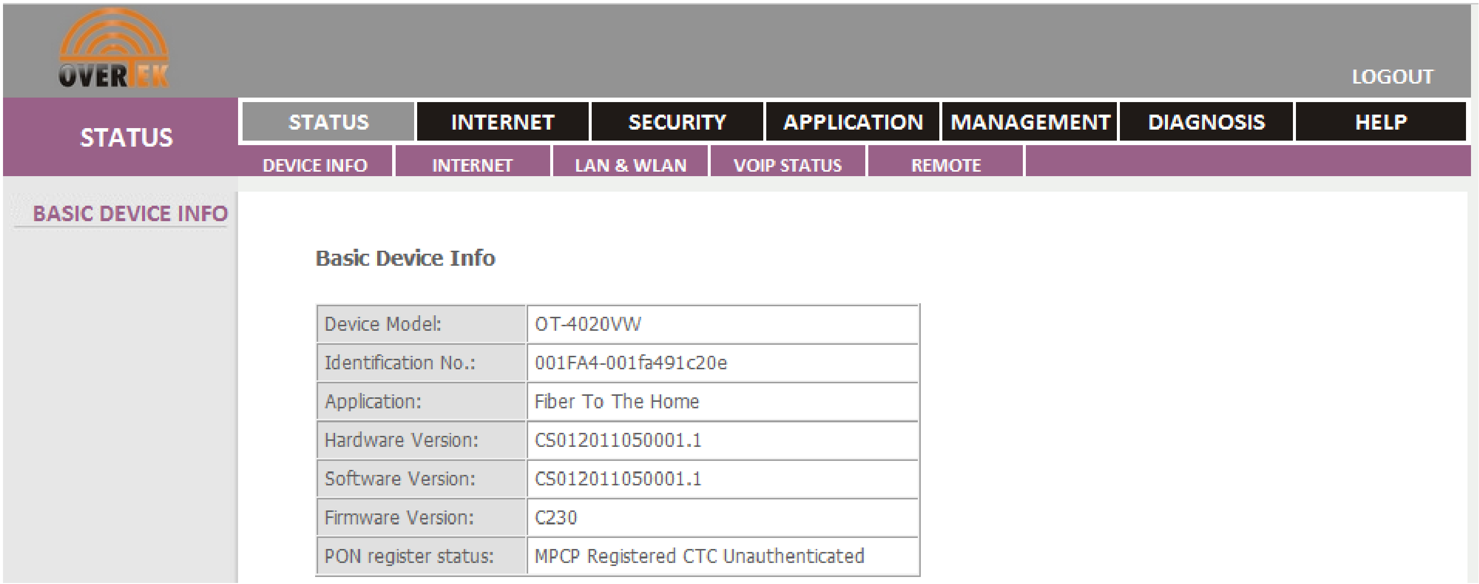
After log in with the Super admin, you can inquiry, configure or modify the settings for the OT-4020VW ONU. For some settings, it’s mandatory to reboot the ONU to take the configuration into effect.

3. Status

After log into the OT-4020VW ONU, you will be direct to the ‘ Status ‘ page. There are 5 sub-options, ‘ Device Info ‘, ‘INTERNET’, ‘LAN & WLAN ’, ‘VoIP Status’, ‘ Remote ‘ under the ‘ Status ‘ page.

3.1. Device Info

Click the ‘ **Device Info** ‘ sub-option, you will see the product information as below:



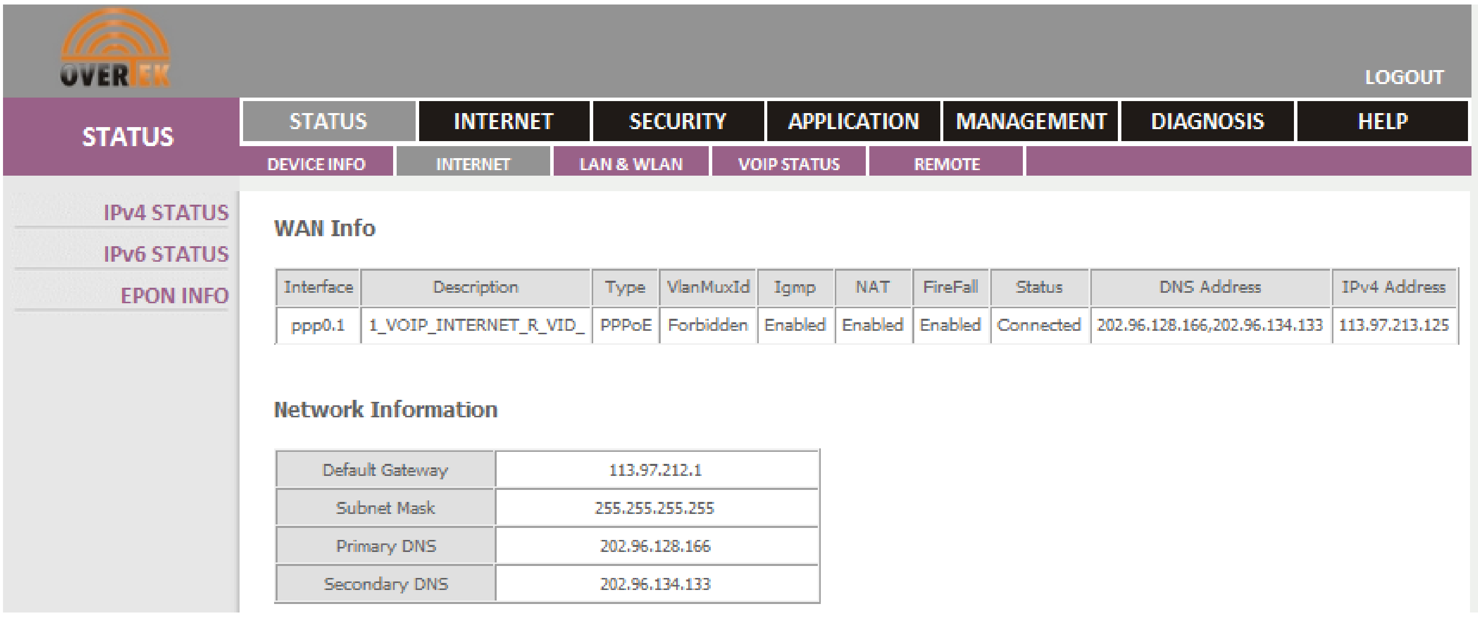
Basic Device Info

Device Model:	OT-4020VW
Identification No.:	001FA4-001fa491c20e
Application:	Fiber To The Home
Hardware Version:	CS012011050001.1
Software Version:	CS012011050001.1
Firmware Version:	C230
PON register status:	MPCP Registered CTC Unauthenticated

3.2. INTERNET

3.2.1. IPV4 Status

Click the '**INTERNET'** – ' **IPV4 Status** ', you will see the IPV4 Internet connection status as below:



WAN Info

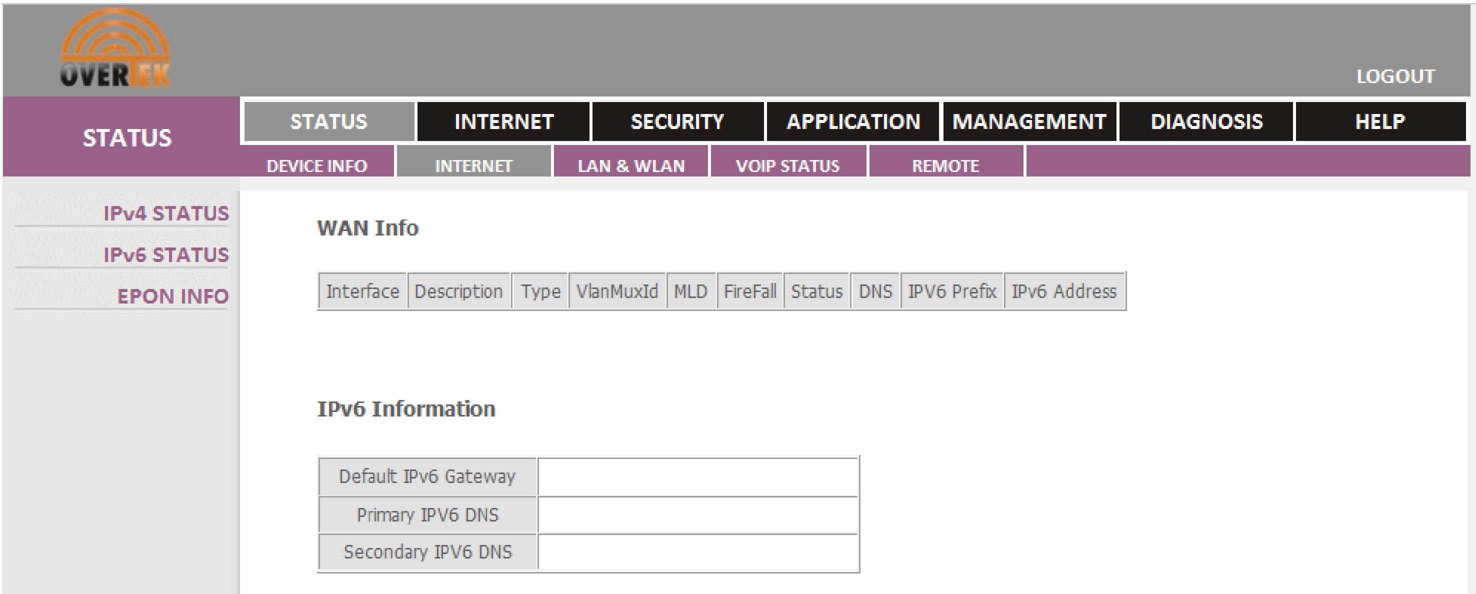
Interface	Description	Type	VlanMuxId	Igmp	NAT	FireFall	Status	DNS Address	IPv4 Address
ppp0.1	1_VOIP_INTERNET_R_VID_	PPPoE	Forbidden	Enabled	Enabled	Enabled	Connected	202.96.128.166,202.96.134.133	113.97.213.125

Network Information

Default Gateway	113.97.212.1
Subnet Mask	255.255.255.255
Primary DNS	202.96.128.166
Secondary DNS	202.96.134.133

3.2.2. IPV6 Status

Click the ' **INTERNET** ' – ' **IPV6 Status** ', you will see the IPV6 internet connection status as below:
If you are connecting through IPV4, there will be no IPV6 internet connection status shown.



WAN Info

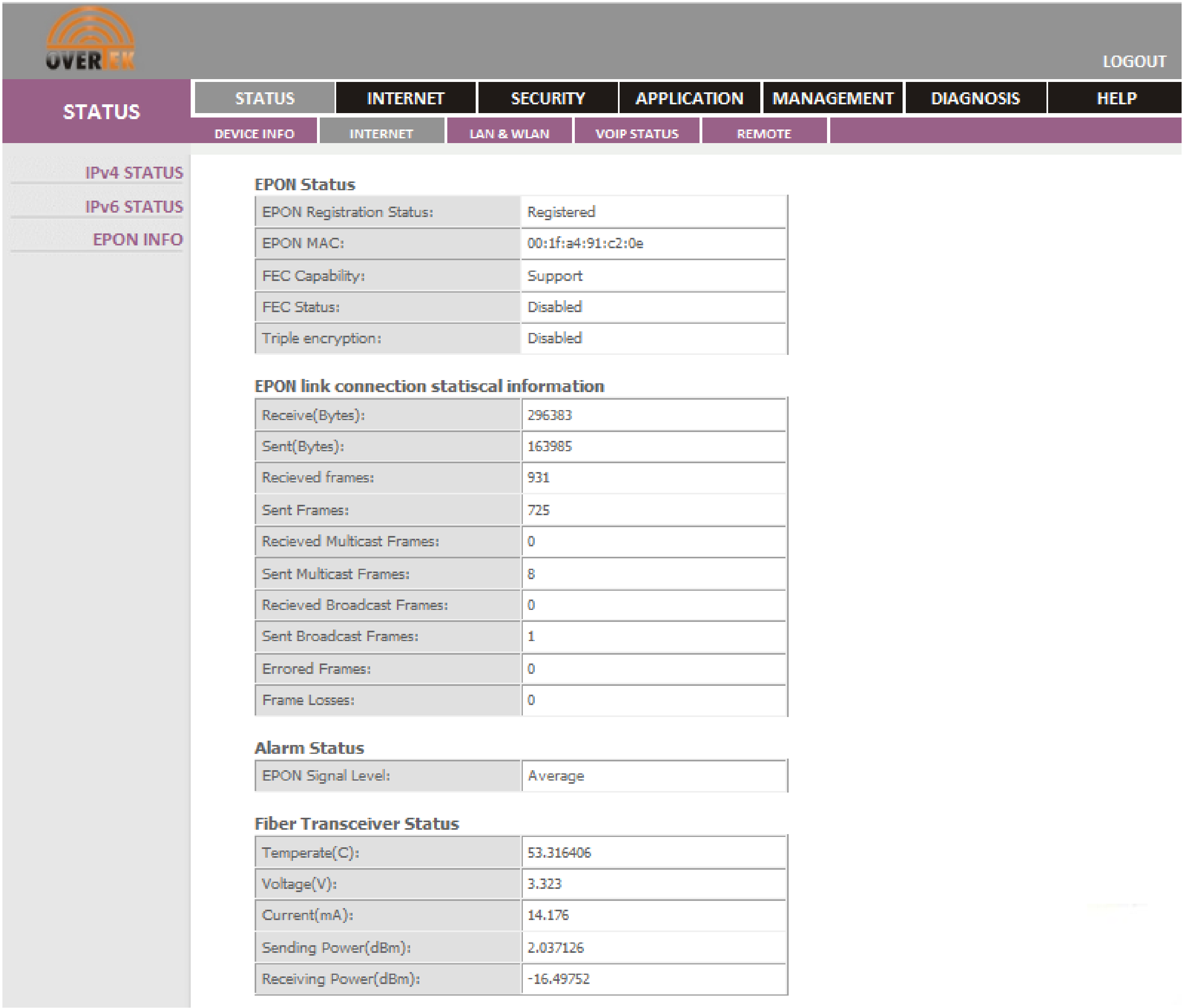
Interface	Description	Type	VlanMuxId	MLD	FireFall	Status	DNS	IPV6 Prefix	IPv6 Address

IPv6 Information

Default IPv6 Gateway	
Primary IPV6 DNS	
Secondary IPV6 DNS	

3.2.3. EPON Info

Click the ‘**INTERNET** ‘ – ‘ **EPON Info** ‘, you can see ‘**EPON STATUS**’, ‘**EPON link connection statiscal information**’, ‘ **Alarm Status** ‘ and ‘ **Fiber Transceiver Details** ’ details as below:



EPON Status

EPON Registration Status:	Registered
EPON MAC:	00:1f:a4:91:c2:0e
FEC Capability:	Support
FEC Status:	Disabled
Triple encryption:	Disabled

EPON link connection statiscal information

Receive(Bytes):	296383
Sent(Bytes):	163985
Recieved frames:	931
Sent Frames:	725
Recieved Multicast Frames:	0
Sent Multicast Frames:	8
Recieved Broadcast Frames:	0
Sent Broadcast Frames:	1
Errored Frames:	0
Frame Losses:	0

Alarm Status

EPON Signal Level:	Average

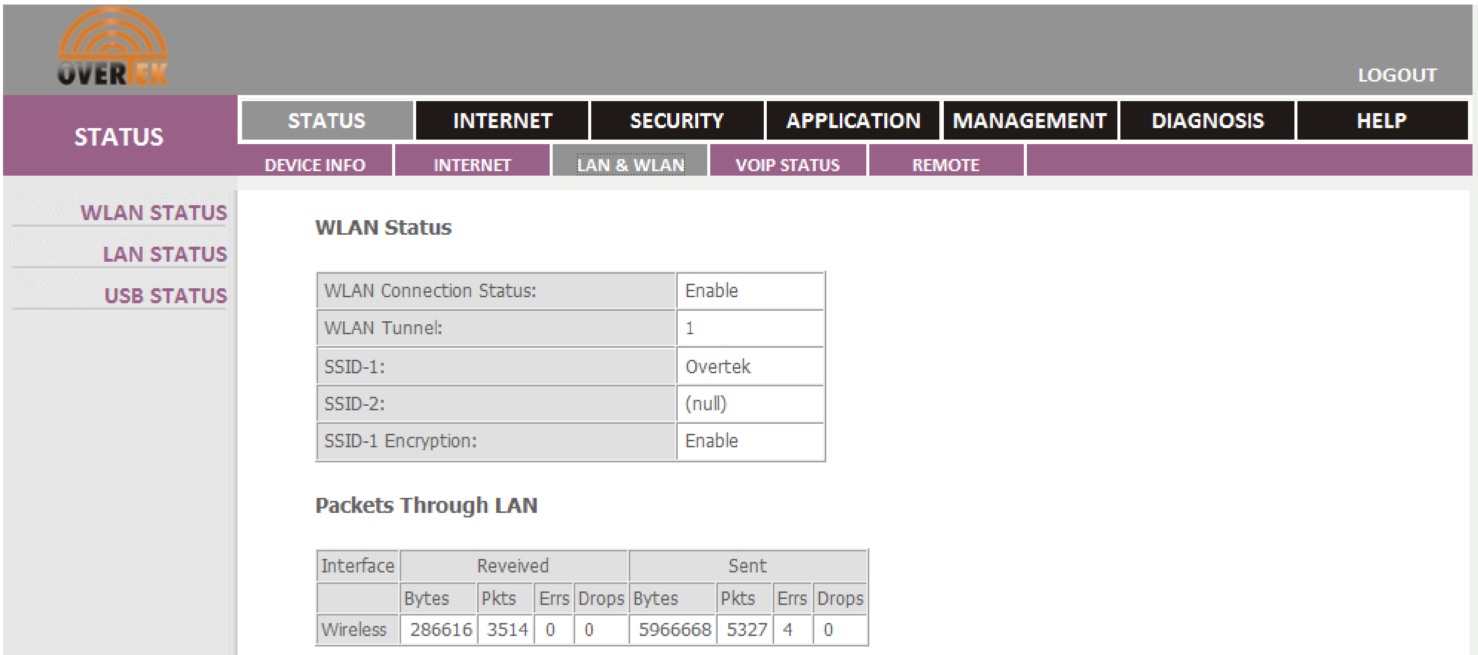
Fiber Transceiver Status

Temperate(C):	53.316406
Voltage(V):	3.323
Current(mA):	14.176
Sending Power(dBm):	2.037126
Receiving Power(dBm):	-16.49752

3.3. LAN & WLAN

3.3.1. WLAN Status

Click the ‘ **LAN & WLAN** ‘ – ‘**WLAN Status** ‘, you will see the Wireless LAN connection information as below:



WLAN Status

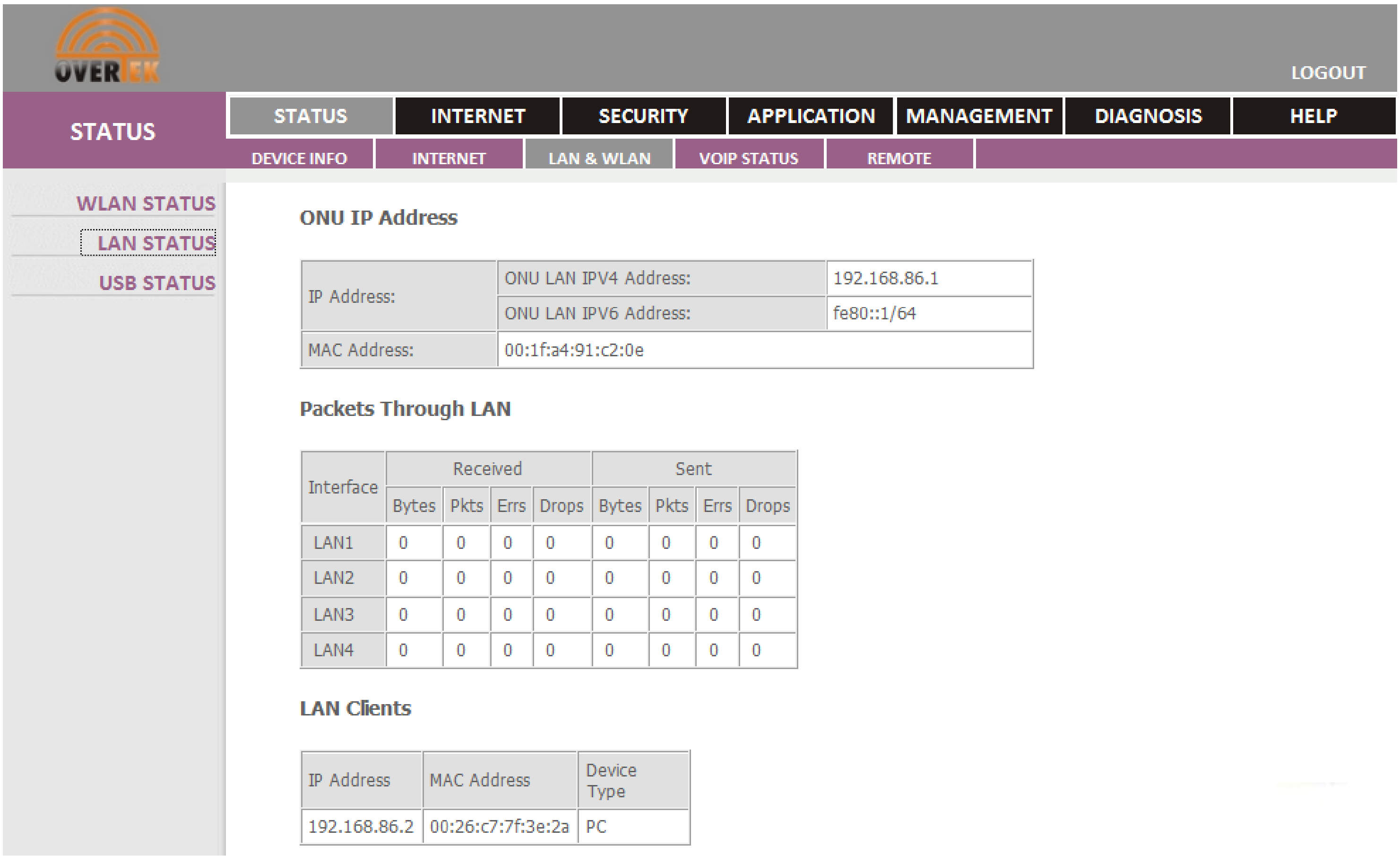
WLAN Connection Status:	Enable
WLAN Tunnel:	1
SSID-1:	Overtek
SSID-2:	(null)
SSID-1 Encryption:	Enable

Packets Through LAN

Interface	Reveived				Sent			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
Wireless	286616	3514	0	0	5966668	5327	4	0

3.3.2. LAN Status

Click the ‘ **LAN & WLAN** ’ – ‘**LAN STATUS** ‘, you will see the ‘ **ONU IP Address** ‘, ‘**Packets Through LAN** ‘ , ‘**LAN Clients**’ information as below:



ONU IP Address

IP Address:	ONU LAN IPV4 Address:	192.168.86.1
	ONU LAN IPV6 Address:	fe80::1/64
MAC Address:	00:1f:a4:91:c2:0e	

Packets Through LAN

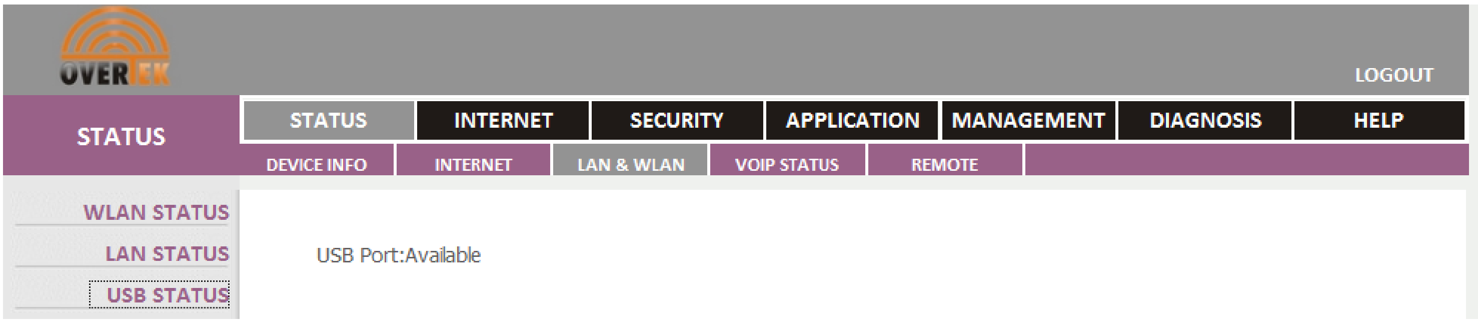
Interface	Received				Sent			
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Errs	Drops
LAN1	0	0	0	0	0	0	0	0
LAN2	0	0	0	0	0	0	0	0
LAN3	0	0	0	0	0	0	0	0
LAN4	0	0	0	0	0	0	0	0

LAN Clients

IP Address	MAC Address	Device Type
192.168.86.2	00:26:c7:7f:3e:2a	PC

3.3.3. USB STATUS

Click the ' **LAN & WLAN** ' – '**USB STATUS**', you will see the connection status for the USB host port.



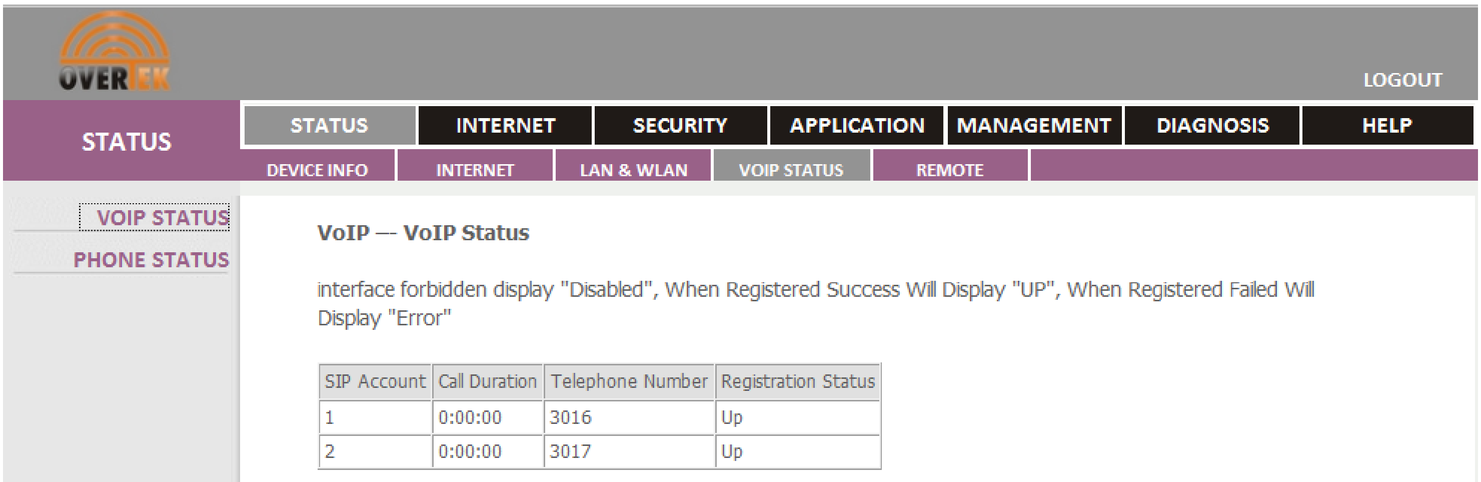
USB Port:Available

3.4. VoIP Status

Click the ' **VoIP Status** ' – '**VoIP Status**', you will see the registration status for VoIP.

If the status is '**up**', VoIP is already registered to the SIP server successfully.

If the status is '**down**', VoIP is not registered to the SIP server.



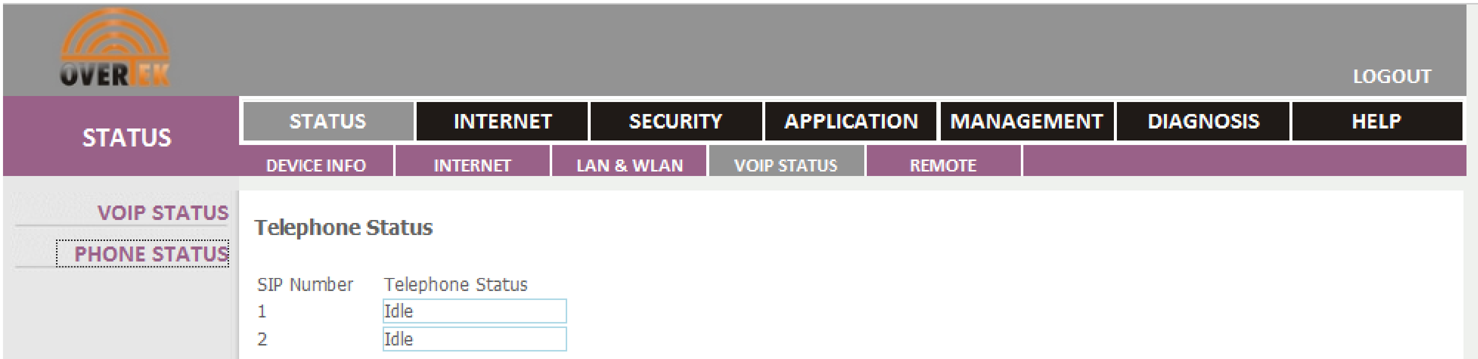
VoIP — VoIP Status

interface forbidden display "Disabled", When Registered Success Will Display "UP", When Registered Failed Will Display "Error"

SIP Account	Call Duration	Telephone Number	Registration Status
1	0:00:00	3016	Up
2	0:00:00	3017	Up

3.4.1. Phone Status

Click the 'Click the ' **VoIP Status** ' – '**PHONE Status'**, you will see the if the SIP accounts are free to use or not.



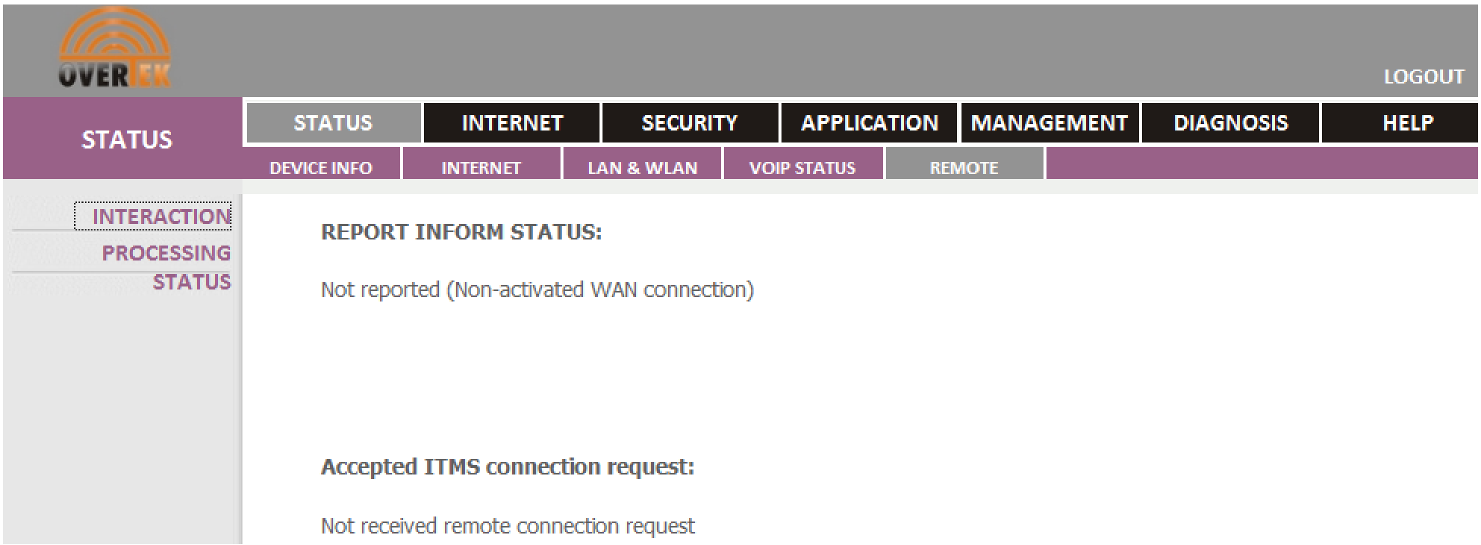
Telephone Status

SIP Number	Telephone Status
1	Idle
2	Idle

3.5. Remote Status

3.5.1. Interaction

Click ‘ **Status** ’ – ‘ **REMOTE** ’ – ‘**Interaction** ‘, you can check the status for the remote interaction established with the remote management ACS Server. This function is for TR069.



REPORT INFORM STATUS:

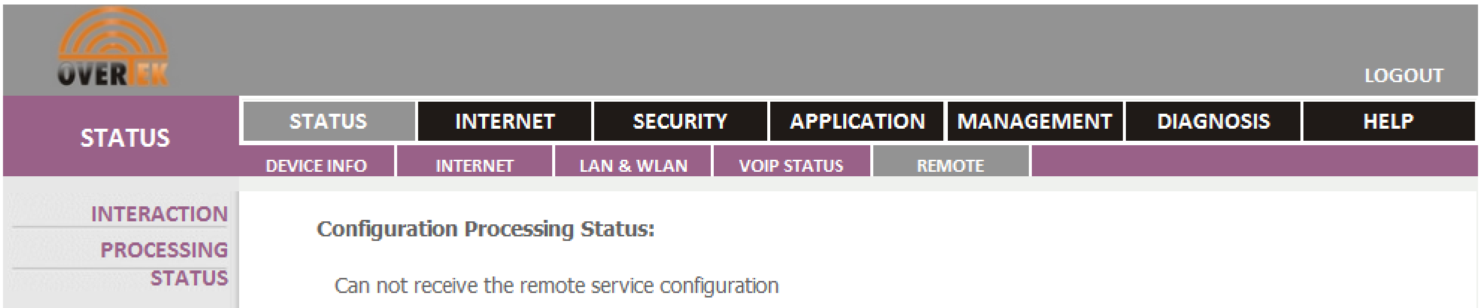
Not reported (Non-activated WAN connection)

Accepted ITMS connection request:

Not received remote connection request

3.5.2. Processing Status

Click ‘ **Status** ’ – ‘ **REMOTE** ’ – ‘**Processing Status**‘,
You can check the status for the remote TR069 ACS Server processing status.



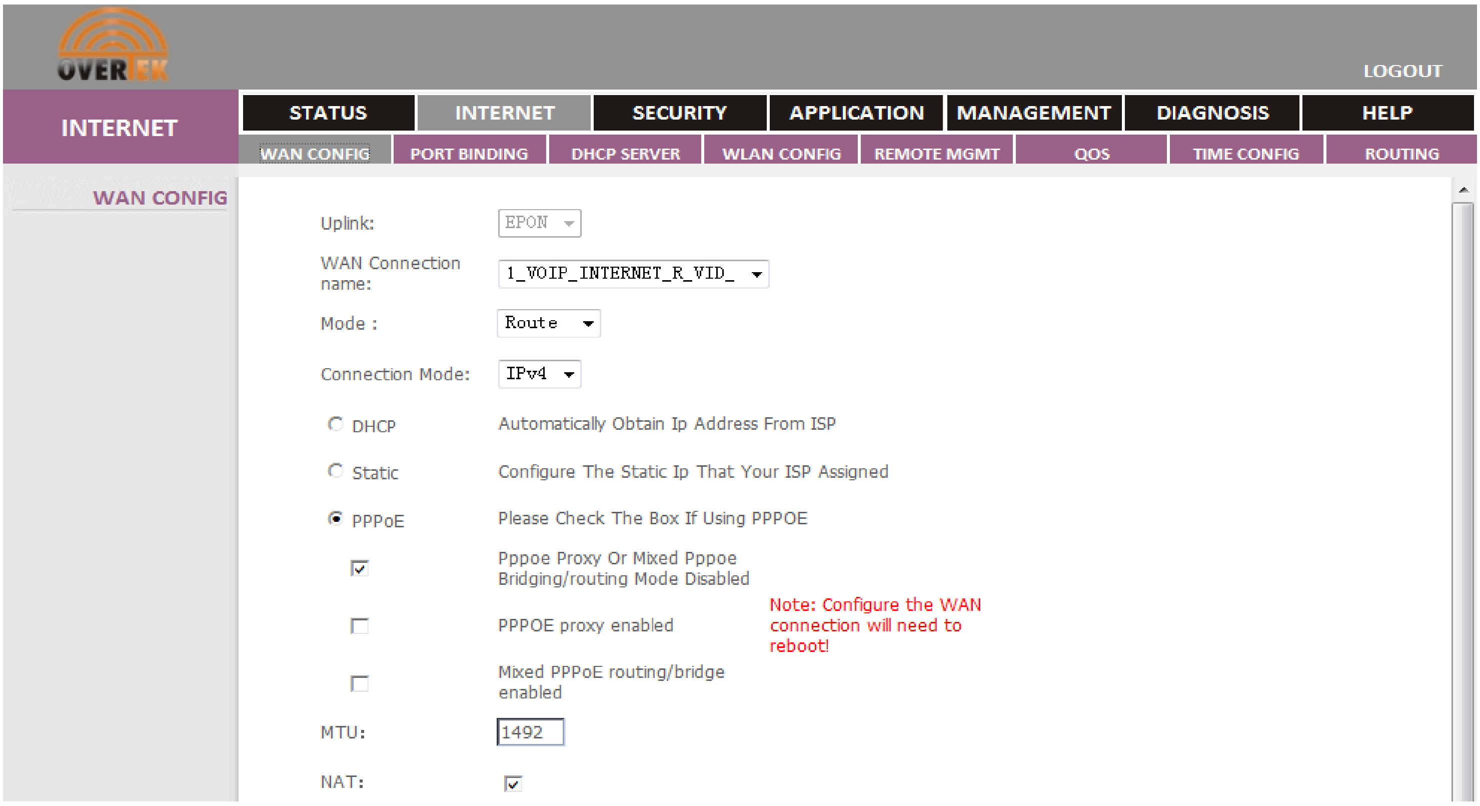
Configuration Processing Status:

Can not receive the remote service configuration

4. INTERNET

4.1. WAN Config

Click ‘ **INTERNET** ‘ – ‘ **WAN Config** ‘ to configure the internet access/WAN access for your OT-4020VW GEPON ONU. You can configure PPPOE, DHCP, Static IP, VLAN as your internet connection mode.



Uplink: EPON

WAN Connection name: 1_VOIP_INTERNET_R_VID_

Mode : Route

Connection Mode: IPv4

○ DHCP Automatically Obtain Ip Address From ISP

○ Static Configure The Static Ip That Your ISP Assigned

● PPPoE Please Check The Box If Using PPPOE

☑ Pppoe Proxy Or Mixed Pppoe Bridging/routing Mode Disabled

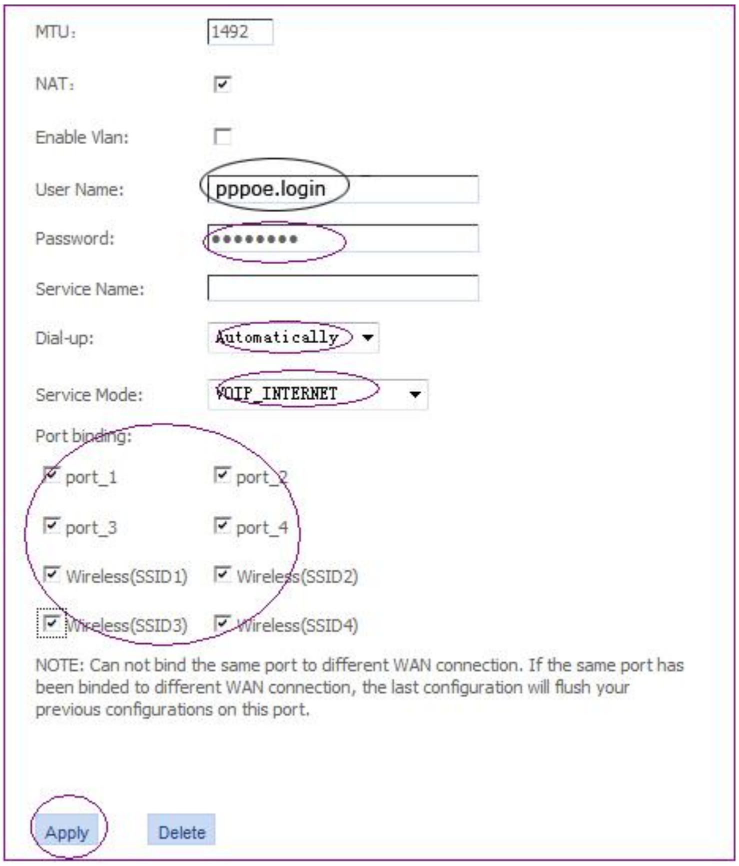
□ PPPOE proxy enabled

□ Mixed PPPoE routing/bridge enabled

Note: Configure the WAN connection will need to reboot!

MTU: 1492

NAT: ☑



MTU: 1492

NAT: ☑

Enable Vlan: □

User Name: pppoe.login

Password: ••••••••

Service Name:

Dial-up: Automatically

Service Mode: VOIP_INTERNET

Port binding:

☑ port_1 ☑ port_2

☑ port_3 ☑ port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2)

☑ Wireless(SSID3) ☑ Wireless(SSID4)

NOTE: Can not bind the same port to different WAN connection. If the same port has been binded to different WAN connection, the last configuration will flush your previous configurations on this port.

Mode: You can use either ‘Route ‘ or ‘ Bridge ‘ mode.

Connection Mode: This option is for defining either to use IPV4 or IPV6 mode. By default, it’s IPV4 mode.

DHCP: On DHCP mode, you will obtain a dynamic IP from your ISP.

STATIC: This option is for Static IP, if you select this option, you need to enter the Static IP Address, Subnet Mask, Gateway and DNS information.

PPPOE: On PPPOE mode, you need to enter the PPPOE user name and password which are assigned by your ISP.

MTU: Max Transmission Unit, this option defines the max size of the packet that will go through the ONU. The default value is 1492.

NAT: Select to enable NAT

Enable VLAN: Check the box to enable VLAN, you need to enter the IEEE802.1Q VLAN ID if VLAN is enabled.

802.1P: If you want to use IEEE802.1P QOS, please select this option. You can also choose the QOS level here.

User Name: Your PPPOE user name

Password: Your PPPOE password

Service Name: The service name of your ISP

Dial-up: You can use default automatically connect

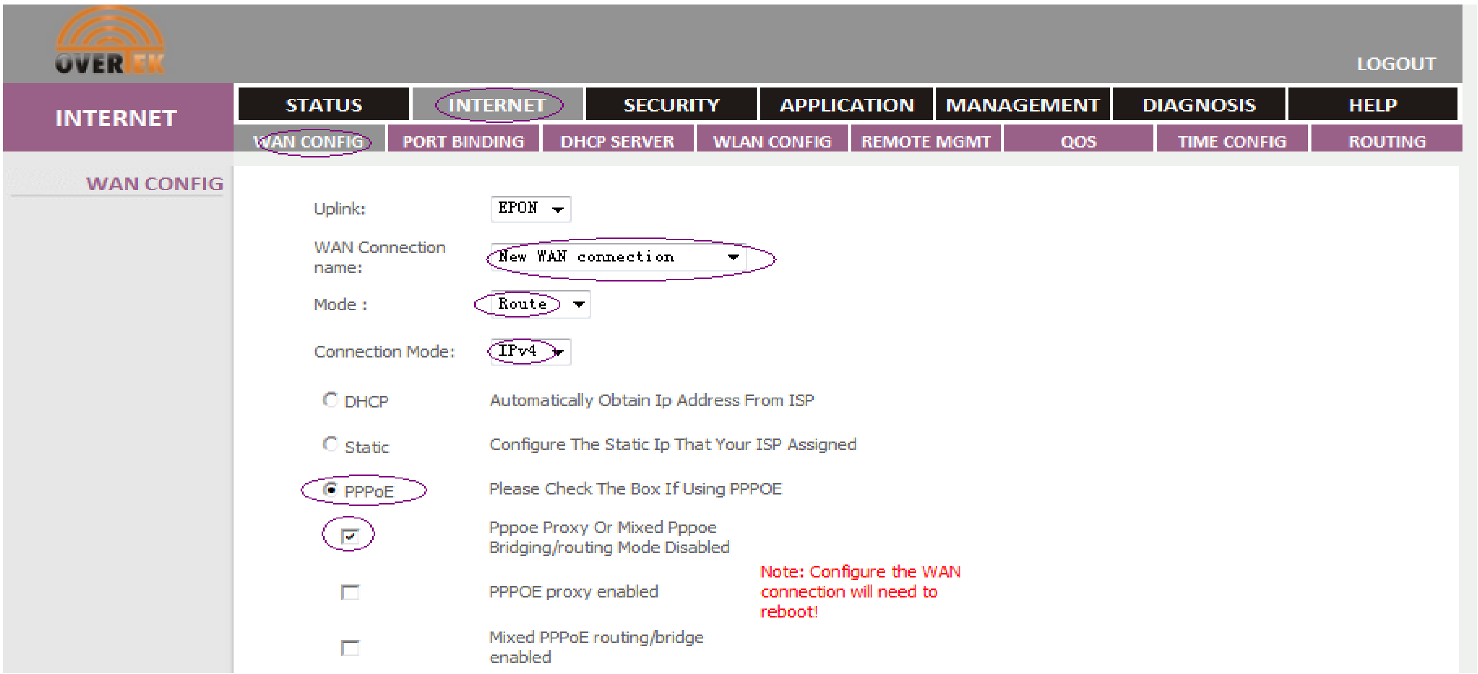
Service Mode: Service mode are separated into different values here. The listed services are for TR069, VoIP, and Internet. You can choose to use different WAN access for the different services.

Binding Port: You can decide which port to be associated with the created WAN access. If you want to use 1 WAN access for all the available wired LAN and wireless LAN, then please select all the interfaces.

4.1.1. Configuration Example for PPPOE:

Click ‘ **INTERNET** ‘ – ‘ **WAN CONFIG** ‘ – ‘ **Connection Name** ‘ – ‘ **Choose a new WAN connection** ‘

- ✓ Go to ‘ Mode ‘ – Select the mode that you want
- ✓ Select ‘ PPPOE ‘ – check the appropriate box for your PPPOE connection
- ✓ Leave the MTU option as default
- ✓ Check the box for NAT



Uplink: EPON

WAN Connection name: New WAN connection

Mode : Route

Connection Mode: IPv4

○ DHCP Automatically Obtain Ip Address From ISP

○ Static Configure The Static Ip That Your ISP Assigned

● PPPoE Please Check The Box If Using PPPOE

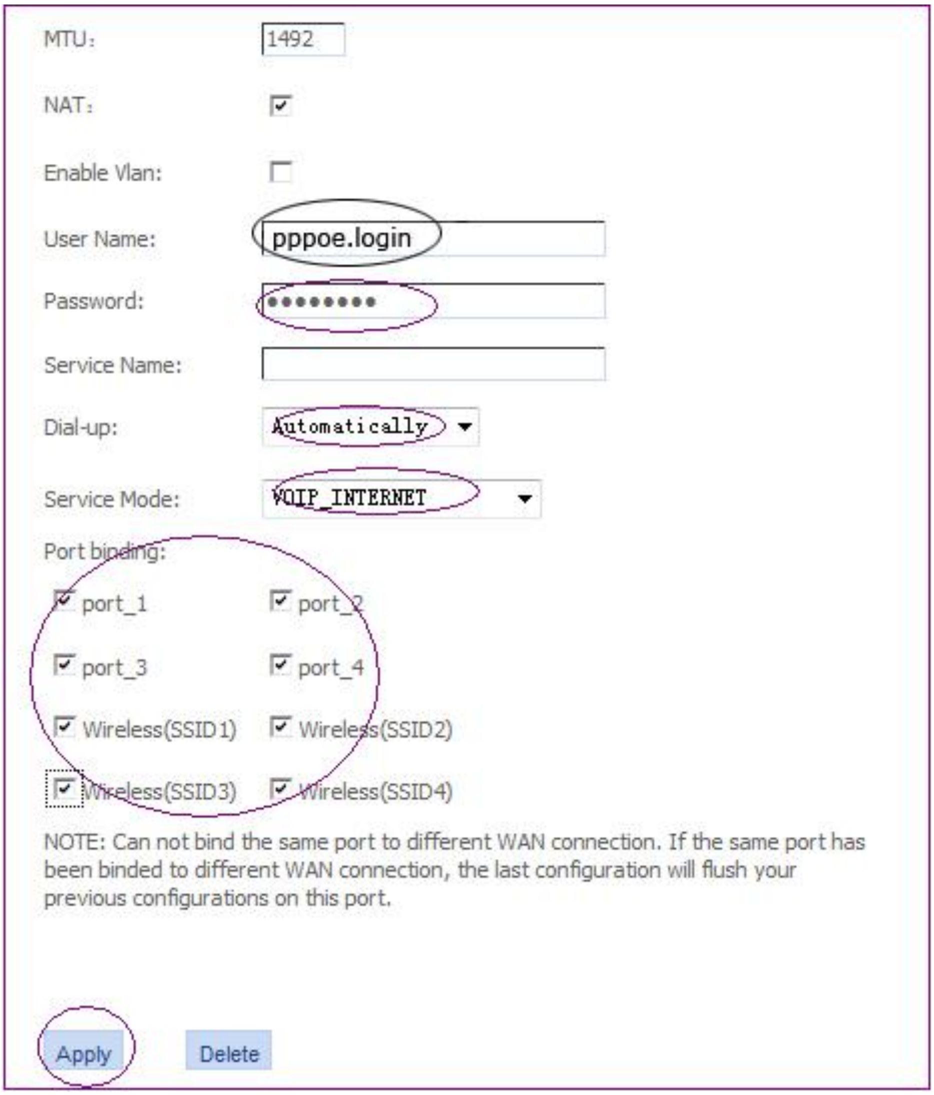
☑ Pppoe Proxy Or Mixed Pppoe Bridging/routing Mode Disabled

□ PPPOE proxy enabled

□ Mixed PPPoE routing/bridge enabled

Note: Configure the WAN connection will need to reboot!

- ✓ Input the PPPOE User Name and password
- ✓ Choose the Dial-up mode ' Automatically Connect '
- ✓ Select the services that you want for this PPPOE connection
- ✓ Select the ports that you want to bind for this PPPOE connection
- ✓ Then click ' **Apply** ' button at the bottom of the page.



MTU: 1492

NAT: ☑

Enable Vlan: □

User Name: pppoe.login

Password: ●●●●●●●●●

Service Name:

Dial-up: Automatically

Service Mode: VOIP_INTERNET

Port binding:

☑ port_1 ☑ port_2

☑ port_3 ☑ port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2)

☑ Wireless(SSID3) ☑ Wireless(SSID4)

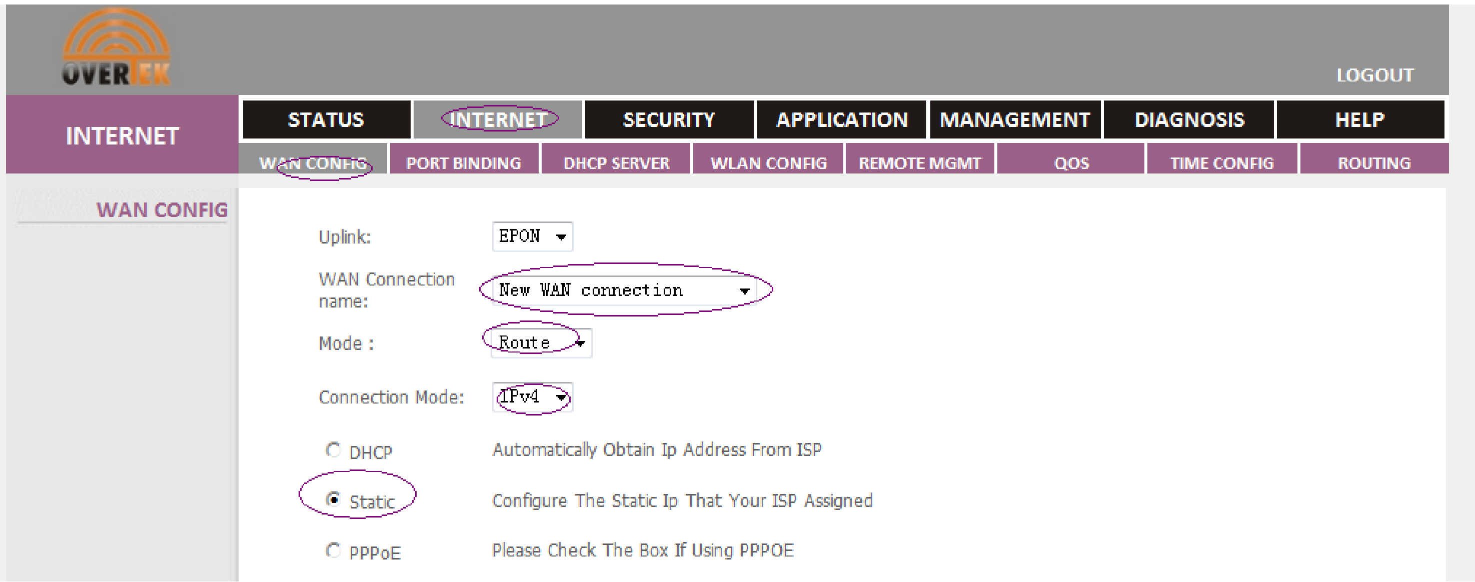
NOTE: Can not bind the same port to different WAN connection. If the same port has been binded to different WAN connection, the last configuration will flush your previous configurations on this port.

Wait for about 15s, you will have your PPPOE connection established successfully.

4.1.2. Configuration Example for STATIC IP:

Click ‘ **INTERNET** ‘ – ‘ **WAN Config** ‘ – ‘ **Connection Name** ‘ – ‘ **Choose a new WAN connection** ‘

- ✓ Go to ‘ Mode ‘ – Select the mode that you want
- ✓ Check the box for ‘ STATIC IP ‘
- ✓ Leave the MTU option as default
- ✓ Check the box for NAT



Uplink: EPON

WAN Connection name: New WAN connection

Mode : Route

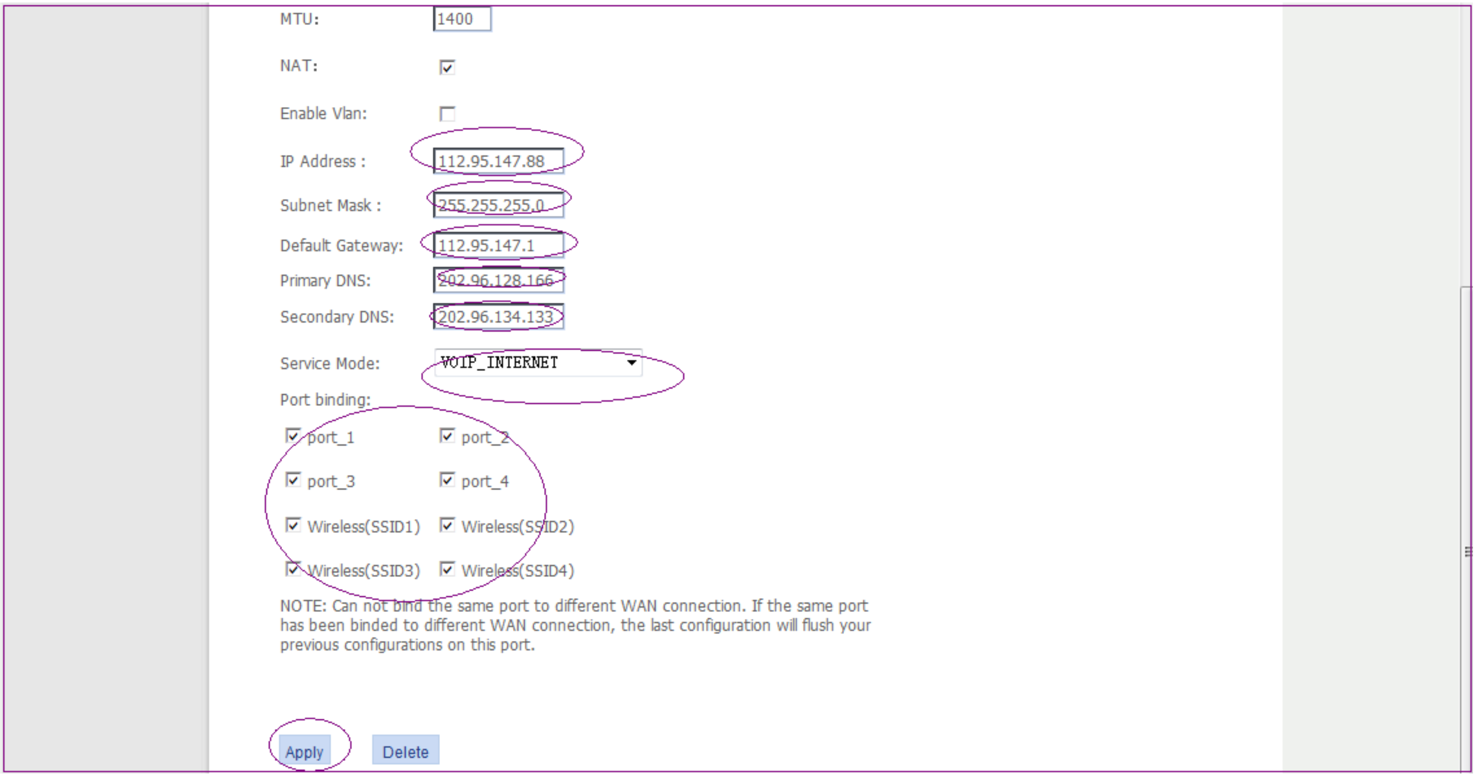
Connection Mode: IPv4

○ DHCP Automatically Obtain Ip Address From ISP

● Static Configure The Static Ip That Your ISP Assigned

○ PPPoE Please Check The Box If Using PPPOE

- ✓ Input the IP address, Subnet Mask, Default Gateway and DNS
- ✓ Select the services that you want for this STATIC IP connection
- ✓ Select the ports that you want to bind for this STATIC IP connection
- ✓ Then click ‘ **Apply** ‘ button at the bottom of the page.



MTU: 1400

NAT: ☑

Enable Vlan: □

IP Address : 112.95.147.88

Subnet Mask : 255.255.255.0

Default Gateway: 112.95.147.1

Primary DNS: 202.96.128.166

Secondary DNS: 202.96.134.133

Service Mode: VOIP_INTERNET

Port binding:

☑ port_1 ☑ port_2

☑ port_3 ☑ port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2)

☑ Wireless(SSID3) ☑ Wireless(SSID4)

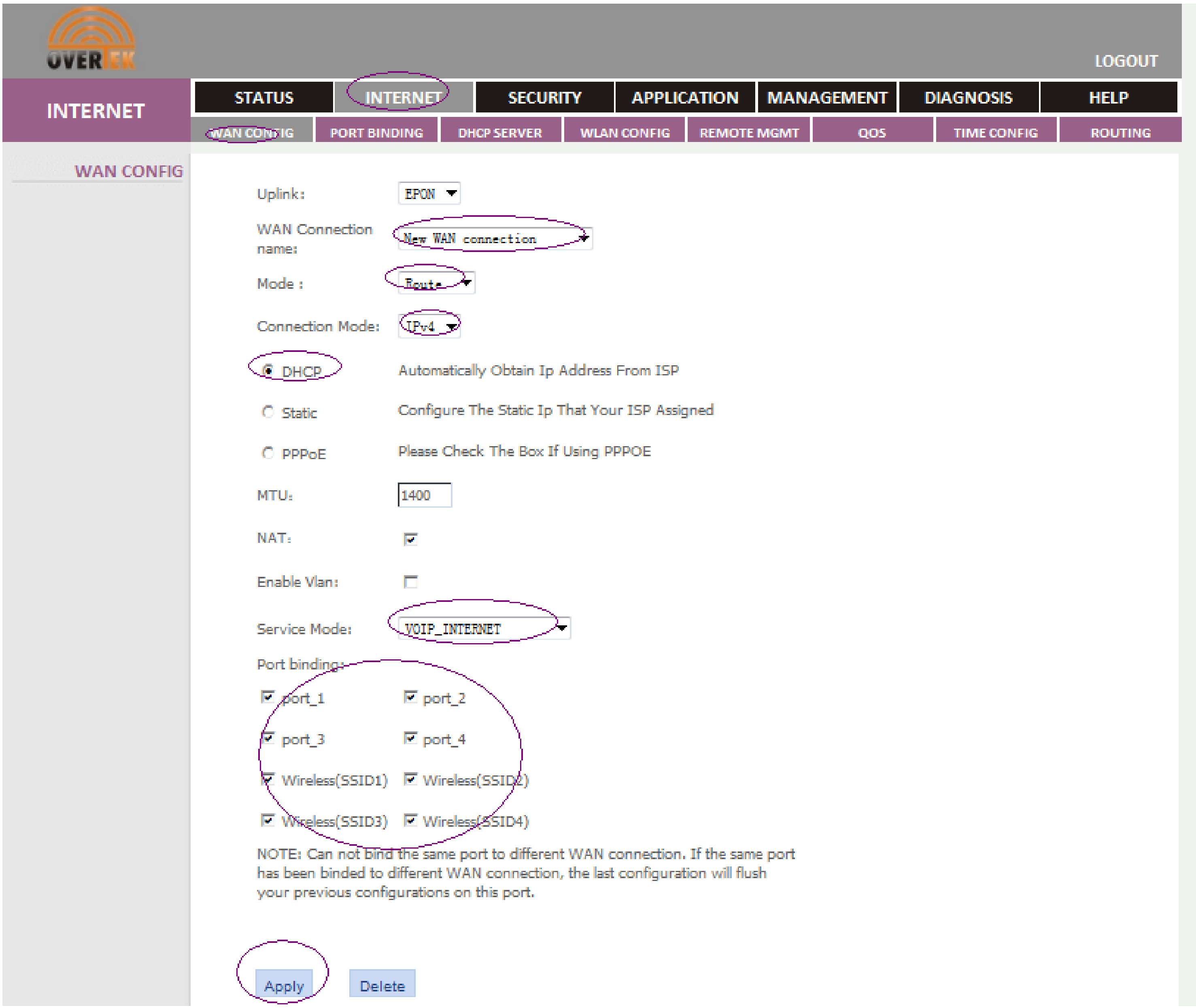
NOTE: Can not bind the same port to different WAN connection. If the same port has been binded to different WAN connection, the last configuration will flush your previous configurations on this port.

Wait for about 15s, your STATIC IP internet access will be established successfully.

4.1.3. Configuration Example for DHCP:

Click ‘ **INTERNET** ‘ – ‘ **WAN Config** ‘ – ‘ **Connection Name** ‘ – ‘ **Choose a new WAN connection** ‘

- ✓ Go to ‘ Mode ‘ – Select the mode that you want
- ✓ Select ‘ **DHCP** ‘ – In this way, your OT-4020VW will obtain an IP address automatically from your ISP
- ✓ Leave the MTU option as default
- ✓ Check the box for NAT
- ✓ Select the services that you want for this DHCP connection
- ✓ Select the ports that you want to bind for this DHCP connection
- ✓ Then click ‘ **Apply** ‘ button at the bottom of the page.



Uplink: EPON

WAN Connection name: New WAN connection

Mode : Route

Connection Mode: IPv4

● DHCP Automatically Obtain Ip Address From ISP

○ Static Configure The Static Ip That Your ISP Assigned

○ PPPoE Please Check The Box If Using PPPOE

MTU: 1400

NAT: ☑

Enable Vlan: □

Service Mode: VOIP_INTERNET

Port binding:

☑ port_1 ☑ port_2

☑ port_3 ☑ port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2)

☑ Wireless(SSID3) ☑ Wireless(SSID4)

NOTE: Can not bind the same port to different WAN connection. If the same port has been binded to different WAN connection, the last configuration will flush your previous configurations on this port.

Apply Delete

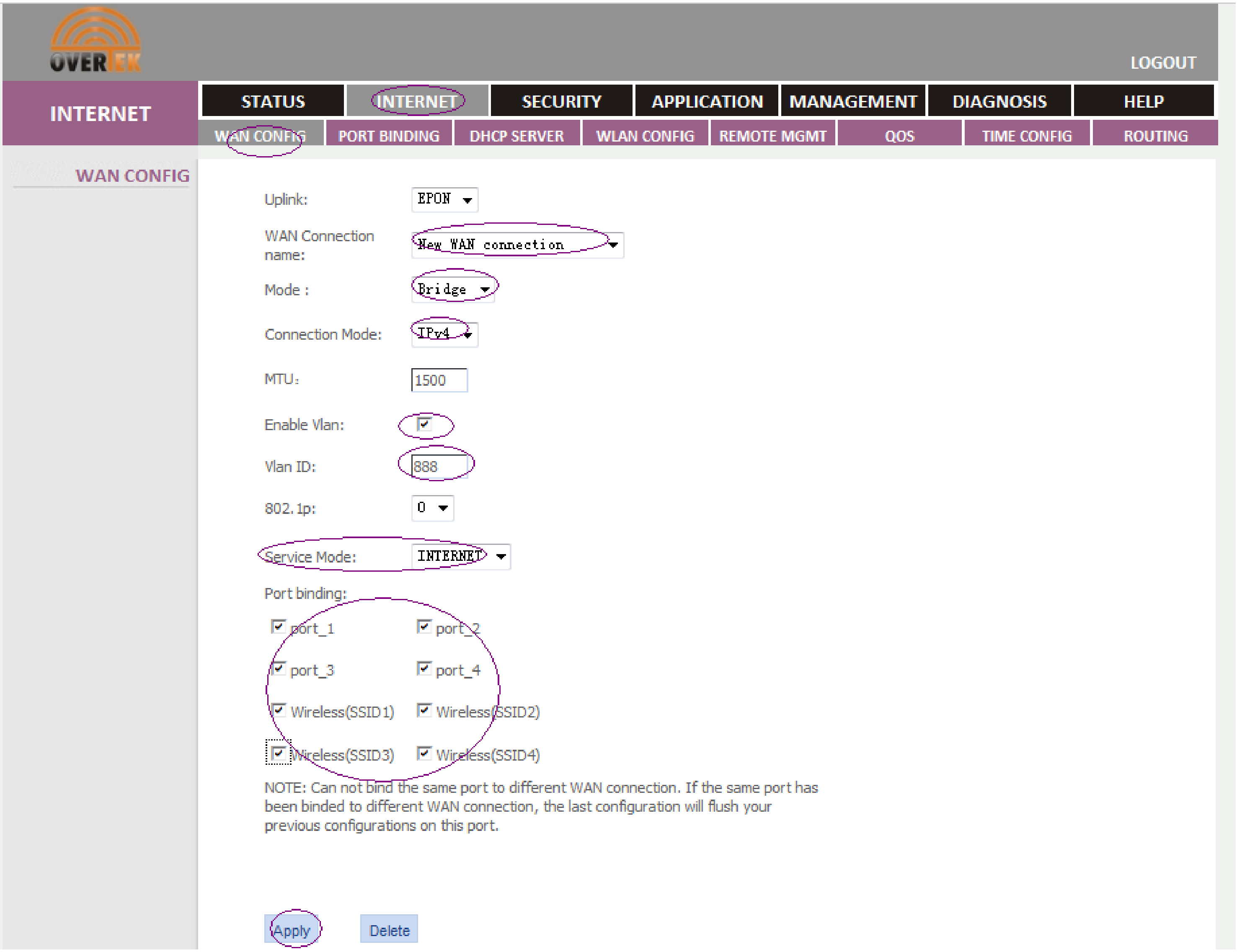
Wait for about 15s, your DHCP internet access will be established successfully.

4.1.4. Configuration Example for VLAN:

Notice: For all DHCP, STATIC IP, PPPOE connection modes, you can configure VLAN IDs as you may wish. Below is the example for you to configure VLAN ID on Bridge mode.

Click ‘ **INTERNET** ‘ – ‘ **WAN Config** ‘ – ‘ **Connection Name** ‘ – ‘ **Choose a new WAN connection** ‘

- ✓ Go to ‘ Mode ‘ – Select the **Bridge Mode**
- ✓ Leave the MTU option as default
- ✓ Check the Box for ‘ Enable Vlan ‘
- ✓ Input the VLAN ID
- ✓ Set the IEEE802.1P QOS level for this VLAN
- ✓ Select the services that you want for this VLAN connection
- ✓ Select the ports that you want to bind for this VLAN connection
- ✓ Then click ‘ **Apply** ‘ button at the bottom of the page.



Uplink: EPON

WAN Connection name: New WAN connection

Mode : Bridge

Connection Mode: IPv4

MTU: 1500

Enable Vlan: ☑

Vlan ID: 888

802.1p: 0

Service Mode: INTERNET

Port binding:

☑ port_1 ☑ port_2

☑ port_3 ☑ port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2)

☑ Wireless(SSID3) ☑ Wireless(SSID4)

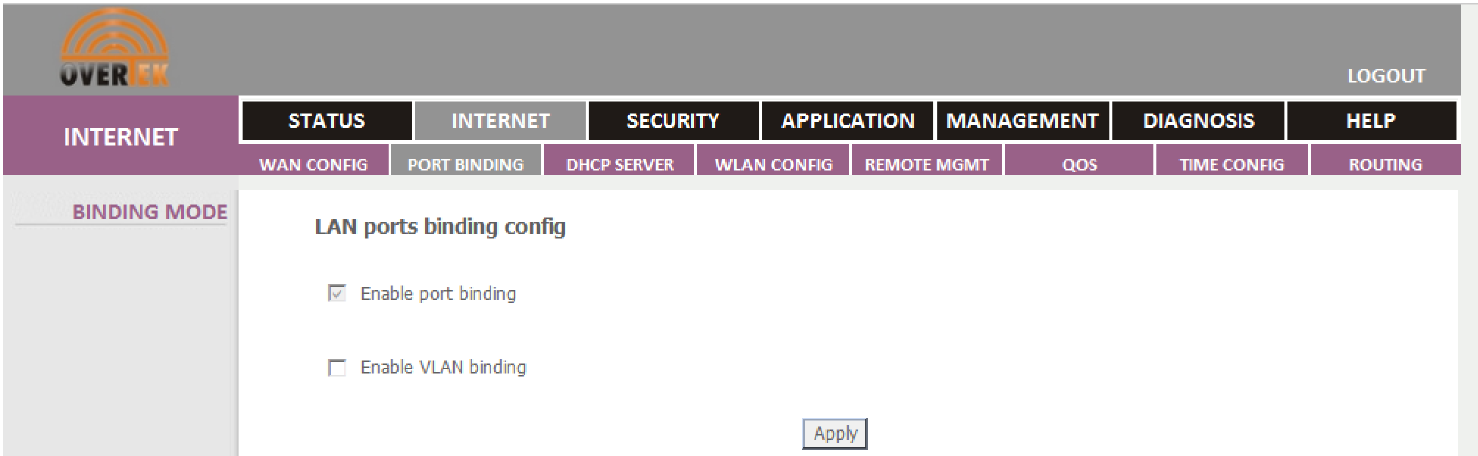
NOTE: Can not bind the same port to different WAN connection. If the same port has been binded to different WAN connection, the last configuration will flush your previous configurations on this port.

Wait for about 15s, your VLAN internet access will be established successfully.

4.2. Port Binding

4.2.1. Enable Port Binding

4.2.2. Enable VLAN Binding



LAN ports binding config

☑ Enable port binding

□ Enable VLAN binding

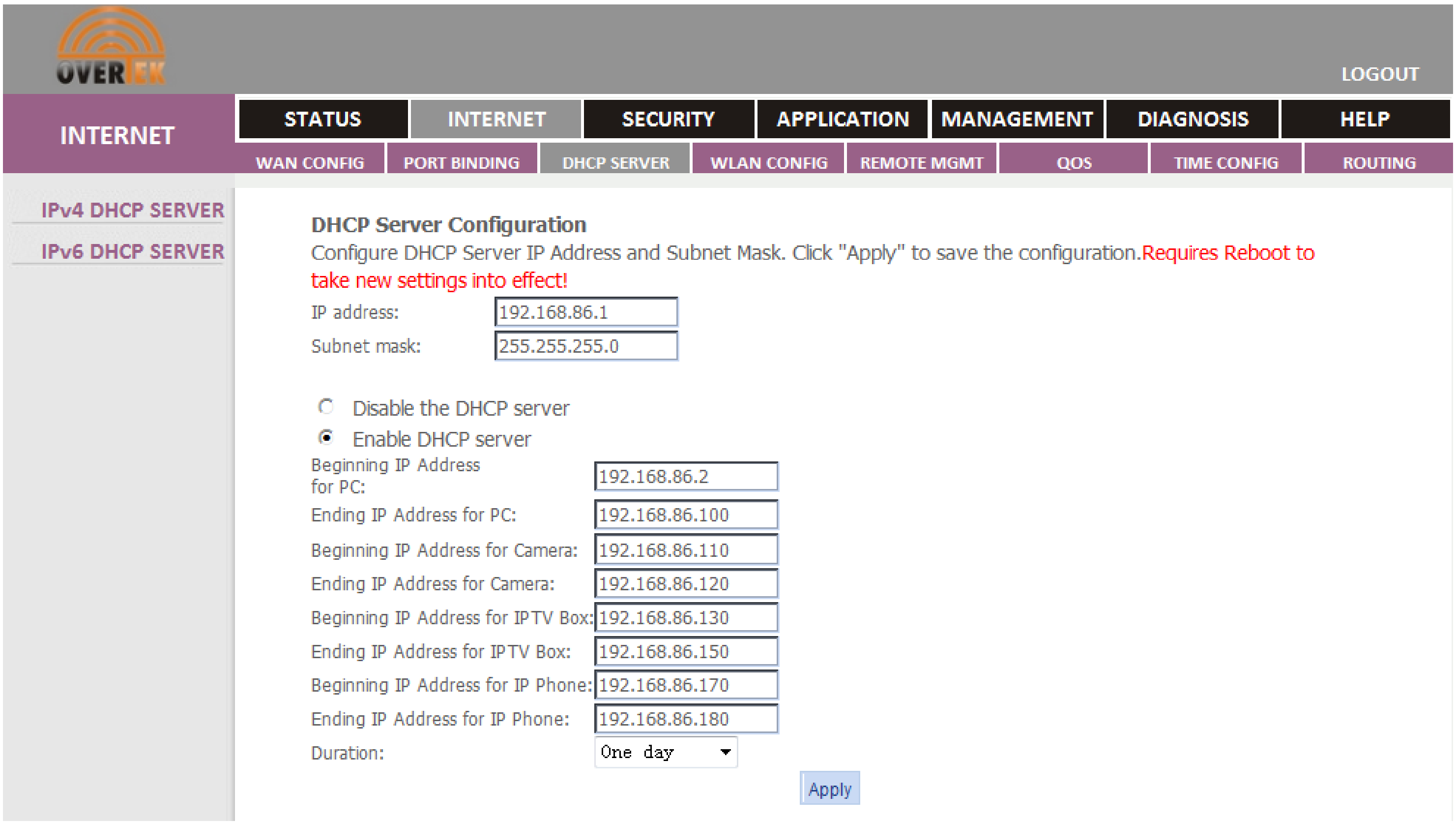
Click ' **Internet** ' – '**Port Binding** ' to configure VLAN binding function which is specially for IPTV VLAN applications. After done, click ' Apply ' button to save and apply new settings.

4.3. DHCP Server

4.3.1. IPV4 DHCP Server

Click ' **INTERNET** ' – '**DHCP Server** ' -- '**IPV4 HCP Server** ' to configure the DHCP Server options.

By default, the DHCP Server begins with 192.168.86.2, end with 192.168.86.254.



DHCP Server Configuration

Configure DHCP Server IP Address and Subnet Mask. Click "Apply" to save the configuration.Requires Reboot to take new settings into effect!

IP address:	192.168.86.1
Subnet mask:	255.255.255.0

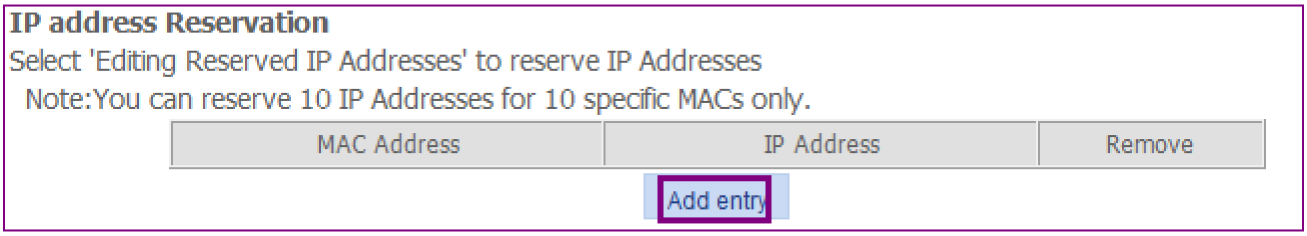
○ Disable the DHCP server

● Enable DHCP server

Beginning IP Address for PC:	192.168.86.2
Ending IP Address for PC:	192.168.86.100
Beginning IP Address for Camera:	192.168.86.110
Ending IP Address for Camera:	192.168.86.120
Beginning IP Address for IPTV Box:	192.168.86.130
Ending IP Address for IPTV Box:	192.168.86.150
Beginning IP Address for IP Phone:	192.168.86.170
Ending IP Address for IP Phone:	192.168.86.180
Duration:	One day

4.3.2. IP address Reservation

Click ‘ **INTERNET** ‘ – ‘**DHCP Server** ‘ -- ‘**IP address Reservation** ‘ to configure the Static IP address for a specific MAC.

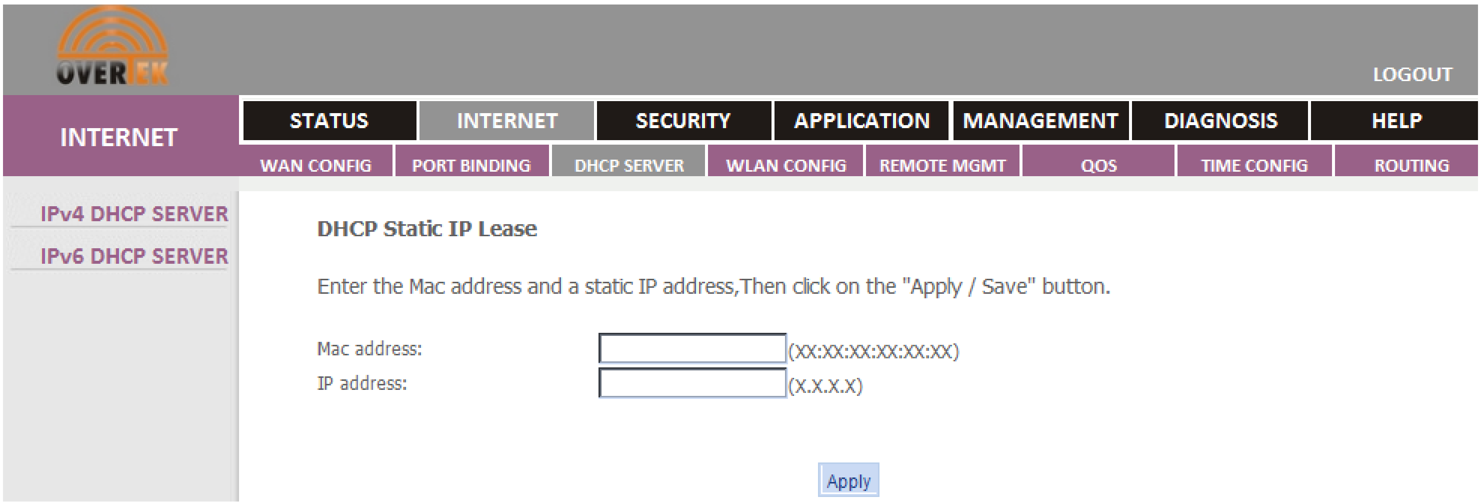


IP address Reservation

Select 'Editing Reserved IP Addresses' to reserve IP Addresses

Note:You can reserve 10 IP Addresses for 10 specific MACs only.

MAC Address	IP Address	Remove



DHCP Static IP Lease

Enter the Mac address and a static IP address,Then click on the "Apply / Save" button.

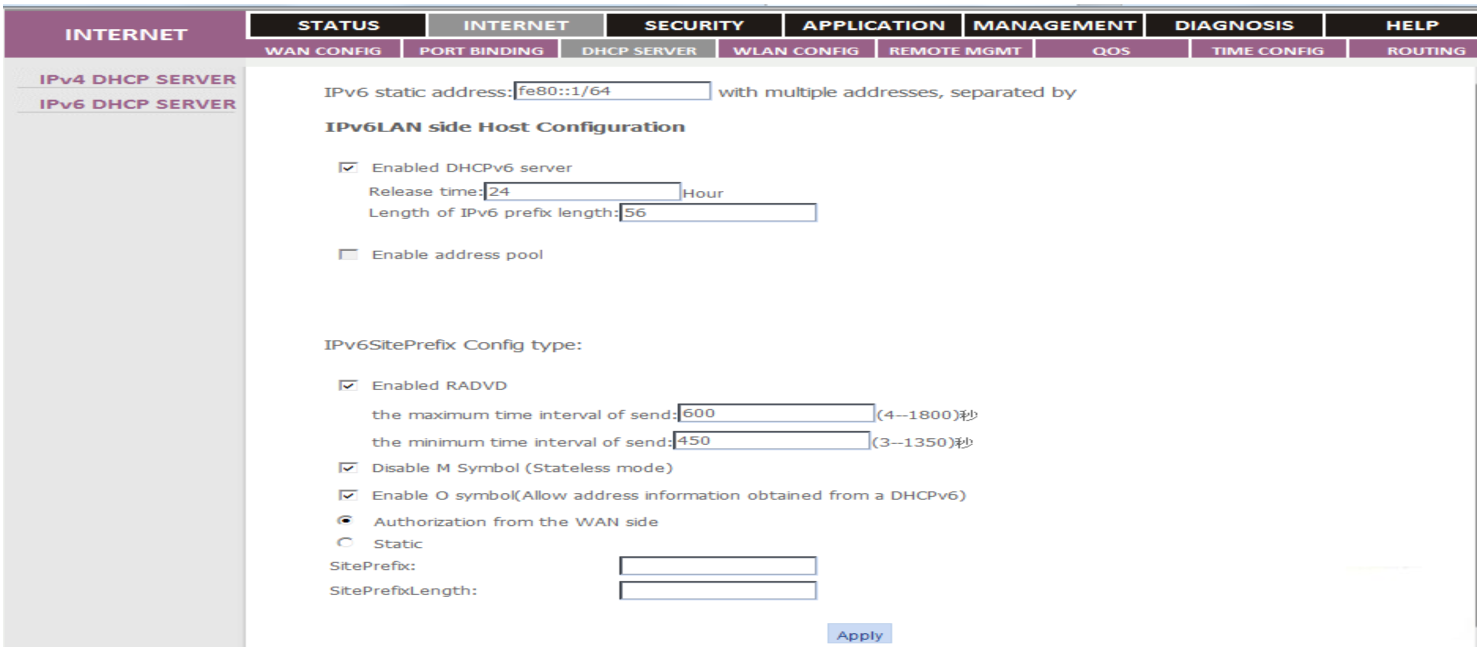
Mac address: (XX:XX:XX:XX:XX:XX)

IP address: (X.X.X.X)

You should configure the MAC address and associate it with an available IP Address. After done, the configured IP Address will be the Static LAN IP address of the device who own the configured MAC address.

4.3.3. IPV6 DHCP Server

Click ‘ **INTERNET** ‘ – ‘**DHCP Server** ‘ -- ‘**IPV6 HCP Server** ‘ to configure the IPV6 DHCP Server .



IPv6 static address: fe80::1/64 with multiple addresses, separated by

IPv6LAN side Host Configuration

☑ Enabled DHCPv6 server

Release time: 24 Hour

Length of IPv6 prefix length: 56

☐ Enable address pool

IPv6SitePrefix Config type:

☑ Enabled RADVD

the maximum time interval of send: 600 (4--1800)秒

the minimum time interval of send: 450 (3--1350)秒

☑ Disable M Symbol (Stateless mode)

☑ Enable O symbol(Allow address information obtained from a DHCPv6)

● Authorization from the WAN side

○ Static

SitePrefix:

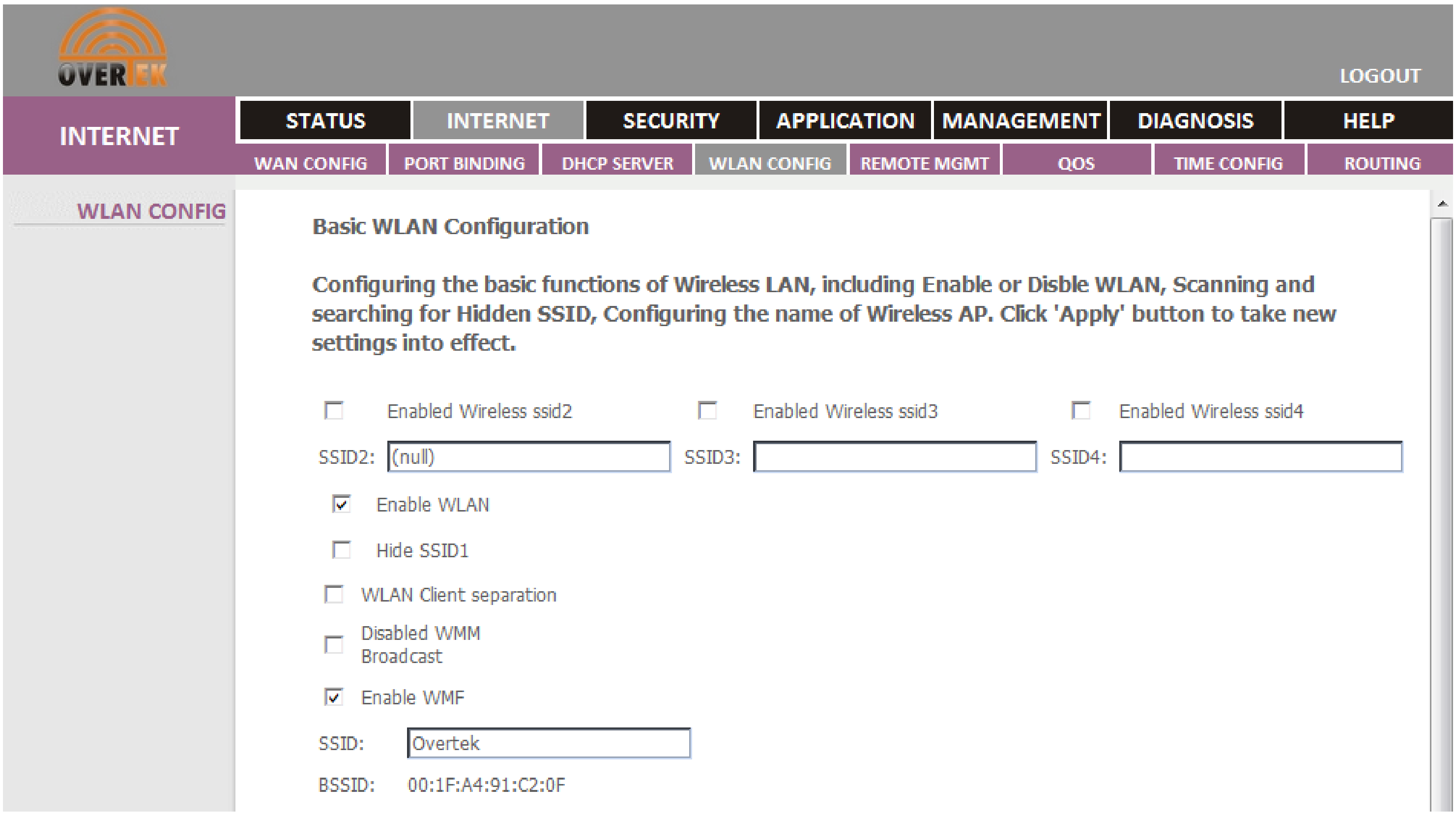
SitePrefixLength:

After done, please click ‘Apply ‘ button to save and apply new settings.

4.4. Wireless LAN Config

4.4.1. WLAN Config

Click ' **INTERNET** ' – '**WLAN Config** ' to configure Wireless parameters:



Basic WLAN Configuration

Configuring the basic functions of Wireless LAN, including Enable or Disble WLAN, Scanning and searching for Hidden SSID, Configuring the name of Wireless AP. Click 'Apply' button to take new settings into effect.

□ Enabled Wireless ssid2 □ Enabled Wireless ssid3 □ Enabled Wireless ssid4

SSID2: (null) SSID3: SSID4:

☑ Enable WLAN

□ Hide SSID1

□ WLAN Client separation

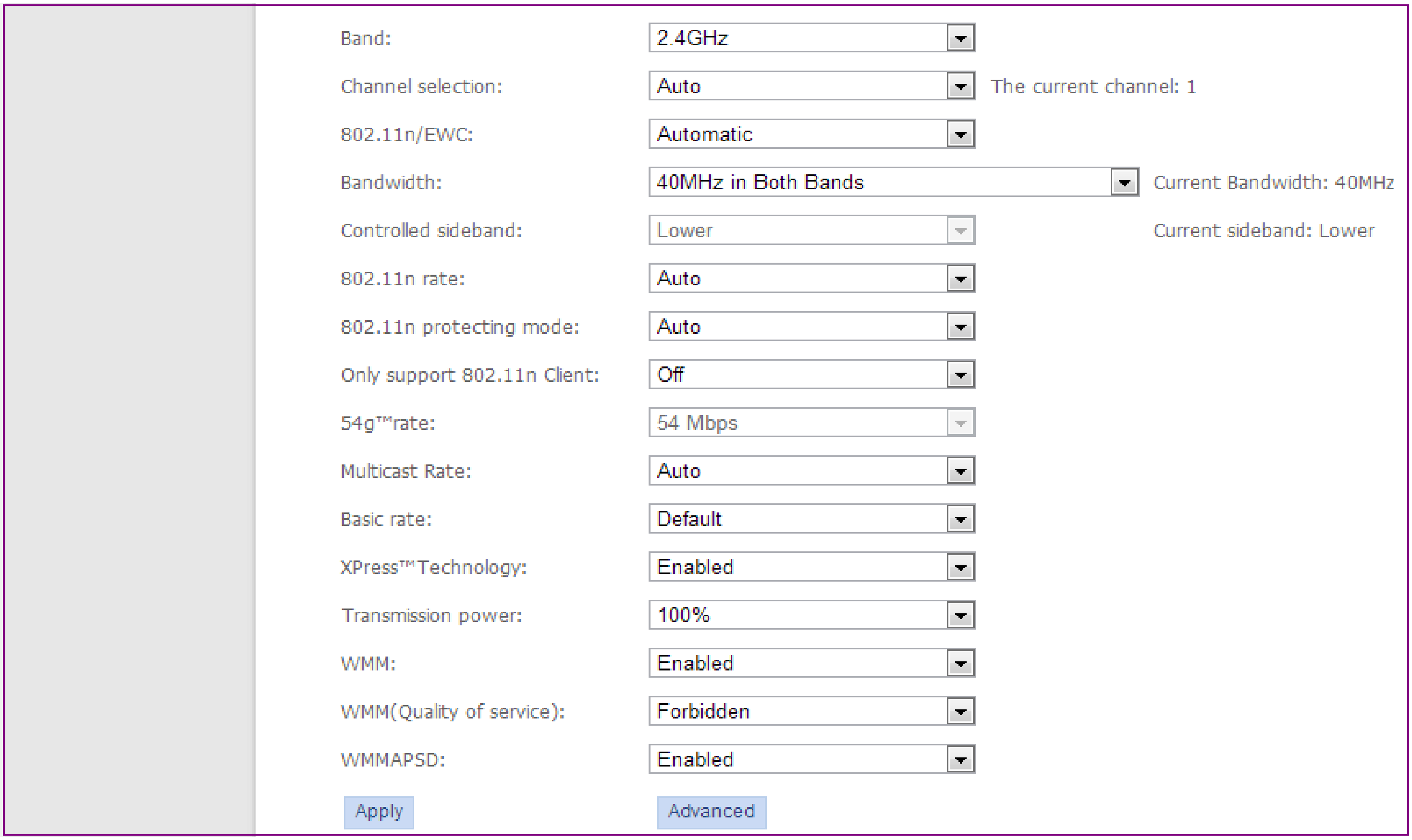
□ Disabled WMM Broadcast

☑ Enable WMF

SSID: Overtek

BSSID: 00:1F:A4:91:C2:0F

Enable Wireless SSID2: Check the box to enable Wireless SSID2
Enable Wireless SSID3: Check the box to enable Wireless SSID3
Enable Wireless SSID4: Check the box to enable Wireless SSID4
Enable WLAN: Check the box to enable Wireless SSID1 (This is the Master Switch for WLAN)
HIDE SSID1: Check the box to hide SSID1
WLAN Client Separation: Check the box to separate users in the same WLAN so they do not have access to each other
Disabled WMM Broadcast: To diable WiFi Multimedia
Enable WMF: To enable Wireless Message Format function
SSID: This is the SSID1, you can set the name of your SSID1 in this column
BSSID: The secondary wireless ID of your wireless router



Band:	2.4GHz	
Channel selection:	Auto	The current channel: 1
802.11n/EWC:	Automatic	
Bandwidth:	40MHz in Both Bands	Current Bandwidth: 40MHz
Controlled sideband:	Lower	Current sideband: Lower
802.11n rate:	Auto	
802.11n protecting mode:	Auto	
Only support 802.11n Client:	Off	
54g™rate:	54 Mbps	
Multicast Rate:	Auto	
Basic rate:	Default	
XPress™Technology:	Enabled	
Transmission power:	100%	
WMM:	Enabled	
WMM(Quality of service):	Forbidden	
WMMAPSD:	Enabled	

Band: The desired wireless band of your wireless router. It is working at 2.4GHz by default

Channel: The Wireless Channel of your wireless Router. You can manually set it to the required channel

802.11n/EWC: Enabling 802.11n/EWC, the wireless speed will be accelerated

Bandwidth: To determine the wireless bandwidth of your wireless router. It could be set to 20M or 40M

Control Sideband: Control the frequency to be higher or lower than standard Telecom frequencies.

802.11n Rate: To set the Wireless Power Level

802.11n Protection Rate: The 802.11n specification provides protection rules to guarantee that 802.11n transmissions do not cause interference with legacy stations or access points. By default, these protection mechanisms are enabled. However, you can turn off these protection mechanisms.

Only support 802.11n Client: If this option is enabled, then the OT-4020VW will not be compatible with your IEEE802.11b/g devices. In such case, the OT-4020VW support only IEEE802.11n devices.

54G Rate: This is to enable Broadcom 54G Wireless Chipset, enabling more compatibility to other IEEE802.11b, IEEE802.11g based devices.

Multicast Rate: To set the wireless transmission power for Multicast applications

Basic Rate: This is to set the wireless transmission power for IEEE802.11b/g

XPress™ Technology: Broadcom's standards-based frame-bursting technology to improve 802.11 wireless LAN performance. If the WMM (Quality of Service) is enabled, the XPress™ Technology option can also be enabled.

Transmission Power: To set the Wireless Transmission power for the wireless router

WMM(Wi-Fi Multimedia): To enable WiFi Multimedia

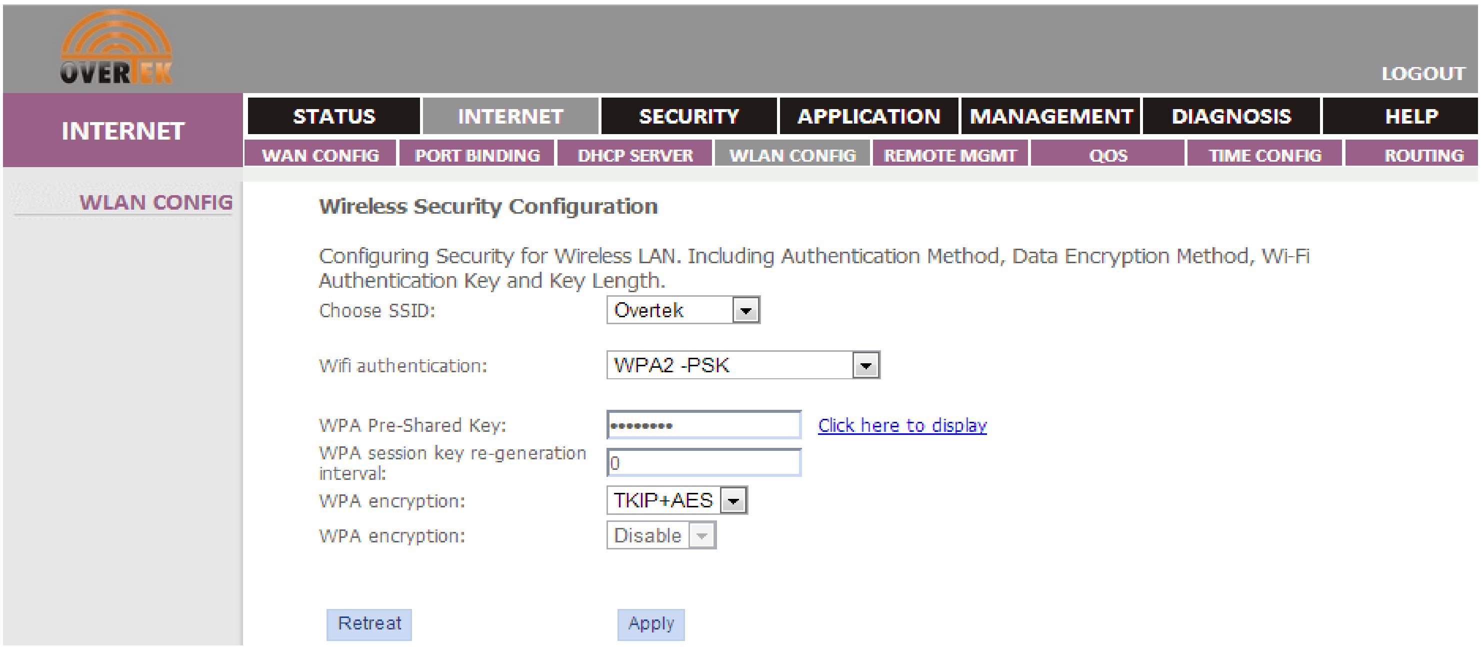
WMM (Quality of Service): To enable QOS in Wireless transmission. You can also enable Xpress Technology after enabling **WMM** (Quality of Service) Option

WMM APSD: To enable the Power Saving mode in WiFi Multimedia

Apply: Click 'Apply' to save and apply new settings.

4.4.2. WLAN Security

Click ‘ **Internet**’ – ‘**WLAN Config** ’ – ‘**Advanced**’ to configure wireless security policies



Wireless Security Configuration

Configuring Security for Wireless LAN. Including Authentication Method, Data Encryption Method, Wi-Fi Authentication Key and Key Length.

Choose SSID: Overtek

Wifi authentication: WPA2 -PSK

WPA Pre-Shared Key: •••••••• Click here to display

WPA session key re-generation interval: 0

WPA encryption: TKIP+AES

WPA encryption: Disable

Choose SSID: To choose the appropriate SSID that you configured.

Wifi Authentication: To configure the wireless authentication mode for your network

A. If you want to set the Network Authentication to WEB based,
then you should enable either ‘Open ‘ or ‘ Shared ‘ mode.

Open: This is to choose the wireless authentication mode to ‘ WEP OPEN’

Shared: This is to choose the wireless authentication mode to ‘ WEP Shared ‘.

WPA encryption: Set the password for the ‘WEP OPEN’ or ‘ WEP Shared ‘ authentication mode.

Key length: This is to determine to use the 64-bit or 128-bit password

Network Key 1, 2, 3, 4: There are 4 64 or 128 bit keys (passwords) able to be set.

The current network key index number: To determine which key to be used.

B. If you want to set Network Authentication to WPA,
you should enable the ‘WPA-PSK’, or ‘WPA2-PSK’ or ‘ Mixed WPA2/WPA-PSK ‘ mode

WPA-PSK: To enable the wireless authentication mode to ‘ WPA-PSK’

WPA2-PSK: To enable the wireless authentication mode to ‘ WPA2-PSK’

Mixed WPA2/WPA-PSK’: To enable the wireless authentication to support both ‘WPA-PSK’ and ‘WPA2-PSK’.

WPA Pre-Shared Key: The encryption key (also called password) for your wireless network

WPA session key update interval: The time interval for auto generating wireless password

WPA Encryption: The desired Encryption method for WPA or WPA

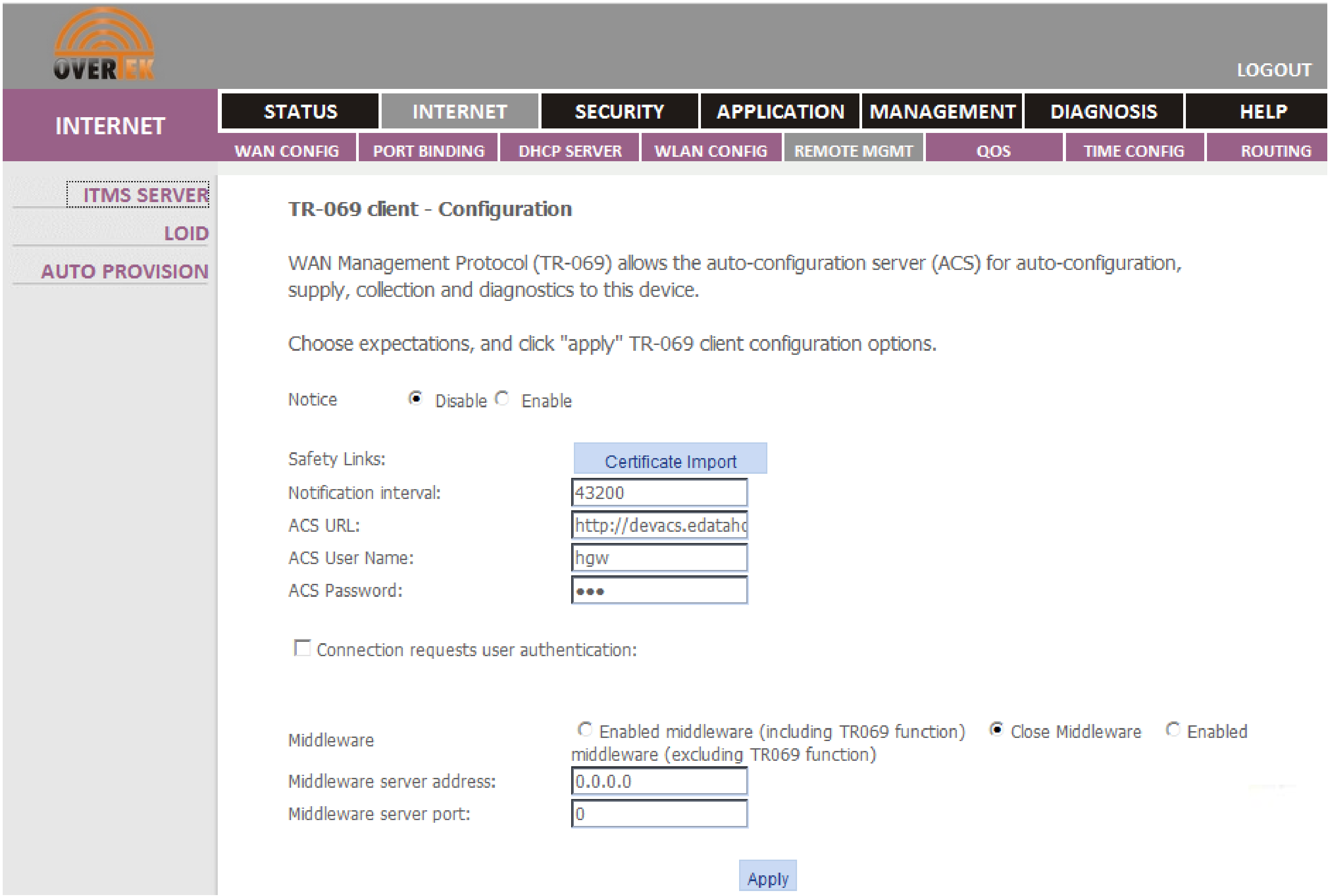
Key Length: This is to set the Encryption key to be either 64-bit or 128-bit based

Click here to display: Click to display the password of your SSID.

4.5. Remote MGMT (Remote Management)

4.5.1. ITMS Server (Insurance TeleMarketing Sales System)

Click ‘ **INTERNET** ‘ – ‘**REMOTE MGMT** ‘ – ‘ **ITMS Server** ‘
to configure the parameters for remote management of the ONU through TR069.



TR-069 client - Configuration

WAN Management Protocol (TR-069) allows the auto-configuration server (ACS) for auto-configuration, supply, collection and diagnostics to this device.

Choose expectations, and click "apply" TR-069 client configuration options.

Notice ● Disable ○ Enable

Safety Links: Certificate Import

Notification interval: 43200

ACS URL: http://devacs.edatahc

ACS User Name: hgw

ACS Password: •••

□ Connection requests user authentication:

Middleware ○ Enabled middleware (including TR069 function) ● Close Middleware ○ Enabled middleware (excluding TR069 function)

Middleware server address: 0.0.0.0

Middleware server port: 0

Notice: To Enable or Disable TR069

Safety Links: To import the license for the ITMS Server

Notification Interval: The time interval to send a notification (seconds)

ACS URL: The TR069 ACS Server address

ACS User Name: The User Name for the Remote Management Server

ACS Password: The password for the associated User Name

Connection requests User Authentication: To Enable or Disable User Authentication for the Remote Management Server

Connection requests a User Name: The Authentication ID for the Remote Management Server

Connection requests a password: The Password for the Authentication ID

Middleware: To Enable or Disable the middleware

Enabled middleware (including TR069 function): To enable middleware with TR069 functionalities

Close Middleware: Check the box to disable middleware

Enabled middleware (excluding TR069 function): To enable middleware without TR069 functionalities

Middleware Server Address: The remote server address for the Middleware

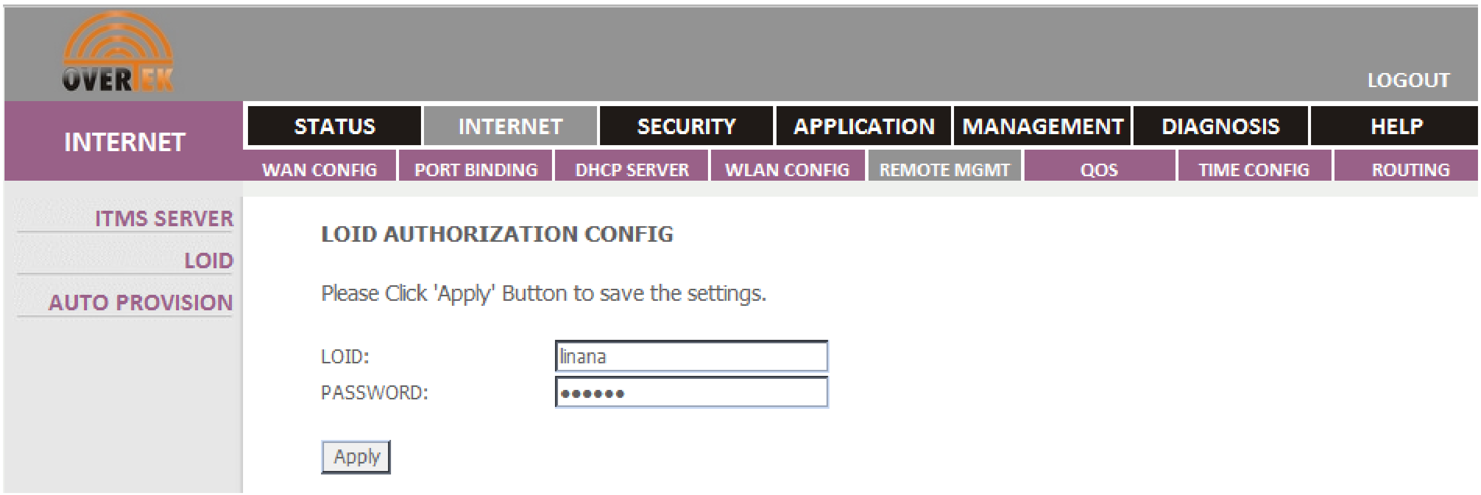
Middleware server port: To set the port number for the Middleware server

4.5.2. LOID

Click ‘ **INTERNET** ‘ – ‘**REMOTE MGMT** ‘ – ‘ **LOID** ‘ to authorize the GEPON OLT with LOID.

Note: This function can prevent your Internet connection being illegally connected by other unknown Users.

This function is available only if your GEPON OLT support LOID authorization.



LOID AUTHORIZATION CONFIG

Please Click 'Apply' Button to save the settings.

LOID: linana

PASSWORD: ●●●●●●

LOID: The Authorization LOID (The length be within 24 digits)

Password: The Password for the associated LOID

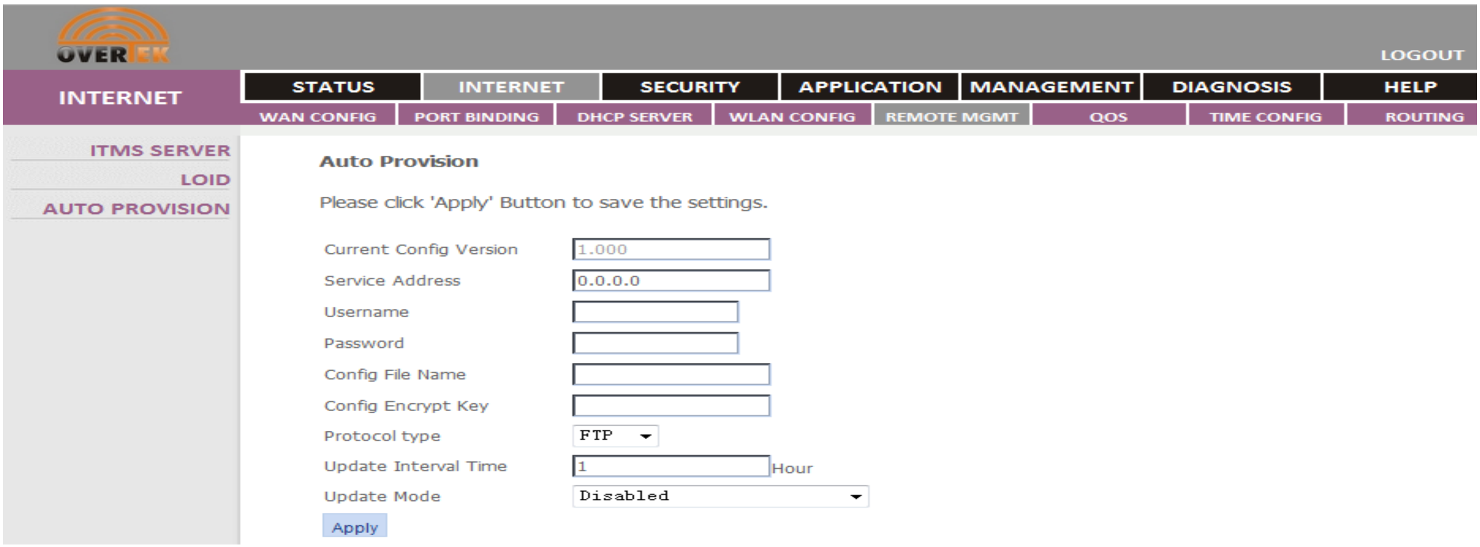
Apply: After input the LOID and password, you should click ‘Apply’ to save and take new settings into effect.

4.5.3. AUTO PROVISION

Click ‘ **INTERNET** ‘ – ‘**REMOTE MGMT** ‘ – ‘**AUTO PROVISION** ‘ to enable Auto Provision function of your ONU.

The Auto Provision function is for remote configure and update firmware of your OT-4020VW ONU. Enabling this function, you can configure the ONU remotely without human involvement. The OT-4020VW support auto provisioning through FTP, TFTP or http servers, you only need to update the configuration files and the firmware on your server, then when the Auto Provision condition is met, the ONU will automatically upgrade to the new configuration or new firmware version.

As the FTP, TFTP, HTTP servers are cost effective to deploy, the Auto Provision function is specially designed for small/medium ISPs to maintain the devices that are placed at Subscriber’s house.



Auto Provision

Please click 'Apply' Button to save the settings.

Current Config Version: 1.000

Service Address: 0.0.0.0

Username:

Password:

Config File Name:

Config Encrypt Key:

Protocol type: FTP

Update Interval Time: 1 Hour

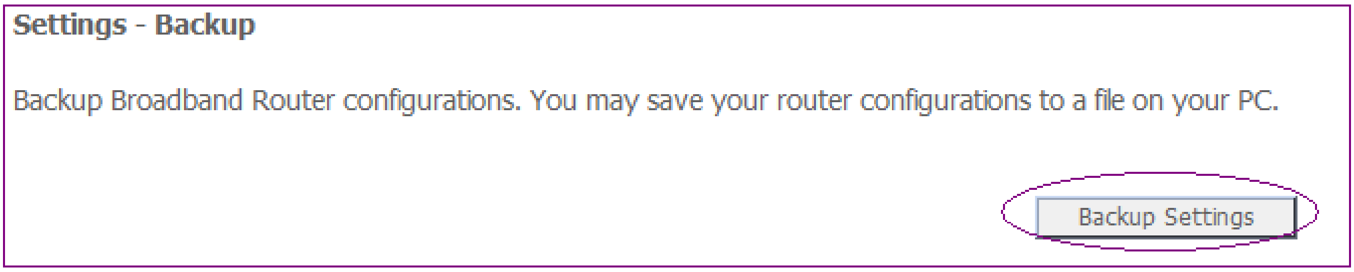
Update Mode: Disabled

Current Config Version: Indicate the current version number of the configuration file. You do not need to configure this option as the configuration file versions are updated automatically.
Service Name: This is the Auto Provision Server address. You must fill this address in order to enable device know where to get the updated configuration file.
User Name: This is the user name for your Auto Provision Server
Password: This is the password for your Auto Provision Server
Config File Name: This is the configuration file name, it's named using the MAC address of the ONU.
You can leave this blank.

Config Encryt Key: The OT-4020VW ONU support AES Encryption. You can encrypt the configuration file with AES and upload it onto the Auto Provision Server. You should fill the Encryption key in the ONU so the ONU can decrypt the configuration file.
Protocol Type: You can set Auto Provision server type to FTP, TFTP or HTTP
Update Interval Time: This is the Auto provision interval time, the ONU can be set to auto download the configuration file within the interval set in this blank. The minimum time interval is 1 hour, the max time interval can be 1440 hours.
Update Mode:
Disabled: It means the Auto Provision function is disabled in the ONU;
Update After Reboot: Set to 'Update After Reboot', the ONU will auto download the configuration file from the server when it's booting up.
Update at time interval: Set to ' Update at time interval', the ONU will auto download the configuration file from the server within the time interval set.
Note: 'Update after reboot ' and ' Update at time interval ' work simultaneously.
If you set the Auto Provision mode to ' Update at time interval', the ONU will auto download the configuration file when it's rebooted.
Apply: Click 'Apply' button to save and take new settings into effect.

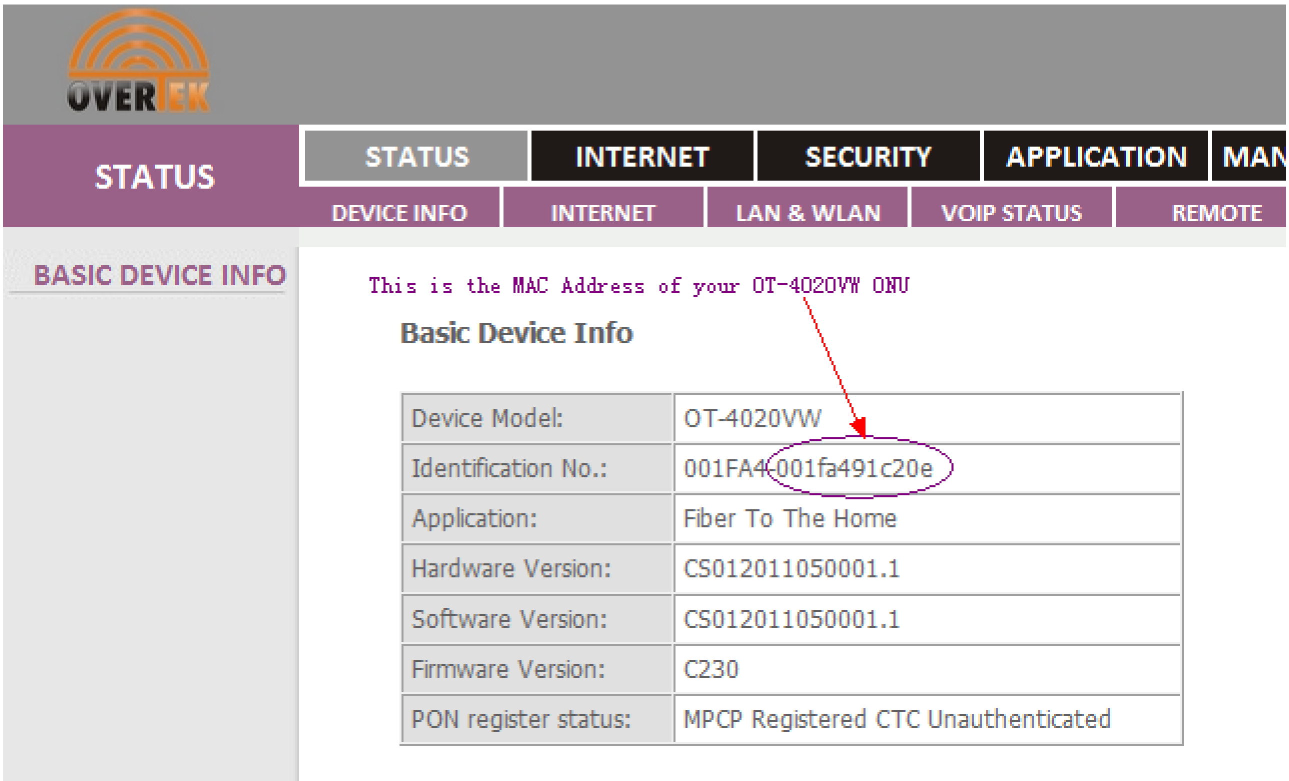
4.5.3.1 Configuration Example for Auto Provision

A. Click ' **INTERNET** ' – '**REMOTE MGMT** ' – '**AUTO PROVISION** ' to configure the right Auto Provision paramters. After done, click 'Apply' to save and activate Auto Provision function.
B. Enter into http://192.168.86.1/backupsettings.html , click 'Backup Setting ' button to download the configuration file to your local folder.


Settings - Backup

Backup Broadband Router configurations. You may save your router configurations to a file on your PC.

C. Go to 'Status' – 'Device Info' Page to find out the MAC address of OT-4020VW ONU.



This is the MAC Address of your OT-4020VW ONU

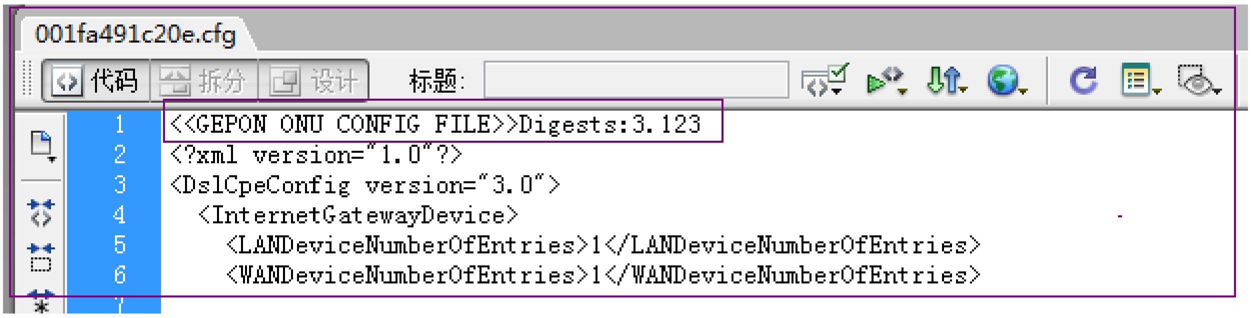
Basic Device Info

Device Model:	OT-4020VW
Identification No.:	001FA4-001fa491c20e
Application:	Fiber To The Home
Hardware Version:	CS012011050001.1
Software Version:	CS012011050001.1
Firmware Version:	C230
PON register status:	MPCP Registered CTC Unauthenticated

D. Name the Configuration file in the format 'mac address +.cfg'. In this example, the MAC address is **001fa491c20e**. So the correct configuration file name should be '**001fa491c20e.cfg**'.

E. Edit the configuration file using any html file editors, such as Dream Weaver.

E.1. To upgrade configuration file, it is mandatory that you add ' **<<GEPON ONU CONFIG FILE>>Digests:3.123** ' into the '**001fa491c20e.cfg'** configuration file to enable Auto Provisioning work correctly. See below for the example:



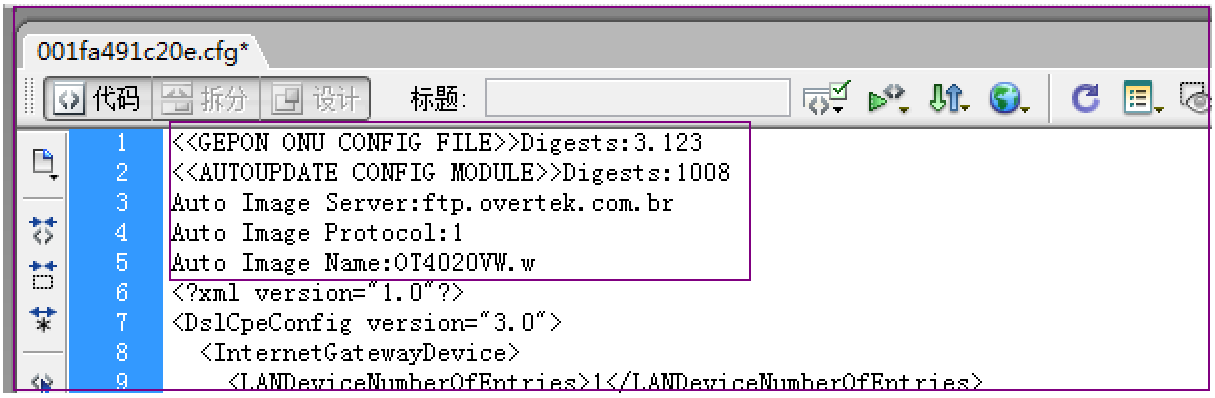
```
<<GEPON ONU CONFIG FILE>>Digests:3.123
<?xml version="1.0"?>
<DslCpeConfig version="3.0">
  <InternetGatewayDevice>
    <LANDeviceNumberOfEntries>1</LANDeviceNumberOfEntries>
    <WANDeviceNumberOfEntries>1</WANDeviceNumberOfEntries>
```

E.2. If you want to update both configuration file and firmware, then you should add the following parameters into the configuration file:

<<GEPON ONU CONFIG FILE>>Digests:3.123
<<AUTOUPDATE CONFIG MODULE>>Digests:1008
Auto Image Server:ftp.overtek.com.br
Auto Image Protocol:2
Auto Image Name:OT4020VW.w

In the above parameters, the Auto Image Server should be your own server address
The Auto Image protocol definition: 1 =FTP, 2 = TFTP, 4 = HTTP, you can set your preferred method.
The Auto Image name can be any name that you prefer, e.g, ' **123.w** '.

Please see below for the example:



```
<<GEPON ONU CONFIG FILE>>Digests:3.123
<<AUTOUPDATE CONFIG MODULE>>Digests:1008
Auto Image Server:ftp.overtek.com.br
Auto Image Protocol:1
Auto Image Name:OT4020VW.w
<?xml version="1.0"?>
<DslCpeConfig version="3.0">
  <InternetGatewayDevice>
    <LANDeviceNumberOfEntries>1</LANDeviceNumberOfEntries>
```

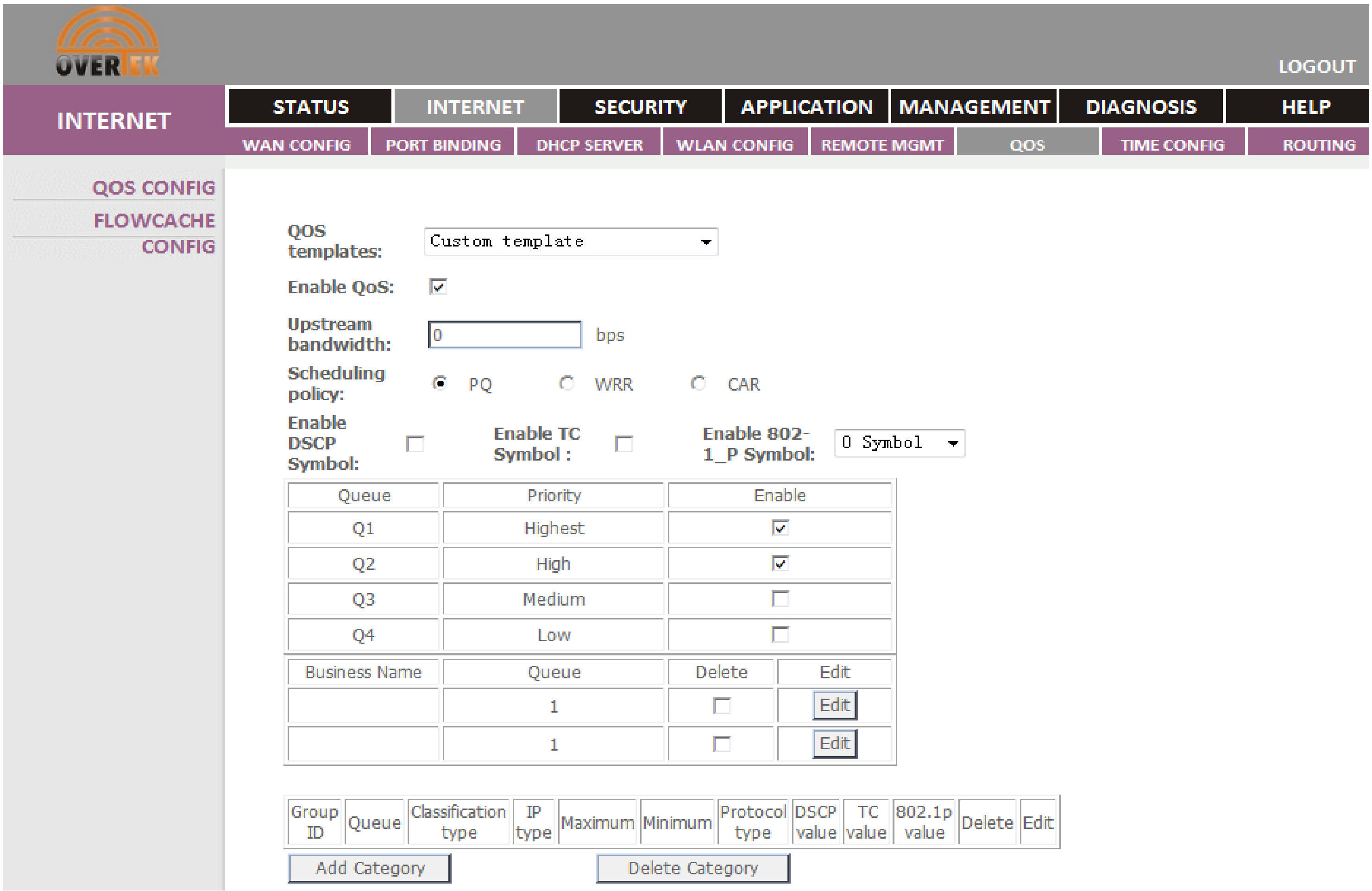
F. After you changed all the configuration parameters you want, upload this configuration file onto your Auto Provision server.

G. If you set the ONU 'Update After Reboot' in the step **A**, then when the ONU is rebooted, it will auto download the new configuration file from the Auto Provision Server, then checksum and apply by itself.

4.6. QOS

4.6.1. QOS Config

Click ' **INTERNET** ' – '**QOS** ' –' **QOS Config** ' to config QOS for your OT-4020VW ONU.



QOS templates: Custom template

Enable QoS: ☑

Upstream bandwidth: 0 bps

Scheduling policy: ● PQ ○ WRR ○ CAR

Enable DSCP Symbol: □ Enable TC Symbol : □ Enable 802-1_P Symbol: 0 Symbol

Queue	Priority	Enable
Q1	Highest	☑
Q2	High	☑
Q3	Medium	□
Q4	Low	□

Business Name	Queue	Delete	Edit
	1	□	Edit
	1	□	Edit

Group ID	Queue	Classification type	IP type	Maximum	Minimum	Protocol type	DSCP value	TC value	802.1p value	Delete	Edit

QOS Templates: To choose the available templates or to customize the template to determine what services to enable the QOS for.

Templates Descriptions:

'Internet, TR069' – To enable QOS for Internet Data and TR069 service

'Internet, TR069, VoIP'- To enable QOS for Internet Data, TR069 and VoIP services

'Internet, TR069, IPTV'- To enable QOS for Internet Data, TR069 and IPTV services

'Internet, TR069, VoIP, IPTV'- To enable QOS for Internet Data, TR069, VoIP and IPTV services

'Custom Template' – To customize the template to determine the services to enable QOS

Enable QOS: Check the box to enable QOS

Upstream Bandwidth: To set the uploading bandwidth for the customized QOS template.

Scheduling Policy: To determine the alternative QOS mode. You can choose to use QOS PQ, QOS WRR or QOS CAR mode.

Enable DSCP Symbol: To enable the DSCP (Differentiated Services Code Point) Symbol for QOS

Enable TC Symbol: To enable the TC (Traffic Categories) Symbol for QOS

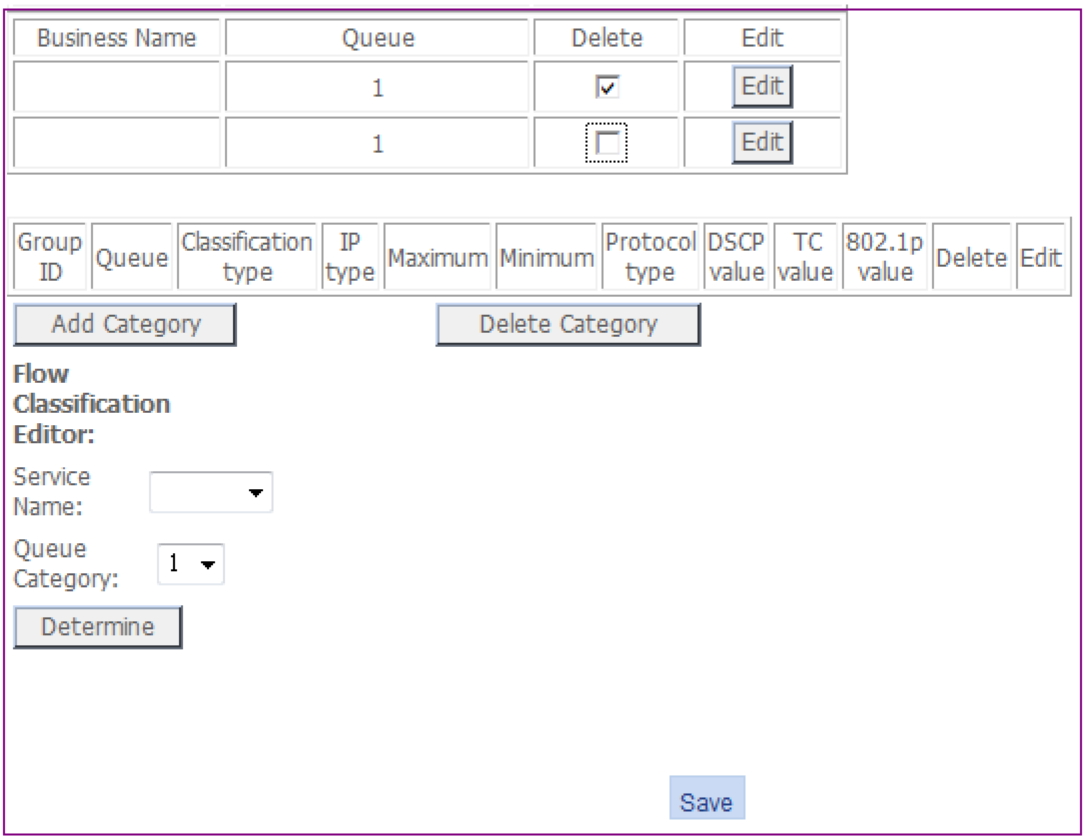
Enable 802.1_P Symbol: To enable IEEE802.1P Symbol for QOS

Q1: To enable the highest QOS level

Q2: To enable a high QOS level

Q3: To enable a medium QOS level

Q4: To enable a low QOS level



Business Name	Queue	Delete	Edit
	1	☑	Edit
	1	☐	Edit

Group ID	Queue	Classification type	IP type	Maximum	Minimum	Protocol type	DSCP value	TC value	802.1p value	Delete	Edit

Flow Classification Editor:

Service Name:

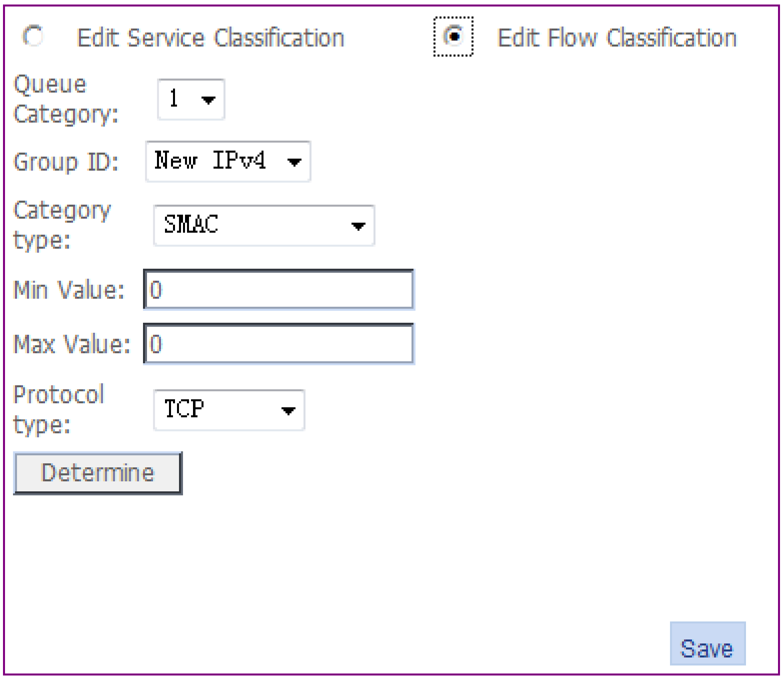
Queue Category: 1

Business Name: The Service Name that you want to enable QOS for, e.g, VoIP, TR069

Queue: The QOS queue for the service specified

Delete: Remove the service from the QOS template

Edit: To edit the service that you want to enable for QOS.
Add Category: Click this button to Edit Service Classification & Edit Flow Classification.
Delete Category: Click this button to delete the configured QOS service and flow classification template
Edit Business Category: Check the box to enable edit QOS for TR069 and VoIP service
Sub-menus under Edit Business Category:
Service Name: The service that you wan to enable QOS for, you can set either VoIP or TR069 service.
Queue Category: The QOS level that you want to enable for the configured service.
Flow Classification Edit: Check the box to enable edit QOS for different flow/packets.



○ Edit Service Classification ● Edit Flow Classification

Queue Category: 1
Group ID: New IPv4
Category type: SMAC
Min Value: 0
Max Value: 0
Protocol type: TCP

Determine

Save

Queue Category: To set the priority for the flow classification that you enabled.
1 is the highest QOS level,
2 is the high QOS level,
3 is the medium QOS level,
4 is the low QOS level

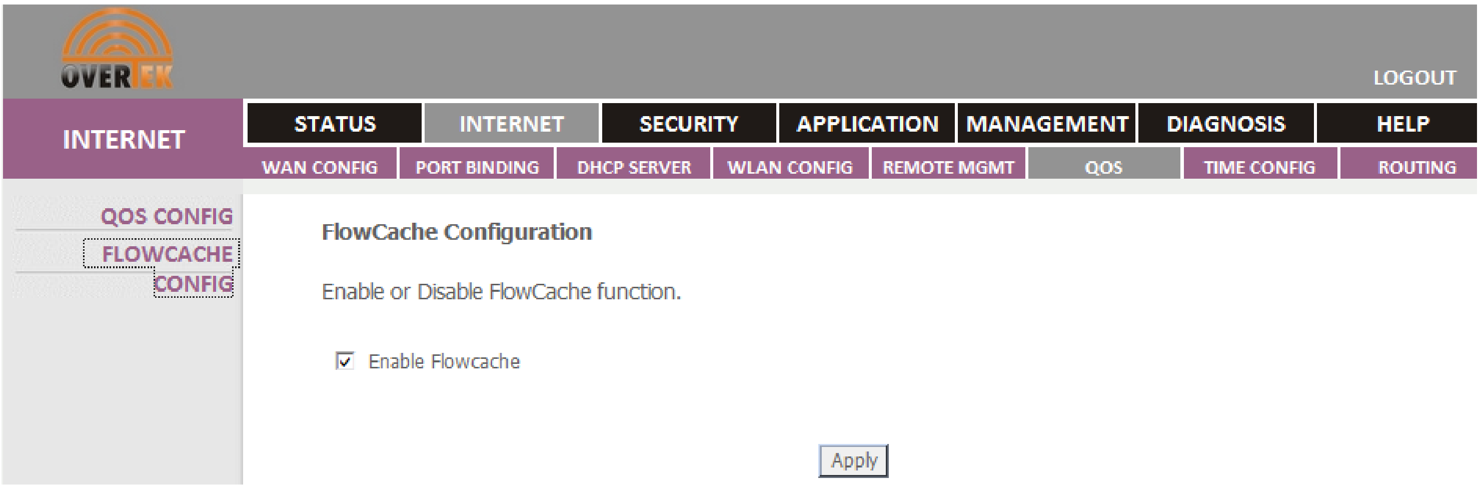
Group ID: To set the IPV4 or IPV6 version for the flow classification.
Category Type: To set different service or interface for flow classification
SMAC: To set flow classification for SMAC service
DMAC: To set flow classification for DMAC Service
802.1P: To set based flow classification for IEEE802.1P service
DIP: To set flow classification for DIP service
SPORT: To set flow classification for SPORT service
DPORT: To set flow classification for DPORT service
TOS: To set flow classification for TOS service
DSCP: To set flow classification for DSCP service
WANInterface: To set flow classification for WAN interface
LANInterface: To set flow classification for LAN interface

Minimum: The minimum QOS level for the enabled Service
Maximum: The maximum QOS level for the enabled Service
Protocol Type: To determine which protocol to enable QOS

After all configurations are done, please click ‘ **Save** ‘ button to save and apply new settings.

4.6.2. Flowcache Config

Click ‘ **INTERNET** ‘ – ‘**QOS** ‘ – ‘ **FlowCache Config** ‘ to enable or disable Cache for the transmission flow:



FlowCache Configuration

Enable or Disable FlowCache function.

☑ Enable Flowcache

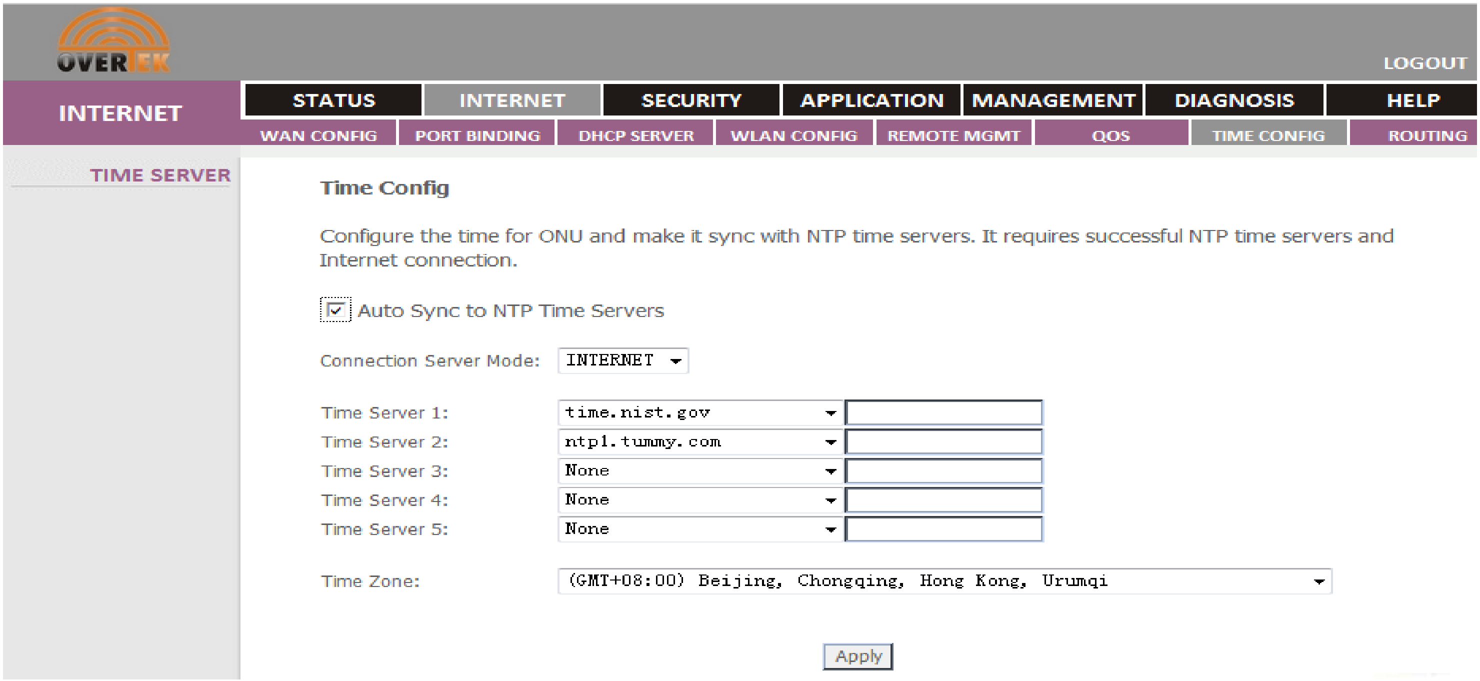
Apply

Enable Flowcache: Check the box for ‘Enable Flowcache’ to enable Cache for the transmission flow
Apply: To save and apply the enabled or disabled Flowcache.

4.7. Time Config

4.7.1. Time Server

Click ‘ **INTERNET** ‘ – ‘**Time Config** ‘ – ‘**Time Server** ‘ to config time for your OT-4020VW ONU:



Time Config

Configure the time for ONU and make it sync with NTP time servers. It requires successful NTP time servers and Internet connection.

☑ Auto Sync to NTP Time Servers

Connection Server Mode: INTERNET

Time Server 1: time.nist.gov
Time Server 2: ntp1.tummy.com
Time Server 3: None
Time Server 4: None
Time Server 5: None

Time Zone: (GMT+08:00) Beijing, Chongqing, Hong Kong, Urumqi

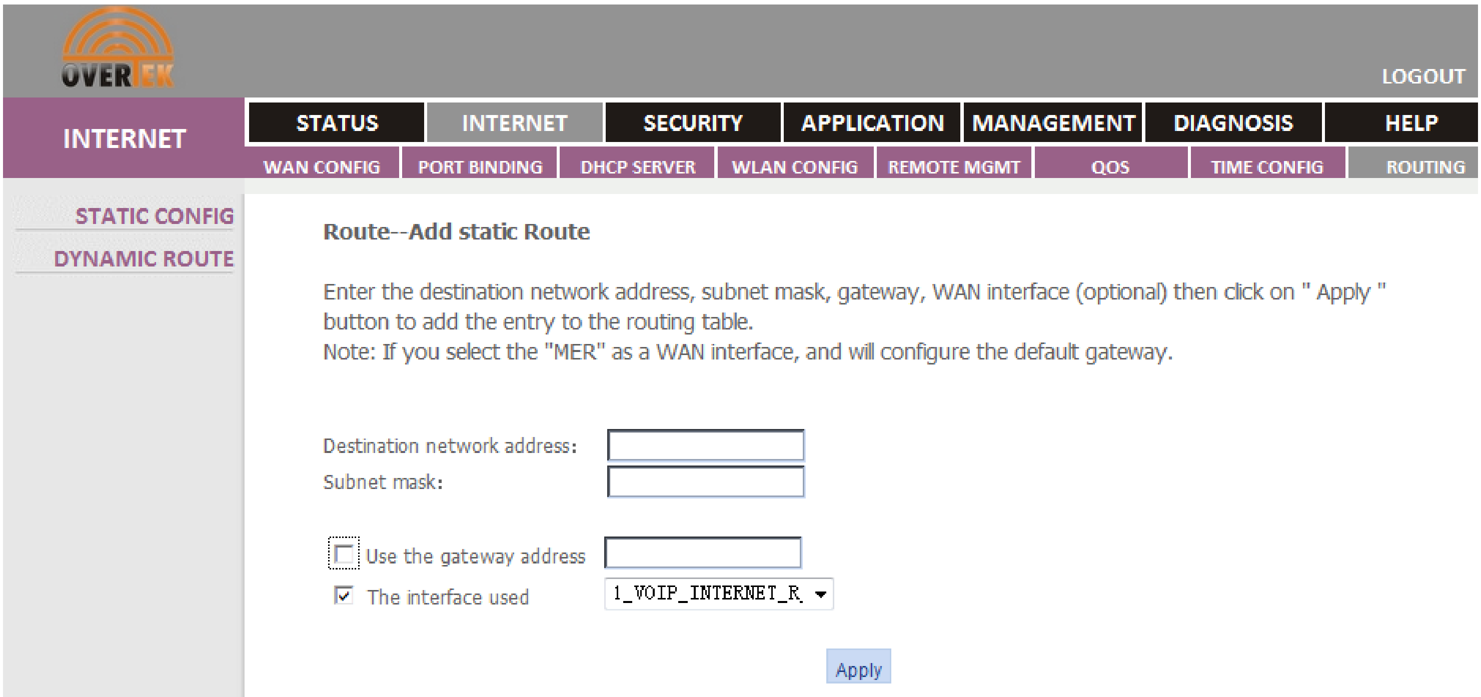
Apply

Auto Sync to NTP Time Servers: Check the box to automatically sync with the available NTP time servers.
Connection Server Mode: To determine the way to connect to NTP servers.
Time Server 1: Select the available NTP servers for your NTP Server 1.
Time Server 2: Select the available NTP servers for your NTP Server 2.
Time Server3: Select the available NTP servers for your NTP Server 3.
Time Server 4: Select the available NTP servers for your NTP Server 4.
Time Server 5: Select the available NTP servers for your NTP Server 5.
Note: You can also specify the URL or IP address for your Time Servers if they are not shown in the options list.
Time Zone: To choose the appropriate Time Zone for your OT-4020VW GEPON ONU.
Apply: Click ' Apply ' button to save and apply new settings.

4.8. Routing

4.8.1. Static Config

Click ' **INTERNET** ' – '**Routing** '– '**Static Config** ', click ' Add' button to config a Static route for your OT-4020VW ONU:



Route--Add static Route

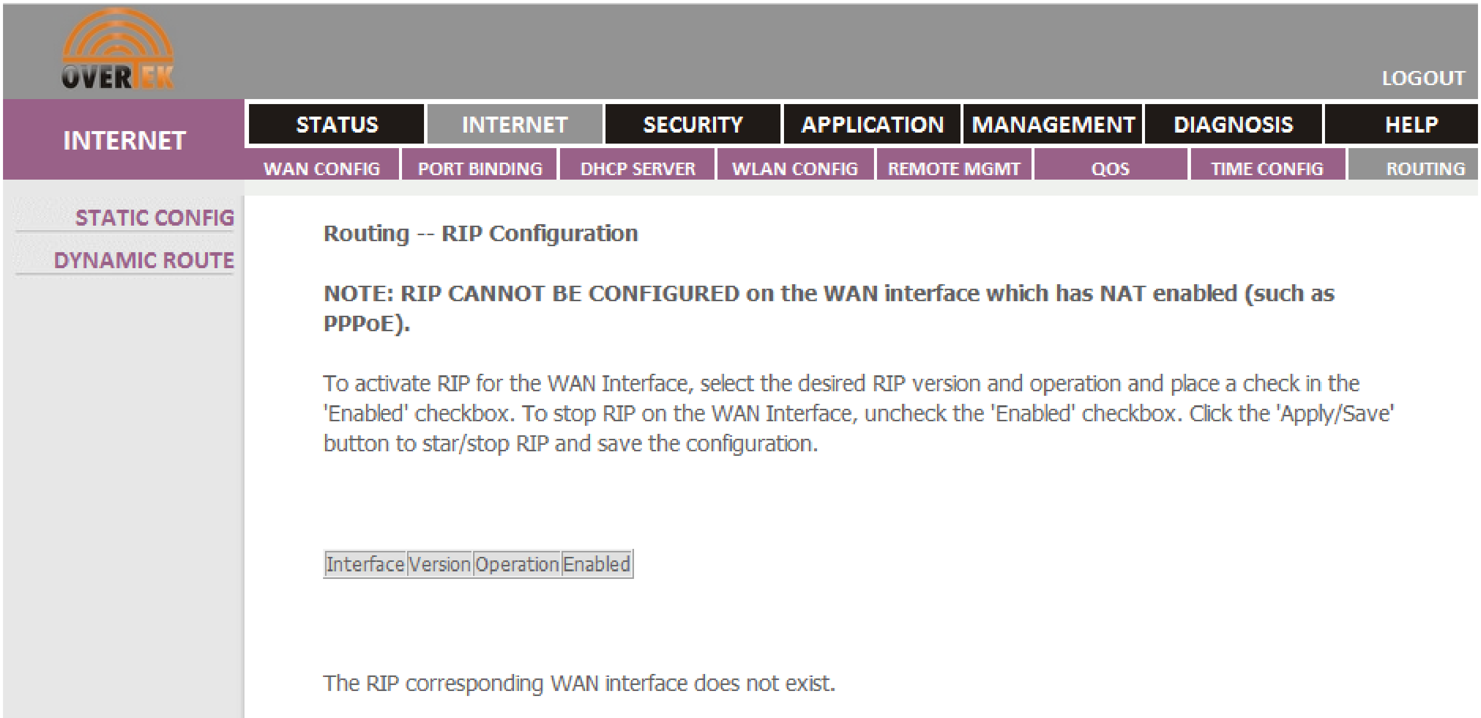
Enter the destination network address, subnet mask, gateway, WAN interface (optional) then click on " Apply " button to add the entry to the routing table.
Note: If you select the "MER" as a WAN interface, and will configure the default gateway.

Destination network address:
Subnet mask:
□ Use the gateway address
☑ The interface used 1_VOIP_INTERNET_R

Destination Network Address: The destination address that you want to add a route for
Subnet Mask: The Subnet Mask for your Destination Routing address
Use Gateway IP Address: The Gateway IP Address for your destination routing address
Use Interface: To determine which interface to enable the Static Route for
Apply: Click ' Apply ' button to save and apply new settings.

4.8.2. Dynamic Route

Click ' **INTERNET** ' – '**Routing** '– '**Dynamic Route** ' to config a Dynamic Route for the LAN interface of your OT-4020VW ONU. When you are connecting your ONU with NAT enabled, you can not configure Dynamic Route. The Dynamic Route is RIP based, you can choose either RIP V1 or RIP V2 to activate Dynamic Route for the LAN interface.



Routing -- RIP Configuration

NOTE: RIP CANNOT BE CONFIGURED on the WAN interface which has NAT enabled (such as PPPoE).

To activate RIP for the WAN Interface, select the desired RIP version and operation and place a check in the 'Enabled' checkbox. To stop RIP on the WAN Interface, uncheck the 'Enabled' checkbox. Click the 'Apply/Save' button to star/stop RIP and save the configuration.

Interface	Version	Operation	Enabled

The RIP corresponding WAN interface does not exist.

Interface: The LAN interface of your OT-4020VW ONU

Version: To determine which RIP Version for the Dynamic Routing

Enable: To enable or disable dynamic routing for the LAN interface

Apply: Click ‘ Apply ‘ button to save and apply new settings.

4.8.3. IPV6 Static Route

Click ‘ **INTERNET** ‘ – ‘**Routing** ‘– ‘**IPV6 Static Route** ‘ to config an IPV6 Static Route for your OT-4020VW ONU.

Add: Click ‘ Add ‘ to add an IPV6 Static Route for your OT-4020VW ONU

Destination IPV6 Address: Input the destination IPV6 address that you want to add a Static Route for

Subnet Prefix Length: To determine the length for your IPV6 Subnet Prefix

Gateway IPV6 Address: Input the Gateway IP address for your destination IPV6 address

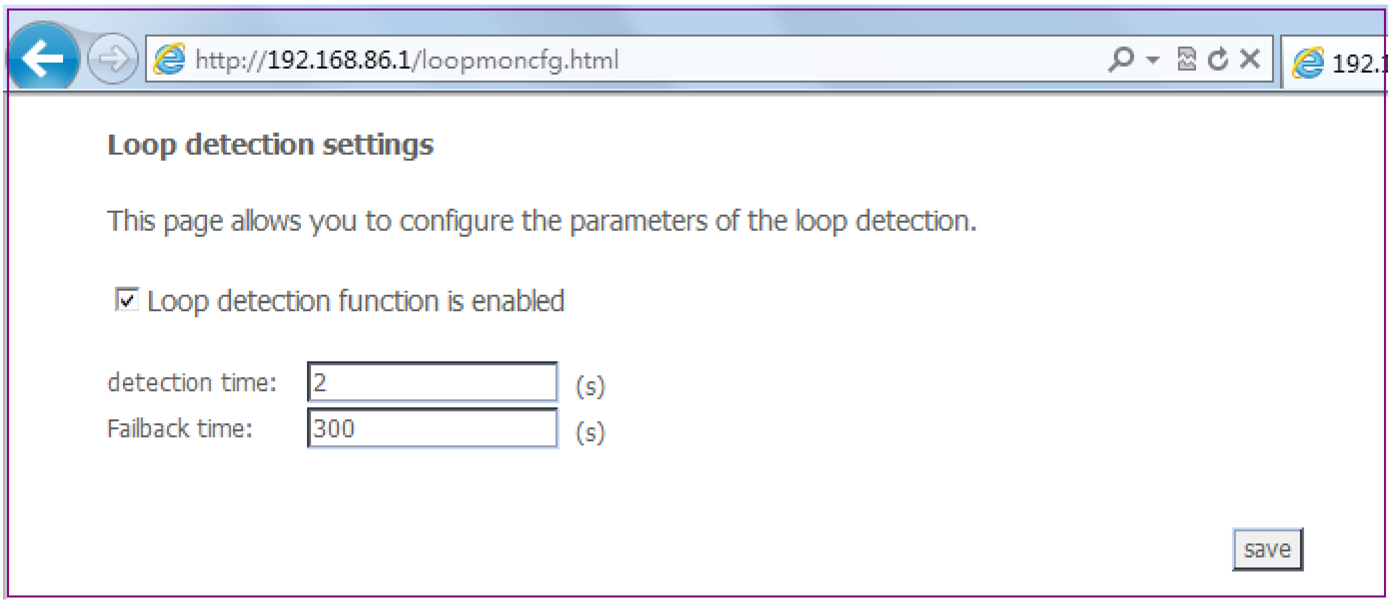
Interface: To determine which WAN interface to associated with the Static IPV6 Route

Metric: To determine the Metric for your IPV6 Static Route (Value in between 0-4261412864)

Apply: Click ‘ Apply ‘ button to save and apply new settings.

4.9. Loop Detection

Open the hidden page http://192.168.86.1/loopmoncfg.html



http://192.168.86.1/loopmoncfg.html

Loop detection settings

This page allows you to configure the parameters of the loop detection.

☑ Loop detection function is enabled

detection time: 2 (s)

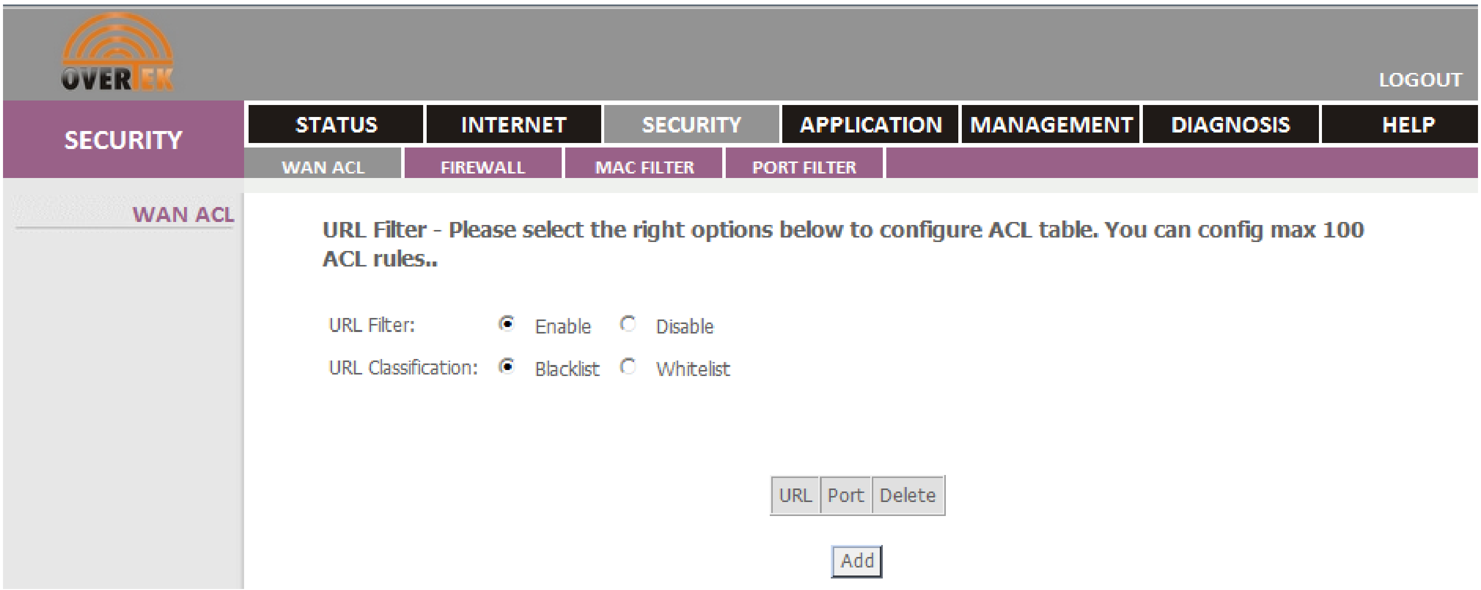
Failback time: 300 (s)

Loop Detection function is enabled: Check the box to enable Loop Detection function.
Detection Time: To config the network loop detecting time interval.
Failback Time: To config the timeout values for your network look detecting request.
Save: Click ‘ Save ‘ button to save and apply new settings.

5. Security

5.1. Wan ACL (Access Control List)

Click ‘ **Security** ’ – ‘**Wan ACL**’– to Enable or Disable URLs to pass through the WAN interface.



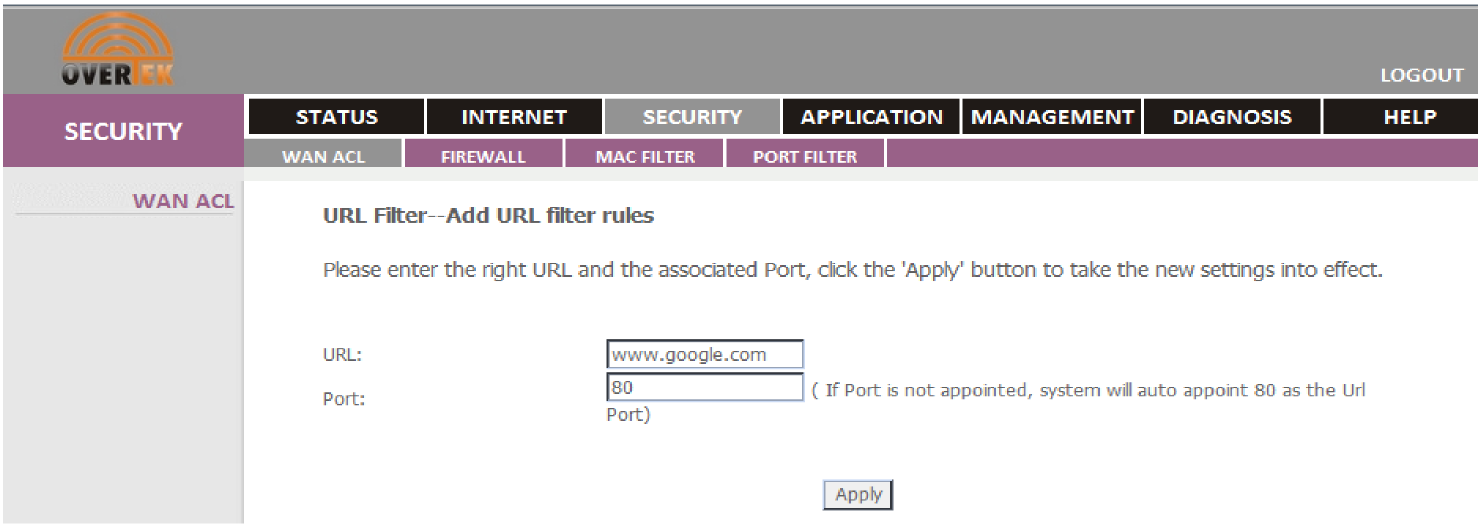
URL Filter - Please select the right options below to configure ACL table. You can config max 100 ACL rules..

URL Filter: ● Enable ○ Disable

URL Classification: ● Blacklist ○ Whitelist

URL	Port	Delete

Url Filter: Check the box on ‘**Enable**’ to enable URL filter, Check the box on ‘**Disable**’ to disable URL Filter
URL Classification:
A. Blacklist: Check the box on ‘Blacklist’ and Click ‘Add’ button to specify a URL in blacklist.



URL Filter--Add URL filter rules

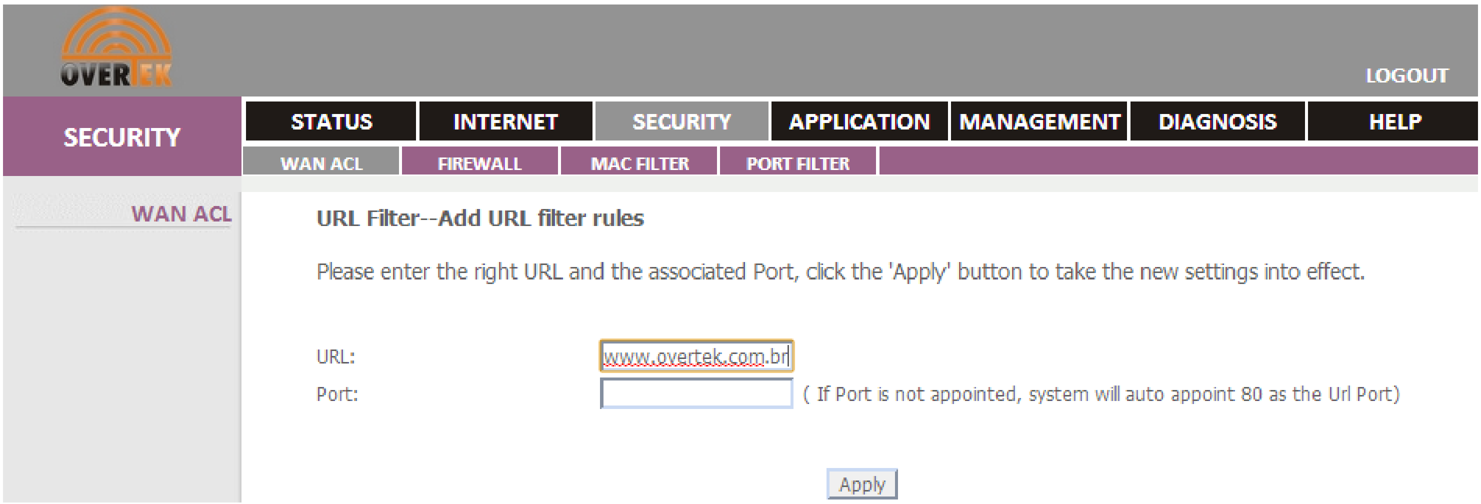
Please enter the right URL and the associated Port, click the 'Apply' button to take the new settings into effect.

URL: www.google.com

Port: 80 (If Port is not appointed, system will auto appoint 80 as the Url Port)

Apply: Click ' **Apply** ' button to save and apply new settings.

B. Whitelist : Check the box on '**Whitelist**' and Click ' **Add** ' button to specify a URL in whitelist.



URL Filter--Add URL filter rules

Please enter the right URL and the associated Port, click the 'Apply' button to take the new settings into effect.

URL: www.overtek.com.br

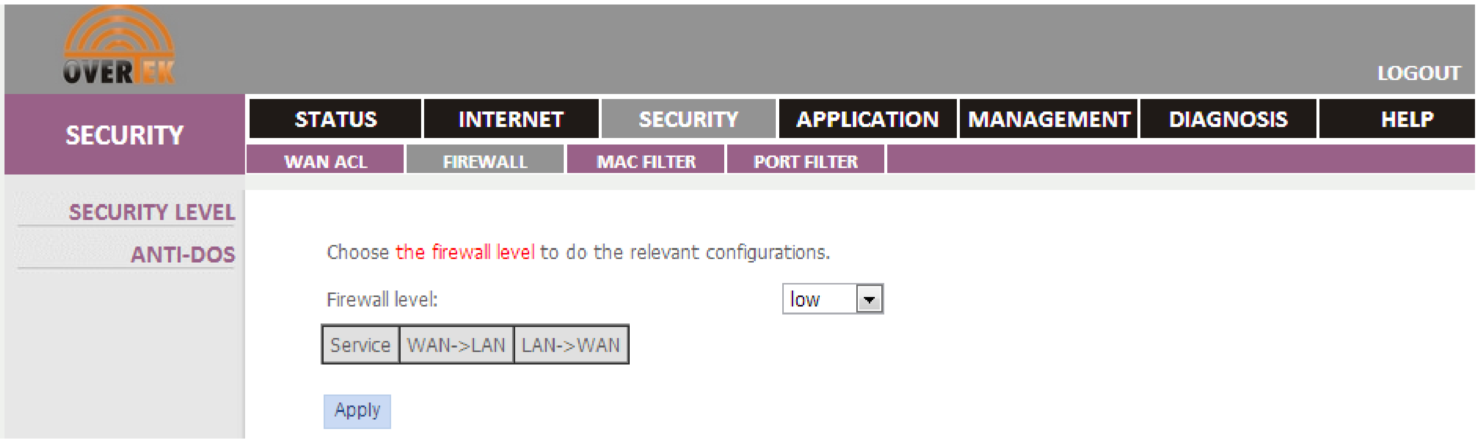
Port: (If Port is not appointed, system will auto appoint 80 as the Url Port)

URL: The URL address that you want to allow access with.
Port Number: The port number that you want to enable for the whitelist URL.
Apply: Click ' **Apply** ' button to save and apply new settings.

5.2. Firewall

5.2.1. Security Level

Click ' **Security** ' – '**Security Level** '– to set the firewall level for the multiple services pass-through the OT-4020VW ONU. Click '**Apply**' to save and apply new settings.



Choose the firewall level to do the relevant configurations.

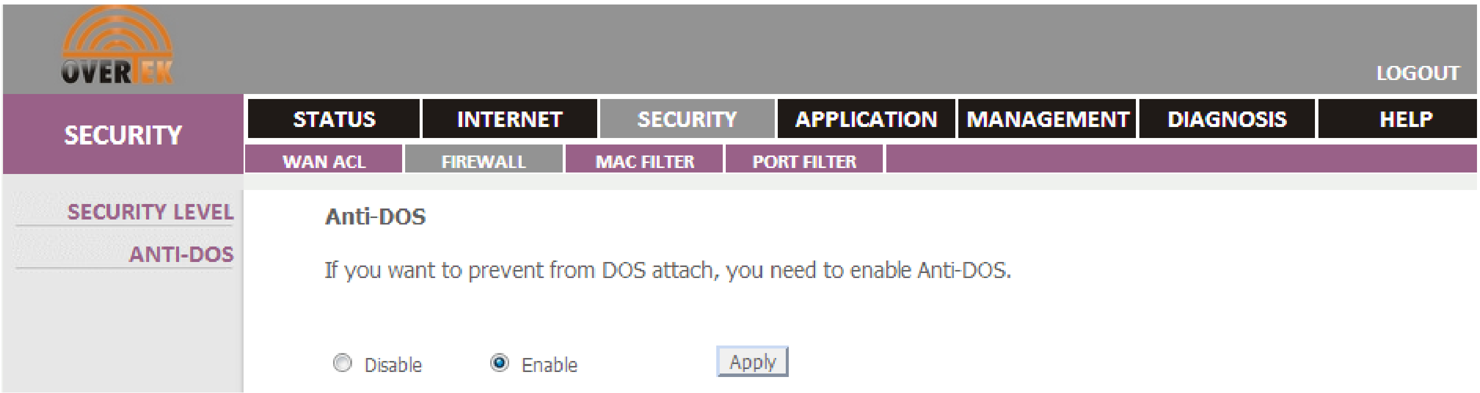
Firewall level: low

Service | WAN->LAN | LAN->WAN

Apply

5.2.2. ANTI-DOS

Click **' Security** ' – '**Firewall** '– '**ANTI-DOS**' to prevent OT-4020VW ONU from DOS attack.



Anti-DOS

If you want to prevent from DOS attach, you need to enable Anti-DOS.

○ Disable ● Enable Apply

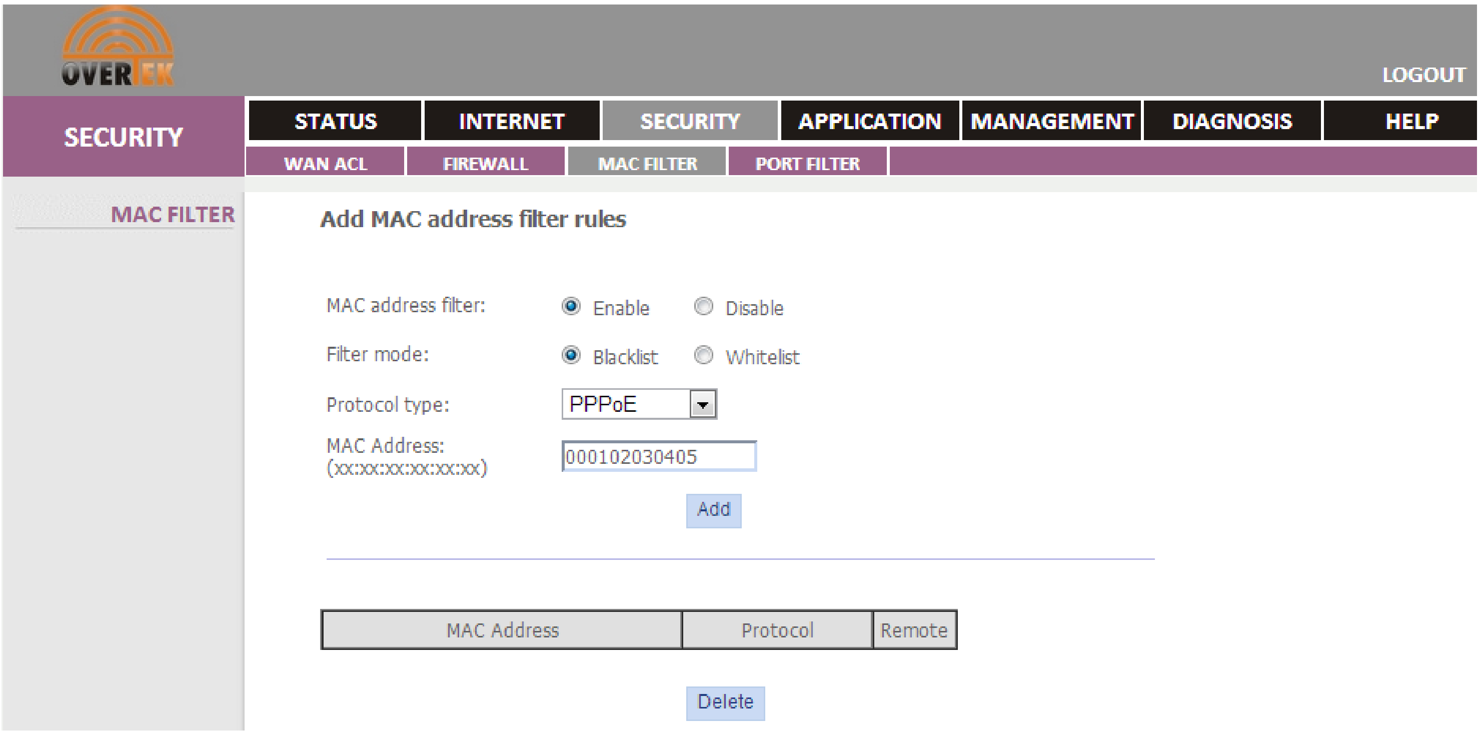
Disable: To disable protection for DOS attack

Enable: To enable protection for DOS attack

Apply: Click ' **Apply** ' button to save and apply new settings.

5.3. MAC Filter

Click ' Security ' – 'MAC Filter '– to creat a firewall filter based on a specific MAC Address.



Add MAC address filter rules

MAC address filter: ● Enable ○ Disable

Filter mode: ● Blacklist ○ Whitelist

Protocol type: PPPoE

MAC Address: (xx:xx:xx:xx:xx:xx) 000102030405

MAC Address	Protocol	Remote

Enable: Enable to creat a filter based on MAC address

Disable: Disable to creat a filter based on MAC address

Blacklist: Enable banning a specific MAC Address

Whiltelist: Enable allowing a specific MAC Address

Protocol: To determine which service to be allowed or denied with the appointed MAC address

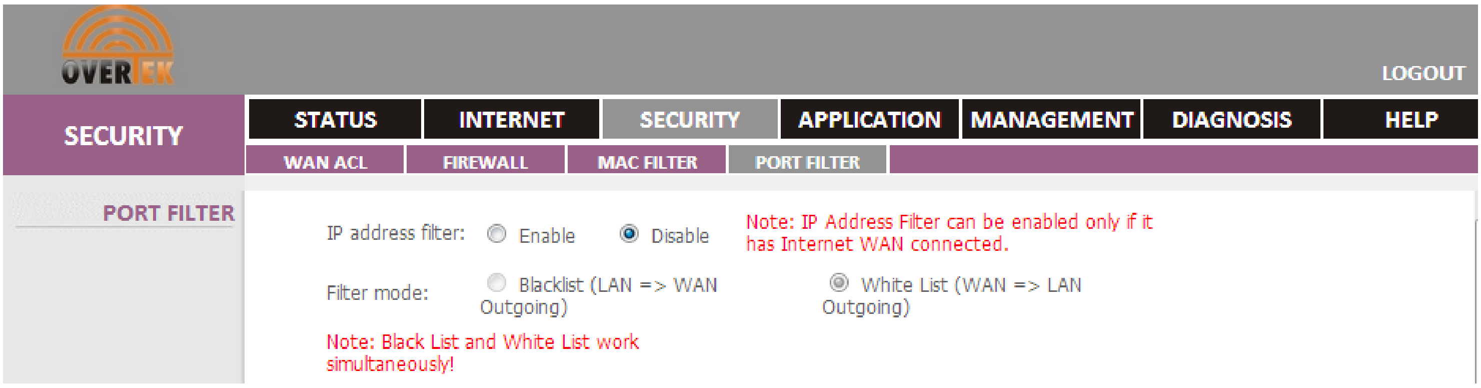
MAC Address: The MAC address that you want to add the MAC Address filter for

Add: Click ‘ Add ‘ button to add a MAC Address filter

Delete: Click ‘ Delete ‘ button to delete a MAC Address filter that you created

5.4. Port Filter

Click ‘ **Security** ‘ – ‘**Port Filter** ‘– to creat a firewall filter based on a specific port.



IP address filter: ○ Enable ● Disable

Note: IP Address Filter can be enabled only if it has Internet WAN connected.

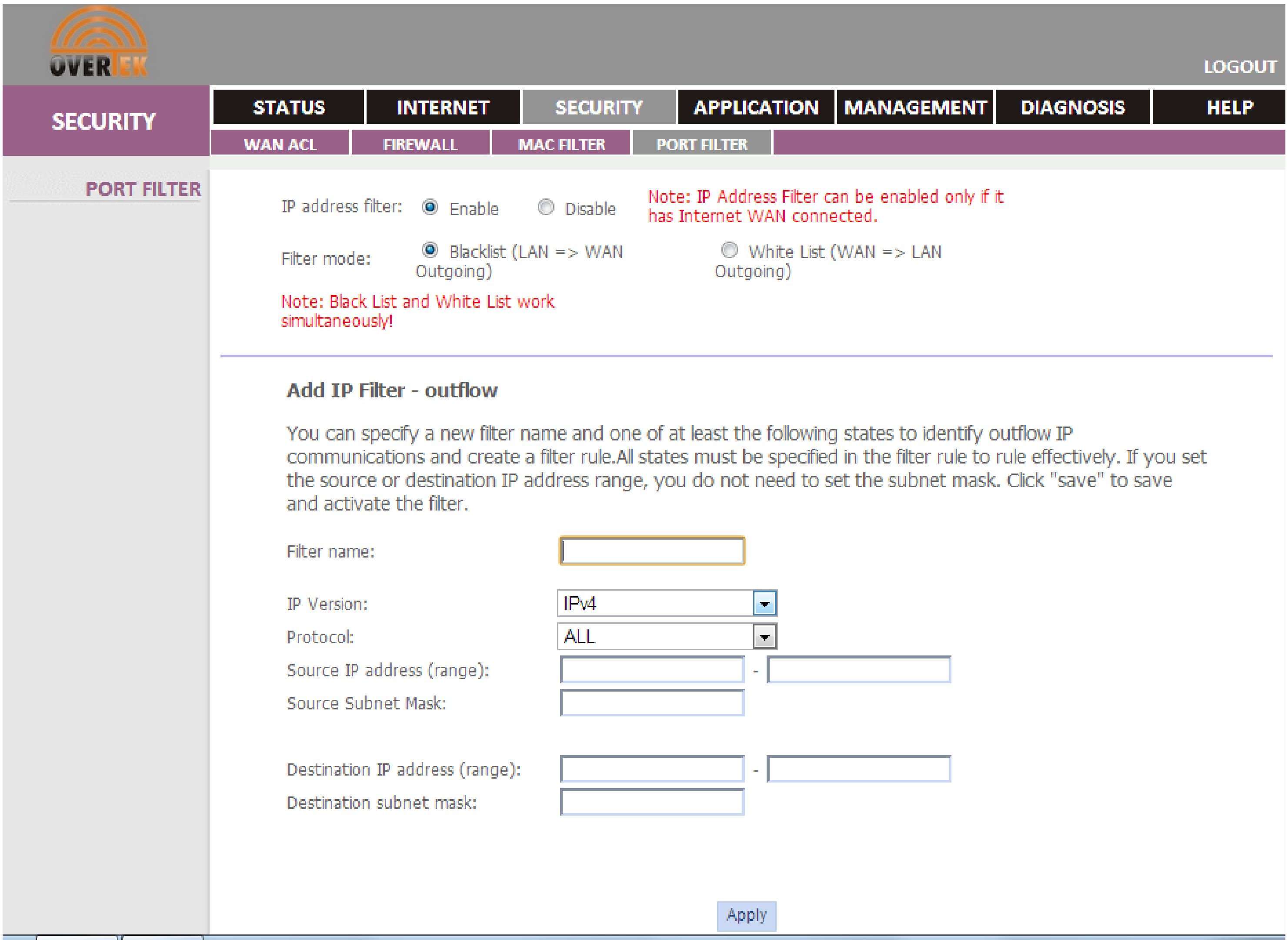
Filter mode: ○ Blacklist (LAN => WAN Outgoing) ● White List (WAN => LAN Outgoing)

Note: Black List and White List work simultaneously!

Enable: To enable the port filter

Disable: To disable the port filter

A. Blacklist (LAN-WAN Flow filtration): To disable the specified port to pass through LAN to WAN



IP address filter: ● Enable ○ Disable

Note: IP Address Filter can be enabled only if it has Internet WAN connected.

Filter mode: ● Blacklist (LAN => WAN Outgoing) ○ White List (WAN => LAN Outgoing)

Note: Black List and White List work simultaneously!

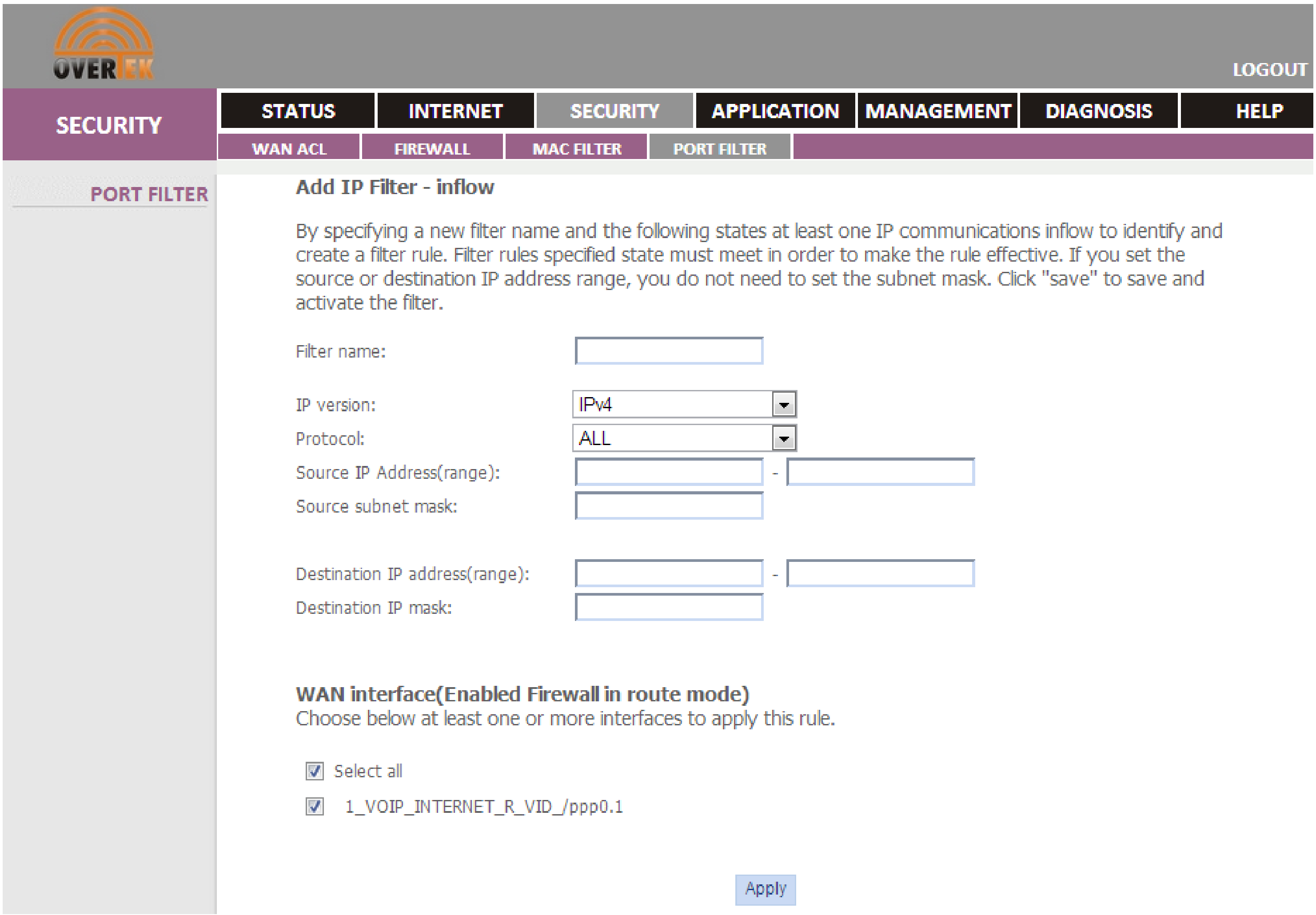
Add IP Filter - outflow

You can specify a new filter name and one of at least the following states to identify outflow IP communications and create a filter rule.All states must be specified in the filter rule to rule effectively. If you set the source or destination IP address range, you do not need to set the subnet mask. Click "save" to save and activate the filter.

Filter name:	
IP Version:	IPv4
Protocol:	ALL
Source IP address (range):	-
Source Subnet Mask:	
Destination IP address (range):	-
Destination subnet mask:	

Filter Name: To specify a name for the filter
IP Version: To determine either IPV4 or IPV6 version for the filter
Protocol: To determine which protocol to be allowed or denied
Source IP Address range: The IP Address range that you want to allow or deny. E.g, 192.168.1.2 – 192.168.1.254
Source Subnet Mask: The subnet mask that for the IP range that you specified
Source Port: The Port Number for which you want to allow or deny
Destination IP Address: The Destination IP or host that you want to allow or deny for the filter
Destination Subnet Mask: The Subnet Mask for the Destination IP or host that you allowed or denied
Destination Port: The Port Number for the Destination IP or host that you allowed or denied.
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

B. White list (WAN-LAN into the filter): To enable the specified port to pass through WAN to LAN



Add IP Filter - inflow

By specifying a new filter name and the following states at least one IP communications inflow to identify and create a filter rule. Filter rules specified state must meet in order to make the rule effective. If you set the source or destination IP address range, you do not need to set the subnet mask. Click "save" to save and activate the filter.

Filter name:

IP version: IPv4

Protocol: ALL

Source IP Address(range): -

Source subnet mask:

Destination IP address(range): -

Destination IP mask:

WAN interface(Enabled Firewall in route mode)

Choose below at least one or more interfaces to apply this rule.

☑ Select all

☑ 1_VOIP_INTERNET_R_VID_/ppp0.1

Filter Name: To specify a name for the filter

IP Version: To determine either IPV4 or IPV6 version for the filter

Protocol: To determine which protocol to be allowed or denied

Source IP Address range: The IP Address range that you want to allow or deny. E.g, 192.168.1.2 – 192.168.1.254

Source Subnet Mask: The subnet mask that for the IP range that you specified

Destination IP Address: The Destination IP or host that you want to allow or deny for the filter

Destination Subnet Mask: The Subnet Mask for the Destination IP or host that you allowed or denied

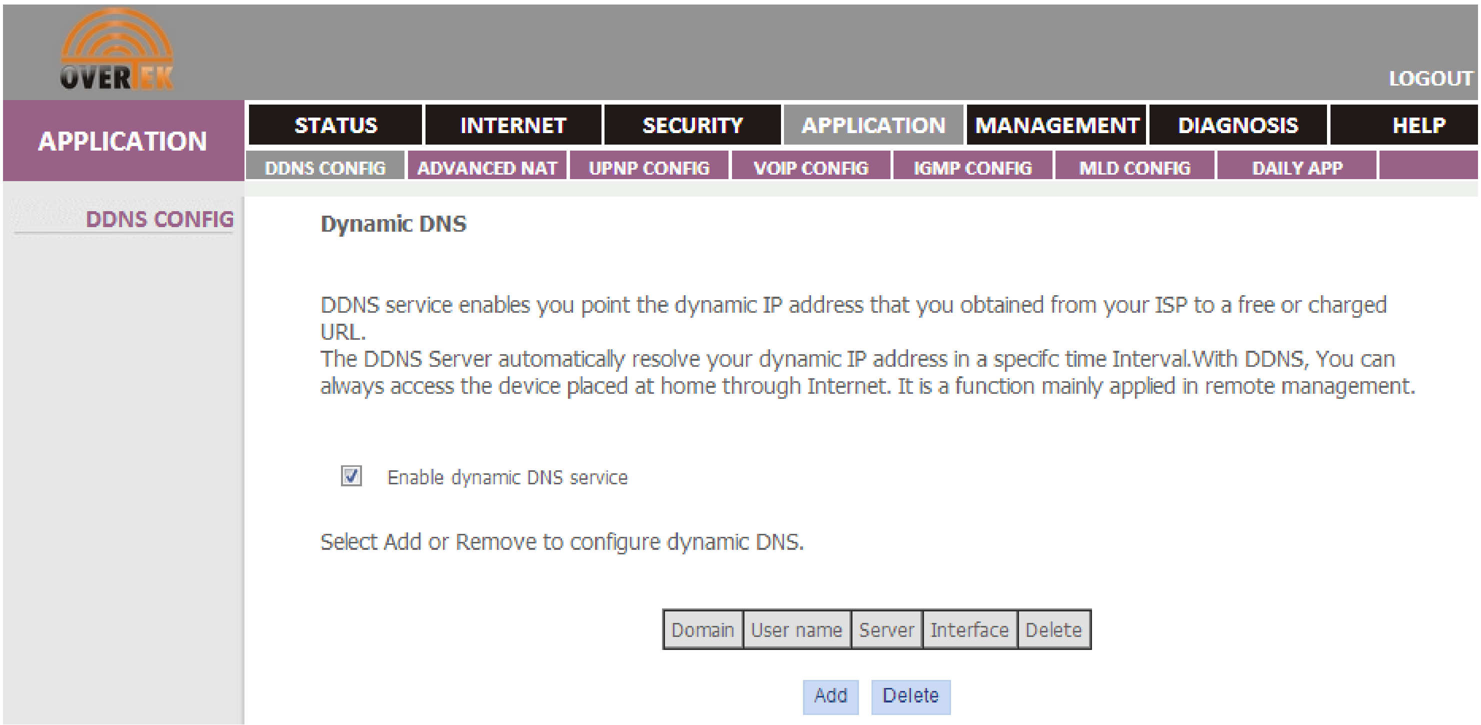
Destination Port: The Port Number for the Destination IP or host that you allowed or denied.

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6. Application

6.1. DDNS config

Click ‘ **Application** ‘ – ‘**DDNS config** ‘– to creat a Dynamic DNS for your OT-4020VW ONU.



Dynamic DNS

DDNS service enables you point the dynamic IP address that you obtained from your ISP to a free or charged URL.
The DDNS Server automatically resolve your dynamic IP address in a specifc time Interval.With DDNS, You can always access the device placed at home through Internet. It is a function mainly applied in remote management.

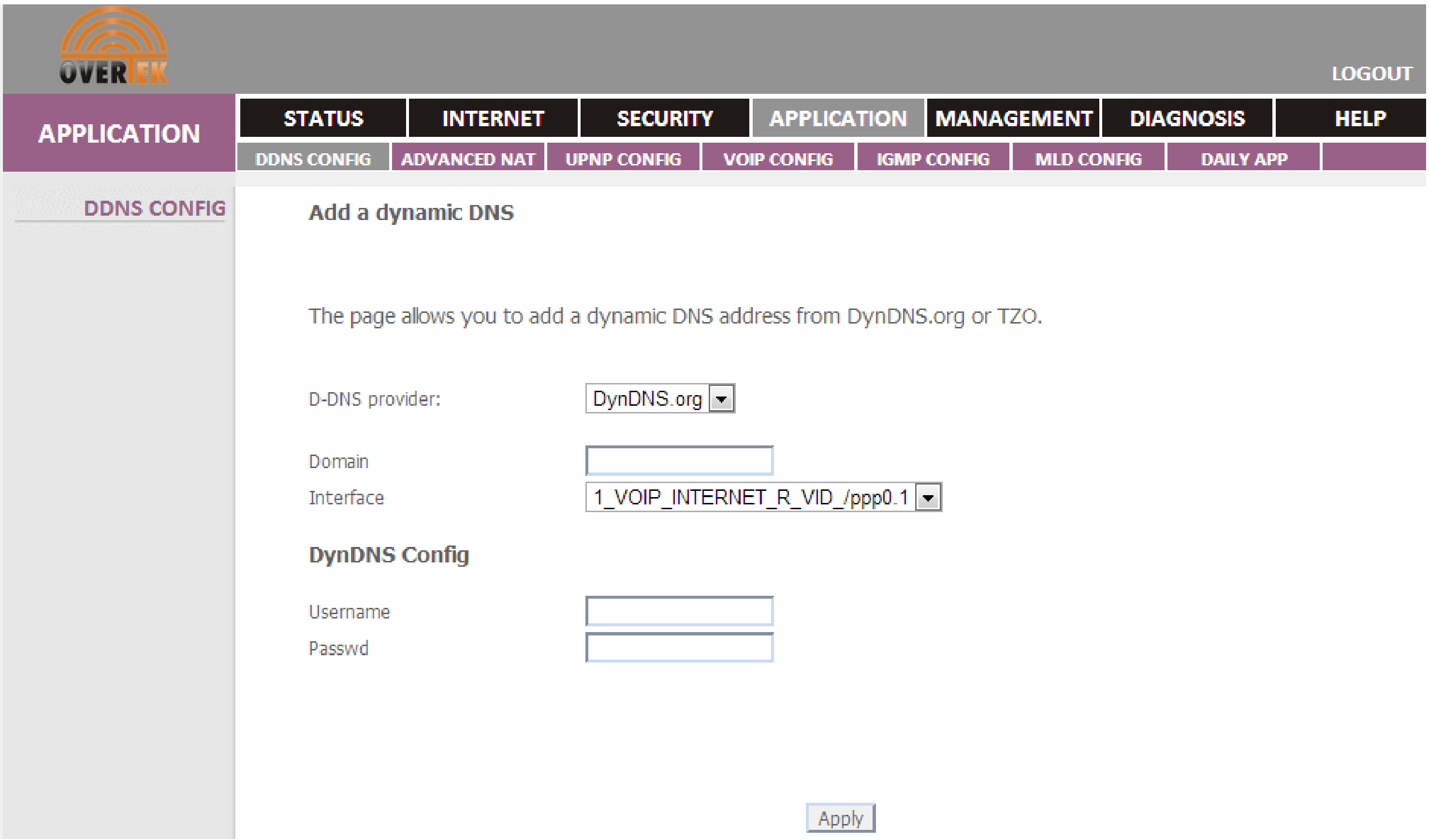
☑ Enable dynamic DNS service

Select Add or Remove to configure dynamic DNS.

Domain	User name	Server	Interface	Delete

Enable Dynamic DNS Service: Check the box to enable Dynamic DNS service

Add: Click 'Add' to add a Dynamic DNS connection



Add a dynamic DNS

The page allows you to add a dynamic DNS address from DynDNS.org or TZO.

D-DNS provider: DynDNS.org

Domain

Interface 1_VOIP_INTERNET_R_VID_/ppp0.1

DynDNS Config

Username

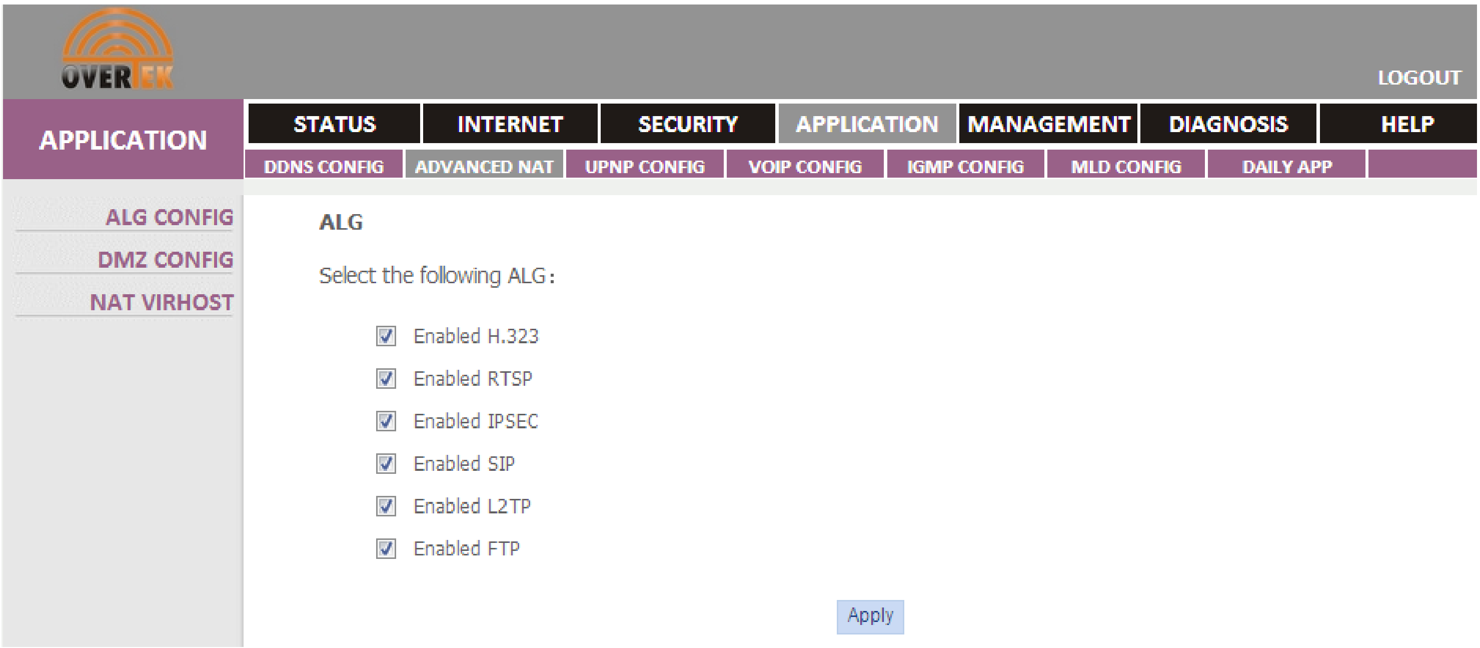
Passwd

D-DNS provider: To determine the DDNS service provider
Domain: The Url/Host name for your DDNS service provider
Interface: To determine which WAN connection to be applied with DDNS service
User Name: Your DDNS user name
Password: Your DDNS password
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.2. Advanced NAT Config

6.2.1. ALG Config

Click **‘ Application** ‘ – ‘**Advanced NAT** ‘- ‘**ALG Config** ‘– to config the Applicatoin Layer Gateway for your OT-4020VW ONU.



ALG

Select the following ALG:

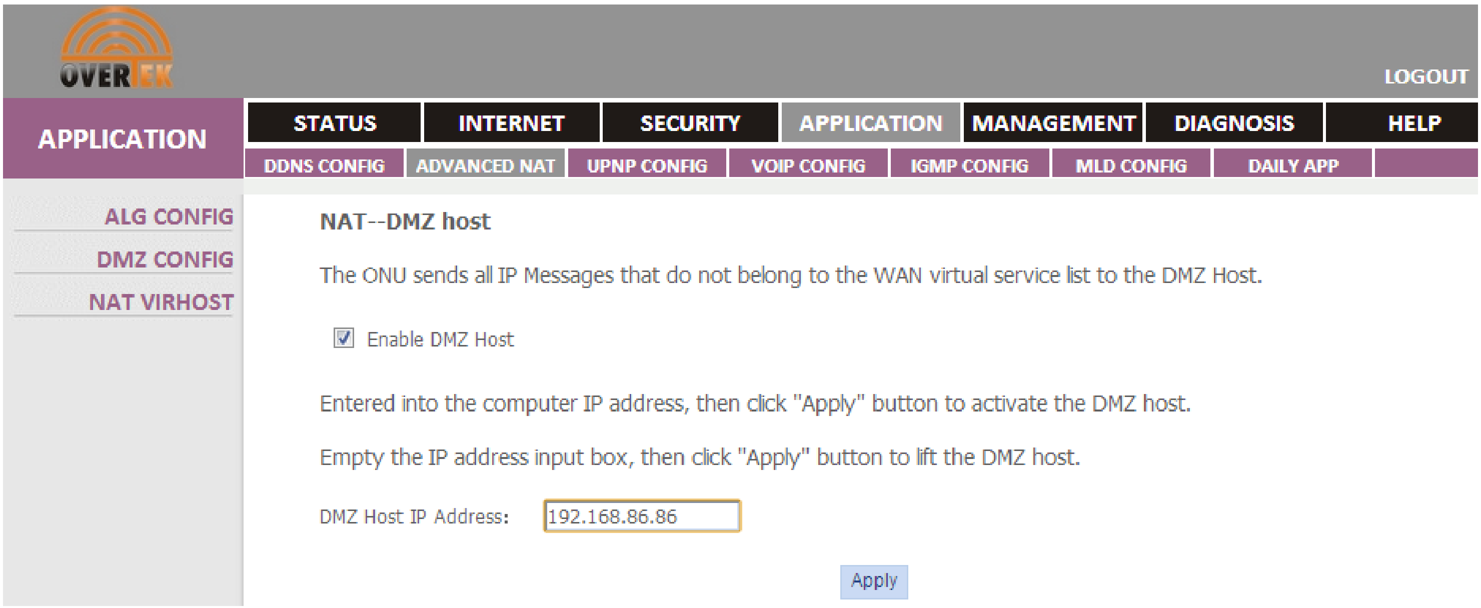
☑ Enabled H.323
☑ Enabled RTSP
☑ Enabled IPSEC
☑ Enabled SIP
☑ Enabled L2TP
☑ Enabled FTP

Enabled H.323: Check the box to enable H.323 ALG
Enabled RTSP: Check the box to enable RTSP ALG
Enabled IPSEC: Check the box to enable RTSP ALG
Enabled SIP: Chek the box to enable SIP ALG

Enabled L2TP: Check the box to enable L2TP ALG
Enabled FTP: Check the box to enable FTP ALG
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.2.2. DMZ Config

Click ' **Application** ' – '**Advanced NAT** '– '**DMZ Config** '– to config DMZ host for your OT-4020VW ONU.



NAT--DMZ host

The ONU sends all IP Messages that do not belong to the WAN virtual service list to the DMZ Host.

☑ Enable DMZ Host

Entered into the computer IP address, then click "Apply" button to activate the DMZ host.

Empty the IP address input box, then click "Apply" button to lift the DMZ host.

DMZ Host IP Address: 192.168.86.86

Apply

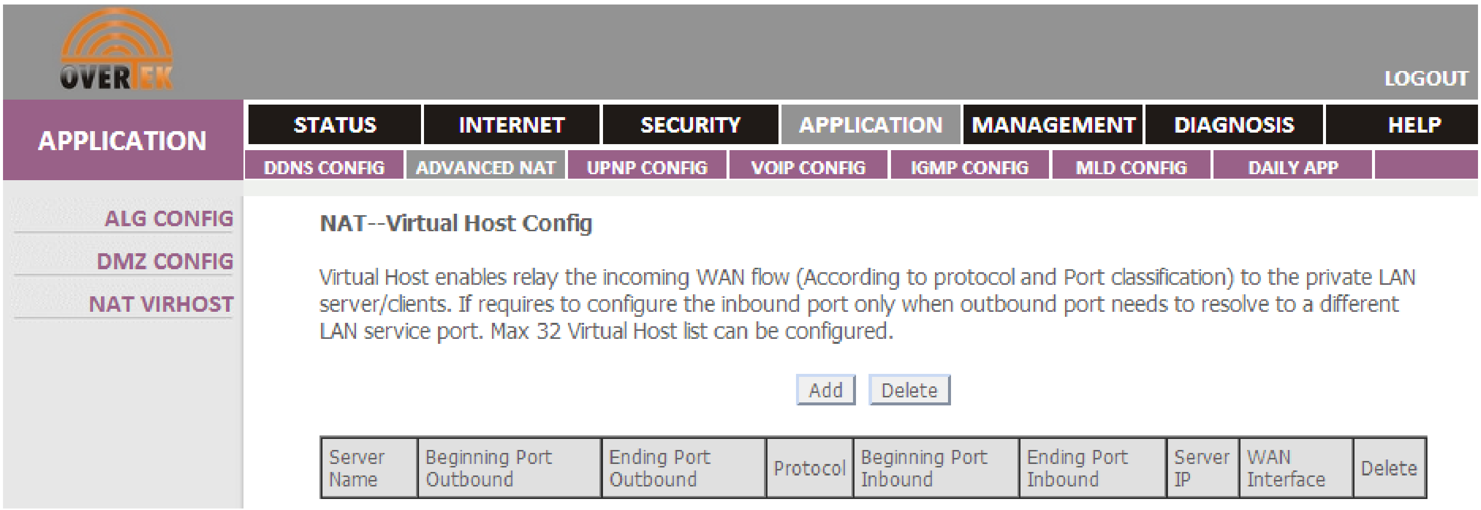
Enable DMZ Host: Check the box to enable DMZ

DMZ Host IP Address: The LAN IP address that you want to enable with DMZ

Apply: Click ' **Apply** ' button to save and apply new settings.

6.2.3. Virtual Host Config

Click ' **Application** ' – '**Advanced NAT** '– '**Virtual Host** '– to config Virtual Host (Also called port forwarding) for your OT-4020VW ONU.



NAT--Virtual Host Config

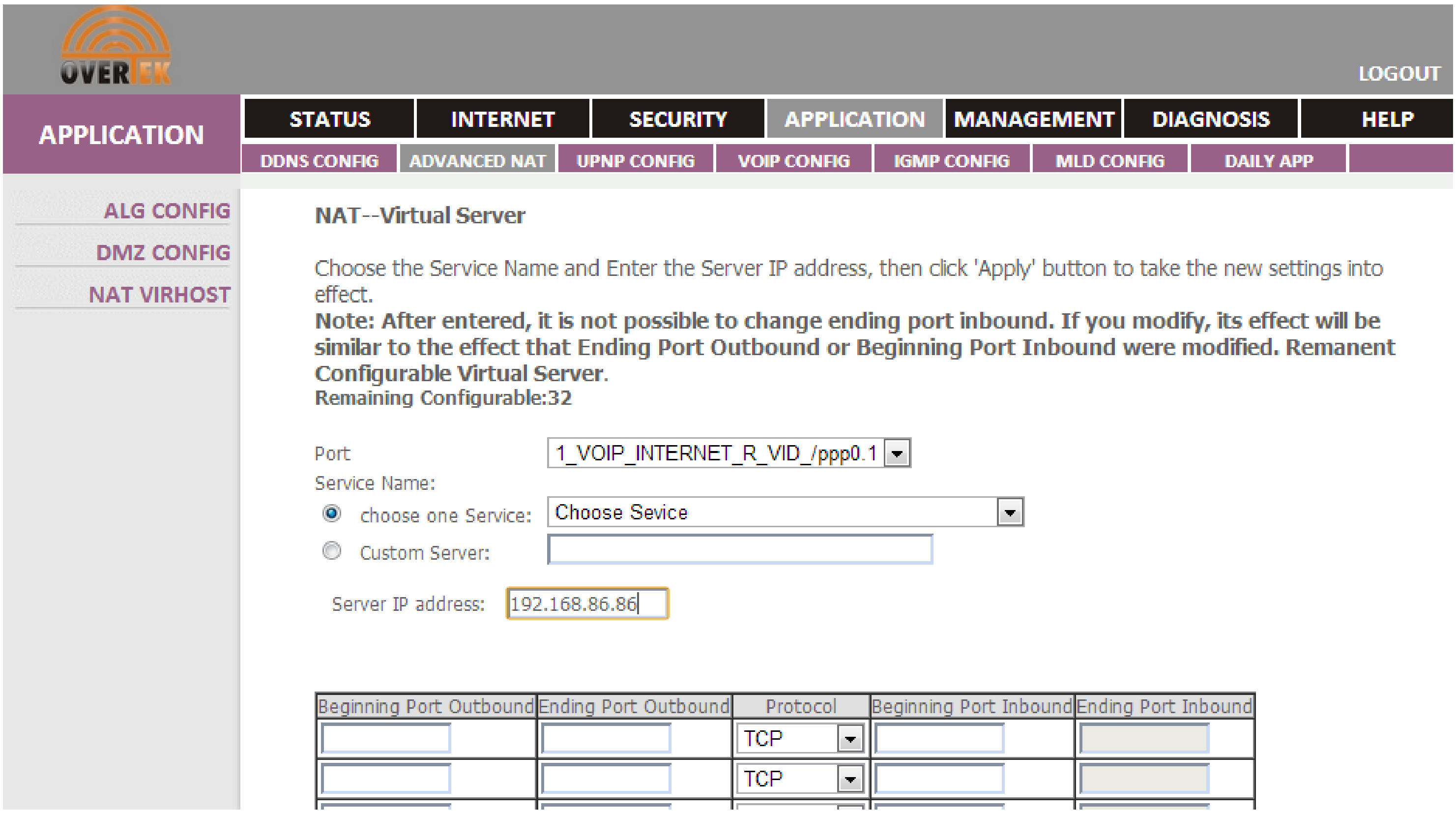
Virtual Host enables relay the incoming WAN flow (According to protocol and Port classification) to the private LAN server/clients. If requires to configure the inbound port only when outbound port needs to resolve to a different LAN service port. Max 32 Virtual Host list can be configured.

Add Delete

Server Name	Beginning Port Outbound	Ending Port Outbound	Protocol	Beginning Port Inbound	Ending Port Inbound	Server IP	WAN Interface	Delete

Add: Click ' Add ' to add a virtual host server

Delete: Click ' Delete' to remove a Virtual Host Server



NAT--Virtual Server

Choose the Service Name and Enter the Server IP address, then click 'Apply' button to take the new settings into effect.

Note: After entered, it is not possible to change ending port inbound. If you modify, its effect will be similar to the effect that Ending Port Outbound or Beginning Port Inbound were modified. Remanent Configurable Virtual Server.

Remaining Configurable:32

Port: 1_VOIP_INTERNET_R_VID_/ppp0.1

Service Name:

● choose one Service: Choose Sevice

○ Custom Server:

Server IP address: 192.168.86.86

Beginning Port Outbound	Ending Port Outbound	Protocol	Beginning Port Inbound	Ending Port Inbound
		TCP		
		TCP		

Port: The WAN interface that you want to enable with Virtual Host Server service

Service Name: Select the services that you want to enable with Virtual Host Server service

Server IP Address: The LAN IP address that you want to enable for Virtual Host Server

Beginning Port Outbound: The outbound beginning port of your Virtual Host server.

Ending Port Outbound: The outbound ending port of your Virtual Host Server

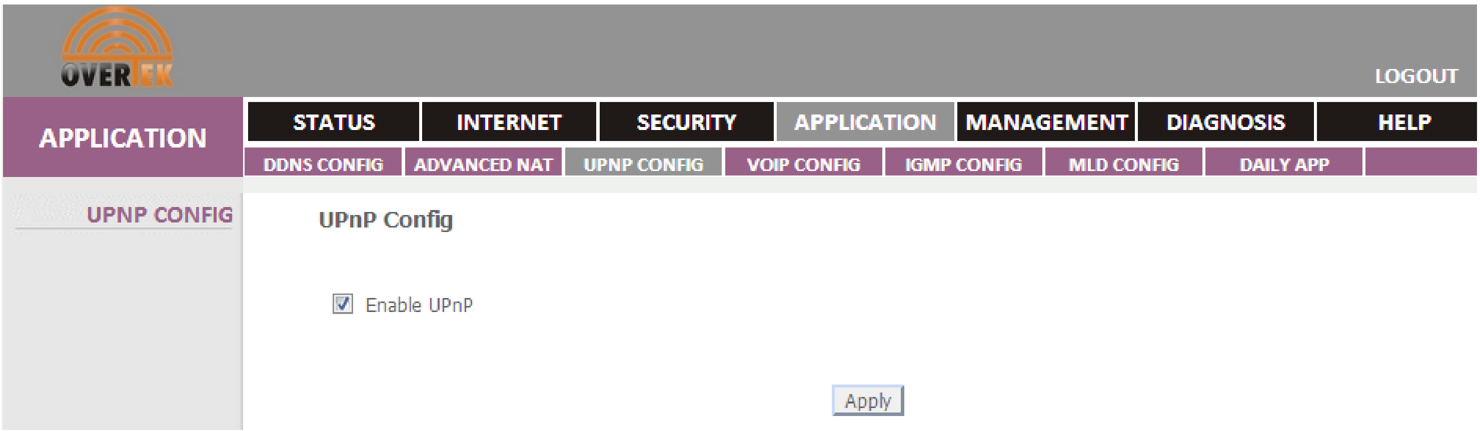
Beginning Port Inbound: The outbound beginning port of your Virtual Host server.

Ending Port Inbound: The outbound ending port of your Virtual Host Server

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.3. Upnp Config

Click ‘ **Application** ‘ – ‘**Upnp Config** ‘– to enable or disable UPNP.



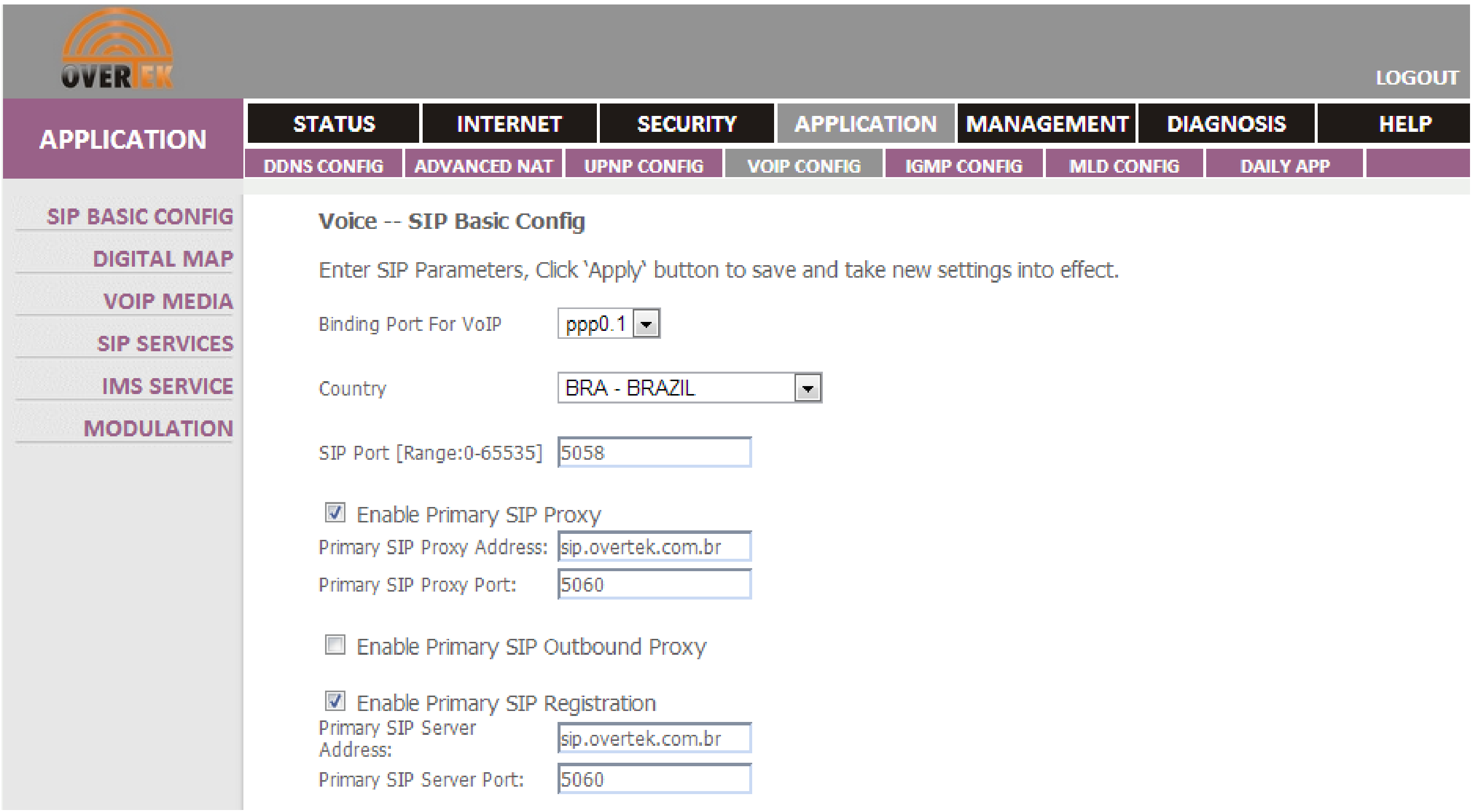
UPnP Config

☑ Enable UPnP

6.4. VoIP Config

6.4.1. SIP Basic Config

Click ‘ **Application** ‘ – ‘**VoIP Config** ‘– ‘**SIP Basic Config** ‘ to configure main VoIP Parameters.



Voice -- SIP Basic Config

Enter SIP Parameters, Click 'Apply' button to save and take new settings into effect.

Binding Port For VoIP: ppp0.1

Country: BRA - BRAZIL

SIP Port [Range:0-65535]: 5058

☑ Enable Primary SIP Proxy

Primary SIP Proxy Address: sip.overtek.com.br

Primary SIP Proxy Port: 5060

☐ Enable Primary SIP Outbound Proxy

☑ Enable Primary SIP Registration

Primary SIP Server Address: sip.overtek.com.br

Primary SIP Server Port: 5060

Bound Port For VoIP: Check the box to select the WAN connection interface for your VoIP service.

Country: Choose the country/territory name available in the template.

Sip local port (0-65535): To input the port number for SIP, generally default SIP port is 5058

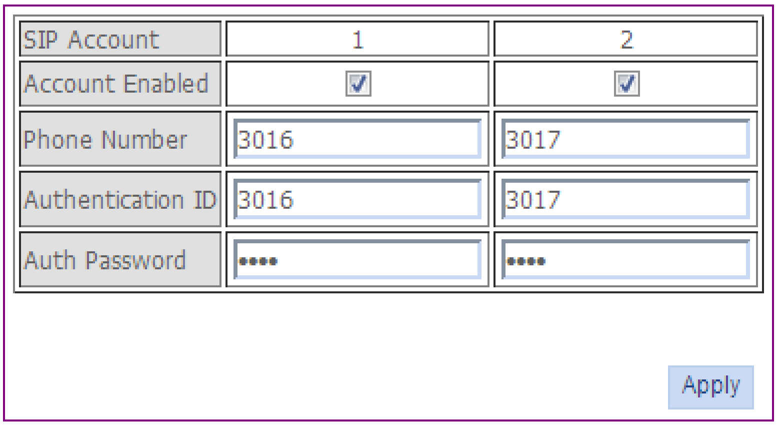
Enable Primary SIP Proxy: Check the box to enable register to a SIP Server

Primary SIP Proxy Address: The primary SIP Server address, can be Host name or IP address

Primary SIP Proxy port: The primary SIP port, the default SIP port is 5060

Enable Primary SIP Registration: Check the box to enable primary SIP registration.

SIP Accounts Configuration

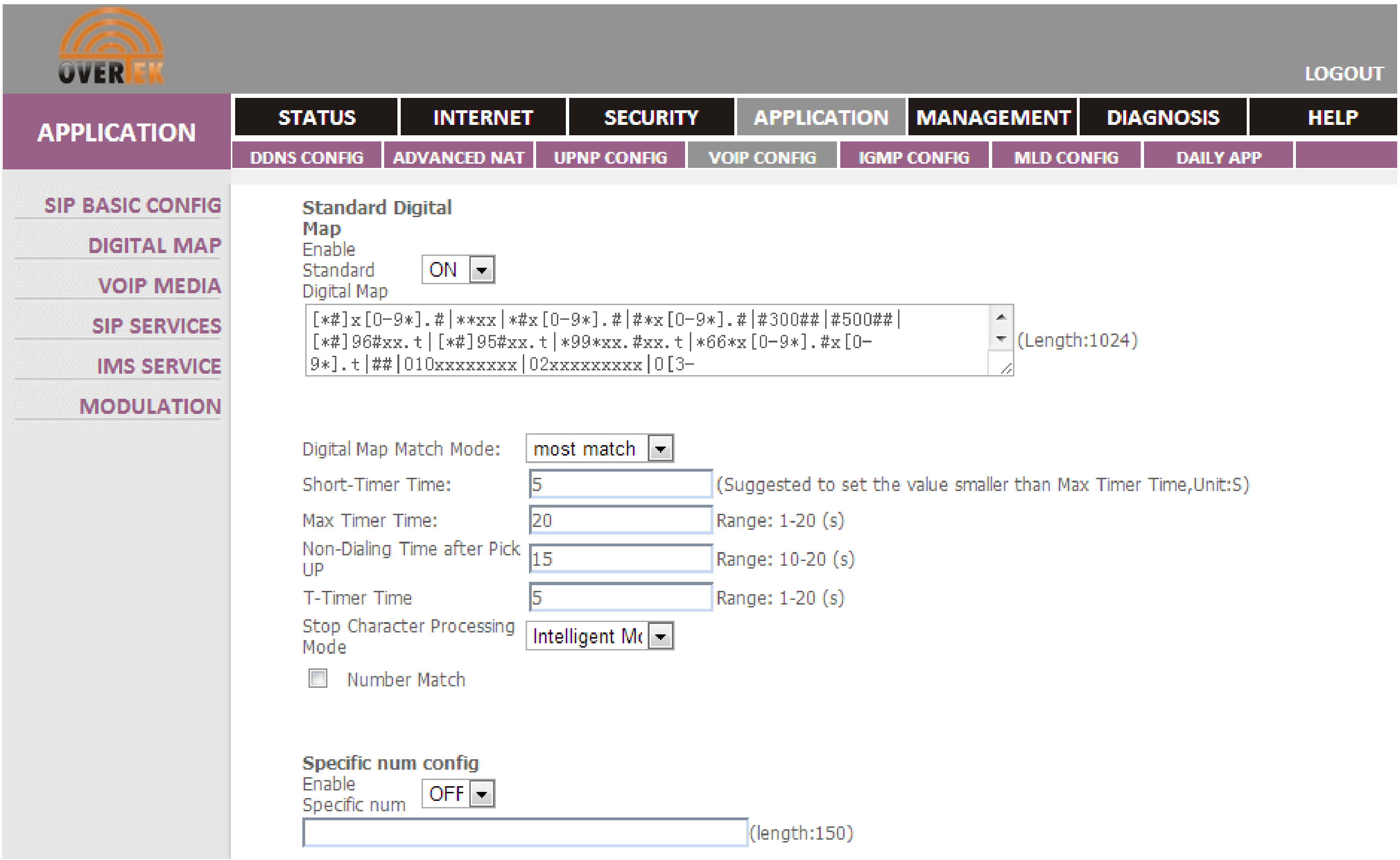


SIP Account	1	2
Account Enabled	☑	☑
Phone Number	3016	3017
Authentication ID	3016	3017
Auth Password	••••	••••

SIP Account 1, 2: There are two SIP accounts able to be registered with OT-4020VW simultaneously.
Account Enabled: Check the boxes to enable the associated SIP 1 and SIP 2 accounts.
User Number: The SIP User name
SIP password: The password for your SIP Account
Preferred ptime: The preferred inquiry time (ms)
Preferred codec 1, 2, 3, 4: The preferred Voice codecs
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.4.2. Digital Map

Click ‘ **Application** ‘ – ‘**VoIP Config** ‘– ‘**Digital Map** ‘ to configure the Dial plan Parameters.



Standard Digital Map

Enable Standard Digital Map: ON

```
[*#]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|02xxxxxxxxx|0[3-
```

(Length:1024)

Digital Map Match Mode: most match
Short-Timer Time: 5 (Suggested to set the value smaller than Max Timer Time,Unit:S)
Max Timer Time: 20 Range: 1-20 (s)
Non-Dialing Time after Pick UP: 15 Range: 10-20 (s)
T-Timer Time: 5 Range: 1-20 (s)
Stop Character Processing Mode: Intelligent Mo
□ Number Match

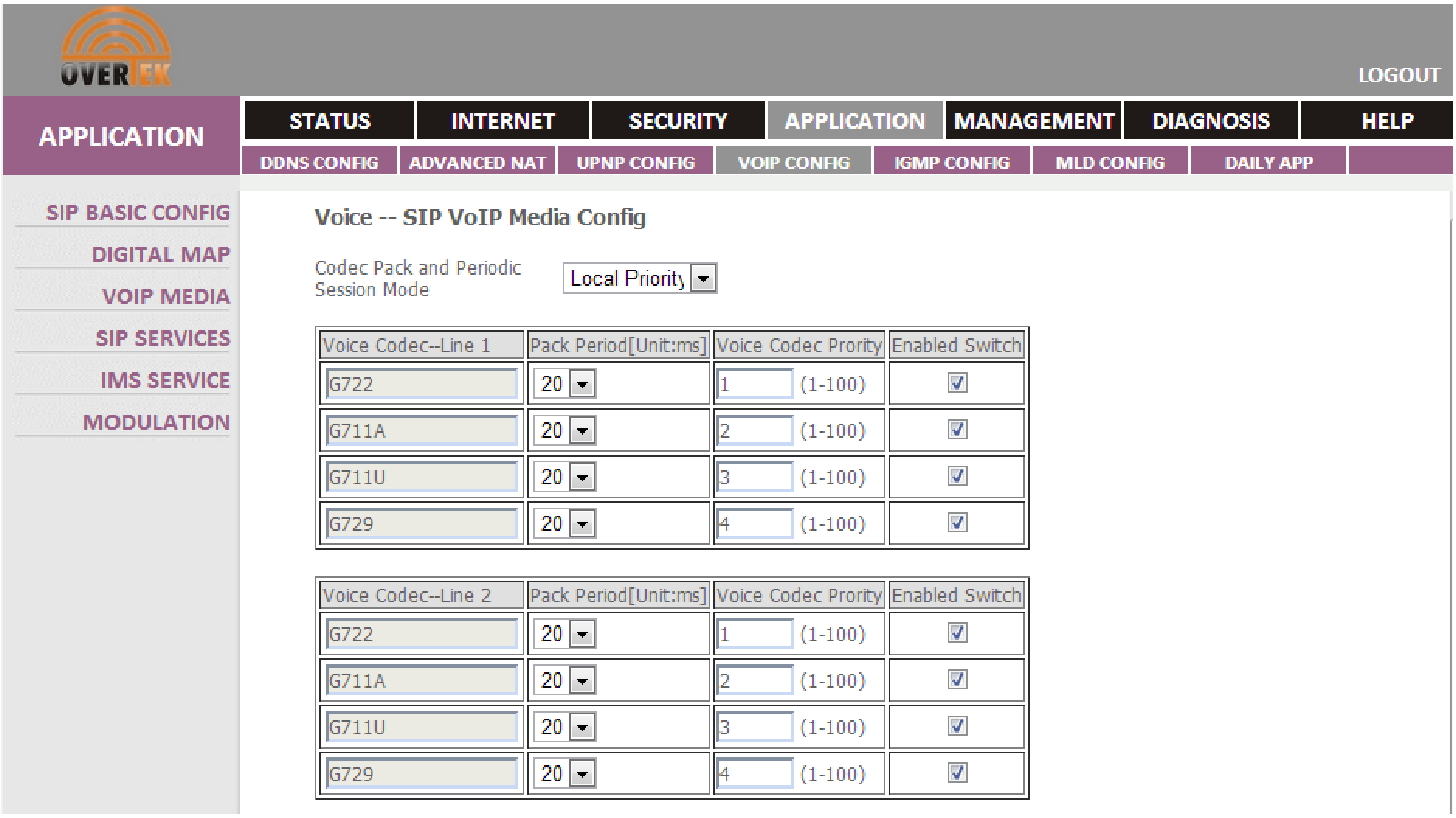
Specific num config

Enable Specific num: OFF
(length:150)

Enable Standard Digital Map: Enable Standard Digital Map/Dial plans for VoIP service
Digital Map Match Mode: The matching mode of the specified dialing plans.
Short-timer Time: Specify the short-timer time
Max Timer Time: Specify the max timer time
Non-Dialing Time after Pick Up: Specify the time of not dialing after you pick up the phone
T-timer Time: Specify the T-timer time
Stop Character Processing mode: To select the stop character processing mode
Number Match: Match with the specified number
Enable Specific Num: Enable hotline number

6.4.3. Voice Media

Click ‘ **Application** ‘ – ‘**VoIP Config** ‘– ‘**VoIP Media** ‘ to configure the Advanced Voice features.



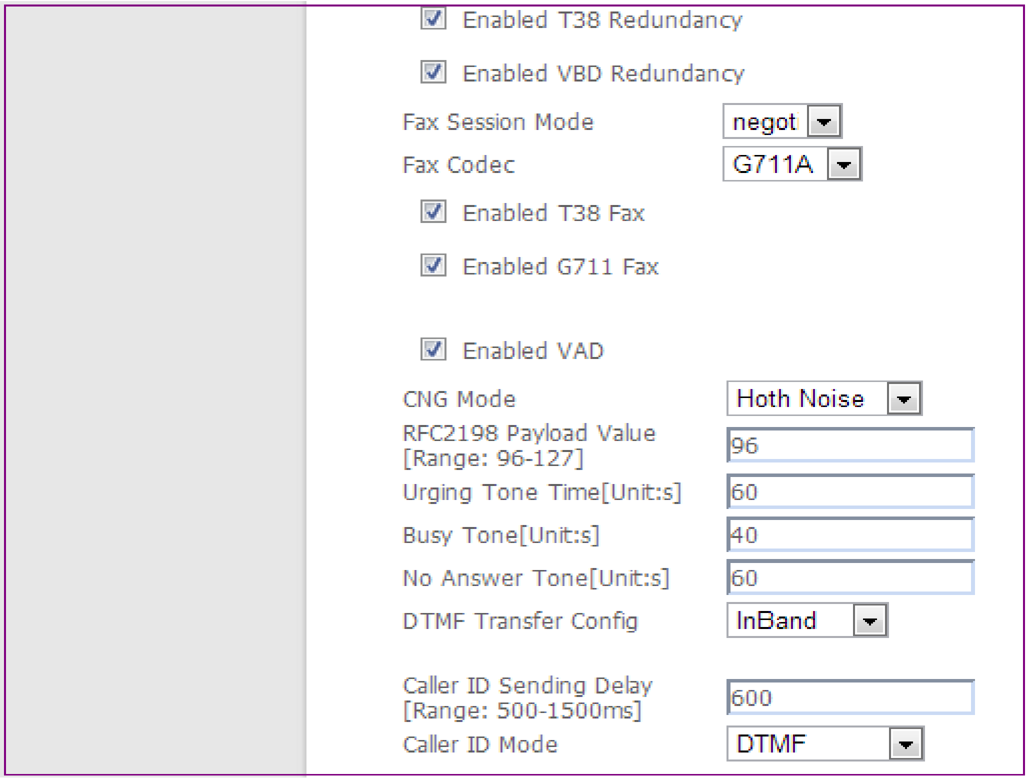
Voice -- SIP VoIP Media Config

Codec Pack and Periodic Session Mode: Local Priority

Voice Codec--Line 1	Pack Period[Unit:ms]	Voice Codec Prority	Enabled Switch
G722	20	1 (1-100)	☑
G711A	20	2 (1-100)	☑
G711U	20	3 (1-100)	☑
G729	20	4 (1-100)	☑

Voice Codec--Line 2	Pack Period[Unit:ms]	Voice Codec Prority	Enabled Switch
G722	20	1 (1-100)	☑
G711A	20	2 (1-100)	☑
G711U	20	3 (1-100)	☑
G729	20	4 (1-100)	☑

Set the Voice codecs for SIP account 1 and 2



☑ Enabled T38 Redundancy

☑ Enabled VBD Redundancy

Fax Session Mode: negot

Fax Codec: G711A

☑ Enabled T38 Fax

☑ Enabled G711 Fax

☑ Enabled VAD

CNG Mode: Hoth Noise

RFC2198 Payload Value [Range: 96-127]: 96

Urging Tone Time[Unit:s]: 60

Busy Tone[Unit:s]: 40

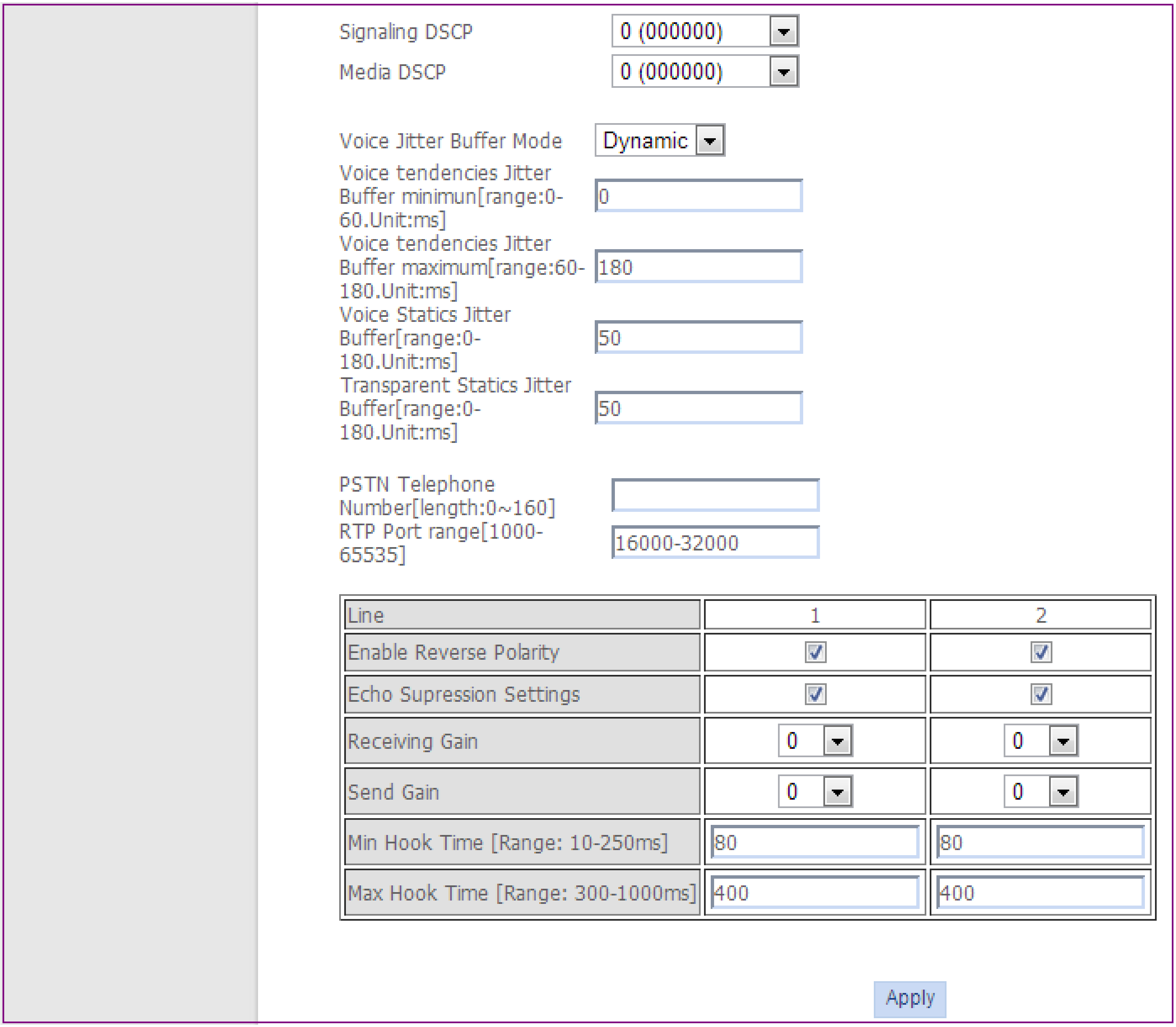
No Answer Tone[Unit:s]: 60

DTMF Transfer Config: InBand

Caller ID Sending Delay [Range: 500-1500ms]: 600

Caller ID Mode: DTMF

Enable T.38 Redundancy: Check the box to enable T.38 fax redundancy.
Enable VBD redundancy: Check the box to enable VBD (Voice Band Data) redundancy
Fax Session Mode: Set the fax session mode
Fax codec: Set the codec for Fax
Enable T38 Fax: Enable T.38 Fax
Enable G711 Fax: Enable Fax with G.711 codec
Enable VAD: Check the box to enable VAD (Voice Activation Detection)
CNG (Comfort Noise Generator) Mode: Select the CNG mode
RFC2198 Payload Value: Set the value of RFC2198 payload, ranges in between 96-127
Urging Tone Time: Set the urging tone time
Busy Tone: Set the busy tone time
No Answer Tone: Set the no answer tone time
DTMF Transfer Config: Set the DTMF mode of VoIP
Caller ID Sending Delay: Set the Caller ID sending delay time
Caller ID mode: Set the Caller ID mode



Signaling DSCP: 0 (000000)
Media DSCP: 0 (000000)

Voice Jitter Buffer Mode: Dynamic
Voice tendencies Jitter Buffer minimun[range:0-60.Unit:ms]: 0
Voice tendencies Jitter Buffer maximum[range:60-180.Unit:ms]: 180
Voice Statics Jitter Buffer[range:0-180.Unit:ms]: 50
Transparent Statics Jitter Buffer[range:0-180.Unit:ms]: 50

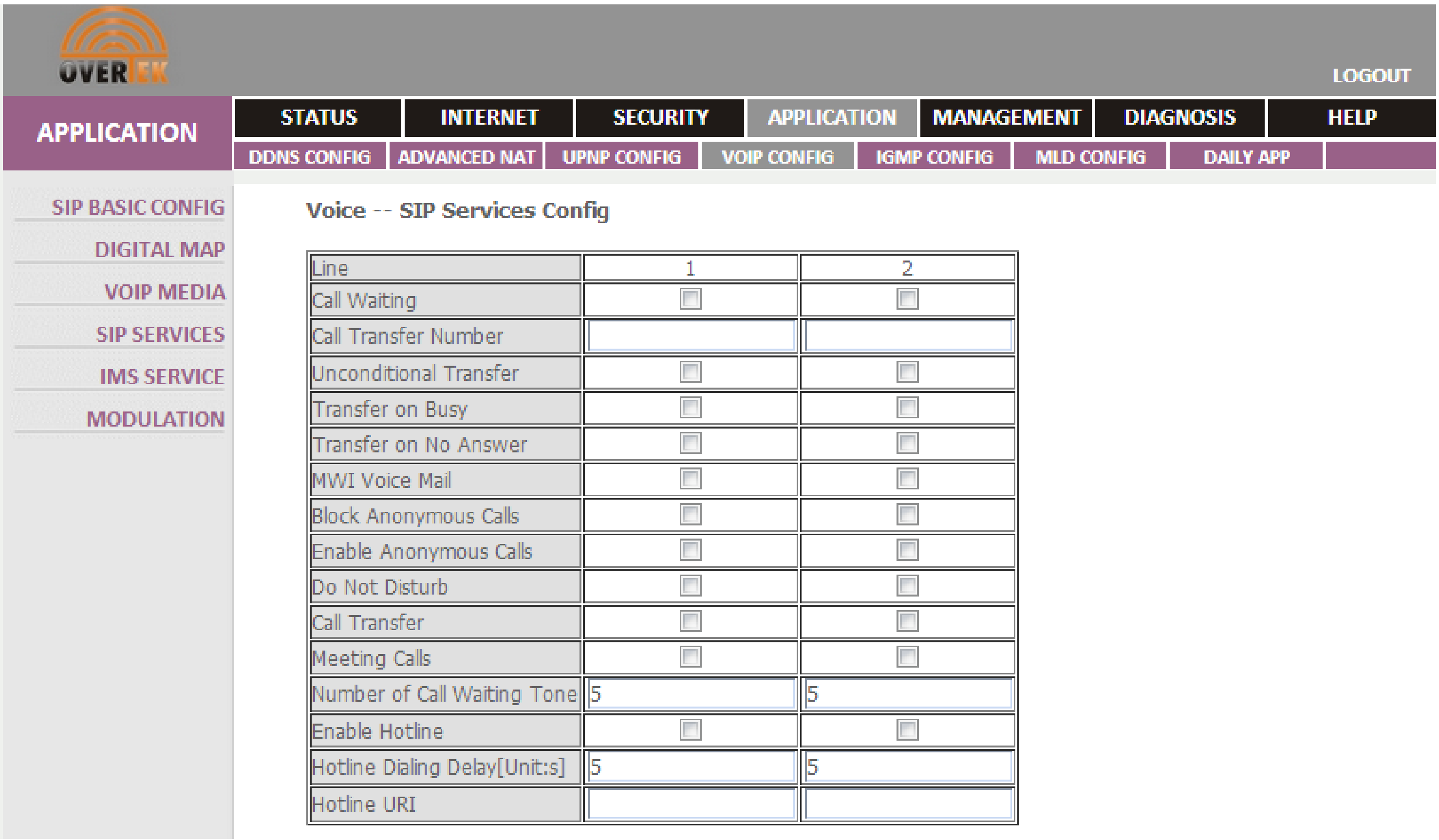
PSTN Telephone Number[length:0~160]:
RTP Port range[1000-65535]: 16000-32000

Line	1	2
Enable Reverse Polarity	☑	☑
Echo Supression Settings	☑	☑
Receiving Gain	0	0
Send Gain	0	0
Min Hook Time [Range: 10-250ms]	80	80
Max Hook Time [Range: 300-1000ms]	400	400

Signaling DSCP: The QOS value of SIP Signaling
Media DSCP: The QOS value for SIP media
Voice Jitter Buffer Mode: Set the Voice Jitter buffer mode
Voice tendencies Jitter Buffer minimum: Set the minimum value of Voice Tendencies Jitter buffer
Voice tendencies Jitter Buffer maximum: Set the maximum value of Voice Tendencies Jitter buffer
Voice Statics Jitter Buffer: Set the value of Voice Static Jitter buffer
Transparent Statics Jitter Buffer: Set the value of Transparent Voice Static Jitter buffer
PSTN Telephone Number: Set the PSTN telephone number
RTP Port range: Set the range of RTP port
Enable Reverse Polarity: Check the box to enable Reverse Polarity for SIP account 1 and 2
Echo Suppression Settings: Check the box to enable Echo Suppression settings for SIP account 1 and 2
Receiving Gain: Set the Receiving Gain value for Echo Suppression
Send Gain: Set the Sending Gain value for Echo Suppression
Min Hook Time [Range: 10-250ms]: Set the minimum Hook Time
Max Hook Time [Range: 10-250ms]: Set the maximum Hook Time
Apply: Click ' **Apply** ' button to save and apply new settings.

6.4.4. SIP Services

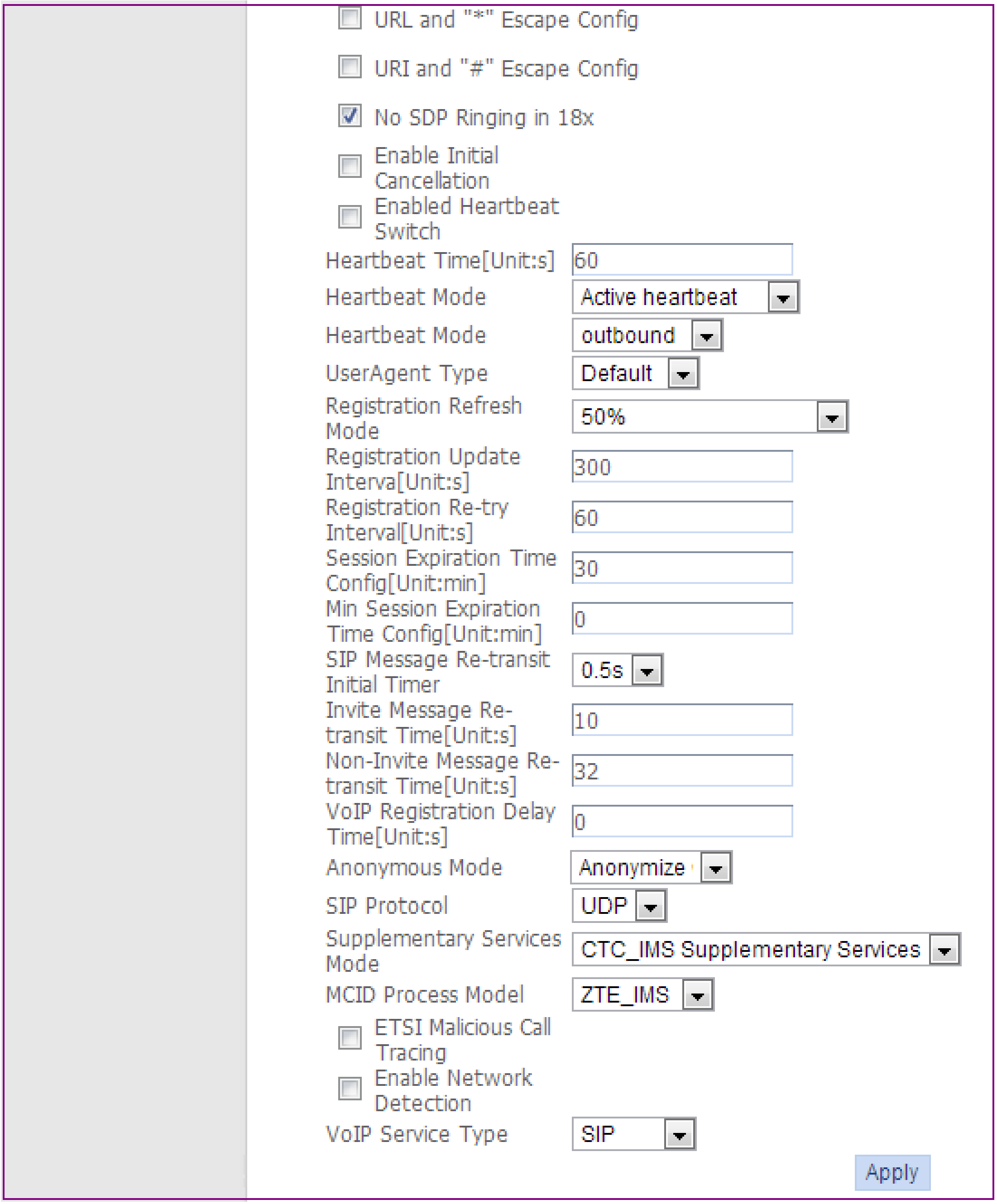
Click ' **Application** ' – '**VoIP Config** '– '**SIP Services** ' to configure the VoIP telephone features.



Voice -- SIP Services Config

Line	1	2
Call Waiting	□	□
Call Transfer Number		
Unconditional Transfer	□	□
Transfer on Busy	□	□
Transfer on No Answer	□	□
MWI Voice Mail	□	□
Block Anonymous Calls	□	□
Enable Anonymous Calls	□	□
Do Not Disturb	□	□
Call Transfer	□	□
Meeting Calls	□	□
Number of Call Waiting Tone	5	5
Enable Hotline	□	□
Hotline Dialing Delay[Unit:s]	5	5
Hotline URI		

Check the boxes available in the above template to enable different SIP telephone features.
After done, click 'Apply' button to save and apply new settings.



☐ URL and "*" Escape Config

☐ URI and "#" Escape Config

☑ No SDP Ringing in 18x

☐ Enable Initial Cancellation

☐ Enabled Heartbeat Switch

Heartbeat Time[Unit:s]	60
Heartbeat Mode	Active heartbeat
Heartbeat Mode	outbound
UserAgent Type	Default
Registration Refresh Mode	50%
Registration Update Interva[Unit:s]	300
Registration Re-try Interval[Unit:s]	60
Session Expiration Time Config[Unit:min]	30
Min Session Expiration Time Config[Unit:min]	0
SIP Message Re-transit Initial Timer	0.5s
Invite Message Re-transit Time[Unit:s]	10
Non-Invite Message Re-transit Time[Unit:s]	32
VoIP Registration Delay Time[Unit:s]	0
Anonymous Mode	Anonymize
SIP Protocol	UDP
Supplementary Services Mode	CTC_IMS Supplementary Services
MCID Process Model	ZTE_IMS

☐ ETSI Malicious Call Tracing

☐ Enable Network Detection

VoIP Service Type	SIP

URL and "*" Escape Config: Check the box to enable URL and '*' Escape config

URI and "#" Escape Config: Check the box to enable URL and '#' Escape config

No SDP Ringing in 18x: Check the box to disable SDP in 18x ring process

Enable Initial Cancellation: Check the box to enable SIP initial cancellation

Enabled Heartbeat Switch: Check the box to enable SIP Heartbeat Switch

Heartbeat Time: Set the SIP Heartbeat Switch time interval

Heartbeat Mode: Set the SIP heartbeat mode

Heartbeat Mode: Set SIP heartbeat switch in different authentication modes

UserAgent Type: Set the SIP agent type

Registration Refresh Mode: Set the SIP registration Refresh mode

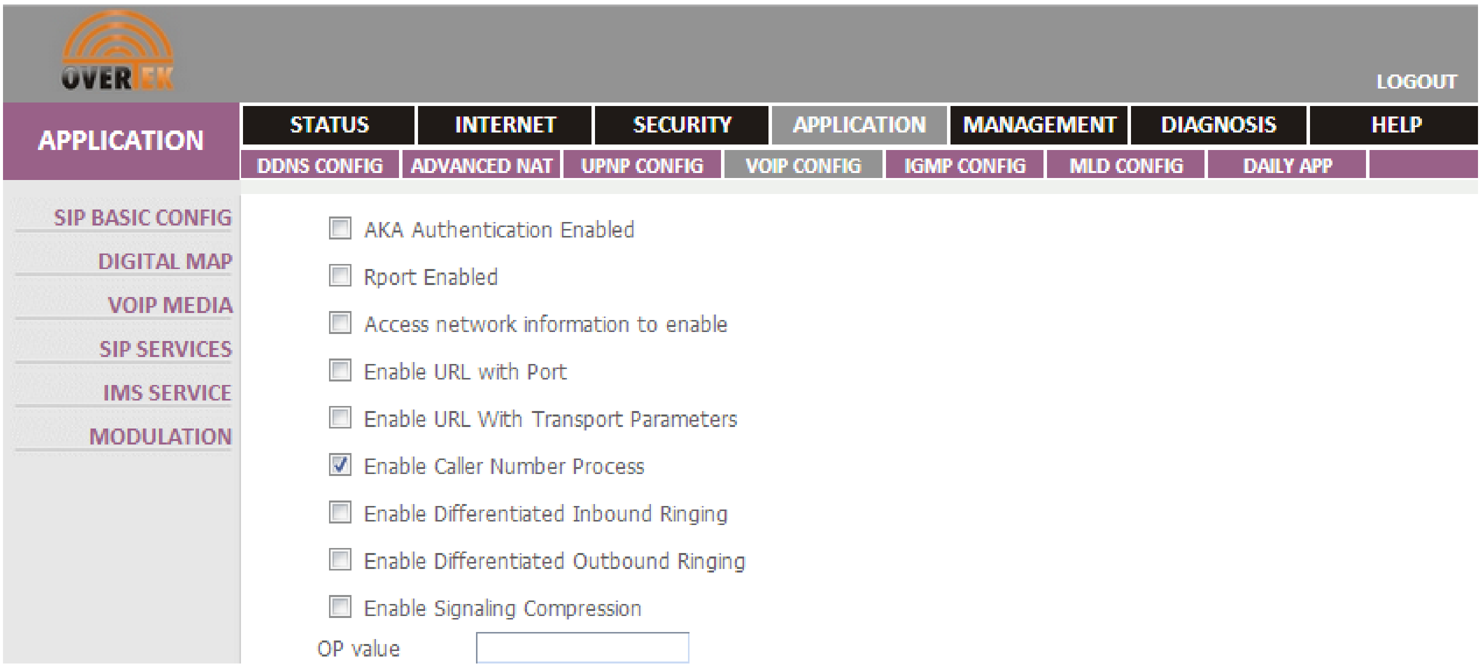
Registration Update Interval: Set the SIP registration Update time interval

Registration Re-try Interval: Set the SIP registration re-try time interval

Session Expiration Time Config: Set the SIP session expiration time
Min Session Expiration Time Config: Set the minimum SIP Session Expiration Time
SIP Message Re-transit Initial Timer: Set the SIP message re-transit initial time
Invite Message Re-transit Time: Set the SIP Invite Message re-transit time
Non-Invite Message Re-transit Time: Set the SIP non-invite message re-transit time
VoIP Registration Delay Time: Set the SIP registration delay time
Anonymous Mode: Set the SIP Anonymous mode
SIP Protocol: Set SIP protocol through UDP or TCP
Supplementary Services Mode: Set the Supplementary service mode.
MCID Process Mode: Set the Malicious Call Identification mode
Enable Network Detection: Check the box to enable Network detection
VoIP Service Type: Set VoIP protocol
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.4.5. IMS SERVICE

Click ‘ **Application** ‘ – ‘**VoIP Config** ‘– ‘**IMS Service** ‘ to configure the Voice IMS Parameters.

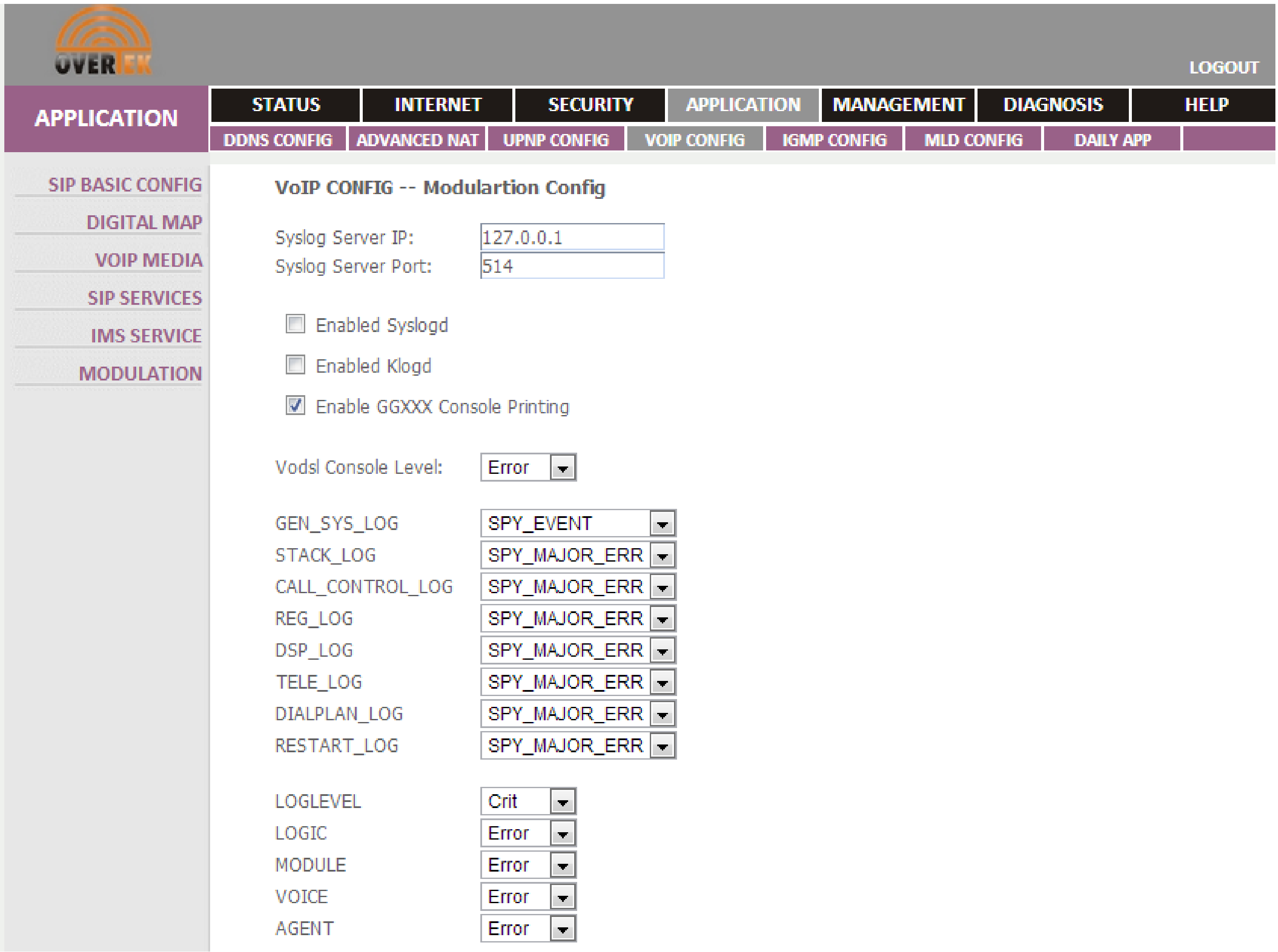


☐ AKA Authentication Enabled
☐ Rport Enabled
☐ Access network information to enable
☐ Enable URL with Port
☐ Enable URL With Transport Parameters
☑ Enable Caller Number Process
☐ Enable Differentiated Inbound Ringing
☐ Enable Differentiated Outbound Ringing
☐ Enable Signaling Compression
OP value

Notice: This is a feature available with IMS server configurations. (Not specified).

6.4.6. Modulation

Click ‘ **Application** ‘ – ‘**VoIP Config** ‘– ‘**Modulation** ‘ to debug the VoIP SIP configurations.



VoIP CONFIG -- Modulartion Config

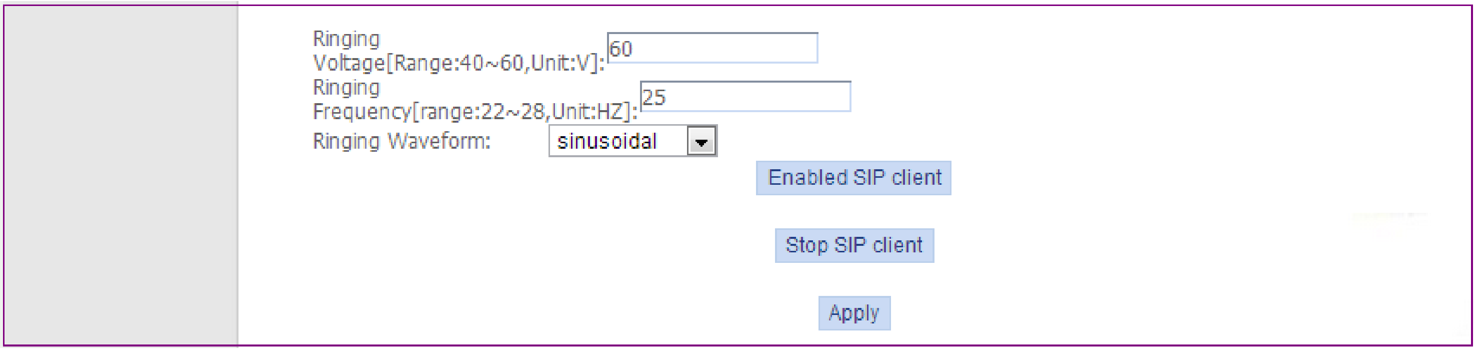
Syslog Server IP:	127.0.0.1
Syslog Server Port:	514

☐ Enabled Syslogd

☐ Enabled Klogd

☑ Enable GGXXX Console Printing

Vodsl Console Level:	Error
GEN_SYS_LOG	SPY_EVENT
STACK_LOG	SPY_MAJOR_ERR
CALL_CONTROL_LOG	SPY_MAJOR_ERR
REG_LOG	SPY_MAJOR_ERR
DSP_LOG	SPY_MAJOR_ERR
TELE_LOG	SPY_MAJOR_ERR
DIALPLAN_LOG	SPY_MAJOR_ERR
RESTART_LOG	SPY_MAJOR_ERR
LOGLEVEL	Crit
LOGIC	Error
MODULE	Error
VOICE	Error
AGENT	Error



Ringing Voltage[Range:40~60,Unit:V]:	60
Ringing Frequency[range:22~28,Unit:HZ]:	25
Ringing Waveform:	sinusoidal

Syslog Server IP: The Server Address that you want to store your SIP Syslog

Syslog Server Port: The port number of your SIP Syslog server

Enabled Syslog: Check the box to enable SIP Syslog

Enabled Klog: Check the box to enable SIP Klog

Vodsl Console Level: Set the Vodsl console level of your SIP Syslog

GEN_SYS_LOG: To determine the general system log level

STACK_LOG: To determine the STACK Log level

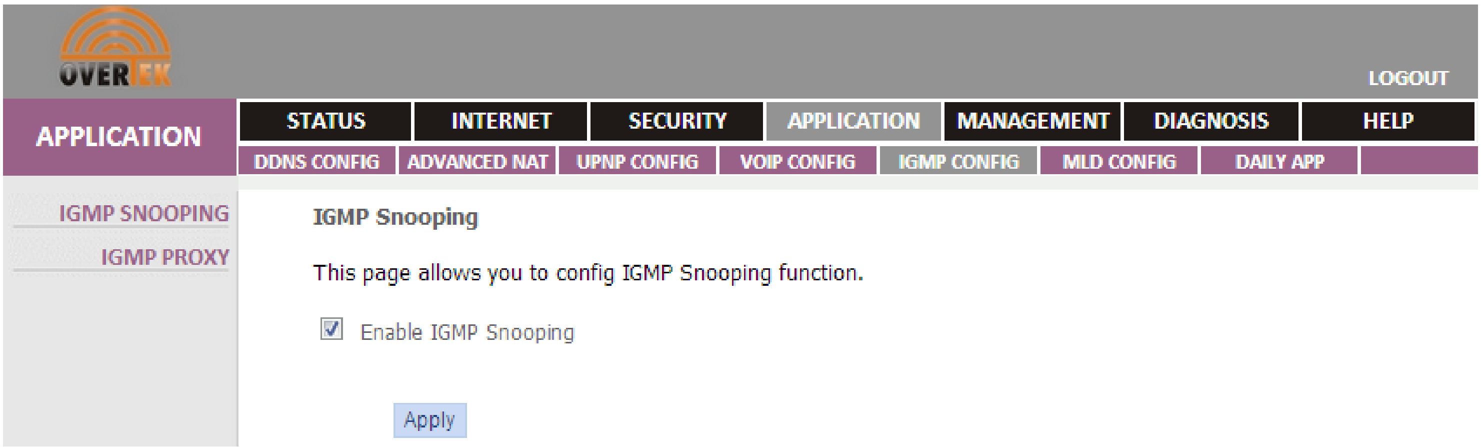
Call_Control_LOG: To determine the Call Control Log level

REG_LOG: To determine the Registration Log level
DSP_LOG: To determine the Voice DSP log level
TELE_LOG: To determine the telecommunication logo level
DIALPLAN_LOG: To determine the Dialplan_LOG level
RESTART_LOG: To determine the Rebooting Log level
Loglevel: To set the log level of your SIP Syslog
Logic: To set different SIP Syslog type of SIP logic
Module: To set different SIP Syslog type of SIP module
Voice: To set different SIP Syslog type of SIP Voice
Agent: To set different SIP Syslog type of SIP Agent
Ringing Voltage: To set the ringing voltage level of your SIP Syslog
Ringing Frequency: To set the ringing frequency of your SIP Syslog
Ringing Waveform: To set the ringing waveform of your SIP Syslog
Enabled SIP Client: Enable SIP client starting to report syslog
Stop SIP Client: Stop SIP client reporting SIP Syslog
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.5. IGMP Config

6.5.1. IGMP Snooping

Click ‘ **Application** ‘ – ‘**IGMP Config** ‘– ‘**IGMP Snooping** ‘ to set up IGMP Snooping for your OT-4020VW ONU.



IGMP Snooping

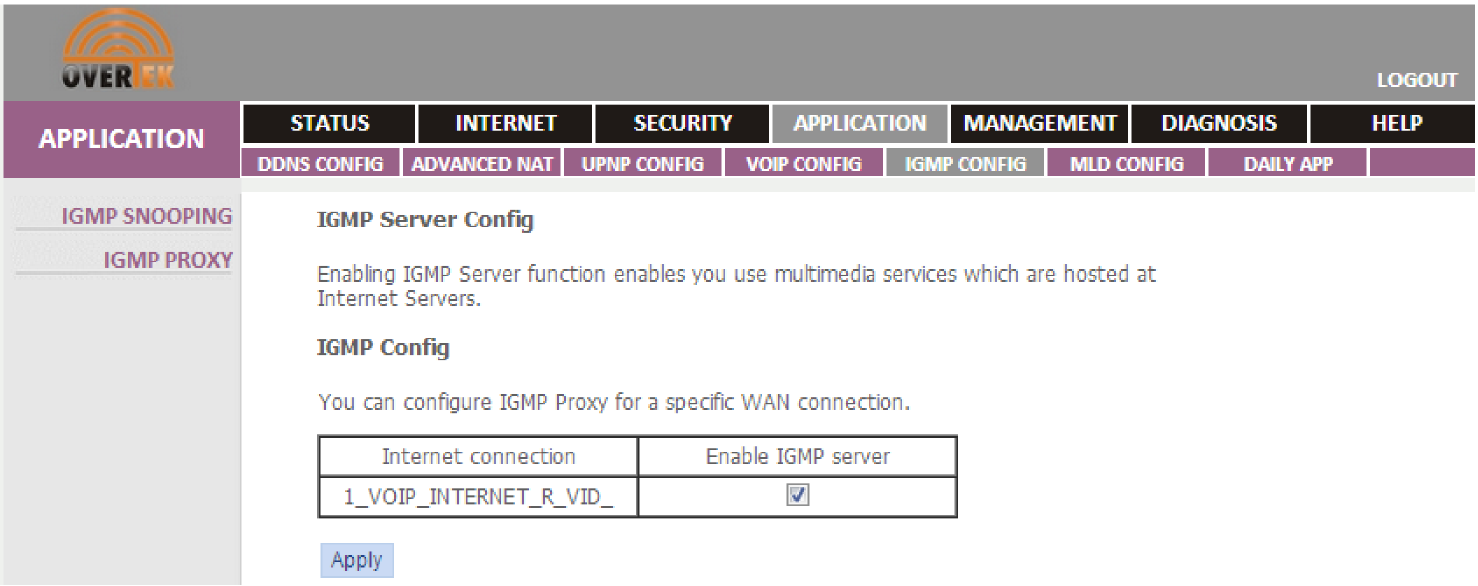
This page allows you to config IGMP Snooping function.

☑ Enable IGMP Snooping

Enable IGMP Snooping: Check the box to enable IGMP Snooping of your ONU.
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.5.2. IGMP Proxy

Click ‘ **Application** ‘ – ‘**IGMP Config** ‘– **‘IGMP Proxy** ‘ to enable IGMP pass-through a specific WAN interface.



IGMP Server Config

Enabling IGMP Server function enables you use multimedia services which are hosted at Internet Servers.

IGMP Config

You can configure IGMP Proxy for a specific WAN connection.

Internet connection	Enable IGMP server
1_VOIP_INTERNET_R_VID_	☑

Internet Connection: The WAN interface that you will enable for the IGMP Server

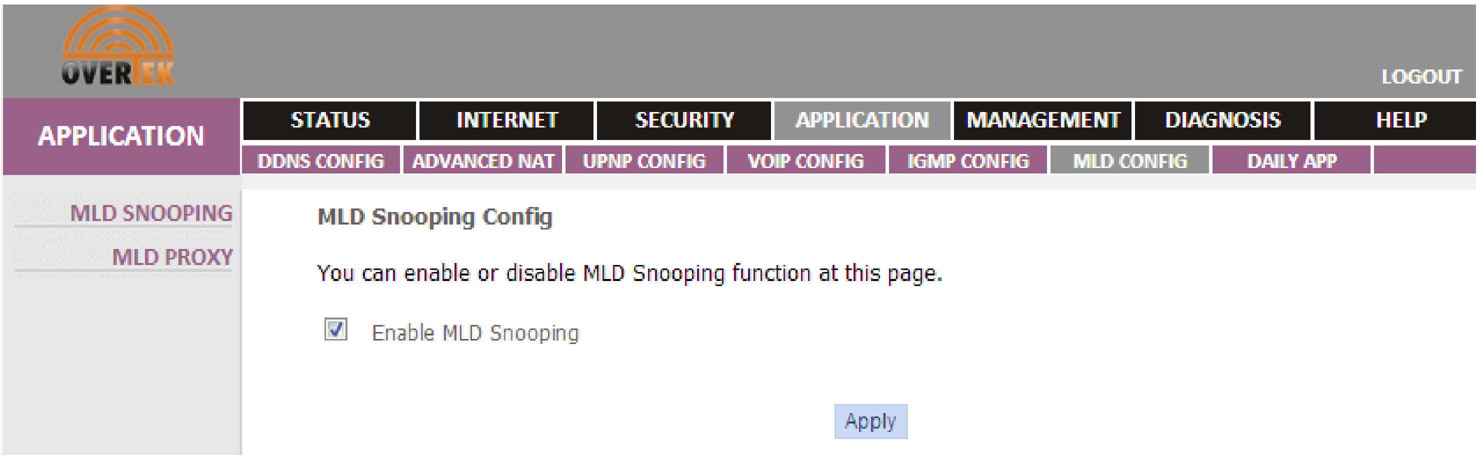
Enable IGMP Server: Check the box to enable IGMP Server

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.6. MLD Config

6.6.1. MLD Snooping

Click ‘ **Application** ‘ – ‘**MLD Config** ‘– ‘**MLD Snooping** ‘ to enable MLD Snooping for your OT-4020VW ONU.



MLD Snooping Config

You can enable or disable MLD Snooping function at this page.

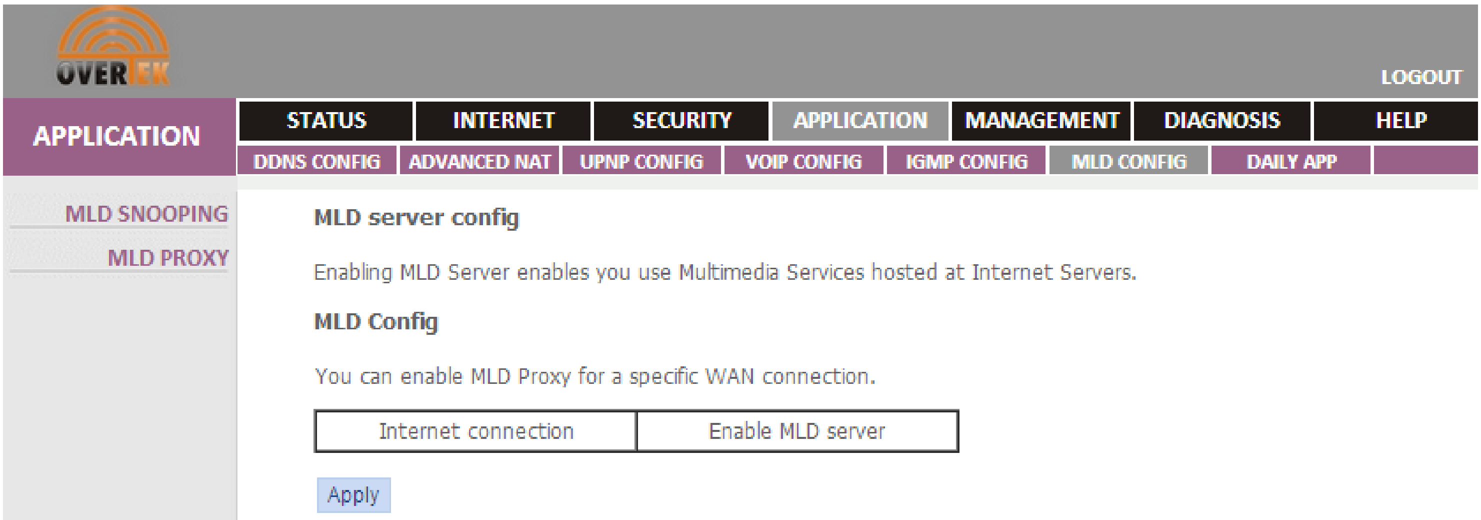
☑ Enable MLD Snooping

Enable MLD Snooping : Check the box to enable MLD (Multicast Listener Discover) Snooping

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.6.2. MLD Proxy

Click ‘ **Application** ‘ – ‘**MLD Config** ‘– ‘**MLD Proxy** ‘ to enable MLD Proxy for your OT-4020VW ONU.



MLD server config

Enabling MLD Server enables you use Multimedia Services hosted at Internet Servers.

MLD Config

You can enable MLD Proxy for a specific WAN connection.

Internet connection	Enable MLD server

Internet Connection: The IGMP WAN interface that you will enable for the MLD Server

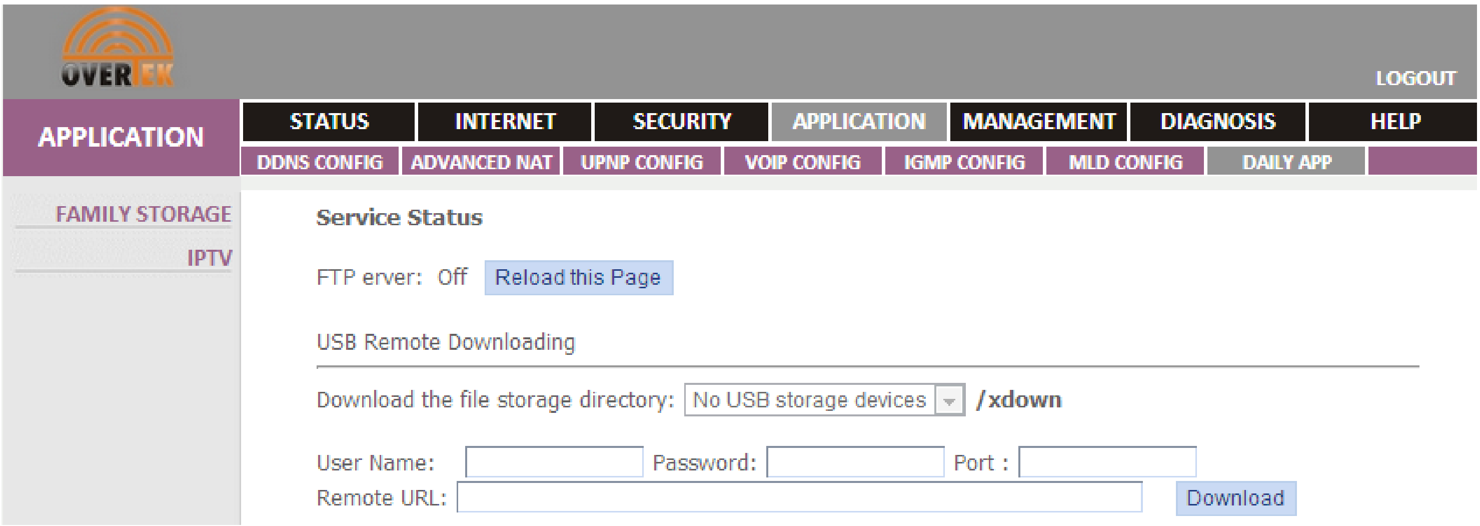
Enable IGMP Server: Check the box to enable MLD Server

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

6.7. Daily APP

6.7.1. Family Storage

Click ‘**Application**’ - ‘**Daily APP** ‘ – ‘**Family Storage**‘ to download files, music, video from internet to the family storage USB device even you are not at home.



Service Status

FTP erver: Off

USB Remote Downloading

Download the file storage directory: No USB storage devices /xdown

User Name: Password: Port :

Remote URL:

Download the file storage directory: Specify the downloading directory of your USB Storage device

User Name: Your remote FTP User name

Password: The password for your remote FTP server

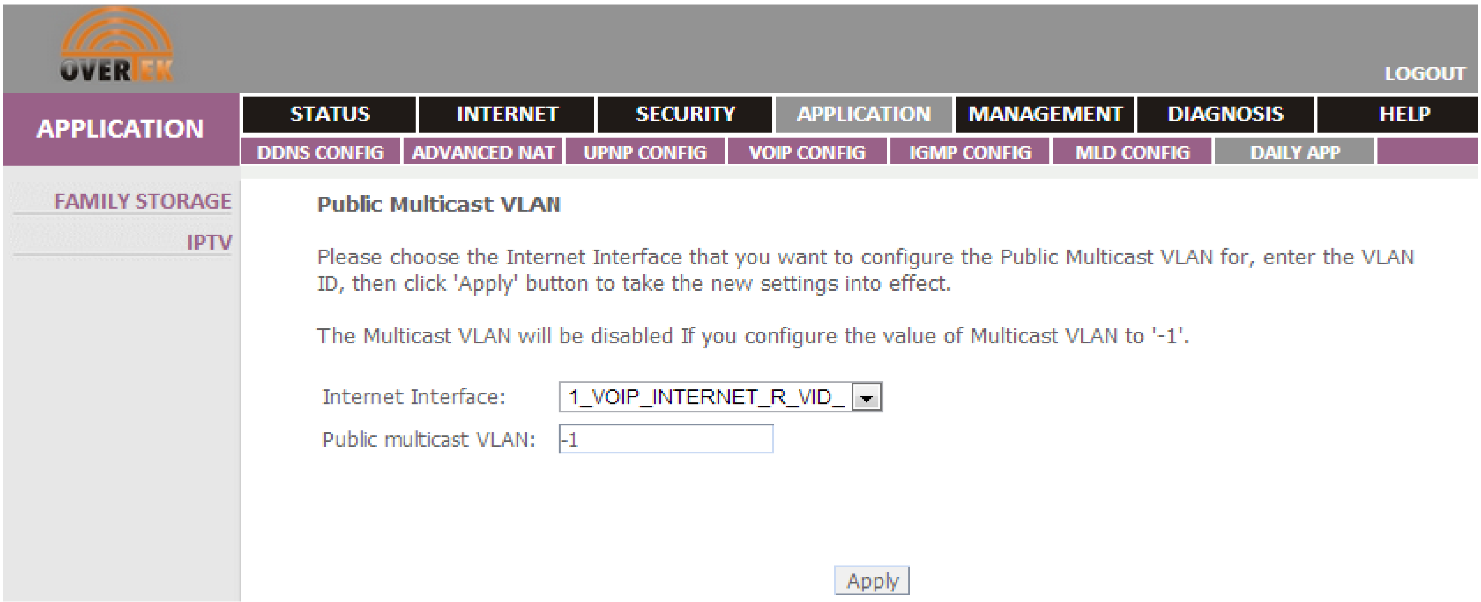
Port: The port number specified for your remote FTP Server

Remote URL: The URL that you download from

Download: Click ‘Download’ button to start downloading files to your USB storage device.

6.7.2. IPTV VLAN

Click ‘**Application**’ - ‘**Daily APP** ‘ – ‘**IPTV** ‘ to configure a specific Multicast VLAN for your IPTV application.



Public Multicast VLAN

Please choose the Internet Interface that you want to configure the Public Multicast VLAN for, enter the VLAN ID, then click 'Apply' button to take the new settings into effect.

The Multicast VLAN will be disabled If you configure the value of Multicast VLAN to '-1'.

Internet Interface: 1_VOIP_INTERNET_R_VID_

Public multicast VLAN: -1

Internet Interface: The WAN interface for your IPTV Application

Public Multicast VLAN: Specify the VLAN ID for your public Multicast streaming

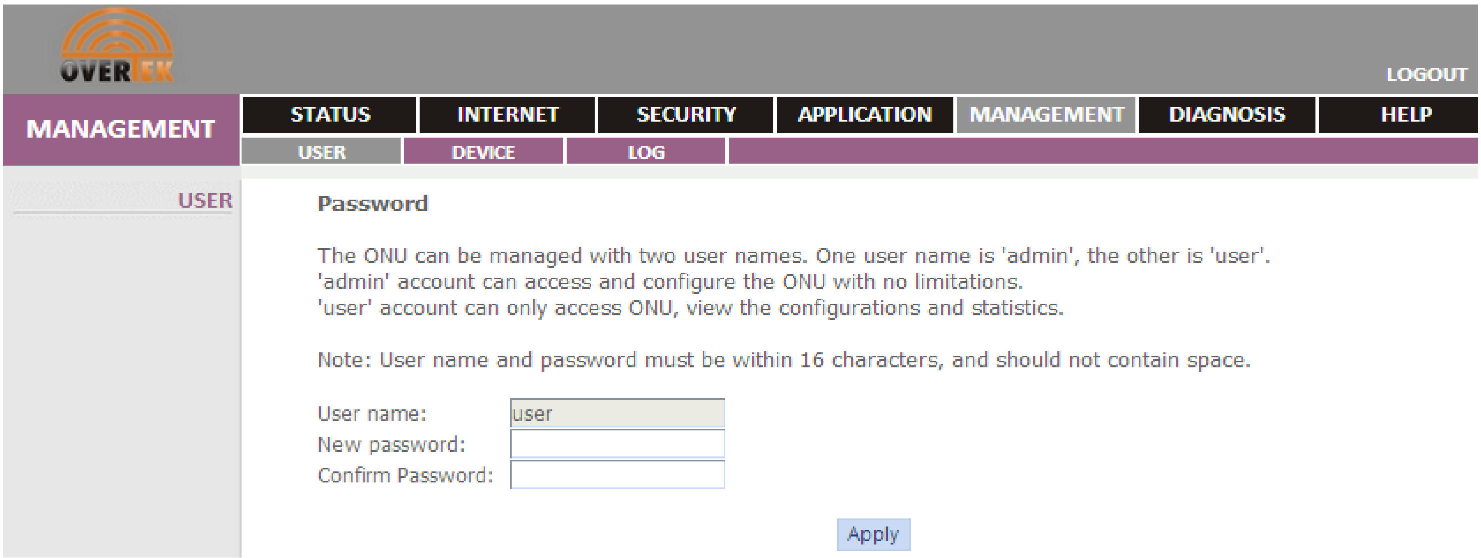
Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

7. Management

7.1. User

Click ‘**Management** ‘ – ‘**User** ‘ to set up the User Account password for your OT-4020VW GEPON ONU.

By default, the password for User account is ‘ user’. You can modify this password.



Password

The ONU can be managed with two user names. One user name is 'admin', the other is 'user'.
'admin' account can access and configure the ONU with no limitations.
'user' account can only access ONU, view the configurations and statistics.

Note: User name and password must be within 16 characters, and should not contain space.

User name: user

New password:

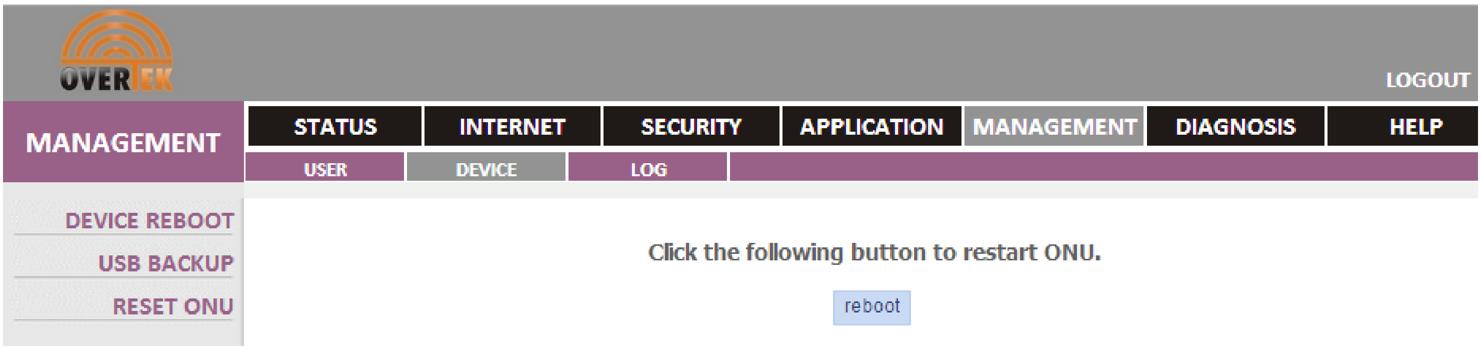
Confirm Password:

User Name: The original user name, by default, it's ' user'.
New Password: The new password that you want to apply to your ONU.
Confirm password: Re-enter the new password.
Apply: Click ' **Apply** ' button to save and apply new settings.

7.2. Device

7.2.1. Device Reboot

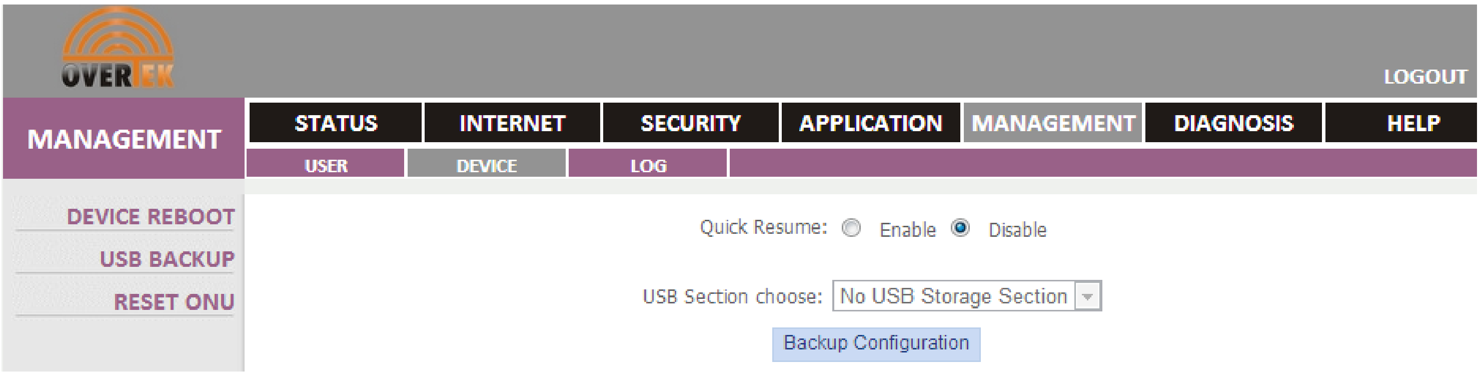
Click '**Management** ' – '**Device** '-'**Device Reboot'** to restart your OT-4020VW ONU.



Click the following button to restart ONU.

7.2.2. USB Backup

Click '**Management** ' – '**Device** ' – '**USB Backup'** to back the configuration file to your USB Storage device.



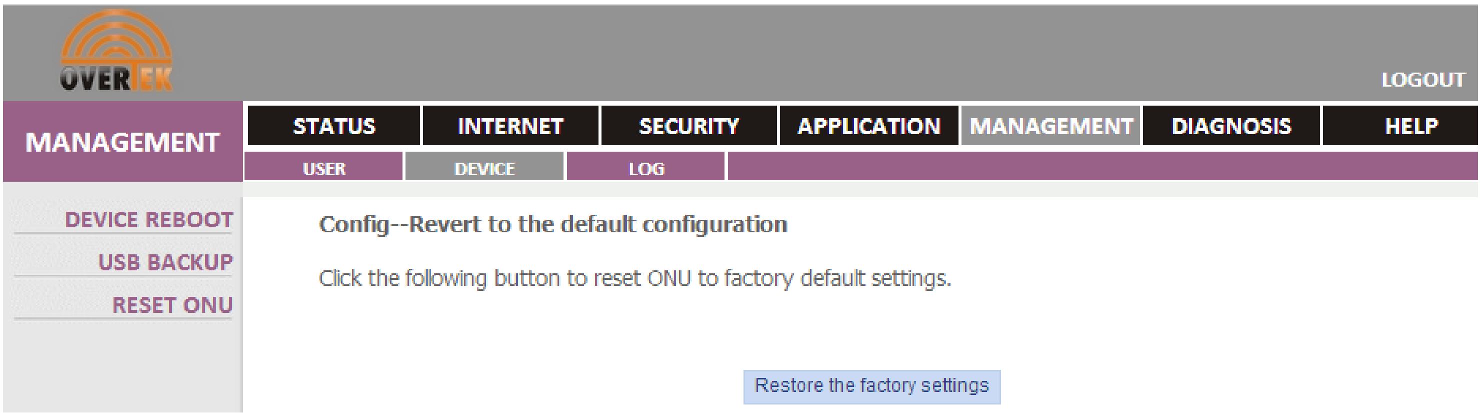
Quick Resume: ○ Enable ● Disable

USB Section choose: No USB Storage Section

7.2.3. Reset ONU

Click '**Management** ' – '**Device** ' – **'Reset ONU** ' to rest your OT-4020VW ONU to factory default settings.

Note: Reset ONU to factory default settings will not flush your Internet and VoIP configurations.



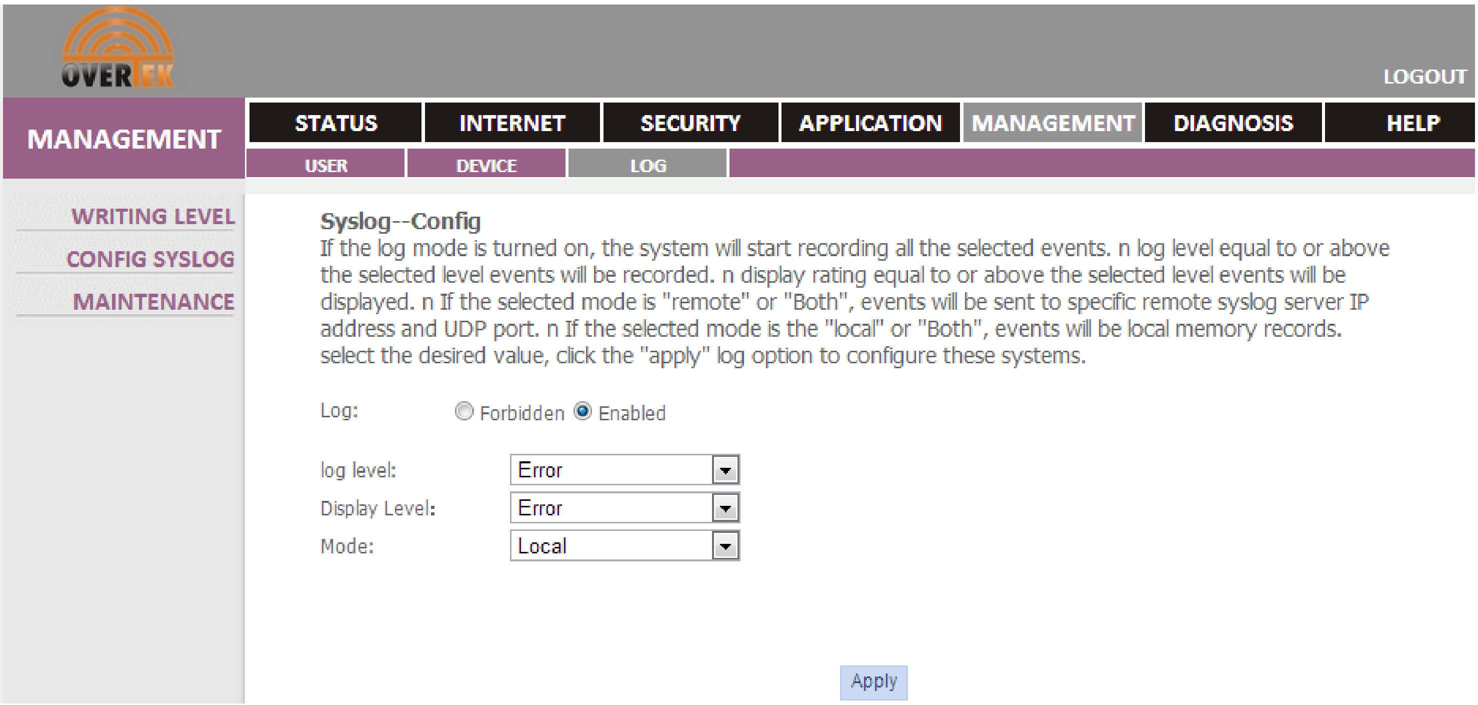
Config--Revert to the default configuration

Click the following button to reset ONU to factory default settings.

7.3. LOG

7.3.1. Writing Level

Click ‘**Management** ’ – ‘**Writing Level**‘ –‘ to manage syslog of your OT-4020VW GEPON ONU.



Syslog--Config

If the log mode is turned on, the system will start recording all the selected events. n log level equal to or above the selected level events will be recorded. n display rating equal to or above the selected level events will be displayed. n If the selected mode is "remote" or "Both", events will be sent to specific remote syslog server IP address and UDP port. n If the selected mode is the "local" or "Both", events will be local memory records. select the desired value, click the "apply" log option to configure these systems.

Log: ○ Forbidden ● Enabled

log level: Error

Display Level: Error

Mode: Local

Log: Check the box to enable or disable Log for your OT-4020VW ONU

Log Level: To determine which type of log to be recorded in the log file

Display Level: To determine which type of log to be displayed in the log file

Mode: To determine either to enable local or remote syslog.

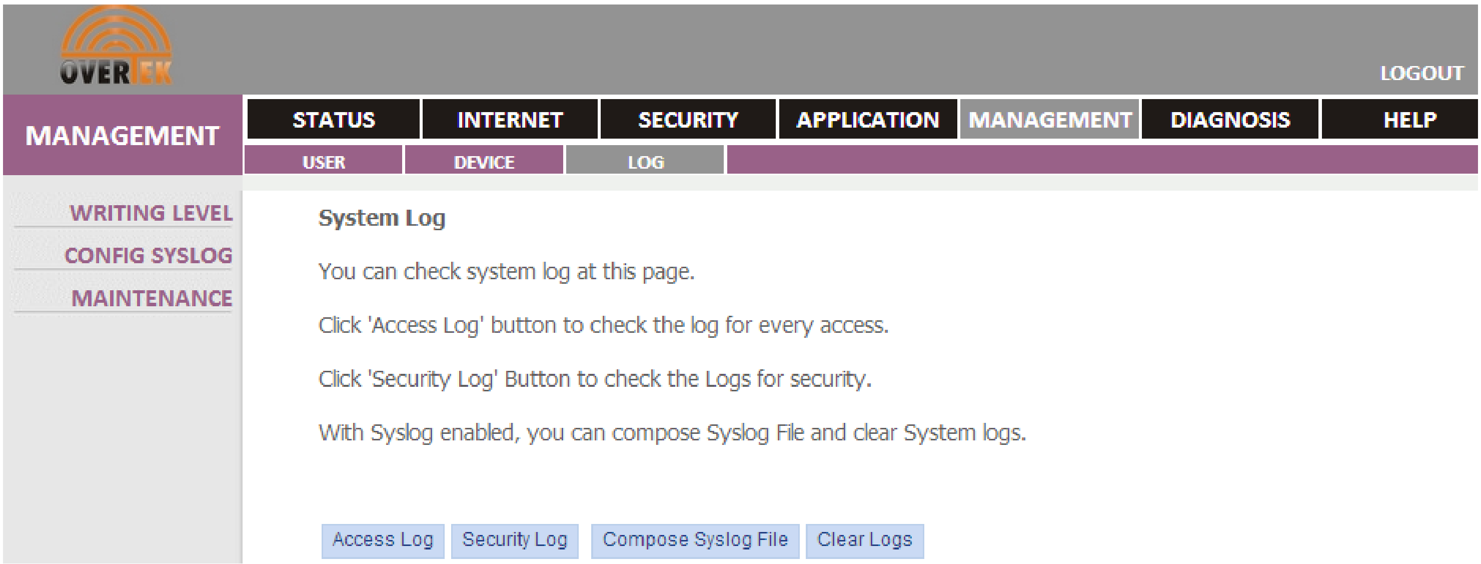
Server IP address: The Server that you will store the Logs

Server UDP Port: The port number for the Server which you will store up the logs.

Apply: Click ‘ **Apply** ‘ button to save and apply new settings.

7.3.2. Config Syslog

Click ‘**Management** ‘ – ‘**LOG**‘ – ‘**Config Syslog** ‘ to check or manage logs of your OT-4020VW GEPON ONU.



System Log

You can check system log at this page.

Click 'Access Log' button to check the log for every access.

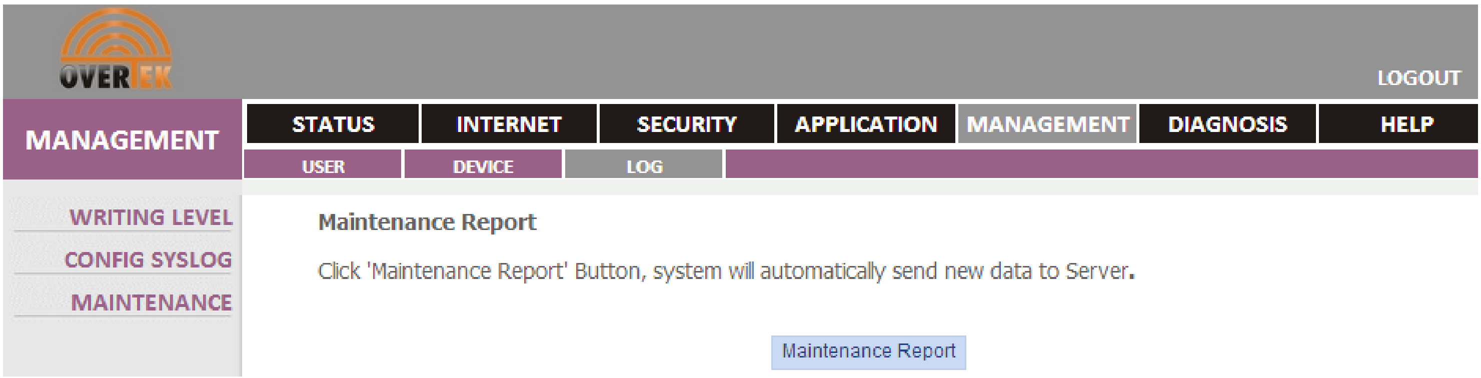
Click 'Security Log' Button to check the Logs for security.

With Syslog enabled, you can compose Syslog File and clear System logs.

Access Log: Click the ‘ Access Log’ button to view the access logs of your ONU.
Security Log: Click the ‘ Security Log’ button to view the Security logs of your ONU.
Compose Syslog File: Click the ‘Compose Syslog File’ button to compose a new syslog file.
Clear Logs: Click the ‘Clear Logs’ button to clear all access logs and security logs of your ONU.

7.3.3. Maintenance

Click ‘**Management** ‘ – ‘**Maintenance** ‘ to send new data to ACS server.
This function is for TR-069 management, it’s for manually provisioning new configurations/data to the remote ACS server.



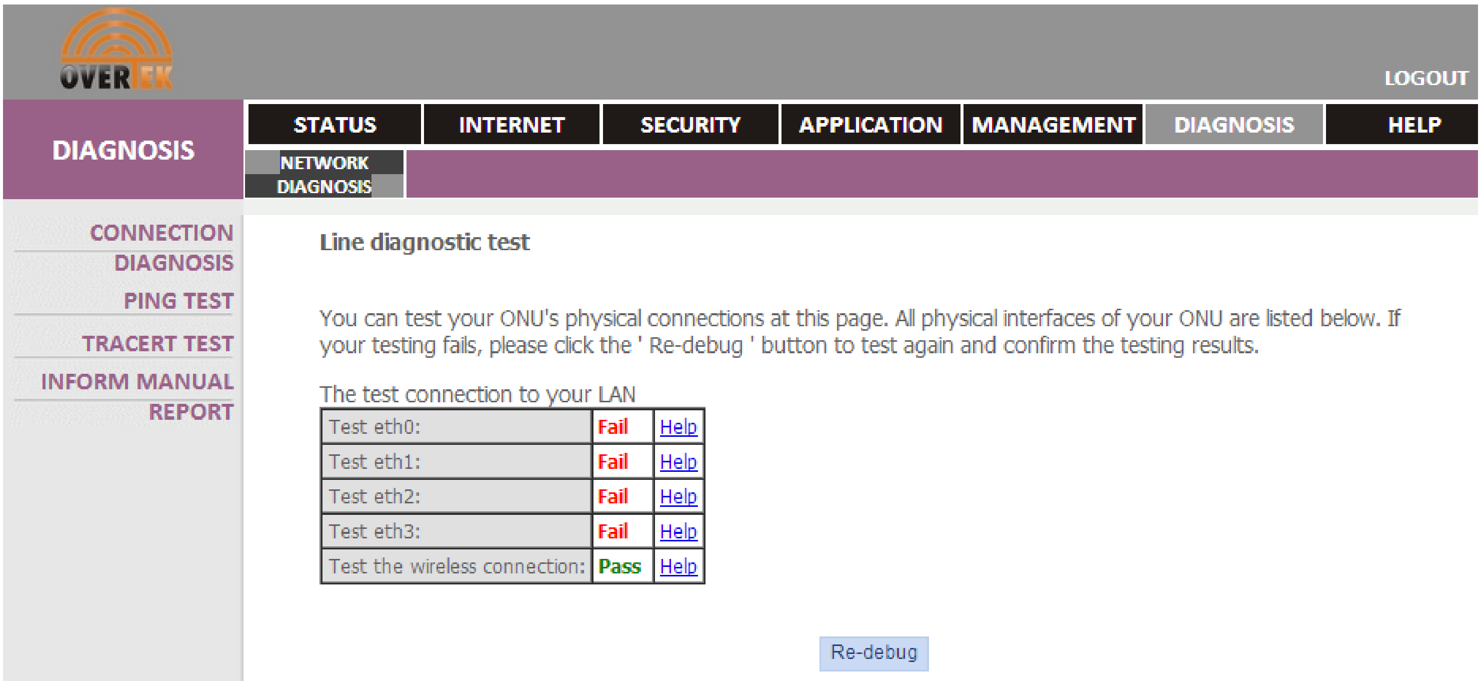
Maintenance Report

Click 'Maintenance Report' Button, system will automatically send new data to Server.

8. Diagnosis – Network Diagnosis

8.1. Connection Diagnosis

Click ‘**Diagnosis** ‘ – ‘**Network Diagnosis** ‘ –‘ **Connection Diagnosis** ‘ to view the connection status of your LAN and WLAN interfaces. Click ‘**Re-debug’** button to refresh the page



Line diagnostic test

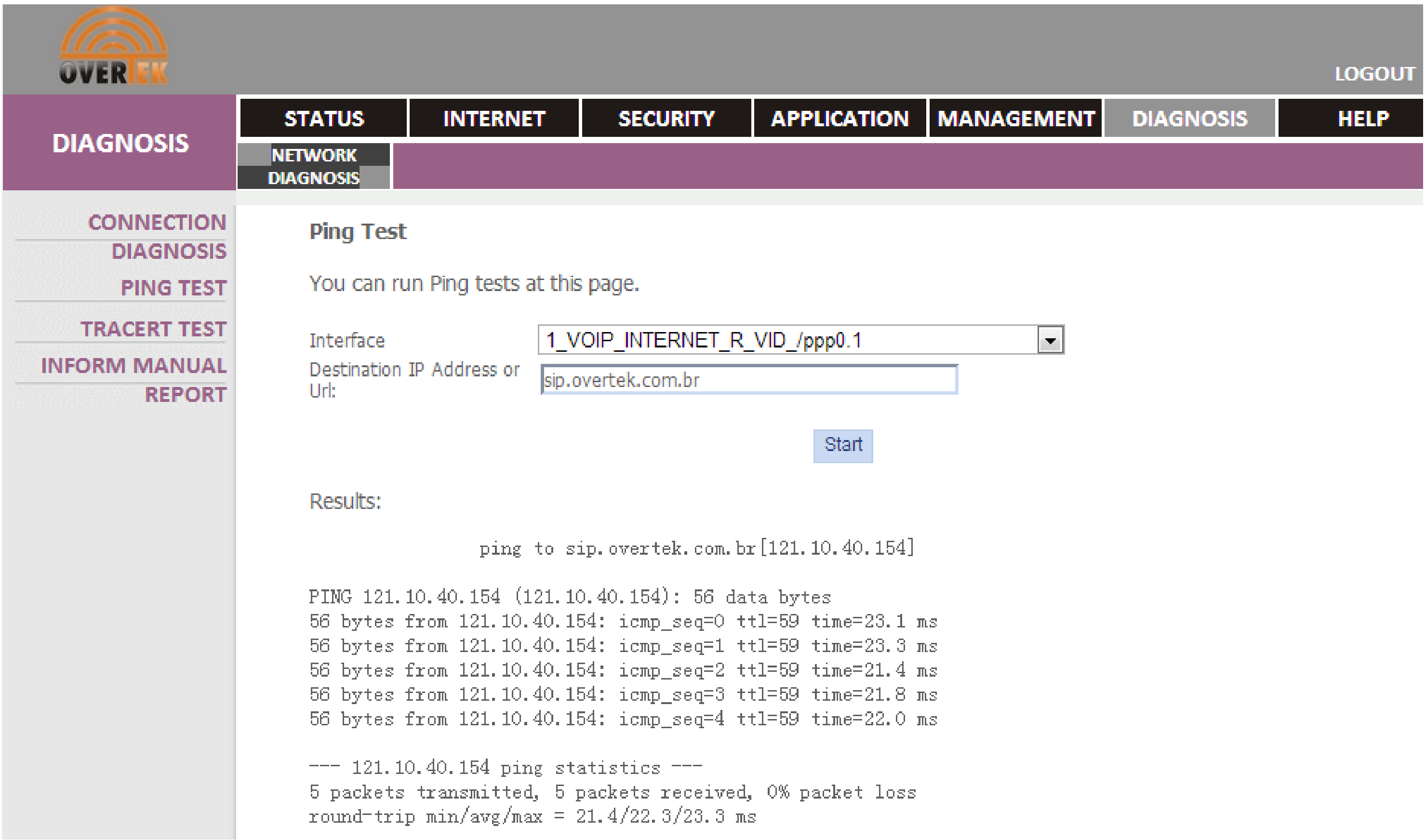
You can test your ONU's physical connections at this page. All physical interfaces of your ONU are listed below. If your testing fails, please click the ' Re-debug ' button to test again and confirm the testing results.

The test connection to your LAN

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

8.2. Ping Test

Click '**Diagnosis** ' – '**Network Diagnosis** ' –' **Ping Test** ' to diagnose the Internet connections.



Ping Test

You can run Ping tests at this page.

Interface: 1_VOIP_INTERNET_R_VID_/ppp0.1

Destination IP Address or Url: sip.overtek.com.br

Results:

```
                ping to sip.overtek.com.br[121.10.40.154]

PING 121.10.40.154 (121.10.40.154): 56 data bytes
56 bytes from 121.10.40.154: icmp_seq=0 ttl=59 time=23.1 ms
56 bytes from 121.10.40.154: icmp_seq=1 ttl=59 time=23.3 ms
56 bytes from 121.10.40.154: icmp_seq=2 ttl=59 time=21.4 ms
56 bytes from 121.10.40.154: icmp_seq=3 ttl=59 time=21.8 ms
56 bytes from 121.10.40.154: icmp_seq=4 ttl=59 time=22.0 ms

--- 121.10.40.154 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 21.4/22.3/23.3 ms
```

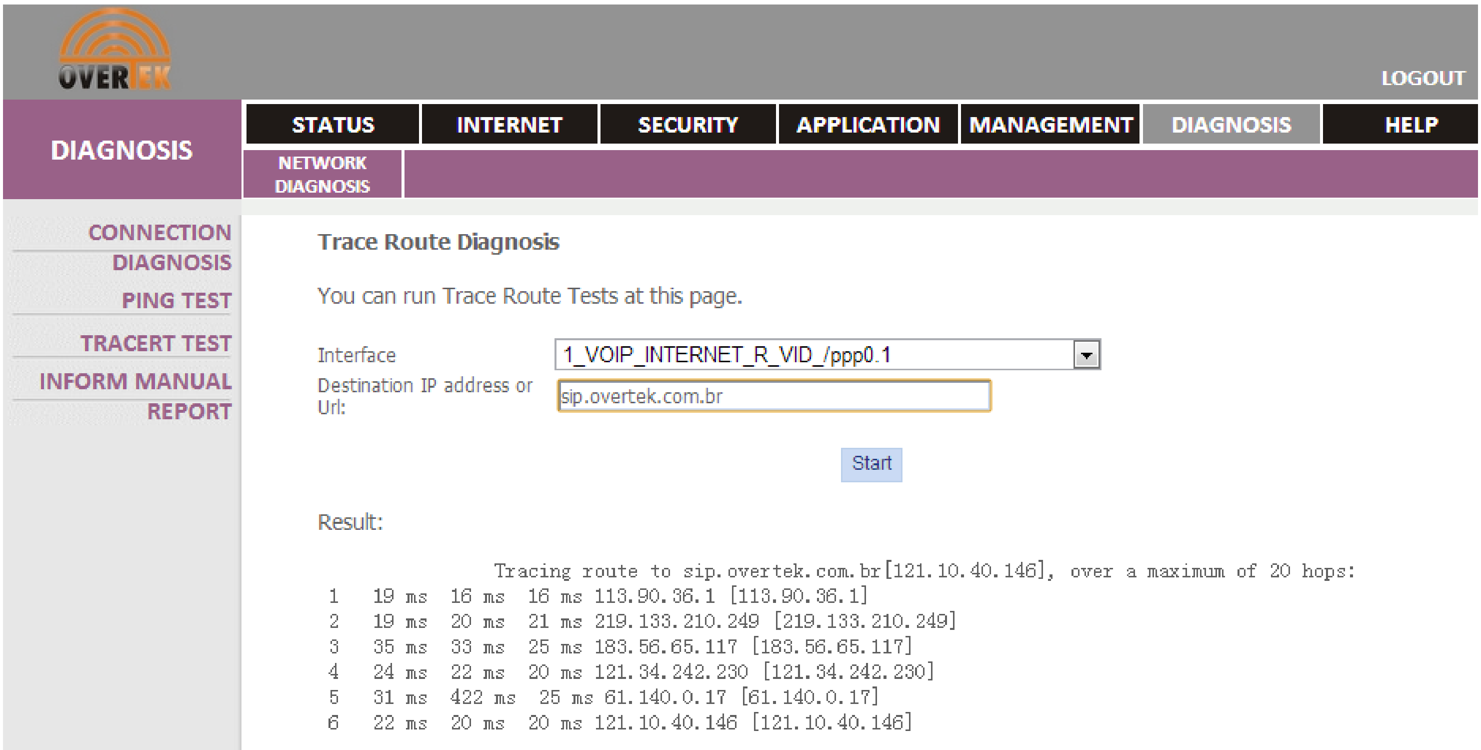
Interface: Choose one of the internet connection to run Ping Tests.

Destination IP address or URL: Enter the IP address or the Host Name that you want to Ping

Start: Click the ‘Start’ button to start ping the destination IP or URL.

8.3. Tracert Test

Click ‘**Diagnosis** ‘ – ‘**Network Diag** ‘ – ‘ **Tracert Test** ‘ to trace the route table for the destination IP address or Host.



Trace Route Diagnosis

You can run Trace Route Tests at this page.

Interface: 1_VOIP_INTERNET_R_VID_/ppp0.1

Destination IP address or Url: sip.overtek.com.br

Result:

```
                  Tracing route to sip.overtek.com.br[121.10.40.146], over a maximum of 20 hops:
 1   19 ms  16 ms  16 ms 113.90.36.1 [113.90.36.1]
 2   19 ms  20 ms  21 ms 219.133.210.249 [219.133.210.249]
 3   35 ms  33 ms  25 ms 183.56.65.117 [183.56.65.117]
 4   24 ms  22 ms  20 ms 121.34.242.230 [121.34.242.230]
 5   31 ms  422 ms  25 ms 61.140.0.17 [61.140.0.17]
 6   22 ms  20 ms  20 ms 121.10.40.146 [121.10.40.146]
```

Interface: Choose one of the internet connection to run Trace Route.

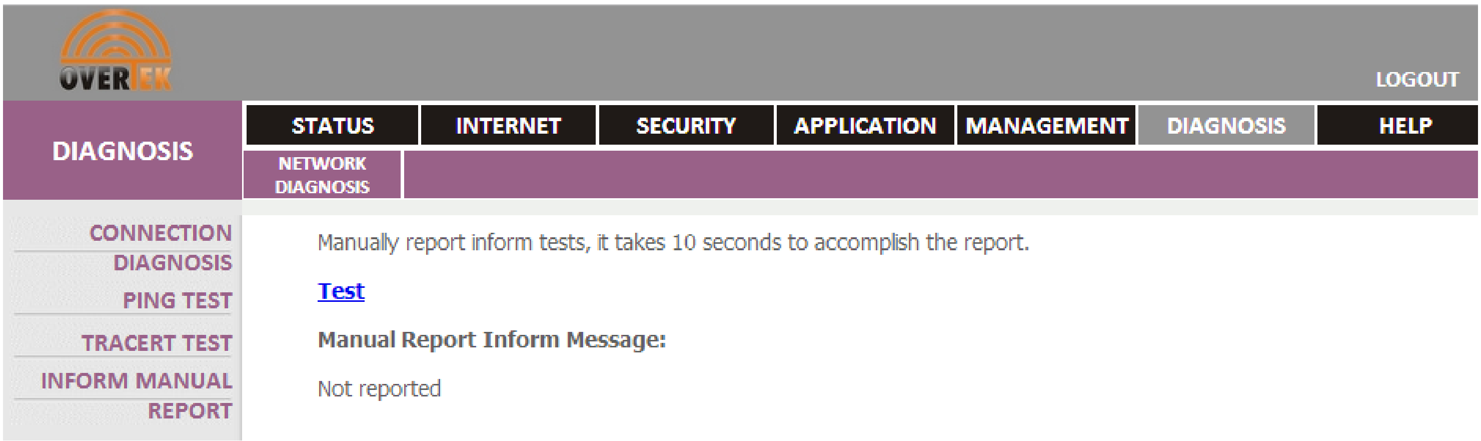
Destination IP address or URL: Enter the IP address or the Host Name that you want to trace route with.

Start: Click the ‘Start’ button to start ping the destination IP or URL.

8.4. Inform Report

Inform Report is a function for reporting failures or logs to the ACS server.

Click ‘**Diagnosis** ‘ – ‘**Network Diag** ‘ – ‘**Inform Report** ‘ to diagnose the Inform Report function of OT-4020VW ONU.



Manually report inform tests, it takes 10 seconds to accomplish the report.

Manual Report Inform Message:

Not reported

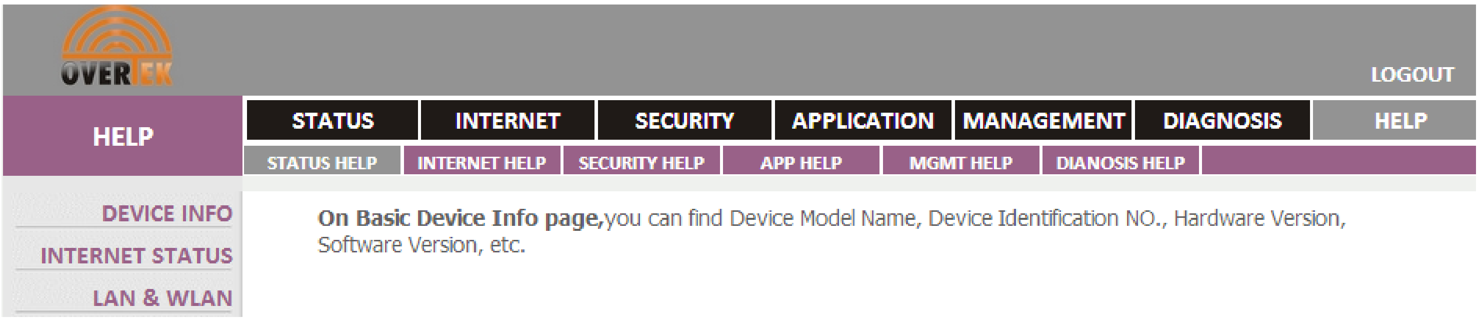
Test: Click the ‘ Test ‘ button to manually send message to a remote TR069 ACS Server.

9. Help

9.1. Status Help

9.1.1. Device Info

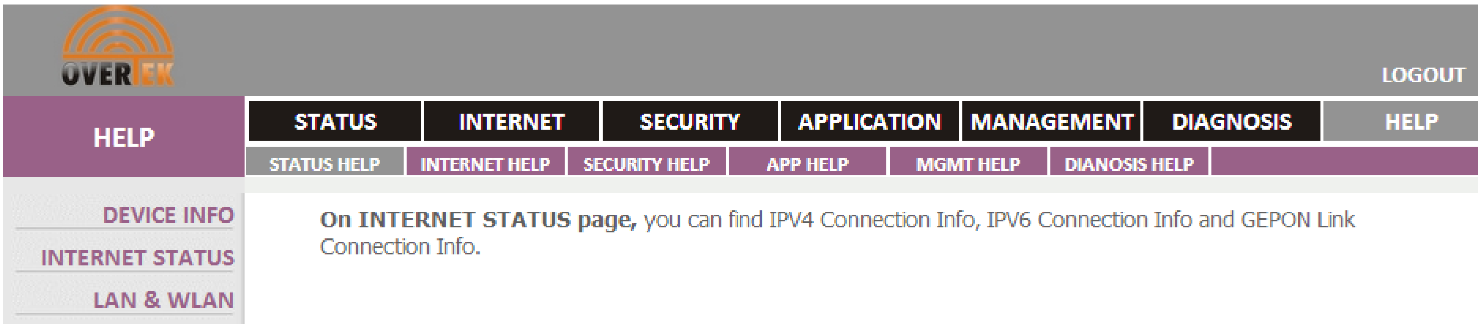
Click ‘ **Help** ‘ – ‘ **Status Help** ‘ – ‘**Device Info**’ to view the help information of device status.



On Basic Device Info page,you can find Device Model Name, Device Identification NO., Hardware Version, Software Version, etc.

9.1.2. Internet Status

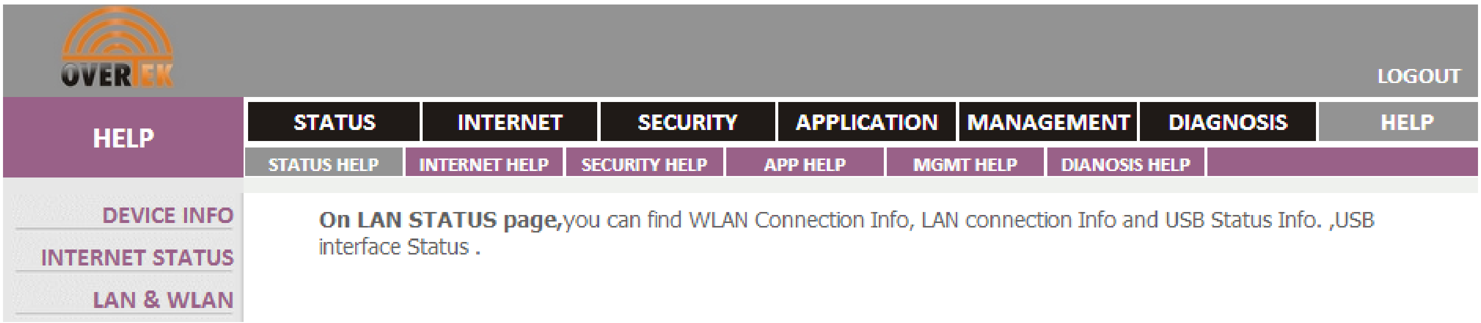
Click ‘ **Help** ‘ – ‘ **Status Help** ‘ – ‘**Internet Status**’ to view the help information of Internet connection status.



On INTERNET STATUS page, you can find IPV4 Connection Info, IPV6 Connection Info and GEPON Link Connection Info.

9.1.3. LAN & WLAN

Click ‘ **Help** ‘ – ‘ **Status Help** ‘ – ‘**LAN & WLAN**’ to view the help information of LAN and WLAN status.

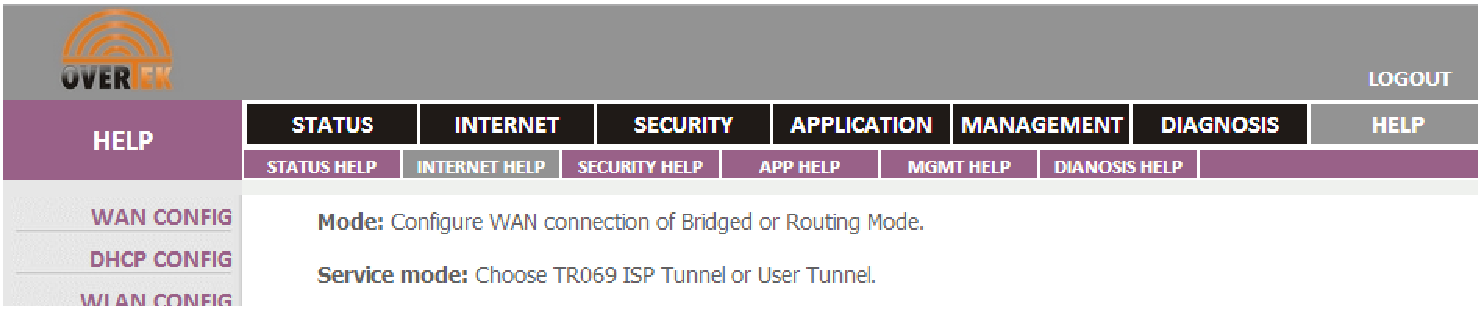


On LAN STATUS page,you can find WLAN Connection Info, LAN connection Info and USB Status Info. ,USB interface Status .

9.2. Internet Help

9.2.1. WAN Config

Click ‘ **Help** ‘ – ‘**Internet Help** ‘ – ‘**WAN Config**’ to view the help information of WAN Configuration/Internet Configuration.

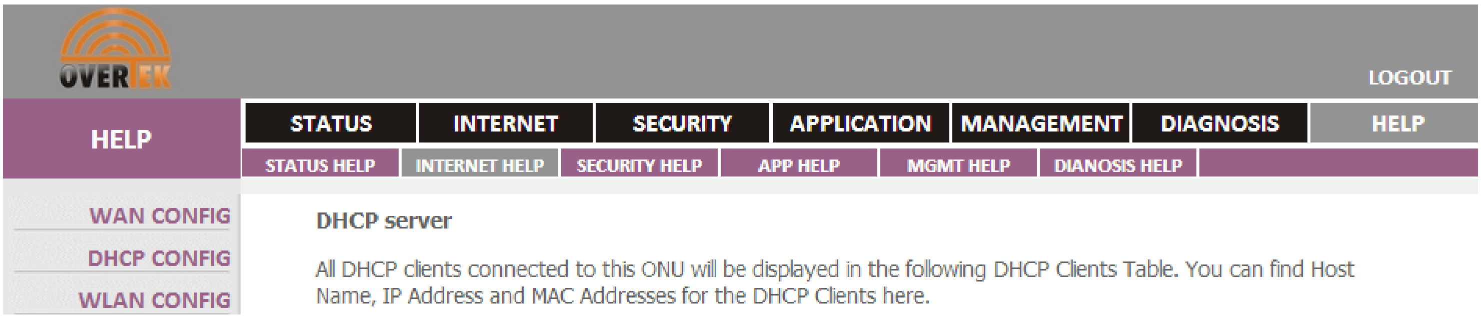


Mode: Configure WAN connection of Bridged or Routing Mode.

Service mode: Choose TR069 ISP Tunnel or User Tunnel.

9.2.2. DHCP Config

Click ‘ **Help** ‘ – ‘**Internet Help** ‘ – ‘**DHCP Config’** to view the help information of DHCP Configuration.

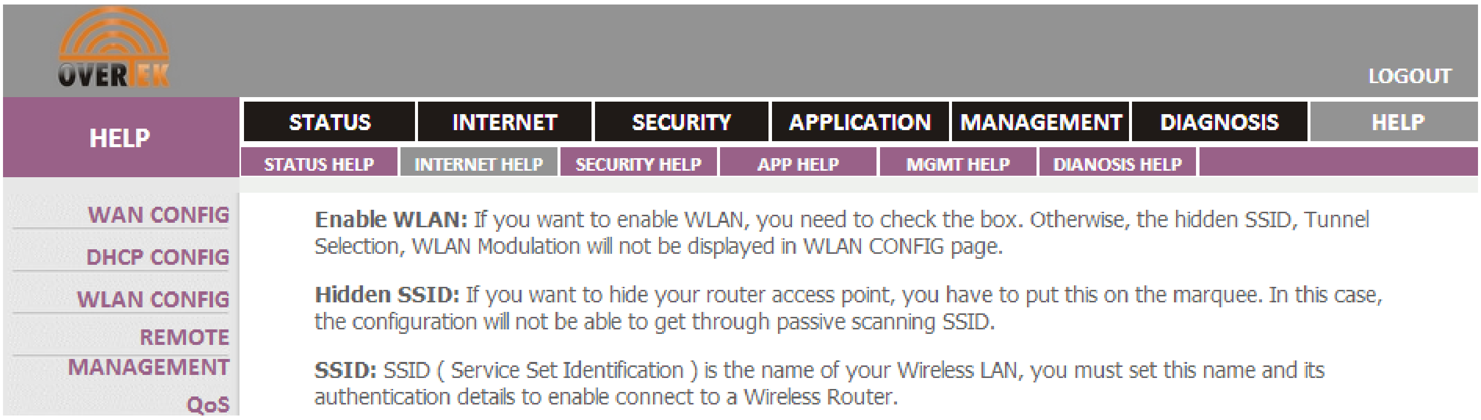


DHCP server

All DHCP clients connected to this ONU will be displayed in the following DHCP Clients Table. You can find Host Name, IP Address and MAC Addresses for the DHCP Clients here.

9.2.3. WLAN Config

Click ‘ **Help** ‘ – ‘**Internet Help** ‘ – ‘**WLAN Config’** to view the help information of Wireless LAN Configuration.



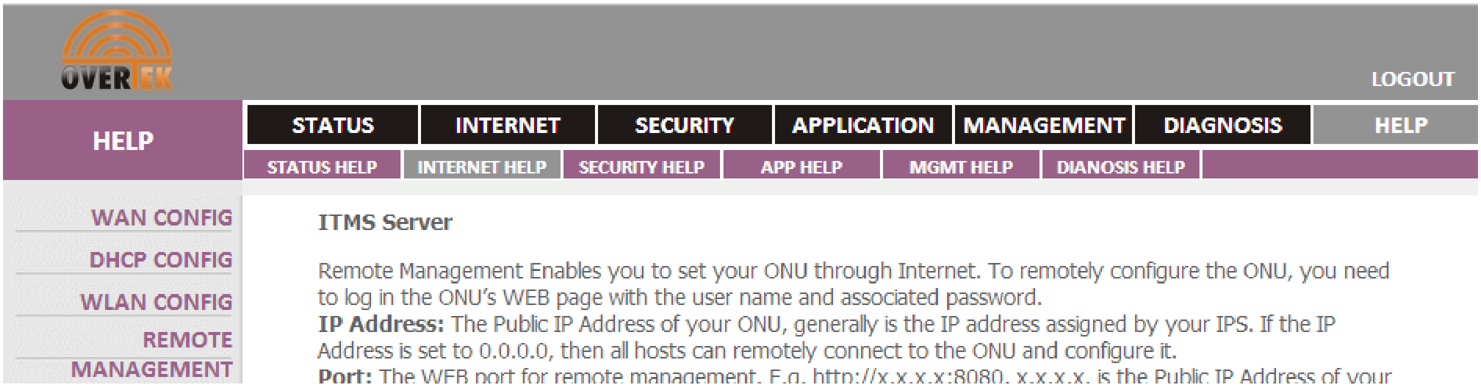
Enable WLAN: If you want to enable WLAN, you need to check the box. Otherwise, the hidden SSID, Tunnel Selection, WLAN Modulation will not be displayed in WLAN CONFIG page.

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

SSID: SSID (Service Set Identification) is the name of your Wireless LAN, you must set this name and its authentication details to enable connect to a Wireless Router.

9.2.4. Remote Management

Click ‘ **Help** ‘ – ‘**Internet Help** ‘ – ‘**Remote Management’** to view the help information of remote management.

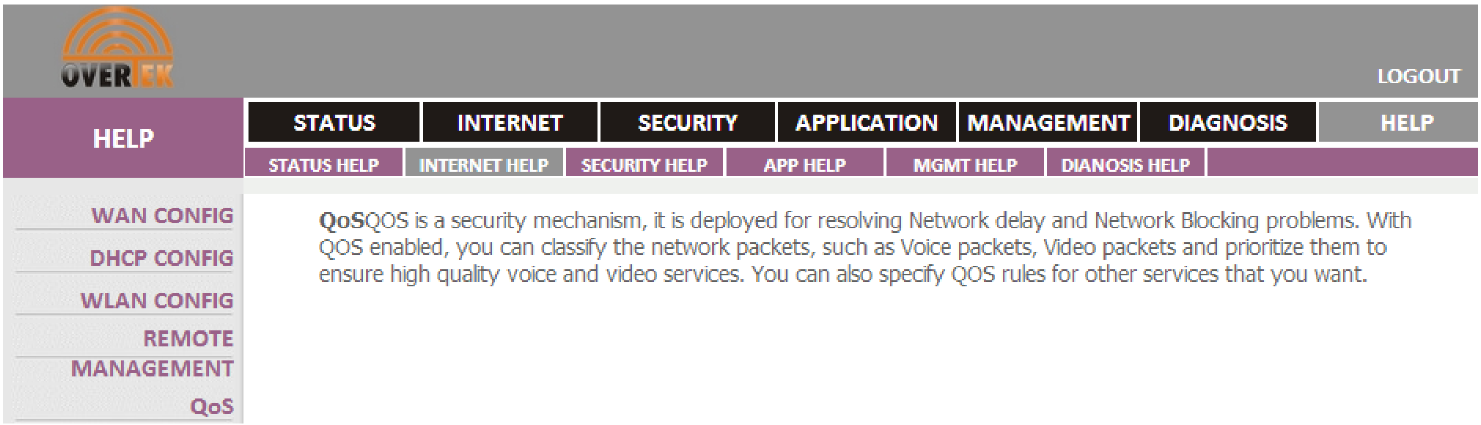


ITMS Server

Remote Management Enables you to set your ONU through Internet. To remotely configure the ONU, you need to log in the ONU's WEB page with the user name and associated password.
IP Address: The Public IP Address of your ONU, generally is the IP address assigned by your IPS. If the IP Address is set to 0.0.0.0, then all hosts can remotely connect to the ONU and configure it.
Port: The WEB port for remote management. E.g. http://x.x.x.x:8080. x.x.x.x. is the Public IP Address of your

9.2.5. QOS

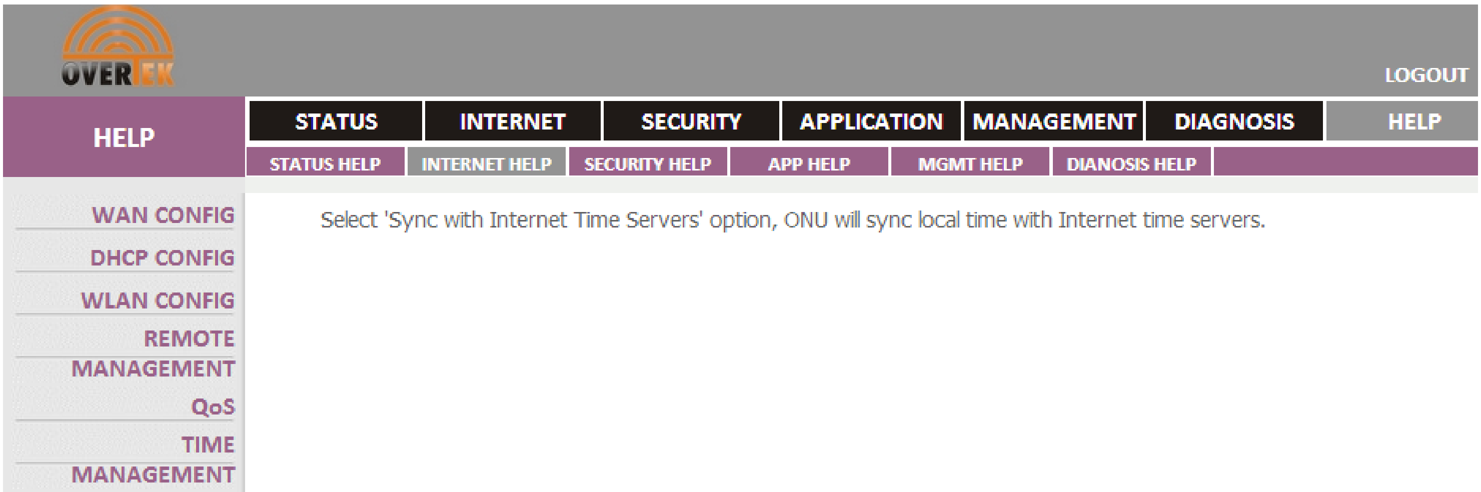
Click ' **Help** ' – '**Internet Help** ' – '**QOS '** to view the help information of QOS Configuration.



QoSQOS is a security mechanism, it is deployed for resolving Network delay and Network Blocking problems. With QOS enabled, you can classify the network packets, such as Voice packets, Video packets and prioritize them to ensure high quality voice and video services. You can also specify QOS rules for other services that you want.

9.2.6. Time Management

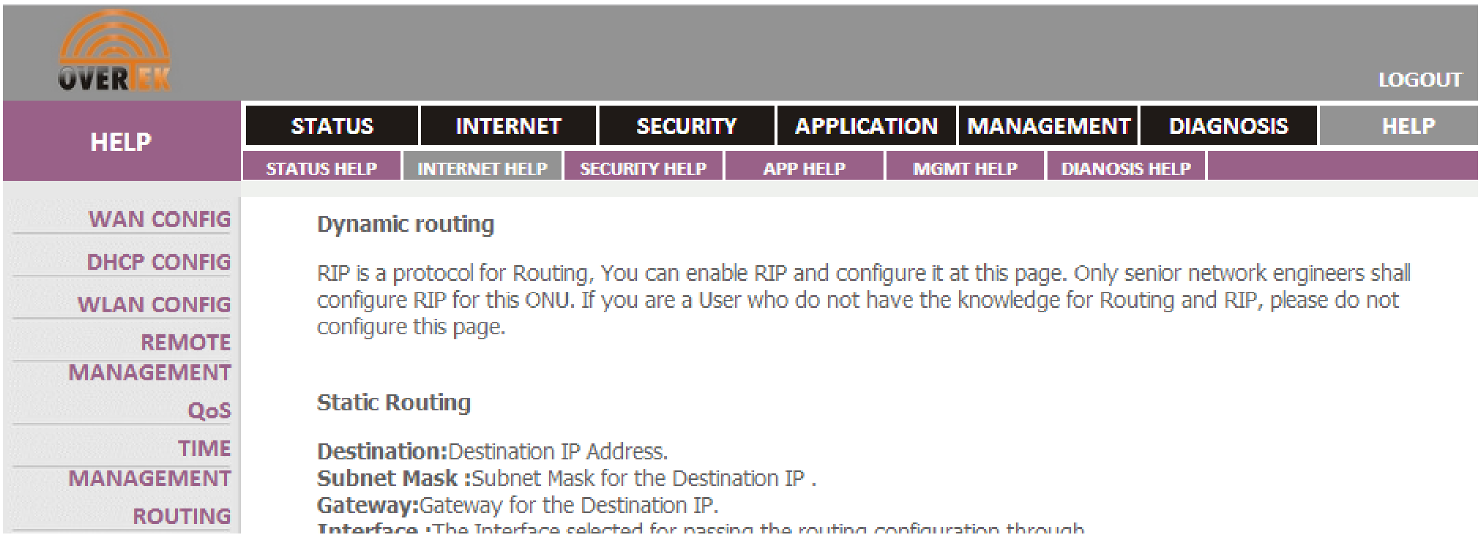
Click ' **Help** ' – '**Internet Help** ' – '**Time Management '** to view the help information of time settings.



Select 'Sync with Internet Time Servers' option, ONU will sync local time with Internet time servers.

9.2.7. Routing

Click ' **Help** ' – '**Internet Help** ' – '**Routing '** to view the help information of Routing Configurations.



Dynamic routing

RIP is a protocol for Routing, You can enable RIP and configure it at this page. Only senior network engineers shall configure RIP for this ONU. If you are a User who do not have the knowledge for Routing and RIP, please do not configure this page.

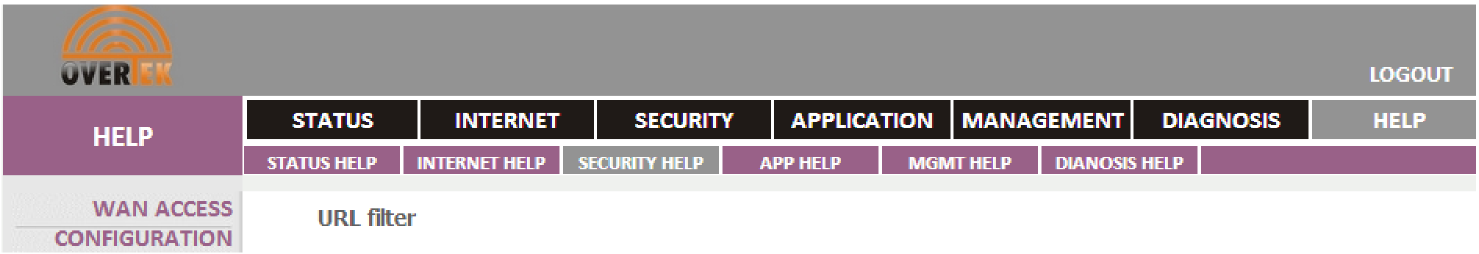
Static Routing

Destination: Destination IP Address.
Subnet Mask : Subnet Mask for the Destination IP .
Gateway: Gateway for the Destination IP.
Interface : The Interface selected for passing the routing configuration through

9.3. Security Help

9.3.1. WAN Access Configuration

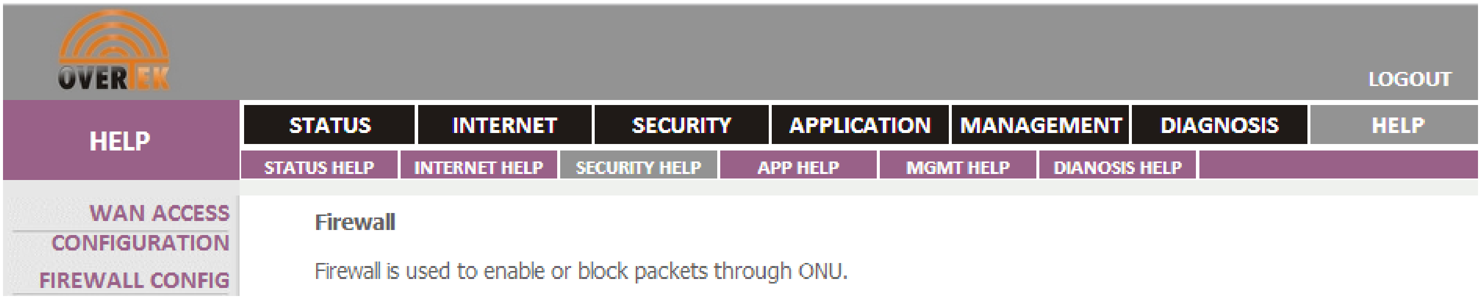
Click ‘ **Help** ‘ – ‘**Security Help** ‘ – ‘**WAN Access Configuration ’** to view the help information of URL Filter.



URL filter

9.3.2. Firewall Config

Click ‘ **Help** ‘ – ‘**Security Help** ‘ – ‘**Firewall Config ’** to view the help information of Firewall configurations.

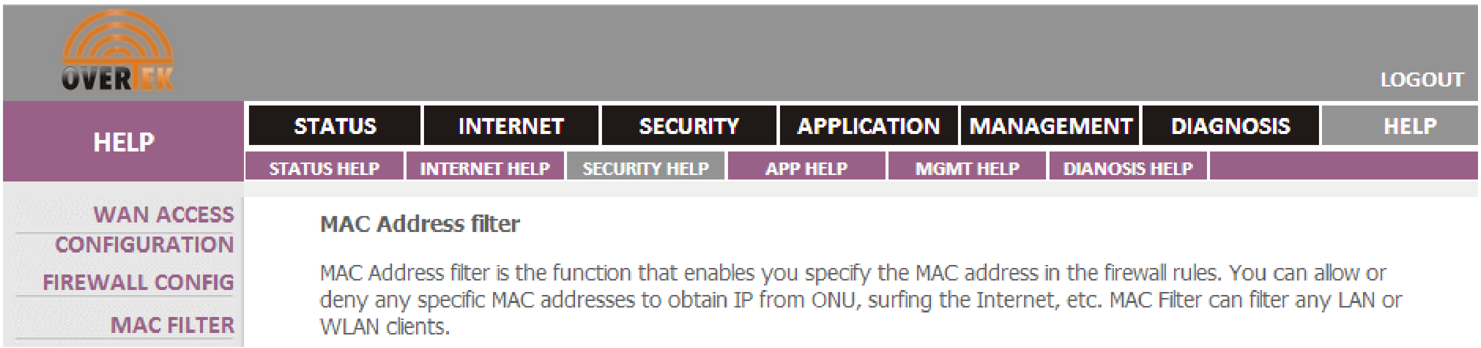


Firewall

Firewall is used to enable or block packets through ONU.

9.3.3. MAC Filter

Click ‘ **Help** ‘ – ‘**Security Help** ‘ – ‘**MAC Filter ’** to view the help information of MAC Filter.

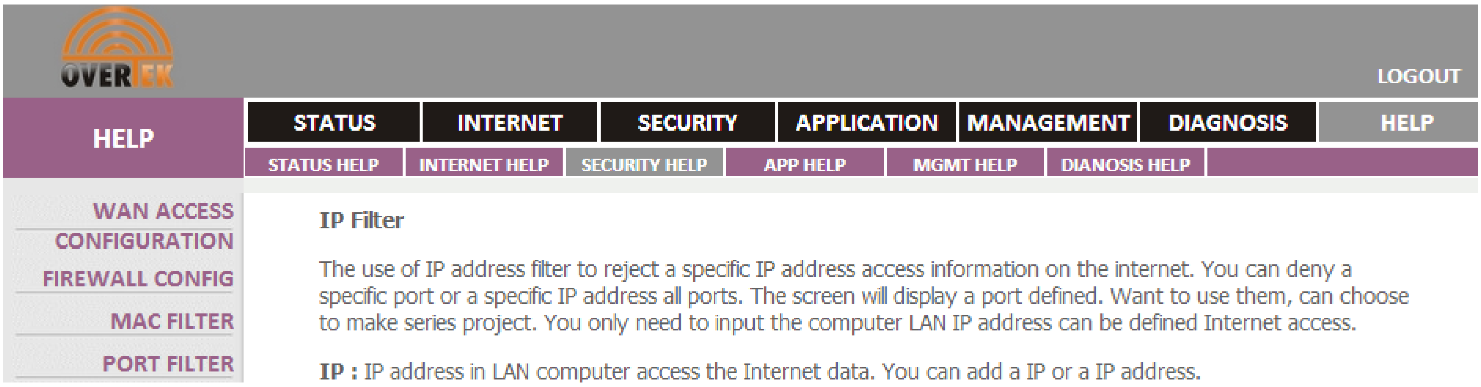


MAC Address filter

MAC Address filter is the function that enables you specify the MAC address in the firewall rules. You can allow or deny any specific MAC addresses to obtain IP from ONU, surfing the Internet, etc. MAC Filter can filter any LAN or WLAN clients.

9.3.4. Port Filter

Click ' **Help** ' – '**Security Help** ' – '**Port Filter '** to view the help information of Port Filter.



IP Filter

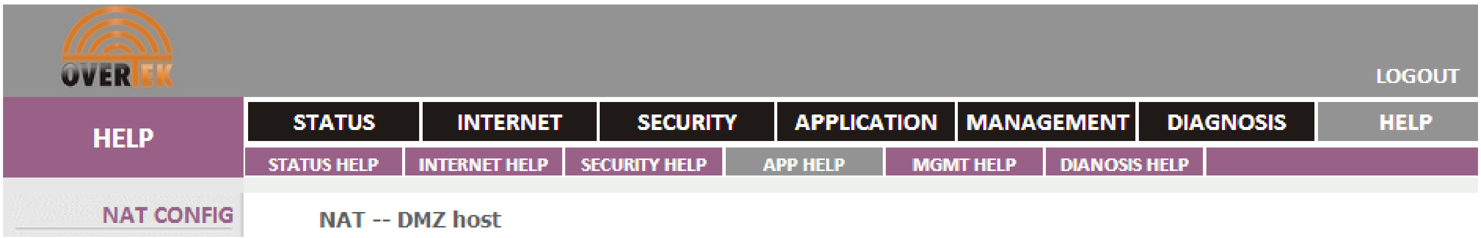
The use of IP address filter to reject a specific IP address access information on the internet. You can deny a specific port or a specific IP address all ports. The screen will display a port defined. Want to use them, can choose to make series project. You only need to input the computer LAN IP address can be defined Internet access.

IP : IP address in LAN computer access the Internet data. You can add a IP or a IP address.

9.4. APP Help

9.4.1. NAT Config

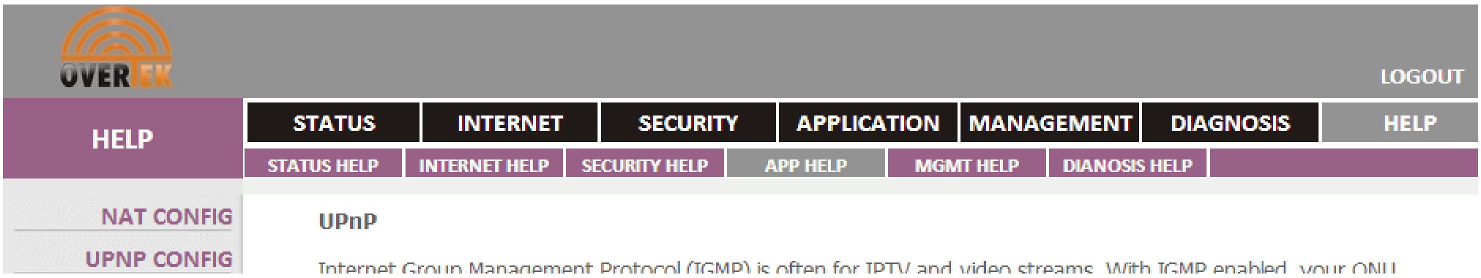
Click ' **Help** ' – '**APP Help** ' – '**NAT Config '** to view the help information of NAT.



NAT -- DMZ host

9.4.2. UPNP Config

Click ' **Help** ' – '**APP Help** ' – '**UPNP Config '** to view the help information of UPNP.

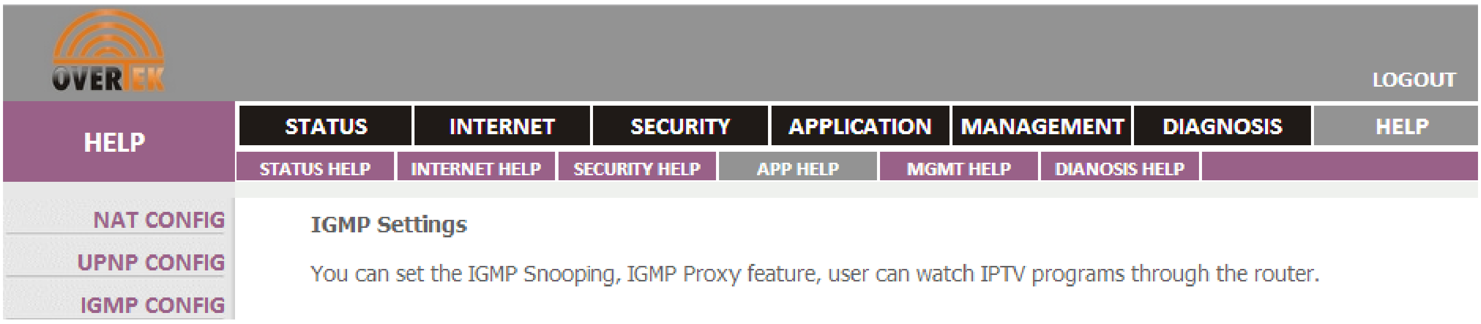


UPnP

Internet Group Management Protocol (IGMP) is often for IPTV and video streams. With IGMP enabled, your ONU

9.4.3. IGMP Config

Click ‘ **Help** ‘ – ‘**APP Help** ‘ – ‘**IGMP Config ’** to view the help information of IGMP.

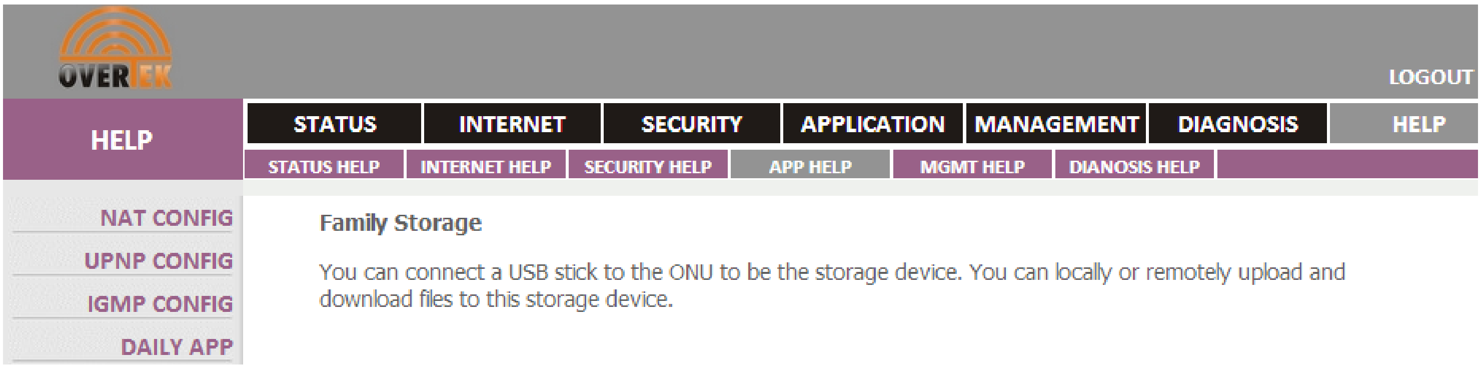


IGMP Settings

You can set the IGMP Snooping, IGMP Proxy feature, user can watch IPTV programs through the router.

9.4.4. Daily APP

Click ‘ **Help** ‘ – ‘**APP Help** ‘ – ‘**Daily APP ’** to view the help information of Daily Applications.

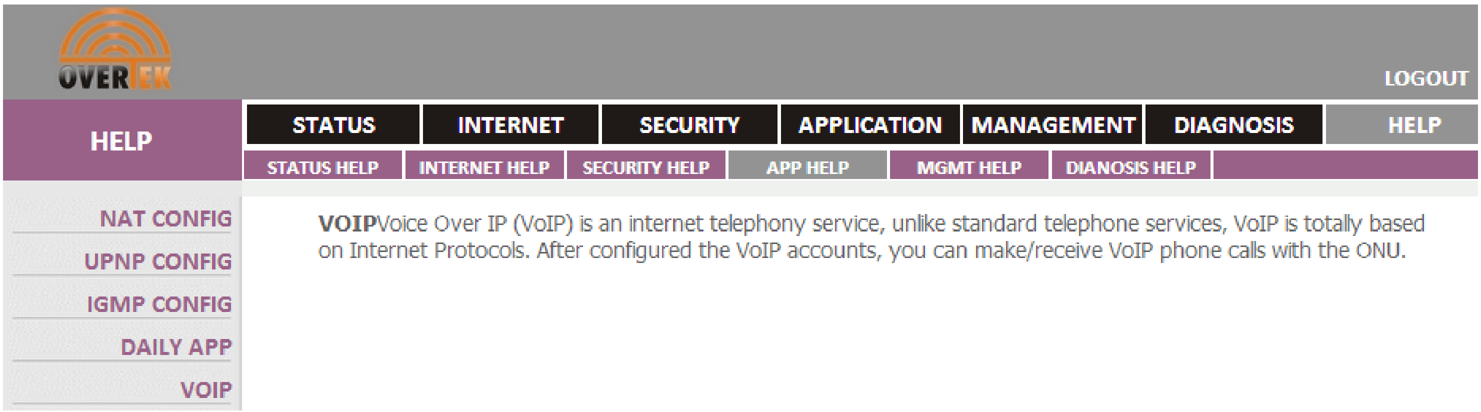


Family Storage

You can connect a USB stick to the ONU to be the storage device. You can locally or remotely upload and download files to this storage device.

9.4.5. VoIP

Click ‘ **Help** ‘ – ‘**APP Help** ‘ – ‘**VoIP ’** to view the help information of VoIP.

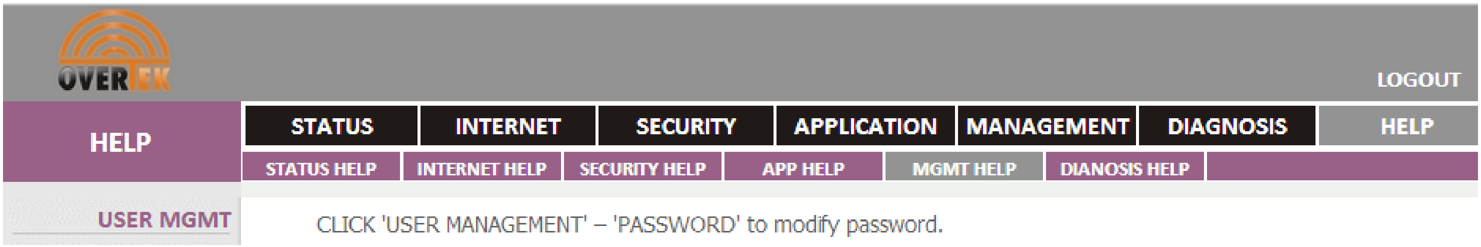


VOIPVoice Over IP (VoIP) is an internet telephony service, unlike standard telephone services, VoIP is totally based on Internet Protocols. After configured the VoIP accounts, you can make/receive VoIP phone calls with the ONU.

9.5. MGMT HELP

9.5.1. User MGMT

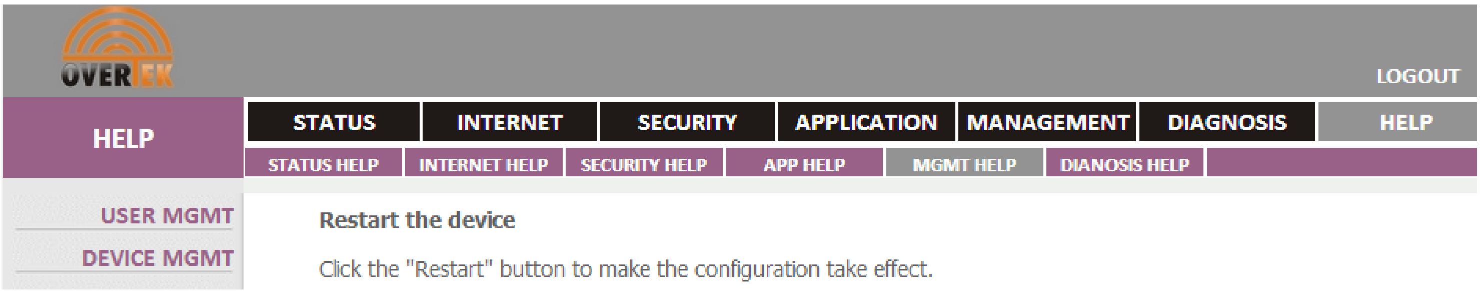
Click ‘ **Help** ‘ – ‘**MGMT Help** ‘ – ‘**USER MGMT ’** to view the help information of User account modification.



CLICK 'USER MANAGEMENT' – 'PASSWORD' to modify password.

9.5.2. Device MGMT

Click ‘ **Help** ‘ – ‘**MGMT Help** ‘ – ‘**DEVICE MGMT ’** to view the help information of Device Management.

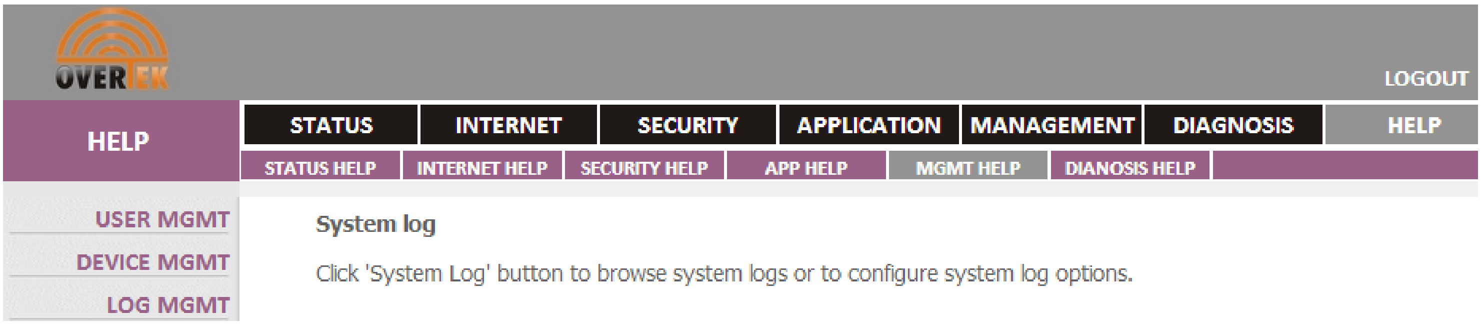


Restart the device

Click the "Restart" button to make the configuration take effect.

9.5.3. LOG MGMT

Click ‘ **Help** ‘ – ‘**MGMT Help** ‘ – ‘**LOG MGMT ’** to view the help information of Log management.

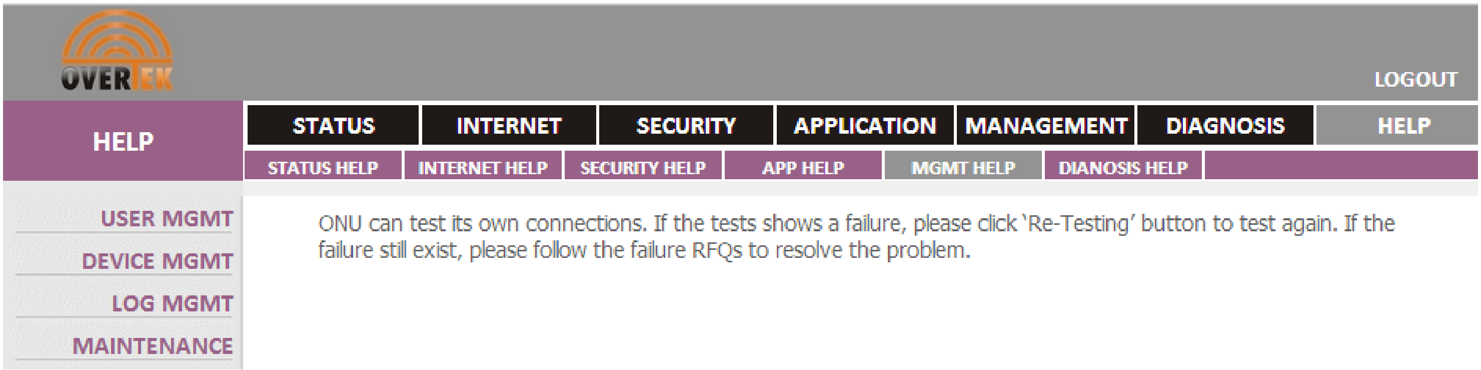


System log

Click 'System Log' button to browse system logs or to configure system log options.

9.5.4. Maintenance

Click ‘ **Help** ‘ – ‘**MGMT Help** ‘ – ‘**Maintenance ’** to view the help information of maintenance.

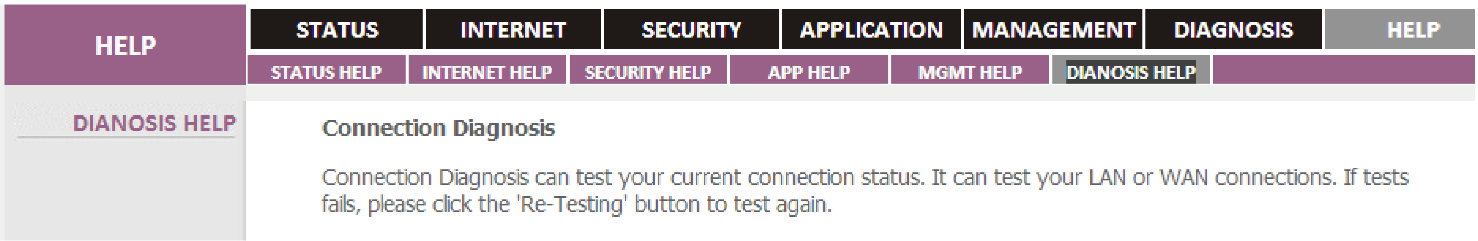


ONU can test its own connections. If the tests shows a failure, please click ‘Re-Testing’ button to test again. If the failure still exist, please follow the failure RFQs to resolve the problem.

9.6. DIANOSIS HELP

9.6.1. DIANOSIS HELP

Click ‘ **Help** ‘ – ‘**DIANOSIS HELP** ‘ – ‘**DIANOSIS HELP’** to view the help information of Diagnosis.



Connection Diagnosis

Connection Diagnosis can test your current connection status. It can test your LAN or WAN connections. If tests fails, please click the 'Re-Testing' button to test again.

---------The End of this User Manual

Copyright Notice:

Disclaimer Notice:

No license is granted, implied or otherwise, under any patent or patent rights of OverTek. OverTek, makes no warranties, implied or otherwise, in regard to this document and to the products described in this document. The information provided by this document is believed to be accurate and reliable to the publication date of this document. However, OverTek assumes no responsibility for any errors in this document. Furthermore, OverTek, assumes no responsibility for the use or misuse of the information in this document and for any patent infringements that may arise from the use of this document. The information and product specifications within this document are subject to change at any time, without notice and without obligation to notify any person of such change.

OverTek

www.overtek.com.br