AN5506-01-A

GPON Optical Network Terminal

Product Manual

Version: A/1

FiberHome Telecommunication Technologies Co., Ltd.

April 2017

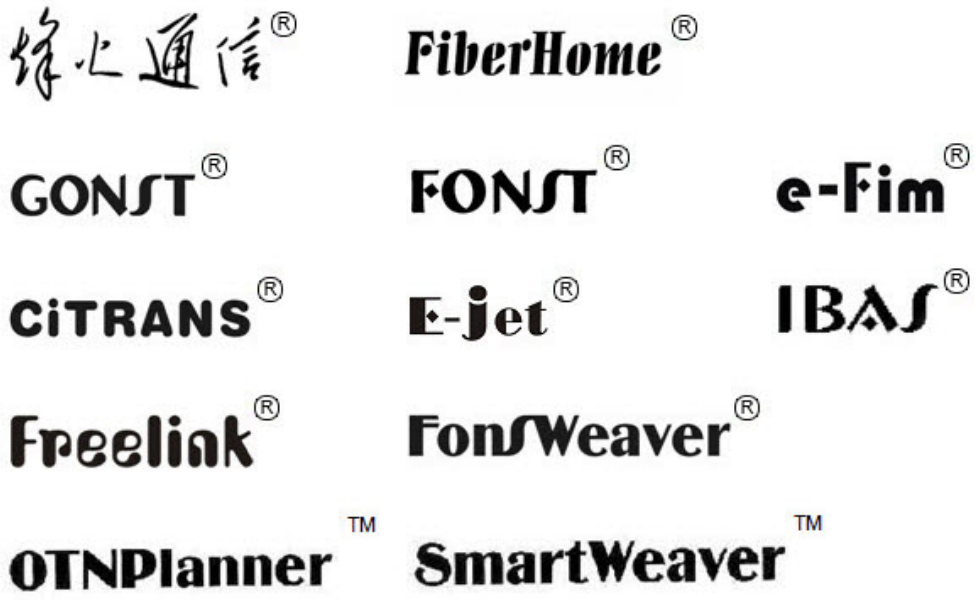
Thank you for choosing our products.

We appreciate your business. Your satisfaction is our goal. We will provide you with comprehensive technical support and after-sales service. Please contact your local sales representative, service representative or distributor for any help needed at the contact information shown below.

Fiberhome Telecommunication Technologies Co., Ltd.

Address: No. 67, Guanggu Chuangye Jie, Wuhan, Hubei, China
Zip code: 430073
Tel: +6 03 7960 0860/0884 (for Malaysia)
+91 98 9985 5448 (for South Asia)
+593 4 501 4529 (for South America)
Fax: +86 27 8717 8521
Website: http://www.fiberhomegroup.com

Legal Notice



are trademarks of FiberHome Telecommunication Technologies Co., Ltd. (Hereinafter referred to as FiberHome)

All brand names and product names used in this document are used for identification purposes only and are trademarks or registered trademarks of their respective holders.

All rights reserved

No part of this document (including the electronic version) may be reproduced or transmitted in any form or by any means without prior written permission from FiberHome.

Information in this document is subject to change without notice.

Safety Precautions

For your correct and safe operations on the equipment, please carefully read and strictly observe the following safety instructions:

- High optical power can cause bodily harm, especially to eyes. Never look directly into the end of the optical transmitter fiber jumper or the end of its active connector.
- Exercise care if you must bend fibers. If bends are necessary, the fiber bending radius should never be less than 38mm.
- Overloaded power sockets or damaged cables and connectors may cause electric shock or fire. Regularly check related electric cables. If any of them is damaged, replace it immediately.
- Use the power supply adapter provided in the package only. Using other adapters may cause equipment damage or operation failures.
- Install the equipment in a well ventilated environment without high temperature or direct sunlight to protect the equipment and its components from overheating, which can result in damage.
- Disconnect the power in lightning weather and disconnect all the wires and cables on the device (such as the power cable, network cable and phone cable), so as to prevent device from being damaged by lightning.
- Do not place this equipment in damp or near moisture environment. Water will lead to abnormal operation of device and even the danger caused by short circuit.
- Do not lay this equipment on an unsteady base.

Contents

1 Documentation Guide

Document Orientation

AN5506-01-A Product Manual introduces the positioning, features, functions, technical specifications of the ONT (Optical Network Terminal) product AN5506-01-A as well as Web configurations and handling of common problems, so that readers can have an overall knowledge about the AN5506-01-A.

Intended Readers

- Marketing personnel
- Commissioning engineers
- Operation and maintenance engineers

Version Information

Version	Version Information
A	Initial version

Content

Chapter	Content
Product Introduction	◆ Product positioning ◆ Product specifications ◆ Interface specifications ◆ Introduction to the AN5506-01-A
Web Configuration Guide	◆ Logging into Web configuration GUI locally ◆ Status ◆ Network ◆ Security ◆ Application ◆ Management
Handling Common Problems	Introduces how to handle common problems encountered during product operation and service test, including abnormal status of indicator LEDs, failing to access the Internet, failure of voice service test, etc.
Standards and Protocols	International standards and communications protocols

2 Product Introduction

- ☑ Product Positioning
- ☑ Product Specifications
- ☑ Interface Specifications
- ☑ Introduction to the AN5506-01-A

2.1 Product Positioning

The AN5506-01-A is an FTTH-type GPON ONT. It provides users with communication and entertainment services in the form of data, voice, video, and so on, to meet the integrated access demand of families and small-scaled enterprises.

See Figure 2-1 for the network positioning of the AN5506-01-A.

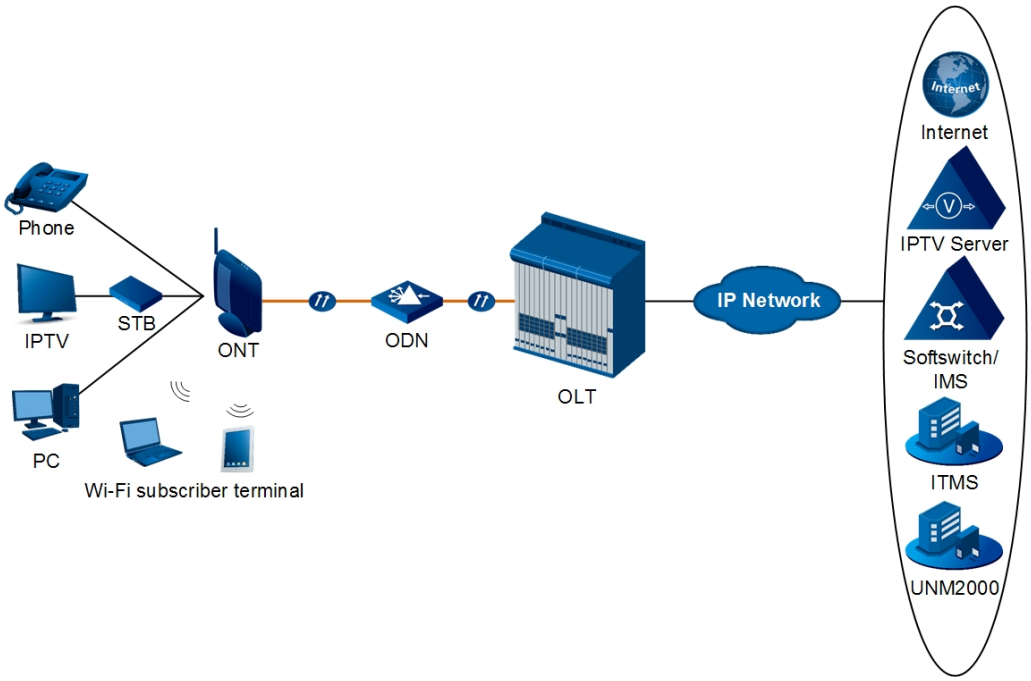


Figure 2-1 Network Application of the AN5506-01-A

2.2 Product Specifications

The tables below list the interfaces on the AN5506-01-A and the services supported by the ONT for users' reference on ONT configuration.

Table 2-1 lists the interfaces supported by the AN5506-01-A.

Table 2-1 Interfaces Supported by the AN5506-01-A

ONT Type	Ethernet Interface Quantity	POTS Interface Quantity	Wi-Fi Interface	USB Interface Quantity	CATV Interface Quantity
AN5506-01-A	1 (GE)	-	-	-	-

Table 2-2 lists the service types supported by the AN5506-01-A.

Table 2-2 Service Types Supported by the AN5506-01-A

ONT Type	Internet Service	Multicast Service	Voice Service	Wi-Fi Service
AN5506-01-A	√	√	×	×
Note: “√”indicates “supported”; “×” indicates “not supported”.				

Service Reliability

The AN5506-01-A supports MTBF up to 30 000 hours.

2.3 Interface Specifications

2.3.1 GPON Interface

See Table 2-3 for the specifications of the GPON interface.

Table 2-3 GPON Interface Specifications

Parameter	Specification
Standard compliance	ITU-T G.984, Class B+
Transmission rate	Rx: 2.5 Gbit/s; Tx: 1.25 Gbit/s
Interface mode	Single-mode
Interface type	SC/UPC or SC/APC
Maximum transmission distance	20 km
Central wavelength	Tx: 1310 nm; Rx: 1490 nm
Optical power	Tx optical power: 0.5 dBm to 5.0 dBm Rx optical power: -8 dBm to -29 dBm
Extinction ratio	More than 10 dB
Receiving sensitivity	-27 dBm to -29 dBm
Maximum overload optical power	-8 dBm

2.3.2 LAN Interface

Table 2-4 shows the specifications of the LAN interface.

Table 2-4 LAN Interface Specifications

Parameter	Specification
Standard compliance	IEEE 802.3ab
Interface type	RJ-45
Interface rate	10 Mbit/s, 100 Mbit/s or 1000 Mbit/s
Maximum transmission distance	100m
Working mode	Supports full-duplex or half-duplex and 10/100/1000 M auto negotiation.
Specifications of the cable used	CAT-5 unshielded twisted pair

2.4 Introduction to the AN5506-01-A

2.4.1 Appearance

The following describes the appearance of the AN5506-01-A, including the overall look, interfaces, buttons, and indicator LEDs.

Note:

The pictures here are only for reference.

Appearance

The overall look of the AN5506-01-A is shown in Figure 2-2.

Figure 2-2 Overall Look of the AN5506-01-A

Interface and Button

Interfaces and buttons of the AN5506-01-A are located on the rear and side panels of the equipment. Figure 2-3 shows the rear panel and Figure 2-4 shows the side panel.

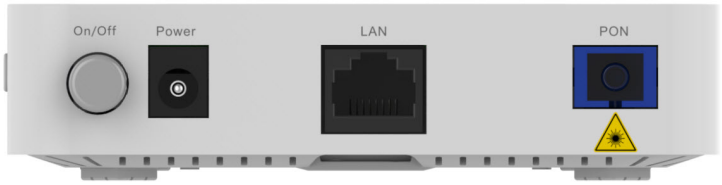


Figure 2-3 Rear Panel of the AN5506-01-A

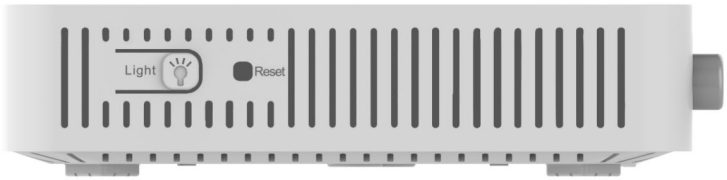


Figure 2-4 Side Panel of the AN5506-01-A

Table 2-5 describes the interfaces and buttons of the AN5506-01-A.

Table 2-5 Interfaces and Buttons of the AN5506-01-A

Interface and Button	Description	Function
On/Off	Power switch	Turns on or off the power for the equipment.
Power	Power interface	Connects with the power adapter.
LAN	Ethernet interface	Connects with the computer, IP router or IP set top box.
PON	Fiber interface	Connects with optical fiber for uplink access.
Light	Indicator LED switch	Turns on or off the indicator LEDs.
Reset	Reboot button	Pressing down the button for no more than 5 seconds to reboot the equipment; pressing down the button for more than 5 seconds to restore the factory settings and reboot the equipment.

Indicator LED Description

Indicator LEDs of the AN5506-01-A are located on the front panel of the equipment. Table 2-6 describes the indicator LEDs.

Table 2-6 Indicator LEDs on the AN5506-01-A

Indicator LEDs	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The equipment is powered on.
			OFF	The equipment is not powered on.
LAN	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data is transmitted.
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
LOS	Optical signal status indicator LED	Red	Blinking	The equipment has not received the optical signal.
			OFF	The equipment has received the optical signal.
PON	Register status indicator LED	Green	ON	The ONT is activated.
			Blinking	The ONT is being activated.
			OFF	Activation of the ONT is not yet started.

2.4.2 Product Characteristics

The AN5506-01-A can be used together with the OLT equipment to make up a GPON system and access multiple services for users. The AN5506-01-A has the following characteristics:

1. GPON access capability

- Conforms to ITU-T G.984 series of standards, with good interoperability.
- Provides large-capacity GPON transmission bandwidth: supports 2.5 Gbit/s for the downlink rate and 1.25 Gbit/s for the uplink rate.
- Supports the DBA (Dynamic Bandwidth Allocation) algorithm.
- Supports long-haul transmission. The maximum transmission distance can reach 20 km.

2. Abundant service types

The equipment provides abundant physical interfaces on the subscriber side to access multiple services such as Internet access and video services.

3. Gateway functions

- Serves as home gateway and provides abundant and reliable gateway functions.
- Functions as the DHCP Server to cater for application demands in different scenarios.
- Supports configuring protection against DoS attack, filtering of MAC addresses, IP addresses and URL addresses, firewall and ACL rules to guarantee safe operation of the equipment.

4. Remote automatic provisioning of services, maintenance and management

- The equipment adopts the management based on TR-069 and OMCI, and supports TR-069 over OMCI. It can manage terminal services without IP network, which facilitates automatic provisioning, maintenance and management of services remotely.

- Supports configuring the global profile and delivering the XML configuration file on the network management system. Only a few changes are required to deliver the ONT services in a batch manner and make network adjustment.
- Supports configuring the user-defined upgrade policies on the network management system so that the equipment can be upgraded automatically after being powered on.
- Supports collecting performance data of the ONT remotely via the network management system to enable real-time monitoring of the network performance.
- Supports remote fault isolation for the ONT via the network management system. Faults can be isolated remotely according to the alarms reported to reduce the maintenance cost.

2.4.3 Functions and Features

Table 2-7 lists the functions and features of the AN5506-01-A

Table 2-7 Functions and Features of the AN5506-01-A

Item		Description
GPON	GPON interface specifications	Compliant with standards ITU-T G.984.1, G.984.2, G.984.3 and G.984.4.
		Supports GEM encapsulation (Ethernet over GEM is supported, but ATM encapsulation is not supported).
		The GPON system adopts the single-fiber bidirectional transmission mechanism, using the TDMA mode with the wavelength 1310 nm in the uplink direction, and the broadcast mode with the wavelength 1490 nm in the downlink direction.
		Supports the embedded OAM message, PLOAM message and OMCI message.
		Supports the splicing of data packets and OMCI protocol packets in the uplink direction. Splicing with adaptive message length and that with fixed length are supported.
	GEM Port	Supports bearing the downlink broadcast packets and unknown multicast packets via the broadcast GEM port.
		Supports mapping from GEM ports to T-CONTs.
		Supports multiple flow mapping modes.
		Supports the GEM port loopback.
	T-CONT	Supports T-CONTs of Type 1 to Type 5.
		A T-CONT supports no less than 64 GEM ports.

Table 2-7 Functions and Features of the AN5506-01-A (Continued)

Item		Description
		Supports eight T-CONTs.
	DBA	Supports DBA in the SR and NSR modes.
		Supports DBA Piggy-back DBRu Mode 0.
	FEC	Supports bi-directional FEC: downlink FEC decoding and uplink FEC encoding.
		Supports downlink FEC performance statistics.
	Encryption	Supports encryption of downlink unicast data channel.
		Supports the AES-128 encryption algorithm.
		Supports generation of the key and response to the OLT's request for key.
		Supports OMCI channel encryption.
	Registration authentication	Supports the ONT registration process as specified in ITU-T. G.984.3.
		Supports four authentication modes: SN, Password, SN + Password and LOID.
		Supports performance statistics for the Ethernet interface.
		Supports performance statistics for the GEM interface.
Ethernet		Complies with the IEEE 802.3 standard.
		Supports configuring the Ethernet interface rate, working mode, and MDI/MDIX auto-negotiation mode.
		Supports manual configuration to the rate 10/100/1000 Mbit/s.
		Supports manual configuration of the half duplex or full duplex mode.
		Supports unlink / downlink rate control based on the Ethernet interface, with the control granularity of 64 kbit/s.
		Supports the PAUSE flow control.
		Supports the loopback detection at the subscriber side.
		Supports learning up to 1024 MAC addresses.
		Supports global configuration of enabling / disabling the MAC address learning function.
		Supports remote configuration of the MAC address aging time. The value ranges between 0s and 300s. The default value is 80s.
Multicast		Supports the IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.
		Supports filtering and forwarding of multicast MAC addresses.
		Supports controllable multicast and uncontrollable multicast.
		Supports fast leave.
		Supports translation, transparent transmission and stripping of the multicast VLAN tags.

Table 2-7 Functions and Features of the AN5506-01-A (Continued)

Item	Description
	Supports VLAN translation for the uplink multicast protocol packets.
	Supports filtering the downlink multicast packets.
	Supports bearing downlink multicast service flow and IGMP signaling packets via different GEM ports.
	Supports configuration of the multicast GEM ports.
	Supports authentication of the GEM ports.
	Supports no less than 256 multicast groups.
	Uses the IPoE/PPPoE mode for the multicast services.
	Supports the IPv6 Snooping multicast service, supports the MLDv1 information, MLDv2 query information and MLDv2 report information.
VLAN	Supports the IEEE 802.1Q VLAN standard.
	Supports joining the 802.1Q VLAN in the tag / untag mode.
	Supports up to 4095 VLANs.
Wire-speed forwarding	Supports Layer 2 / Layer 3 wire-speed forwarding.
Layer 3 features	Supports the IPv4/v6 dual stack.
	Supports obtaining network parameters such as the user IP address, subnet mask and DNS in the DHCP mode. Supports reporting the physical location of the Ethernet interface based on DHCP Option82.
	Supports obtaining user IP addresses in the PPPoE mode, and supports the PPPoE+ function for precise identification of users.
	Supports static routing and default routing.
	Supports DDNS, NAT, port forwarding and DMZ.
	Supports ARP, UPnP, ALG, Portal and QoS.
Security	Supports the firewall.
	Supports packet filtering.
	Supports filtering MAC addresses.
	Supports filtering URL addresses.
	Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
	Supports configuring the HTTPS safe channel.
	Supports configuring ACL rules for the ONT.
	Supports remote control.
Management and maintenance	Supports local service configuration, query and software upgrade based on the Web page.
	Supports management of the OMCI configuration and queries.

Table 2-7 Functions and Features of the AN5506-01-A (Continued)

Item	Description
	Supports delivering the XML configuration file via the OMCI, alarm reporting, alarm synchronization and performance statistics.
	Supports automatic provisioning of services, equipment management and software upgrade remotely based on OMCI/TR-069.
	Supports query of the ONT optical module information.
	Supports TYPE B protection.
QoS	Provides abundant QoS functions; supports global configuration of queue priorities and flexible mapping of 802.1p values in packets.
	Supports the ACL function to match traffic based on the ACL rules.
	Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of the queues under scheduling, so as to guarantee the quality of high-QoS services such as voice and video in the multi-service scenario.

2.4.4 Technical Specifications

See Table 2-8 for the technical specifications of the AN5506-01-A.

Table 2-8 Technical Specifications of the AN5506-01-A

Classification	Item	Description
Mechanical parameters	Dimensions	25.5mm × 112mm × 112mm (H × W × D)
	Wall mounting hole distance	75mm
	Weight	About 120g
Power supply parameter	DC	DC 12 V/0.5A
Power consumption parameters	Static power consumption	3W
	Maximum power consumption	4W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation)

3 Web Configuration Guide

The following introduces the Web GUIs for the administrator users of the AN5506-01-A, including the parameter meanings and operation methods.

 Note:

Configure the ONT on the OLT using the access network management system. Please refer to the relevant OLT configuration guide.

- Logging into Web Configuration GUI Locally
- Status
- Network
- Security
- Application
- Management

3.1 Logging into Web Configuration GUI Locally

The following discusses how to log into the ONT Web GUI locally and introduces the configuration GUI layout.

Prerequisites

- The ONT has been connected with the computer correctly.
- The user computer is started normally.
- The ONT is started normally.

  Press down the ONT power button. If the power indicator LED is ON, the ONT is powered on normally.

Planning Data

Before setting up the configuration environment, prepare the data as shown in Table 3-1.

Table 3-1 Planning Data for Logging into the Web GUI Locally

Item	Description
Username and password	Factory default value: ◆ Administrator ▶ Username: admin ▶ Password: admin ◆ Common user ▶ Username: user ▶ Password: user1234 **Note: Some operators have customized username and password, so that the default username and password may be different from the ones mentioned above. In this case, ask local operator for the administrator information. For common users, please refer to the *User Guide* attached to the device or the label at the bottom of the device.** **Note: The password is case sensitive.**
Management IP address and subnet mask of the ONT	Factory default value: ◆ IP address: 192.168.1.1 ◆ Subnet mask: 255.255.255.0 **Note: Some operators require customized management IP address, so that the default management IP address may be different from the one mentioned above. In this case, please refer to the *User Guide* attached to the device or the label at the bottom of the device.**
The IP address and the subnet mask of the user computer	◆ Set this item to obtaining IP address automatically (recommended) based on DHCP. ◆ Set this item to static IP address, which should be in the same network segment with the management IP address of the ONT. ▶ IP address: 192.168.1.X (X is a decimal integer between 2 and 253) ▶ Subnet mask: 255.255.255.0

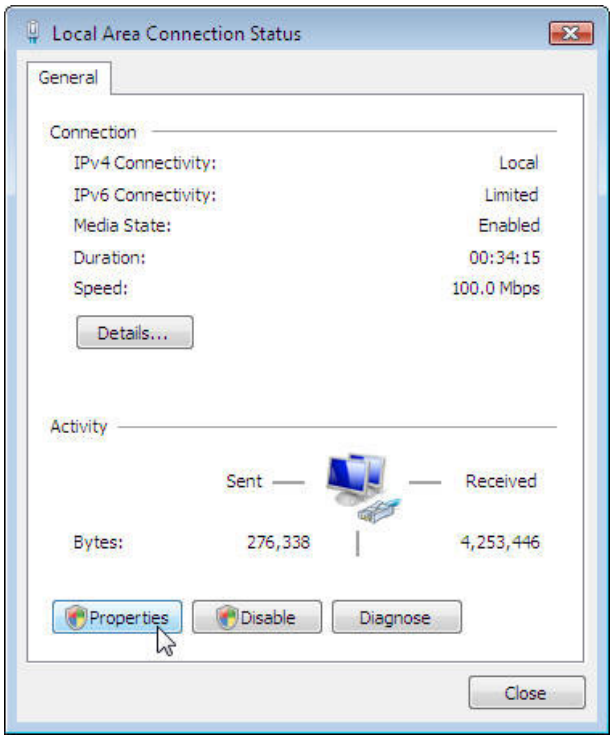
Operation Procedure

1. Set the IP address and the subnet mask of the computer.

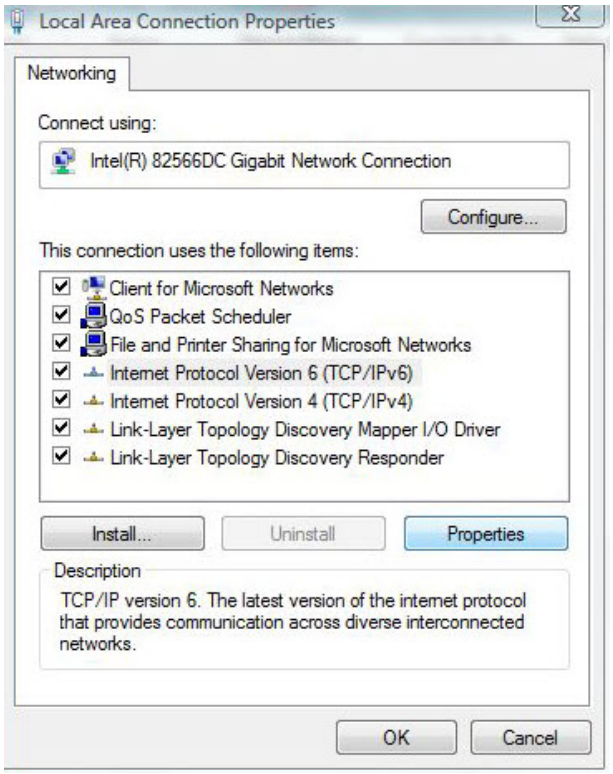
   ▶ The operations on the Windows 7 operating system are as follows:

a) In the Windows taskbar, select **Start→Control Panel** and click **Network and Sharing Center**.

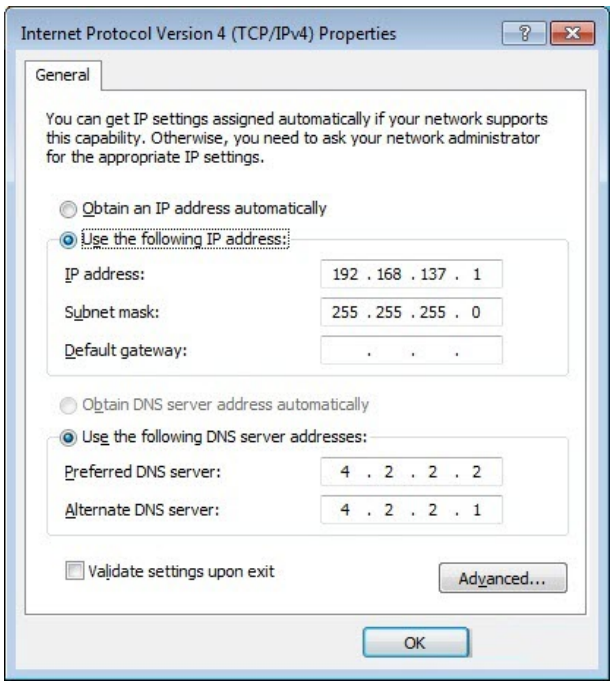
b) Click **Local Area Connection** to bring up the **Local Area Connection Status** dialog box, and click **Properties**.



c) In the **Local Area Connection Properties** dialog box that appears, double-click **Internet Protocol Version 4 (TCP/IPv4)**.



d) In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box that appears, set the IP address and subnet mask of the computer. (See Table 3-1 for the detailed values).

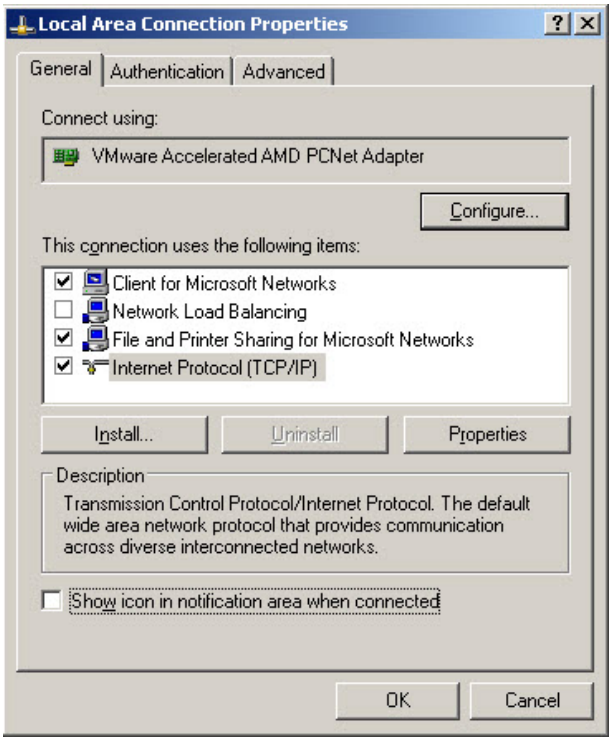


e) Click the **OK** button to save the configuration.

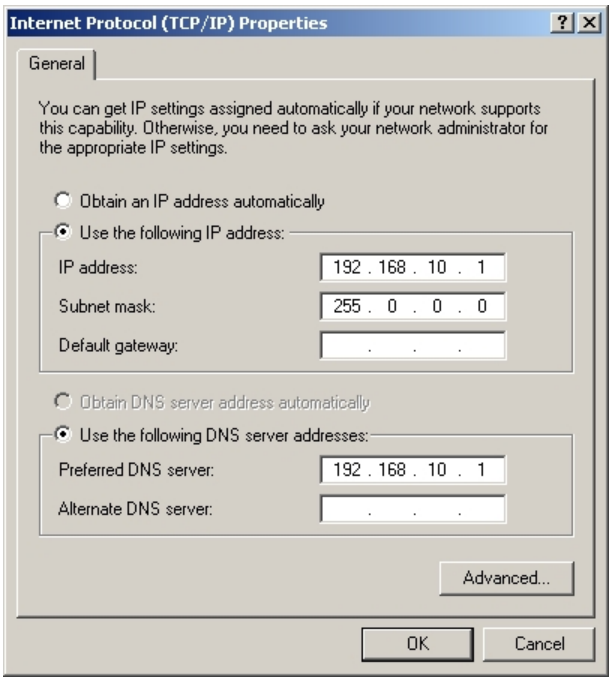
- The operations on the Windows XP operating system are as follows:

a) In the Windows taskbar, select **Start→Control Panel**. Double-click **Network Connection** to enter the network connection window.

b) Right-click **Local Connection** and select **Properties** from the shortcut menu to bring up the **Local Connection Properties** dialog box.



c) Double-click **Internet Protocol (TCP/IP)**. In the **Internet Protocol (TCP/IP) Properties** dialog box that appears, set the IP address and subnet mask of the computer. (See Table 3-1 for the detailed values).



d) Click the **OK** button to save the configuration.

2. Enter **http://192.168.1.1** (default management IP address of the ONT) in the browser address bar of the computer, and press the Enter key to bring up the user login dialog box.
3. Enter the administrator username and password in the login dialog box. Access the Web GUI after the password is authenticated.

Caution:

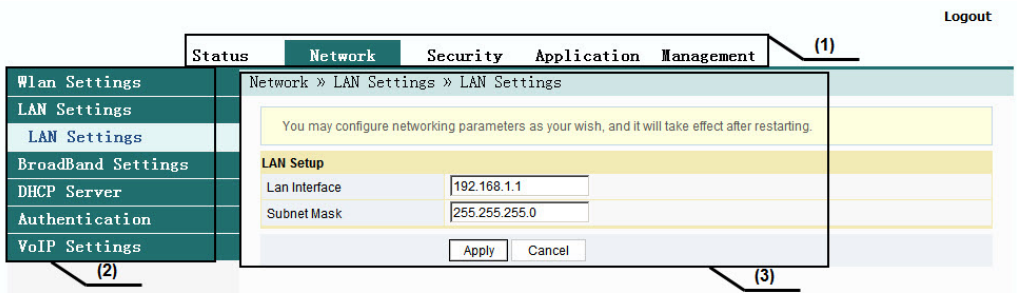
The system will log out automatically if no operation is performed in five minutes.

Web Configuration GUI Layout

The Web configuration GUI comprises three parts, as shown in Figure 3-1.

- Navigation bar. Click the link to enter the corresponding configuration management page.
- Link bar. Click the link to enter the sub-page for corresponding configuration management.

- Configuration management area. Displays the contents of the selected navigation bar and link bar.



(1) Navigation bar (2) Link bar (3) Configuration management area

Figure 3-1 Web Configuration GUI

Note:

The screenshots provided here are for reference only, and the actual Web GUIs for the equipment shall prevail.

The configuration GUI for the administrator is different from that for common users:

- The administrator can view and configure all the node items in the Web GUI.
- The common users can view and configure only part of the node items. The following lists the key nodes available for common users. The configuration items actually available in the Web GUI for common users shall prevail.
  - The **Status** tab.
  - **User Account** and **Device Reboot** in the **Management** tab.

3.2 Status

The following introduces how to view basic information about the ONT, including the device information, WAN side status, LAN side status and optical power status, etc.

3.2.1 Device Information

Select **Status** in the navigation bar, and select **Device Information→Device Information** in the left link bar to view the information such as the software version, hardware version, device model and device description. See Figure 3-2.

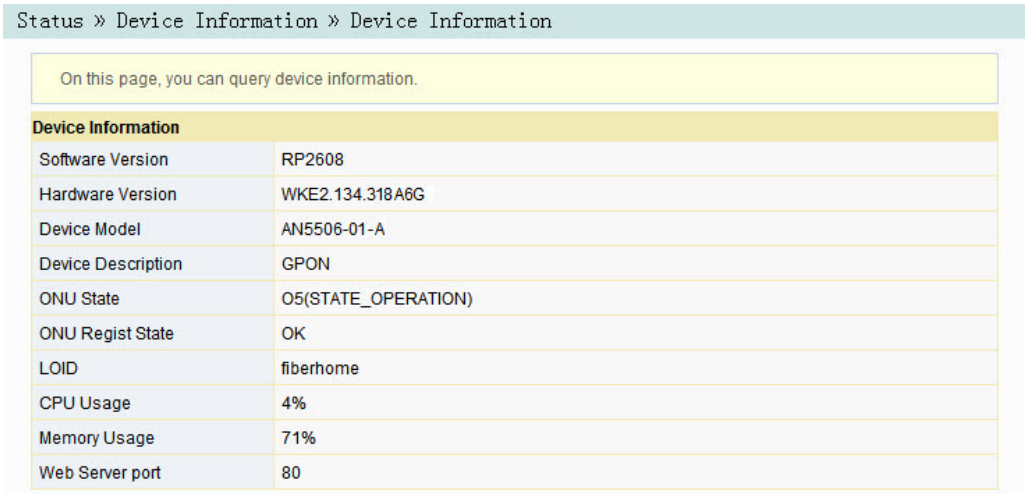


Figure 3-2 Device Information

3.2.2 WAN Side Status

Select **Status** in the navigation bar and select **Wan Status→Wan Status** in the left link bar to view the information such as the status, IP obtaining mode, IP address and subnet mask of the WAN interface. See Figure 3-3.

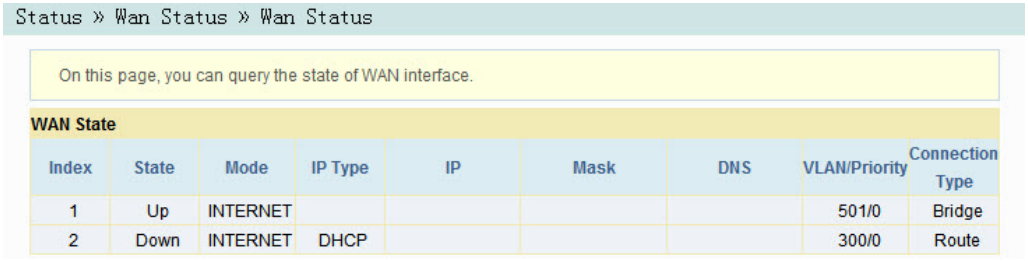


Figure 3-3 WAN Side Status

3.2.3 LAN Side Status

Check the status information about the LAN interface and the DHCP client end.

3.2.3.1 LAN Side Status

Select **Status** in the navigation bar and select **Lan Status→Lan Status** in the left link bar to view the information such as the IP address, subnet mask of the LAN side. See Figure 3-4.

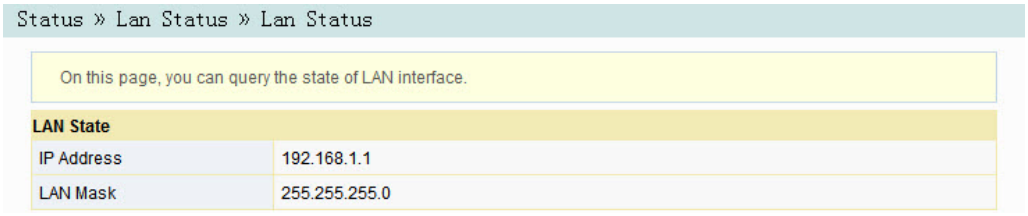


Figure 3-4 LAN Side Status

3.2.3.2 DHCP User List

Select **Status** in the navigation bar and select **Lan Status→DHCP Clients List** in the left link bar to view the information about the DHCP client end such as the IP address, MAC address and hired time. See Figure 3-5.

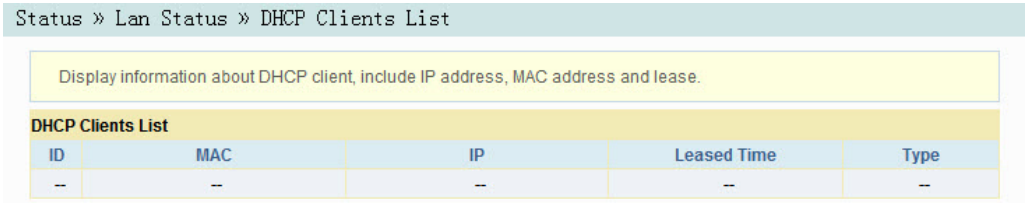


Figure 3-5 DHCP User List

3.2.4 Optical Power Status

Select **Status** in the navigation bar and select **Optical Info→Optical Info** in the left link bar to view the optical module information such as the Tx optical power, Rx optical power and working temperature. See Figure 3-6.

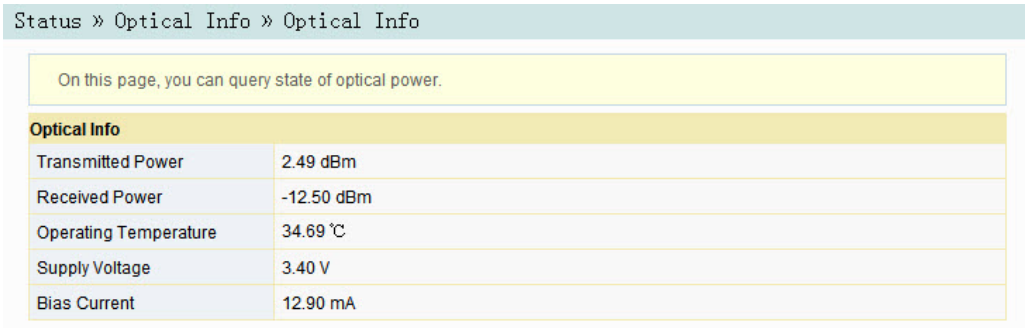


Figure 3-6 Optical Power Status

3.3 Network

The following introduces how to configure the LAN, broadband, DHCP server and authentication in the Web GUI.

3.3.1 LAN Settings

Configure the management IP address and subnet mask at the LAN side.

1. Select **Network** in the navigation bar and select **LAN Settings→LAN Settings** in the left link bar to open the LAN settings page, as shown in Figure 3-7.

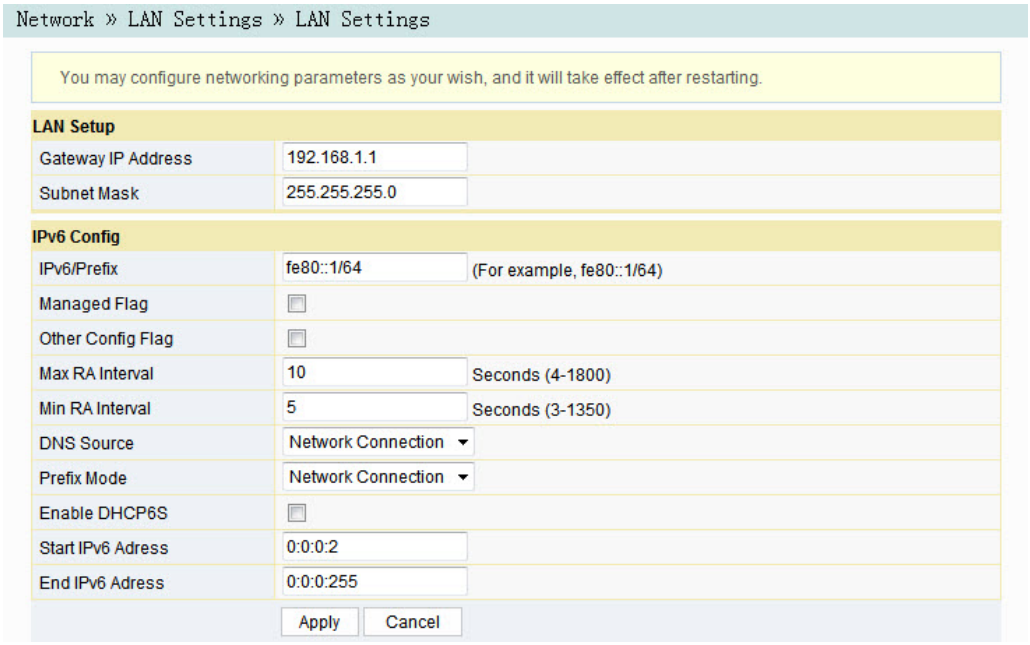


Figure 3-7 LAN Settings

2. Configure the management IP address and subnet mask at the LAN side. See Table 3-2 for the parameter description.

3. Click **Apply** to save and apply the configuration.

Table 3-2 Parameters of LAN Settings

Item	Description
IP address	The management IP address at the LAN side of the ONT. The default value is 192.168.1.1.
Subnet Mask	The subnet mask of the ONT for the LAN. The default value is 255.255. 255.0.
IPv6/Prefix	The IPv6 gateway address, including a prefix of 64 bits. The default value is fe80::1/64.
Managed Flag	Select whether to distribute the IPv6 address based on DHCP. The default value is Disable.
Other Config Flag	Select whether to distribute the IPv6 DNS information based on DHCP. The default value is Enable.
Max RA interval	The maximum interval for announcing the gateway information. The default value is 10.
Min RA interval	The minimum interval for announcing the gateway information. The default value is 5.

Table 3-2 Parameters of LAN Settings (Continued)

Item	Description
DNS source	The source of the DNS distributed to PC, including WAN connection, ONT proxy and static configuration. The default value is WAN connection.
Prefix mode	The source of the prefix information distributed to PC, including WAN connection and static configuration. The default value is WAN connection.
Enable DHCP6S	Sets whether to enable the DHCPv6 server. This item should be selected if Managed Flag or Other Config Flag is selected; otherwise the IP address or DNS information cannot be distributed. Enabled by default.
Start IPv6 Address	The starting address ID of the address pool for distribution of DHCPv6 IP addresses. The default value is 0:0:0:2.
End IPv6 Address	The ending address ID of the address pool for distribution of DHCPv6 IP addresses. The default value is 0:0:0:255.

3.3.2 Broadband Settings

Select different WAN connections for different network environment, or configure corresponding parameters for the selected WAN connection.

1. Select **Network** in the navigation bar and select **BroadBand Settings→ Internet Settings** in the left link bar to open the Internet settings page, as shown in Figure 3-8.

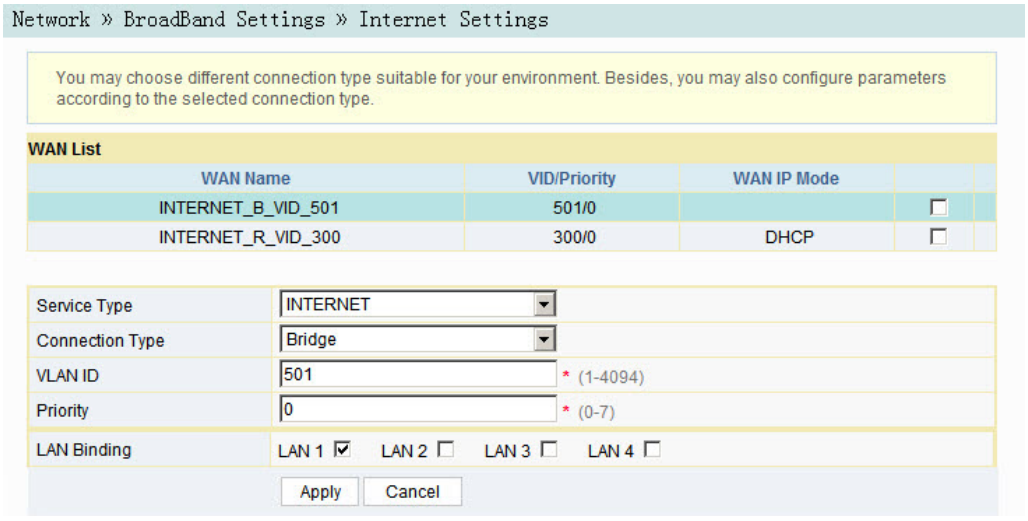


Figure 3-8 Internet Settings

2. Configure parameters relevant to the Internet at the WAN side. Table 3-3 introduces the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-3 Parameters for Internet Settings

Item	Description	
Service Type	Select the WAN port service type. ◆ TR069: this connection is only applicable for TR069. ◆ INTERNET: this connection is only applicable for Internet access. ◆ TR069_INTERNET: this connection is applicable for both TR069 and Internet access. ◆ VOIP: this connection is only applicable for voice application. ◆ VOIP_INTERNET: this connection is applicable for voice and Internet access. ◆ OTHER: other connections.	
Connection Type	Select the connection type of the WAN port. ◆ Bridge: the Layer 2 bridge connection mode. This connection mode can be used when the service type is set to INTERNET, IPTV or OTHER. ◆ Route: the Layer 3 router connection mode. This connection mode can be used when the service type is set to INTERNET, IPTV or OTHER.	
VLAN ID	Sets the VLAN ID of the WAN connection. The value ranges from 1 to 4094. The VLAN ID value here should be consistent with that on the user side of the OLT.	
COS	Sets the priority of the VLAN. The value ranges from 0 to 7.	
NAT	Enables or disables the NAT function.	◆ Users need to configure this item when the service type is set to **TR069_INTERNET** or **VOIP_INTERNET**. ◆ Users need to configure this item when the service type is set to **INTERNET** or **OTHER** and the connection type is set to **Route**.
DNS Relay	Enables or disables the DNS relay function.	
MTU	Enter the maximum transmission unit. It is advised to use the default value.	
LAN Binding	Select the LAN port to be bound with the WAN port.	

Table 3-3 Parameters for Internet Settings (Continued)

Item	Description	
IP Mode	The options include IPv4&IPv6, IPv4 and IPv6.	◆ Users need to configure this item when the service type is set to **TR069_INTERNET** or **VOIP_INTERNET**. ◆ Users need to configure this item when the service type is set to **INTERNET** or **OTHER** and the connection type is set to **Route**.
WAN IP Mode	Sets the IP address obtaining mode at the WAN side of the ONT. The options include DHCP, static and PPPoE. ◆ DHCP: Obtaining the IP address dynamically. ◆ Static: Setting the IP address in a static mode. ◆ PPPoE: PPPoE dialing mode.	This item should be set if the connection type is Route.
User Name	Enter the username provided by ISP.	This item should be set if the WAN IP Mode is set to PPPoE.
Password	Enter the password provided by ISP.	
Operation Mode	Sets the PPPoE connection mode. The default setting is "Keep Alive".	
IP Address	Enter the static IP address at the WAN side provided by ISP.	This item should be set when the IP Mode **is set to IPv4&IPv6** or **IPv4** and the WAN IP Mode is set to **static**.
Subnet Mask	Enter the subnet mask provided by ISP.	
Default Gateway	Enter the default gateway provided by ISP.	
Primary DNS Server	Enter the IP address of the active DNS server provided by ISP.	
Secondary DNS Server	Enter the IP address of the standby DNS server provided by ISP.	

Table 3-3 Parameters for Internet Settings (Continued)

Item	Description	
IPv6 Address	Enter the static IPv6 address at the WAN side provided by ISP.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv6** and the WAN IP Mode is set to **static**.
IPv6 Prefix Length	Enter the static IPv6 address prefix length at the WAN side provided by ISP.	
Default Gateway	Enter the default gateway provided by ISP.	
Primary DNS Server	Enter the IP address of the active DNS server provided by ISP.	
Secondary DNS Server	Enter the IP address of the standby DNS server provided by ISP.	
IPv6 Address Mode / IPv6 Prefix Mode	Select the IPv6 address obtaining mode / prefix obtaining mode.	This item should be set when the IP Mode is set to **IPv4&IPv6** or **IPv6** and the WAN IP Mode is set to **DHCP** or **PPPoE**.

3.3.3 DHCP Server

Using the DHCP function, the ONT can distribute the network parameters (such as IP address, gateway and DNS server IP address) to the devices (such as computer) within the LAN. Users can manage the IP addresses collectively using this function.

1. Select **Network** in the navigation bar, and then select **DHCP Server→DHCP Service** from the left link bar to open the DHCP server configuration page, as shown in Figure 3-9.

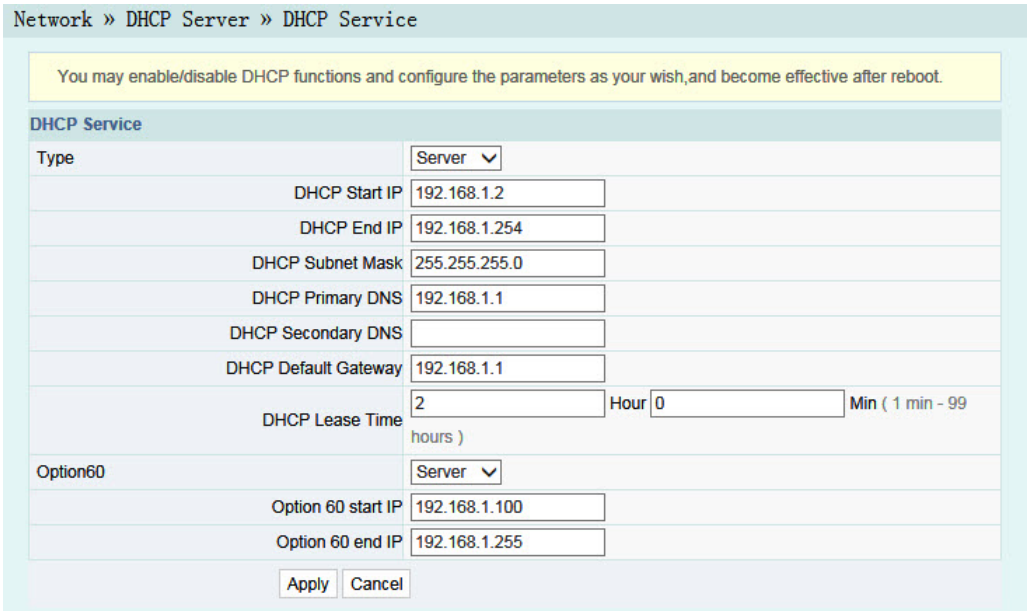


Figure 3-9 DHCP Service

2. Configure the DHCP server parameters as required. Table 3-4 describes the parameters.

3. Click **Apply** to save the configuration information. The configuration will take effect after the ONT is rebooted.

Table 3-4 Parameters for the DHCP Server

Item	Description	
Classification	Enables or disables the DHCP server. ◆ Server: Enables the DHCP server. The ONT can dynamically distribute IP addresses to user terminals. ◆ Disable: The user terminals connected to the ONT cannot obtain the private network IP address using the DHCP.	
DHCP Start IP	The starting IP address of the IP address pool for the active DHCP server.	**Note: The IP address set here should be in the same network segment with the IP address set in LAN Settings; otherwise, the DHCP server will not operate normally.**
DHCP End IP	The ending IP address of the IP address pool for the DHCP server.	
DHCP Subnet Mask	The mask of the active DHCP server.	
DHCP Primary DNS	The IP address of the active DNS server.	
DHCP Secondary DNS	The IP address of the standby DNS server.	

Table 3-4 Parameters for the DHCP Server (Continued)

Item	Description	
DHCP Default Gateway	The default gateway of the active DHCP server.	
DHCP Lease Time	The lease time of the IP address pool of the DHCP server.	
Option60	Enables or disables the Option 60 property to identify the user terminal.	
Option 60 start IP	The starting IP address of the network segment distributed to the Option 60 property terminal by the DHCP server.	This item should be configured when the Option 60 field of the DHCP server is enabled.
Option 60 end IP	The ending IP address of the network segment distributed to the Option 60 property terminal by the DHCP server.	

3.3.4 Authentication Setting

Configure the parameters relevant to the ONT authentication mode, so that the ONT can pass the OLT authentication.

1. Select **Network** in the navigation bar and select **Authentication→OLT Authentication** in the left link bar to open the OLT authentication configuration page, as shown in Figure 3-10.

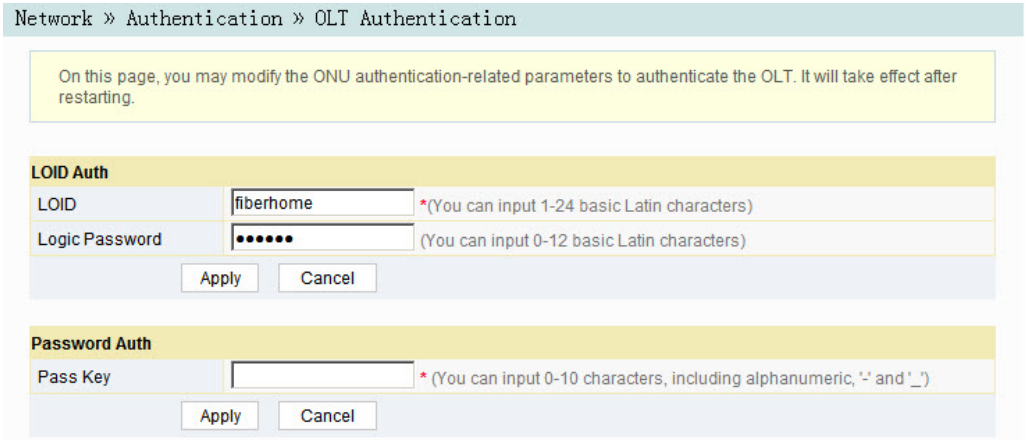


Figure 3-10 OLT Authentication

2. Configure the parameters as required. Table 3-5 describes the parameters.
3. Click **Apply** to save the configuration information. The configuration will take effect after the ONT is rebooted.

Table 3-5 Parameters for OLT Authentication

Item	Description	
LOID	Sets the LOID user name.	This item is configurable when the ONT uses the LOID authentication mode.
Logic Password	Sets the LOID password.	
Password Auth	Sets the authentication password when the ONT is authenticated by password.	

3.4 Security

The following introduces how to configure the firewall, remote control, dynamic DoS and HTTPS in the Web GUI.

3.4.1 Firewall

The firewall configuration includes

- Firewall Control
- IPv4 Filtering
- IPv6 Filtering
- URL Filtering
- DHCP Filtering
- Anti-port Scan
- MAC Filtering
- IPv6 MAC Filtering

3.4.1.1 Firewall Control

Enabling the firewall can prevent malicious access to the WAN port of the ONT.

1. Select **Security** in the navigation bar and select **Firewall→Firewall Control** in the left link bar to open the firewall enabling page, as shown in Figure 3-11.

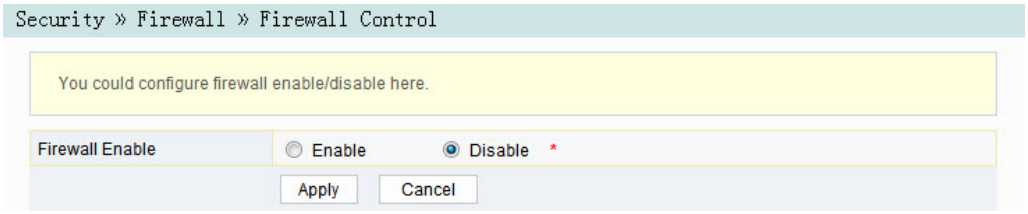


Figure 3-11 Firewall Enabling

2. Select to **Enable** or **Disable** the firewall as required.
3. Click **Apply** to save and apply the configuration.

3.4.1.2 IP Filtering

Allow or forbid the incoming or outgoing flow of the IP packets that comply with the filtering conditions. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→IPv4 Filtering** in the left link bar. Click **Add** to open the filtering rule list configuration page, as shown in Figure 3-12.

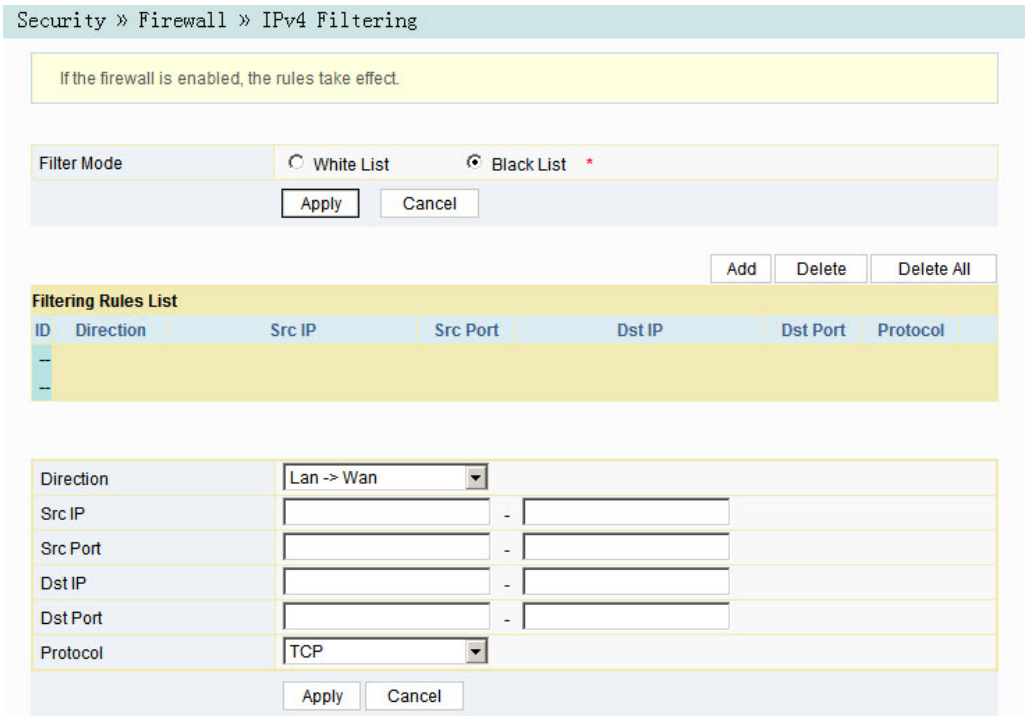


Figure 3-12 IPv4 Filtering

2. Configure the parameters relevant to filtering as required. Table 3-6 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-6 Parameters for IP Address Filtering

Item	Description	
Filter Mode	Select the filtering mode. ◆ Whitelist indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.	After the aforesaid operation, click the **Apply** button to validate the configuration.
Direction	Sets the direction of the filtering rule. ◆ LAN->WAN: uplink direction. ◆ WAN->LAN: downlink direction.	
Src IP	Enter the IP address at the LAN side if the direction is LAN->WAN. Enter the IP address at the WAN side if the direction is WAN->LAN.	
Src Port	The port range of the source IP address. This item is configurable when the **Protocol** is set to TCP or UDP.	
Dst IP	Enter the IP address at the WAN side if the direction is LAN->WAN. Enter the IP address at the LAN side if the direction is WAN->LAN.	
Dst Port	The port range of the destination IP address. This item is configurable when the **Protocol** is set to TCP or UDP.	
Protocol	Protocol type, including TCP, UDP, ICMP and ALL.	

3.4.1.3 IPv6 Filtering

Allow or forbid the IPv6 packets that comply with the filtering condition to be transmitted from the LAN or transmitted into MAN. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→IPv6 Filtering** in the left link bar. Then click **Add** to open the IPv6 filtering rule list configuration page, as shown in Figure 3-13.

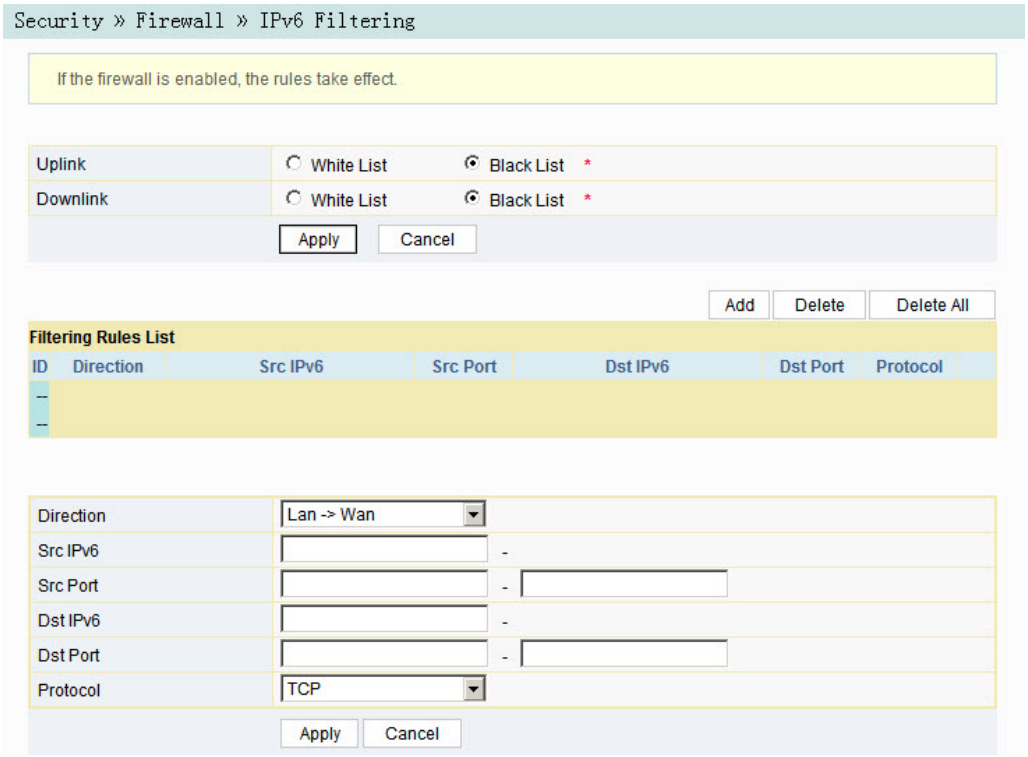


Figure 3-13 IPv6 Filtering

2. Configure the parameters relevant to filtering as required. Table 3-7 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-7 Parameters of IPv6 Filtering

Item	Description	
Uplink	Select the uplink filtering mode. ◆ Whitelist indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.	After the aforesaid operation, click the **Apply** button to validate the configuration.

Table 3-7 Parameters of IPv6 Filtering (Continued)

Item	Description
Downlink	Select the downlink filtering mode. ◆ Whitelist indicates that the data complying with the rules in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules in the filtering rule table will not be allowed to pass.
Direction	Sets the direction of the filtering rule. ◆ LAN->WAN: uplink direction. ◆ WAN->LAN: downlink direction.
Src IPv6	Enter the IPv6 address at the LAN side if the direction is set to LAN->WAN. Enter the IPv6 address at the WAN side if the direction is set to WAN->LAN.
Src Port	The port range of the source IP address. This item is configurable when the **Protocol** is set to TCP or UDP.
Dst IPv6	Enter the IPv6 address at the WAN side if the direction is set to LAN->WAN. Enter the IPv6 address at the LAN side if the direction is set to WAN->LAN.
Dst Port	The port range of the destination IP address. This item is configurable when the **Protocol** is set to TCP or UDP.
Protocol	Protocol type, including TCP, UDP, ICMP and ALL.

3.4.1.4 URL Filtering

By setting the URL filtering rules, users can forbid or allow all the data packets sent to or received from a certain IP address. After the fire wall is enabled, the pre-set URL filtering rule will take effect, and the domain names that meet the filtering conditions will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→URL Filtering** in the left link bar, and then click **Add** to open the URL filtering table configuration page, as shown in Figure 3-14.

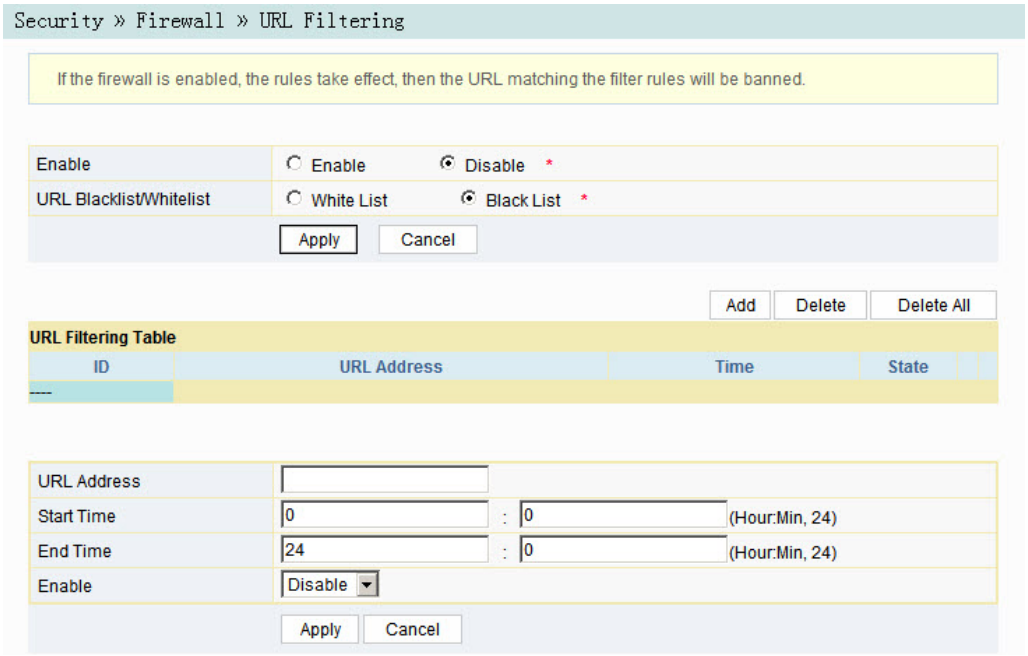


Figure 3-14 URL Filtering

2. Configure the parameters relevant to filtering as required. Table 3-8 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-8 Parameters for URL Filtering Parameters

Item	Description	
Enable	Enables or disables the URL filtering function.	After setting, click **Apply** below to take effect.
URL Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are configured globally, and cannot be enabled simultaneously. ◆ Whitelist indicates that the data complying with the rules defined in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules defined in the filtering rule table will not be allowed to pass.	
URL Address	The URL address accessed by users.	
Start Time	The starting time of the filtering rule.	
End Time	The ending time of the filtering rule.	
Enable	Enables or disables this filtering rule. The options include Disable and Enable.	

3.4.1.5 DHCP Filtering

Forbid or allow the user device configured with the MAC address to obtain an IP address in the DHCP mode to prevent DOS attacks. After the firewall is enabled, the pre-set rules will take effect.

1. Select **Security** in the navigation bar and select **Firewall→DHCP Filtering** in the left link bar. Then click **Add** to open the DHCP Filtering Table configuration page, as shown in Figure 3-15.

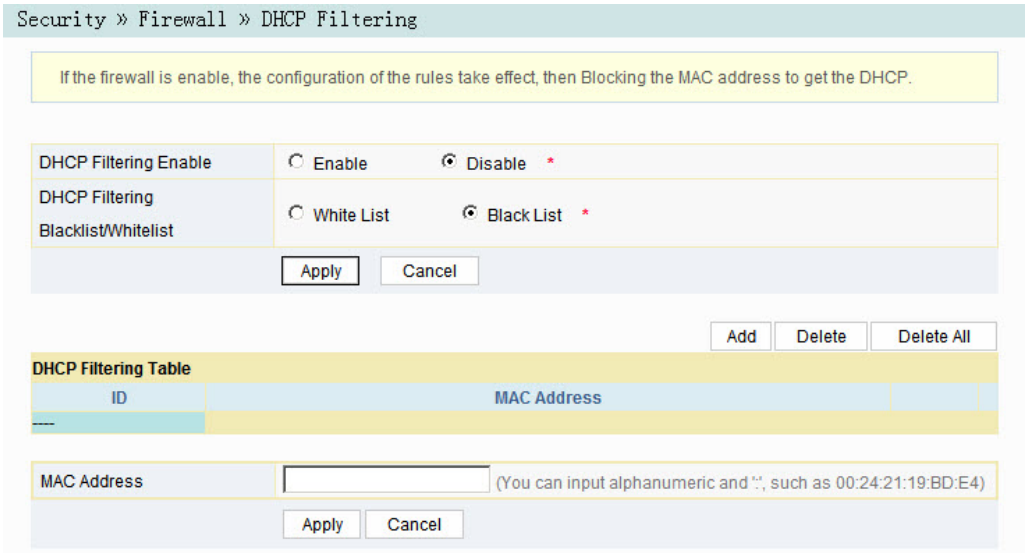


Figure 3-15 DHCP Filtering

2. Configure the parameters relevant to filtering as required. Table 3-9 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 3-9 Parameters for DHCP Filtering

Item	Description	
DHCP Filtering Enable	Enables or disables the DHCP filtering.	After setting, click **Apply** below to take effect.

Table 3-9 Parameters for DHCP Filtering (Continued)

Item	Description	
DHCP Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are global configuration, which cannot be enabled simultaneously. ◆ Whitelist indicates allowing the device configured with the MAC address to obtain the IP address using the DHCP. ◆ Blacklist indicates forbidding the device configured with the MAC address to obtain the IP address using the DHCP.	
MAC Address	The MAC address of the user device subject to the DHCP filtering rule.	

3.4.1.6 Anti-port Scan

Enable or disable the anti-port scan function.

1. Select **Security** in the navigation bar and select **Firewall→Anti Port Scan** in the left link bar to open the anti-port scan page, as shown in Figure 3-16.

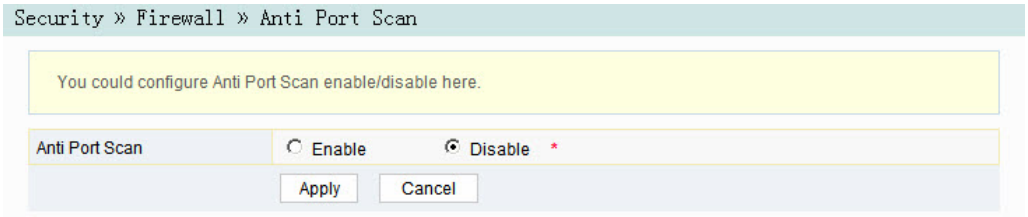


Figure 3-16 Anti-port Scan

2. Select to **Enable** or **Disable** the anti-port scan function as required.
3. Click **Apply** to save and apply the configuration.

3.4.1.7 MAC Address Filtering

One user device may have multiple IP addresses but only one MAC address. The user device access authority in the LAN can be controlled effectively by setting the MAC address filtering. After the fire wall is enabled, the pre-set rules will take effect, and the MAC addresses that meet the filtering conditions will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→MAC Filtering** in the left link bar, and then click **Add** to open the MAC address filtering table configuration page, as shown in Figure 3-17.

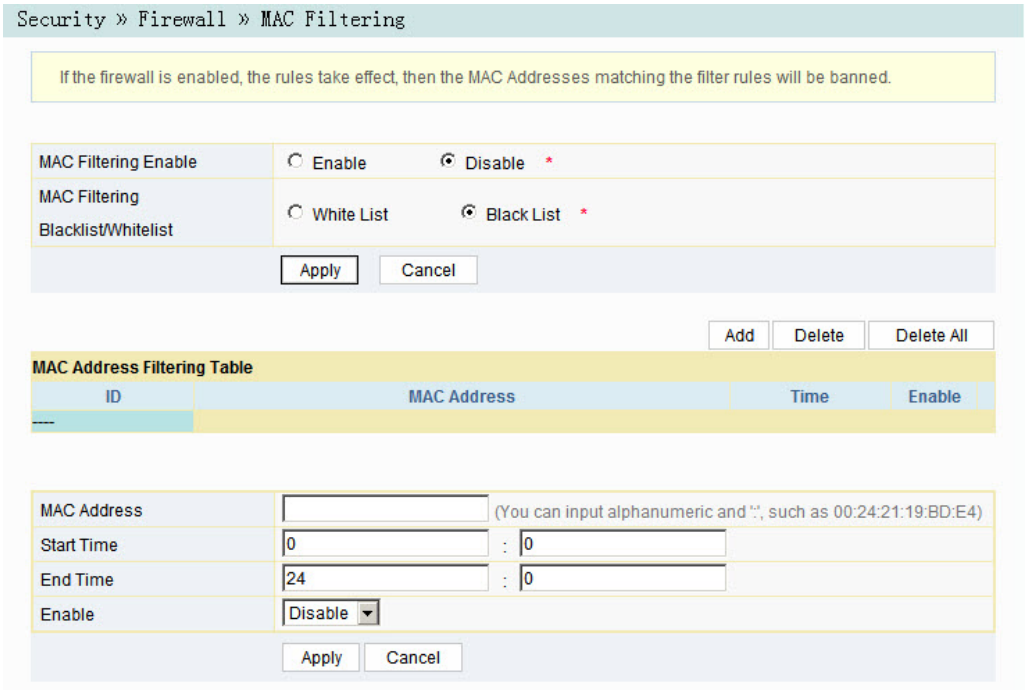


Figure 3-17 MAC Filtering

2. Configure parameters relevant to filtering as required. Table 3-10 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-10 Parameters for MAC Address Filtering

Item	Description	
MAC Filtering Enable	Enables or disables the MAC address filtering function.	After setting, click **Apply** below to take effect.
MAC Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are global configuration, which cannot be enabled simultaneously. ◆ Whitelist indicates that the data complying with the rules defined in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules defined in the filtering rule table will not be allowed to pass.	
MAC Address	The MAC address in the MAC address filtering rule.	

Table 3-10 Parameters for MAC Address Filtering (Continued)

Item	Description
Start Time	The starting time of the filtering rule.
End Time	The ending time of the filtering rule.
Enable	Enables or disables this filtering rule. The options include Disable and Enable.

3.4.1.8 IPv6 Mac Filtering

One user device may have multiple IPv6 addresses but only one MAC address. The user device access authority in the LAN can be controlled effectively by setting the MAC address filtering. After the fire wall is enabled, the pre-set rules will take effect, and the MAC addresses that meet the filtering conditions will be filtered.

1. Select **Security** in the navigation bar and select **Firewall→IPv6 MAC Filtering** in the left link bar, and then click **Add** to open the page for configuring the MAC address filtering table, as shown in Figure 3-18.

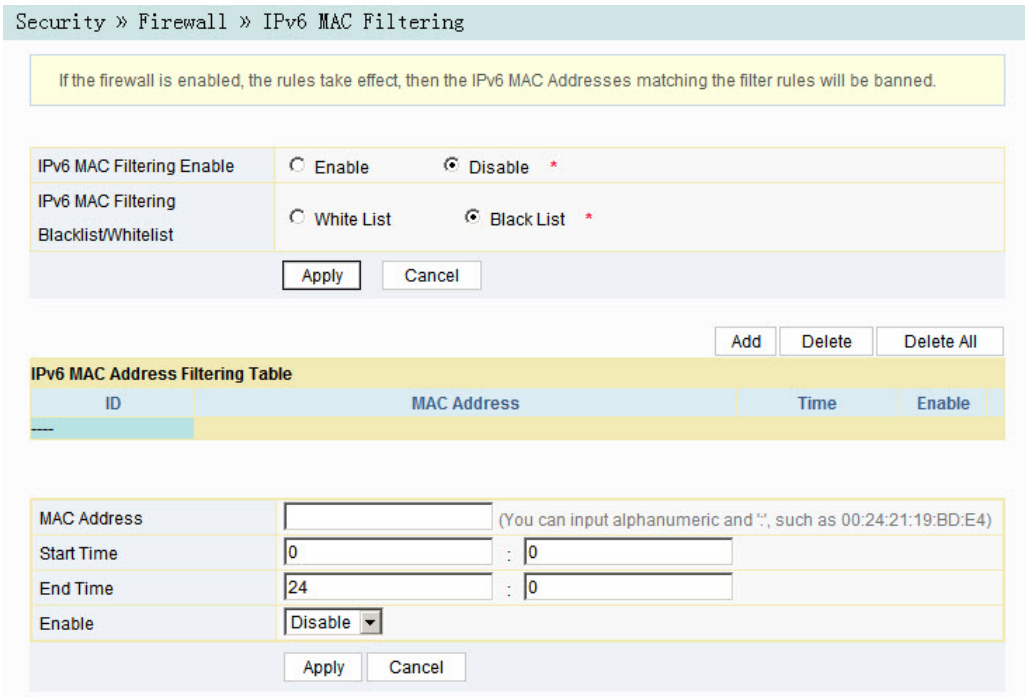


Figure 3-18 IPv6 Mac Filtering

2. Configure the parameters relevant to filtering as required. Table 3-11 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-11 Parameters for IPv6 MAC Address Filtering

Item	Description	
MAC Filtering Enable	Enables or disables the MAC address filtering function.	After setting, click **Apply** below to take effect.
MAC Filtering Blacklist / Whitelist	Select the filtering mode. The white list and black list modes are global configuration, which cannot be enabled simultaneously. ◆ Whitelist indicates that the data complying with the rules defined in the filtering rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules defined in the filtering rule table will not be allowed to pass.	
MAC Address	The MAC address in the MAC address filtering rule.	
Start Time	The starting time of the filtering rule.	
End Time	The ending time of the filtering rule.	
Enable	Enables or disables this filtering rule. The options include Disable and Enable.	

3.4.2 Remote Control

Enable or disable the remote access control. If the remote control is disabled, the PCs in the Internet cannot access the Web GUI of the ONT using the IP addresses at the WAN side; if enabled, the PCs in the Internet can access the Web GUI.

1. Select **Security** in the navigation bar and select **Remote Control→Remote Control** in the left link bar to open the remote control configuration page, as shown in Figure 3-19.

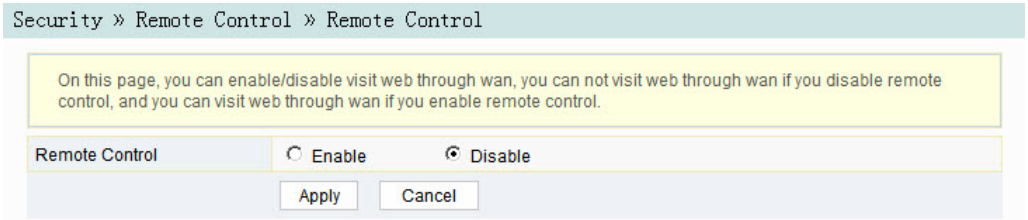


Figure 3-19 Remote Control

2. **Enable** or **Disable** the remote access control as required.

3. Click **Apply** to save and apply the configuration.

3.4.3 Dynamic DoS

The DoS attack exhausts the resource of target computer using massive virtual information flow, so that the attacked computer has to handle the virtual information with all strength, which influences the handling of normal information flow. The ONT provides the protection against the DoS attack.

1. Select **Security** in the navigation bar and select **DDOS→DDOS** in the left link bar to open the anti-DoS attack configuration page, as shown in Figure 3-20.

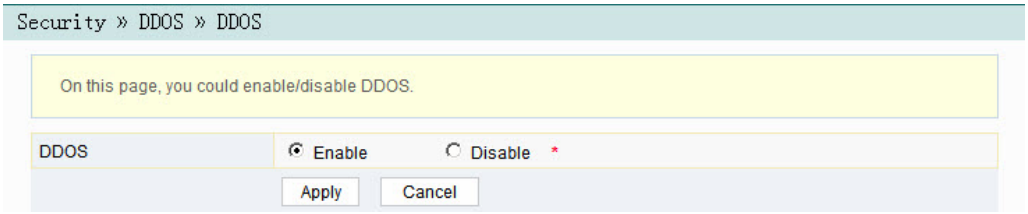


Figure 3-20 Dynamic DoS

2. Select to **Enable** or **Disable** the anti-dos attack function as required.
3. Click **Apply** to save and apply the configuration.

3.4.4 HTTPS

The ONT provides the HTTPS function. The HTTPS is the HTTP channel for security. It is built on the SSL+HTTP protocol, which can perform encryption transmission and identity authentication.

1. Select **Security** in the navigation bar and select **HTTPS→HTTPS** in the left link bar to open the HTTPS function configuration page, as shown in Figure 3-21.

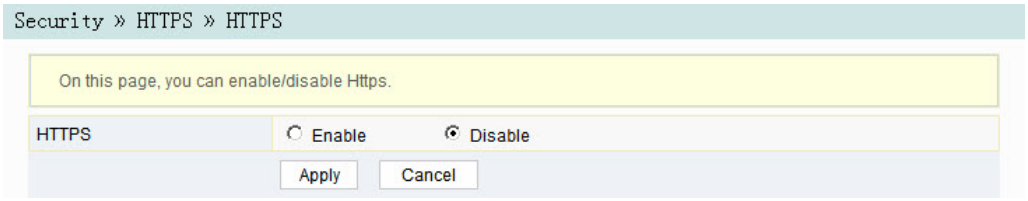


Figure 3-21 HTTPS

2. Select to **Enable** or **Disable** the HTTPS function as required.

Caution:

After enabling the HTTPS function, log into the Web GUI. The protocol type in URL should be https and the management IP address should be added with the port number 4433, e.g. **https://192.168.1.1:4433**.

3. Click **Apply** to save and apply the configuration.

3.5 Application

The following introduces how to configure the DDNS, port forwarding, NAT, UPnP, DMZ and network diagnosis in the Web GUI.

3.5.1 DDNS

The DDNS server transforms the dynamic IP address at the WAN side of the ONT into a static domain name. Users from Internet can easily access the gateway using this domain name.

1. Select **Application** in the navigation bar and select **DDNS→DDNS Settings** in the left link bar to open the DDNS configuration page, as shown in Figure 3-22.

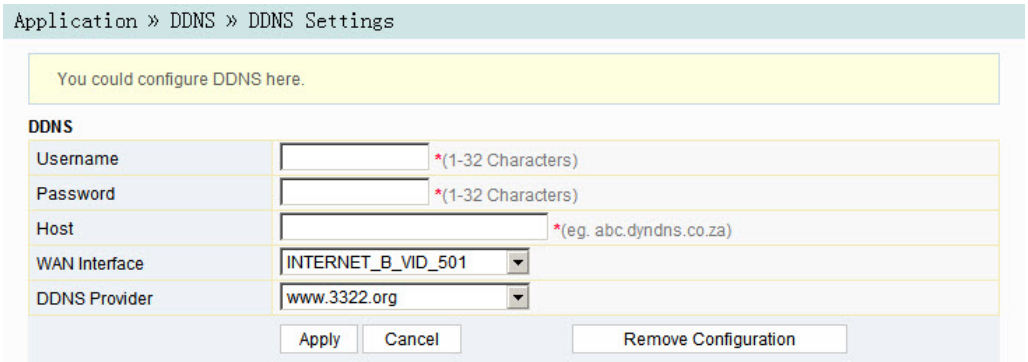


Figure 3-22 DDNS Settings

2. Configure parameters relevant to DDNS according to the requirement. Table 3-12 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-12 Parameters for DDNS Settings

Item	Description
Username	The username allocated by the DDNS provider.
Password	The password allocated by the DDNS provider.
Host	The domain name allocated by the DDNS provider.
WAN Interface	Name of the created WAN connection.
DDNS Provider	The DDNS service provider. Users can select the preset DDNS provider or select **Other** to customize the provider and set the domain name, server IP address, protocol type and URL.

3.5.2 Port Forwarding

The port forwarding can create the mapping between the WAN port IP address / common port number and the LAN server IP address / private port number. In this way, all the accesses to a certain service port at this WAN port will be re-directed to the corresponding port of the server in the designated LAN.

1. Select **Application** in the navigation bar and select **Port Forwarding→Port Forwarding** in the left link bar. Click **Add** to open the port forwarding configuration page, as shown in Figure 3-23.

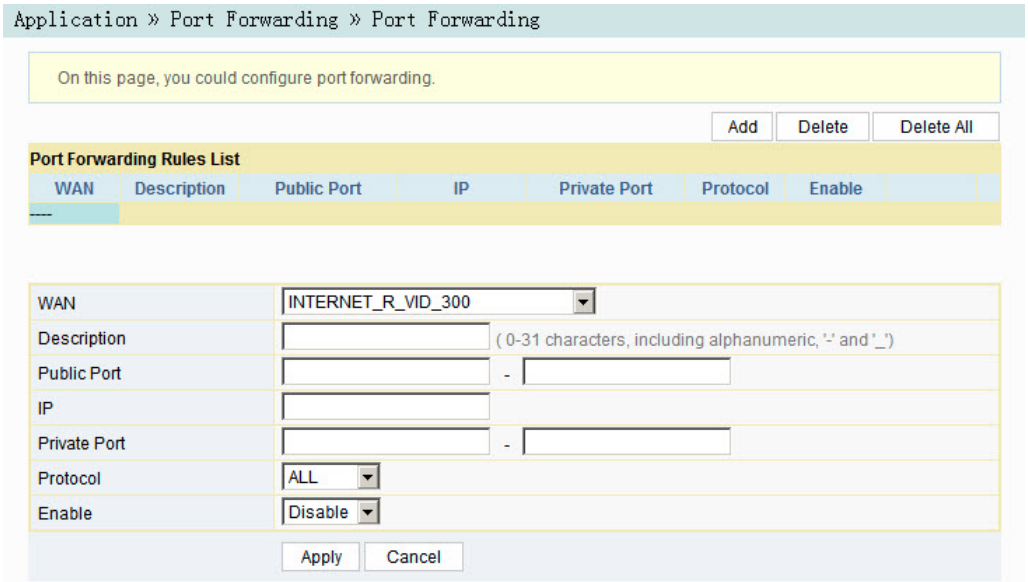


Figure 3-23 Port Forwarding

2. Configure parameters relevant to port forwarding according to the requirement. Table 3-13 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-13 Parameters for Port Forwarding

Item	Description
WAN	The corresponding WAN connection bound with the port forwarding rule.
Description	The port forwarding rule name.
Public Port	The range of ports for Extranet data packets. If only one port exists, enter the same port number.
IP	The IP address of the LAN virtual server for port forwarding.
Private Port	The range of the LAN port for port forwarding. If only one port exists, enter the same port number.
Protocol	The protocol used for the port to forward data packets, including ALL, TCP and UDP.
Enable	Enables or disables the rule.

3.5.3 NAT

NAT allows the conversion between intranet IP addresses and public network IP addresses. NAT converts a great number of intranet IP addresses into one or a small number of public network IP addresses, so as to save the resource of public network IP addresses.

The NAT configuration below can take effect only when the NAT function is enabled in **Network→BroadBand Settings→Internet Settings**.

1. Select **Application** in the navigation bar and select **NAT→NAT** in the left link bar. Click **Add** to open the NAT rule list configuration page, as shown in Figure 3-24.

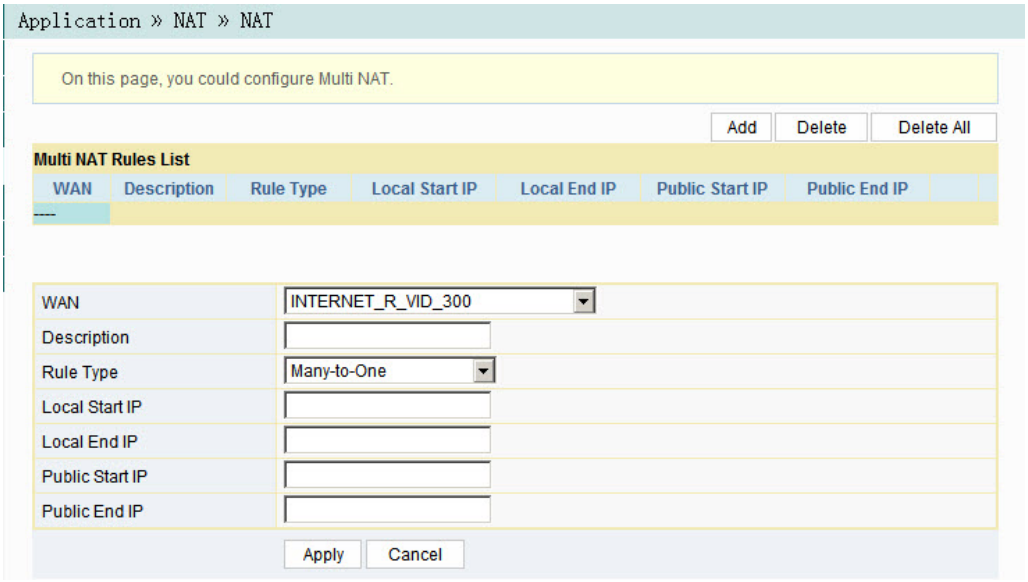


Figure 3-24 NAT

2. Configure relevant parameters according to the requirement. Table 3-14 describes the parameters.

3. Click **Apply** to save and apply the configuration.

Table 3-14 Parameters for NAT Configuration

Item	Description
WAN	The corresponding WAN connection bound with the NAT rule.
Description	NAT rule name.
Rule Type	Select the NAT conversion mode. It is advisable to select One-to-One or Many-to-One.
Locate Start IP	The starting IP address of intranet.
Locate End IP	The ending IP address of intranet.
Public Start IP	The starting IP address of the public network.
Public End IP	The ending IP address of the public network.

3.5.4 UPnP

The UPnP supports the plug and play function and the automatic discovery function of multiple network devices. When UPnP is enabled, the devices that supports UPnP can be added into the network dynamically. In this way, an external computer can access the resource on the internal computer when necessary. For example, when some application software are running on a PC, the port mapping table will be generated on the ONT automatically using the UPnP protocol, so that the operation can be sped up.

1. Select **Application** in the navigation bar and select **UPNP→UPNP** in the left link bar to open the UPnP configuration page, as shown in Figure 3-25.

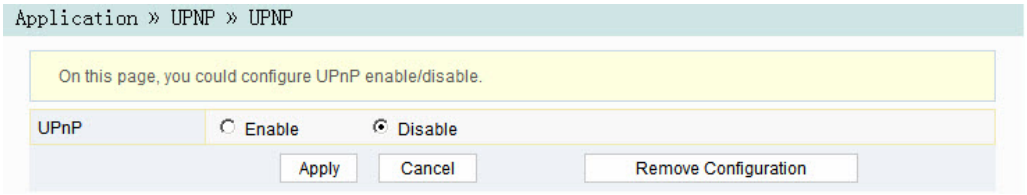


Figure 3-25 UPnP

2. Select to **Enable** or **Disable** the UPnP function as required.
3. Click **Apply** to save and apply the configuration.

3.5.5 DMZ

When the ONT is working in the routing mode, users should enable the DMZ function if a host at the WAN side needs to access a certain host at the LAN side. The ONT will forward all the IP packets from the WAN to the designated DMZ host.

1. Select **Application** in the navigation bar and select **DMZ→DMZ** in the left link bar to open the DMZ configuration page, as shown in Figure 3-26.

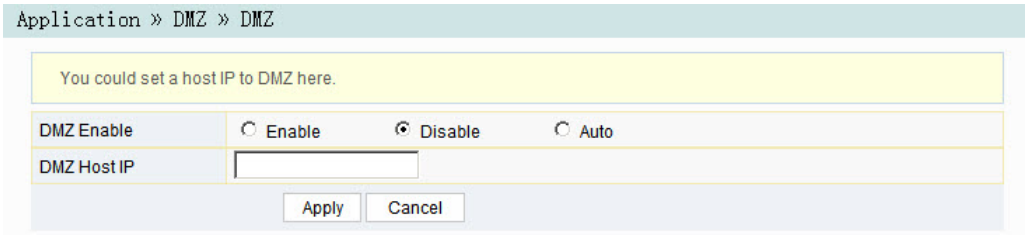


Figure 3-26 DMZ

2. Configure relevant parameters according to the requirement. Table 3-15 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 3-15 Parameters for DMZ Configuration

Item	Description
DMZ Enable	Enables or disables the DMZ function. The options include Enable, Disable and Auto. If Enable is selected, the DMZ host IP address should be set. If Auto is selected, the DMZ host uses the first IP address allocated by DHCP.
DMZ Host IP	The host IP address of the DMZ.

3.5.6 Network Diagnosis

Network diagnosis includes network diagnosis and Nat conversation.

3.5.6.1 Network Diagnosis

The ONT provides two network diagnosis tools.

- Ping test: Test whether the router is normally connected with the target host or another device.
- Traceroute test: Check the routing condition from the router to the target host.

1. Select **Application** in the navigation bar and select **Diagnosis→Diagnosis** in the left link bar to open the network diagnosis page, as shown in Figure 3-27.

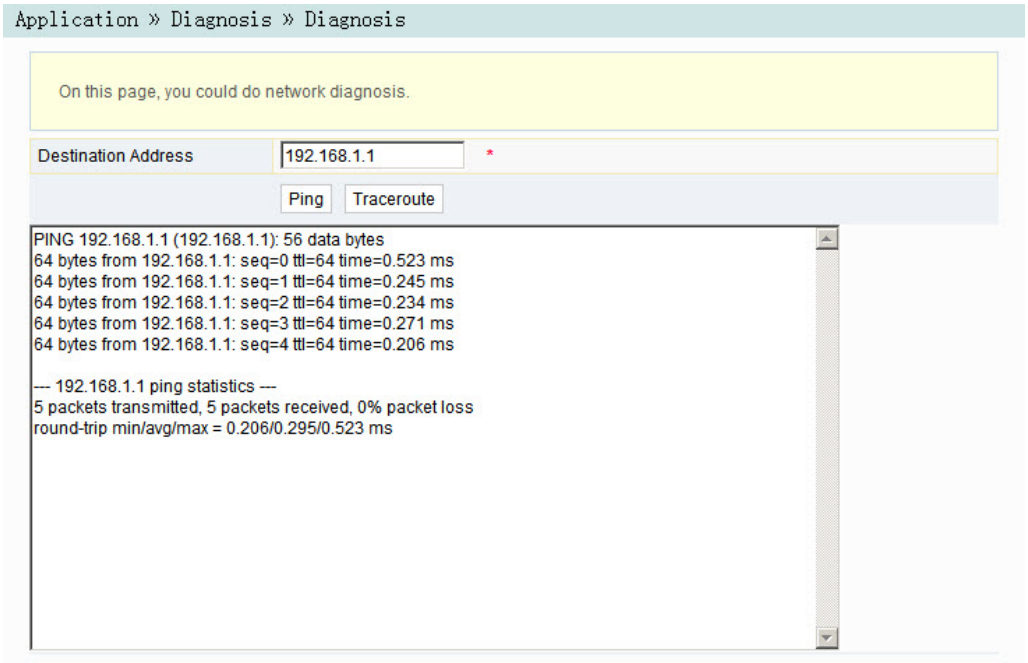


Figure 3-27 Network Diagnosis

2. Enter the destination IP address to be tested in the **Destination Address** box, and click **Ping** or **Traceroute** to test. The test result will be displayed in the lower text box.

3.5.6.2 Nat Session

Click **Application** and select **Diagnosis→Nat Session** at the left side to open the Nat session page and query the mappings between the inner / outer network IP address of NAT and the ports, as shown in Figure 3-28.

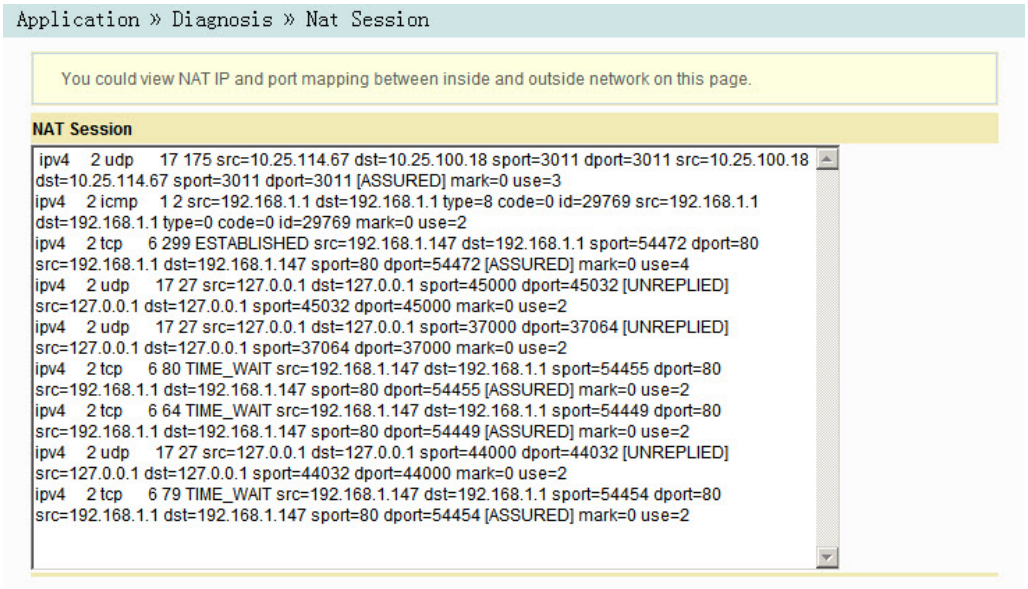


Figure 3-28 Nat Session

3.6 Management

The following introduces how to perform account management, device management and log management in the Web GUI.

3.6.1 Account Management

Account management includes user account management and maintenance account management.

3.6.1.1 User Account Management

Users can add or delete a common user account or modify the password of a common user account.

1. Select **Management** in the navigation bar. Select **Account Management→ User Account** from the left link bar to open the user account management page, as shown in Figure 3-29.

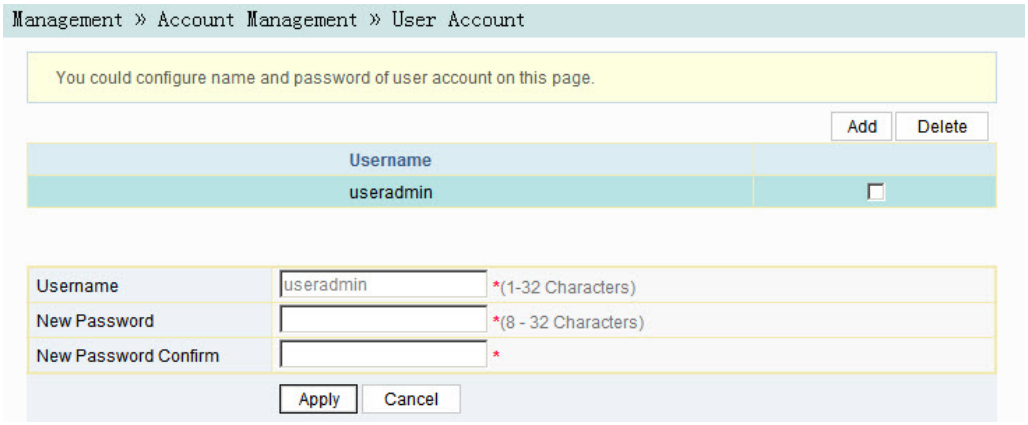


Figure 3-29 User Account Management

2. Add or delete a common user account or modify the password of a common user account as required.
3. Click **Apply** to save and apply the configuration.

3.6.1.2 Maintenance Account Management

Users can modify the username and password of the current account.

1. Select **Management** in the navigation bar. Select **Account Management→ Maintenance Account** from the left link bar to open the maintenance account management page, as shown in Figure 3-30.

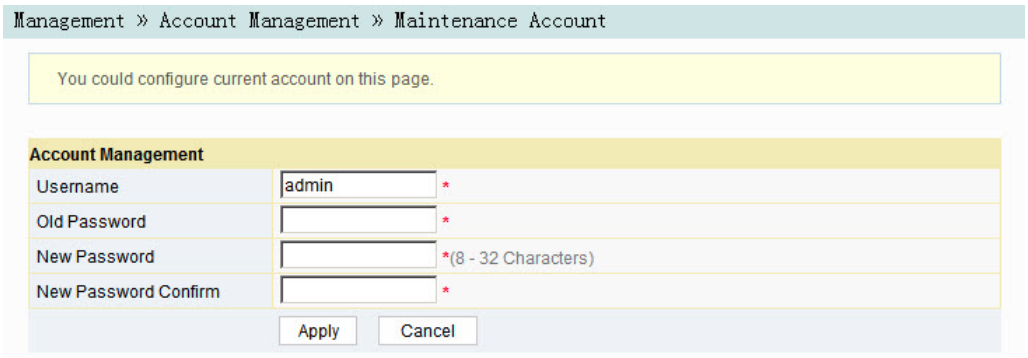


Figure 3-30 Maintenance Account Management

2. Modify the username and password of the current account as required.
3. Click **Apply** to save and apply the configuration.

3.6.2 Device Management

The ONT provides multiple device management functions such as restoring some of the configuration data, restoring all configuration data, local upgrade, configuration backup, device reboot, and NTP time calibration.

3.6.2.1 Restoring the Configuration Data

Restore factory settings of the ONT, including user name and password for Web login, SSID and password for wireless network, etc.

1. Select **Management** in the navigation bar. Select **Device Management→ Restore** from the left link bar to open the configuration restoring page, as shown in Figure 3-31.

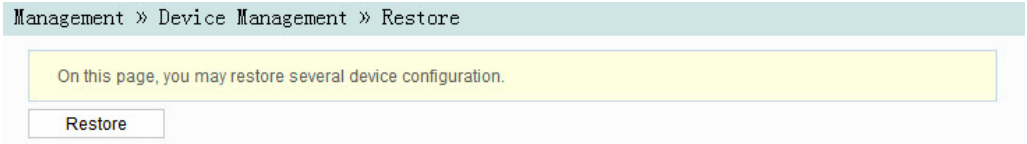


Figure 3-31 Restoring the Configuration Data

2. Click **Restore** and then click **OK** in the alert box that appears. Wait until the configuration data are completely restored.

3.6.2.2 Restoring All the Configuration

Restore all the configuration data of the ONT to factory settings.

1. Select **Management** in the link bar and select **Device Management→Restore All** on the left side to open the configuration restoration page, as shown in Figure 3-32.

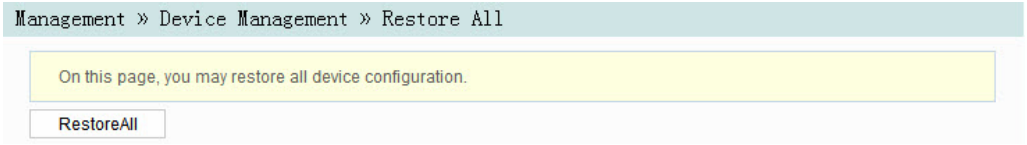


Figure 3-32 Restoring All the Configuration

2. Click **Restore All** and then click **OK** in the alert box that appears. Wait until the configuration data are completely restored.

3.6.2.3 Local Upgrade

Select the local file and upgrade the ONT software. During upgrade, do not power off the device or perform other operations to prevent damage to the device.

1. Select **Management** in the navigation bar. Select **Device Management→ Local Upgrade** from the left link bar to open the local upgrade page, as shown in Figure 3-33.

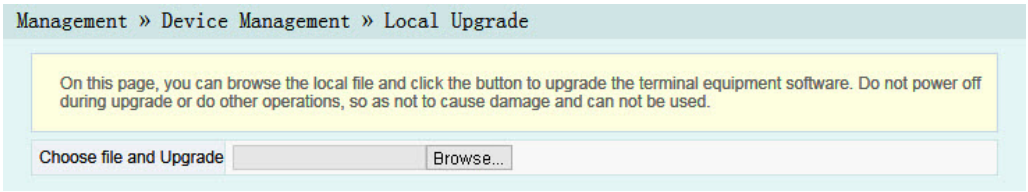


Figure 3-33 Local Upgrade

2. Click **Browse**. In the dialog box that appears, select the device software version to be upgraded and click **Open** to upgrade the ONT software version.
3. When the upgrade succeeds, the page will prompt for device rebooting. Click "Reboot". After rebooting, the device will be upgraded to the new version.

Note:

After the upgrade, users can view the **Software Version** in the device information page to check whether the current version is correct.

3.6.2.4 Configuration Backup

Back up and save the ONT configuration files for restoring the configuration data later on. Before backup, enable the FTP tool in the computer.

1. Select **Management** in the navigation bar. Select **Device Management→ Config Backup** from the left link bar to open the configuration backup page, as shown in Figure 3-34.

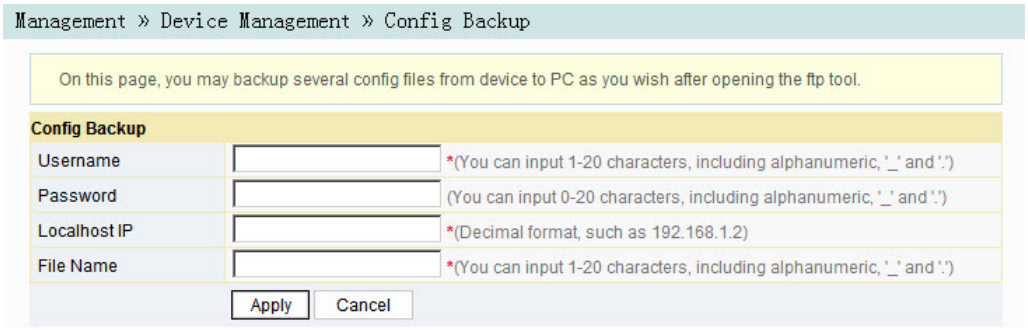


Figure 3-34 Configuration Backup

2. Configure parameters relevant to file backup. Table 3-16 describes the parameters.

3. Click **Apply** to save the configuration backup file.

Table 3-16 Parameters for Configuration Backup

Item	Description
Username	The FTP username.
Password	The FTP password.
Localhost IP	Local IP address.
File name	The existing file name in the ONT.

3.6.2.5 Device Reboot

1. Select **Management** in the navigation bar. Select **Device Management→ Device Reboot** from the left link bar to open the device reboot page, as shown in Figure 3-35.

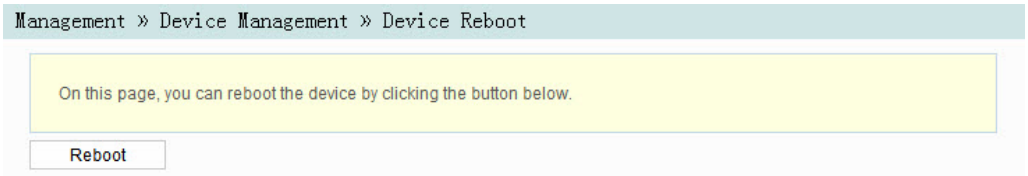


Figure 3-35 Device Reboot

2. Click **Reboot** and click **OK** in the alert box that appears and wait for the device to reboot.

Caution:

Save the configuring data before rebooting the device to prevent loss of the configuration data.

After the device is rebooted, you need to wait for about two minutes to re-log into the Web GUI of the device.

3.6.2.6 NTP Time Calibration

Users can obtain the precise time by connecting the ONT to a NTP server.

1. Select **Management** in the navigation bar. Select **Device Management→NTP Check Time** from the left link bar to open the NTP check time page, as shown in Figure 3-36.

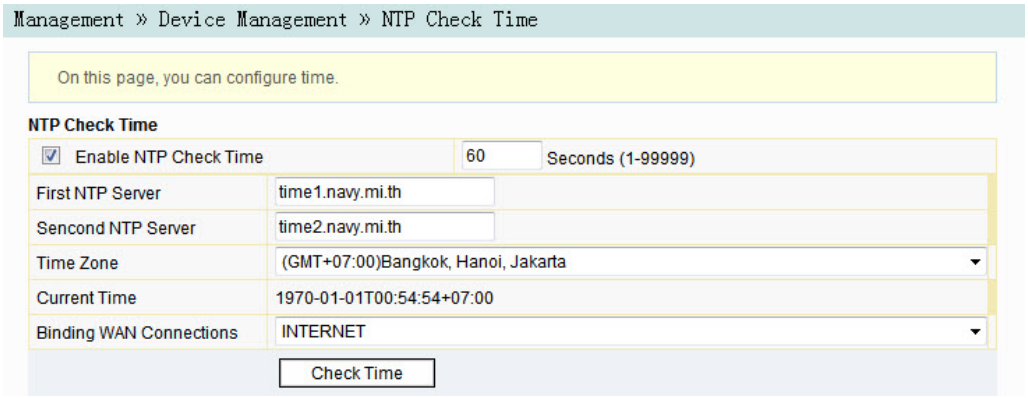


Figure 3-36 NTP Time Calibration

2. Configure parameters relevant to the NTP time calibration. Table 3-17 describes the parameters.
3. Click **Check Time** to save and apply the configuration.

Table 3-17 Parameters for NTP Time Calibration

Item	Description
Enable NTP Check Time	Select whether to enable the NTP time calibration function.
seconds	Sets the time interval for synchronization with the time server.
First NTP Server	Enter the IP address of the active NTP server.

Table 3-17 Parameters for NTP Time Calibration (Continued)

Item	Description
Second NTP Server	Enter the IP address of the standby NTP server.
Time Zone	Select the time zone according to the location of the device.
Current Time	When NTP Check Time is enabled, time will be calibrated according to the equipment location, and the local time will be displayed. When NTP Check Time is disabled, the system initial time (1970-01-01) or the previous calibrated time will be displayed.
Binding WAN Connections	Select the WAN connection type for time calibration.

3.6.3 Log Management

The Log files record key operations and actions on the ONT. Users can view the information saved in log as needed.

Select **Management** in the navigation bar. Select **Log→Log** from the left link bar to open the log information page, as shown in Figure 3-37.

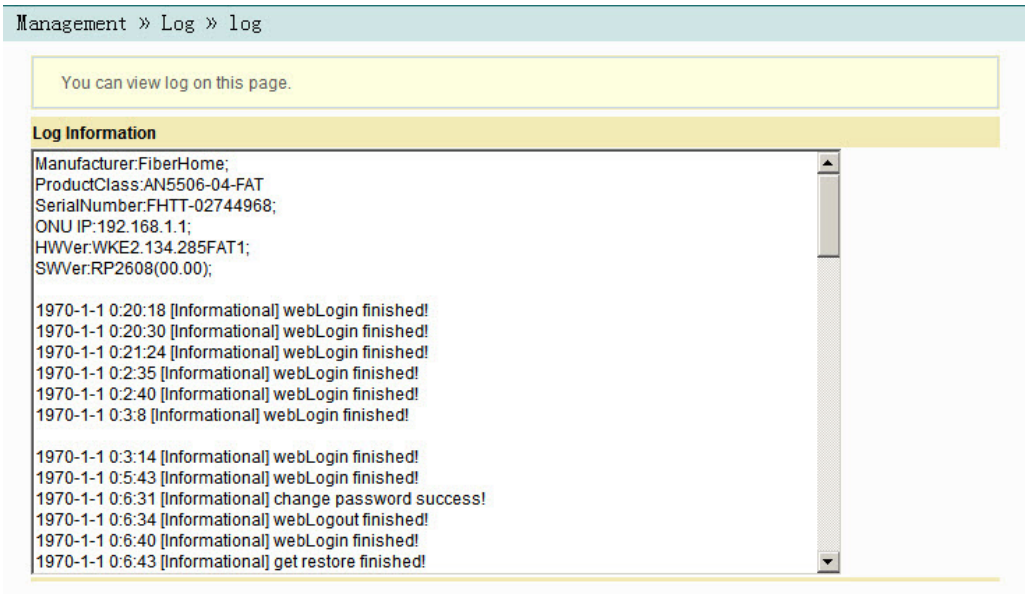


Figure 3-37 Log

4 Handling Common Problems

The following introduces how to handle common problems encountered in equipment operation and service test.

- ☑ Power Status Indicator LED Extinguished
- ☑ Register Status Indicator LED Extinguished
- ☑ Optical Signal Status Indicator LED Blinking
- ☑ Ethernet Interface Status Indicator LED Extinguished
- ☑ Failing to Access Local Web Login GUI and Failing to Ping 192.168.1.1
- ☑ Failing to Access Internet Using the LAN Port
- ☑ Measured Internet Access Rate Lower or Higher Than The Standard Value

4.1 Power Status Indicator LED Extinguished

Handle the problem according to the procedures below:

1. Check whether the mains supply is normal.
2. Check whether the power adapter matches the device.
3. Check whether the power button is pressed down.
4. Check whether the power cable connection is normal.

4.2 Register Status Indicator LED Extinguished

Handle the problem according to the procedures below:

1. Check whether the device power supply is normal.
2. Check whether the optical fiber connection is normal.
3. Check whether the ONT has obtained the ISP authorization.
4. Check whether the optical interface is normal; if not, replace the device.

4.3 Optical Signal Status Indicator LED Blinking

Handle the problem according to the procedures below:

1. Check whether the optical fiber is damaged.
2. Check whether the optical fiber is connected to the correct interface.
3. Check whether the Rx optical power of the ONT (measured with the optical power meter) is below specifications.
4. Check whether the ONT optical module is aged or damaged.
5. Check whether the local device is faulty.

4.4 Ethernet Interface Status Indicator LED Extinguished

Handle the problem according to the procedures below:

1. Check whether the network cable is damaged or connected incorrectly.
2. Check whether the color-coding scheme of the network cable is incorrect; if so, replace it with a standard CAT-5 twisted pair network cable.
3. Check whether the network cable length exceeds the allowed range (100m).

4.5 Failing to Access Local Web Login GUI and Failing to Ping 192.168.1.1

Handle the problem according to the procedures below:

1. Check whether the LAN port indicator LED is ON; if not, replace the network cable.
2. Check whether the computer is set with a fixed IP address in the network segment of 192.168.1.x.

4.6 Failing to Access Internet Using the LAN Port

Handle the problem according to the procedures below:

1. Check whether the computer is set with a fixed IP address. If yes, modify the configuration so that the computer can obtain an IP address automatically. Then retry the connection.
2. If the computer is obtaining IP addresses automatically, check whether the computer has obtained an IP address in the network segment of 192.168.x.x.
3. Contact the personnel in the network management center to check whether the WAN is connected correctly and bound with the LAN port.

4.7 Measured Internet Access Rate Lower or Higher Than The Standard Value

Contact the personnel in the network management center to check whether the bandwidth profile is configured correctly and bound to the ONT.

5 Standards and Protocols

Classification	Standard Number	Title
GPON	ITU-T G.984.1	Gigabit-capable passive optical networks (GPON): General characteristics
	ITU-T G.984.2	Gigabit-capable Passive Optical Networks (GPON): Physical Media Dependent (PMD) layer specification
	ITU-T G.984.3	Gigabit-capable Passive Optical Networks (G-PON): Transmission convergence layer specification
	ITU-T G.984.4	Gigabit-capable passive optical networks (G-PON): ONT management and control interface specification
Ethernet	IEEE 802-2001	IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture
	IEEE 802.1D-2004	IEEE Standard for Local and metropolitan area networks: Media Access Control (MAC) Bridges
	IEEE 802.1Q-2005	IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges
	IEEE 802.1ad	IEEE Standard for Local and Metropolitan Area Networks - Virtual Bridged Local Area Networks - Amendment 4: Provider Bridges
	IEEE 802.1x-2004	IEEE Standard for Local and Metropolitan Area Networks Port- Based Network Access Control
	IEEE 802.1ag-2007	IEEE Standard for Local and Metropolitan Area Networks Virtual Bridged Local Area Networks Amendment 5: Connectivity Fault Management
	IEEE 802.3-2005	IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 3: Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications
	IEEE 802.3z	Gigabit Ethernet Standard
	IEEE 802.1p	Traffic class expediting and dynamic multicast filtering. Describes important methods for providing QoS at MAC level
	TR-101	Migration to Ethernet-Based Broadband Aggregation
	TR-143	Enabling Network Throughput Performance Tests and Statistical Monitoring
VoIP	ITU-T G.711	Pulse code modulation (PCM) of voice frequencies
	ITU-T G.711.1	Wideband embedded extension for G.711 pulse code modulation
	ITU-T G.722	7 kHz audio-coding within 64 kbit/s

Classification	Standard Number	Title
	ITU-T G.723.1	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s
	ITU-T G.729	Coding of speech at 8 kbit/s using conjugate-structure algebraic-code-excited linear prediction (CS-ACELP)
	ITU-T G.729.1	G.729 based Embedded Variable bit-rate coder: An 8-32 kbit/s scalable wideband coder bitstream interoperable with G.729
	ITU-T G.165	Echo Cancellers
	ITU-T G.168	Digital network echo cancellers
Multicast	IETF RFC 2236	Internet Group Management Protocol, Version 2
	IETF RFC 3376	Internet Group Management Protocol, Version 3
	IETF RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
Time	IETF RFC 1305	Network Time Protocol (Version 3) Specification, Implementation and Analysis
	IETF RFC 2030	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
EMC	EN 300 386	Electromagnetic compatibility and Radio spectrum Matters (ERM); Telecommunication network equipment; Electromagnetic Compatibility (EMC) requirements
	CISPR 22 (EN55022)	Information technology equipment - Radio disturbance characteristics - Limits and methods of measurement
	CISPR 24 (EN55024)	Information technology equipment - Immunity characteristics - Limits and methods of measurement
Other	TR-069	CPE WAN Management Protocol

Appendix A Abbreviations

ONT	Optical Network Terminal
FTTH	Fiber To The Home
GPON	Gigabit-capable Passive Optical Network
ODN	Optical Distribution Network
OLT	Optical Line Termination
DBA	Dynamic Bandwidth Allocation
XML	Extensible Markup Language
GEM	GPON Encapsulation Mode
ATM	Asynchronous Transfer Mode
OAM	Operation, Administration And Maintenance
FEC	Forward Error Correction
TDMA	Time Division Multiple Access
PLOAM	Physical Layer Operations, Administration and Maintenance
OMCI	ONU Management and Control Interface
T-CONT	Transmission Container
NSR	Network Security Recorder
AES	Advanced Encryption Standard
MAC	Medium Access Control
IGMP	Internet Group Management Protocol
VLAN	Virtual Local Area Network
QoS	Quality of Service
ACL	Access Control List
WRR	Weighted Round Robin
DHCP	Dynamic Host Configuration Protocol
PPPoE	Point to Point Protocol over Ethernet
NAT	Network Address Translation
DMZ	Demilitarized Zone

ARP	Address Resolution Protocol
UPnP	Universal Plug and Play
DoS	Denial of Service
DDoS	Distributed Denial of Service
URL	Uniform Resource Locator
HTTPS	Hyper Text Transfer Protocol over Secure Socket Layer
CATV	Cable Antenna Television
CoS	Class of Service
SIP	Session Initiation Protocol
VoIP	Voice over Internet Protocol
RTP	Real-time Transport Protocol
IGD_WLAN_SSID	Service Set Identifier
WAN	Wide Area Network
LAN	Local Area Network
WLAN	Wireless Local Area Networks
MTU	Maximum Transmission Unit
PPPoE	Point to Point Protocol over Ethernet
DTMF	Dual Tone Multi Frequency
VPN	Virtual Private Network
DDNS	Dynamic Domain Name Server
FTP	File Transfer Protocol
ADSL	Asymmetric Digital Subscriber Line
BRAS	Broadband Remote Access Server
BSC	Base Station Controller
CDR	Call Detail Record
CPE	Customer Premise Equipment
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
EFM	Ethernet in the First Mile
EMC	Electro Magnetic Compatibility
EPON	Ethernet Passive Optical Network
EPRS	Ethernet Ring Protection Switching

FDB	Forwarding Database
FoIP	Fax over IP
FTTA	Fiber To The Antenna
FTTB	Fiber To The Building
FTTC	Fiber To The Curb
FTTDp	Fiber To The Distribution Point
FTTM	Fiber To The Mobile
FTTO	Fiber To The Office
GUI	Graphical User Interface
HG	Home Gateway
ISDN	Integrated Services Digital Network
ICMP	Internet Control Message Protocol
IMS	IP Multimedia Subsystem
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
MDU	Multi-Dwelling Unit
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MLD	Multicast Listener Discover
MoIP	Modem over IP
MTBF	Mean Time Between Failure
MSAN	Multi-Service Access Network
MSTP	Multiple Spanning Tree Protocol
NGN	Next Generation Network
OLT	Optical Line Termination
OSPF	Open Shortest Path First
OTDR	Optical Time Domain Reflectometer
PON	Passive Optical Network
POTS	Plain Old Telephone Service
ppm	parts per million
PRI	Primary Rate Interface
PSTN	Public Switched Telephone Network
QinQ	802.1Q-in-802.1Q

RIP	Routing Information Protocol
RNC	Radio Network Controller
RSTP	Rapid Spanning Tree Protocol
RSSI	Received Signal Strength Indication
SBA	Static Bandwidth Allocation
SBU	Single Business Unit
SCB	Single Copy Broadcast
SDH	Synchronous Digital Hierarchy
SFU	Single Family Unit
SHDSL	Single-pair High bit rate Digital Subscriber Line
SNI	Service Node Interface
SNMP	Simple Network Management Protocol
SP	Strict Priority
STB	Set Top Box
STM	Synchronous Transport Module
STP	Straight-Through Processing
SSH	Secure Shell
TCP	Transmission Control Protocol
TDM	Time Division Multiplex
TG	Trunk Gateway
TOD	Time of Day
ToS	Type of Service
UDP	User Datagram Protocol
UNI	User-Network Interface
VDN	Video Distribution Network
VDSL	Very High Speed Digital Subscriber Line
WDM	Wavelength Division Multiplexing

Product Documentation Customer Satisfaction Survey

Thank you for reading and using the product documentation provided by FiberHome. Please take a moment to complete this survey. Your answers will help us to improve the documentation and better suit your needs. Your responses will be confidential and given serious consideration. The personal information requested is used for no other purposes than to respond to your feedback.

Name	
Phone Number	
Email Address	
Company	

To help us better understand your needs, please focus your answers on a single documentation or a complete documentation set.

Documentation Name	
Code and Version	

Usage of the product documentation:

1. How often do you use the documentation?

☐ Frequently ☐ Rarely ☐ Never ☐ Other (please specify) _____

2. When do you use the documentation?

☐ in starting up a project ☐ in installing the product ☐ in daily maintenance ☐ in trouble shooting ☐ Other (please specify) _____

3. What is the percentage of the operations on the product for which you can get instruction from the documentation?

☐ 100% ☐ 80% ☐ 50% ☐ 0% ☐ Other (please specify) _____

4. Are you satisfied with the promptness with which we update the documentation?

☐ Satisfied ☐ Unsatisfied (your advice) _____

5. Which documentation form do you prefer?

☐ Print edition ☐ Electronic edition ☐ Other (please specify) _____

Quality of the product documentation:

1. Is the information organized and presented clearly?

☐ Very ☐ Somewhat ☐ Not at all (your advice) _____

2. How do you like the language style of the documentation?

☐ Good ☐ Normal ☐ Poor (please specify) _____

3. Are any contents in the documentation inconsistent with the product?

_____

4. Is the information complete in the documentation?

☐ Yes

☐ No (Please specify) _____

5. Are the product working principles and the relevant technologies covered in the documentation sufficient for you to get known and use the product?

☐ Yes

☐ No (Please specify) _____

6. Can you successfully implement a task following the operation steps given in the documentation?

☐ Yes (Please give an example) _____

☐ No (Please specify the reason) _____

7. Which parts of the documentation are you satisfied with?

_____

8. Which parts of the documentation are you unsatisfied with?Why?

_____

9. What is your opinion on the Figures in the documentation?

☐ Beautiful ☐ Unbeautiful (your advice) _____

☐ Practical ☐ Unpractical (your advice) _____

10. What is your opinion on the layout of the documentation?

☐ Beautiful ☐ Unbeautiful (your advice) _____

11. Thinking of the documentations you have ever read offered by other companies, how would you compare our documentation to them?

Product documentations from other companies:_____

Satisfied (please specify) _____

Unsatisfied (please specify) _____

12. Additional comments about our documentation or suggestions on how we can improve:

_____

_____

Thank you for your assistance. Please fax or send the completed survey to us at the contact information included in the documentation. If you have any questions or concerns about this survey please email at edit@fiberhome.com