

Product Manual

AN5506-01 / 02 Series GPON Optical Network Unit

Version: A

Code: MN000002300

Date: June 2015

Version

Version	Description
A	Initial version.



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.

Contents

1 Safety Precautions	1
2 Product Specification	2
3 Product Overview	3
3.1 Introduction to the AN5506-01-A	3
3.2 Introduction to the AN5506-01-B	10
3.3 Introduction to the AN5506-02-A	15
3.4 Introduction to the AN5506-02-B	20
4 Web Configuration Guide	26
4.1 Logging into the Web GUI Locally	26
4.2 Status.....	33
4.2.1 Equipment Information	33
4.2.2 WAN Side Status.....	33
4.2.3 LAN Side Status.....	34
4.2.4 Optical Power Status	35
4.3 Network.....	35
4.3.1 LAN Setting.....	35
4.3.2 Broadband Setting.....	36
4.3.3 DHCP Server	41
4.3.4 Authentication Setting.....	43
4.4 Security	44
4.4.1 Firewall	45
4.4.2 Remote Control	51
4.4.3 DDOS	52
4.4.4 HTTPS.....	53

4.5 Application	53
4.5.1 DDNS	54
4.5.2 Port Forwarding.....	55
4.5.3 NAT	56
4.5.4 Network Diagnosis	58
4.6 Management	58
4.6.1 User Management.....	59
4.6.2 Equipment Management.....	60
4.6.3 Log	63
5 Handling Common Problems	65
5.1 Power Supply Status Indicator LED OFF	65
5.2 Register Status Indicator LED OFF	65
5.3 Optical Signal Status Indicator LED ON or Blinking.....	65
5.4 Ethernet Interface Status Indicator LED OFF	66
6 Standard and Protocol	67

1 Safety Precautions

For your correct and safe operations on the equipment, please read carefully 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 38 mm.
- ◆ 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 temperatures 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.

2 Product Specification

The tables below present the interfaces on the AN5506-01 / 02 Series ONUs and the services supported by these ONUs for users' reference on ONU configuration.

Table 2.1 lists the interfaces supported by the AN5506-01 / 02 Series ONUs.

Table 2.1 Interfaces Supported by the ONUs

ONU Type	Ethernet Interface Quantity	Phone Interface Quantity
AN5506-01-A	1 (GE)	-
AN5506-01-B	1 (GE)	1
AN5506-02-A	2 (GE)	-
AN5506-02-B	2 (GE)	1

Table 2.2 lists the service types supported by the AN5506-01 / 02 Series ONUs.

Table 2.2 Service Types Supported by the ONUs

ONU Type	Internet Service	Multicast Service	Voice Service
AN5506-01-A	Supported	Supported	Not supported
AN5506-01-B	Supported	Supported	Supported
AN5506-02-A	Supported	Supported	Not supported
AN5506-02-B	Supported	Supported	Supported

3 Product Overview

The following introduces the appearance, specifications and indicator LEDs of the AN5506-01 / 02 Series series ONUs.

3.1 Introduction to the AN5506-01-A

The AN5506-01-A is an FTTH GPON ONU. It provides users with communication and entertainment services in the form of data, video, and so on, to meet the integrated access demand of families and small-scaled enterprises. It includes two sub-types: the AN5506-01-A6G and the AN5506-01-A9G. The two sub-types mainly differ in their specifications and LED indicators.

Appearance

The overall appearance of the AN5506-01-A is shown in Figure 3.1.



Figure 3.1 Overall Appearance of the AN5506-01-A

The rear panel of the AN5506-01-A is shown in Figure 3.2.

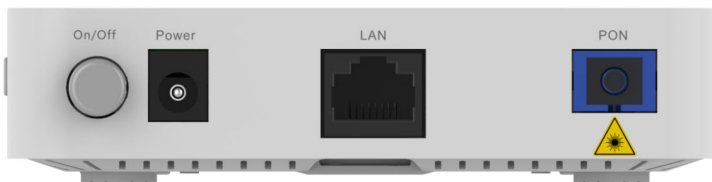


Figure 3.2 Rear Panel of the AN5506-01-A

The side panel of the AN5506-01-A is shown in Figure 3.3.

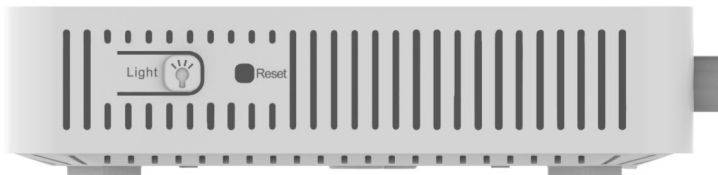


Figure 3.3 Side Panel of the AN5506-01-A

Equipment Specifications

The AN5506-01-A specifications include technical parameters and specifications. Table 3.1 shows the technical parameters. Table 3.2 and Table 3.3 show the specifications.

Table 3.1 Technical Parameters of the AN5506-01-A

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining the 802.1Q VLAN in the tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports the IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.
	Wire-speed forward-ing	Supports Layer 2 / Layer 3 wire-speed forwarding.
	IP	Supports the IPv4/v6 dual stack.
	Security	Supports the packet filtering, MAC address filtering and URL filtering.
		Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
		Supports obtaining the user IP address in the DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining the user IP address in the PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports encryption of downlink data using the AES-128 algorithm.

Table 3.1 Technical Parameters of the AN5506-01-A (Continued)

Type	Item	Description
	QoS	Supports the ACL function to match traffic based on the ACL rules.
		Supports global configuration of queue priority and flexible mapping of 802.1p values in packets.
		Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of the scheduled queue, so as to guarantee the service quality of high-QoS services such as video in the multi-service environment.
Network side interface	GPON interface	Provides one GPON interface (SC/UPC or SC/APC interface), supporting transmission distance up to 20km and complying with the ITU-T G.984 standard.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides one LAN interface (RJ-45 interface), supporting full-duplex or half-duplex and 10 / 100 / 1000 Mbit/s auto negotiation. The maximum transmission distance is 100 m.
		MAC address capacity: 1K

Table 3.2 Specifications of the AN5506-01-A6G

Type	Item	Description
Mechanical parameters	Dimensions	25.5mm × 112mm × 112mm (height x width x depth)
	Wall mounting hole distance	75mm
	Weight	About 120g
Power supply parameters	DC	DC 12 V/0.5 A

Table 3.2 Specifications of the AN5506-01-A6G (Continued)

Type	Item	Description
Power consumption parameters	-	<4W
Environment parameters	Operating temperature	-5°C to 45°C
	Storage temperature	-40°C to 70°C
	Environmental humidity	10% to 95% (no condensation)

Table 3.3 Specifications of the AN5506-01-A9G

Type	Item	Description
Mechanical parameters	Dimensions	23.5mm × 80mm × 80mm (height x width x depth)
	Wall mounting hole distance	45mm
	Weight	About 90g
Power supply parameters	DC	DC 12 V/0.5 A
Power consumption parameters	-	<1.8W
Environment parameters	Operating temperature	-5°C to 45°C
	Storage temperature	-40°C to 70°C
	Environmental humidity	10% to 95% (no condensation)

Indicator LED Description

See Table 3.4 and Table 3.5 for the description of indicator LEDs on the AN5506-01-A.

Table 3.4 Description of Indicator LEDs on the AN5506-01-A6G

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

Table 3.5 Description of Indicator LEDs on the AN5506-01-A9G

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			Blinking	The ONU is being activated.
			OFF	The ONU is not activated.
LOS	Optical signal status indicator LED	Red	ON	The power supply for the PON port optical module of the ONU is shut down.
			Blinking	The Rx optical power of the ONU is lower than the optical Rx sensitivity.
			OFF	The Rx optical power of the ONU is normal.
LAN	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data are transmitted.
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
Power	Power status indicator LED	Green	ON	The ONU is powered on.
			OFF	The ONU is not powered on.

3.2 Introduction to the AN5506-01-B

The AN5506-01-B is an FTTH GPON ONU. 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.

Appearance

The overall appearance of the AN5506-01-B is shown in Figure 3.4.



Figure 3.4 Overall Appearance of the AN5506-01-B

The rear panel of the AN5506-01-B is shown in Figure 3.5.

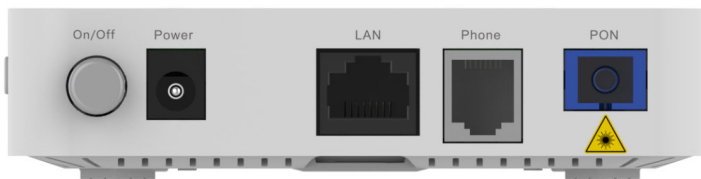


Figure 3.5 Rear Panel of the AN5506-01-B

The side panel of the AN5506-01-B is shown in Figure 3.6.

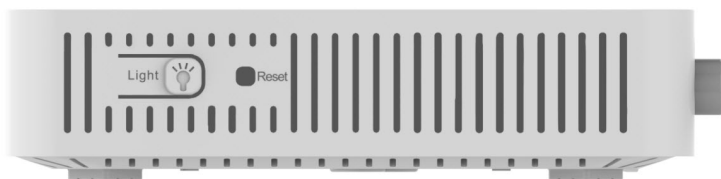


Figure 3.6 Side Panel of the AN5506-01-B

Equipment Specifications

The AN5506-01-B specifications include technical parameters and specifications. Table 3.6 shows the technical parameters. Table 3.7 shows the specifications.

Table 3.6 Technical Parameters of the AN5506-01-B

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining the 802.1Q VLAN in the tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports the IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.
	Wire-speed forwarding	Supports Layer 2 / Layer 3 wire-speed forwarding.

Table 3.6 Technical Parameters of the AN5506-01-B (Continued)

Type	Item	Description
	IP	Supports the IPv4/v6 dual stack.
	Security	Supports the packet filtering, MAC address filtering and URL filtering.
		Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
		Supports obtaining the user IP address in the DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining the user IP address in the PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports encryption of downlink data using the AES-128 algorithm.
	QoS	Supports the ACL function to match traffic based on the ACL rules.
		Supports global configuration of queue priority and flexible mapping of 802.1p values in packets.
		Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of the scheduled queue, so as to guarantee the service quality of high-QoS services such as voice and video in the multi-service environment.
Network side interface	GPON interface	Provides one GPON interface (SC/UPC or SC/APC interface), supporting transmission distance up to 20km and complying with the ITU-T G.984 standard.

Table 3.6 Technical Parameters of the AN5506-01-B (Continued)

Type	Item	Description
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides one LAN interface (RJ-45 interface), supporting full-duplex or half-duplex and 10 / 100 / 1000 Mbit/s auto negotiation. The maximum transmission distance is 100 m.
		MAC address capacity: 1K
	Phone interface	Provides one phone interface (RJ-11 interface).

Table 3.7 Specifications of the AN5506-01-B

Type	Item	Description
Mechanical parameters	Dimensions	25.5mm × 112mm × 112mm (height x width x depth)
	Wall mounting hole distance	75mm
	Weight	About 131g
Power supply parameters	DC	DC 12 V/1 A
Power consumption parameters	-	<5W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃

Table 3.7 Specifications of the AN5506-01-B (Continued)

Type	Item	Description
	Environmental humidity	10% to 95% (no condensation)

Indicator LED Description

See Table 3.8 for the description of indicator LEDs on the AN5506-01-B.

Table 3.8 Description of Indicator LEDs on the AN5506-01-B

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			Blinking	The ONU is being activated.
			OFF	The ONU is not activated.
LOS	Optical signal status indicator LED	Red	Blinking	The ONU has not received the optical signal.
			OFF	The ONU has received the optical signal.
Voice	Phone port status indicator LED	Green	ON	The port is registered in the softswitch system.
			Blinking	Service flow is found at the port.
			OFF	The port is not registered in the softswitch system.
Ethernet port	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data are transmitted.
			Blinking	The interface is transmitting / receiving data.

Table 3.8 Description of Indicator LEDs on the AN5506-01-B (Continued)

Indicator LED	Meaning	Color	Status	Status Description
			OFF	The interface is not connected to the user terminal.
Power	Power status indicator LED	Green	ON	The ONU is powered on.
			OFF	The ONU is not powered on.

3.3 Introduction to the AN5506-02-A

The AN5506-02-A is an FTTH GPON ONU. It provides users with communication and entertainment services in the form of data, video, and so on, to meet the integrated access demand of families and small-scaled enterprises.

Appearance

The overall appearance of the AN5506-02-A is shown in Figure 3.7.



Figure 3.7 Overall Appearance of the AN5506-02-A

The rear panel of the AN5506-02-A is shown in Figure 3.8.

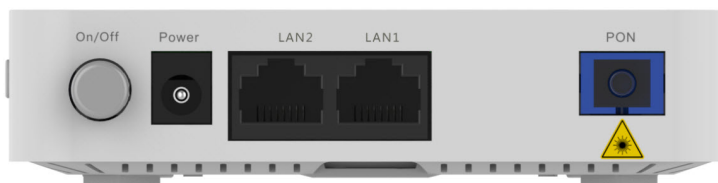


Figure 3.8 Rear Panel of the AN5506-02-A

The side panel of the AN5506-02-A is shown in Figure 3.9.

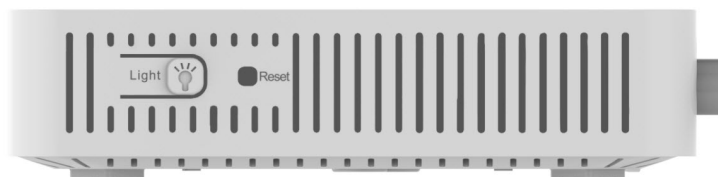


Figure 3.9 Side Panel of the AN5506-02-A

Equipment Specifications

The AN5506-02-A specifications include technical parameters and specifications. Table 3.9 shows the technical parameters. Table 3.10 shows the specifications.

Table 3.9 Technical Parameters of the AN5506-02-A

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining the 802.1Q VLAN in the tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports the IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.
	Wire-speed forwarding	Supports Layer 2 / Layer 3 wire-speed forwarding.
	IP	Supports the IPv4/v6 dual stack.
	Security	Supports the packet filtering, MAC address filtering and URL filtering.
		Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
		Supports obtaining the user IP address in the DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining the user IP address in the PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports encryption of downlink data using the AES-128 algorithm.

Table 3.9 Technical Parameters of the AN5506-02-A (Continued)

Type	Item	Description
	QoS	Supports the ACL function to match traffic based on the ACL rules.
		Supports global configuration of queue priority and flexible mapping of 802.1p values in packets.
		Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of the scheduled queue, so as to guarantee the service quality of high-QoS services such as video in the multi-service environment.
Network side interface	GPON interface	Provides one GPON interface (SC/UPC or SC/APC interface), supporting transmission distance up to 20km and complying with the ITU-T G.984 standard.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides two LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10 / 100 / 1000 Mbit/s auto negotiation. The maximum transmission distance is 100 m.
		MAC address capacity: 1K

Table 3.10 Specifications of the AN5506-02-A

Type	Item	Description
Mechanical parameters	Dimensions	25.5mm × 112mm × 112mm (height x width x depth)
	Wall mounting hole distance	75mm

Table 3.10 Specifications of the AN5506-02-A (Continued)

Type	Item	Description
	Weight	About 138g
Power supply parameters	DC	DC 12 V/0.5 A
Power consumption parameters	-	<4W
Environment parameters	Operating temperature	-5°C to 45°C
	Storage temperature	-40°C to 70°C
	Environmental humidity	10% to 95% (no condensation)

Indicator LED Description

See Table 3.11 for the description of indicator LEDs on the AN5506-02-A.

Table 3.11 Description of Indicator LEDs on the AN5506-02-A

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			Blinking	The ONU is being activated.
			OFF	The ONU is not activated.
LOS	Optical signal status indicator LED	Red	Blinking	The ONU has not received the optical signal.
			OFF	The ONU has received the optical signal.

Table 3.11 Description of Indicator LEDs on the AN5506-02-A (Continued)

Indicator LED	Meaning	Color	Status	Status Description
Ethernet port	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data are transmitted.
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
Power	Power status indicator LED	Green	ON	The ONU is powered on.
			OFF	The ONU is not powered on.

3.4 Introduction to the AN5506-02-B

The AN5506-02-B is an FTTH GPON ONU. 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.

Appearance

The overall appearance of the AN5506-02-B is shown in Figure 3.10.



Figure 3.10 Overall Appearance of the AN5506-02-B

The rear panel of the AN5506-02-B is shown in Figure 3.11.

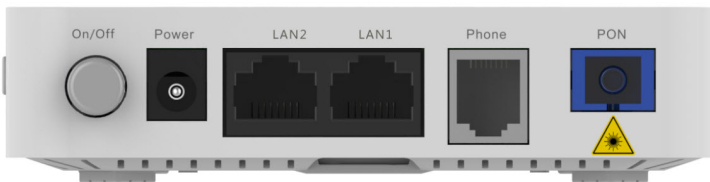


Figure 3.11 Rear Panel of the AN5506-02-B

The side panel of the AN5506-02-B is shown in Figure 3.12.

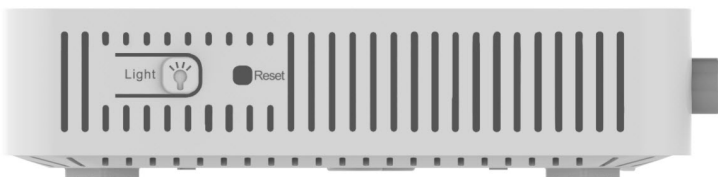


Figure 3.12 Side Panel of the AN5506-02-B

Equipment Specifications

The AN5506-02-B specifications include technical parameters and specifications. Table 3.12 shows the technical parameters. Table 3.13 shows the specifications.

Table 3.12 Technical Parameters of the AN5506-02-B

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining the 802.1Q VLAN in the tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports the IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.
	Wire-speed forwarding	Supports Layer 2 / Layer 3 wire-speed forwarding.
	IP	Supports the IPv4/v6 dual stack.
	Security	Supports the packet filtering, MAC address filtering and URL filtering.
		Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
		Supports obtaining the user IP address in the DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining the user IP address in the PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports encryption of downlink data using the AES-128 algorithm.

Table 3.12 Technical Parameters of the AN5506-02-B (Continued)

Type	Item	Description
	QoS	Supports the ACL function to match traffic based on the ACL rules.
		Supports global configuration of queue priority and flexible mapping of 802.1p values in packets.
		Supports three queue scheduling modes (PQ, WRR and PQ+WRR); supports configuring the weight of the scheduled queue, so as to guarantee the service quality of high-QoS services such as voice and video in the multi-service environment.
Network side interface	GPON interface	Provides one GPON interface (SC/UPC or SC/APC interface), supporting transmission distance up to 20 km and complying with the ITU-T G.984 standard.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides two LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10 / 100 / 1000 Mbit/s auto negotiation. The maximum transmission distance is 100 m.
		MAC address capacity: 1K
	Phone interface	Provides one phone interface (RJ-11 interface).

Table 3.13 Specifications of the AN5506-02-B

Type	Item	Description
Mechanical parameters	Dimensions	25.5mm × 112mm × 112mm (height x width x depth)

Table 3.13 Specifications of the AN5506-02-B (Continued)

Type	Item	Description
	Wall mounting hole distance	75mm
	Weight	About 141g
Power supply parameters	DC	DC 12 V/1 A
Power consumption parameters	-	<5W
Environment parameters	Operating temperature	-5°C to 45°C
	Storage temperature	-40°C to 70°C
	Environmental humidity	10% to 95% (no condensation)

Indicator LED Description

See Table 3.14 for the description of indicator LEDs on the AN5506-02-B.

Table 3.14 Description of Indicator LEDs on the AN5506-02-B

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			Blinking	The ONU is being activated.
			OFF	The ONU is not activated.

Table 3.14 Description of Indicator LEDs on the AN5506-02-B (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LOS	Optical signal status indicator LED	Red	Blinking	The ONU has not received the optical signal.
			OFF	The ONU has received the optical signal.
Voice	Phone port status indicator LED	Green	ON	The port is registered in the softswitch system.
			Blinking	Service flow is found at the port.
			OFF	The port is not registered in the softswitch system.
Ethernet port	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data are transmitted.
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
Power	Power status indicator LED	Green	ON	The ONU is powered on.
			OFF	The ONU is not powered on.

4 Web Configuration Guide

The following introduces the Web GUI of the AN5506-01 / 02 Series ONU administrator, including the parameter meanings and operation methods.



Tip:

Configure the ONU using the access network management system on the OLT. Refer to the corresponding OLT configuration guide.

4.1 Logging into the Web GUI Locally

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

Prerequisites

- ◆ The ONU has connected with the computer correctly.
- ◆ The user computer is started normally.
- ◆ The ONU is started normally.

Press the ONU power button. If the power indicator LED is ON, the ONU is powered on successfully.

Planning Data

Before setting the configuration environment, prepare the data information as shown in Table 4.1.

Table 4.1 Planning Data for Logging into the Web GUI Locally

Item	Description
User name and password	Factory default value: <ul style="list-style-type: none"> ◆ Administrator <ul style="list-style-type: none"> ▶ User name: admin ▶ Password: admin

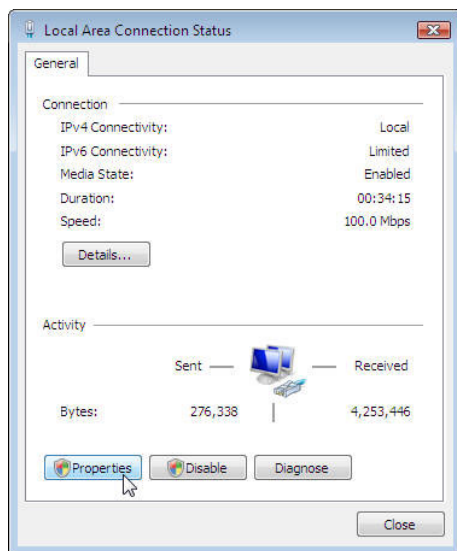
Table 4.1 Planning Data for Logging into the Web GUI Locally (Continued)

Item	Description
	<ul style="list-style-type: none"> ◆ Common user <ul style="list-style-type: none"> ▶ User name: useradmin ▶ Password: user1234 <p>Note: Some operators customized the user name and password, so that the default user name and password may have been modified. In this case, please contact the local operator.</p> <p>Note: The password is case sensitive.</p>
Management IP address and subnet mask of the ONU	<p>Factory default value:</p> <ul style="list-style-type: none"> ◆ IP address: 192.168.1.1 ◆ Subnet mask: 255.255.255.0 <p>Note: Some operators customized the management IP address, so that the default management IP address may have been modified. In this case, please refer to the User Guide attached to the equipment or the label at the bottom of the equipment.</p>
The IP address and the subnet mask of the user computer	<ul style="list-style-type: none"> ◆ Set this item to DHCP obtaining IP address automatically (recommended). ◆ Set this item to static IP address, which should be in the same network segment with the management IP address of the ONU. <ul style="list-style-type: none"> ▶ IP address: 192.168.1.X (X is a decimal integer between 2 to 253) ▶ Subnet mask: 255.255.255.0

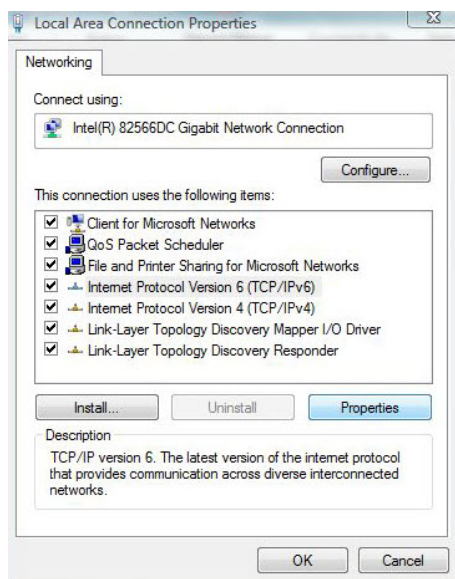
Procedure

1. Set the IP address and the subnet mask of the computer.
 - ▶ The operation method of the Windows 7 operating system is as follows:
 - a) In the Windows taskbar, select **Start→Control Panel** and click **Network and Sharing Center**.

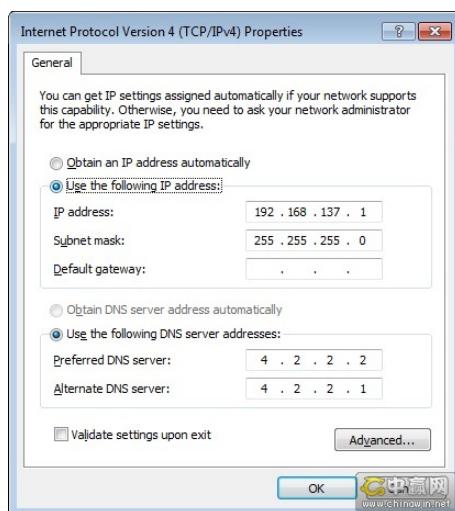
- b) Click **Local Area Connection** to bring up the **Local Area Connection Properties**, and click **Properties**.



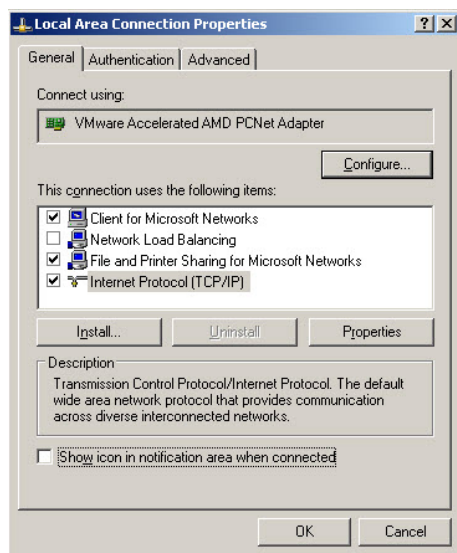
- c) In the **Local Area Connection Properties** dialog box, double-click **Internet Protocol 4 (TCP/IPv4)**.



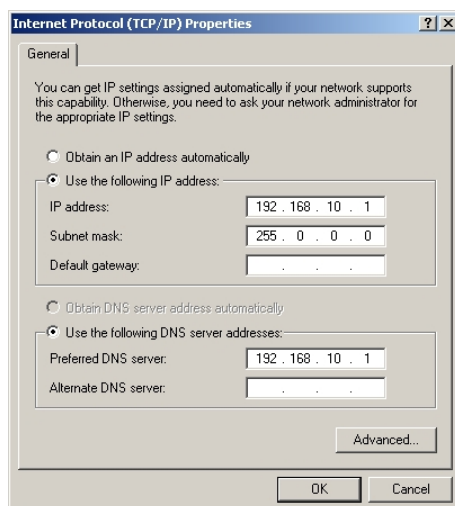
- d) In the **Internet Protocol 4 (TCP/IPv4) Properties** dialog box, set the IP address and subnet mask of the computer. (See Table 4.1 for the detailed values).



- e) Click the **OK** button to save the configuration.
- ▶ The operation method of the Windows XP operating system is described 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 4.1 for the detailed values).



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

2. Enter **http://192.168.1.1** (default management IP address of the ONU) in the browser address bar in the computer, and press the Enter key to bring up the user login dialog box.
3. Enter the administrator user name 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.

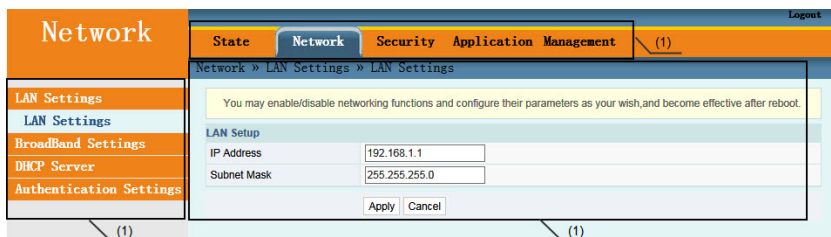
Web Configuration GUI Layout

The Web configuration GUI comprises three parts, as shown in Figure 4.1.

- ◆ Navigation bar. Click the link to enter the corresponding configuration management tab.
- ◆ Link bar. Click the link to enter the corresponding configuration management sub-tab.

4 Web Configuration Guide

- ◆ Configuration management area. Displays the corresponding content of the selected navigation bar and link bar.



(1) Navigation bar

(2) Link bar

(3) Configuration
management area

Figure 4.1 Web Configuration GUI

The Web GUI configuration is basically the same for the AN5506-01 / 02 Series ONUs. The following illustrates how an administrator user (admin) of the AN5506-02-B logs into the Web GUI (version RP2520). The snapshot pictures for other devices may be a little different from the ones here. The practical GUI 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 **State** tab.
 - ▶ **Maintenance Account** and **Device Reboot** in the **Management** tab.

4.2 Status

The following introduces how to view the basic information of the ONU in the Web GUI, including the equipment information, WAN side status, LAN side status, and optical power status.

4.2.1 Equipment Information

Select "State" in the navigation bar and select "Device Information" in the left link bar to view the information such as the product name, hardware version and software version. See Figure 4.2.

State » Device Information » Device Information	
You can query device information here !	
Device Information	
Software Version	RP2520
Hardware Version	WKE2.134.321B6G
Device Model	AN5506-02-B
Device Description	GPON
ONU State	O1(STATE_INIT)
ONU Regist State	INIT
CPU Usage	21%
Memory Usage	77%
Web Server port	80

Figure 4.2 Equipment Information

4.2.2 WAN Side Status

Select "State" in the navigation bar and select "Wan State" in the left link bar to view the information such as the status, IP obtaining mode, IP address and subnet mask of the WAN side. See Figure 4.3.

State » Wan State » Wan State								
You can query the state of wan interface here!								
WAN State								
Index	State	Mode	IP Type	IP	Mask	DNS	VLAN/Priority	Connection type
1	up	INTERNET	STATIC	10.190.17.186	255.255.255.0	10.19.8.10	4006/0	Route

Figure 4.3 WAN Side Status

4.2.3 LAN Side Status

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

LAN Side Status

Select **State** in the navigation bar and select **Lan State**→**Lan State** in the left link bar to view the information such as the IP address, subnet mask, service type and status of the LAN side. See Figure 4.4.

State » Lan State » Lan State	
You can query the state of lan interface here!	
LAN State	
IP Address	192.168.1.1
LAN Mask	255.255.255.0

Figure 4.4 LAN Side Status

DHCP User List

Select **State** in the navigation bar and select **Lan State**→**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 4.5.

State » Lan State » DHCP Clients List				
Display information about DHCP client, include IP address, MAC address, and lease				
DHCP Clients List				
ID	MAC	IP	Hired Time	Type
1	ac:e2:15:10:ca:fd	192.168.1.2	5194 sec	Dynamic

Figure 4.5 DHCP User List

4.2.4 Optical Power Status

Select **State** in the navigation bar and select **Optical Power** 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 4.6.

State » Optical Power » Optical Power	
You can query State of optical power here!	
optical Info	
Transmitted Power	0.00 dBm
Recived Power	-99.00 dBm
Operating Temperature	52.08 °C
Supply Voltage	3.25 V
Bais Current	0.00 mA

Figure 4.6 Optical Power Status

4.3 Network

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

4.3.1 LAN Setting

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

4 Web Configuration Guide

1. Select **Network** in the navigation bar and select **LAN Settings** → **LAN Settings** in the left link bar to open the LAN settings tab, as shown in Figure 4.7.

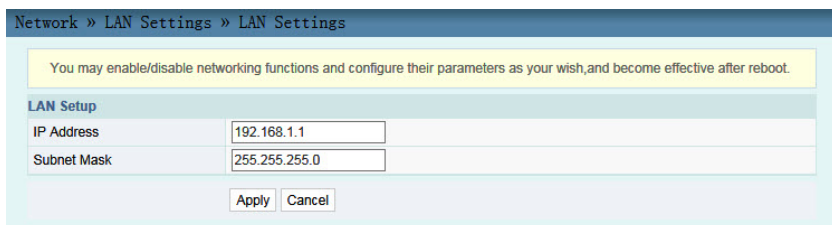


Figure 4.7 LAN Settings

2. Configure the management IP address and subnet mask at the LAN side. See Table 4.2 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 4.2 Parameters of LAN Settings

Item	Description
IP Address	The management IP address at the LAN side of the ONU. The default value is 192.168.1.1.
Subnet Mask	The subnet mask of the ONU for the LAN. The default value is 255.255.255.0.

4.3.2 Broadband Setting

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** in the left link bar to open the Broadband setting tab, as shown in Figure 4.8.

Network » BroadBand Settings » Internet Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Name	VID/Priority	WAN IP Mode	
1_INTERNET_R_4006	4006/0	STATIC	<input type="checkbox"/>

WAN Enable:

Service Type:

connection Type:

VLAN ID:

Priority:

Nat:

DNS Relay:

Lan Binding: LAN 1 ☒ LAN 2 ☐ LAN 3 ☐ LAN 4 ☐

SSID Binding: SSID 1 ☐ SSID 2 ☐ SSID 3 ☐ SSID 4 ☐

IP Mode:

WAN IP Mode:

Static Mode

IP Address:

Subnet Mask:

Default Gateway:

Primary DNS Server:

Secondary DNS Server:

Figure 4.8 Broadband Settings

- Configure the parameters related to the broadband at the WAN side. Table 4.3 describes the parameters.
- Click **Apply** to save and apply the configuration.

Table 4.3 Parameters for Broadband Settings

Item	Description
WAN Enable	Enables or disables the WAN connection.
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.

Table 4.3 Parameters for Broadband Settings (Continued)

Item	Description	
	<ul style="list-style-type: none">◆ TR069_INTERNET: this connection is applicable for both TR069 and Internet access.◆ Other: other connection.◆ VOIP: this connection is only applicable for voice application.◆ VOIP_INTERNET: this connection is applicable for voice and Internet access.	
Connection Type	Select the connection type of the WAN port. <ul style="list-style-type: none">◆ Bridge: the Layer 2 bridge connection mode. This connection mode can be used when the service type is set to INTERNET, TR069_INTERNET, or VOIP_INTERNET.◆ Route: the Layer 3 router connection mode. This connection mode can be used for all the service types except for Other.	
VLAN ID	Sets the VLAN ID of the WAN connection. The VLAN ID value here should be consistent with that on the user side of the OLT.	
Priority	Sets the priority of the VLAN.	
Nat	Enables or disables the NAT function.	Users need to configure this item when the service type is set to INTERNET, TR069_INTERNET or VOIP_INTERNET 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 recommended to use the default value.	
Lan Binding	Select the LAN port to be bound with the WAN port.	

Table 4.3 Parameters for Broadband Settings (Continued)

Item	Description	
IP Mode	Select IPv4 or IPv4&IPv6.	Users need to configure this item when the service type is set to INTERNET, TR069_INTERNET or VOIP_INTERNET and the connection type is set to Route.
WAN IP Mode	Sets the IP address obtaining mode at the WAN side of the ONU. 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 user name 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. ◆ Keep Alive Mode: Retry Period seconds: The ONU dials automatically to connect. If the dialing fails, the ONU will re-try dialing automatically when the retry period expires. ◆ Connect when Traffic Exists: Disconnect Period seconds: The ONU performs connection only when it has detected traffic. When a subscriber accesses	

Table 4.3 Parameters for Broadband Settings (Continued)

Item	Description	
	<p>the Internet and generates traffic, the ONU dials automatically to connect. When the subscriber is idle and no traffic exists, the ONU will stop dialing automatically after the set disconnection time interval expires.</p> <p>◆ Manual: Connects by dialing manually.</p>	
IP Address	Enter the static IP address at the WAN side provided by ISP.	This item should be configured when 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.	
IPv6 Address	Enter the static IPv6 address at the WAN side provided by ISP.	This item should be configured when the IP Mode is set to IPv4&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.	

Table 4.3 Parameters for Broadband Settings (Continued)

Item	Description	
Secondary DNS Server	Enter the IP address of the standby DNS server provided by ISP.	
IPv6 Prefix	Enter the static IPv6 address prefix at the WAN side provided by the ISP.	
IPv6 Address Obtain Mode	Selects the IPv6 address obtaining mode.	This item should be configured when the IP Mode is set to IPv4&IPv6 and the WAN IP Mode is set to DHCP or PPPoE.
Prefix_title	Selects the IPv6 address prefix obtaining mode.	

4.3.3 DHCP Server

Using the DHCP function, the ONU 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 the function.

1. Select **Network** in the navigation bar. Select **DHCP Server** from the left link bar to open the DHCP server configuration tab, as shown in Figure 4.9.

Network » DHCP Server » DHCP Service

You may enable/disable DHCP functions and configure the parameters as your wish, and become effective after reboot.

DHCP Service

Type Server

DHCP Start IP 192.168.1.2

DHCP End IP 192.168.1.254

DHCP Subnet Mask 255.255.255.0

DHCP Primary DNS 192.168.1.1

DHCP Secondary DNS

DHCP Default Gateway 192.168.1.1

Option60 Server

Option 60 start IP 192.168.1.100

Option 60 end IP 192.168.1.255

Apply Cancel

Figure 4.9 DHCP Server

- Configure the DHCP server parameters as required. Table 4.4 describes the parameters.
- Click **Apply** to save the configuration information. The configuration will take effect after the ONU is rebooted.

Table 4.4 Parameters for the DHCP Server

Item	Description	
Type	<p>Enables or disables the DHCP server.</p> <ul style="list-style-type: none"> ◆ Server: Enables the DHCP server. The ONU can dynamically distribute IP addresses to user terminals. ◆ Disable: The user terminals connected to the ONU cannot obtain the private network IP address using the DHCP. 	
DHCP Start IP	The starting IP address of the IP address pool of the DHCP server.	<p>Note: The IP address set here should be in the same network segment with the IP address set in LAN Setting; otherwise, the DHCP server will not operate normally.</p>
DHCP End IP	The end IP address of the IP address pool of the DHCP server.	

Table 4.4 Parameters for the DHCP Server (Continued)

Item	Description	
DHCP Subnet Mask	The mask of the active DHCP server.	
DHCP Primary DNS	The IP address of the active DNS server provided by ISP.	
DHCP Secondary DNS	The IP address of the standby DNS server provided by ISP.	
DHCP Default Gateway	The default gateway of the active 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 of the Option 60 property terminal distributed by the DHCP server.	This item should be set when the Option 60 property of the DHCP server is enabled.
Option 60 end IP	The end IP address of the network segment of the Option 60 property terminal distributed by the DHCP server.	

4.3.4 Authentication Setting

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

4 Web Configuration Guide

1. Select **Network** in the navigation bar and select **OLT Authentication** in the left link bar to open the OLT authentication configuration tab, as shown in Figure 4.10.

Network » Authentication Settings » OLT Authentication

You may modify the ONU authentication-related parameters, so certified by the OLT. Modify the ONU authentication parameters, reset effect.

LOID Auth

LOID * (You can input 1-24 basic Latin characters)

Logic Password (You can input 0-12 basic Latin characters)

Password Auth

Password * (You can input 0-10 characters, including alphanumeric, '-' and '_')

Figure 4.10 OLT Authentication

2. Configure the parameters as required. Table 4.5 describes the parameters.
3. Click **Apply** to save the configuration information. The configuration will take effect after the ONU is rebooted.

Table 4.5 Parameters for OLT Authentication

Item	Description	
LOID	Sets the logical SN user name.	This item is configurable when the ONU uses the logical ID authentication.
Logic Password	Sets the logical SN password.	
Password	Sets the authentication password when the ONU is authenticated by password.	

4.4 Security

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

4.4.1 Firewall

The firewall configuration covers the following items:

- ◆ Firewall enabling
- ◆ IP filtering
- ◆ URL filtering
- ◆ Anti-port scan
- ◆ MAC address filtering

4.4.1.1 Firewall Enabling

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

1. Select **Security** in the navigation bar and select **Firewall**→**Firewall Enable** in the left link bar to open the firewall enabling tab, as shown in Figure 4.11.

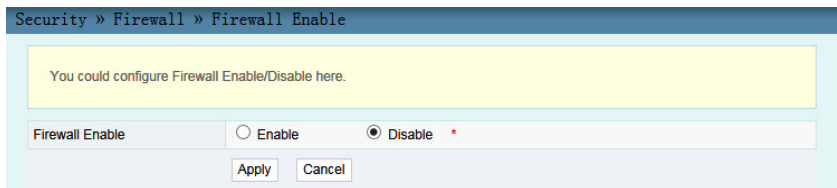


Figure 4.11 Firewall Enabling

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

4.4.1.2 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.

4 Web Configuration Guide

1. Select **Security** in the navigation bar and select **Firewall→IP Filtering** in the left link bar. Click **Add** to open the filtering rule list configuration tab, as shown in Figure 4.12.

Security » Firewall » IP Filtering

If the Firewall is enable, the configuration of the rules take effect, then forbid the IP packet which matches the filtering rules to pass through the device.

Uplink: ☐ White List ☒ Black List *

Downlink: ☐ White List ☒ Black List *

Filtering Rules List

ID	Direction	Src IP	Src Port	Dst IP	Dst Port	Protocol

Direction:

Src IP: -

Src Port: -

Dst IP: -

Dst Port: -

Protocol:

Figure 4.12 IP Filtering

2. Configure the parameters relevant to filtering as required. Table 4.6 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 4.6 Parameters for IP Address Filtering

Item	Description	
Uplink	Select the uplink filtering mode. <ul style="list-style-type: none">◆ 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 setting, click the Apply button to validate the configuration.
Downlink	Select the downlink filtering mode.	

Table 4.6 Parameters for IP Address Filtering (Continued)

Item	Description
	<ul style="list-style-type: none"> ◆ 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. <ul style="list-style-type: none"> ◆ LAN->WAN: uplink direction. ◆ WAN->LAN: downlink direction.
Source 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.
Destination 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.

4.4.1.3 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.

4 Web Configuration Guide

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 tab, as shown in Figure 4.13.

Security » Firewall » URL Filtering

If the Firewall is enable, the configuration of the rules take effect, then forbid the URL which matches the filtering rules to pass through the device.

Enable ☐ Enable ☒ Disable *

URL Blacklist/Whitelist ☐ White List ☒ Black List *

Apply Cancel

Add Delete Delete All

URL Filtering Table

ID	URL Address	Time	State
----	-------------	------	-------

URL Address

Start Time : (Hour:Min, 24)

End Time : (Hour:Min, 24)

Enable

Apply Cancel

Figure 4.13 URL Filtering

2. Configure the parameters relevant to filtering as required. Table 4.7 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 4.7 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 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	

Table 4.7 Parameters for URL Filtering Parameters (Continued)

Item	Description
	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.

4.4.1.4 Anti-port Scan

Enable or disable the anti-port scan function.

1. Select **Security** in the navigation bar and select **Firewall**→**Port Scan** in the left link bar to open the anti-port scan tab, as shown in Figure 4.14.

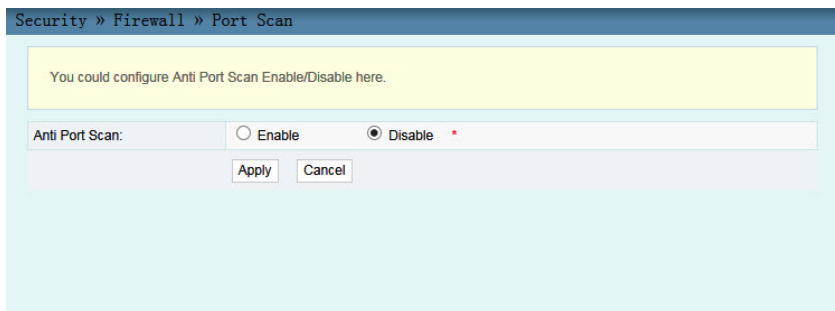


Figure 4.14 Anti-port Scan

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

4.4.1.5 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 address Filtering** in the left link bar, and then click **Add** to open the MAC address filtering table configuration tab, as shown in Figure 4.15.

Security » Firewall » MAC address Filtering

If the Firewall is enable, the configuration of the rules take effect, then forbid the MAC Address which matches the filtering rules to pass through the device.

MAC Filtering Enable: ☐ Enable ☒ Disable *

MAC Filtering Blacklist/Whitelist: ☐ White List ☒ Black List *

Apply Cancel

Add Delete Delete All

ID	MAC Address	Time	Enable

MAC Address: (You can input alphanumeric and *, such as: 00:24:21:19:BD:E4)

Start Time: 0 : 0

End Time: 24 : 0

Enable: Disable

Apply Cancel

Figure 4.15 MAC Address Filtering

2. Configure parameters related to filtering as required. Table 4.8 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.8 Parameters for MAC Address Filtering

Item	Description	
MAC Filtering Enable	Enables or disables the MAC address filtering function.	After setting, click the Apply button to validate the configuration.
MAC Filtering Blacklist / Whitelist	<p>Select the filtering mode. The white list and black list modes are global configuration, which cannot be enabled simultaneously.</p> <ul style="list-style-type: none">◆ 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.	

4.4.2 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 ONU using the IP addresses at the WAN side; if enabled, the PCs in the Internet can access the Web GUI.

4 Web Configuration Guide

1. Select **Security** in the navigation bar and select **Remote Control** in the left link bar to open the remote control configuration tab, as shown in Figure 4.16.

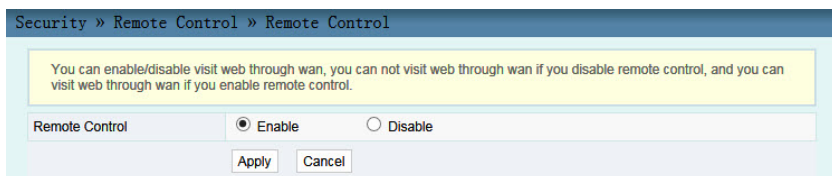


Figure 4.16 Remote Control

2. **Enable** or **Disable** the remote access control as required.
3. Click **Apply** to save and apply the configuration.

4.4.3 DDOS

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 ONU provides the protection against the DoS attack.

1. Select **Security** in the navigation bar and select **DDOS** in the left link bar to open the anti-dos attack tab, as shown in Figure 4.17.

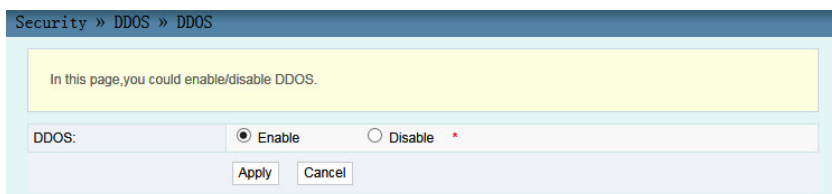


Figure 4.17 DDOS

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

4.4.4 HTTPS

The ONU 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** in the left link bar to open the HTTPS function configuration tab, as shown in Figure 4.18.

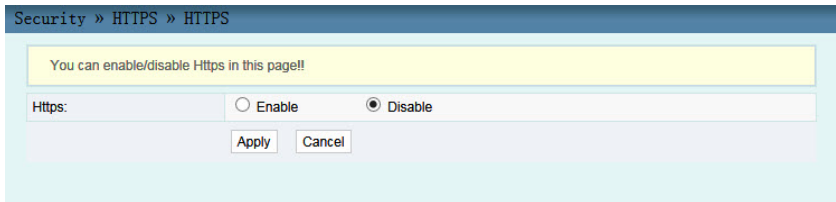


Figure 4.18 HTTPS

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.

4.5 Application

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

4.5.1 DDNS

The DDNS server transforms the dynamic IP address at the WAN side of the ONU 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** in the left link bar to open the DDNS configuration tab, as shown in Figure 4.19.

Figure 4.19 DDNS Settings

2. Configure parameters relevant to DDNS according to the requirement. Table 4.9 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.9 Parameters for DDNS Settings

Item	Description
Username	The user name allocated by the DDNS provider.
Password	The password allocated by the DDNS provider.
Host Domain Name	The domain name allocated by the DDNS provider.
DDNS Interface	The created WAN connection.
DDNS Provider	The DDNS service provider. Users can select the pre-set DDNS service provider.

4.5.2 Port Forwarding

The port forwarding can create the mapping relation 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** in the left link bar. Click **Add** to open the port forwarding configuration tab, as shown in Figure 4.20.

Application » Port Forwarding » Port Forwarding

You could configure port forwarding here!

Add Delete Delete All

Portforwarding Rules List

WAN	Discription	Public Port	IP	Private Port	Protocol	Enable	
WAN	Discription	Public Port	IP	Private Port	Protocol	Enable	

WAN: WANO
 Discription:
 Public Port: -
 IP:
 Private Port: -
 Protocol: ALL
 Enable: Disable

Apply Cancel

Figure 4.20 Port Forwarding

2. Configure parameters related to port forwarding according to the requirement. Table 4.10 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.10 Parameters for Port Forwarding

Item	Description
WAN	The corresponding WAN connection bound with the port forwarding rule.

Table 4.10 Parameters for Port Forwarding (Continued)

Item	Description
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.

4.5.3 NAT

NAT can implement 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**.

1. Select **Application** in the navigation bar and select **NAT** in the left link bar. Click **Add** to open the NAT configuration tab, as shown in Figure 4.21.

Application » NAT » NAT

You could configure Muti NAT here!

Add Delete Delete All

Muti Nat Rules List

WAN	Description	Rule Type	Locate Start IP	Locate End IP	Public Start IP	Public End IP
WAN		WANO				
Description						
Rule Type		Many-to-One				
Locate Start IP						
Locate End IP						
Public Start IP						
Public End IP						

Apply Cancel

Figure 4.21 NAT

- Configure relevant parameters according to the requirement. Table 4.11 describes the parameters.
- Click **Apply** to apply and save the configuration.

Table 4.11 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 the intranet.
Locate End IP	The ending IP address of the intranet.
Public Start IP	The starting IP address of the public network.
Public End IP	The ending IP address of the public network.

4.5.4 Network Diagnosis

The ONU 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** in the left link bar to open the network diagnosis tab, as shown in Figure 4.22.

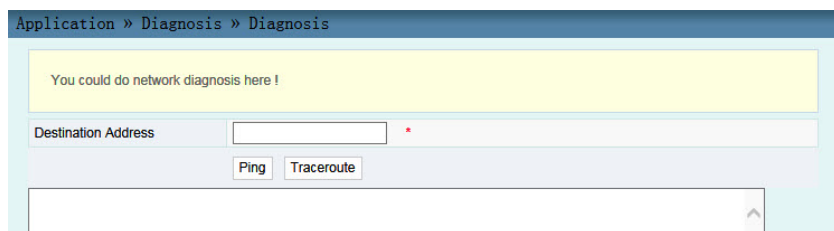


Figure 4.22 Network Diagnosis

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.

4.6 Management

The following introduces how to perform user management, equipment management and log query in the Web GUI.

4.6.1 User Management

User management includes user account management and maintenance account management.

4.6.1.1 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 tab, as shown in Figure 4.23.

Management > Account Management > User Account

You could configure name and password of admin account here!

	Username
<input type="checkbox"/>	useradmin

Add Delete

Username: useradmin

New Password:

Passwod confirm:

Apply Cancel

Figure 4.23 User Account Management

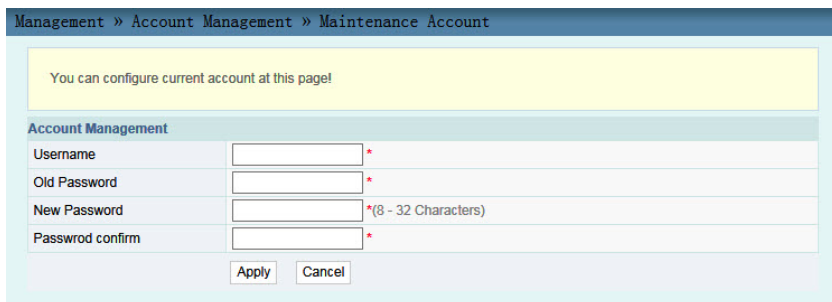
2. Add or delete a common user account or modify the password of a common user account as required.
3. Click **Apply** to apply and save the configuration.

4.6.1.2 Maintenance Account Management

Users can modify the user name and password of the current account.

4 Web Configuration Guide

1. Select **Management** in the navigation bar. Select **Account Management**→**Maintenance Account** from the left link bar to open the maintenance account management tab, as shown in Figure 4.24.



The screenshot shows a web interface for 'Maintenance Account Management'. At the top, a breadcrumb trail reads 'Management » Account Management » Maintenance Account'. Below this is a yellow message box stating 'You can configure current account at this page!'. The main section is titled 'Account Management' and contains four input fields: 'Username', 'Old Password', 'New Password', and 'Password confirm'. Each field has a red asterisk indicating it is required. The 'New Password' field has a hint '(8 - 32 Characters)'. At the bottom of the form are 'Apply' and 'Cancel' buttons.

Figure 4.24 Maintenance Account Management

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

4.6.2 Equipment Management

The ONU provides multiple equipment management functions such as configuration restoring, configuration complete restoring, local upgrade, configuration backup, and equipment reboot.

4.6.2.1 Configuration Restoring

Restore the ONU to the factory default settings, including the Web login user name and password, the SSID and password of the radio network, etc.

1. Select **Management** in the navigation bar. Select **Device Management**→**Restore** from the left link bar to open the restoring tab, as shown in Figure 4.25.

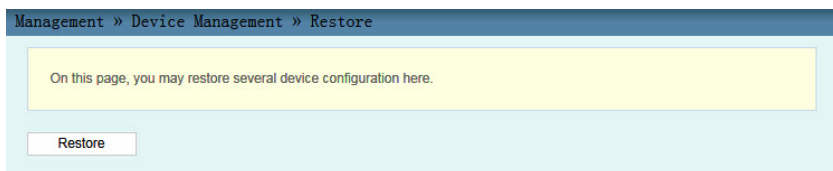


Figure 4.25 Restoring the Configuration Data

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

4.6.2.2 Configuration Complete Restoring

This function is reserved for other equipment sets. To restore the ONU configuration, operate according to [Configuration Restoring](#).

4.6.2.3 Local Upgrade

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

- Select **Management** in the navigation bar. Select **Device Management**→**Local Upgrade** from the left link bar to open the local upgrade tab, as shown in Figure 4.26.

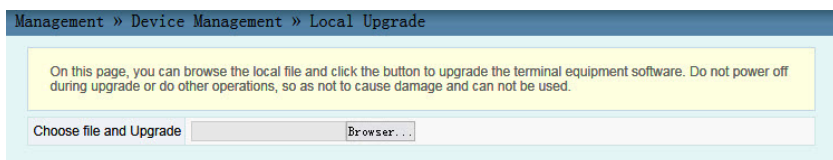


Figure 4.26 Local Upgrade

- Click **Browse**. In the dialog box that appears, select the equipment software version to be upgraded and click **Open** to upgrade the ONU software version.

- When the upgrade succeeds, the page will prompt for equipment rebooting. Click "Reboot". After rebooting, the equipment will be upgraded to the new version.



Tip:

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

4.6.2.4 Configuration Backup

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

- Select **Management** in the navigation bar. Select **Device Management**→**Config Backup** from the left link bar to open the restoring tab, as shown in Figure 4.27.

Figure 4.27 Configuration Backup

- Configure parameters related to file backup. Table 4.12 describes the parameters.
- Click **Apply** to save the configuration backup file.

Table 4.12 Parameters for Configuration Backup

Item	Description
Username	The FTP user name.
Password	The FTP password.

Table 4.12 Parameters for Configuration Backup (Continued)

Item	Description
Localhost IP	Local IP address.
File Name	The existing file name in the ONU.

4.6.2.5 Equipment Reboot

1. Select **Management** in the navigation bar. Select **Device Management**→**Device Reboot** from the left link bar to open the equipment reboot tab, as shown in Figure 4.28.

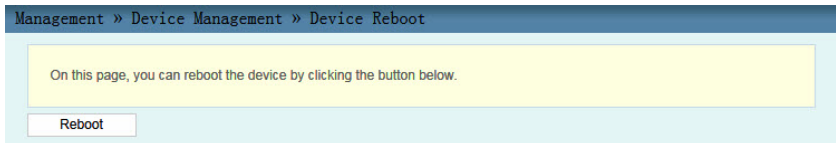


Figure 4.28 Equipment Reboot

2. Click **Reboot**. In the alert box that appears, click **OK** and wait for the equipment reboot.



Caution:

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

After the equipment is rebooted, wait for about two minutes and then re-log into the Web GUI of the equipment.

4.6.3 Log

The log files record key operations and behaviors on the ONU.

Users can view or download the information saved in log as needed.

4 Web Configuration Guide

1. Select **Management** in the navigation bar. Select **Device Management**→**Log** from the left link bar to open the log view tab, as shown in Figure 4.29.

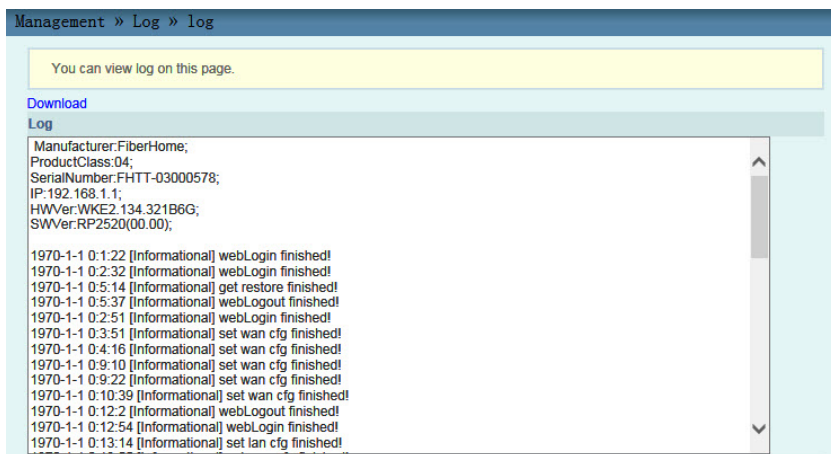


Figure 4.29 Log

2. View or download the saved information as required.

5 Handling Common Problems

The following introduces how to handle common router faults.

5.1 Power Supply Status Indicator LED OFF

Follow the procedures below for troubleshooting:

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

5.2 Register Status Indicator LED OFF

Follow the procedures below for troubleshooting:

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

5.3 Optical Signal Status Indicator LED ON or Blinking

Follow the procedures below for troubleshooting:

5 Handling Common Problems

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 ONU is over low (using the optical power meter).
4. Check whether the ONU optical module is aged or damaged.
5. Check whether the local equipment is faulty.

5.4 Ethernet Interface Status Indicator LED OFF

Follow the procedures below for troubleshooting:

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).

6 Standard and Protocol

Type	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

Type	Standard Number	Title
	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	IETF RFC 3435	Media Gateway Control Protocol (MGCP) Version 1.0
	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.723.1	Dual rate speech coder for multimedia communications transmitting at 5.3 and 6.3 kbit/s

Type	Standard Number	Title
	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.Imp 729	Implementers' Guide for G.729 Annexes B, F, G, I and C+ (Coding of speech at 8 kbit/s using CS-ACELP)
	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
TDM service	ITU-T G.8261	Timing and synchronization aspects in packet networks
	ITU-T G.8262	Timing characteristics of a synchronous Ethernet equipment slave clock
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

Type	Standard Number	Title
	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

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	
Contact	
Phone Number	
E-Mail	

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:

- How often do you use the documentation?
☐Frequently ☐Rarely ☐Never ☐Other (please specify)_____
- When do you use the documentation?
☐in starting up a project ☐in installing the product ☐in daily maintenance ☐in troubleshooting ☐Other (please specify)_____
- 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)_____
- Are you satisfied with the promptness with which we update the documentation?
☐Satisfied ☐Unsatisfied (your advice)_____
- Which documentation form do you prefer?
☐Print edition ☐Electronic edition ☐Other (please specify)_____

Quality of the product documentation:

- Is the information organized and presented clearly?
☐Very ☐Somewhat ☐Not at all (your advice)_____
- 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.

FiberHome Telecommunication Technologies Co., Ltd.

Address: No. 88 Youkeyuan Rd., Wuhan, Hubei, China

Zip code: 430074

Website: www.fiberhomegroup.com