An Expert in Optical Communications

Product Manual

AN5506-04 Series GPON Optical Network Unit

Version: A

Code: MN000002260

Date: May 2015

FiberHome Telecommunication Technologies Co., Ltd.

Version

Version	Description
A	Initial version

Contents

1 Safety Precautions

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

- Large-power laser is dangerous to human body, especially to eyes. Do not face the pigtail fiber of the optical transmitter or the end of the fiber cable connector to eyes.
- 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 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 AN5506-04 Series ONUs and the services supported by these ONUs for users' reference on ONU configuration.

Table 2.1 lists the interfaces supported by the AN5506-04 Series ONUs.

Table 2.1 Interfaces Supported by the ONUs

ONU Type	Ethernet Interface Quantity	Phone Interface Quantity	Wi-Fi Interface	USB Interface Quantity	CATV Interface Quantity
AN5506-04-A	4 (GE)	-	-	-	-
AN5506-04-B	4 (GE)	2	-	-	-
AN5506-04-CG	4 (GE)	2	-	1	1
AN5506-04-DG	4 (GE)	-	√	1	-
AN5506-04-F	4 (FE)	2	√	1	-
AN5506-04-FG	4 (GE)	2	√	1	-
AN5506-04-FS	4 (GE)	2	√	1	-
AN5506-04-GG	4 (GE)	2	√	1	1

Table 2.2 lists the service types supported by the AN5506-04 Series ONUs.

Table 2.2 Service Types Supported by the ONUs

ONU Type	Internet Service	Multicast Service	Voice Service	Wi-Fi Service
AN5506-04-A	Supported	Supported	Not supported	Not supported
AN5506-04-B	Supported	Supported	Supported	Not supported
AN5506-04-CG	Supported	Supported	Supported	Not supported
AN5506-04-DG	Supported	Supported	Not supported	Supported
AN5506-04-F	Supported	Supported	Supported	Supported
AN5506-04-FG	Supported	Supported	Supported	Supported
AN5506-04-FS	Supported	Supported	Supported	Supported
AN5506-04-GG	Supported	Supported	Supported	Supported

3 Product Overview

The following introduces the appearance, specifications and indicator LEDs of the AN5506-04 Series series ONUs.

3.1 Introduction to the AN5506-04-A

The AN5506-04-A is an FTTH-type 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 AN5506-04-A is shown in Figure 3.1.

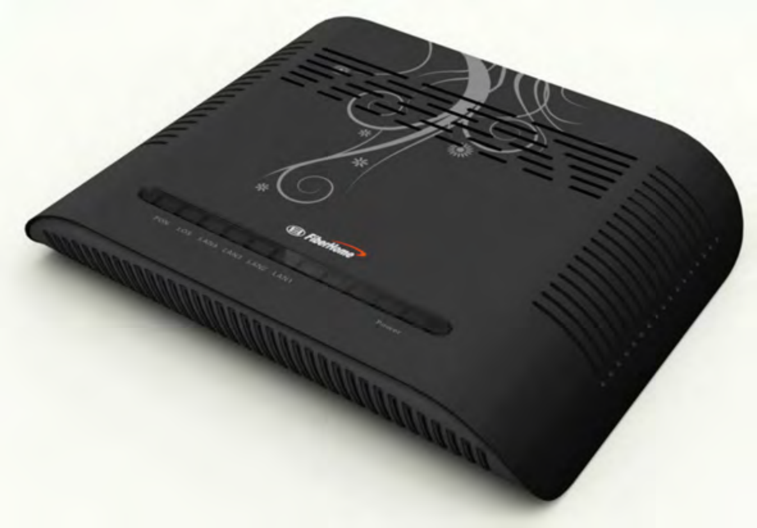


Figure 3.1 Overall Appearance of the AN5506-04-A

The rear panel of the AN5506-04-A is shown in Figure 3.2.

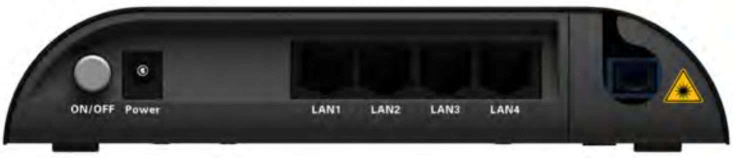


Figure 3.2 Rear Panel of the AN5506-04-A

Equipment Specifications

The AN5506-04-A specifications include technical parameters and specifications. See Table 3.1 for the technical parameters and see Table 3.2 for the specifications.

Table 3.1 Technical Parameters of the AN5506-04-A

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in 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.

Table 3.1 Technical Parameters of the AN5506-04-A (Continued)

Type	Item	Description
		Supports obtaining user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining 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 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 four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K

Table 3.2 Specifications of the AN5506-04-A

Type	Item	Description
Mechanical parameters	Dimensions	32mm × 170mm × 130mm (height x width x depth).
	Wall mounting hole distance	83mm
	Weight	About 240g
Power supply parameters	DC	DC 12 V/1A
Power consumption parameters	-	＜6.1W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation).

Indicator LED Description

See Table 3.3 for the description of indicator LEDs on the AN5506-04-A.

Table 3.3 Description of Indicator LEDs on the AN5506-04-A

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.

Table 3.3 Description of Indicator LEDs on the AN5506-04-A (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
LAN1 to LAN4	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.
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.

3.2 Introduction to the AN5506-04-B

The AN5506-04-B is an FTTH-type 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 AN5506-04-B is shown in Figure 3.3.

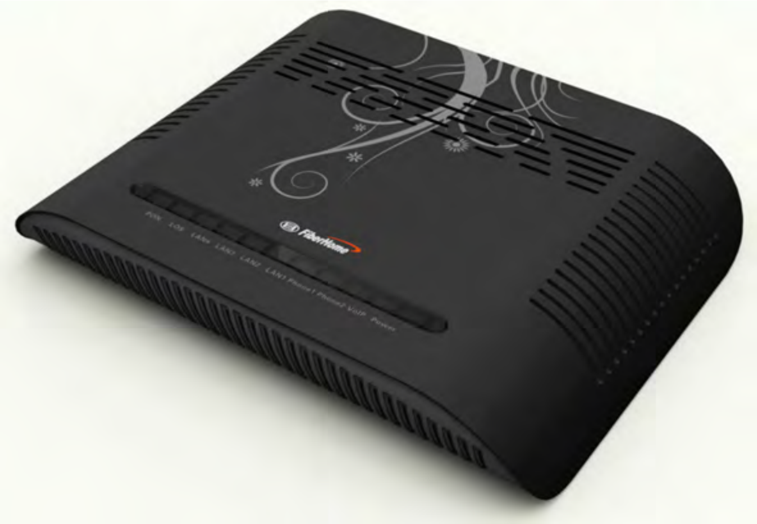


Figure 3.3 Overall Appearance of the AN5506-04-B

The rear panel of the AN5506-04-B is shown in Figure 3.4.

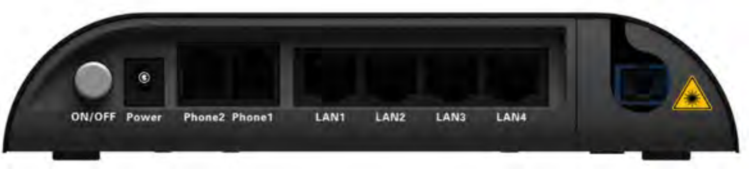


Figure 3.4 Rear Panel of the AN5506-04-B

Equipment Specifications

The AN5506-04-B specifications include technical parameters and specifications. See Table 3.4 for the technical parameters and see Table 3.5 for the specifications.

Table 3.4 Technical Parameters of the AN5506-04-B

Type	Item	Description
Service parameters	Voice	Supports the protocols H.248 and SIP.

Table 3.4 Technical Parameters of the AN5506-04-B (Continued)

Type	Item	Description
		Supports the speech encoding modes such as G.711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in 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 user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining 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.

Table 3.4 Technical Parameters of the AN5506-04-B (Continued)

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

Table 3.5 Specifications of the AN5506-04-B

Type	Item	Description
Mechanical parameters	Dimensions	32mm × 170mm × 130mm (height x width x depth).
	Wall mounting hole distance	83mm
	Weight	About 256g

Table 3.5 Specifications of the AN5506-04-B (Continued)

Type	Item	Description
Power supply parameters	DC	DC 12 V/1A
Power consumption parameters	-	＜6.5W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation).

Indicator LED Description

See Table 3.6 for the description of indicator LEDs on the AN5506-04-B.

Table 3.6 Description of Indicator LEDs on the AN5506-04-B

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
LAN1 to LAN4	Ethernet interface status indicator LED	Green	ON	The interface is connected to the user terminal and no data is transmitted.

Table 3.6 Description of Indicator LEDs on the AN5506-04-B (Continued)

Indicator LED	Meaning	Color	Status	Status Description
			Blinking	The interface is transmitting / receiving data.
			OFF	The interface is not connected to the user terminal.
Phone1, Phone2	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.
VoIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.

3.3 Introduction to the AN5506-04-CG

The AN5506-04-CG is an FTTH-type 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 AN5506-04-CG is shown in Figure 3.5.

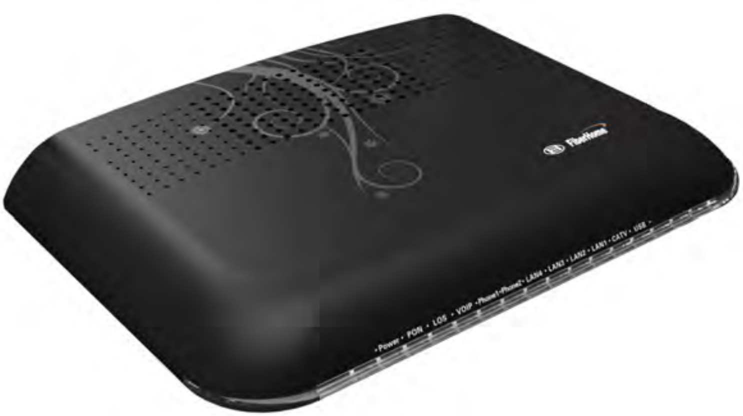


Figure 3.5 Overall Appearance of the AN5506-04-CG

The rear panel of the AN5506-04-CG is shown in Figure 3.6.

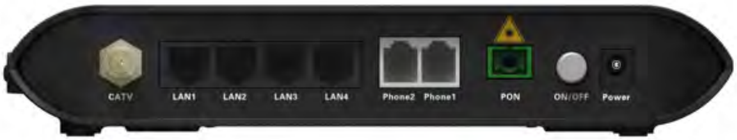


Figure 3.6 Rear Panel of the AN5506-04-CG

The side panel of the AN5506-04-CG is shown in Figure 3.7.

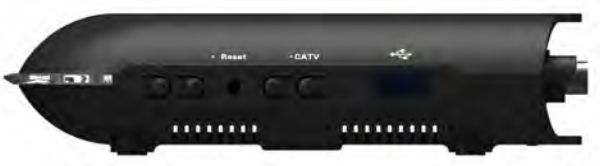


Figure 3.7 Side Panel of the AN5506-04-CG

Equipment Specifications

The AN5506-04-CG specifications include technical parameters and specifications. See Table 3.7 for the technical parameters and see Table 3.8 for the specifications.

Table 3.7 Technical Parameters of the AN5506-04-CG

Type	Item	Description
Service parameters	Voice	Supports the protocols H.248 and SIP.
		Supports the speech encoding modes such as G. 711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in 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.

Table 3.7 Technical Parameters of the AN5506-04-CG (Continued)

Type	Item	Description
		Supports protection against illegal message (DoS, ARP) attacks; supports suppression of broadcast storms.
		Supports obtaining user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining user IP address using PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports downlink data using the AES-128 algorithm for encryption.
	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.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K

Table 3.7 Technical Parameters of the AN5506-04-CG (Continued)

Type	Item	Description
	Phone interface	Provides two phone interfaces (RJ-11 interfaces).
	USB interface	Provides one USB interface. Supports USB2.0 / USB1.1.
	CATV interface	Provides one CATV interface (RF interface). RF output ＞18dBmV.

Table 3.8 Specifications of the AN5506-04-CG

Type	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth).
	Wall mounting hole distance	121mm
	Weight	About 418g
Power supply parameters	DC	DC 12 V/1.5A
Power consumption parameters	-	＜11.5W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation).

Indicator LED Description

See Table 3.9 for the description of indicator LEDs on the AN5506-04-CG.

Table 3.9 Description of Indicator LEDs on the AN5506-04-CG

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
VOIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Phone1, Phone2	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.

Table 3.9 Description of Indicator LEDs on the AN5506-04-CG (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LAN1 to LAN4	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.
CATV	CATV interface indicator LED	Green	ON	The CATV function is enabled and the CATV signal can be received normally.
			Blinking	The CATV function is enabled and the CATV signal is poor.
			OFF	The CATV function is not enabled, the CATV signal is not received or the signal is poor.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.

3.4 Introduction to the AN5506-04-DG

The AN5506-04-DG is an FTTH-type 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 AN5506-04-DG is shown in Figure 3.8.

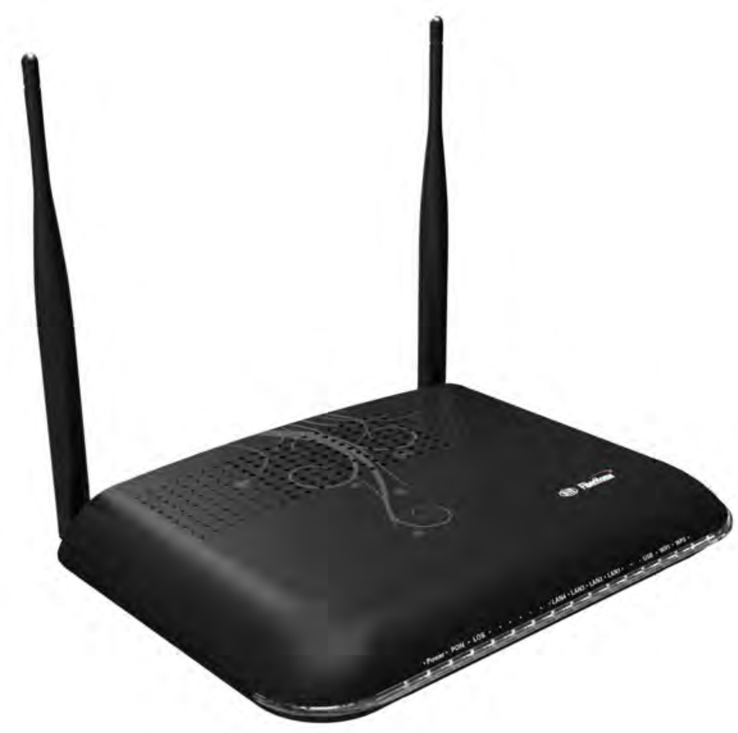


Figure 3.8 Overall Appearance of the AN5506-04-DG

The rear panel of the AN5506-04-DG is shown in Figure 3.9.

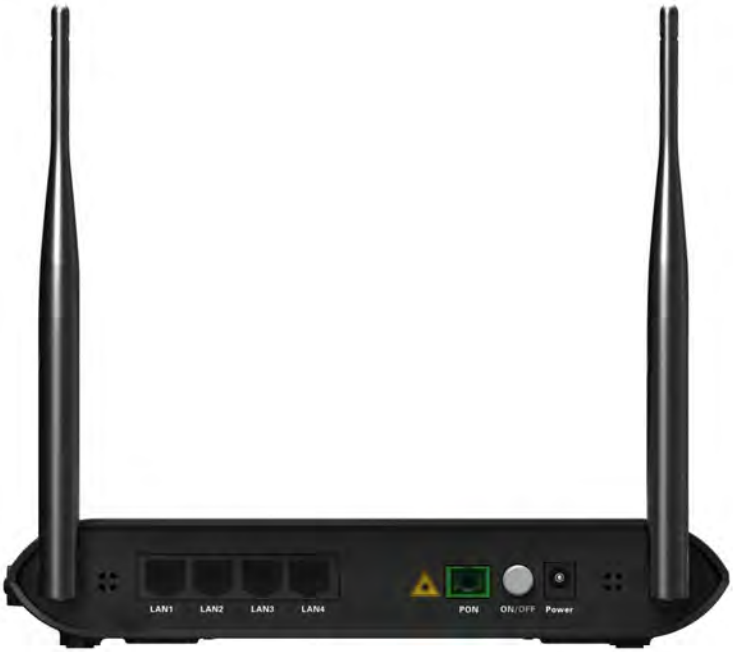


Figure 3.9 Rear Panel of the AN5506-04-DG

The side panel of the AN5506-04-DG is shown in Figure 3.10.

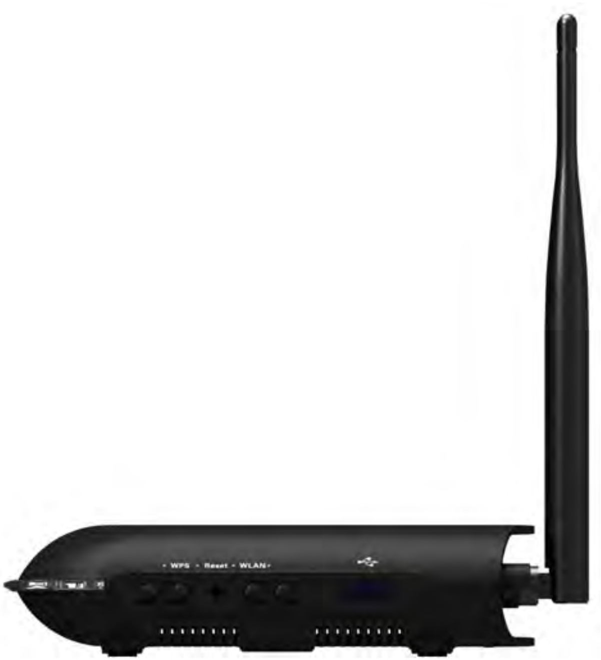


Figure 3.10 Side Panel of the AN5506-04-DG

Equipment Specifications

The AN5506-04-DG specifications include technical parameters and specifications. See Table 3.10 for the technical parameters and see Table 3.11 for the specifications.

Table 3.10 Technical Parameters of the AN5506-04-DG

Type	Item	Description
Service parameters	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports IGMP Snooping protocol.
		Supports IGMP v1/v2/v3.

Table 3.10 Technical Parameters of the AN5506-04-DG (Continued)

Type	Item	Description
	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 user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining user IP address using PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports downlink data using the AES-128 algorithm for encryption.
	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.

Table 3.10 Technical Parameters of the AN5506-04-DG (Continued)

Type	Item	Description
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 four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K
	Wi-Fi Interface	2.4GHz; supports the 802.11b/g/n mode.
		Supports four SSIDs and thirteen working channels; supports automatic rate adjustment and launched power adjustment.
		Supports the OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK authentication modes. Supports the TKIP, AES and TKIPAES encryption modes.
	USB interface	Provides one USB interface. Supports USB2.0 / USB1.1.

Table 3.11 Specifications of the AN5506-04-DG

Type	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth).
	Wall mounting hole distance	121mm
	Weight	About 383g (5dB antenna)

Table 3.11 Specifications of the AN5506-04-DG (Continued)

Type	Item	Description
Power supply parameters	DC	DC 12 V/1.5A
Power consumption parameters	-	＜10W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation).

Indicator LED Description

See Table 3.12 for the description of indicator LEDs on the AN5506-04-DG.

Table 3.12 Description of Indicator LEDs on the AN5506-04-DG

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.

Table 3.12 Description of Indicator LEDs on the AN5506-04-DG (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LAN1 to LAN4	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.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.
WIFI	Wireless signal status indicator LED	Green	ON	The wireless interface is enabled.
			Blinking	The interface is transmitting / receiving data.
			OFF	The wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled and connected to the device.
			Blinking	WPS is in use for relevant negotiation.
			OFF	WPS is not enabled or not connected to device.

3.5 Introduction to the AN5506-04-F

The AN5506-04-F is an FTTH-type 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 AN5506-04-F is shown in Figure 3.11.

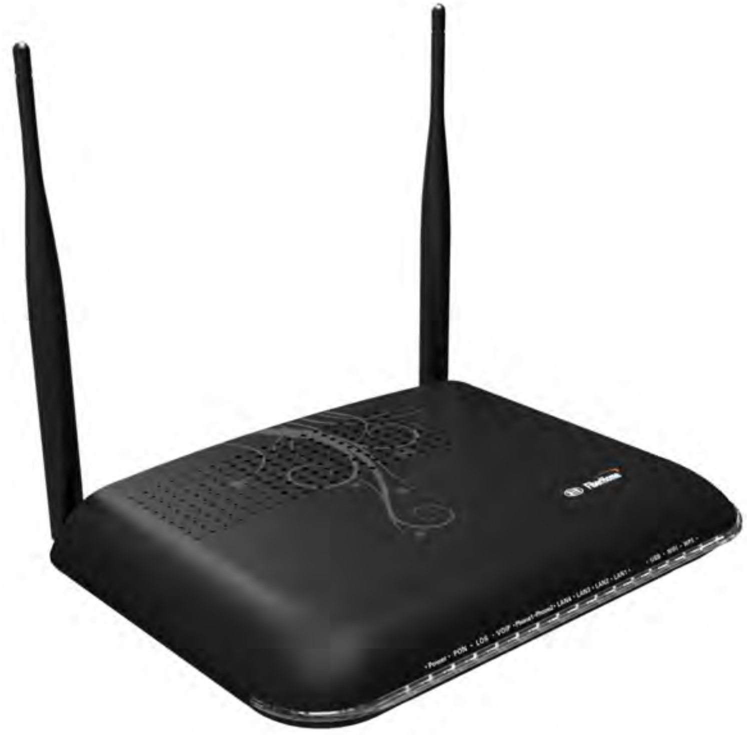


Figure 3.11 Overall Appearance of the AN5506-04-F

The rear panel of the AN5506-04-F is shown in Figure 3.12.

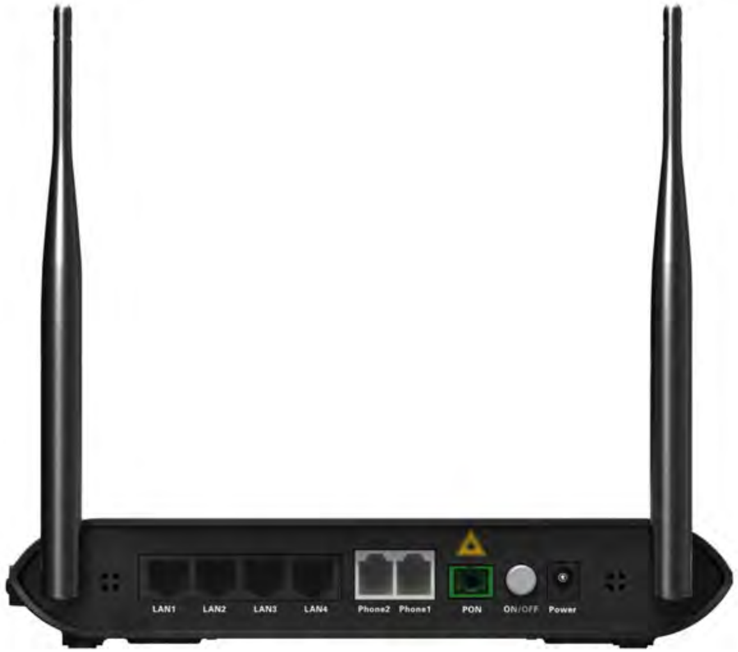


Figure 3.12 Rear Panel of the AN5506-04-F

The side panel of the AN5506-04-F is shown in Figure 3.13.

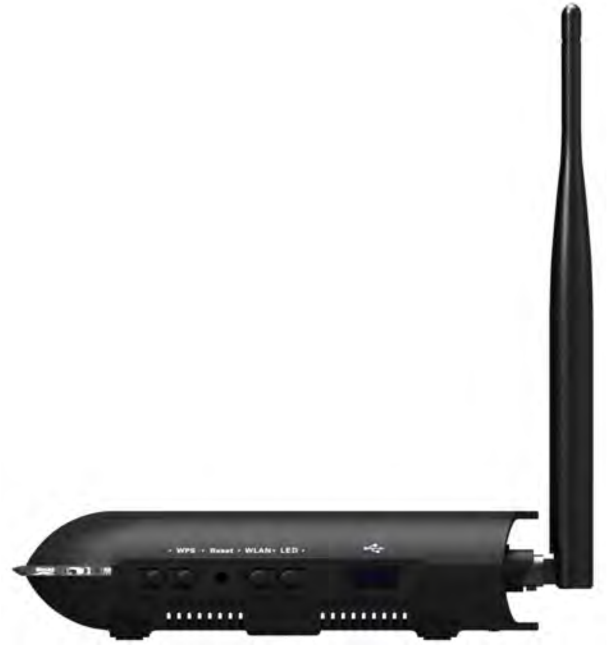


Figure 3.13 Side Panel of the AN5506-04-F

Equipment Specifications

The AN5506-04-F specifications include technical parameters and specifications. See Table 3.13 for the technical parameters and see Table 3.14 for the specifications.

Table 3.13 Technical Parameters of the AN5506-04-F

Type	**Item**	**Description**
Service parameters	Voice	Supports the protocols H.248 and SIP.
		Supports the speech encoding modes such as G. 711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in tag / untag mode.

Table 3.13 Technical Parameters of the AN5506-04-F (Continued)

Type	Item	Description
		Supports up to 4095 VLANs.
	Multicast	Supports 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 user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining user IP address using PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports downlink data using the AES-128 algorithm for encryption.
	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.

Table 3.13 Technical Parameters of the AN5506-04-F (Continued)

Type	Item	Description
		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.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100 auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K
	Phone interface	Provides two phone interfaces (RJ-11 interfaces).
	Wi-Fi Interface	2.4GHz; supports the 802.11b/g/n mode.
		Supports four SSIDs and thirteen working channels; supports automatic rate adjustment and launched power adjustment.
		Supports the OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK authentication modes. Supports the TKIP, AES and TKIPAES encryption modes.
	USB interface	Provides one USB interface. Supports USB2.0 / USB1.1.

Table 3.14 Specifications of the AN5506-04-F

Type	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth)
	Wall mounting hole distance	121mm
	Weight	About 409g (5dB antenna)
Power supply parameters	DC	DC 12 V/1.5A
Power consumption parameters	-	＜12W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation)

Indicator LED Description

See Table 3.15 for the description of indicator LEDs on the AN5506-04-F.

Table 3.15 Description of Indicator LEDs on the AN5506-04-F

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.

Table 3.15 Description of Indicator LEDs on the AN5506-04-F (Continued)

Indicator LED	Meaning	Color	Status	Status Description
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
VOIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Phone1, Phone2	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.
LAN1 to LAN4	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.

Table 3.15 Description of Indicator LEDs on the AN5506-04-F (Continued)

Indicator LED	**Meaning**	**Color**	**Status**	**Status Description**
			OFF	The interface is not connected to the user terminal.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.
WIFI	Wireless signal status indicator LED	Green	ON	The wireless interface is enabled.
			Blinking	The interface is transmitting / receiving data.
			OFF	The wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled and connected to the device.
			Blinking	WPS is in use for relevant negotiation.
			OFF	WPS is not enabled or not connected to device.

3.6 Introduction to the AN5506-04-FG

The AN5506-04-FG is an FTTH-type 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 AN5506-04-FG is shown in Figure 3.14.

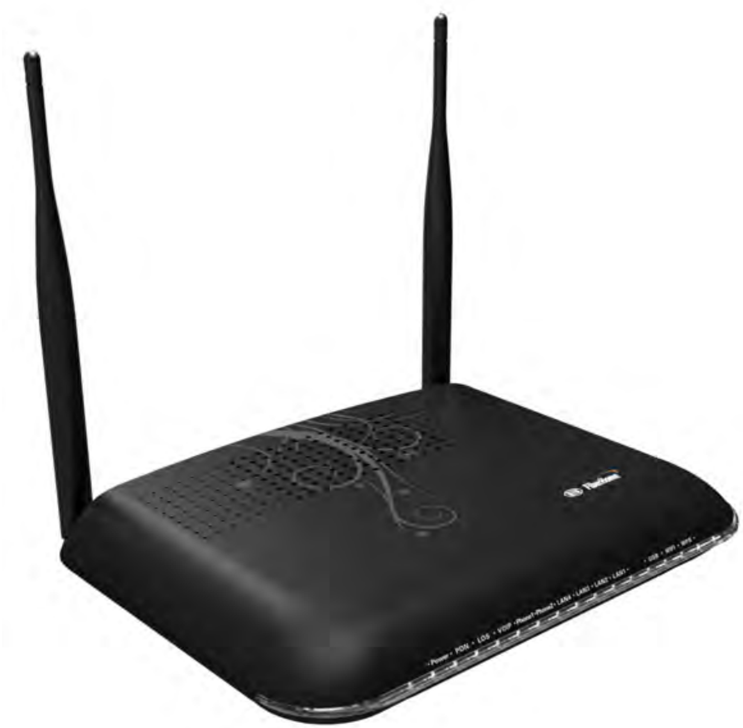


Figure 3.14 Overall Appearance of the AN5506-04-FG

The rear panel of the AN5506-04-FG is shown in Figure 3.15.

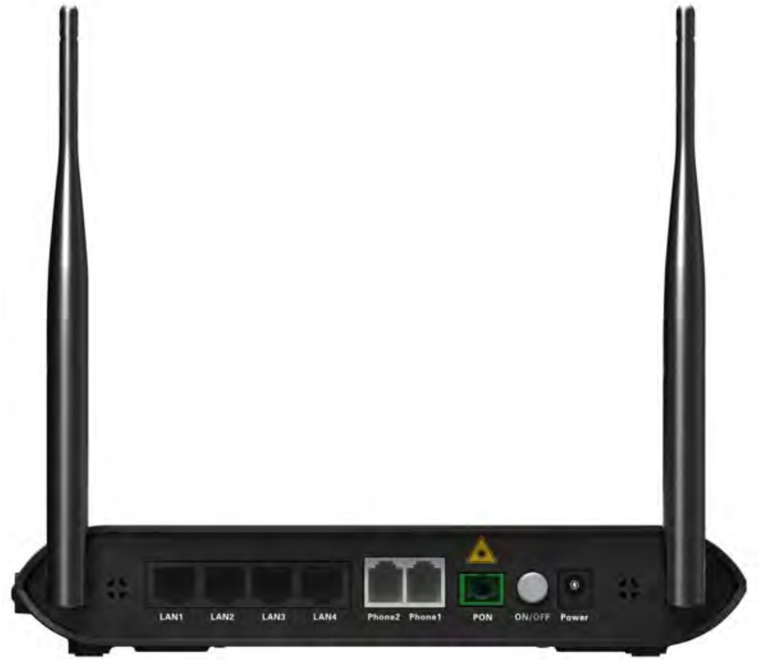


Figure 3.15 Rear Panel of the AN5506-04-FG

The side panel of the AN5506-04-FG is shown in Figure 3.16.

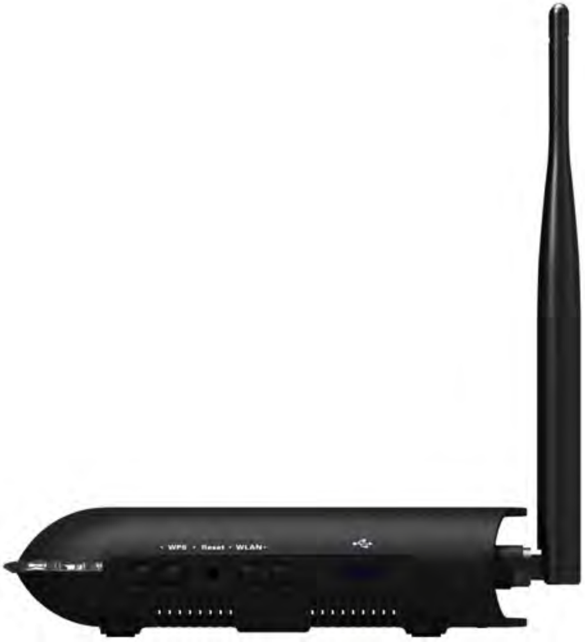


Figure 3.16 Side Panel of the AN5506-04-FG

Equipment Specifications

The AN5506-04-FG specifications include technical parameters and specifications. See Table 3.16 for the technical parameters and see Table 3.17 for the specifications.

Table 3.16 Technical Parameters of the AN5506-04-FG

Type	Item	Description
Service parameters	Voice	Supports the protocols H.248 and SIP.
		Supports the speech encoding modes such as G.711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.

Table 3.16 Technical Parameters of the AN5506-04-FG (Continued)

Type	Item	Description
		Supports joining 802.1Q VLAN in tag / untag mode.
		Supports up to 4095 VLANs.
	Multicast	Supports 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 user IP address using DHCP mode; supports DHCP Option82 reporting the physical location information of the Ethernet interface.
		Supports obtaining user IP address using PPPoE mode; supports the PPPoE+ function, used to identify users accurately.
		Supports downlink data using the AES-128 algorithm for encryption.
	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.

Table 3.16 Technical Parameters of the AN5506-04-FG (Continued)

Type	**Item**	**Description**
		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.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K
	Phone interface	Provides two phone interfaces (RJ-11 interfaces).
	Wi-Fi Interface	2.4GHz; supports the 802.11b/g/n mode.
		Supports four SSIDs and thirteen working channels; supports automatic rate adjustment and launched power adjustment.

Table 3.16 Technical Parameters of the AN5506-04-FG (Continued)

Type	Item	Description
		Supports the OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK authentication modes. Supports the TKIP, AES and TKIPAES encryption modes.
	USB interface	Provides one USB interface. Supports USB2.0 / USB1.1.

Table 3.17 Specifications of the AN5506-04-FG

Type	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth)
	Wall mounting hole distance	121mm
	Weight	About 409g (5dB antenna)
Power supply parameters	DC	DC 12 V/1.5A
Power consumption parameters	-	＜12W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation)

Indicator LED Description

See Table 3.18 for the description of indicator LEDs on the AN5506-04-FG.

Table 3.18 Description of Indicator LEDs on the AN5506-04-FG

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
VOIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Phone1, Phone2	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.
LAN1 to LAN4	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.

Table 3.18 Description of Indicator LEDs on the AN5506-04-FG (Continued)

Indicator LED	Meaning	Color	Status	Status Description
			OFF	The interface is not connected to the user terminal.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.
WIFI	Wireless signal status indicator LED	Green	ON	The wireless interface is enabled.
			Blinking	The interface is transmitting / receiving data.
			OFF	The wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled and connected to the device.
			Blinking	WPS is in use for relevant negotiation.
			OFF	WPS is not enabled or not connected to device.

3.7 Introduction to the AN5506-04-FS

The AN5506-04-FS is an FTTH-type 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 AN5506-04-FS is shown in Figure 3.17.

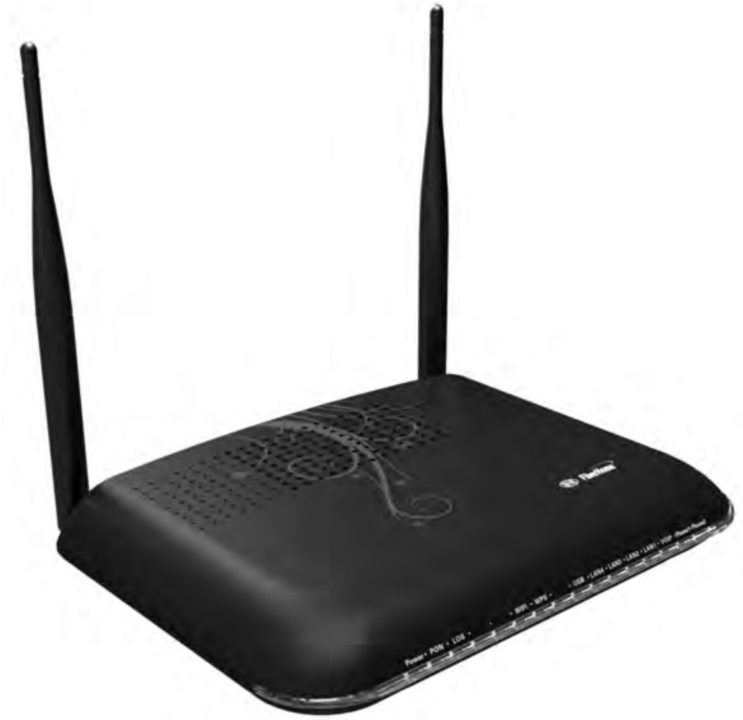


Figure 3.17 Overall Appearance of the AN5506-04-FS

The rear panel of the AN5506-04-FS is shown in Figure 3.18.

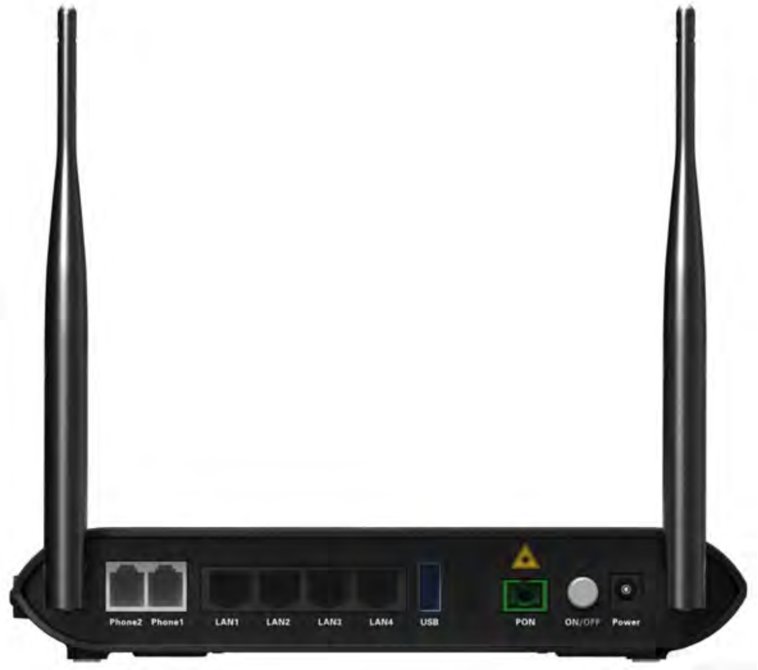


Figure 3.18 Rear Panel of the AN5506-04-FS

The side panel of the AN5506-04-FS is shown in Figure 3.19.

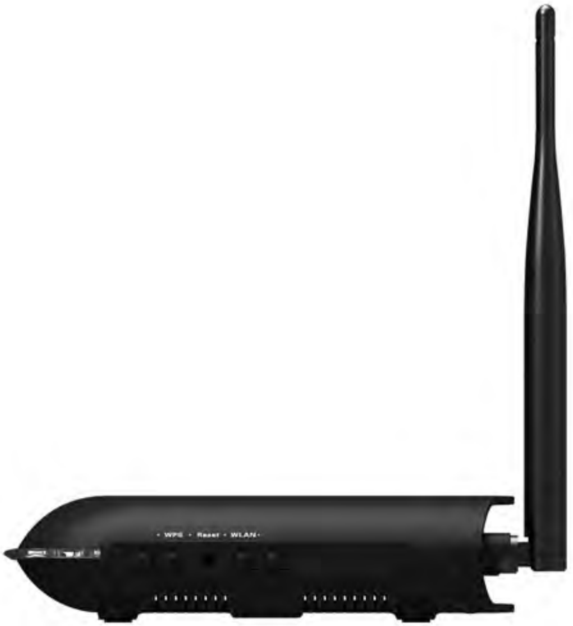


Figure 3.19 Side Panel of the AN5506-04-FS

Equipment Specifications

The AN5506-04-FS specifications include technical parameters and specifications. See Table 3.19 for the technical parameters and see Table 3.20 for the specifications.

Table 3.19 Technical Parameters of the AN5506-04-FS

Category	Item	Description
Service parameters	Voice	Supports the protocols H.248 and SIP.
		Supports the speech encoding modes such as G.711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.
		Supports joining 802.1Q VLAN in the tag / untag mode.

Table 3.19 Technical Parameters of the AN5506-04-FS (Continued)

Category	Item	Description
		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 user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining 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.

Table 3.19 Technical Parameters of the AN5506-04-FS (Continued)

Category	Item	Description
		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.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K
	Phone interface	Provides two phone interfaces (RJ-11 interfaces).
	Wi-Fi interface	2.4GHz; supports the 802.11b/g/n mode.
		Supports four SSIDs and thirteen working channels; supports automatic rate adjustment and launched power adjustment.
		Supports the OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK authentication modes. Supports the TKIP, AES and TKIPAES encryption modes.
	USB interface	Provides one USB interface; supports USB2. 0 / USB1.1.

Table 3.20 Specifications of the AN5506-04-FS

Category	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth)
	Wall mounting hole distance	121mm
	Weight	About 409g (5dB antenna)
Power supply parameter	DC	DC 12 V/1.5A
Power consumption parameter	-	＜12W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation)

Indicator LED Description

See Table 3.21 for the description of indicator LEDs on the AN5506-04-FS.

Table 3.21 Description of Indicator LEDs on the AN5506-04-FS

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.

Table 3.21 Description of Indicator LEDs on the AN5506-04-FS (Continued)

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	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
WIFI	Wireless signal status indicator LED	Green	ON	The wireless interface is enabled.
			Blinking	The interface is transmitting / receiving data.
			OFF	The wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled and connected to the device.
			Blinking	WPS is in use for relevant negotiation.
			OFF	WPS is not enabled or not connected to device.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.

Table 3.21 Description of Indicator LEDs on the AN5506-04-FS (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LAN1 to LAN4	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.
VOIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Phone1, Phone2	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.

3.8 Introduction to the AN5506-04-GG

The AN5506-04-GG is an FTTH-type 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 AN5506-04-GG is shown in Figure 3.20.

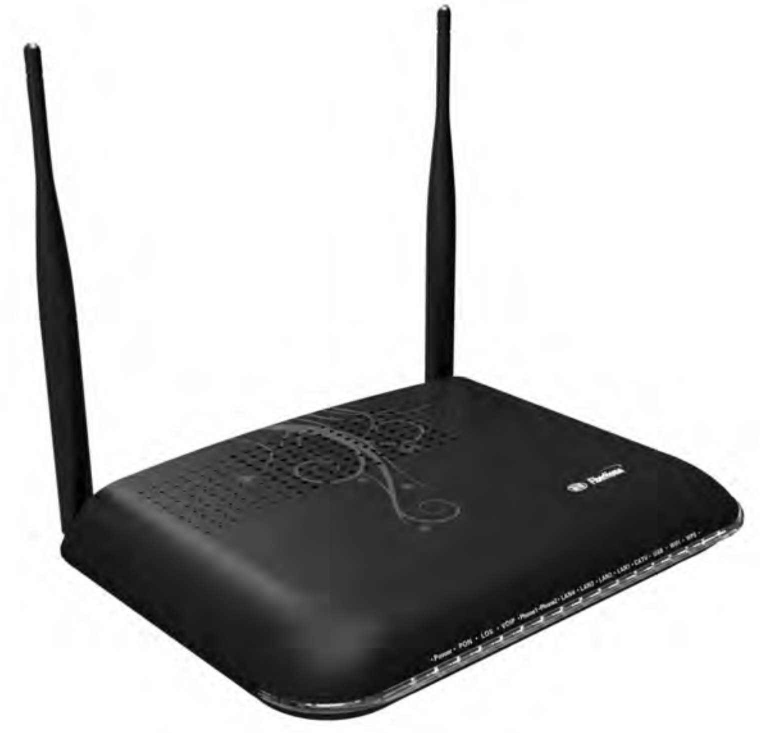


Figure 3.20 Overall Appearance of the AN5506-04-GG

The rear panel of the AN5506-04-GG is shown in Figure 3.21.

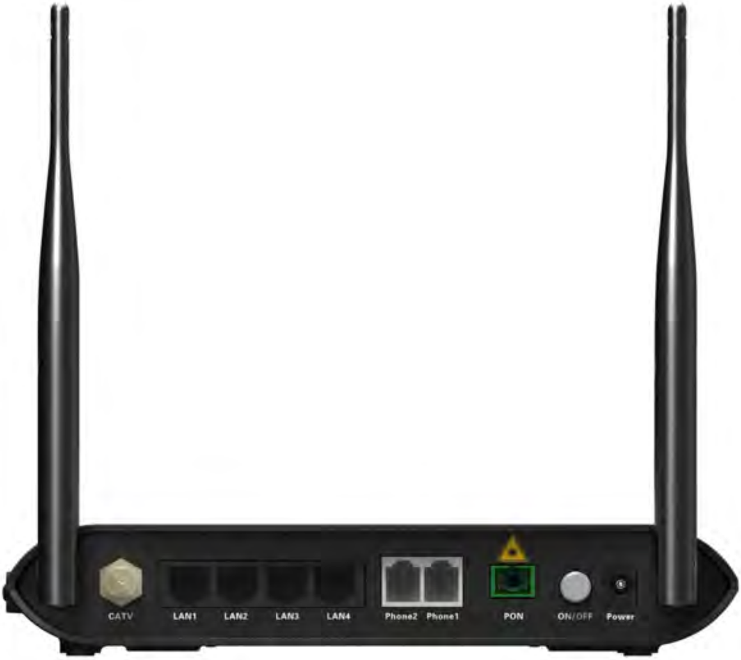


Figure 3.21 Rear Panel of the AN5506-04-GG

The side panel of the AN5506-04-GG is shown in Figure 3.22.

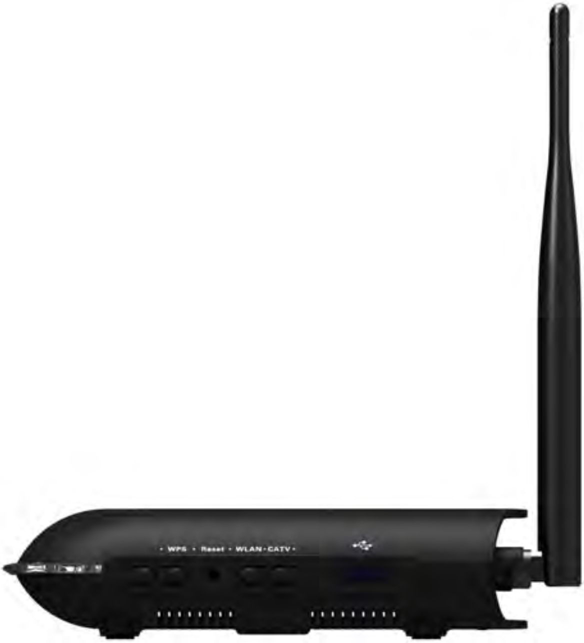


Figure 3.22 Side Panel of the AN5506-04-GG

Equipment Specifications

The AN5506-04-GG specifications include technical parameters and specifications. See Table 3.22 for the technical parameters and see Table 3.23 for the specifications.

Table 3.22 Technical Parameters of the AN5506-04-GG

Type	Item	Description
Service parameters	Voice	Supports the protocols H.248 and SIP.
		Supports the speech encoding modes such as G.711, G.723 and G.729.
	VLAN	Supports the IEEE 802.1Q VLAN standard.

Table 3.22 Technical Parameters of the AN5506-04-GG (Continued)

Type	Item	Description
		Supports joining 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 user IP address in DHCP mode; supports reporting physical location of the Ethernet interface using DHCP Option82.
		Supports obtaining 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.

Table 3.22 Technical Parameters of the AN5506-04-GG (Continued)

Type	Item	Description
		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.
		Supports Class B+, with receiving sensitivity less than -29 dBm.
User side interface	LAN interface	Provides four LAN interfaces (RJ-45 interfaces), supporting full-duplex or half-duplex and 10/100/1000M auto negotiation. The maximum transmission distance is 100m.
		MAC address capacity: 1K
	Phone interface	Provides two phone interfaces (RJ-11 interfaces).
	Wi-Fi interface	2.4GHz; supports the 802.11b/g/n mode.
		Supports four SSIDs and thirteen working channels; supports automatic rate adjustment and launched power adjustment.

Table 3.22 Technical Parameters of the AN5506-04-GG (Continued)

Type	Item	Description
		Supports the OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK authentication modes. Supports the TKIP, AES and TKIPAES encryption modes.
	USB interface	Provides one USB interface; supports USB2.0 / USB1.1.
	CATV interface	Provides one CATV interface (RF interface). RF output ＞18dBmV.

Table 3.23 Specifications of the AN5506-04-GG

Type	Item	Description
Mechanical parameters	Dimensions	36mm × 211mm × 154mm (height x width x depth).
	Wall mounting hole distance	121mm
	Weight	About 460g (5dB antenna)
Power supply parameters	DC	DC 12 V/1.5A
Power consumption parameters	-	＜12W
Environment parameters	Operating temperature	-5℃ to 45℃
	Storage temperature	-40℃ to 70℃
	Environmental humidity	10% to 90% (no condensation).

Indicator LED Description

See Table 3.24 for the description of indicator LEDs on the AN5506-04-GG.

Table 3.24 Description of Indicator LEDs on the AN5506-04-GG

Indicator LED	Meaning	Color	Status	Status Description
Power	Power status indicator LED	Green	ON	The device is powered on.
			OFF	The device is not powered on.
PON	Register status indicator LED	Green	ON	The ONU is activated.
			OFF	Activation of the ONU is not yet started.
LOS	Optical signal status indicator LED	Red	Blinking	The device has not received the optical signal.
			OFF	The device has received the optical signal.
VOIP	Voice service register status indicator LED	Green	ON	The device is registered in the softswitch system.
			OFF	The device is not registered in the softswitch system.
Phone1, Phone2	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.

Table 3.24 Description of Indicator LEDs on the AN5506-04-GG (Continued)

Indicator LED	Meaning	Color	Status	Status Description
LAN1 to LAN4	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.
CATV	CATV interface indicator LED	Green	ON	The CATV function is enabled and the CATV signal can be received normally.
			Blinking	The CATV function is enabled and the CATV signal is poor.
			OFF	The CATV function is not enabled, the CATV signal is not received or the signal is poor.
USB	USB indicator LED	Green	ON	The USB is connected.
			OFF	The USB is not connected.
WIFI	Wireless signal status indicator LED	Green	ON	The wireless interface is enabled.
			Blinking	The interface is transmitting / receiving data.
			OFF	The wireless interface is disabled.
WPS	WPS status indicator LED	Green	ON	WPS is enabled and connected to the device.
			Blinking	WPS is in use for relevant negotiation.

Table 3.24 Description of Indicator LEDs on the AN5506-04-GG (Continued)

Indicator LED	Meaning	Color	Status	Status Description
			OFF	WPS is not enabled or not connected to device.

4 Web Configuration Guide

The following introduces the Web GUI of the AN5506-04 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 relevant OLT configuration guide.

4.1 Logging into 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

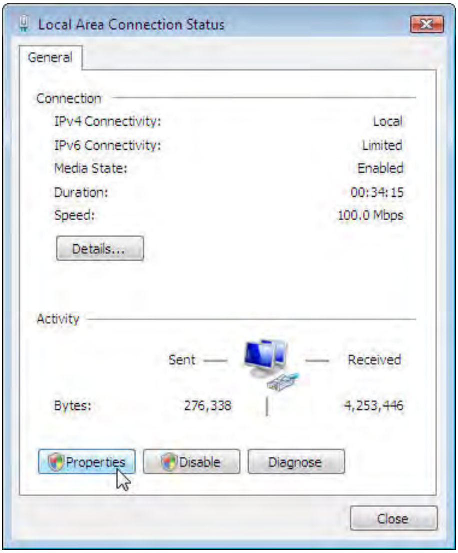
Item	Description
Username and password	Factory default value: ◆ Administrator ▸ Username: admin ▸ Password: admin

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

Item	Description
	◆ Common user ▸ AN5506-04-A / AN5506-04-B: username: useradmin; password: user1234 ▸ AN5506-04-CG/AN5506-04-DG/AN5506-04-F/ AN5506-04-FG/AN5506-04-FS/AN5506-04-GG: See the label at the bottom of the device. **Note: Some operators customized the username and password, so that the default username and password may have been modified. In this case, ask local operator for the administrator information. For common user, 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 ONU	Factory default value: ◆ IP address: 192.168.1.1 ◆ Subnet mask: 255.255.255.0 **Note: Some operators have customized IP address requirement, so the system default management IP address may be different from the IP address above. In this case, refer to the *User Manual* attached to the equipment or the label at the bottom of the equipment.**
The IP address and the subnet mask of the user computer	◆ 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. ▸ 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**.



Local Area Connection Status

General

Connection

IPv4 Connectivity: Local

IPv6 Connectivity: Limited

Media State: Enabled

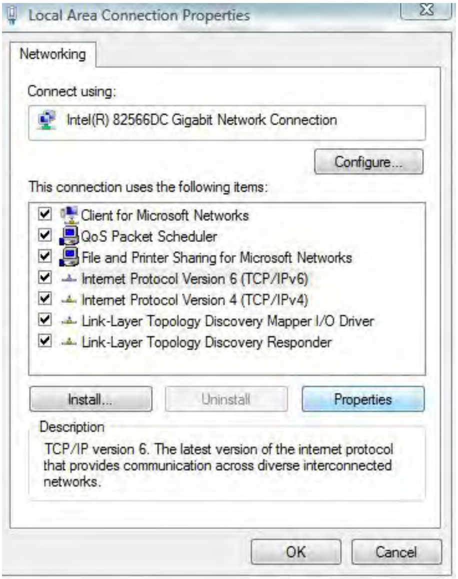
Duration: 00:34:15

Speed: 100.0 Mbps

Activity

Bytes: Sent 276,338 Received 4,253,446

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



Local Area Connection Properties

Networking

Connect using:

Intel(R) 82566DC Gigabit Network Connection

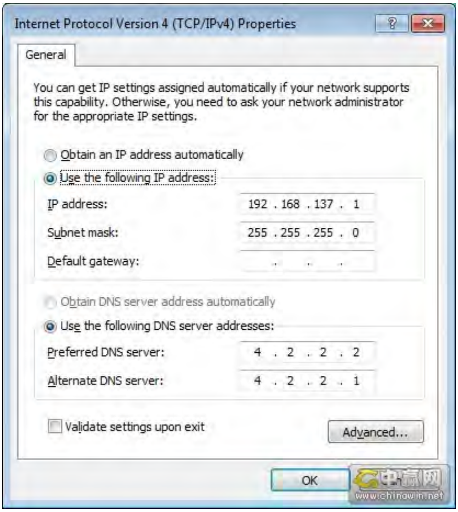
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The latest version of the internet protocol that provides communication across diverse interconnected networks.

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).



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 137 . 1

Subnet mask: 255 . 255 . 255 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 4 . 2 . 2 . 2

Alternate DNS server: 4 . 2 . 2 . 1

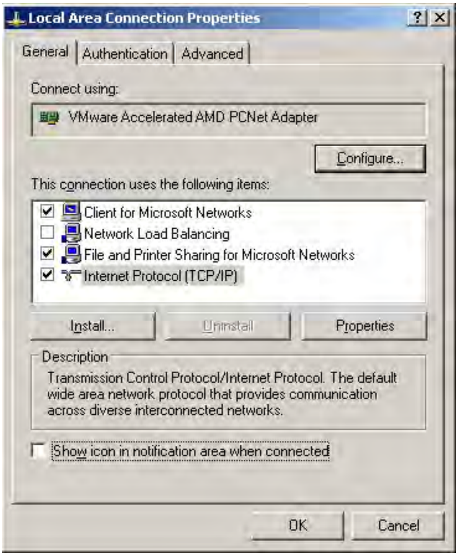
□ Validate settings upon exit

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

- The operation method of the Windows XP operating system is 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.



Local Area Connection Properties

Connect using:

VMware Accelerated AMD PCNet Adapter

This connection uses the following items:

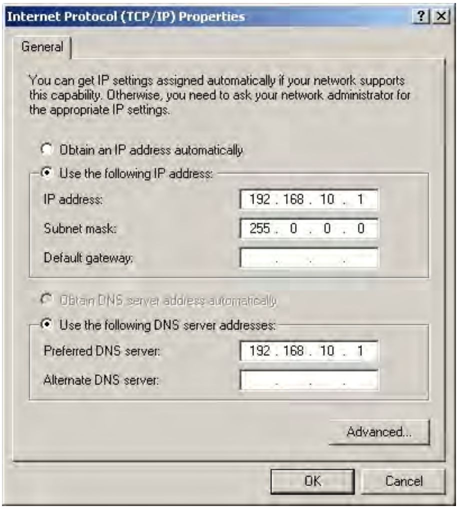
☑ Client for Microsoft Networks
☐ Network Load Balancing
☑ File and Printer Sharing for Microsoft Networks
☑ Internet Protocol (TCP/IP)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

☐ Show icon in notification area when connected

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).



Internet Protocol (TCP/IP) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 10 . 1

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 10 . 1

Alternate DNS server: . . .

d) 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 username and password in the login dialog box. Access the Web GUI after the password is authenticated.

Caution:

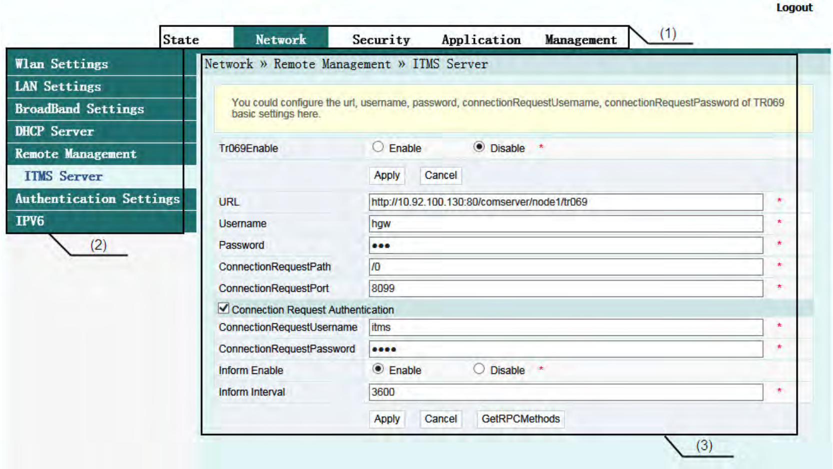
The system will log out automatically if no operation is performed in five minutes.

Web Configuration GUI Layout

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

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



Network » Remote Management » ITMS Server

You could configure the url, username, password, connectionRequestUsername, connectionRequestPassword of TR069 basic settings here.

Tr069Enable	○ Enable ● Disable	*
URL	http://10.92.100.130:80/comserver/node1/tr069	*
Username	hgw	*
Password	•••	*
ConnectionRequestPath	/0	*
ConnectionRequestPort	8099	*
☑ Connection Request Authentication		
ConnectionRequestUsername	itms	*
ConnectionRequestPassword	••••	*
Inform Enable	● Enable ○ Disable	*
Inform Interval	3600	*

(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 AN5506-04 Series ONUs. The following illustrates how an administrator user (admin) of the AN5506-04-GG logs into the Web GUI (version RP2560). 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.

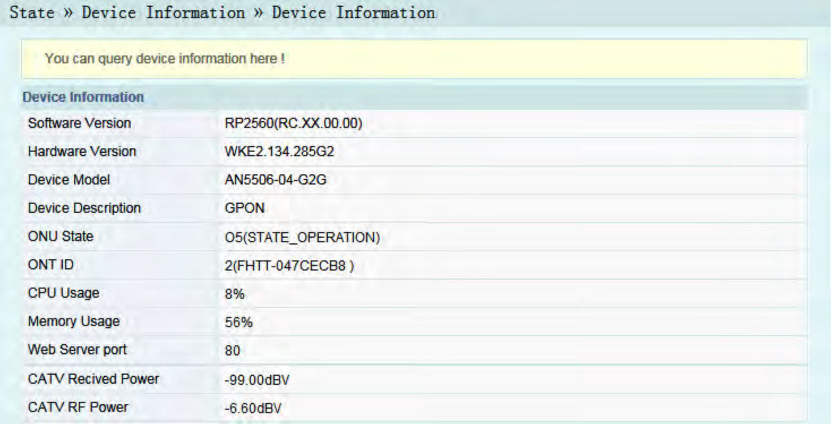
- The **State** tab.
- **WLAN Settings** in the **Network** tab.
- **Maintenance Account** and **Device Reboot** in the **Management** tab.

4.2 Status

The following introduces how to view the ONU basic information (including device information, WAN side status, LAN side status, optical power status, voice status and wireless network status) in the Web GUI.

4.2.1 Device 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 !

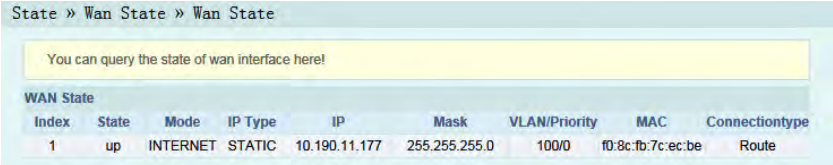
Device Information

Software Version	RP2560(RC.XX.00.00)
Hardware Version	WKE2.134.285G2
Device Model	AN5506-04-G2G
Device Description	GPON
ONU State	O5(STATE_OPERATION)
ONT ID	2(FHTT-047CECB8)
CPU Usage	8%
Memory Usage	56%
Web Server port	80
CATV Recived Power	-99.00dBV
CATV RF Power	-6.60dBV

Figure 4.2 Device 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	VLAN/Priority	MAC	Connectiontype
1	up	INTERNET	STATIC	10.190.11.177	255.255.255.0	100/0	f0:8c:fb:7c:ec:be	Route

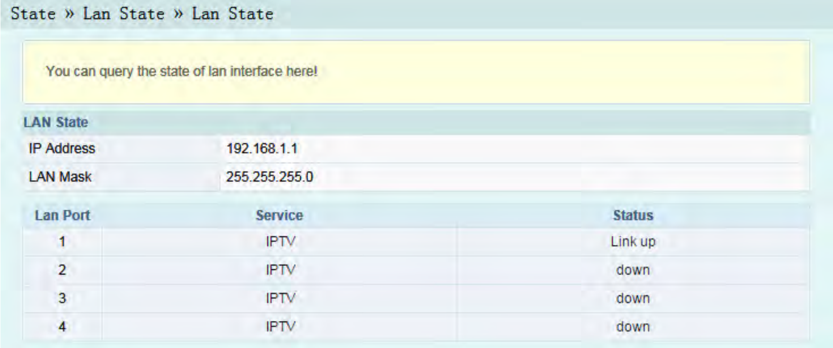
Figure 4.3 WAN Side Status

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

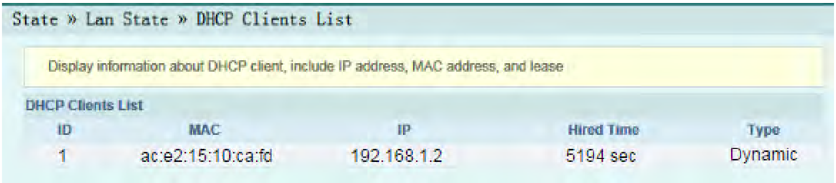
IP Address	192.168.1.1
LAN Mask	255.255.255.0

Lan Port	Service	Status
1	IPTV	Link up
2	IPTV	down
3	IPTV	down
4	IPTV	down

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

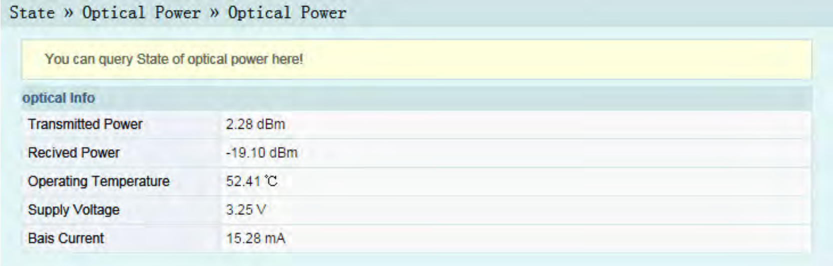
DHCP Clients List

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!

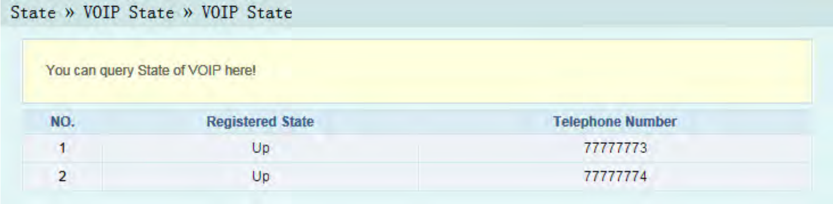
optical Info

Transmitted Power	2.28 dBm
Recived Power	-19.10 dBm
Operating Temperature	52.41 ℃
Supply Voltage	3.25 V
Bais Current	15.28 mA

Figure 4.6 Optical Power Status

4.2.5 Voice Status

Select **State** in the navigation bar and select **VOIP State** in the left link bar to view the information such as the the user status and phone number. See Figure 4.7.



State » VOIP State » VOIP State

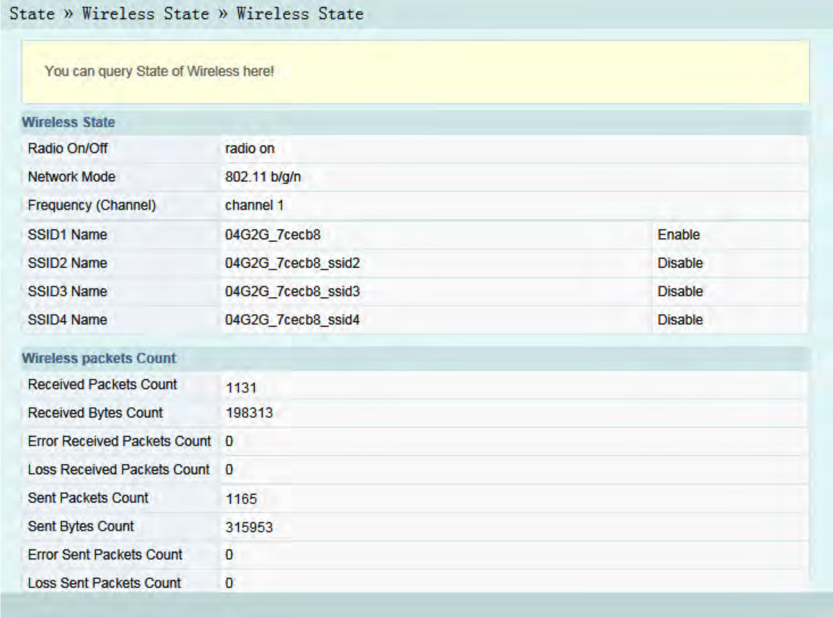
You can query State of VOIP here!

NO.	Registered State	Telephone Number
1	Up	77777773
2	Up	77777774

Figure 4.7 Voice Status

4.2.6 Wireless Network Status

Select **State** in the navigation bar. Select **Wireless State** in the left link bar to view the information of the wireless network, such as network mode, band, SSID and wireless packet statistics. See Figure 4.8.



State » Wireless State » Wireless State

You can query State of Wireless here!

Wireless State

Radio On/Off	radio on	
Network Mode	802.11 b/g/n	
Frequency (Channel)	channel 1	
SSID1 Name	04G2G_7cecb8	Enable
SSID2 Name	04G2G_7cecb8_ssid2	Disable
SSID3 Name	04G2G_7cecb8_ssid3	Disable
SSID4 Name	04G2G_7cecb8_ssid4	Disable

Wireless packets Count

Received Packets Count	1131
Received Bytes Count	198313
Error Received Packets Count	0
Loss Received Packets Count	0
Sent Packets Count	1165
Sent Bytes Count	315953
Error Sent Packets Count	0
Loss Sent Packets Count	0

Figure 4.8 Wireless Network Status

4.3 Network

The following introduces how to configure the WLAN, LAN, broadband, DHCP server, remote management, authentication and IPv6 in the Web GUI.

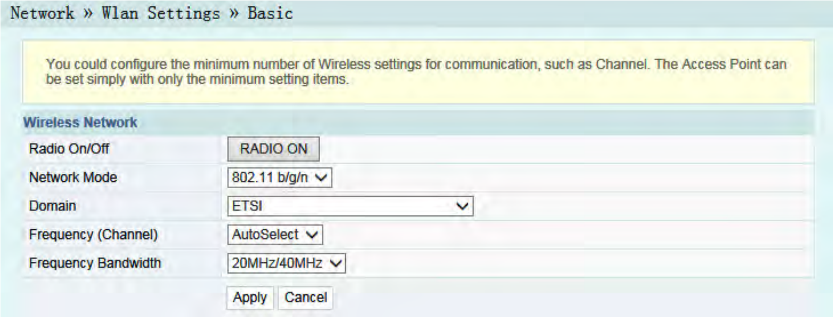
4.3.1 WLAN Settings

The following introduces how to configure basic and advanced parameters of the wireless network, WIFI control and view of WIFI user list on the Web page.

4.3.1.1 Basic Configuration

Configure the parameters of the wireless network such as the switch, network mode, area, band and frequency bandwidth.

1. Select **Network** in the navigation bar and select **Wlan Settings →Basic** in the left link bar to open the basic setting tab of the wireless access service, as shown in Figure 4.9.



Network » Wlan Settings » Basic

You could configure the minimum number of Wireless settings for communication, such as Channel. The Access Point can be set simply with only the minimum setting items.

Wireless Network

Radio On/Off	RADIO ON
Network Mode	802.11 b/g/n
Domain	ETSI
Frequency (Channel)	AutoSelect
Frequency Bandwidth	20MHz/40MHz

Figure 4.9 Basic Configuration of Wireless Network

2. Configure the basic parameters of the wireless network. See Table 4.2 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 4.2 Basic Parameters of the Wireless Network

Item	**Description**
Radio ON/OFF	Enables or disables the WLAN service. RADIO ON: the wireless network is enabled; RADIO OFF: the wireless network is disabled.
Network Mode	The mode supported by the wireless network. The values include: 802.11b, 802.11g, 802.11b/g, 802.11n and 802.11b/g/n. The default setting is 802.11b/g/n.
Domain	Nation.

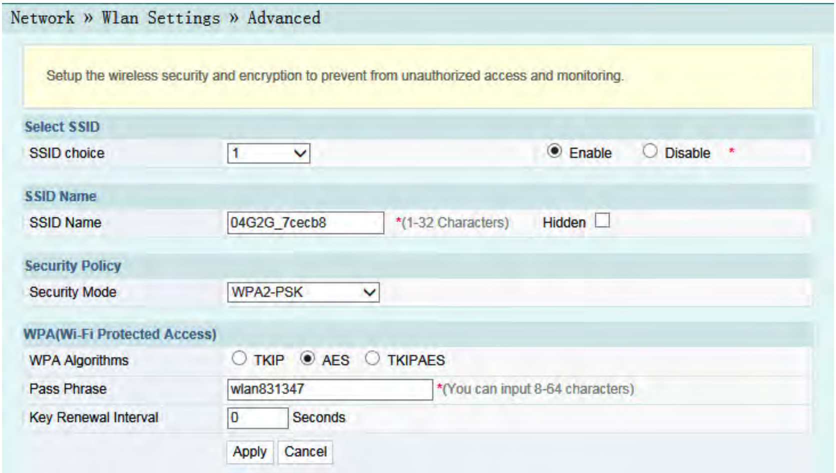
Table 4.2 Basic Parameters of the Wireless Network (Continued)

Item	Description
Frequency (Channel)	The channel used for communication between the wireless access point and the wireless station. The options includes AutoSelect, Channel1 to Channel13. The default setting is AutoSelect.
Frequency Bandwidth	The width of wireless band. The values include 20MHz/40MHz, 20MHz and 40MHz. The default setting is 20MHz/40MHz.

4.3.1.2 Advanced Configuration

Configure the parameters of the wireless network, such as the SSID, password, security mode and algorithm.

1. Select **Network** in the navigation bar and select **Wlan Settings** →**Advanced** in the left link bar to open the advanced setting tab of the wireless access service, as shown in Figure 4.10.



Network » Wlan Settings » Advanced

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Select SSID

SSID choice	1	● Enable ○ Disable *

SSID Name

SSID Name	04G2G_7cecb8	*(1-32 Characters) Hidden □

Security Policy

Security Mode	WPA2-PSK

WPA(Wi-Fi Protected Access)

WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	wlan831347 *(You can input 8-64 characters)
Key Renewal Interval	0 Seconds

Figure 4.10 Advanced Settings of the Wireless Network

2. Configure the parameters of the wireless network, such as the SSID, password, security mode and algorithm. See Table 4.3 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 4.3 Advanced Setting Parameters of Wireless Network

Item	**Description**
SSID Choice	Select the SSID serial number. The value ranges from 1 to 4.
Enable / Disable	Enables or disables the corresponding SSID.
SSID Name	The wireless network name, used to identify different wireless networks.
Hidden	Select whether to hide the SSID. When the SSID is hidden, the wireless terminal cannot detect the wireless signals unless the SSID is entered.
Security Mode	The authentication mode of the wireless terminal requesting to access the wireless network. The options include OPEN, SHARED, WPA-PSK, WPA2-PSK and WPAPSKWPA2PSK. ◆ OPEN: Unencrypted. Any terminal can access to the wireless network, so that the security cannot be guaranteed. This mode is not advisable. ◆ SHARED: Based on the WEP encryption protocol, this mode uses the same key for the wireless access client end and the equipment side, and provides the security at the level equal to that of the wired LAN. It is a traditional WLAN security protocol. ◆ WPA-PSK: This mode is based on the WLAN security protocol, where a key is pre-configured for the wireless access client end. The equipment side authenticates the legality of the wireless access client end key by the 4-way handshake key agreement protocol. This provides a safer and more confidential wireless network service than WEP. ◆ WPA2-PSK: WPA2 is the second edition of WPA. ◆ WPAPSKWPA2PSK: the authentication mode combining

Table 4.3 Advanced Setting Parameters of Wireless Network (Continued)

Item	Description	
	WPA and WPA2.	
WPA Algorithms	The encryption algorithms include TKIP, AES and TKIPAES.	This item should be set if the authentication mode is WPA-PSK, WPA2-PSK or WPAPSKWPA2PS.
Pass Phrase	Enter the SSID key.	
Key Renewal Interval	Enter the time interval for key update (unit: s).	
Encrypt Type	Select to enable or disable the WEP encryption when the network authentication mode is OPEN.	
Default Key	Select Key1 to Key4; that is, select one of the four configured network keys.	This item should be configured when the authentication mode is OPEN and the WEP encryption is enabled or the authentication mode is SHARED.
WEP Key 1 to WEP Key 4	Enter the key value and select the key value type. At least enter the item selected in **Default Key**. ◆ If ASCII is selected, users should enter 5 to 13 characters for the key value. ◆ If Hex is selected, users should enter a hexadecimal figure containing 10 to 26 characters for the key value.	

Tip:

Pressing the **Apply** button will validate a single **SSID choice** configuration item. If users does not click **Apply** after modifying the SSID 1 setting, the modification will not take effect.

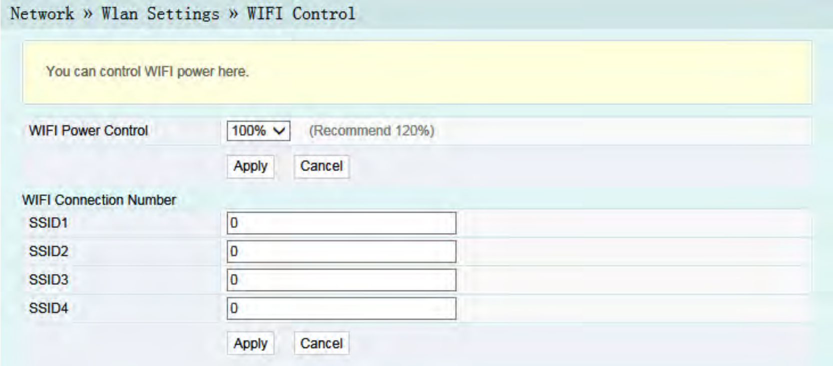
If the SSID1 setting is modified, the factory default wireless network account will be invalid.

If users lose the customized wireless network account, they can restore the factory default account (long press the Reset button for at least 5s).

4.3.1.3 WIFI Control

Configure the parameters of the wireless network, such as WIFI power and quantity of connected client ends.

1. Select **Network** in the navigation bar and select **Wlan Settings** →**WIFI Control** in the left link bar to open the WIFI control setting tab of the wireless access service, as shown in Figure 4.11.



Network » Wlan Settings » WIFI Control

You can control WIFI power here.

WIFI Power Control	100% (Recommend 120%)

WIFI Connection Number

SSID1	0
SSID2	0
SSID3	0
SSID4	0

Figure 4.11 WIFI Control

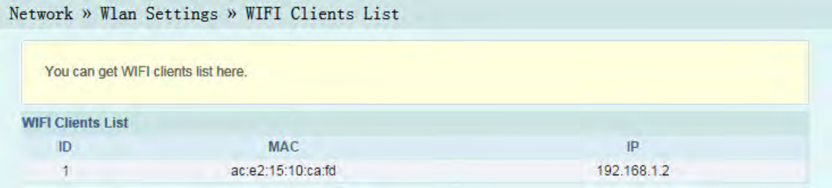
2. Configure the parameters of the wireless network, such as WIFI power and quantity of connected client ends. See Table 4.4 for the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 4.4 Parameters of WIFI Control

Item	**Description**
WIFI Power Control	The Tx power of the wireless signal. Larger value indicates wider signal coverage.
WIFI Connection Number	The maximum quantity of client ends supported by SSID, ranging from 0 to 32.

4.3.1.4 WIFI User List

Select **Network** in the navigation bar and select **Wlan Settings→ WIFI Client List** in the left link bar to view the list of client ends that connect to the ONU wireless network , as shown in Figure 4.12.



Network » Wlan Settings » WIFI Clients List

You can get WIFI clients list here.

WIFI Clients List

ID	MAC	IP
1	ac:e2:15:10:ca:fd	192.168.1.2

Figure 4.12 WIFI User List

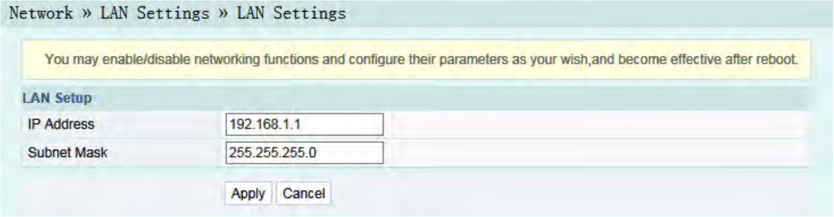
4.3.2 LAN Settings

The following introduces how to set the LAN and adjust the RF output level.

4.3.2.1 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 tab, as shown in Figure 4.13.



Network » LAN Settings » LAN Settings

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

LAN Setup

IP Address: 192.168.1.1

Subnet Mask: 255.255.255.0

Figure 4.13 LAN Settings

2. Configure the management IP address and subnet mask at the LAN side. See Table 4.5 for the parameter description.
3. Click **Apply** to save and apply the configuration.

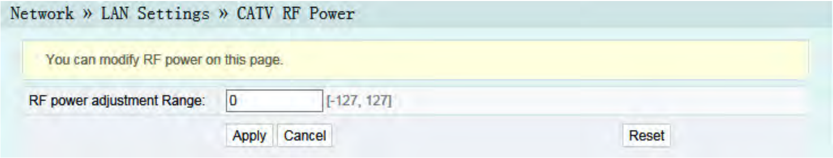
Table 4.5 Parameters of LAN Settings

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.

4.3.2.2 RF Output Level Adjustment

Configure the RF output level adjustment range.

1. Select **Network** in the navigation bar, and select **LAN Settings →CATV RF Power** in the left link bar to open the RF output level adjustment tab, as shown in Figure 4.14.



Network » LAN Settings » CATV RF Power

You can modify RF power on this page.

RF power adjustment Range: 0 [-127, 127]

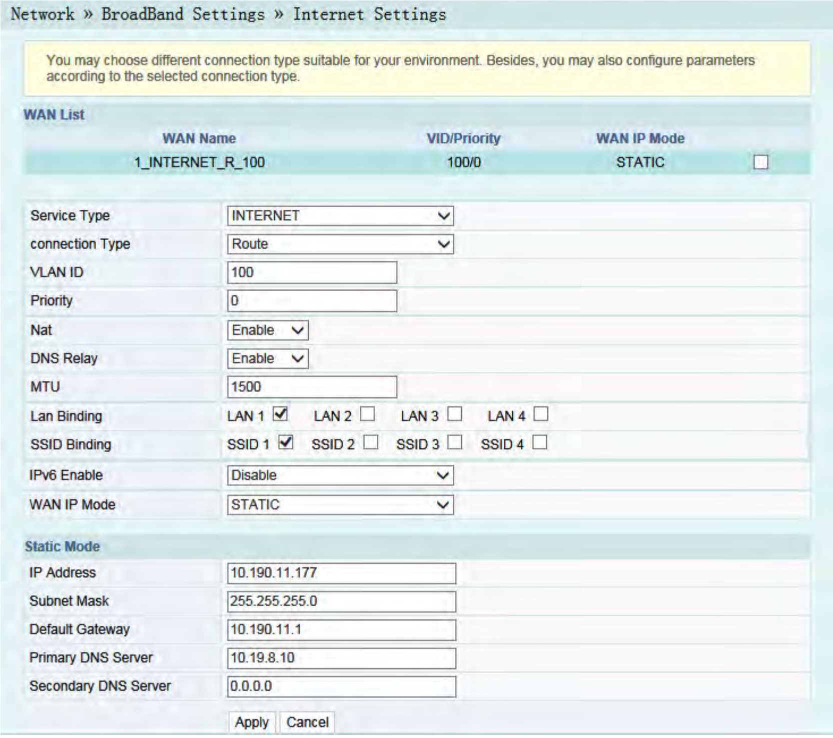
Figure 4.14 RF Output Level Adjustment

2. Enter the RF output level adjustment range. Click **Apply** to save and apply the configuration.
3. (Optional) Click **Reset** to restore to the default RF output level adjustment range.

4.3.3 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** in the left link bar to open the Broadband setting tab, as shown in Figure 4.15.



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 List

WAN Name	VID/Priority	WAN IP Mode	
1_INTERNET_R_100	100/0	STATIC	□

Service Type	INTERNET
connection Type	Route
VLAN ID	100
Priority	0
Nat	Enable
DNS Relay	Enable
MTU	1500
Lan Binding	LAN 1 ☑ LAN 2 □ LAN 3 □ LAN 4 □
SSID Binding	SSID 1 ☑ SSID 2 □ SSID 3 □ SSID 4 □
IPv6 Enable	Disable
WAN IP Mode	STATIC

Static Mode

IP Address	10.190.11.177
Subnet Mask	255.255.255.0
Default Gateway	10.190.11.1
Primary DNS Server	10.19.8.10
Secondary DNS Server	0.0.0.0

Figure 4.15 Broadband Setting

2. Configure parameters relevant to the broadband at the WAN side. Table 4.6 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 4.6 Parameters for Broadband 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.

Table 4.6 Parameters for Broadband Settings (Continued)

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td></td><td colspan="2">◆ multicast: this connection is applicable for TR069, voice 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 connection.</td></tr>
<tr><td>connection Type</td><td colspan="2">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, TR069_INTERNET, VOIP_INTERNET or Other.
◆ Route: the Layer 3 router connection mode. This connection mode can be used for all the service types except for multicast.</td></tr>
<tr><td>VLAN ID</td><td colspan="2">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.</td></tr>
<tr><td>Priority</td><td colspan="2">Sets the priority of the VLAN.</td></tr>
<tr><td>Nat</td><td>Enables or disables the NAT function.</td><td rowspan="3">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.</td></tr>
<tr><td>DNS Relay</td><td>Enables or disables the DNS relay function.</td></tr>
<tr><td>MTU</td><td>Enter the maximum transmission unit. It is recommended to use the default value.</td></tr>
<tr><td>Lan Binding</td><td colspan="2">Select the LAN port to be bound with the WAN port.</td></tr>
</table>

Table 4.6 Parameters for Broadband Settings (Continued)

Item	Description	
SSID Binding	Select the wireless SSID to be bound with the WAN port.	
IPv6 Enable	Enables or disables the IPv6 function. The default setting is Disable.	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 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. ◆ Manual: Connect by dialing manually. ◆ 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	

Table 4.6 Parameters for Broadband Settings (Continued)

Item	Description	
	period expires.	
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 set when IPv6 is enabled 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.	

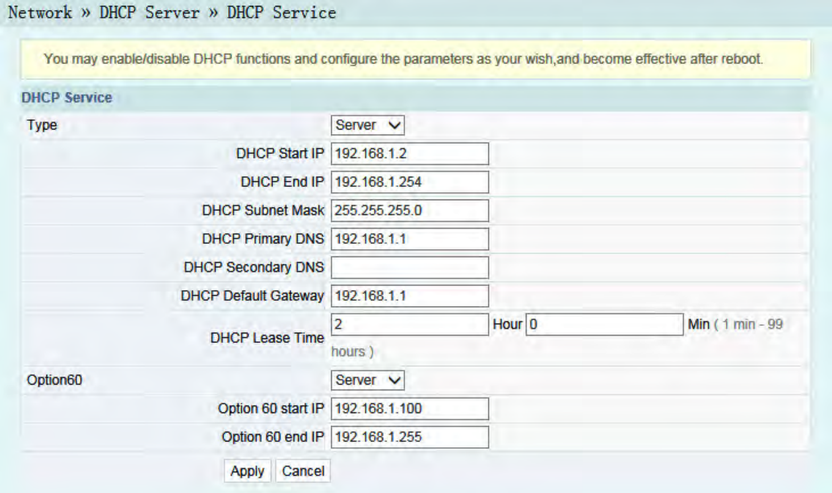
Table 4.6 Parameters for Broadband Settings (Continued)

Item	Description	
IPv6 Address/Prefix	Select the IPv6 address obtaining mode / prefix obtaining mode.	This item should be set when IPv6 is enabled and the WAN IP Mode is set to DHCP or PPPoE.

4.3.4 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 4.16.



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

DHCP Lease Time: 2 Hour 0 Min (1 min - 99 hours)

Option60: Server

Option 60 start IP: 192.168.1.100

Option 60 end IP: 192.168.1.255

Figure 4.16 DHCP Server

2. Configure the DHCP server parameters as required. Table 4.7 describes the parameters.
3. Click **Apply** to save the configuration information. The configuration will take effect after the ONU is rebooted.

Table 4.7 Parameters for the DHCP Server

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>Type</td><td colspan="2">Enables or disables the DHCP server.
◆ 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.</td></tr>
<tr><td>DHCP Start IP</td><td>The starting IP address of the IP address pool of the DHCP server.</td><td rowspan="2"><b>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.</b></td></tr>
<tr><td>DHCP End IP</td><td>The end IP address of the IP address pool of the DHCP server.</td></tr>
<tr><td>DHCP Subnet Mask</td><td colspan="2">The mask of the active DHCP server.</td></tr>
<tr><td>DHCP Primary DNS</td><td colspan="2">The IP address of the active DNS server.</td></tr>
<tr><td>DHCP Secondary DNS</td><td colspan="2">The IP address of the standby DNS server.</td></tr>
<tr><td>DHCP Default Gateway</td><td colspan="2">The default gateway of the active DHCP server.</td></tr>
</table>

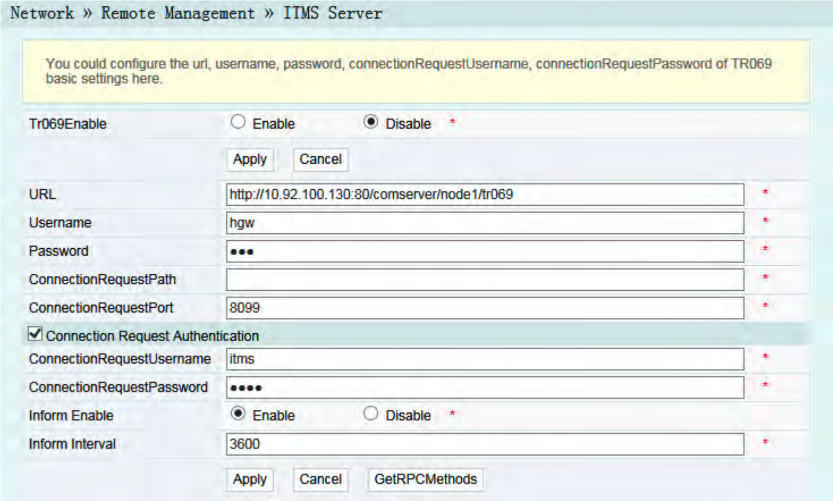
Table 4.7 Parameters for the DHCP Server (Continued)

<table>
<tr><th>Item</th><th colspan="2">Description</th></tr>
<tr><td>DHCP Lease Time</td><td colspan="2">The lease time of the IP address pool of the DHCP server.</td></tr>
<tr><td>Option60</td><td colspan="2">Enables or disables the Option 60 property to identify the user terminal.</td></tr>
<tr><td>Option 60 start IP</td><td>The starting IP address of the network segment of the Option 60 property terminal distributed by the DHCP server.</td><td rowspan="2">This item should be set when the Option 60 field of the DHCP server is enabled.</td></tr>
<tr><td>Option 60 end IP</td><td>The end IP address of the network segment of the Option 60 property terminal distributed by the DHCP server.</td></tr>
</table>

4.3.5 Remote Management

The TR-069 protocol is a communication specification between the terminal equipment and the ACS. If the TR-069 automatic service issue is enabled for the ISP, the configuration of terminals will be issued automatically by the ACS. The network parameters can be configured automatically using the TR-069 function provided that the ACS parameters have been configured on the ONU and the corresponding configuration on the ACS has been completed. In this case, users need not configure any parameters on the ONU manually.

1. Select **Network** in the navigation bar and select **Remote Management** in the left link bar to open the TR-069 basic configuration tab, as shown in Figure 4.17.



Network » Remote Management » ITMS Server

You could configure the url, username, password, connectionRequestUsername, connectionRequestPassword of TR069 basic settings here.

Tr069Enable ○ Enable ● Disable *

Apply Cancel

URL http://10.92.100.130:80/comserver/node1/tr069 *

Username hgw *

Password ●●● *

ConnectionRequestPath *

ConnectionRequestPort 8099 *

☑ Connection Request Authentication

ConnectionRequestUsername itms *

ConnectionRequestPassword ●●●● *

Inform Enable ● Enable ○ Disable *

Inform Interval 3600 *

Apply Cancel GetRPCMethods

Figure 4.17 TR-069 Configuration

2. Configure relevant parameters according to the requirement. Table 4.8 shows the parameter description.
3. Click **Apply** to save and apply the configuration.

Table 4.8 Parameters for TR-069 Configuration

Item	**Description**
TR069Enable	Enables or disables the TR069 function. After the aforesaid operation, click the **Apply** button to validate the configuration.
URL	The ACS server path provided by ISP for the ONU to send the connection request.
Username	The username for the ONU to register on the ACS.
Password	The password for the ONU to register on the ACS.
Connection Request Path	The URL used for connecting the ACS to the ONU. Set this item to /0.
Connection Request Port	The port of the ACS that sends the connection request to ONU.

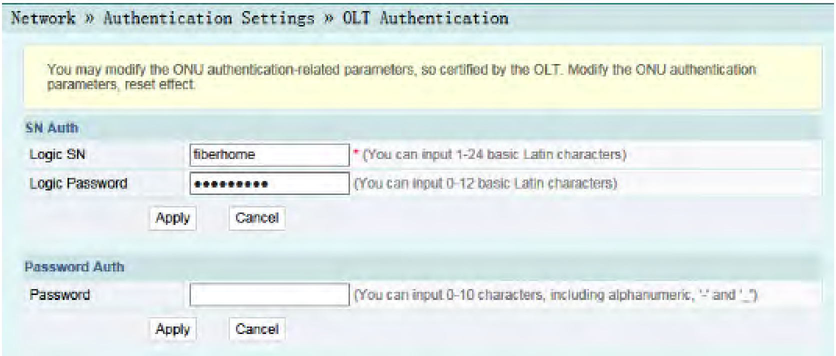
Table 4.8 Parameters for TR-069 Configuration (Continued)

Item	Description
Connection Request Authentication	Enables or disables the user authentication when the ACS sends the connection request to the ONU.
Connection Request Username	Authentication username of the ACS sending the connection request to the ONU.
Connection Request Password	Authentication password of the ACS sending the connection request to the ONU.
Inform Enable	Enables or disables periodic report of Inform messages, used for regular communication between the ONU and the ACS. After the Inform message is enabled, the ONU will authenticate and connect with the ACS at the end of each informing interval, reporting the Inform messages for information exchange between them.
Inform Interval	After the Inform message is enabled, set the time interval of sending Inform messages (unit: s).
Get RPC Methods	Click this button and the current ONU and ACS will discover the operation methods supported by each other.

4.3.6 Authentication Setting

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

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 4.18.



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.

SN Auth

Logic SN: fiberhome * (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 4.18 OLT Authentication

2. Configure the parameters as required. Table 4.9 describes the parameters.
3. Click **Apply** to save the configuration information. The configuration will take effect after the ONU is rebooted.

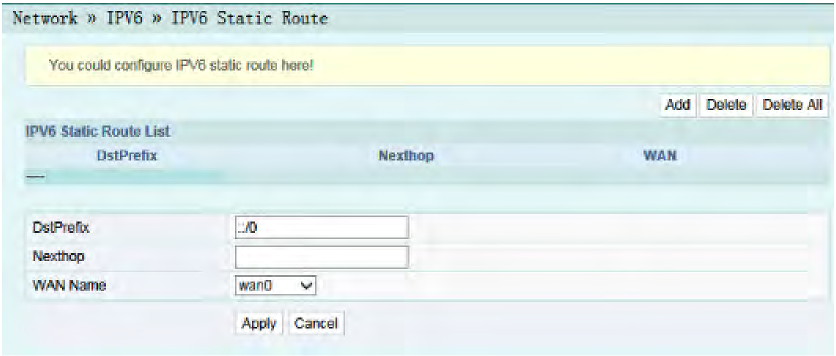
Table 4.9 Parameters for OLT Authentication

Item	**Description**	
Logic SN	Sets the logical SN username.	This item is configurable when the ONU uses the SN authentication.
Logic Password	Sets the logical SN password.	
Password authentication	Sets the authentication password when the ONU is authenticated by password.	

4.3.7 IPV6

Configure the IPv6 static routing.

1. Select **Network** in the navigation bar. Select **IPV6** from the left link bar and click **Add** in the information bar that appears at right part to open the IPv6 static routing table configuration tab, as shown in Figure 4.19.



Network » IPV6 » IPV6 Static Route

You could configure IPV6 static route here!

IPV6 Static Route List

DstPrefix	Nexthop	WAN

DstPrefix	::/0
Nexthop	
WAN Name	wan0

Figure 4.19 IPv6 Static Routing

2. Configure the parameters relevant to static routing as required. Table 4.10 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 4.10 Parameters for the IPv6 Static Routing

Item	**Description**
DstPrefix	The destination IP address to be accessed by the host.
Nexthop	The IP address of the next-hop gateway.
WAN	The WAN port passed by the static routing. Select the available WAN port.

4.4 Security

The following introduces how to configure the firewall, remote control, route QOS, WPS, ACL configuration, DDOS and HTTPS in Web GUI.

4.4.1 Firewall

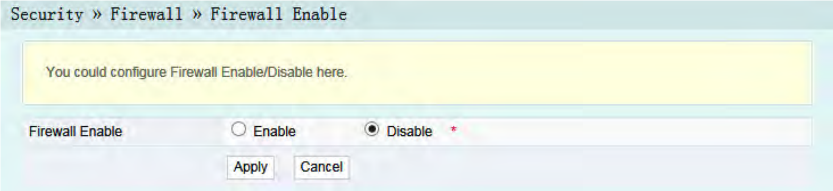
The firewall configuration includes

- Firewall enabling
- IP filtering
- IPv6 filtering
- URL filtering
- Anti-port scan
- DHCP filtering
- MAC address filtering
- IPv6 Mac 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 4.20.



Security » Firewall » Firewall Enable

You could configure Firewall Enable/Disable here.

Firewall Enable ○ Enable ● Disable *

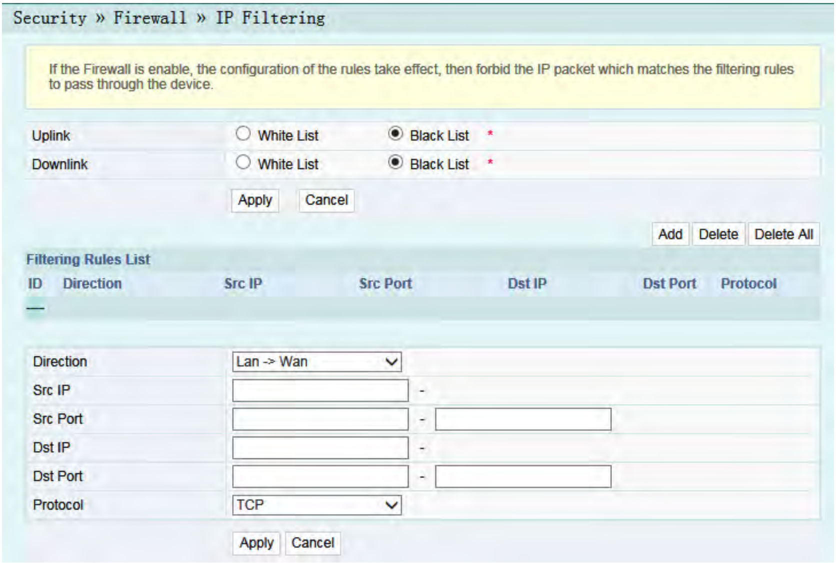
Figure 4.20 Firewall Enabling

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.

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 4.21.



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	Lan -> Wan
Src IP	-
Src Port	-
Dst IP	-
Dst Port	-
Protocol	TCP

Figure 4.21 IP Filtering

2. Configure the parameters relevant to filtering as required. Table 4.11 describes the parameters.
3. Click **Apply** to save and apply the configuration.

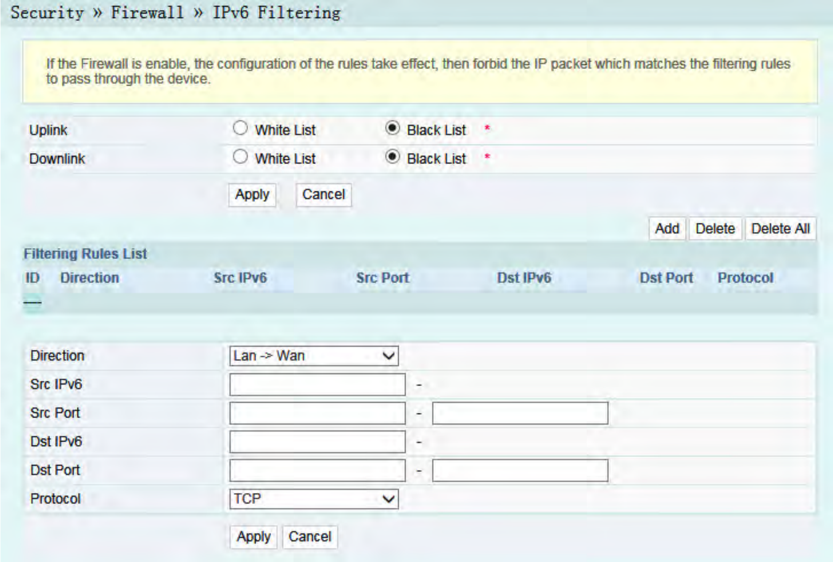
Table 4.11 Parameters for IP Address Filtering

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.
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 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.	

4.4.1.3 IPv6 Filtering

Allow or forbid the IPv6 messages 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 tab, as shown in Figure 4.22.



Security » Firewall » IPv6 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 IPv6	Src Port	Dst IPv6	Dst Port	Protocol
—						

Direction	Lan -> Wan	
Src IPv6		-
Src Port		-
Dst IPv6		-
Dst Port		-
Protocol	TCP	

Figure 4.22 IPv6 Filtering

2. Configure the parameters relevant to filtering as required. Table 4.12 describes the parameters.
3. Click **Apply** to save and apply the configuration.

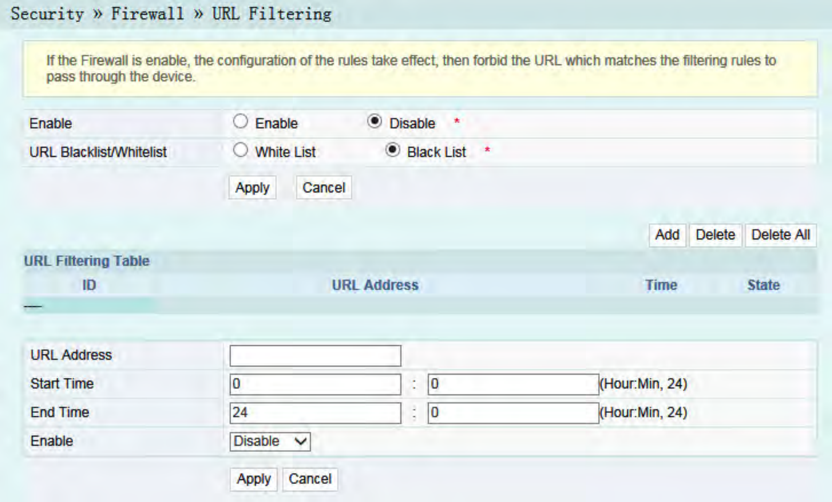
Table 4.12 Parameters of IPv6 Filtering

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.
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 IP	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.	

4.4.1.4 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 tab, as shown in Figure 4.23.



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	0	: 0	(Hour:Min, 24)
End Time	24	: 0	(Hour:Min, 24)
Enable	Disable		

Apply Cancel

Figure 4.23 URL Filtering

2. Configure the parameters relevant to filtering as required. Table 4.13 describes the parameters.
3. Click **Apply** to save and apply the configuration.

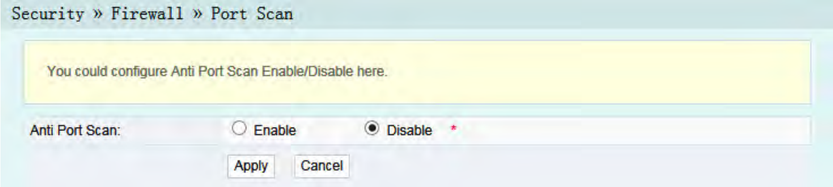
Table 4.13 Parameters for URL Filtering Parameters

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 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.	

4.4.1.5 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 4.24.



Security » Firewall » Port Scan

You could configure Anti Port Scan Enable/Disable here.

Anti Port Scan: ○ Enable ● Disable *

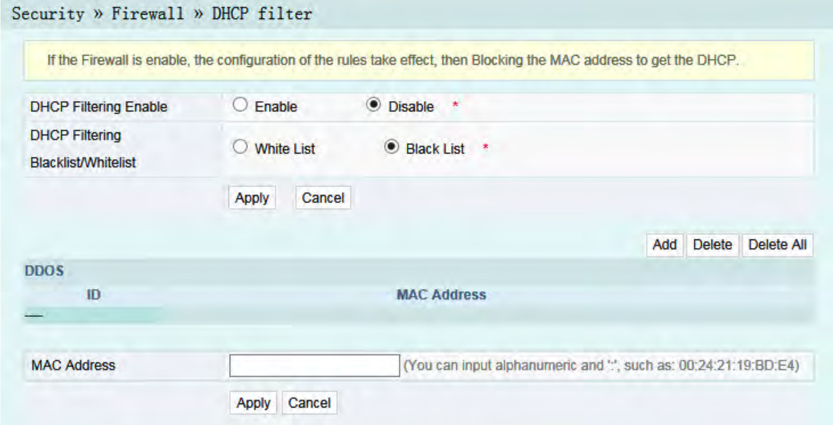
Figure 4.24 Anti-port Scan

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

4.4.1.6 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 filter** in the left link bar, and then click **Add** to open the anti-DOS attack configuration tab, as shown in Figure 4.25.



Security » Firewall » DHCP filter

If the Firewall is enable, the configuration of the rules take effect, then Blocking the MAC address to get the DHCP.

DHCP Filtering Enable ○ Enable ● Disable *

DHCP Filtering Blacklist/Whitelist ○ White List ● Black List *

DDOS

ID	MAC Address
--	

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

Figure 4.25 DHCP Filtering

2. Configure the parameters relevant to filtering as required. Table 4.14 describes the parameters.
3. Click **Apply** to save and apply the configuration.

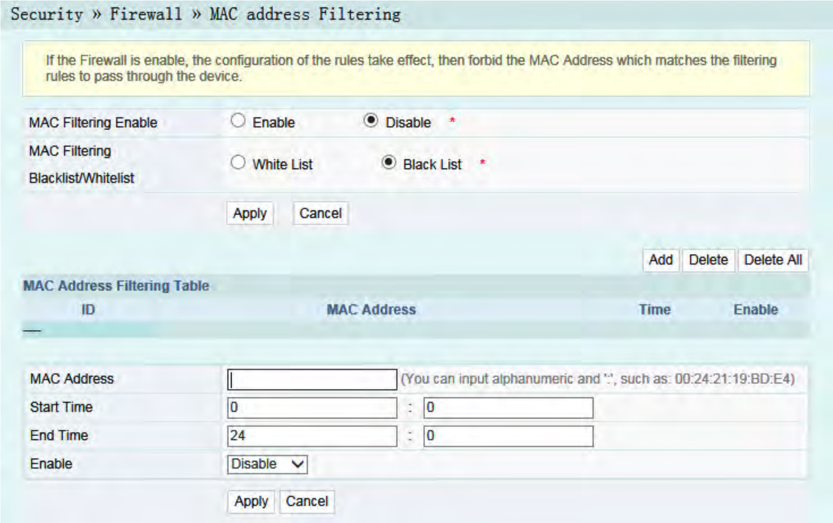
Table 4.14 Parameters for DHCP Filtering

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

4.4.1.7 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 address Filtering** in the left link bar, and then click **Add** to open the MAC address filtering table configuration tab, as shown in Figure 4.26.



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 *

MAC Address Filtering Table

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	

Figure 4.26 MAC Addresses Filtering

2. Configure parameters relevant to filtering as required. Table 4.15 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.15 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	

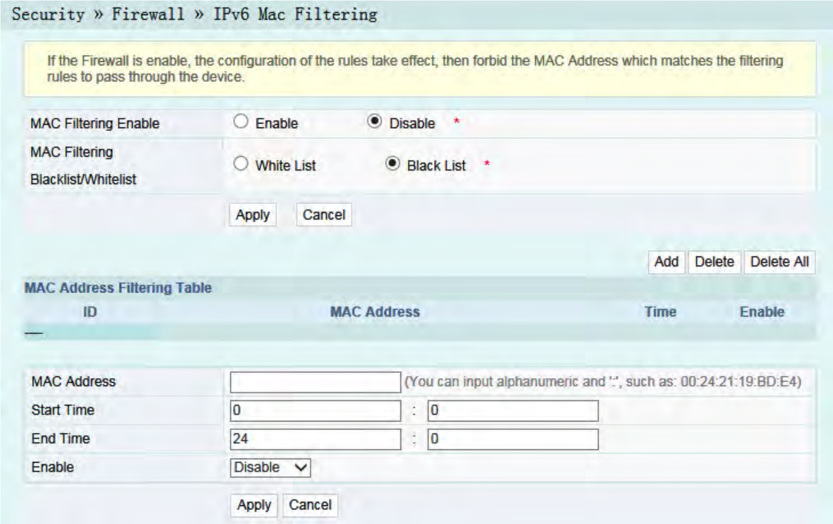
Table 4.15 Parameters for MAC Address Filtering (Continued)

Item	Description
	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.

4.4.1.8 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 MAC address filtering table configuration tab, as shown in Figure 4.27.



Security » Firewall » IPv6 Mac 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

MAC Address Filtering Table

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 4.27 IPv6 Mac Filtering

2. Configure the parameters relevant to filtering as required. Table 4.16 describes the parameters.
3. Click **Apply** to save and apply the configuration.

Table 4.16 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	

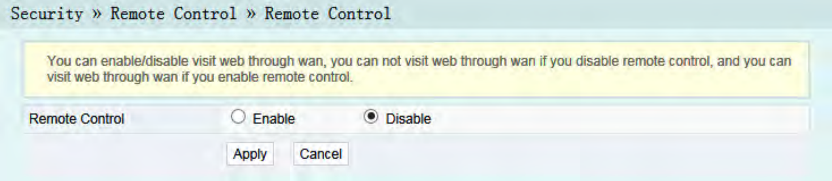
Table 4.16 Parameters for IPv6 MAC Address Filtering (Continued)

Item	Description	
	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.

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 4.28.



Security » Remote Control » Remote Control

You can enable/disable visit web through wan, you can not visit web through wan if you disable remote control, and you can visit web through wan if you enable remote control.

Remote Control ○ Enable ● Disable

Figure 4.28 Remote Control

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

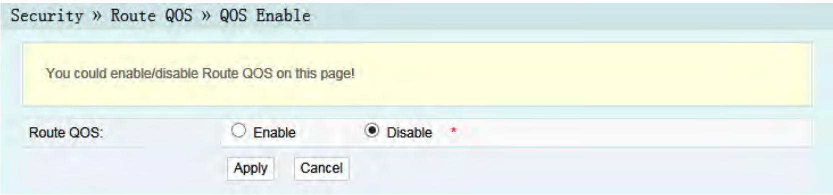
4.4.3 Route QoS

The route QoS includes route QoS enabling and route QoS configuration.

4.4.3.1 Route QOS Enable

Enable / disable the route QOS function.

1. Select **Security** in the navigation bar and select **Route QOS→ QOS Enable** in the left link bar to open the route QOS enabling tab, as shown in Figure 4.29.



Security » Route QOS » QOS Enable

You could enable/disable Route QOS on this page!

Route QOS: ○ Enable ● Disable *

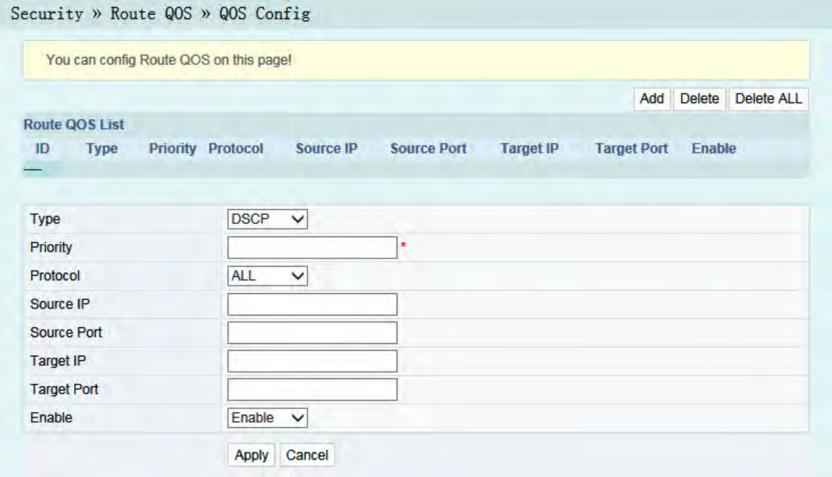
Figure 4.29 Route QoS Enabling

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

4.4.3.2 Route QOS Configuration

While configuring the route QOS parameters, user can classify the queues based on priority and process the messages with high priority first when system congestion occurs.

1. Select **Security** in the navigation bar and select **Route QOS→ QOS Config** in the left link bar. Then click **Add** to open the route QOS configuration tab, as shown in Figure 4.30.



Security » Route QOS » QOS Config

You can config Route QOS on this page!

Route QOS List

ID	Type	Priority	Protocol	Source IP	Source Port	Target IP	Target Port	Enable

Type	DSCP
Priority	*
Protocol	ALL
Source IP	
Source Port	
Target IP	
Target Port	
Enable	Enable

Figure 4.30 Route QoS Configuration

2. Configure the parameters relevant to QoS according to the requirement. Table 4.17 describes the parameters.
3. Click **Apply** to save and apply the configuration.

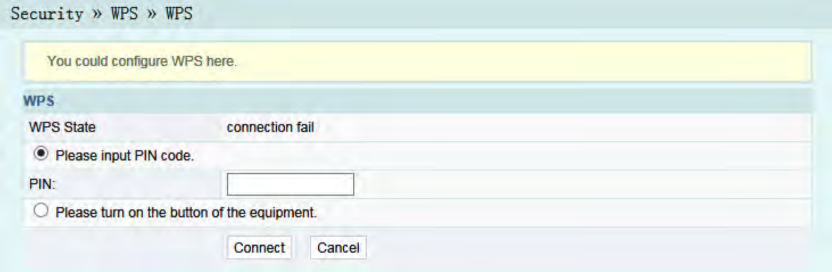
Table 4.17 Parameters of Route QoS Configuration

Item	**Description**
Type	Select the priority type.
Priority	Sets the priority value. The DSCP priority value ranges from 0 to 63; the 802.1p priority value ranges from 0 to 7.
Protocol	The protocol types include ALL, TCP and UDP.
Source IP	Source IP address.
Source Port	Source port.
Target IP	The destination IP address.
Target Port	The destination port.
Enable	Enables or disables the QoS rule.

4.4.4 WPS

WPS can automatically set the network name (SSID) and wireless encryption key for the AN5506-04 Series ONUs and the client end supporting the Wi-Fi service. Users need only to press down the WPS button or enter PIN to achieve safe connection. Users need not remember the long encryption key and are free of the trouble caused by forgetting the password.

1. Select **Security** in the navigation bar and select **WPS** in the left link bar to open the WPS configuration tab, as shown in Figure 4.31.


Security » WPS » WPS

You could configure WPS here.

WPS

WPS State connection fail

● Please input PIN code.

PIN:

○ Please turn on the button of the equipment.

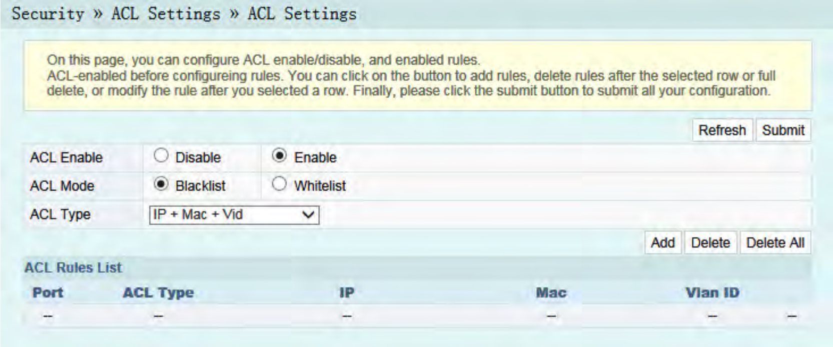
Figure 4.31 WPS

2. Select the WPS connection mode as required.
   - Select **Please input PIN code.**, and enter the PIN code in the **PIN** text box. Then click **Connect**.
   - Select **Please turn on the button of the equipment** and press down the **WPS** button on panel at the ONU side. Then press down the WPS button or the WPS software key on the client end.
3. Wait until the connection is completed.

4.4.5 ACL Configuration

Users can configure ACL (Access Control List) to filter designated data packets using the matching rules. After the ACL rule is enabled, the corresponding port will filter the packets as per the configured ACL rules.

1. Select **Security** in the navigation bar and select **ACL Settings** in the left link bar to open the ACL configuration tab, as shown in Figure 4.32.



Security » ACL Settings » ACL Settings

On this page, you can configure ACL enable/disable, and enabled rules.
ACL-enabled before configureing rules. You can click on the button to add rules, delete rules after the selected row or full delete, or modify the rule after you selected a row. Finally, please click the submit button to submit all your configuration.

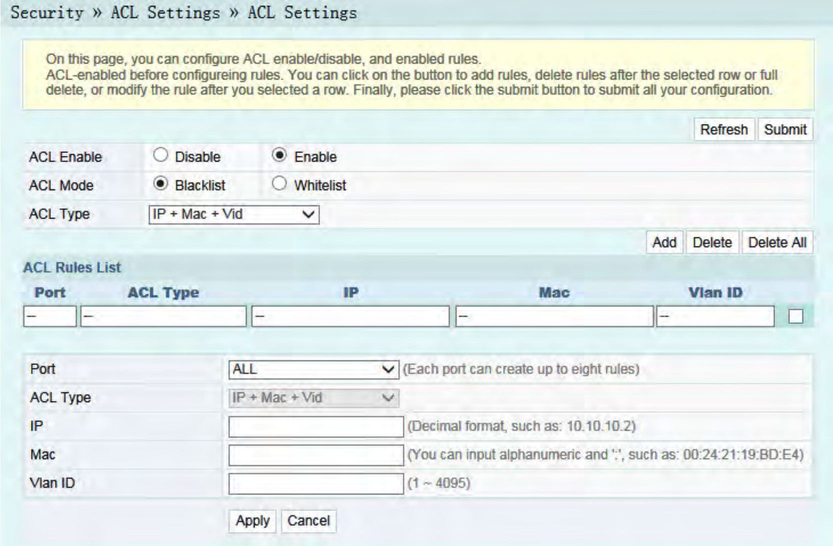
ACL Enable	○ Disable	● Enable
ACL Mode	● Blacklist	○ Whitelist
ACL Type	IP + Mac + Vid	

ACL Rules List

Port	ACL Type	IP	Mac	Vlan ID	
--	--	--	--	--	--

Figure 4.32 ACL Configuration

2. Select **Enable** and set **ACL Mode** and **ACL Type**. Then click **Add** to open the ACL rule list configuration tab, as shown in Figure 4.33.



Security » ACL Settings » ACL Settings

On this page, you can configure ACL enable/disable, and enabled rules.
ACL-enabled before configureing rules. You can click on the button to add rules, delete rules after the selected row or full delete, or modify the rule after you selected a row. Finally, please click the submit button to submit all your configuration.

ACL Enable	○ Disable	● Enable
ACL Mode	● Blacklist	○ Whitelist
ACL Type	IP + Mac + Vid	

ACL Rules List

Port	ACL Type	IP	Mac	Vlan ID	
--	--	--	--	--	□

Port	ALL	(Each port can create up to eight rules)
ACL Type	IP + Mac + Vid	
IP		(Decimal format, such as: 10.10.10.2)
Mac		(You can input alphanumeric and ':', such as: 00:24:21:19:BD:E4)
Vlan ID		(1 ~ 4095)

Figure 4.33 ACL Configuration Rule

3. Configure parameters relevant to filtering as required. Table 4.18 describes the parameters.
4. Click **Submit** to generate the corresponding ACL rule item.
5. Click **Apply** to save and apply the configuration.

Table 4.18 Parameters for ACL Configuration

Item	**Description**	
ACL Enable	Select to enable or disable the access control.	After setting, click **Submit** at the upper right part to take effect.
ACL Mode	Select the access control mode. ◆ Whitelist indicates that the data complying with the rules in the ACL rule table will be allowed to pass. ◆ Blacklist indicates that the data complying with the rules in the ACL rule table will not be allowed to pass.	

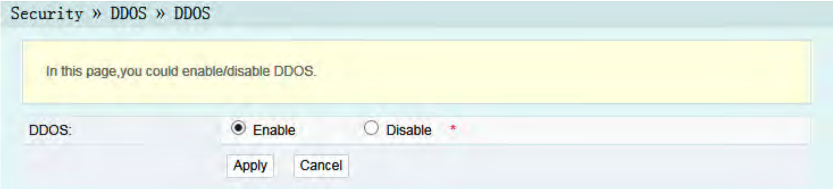
Table 4.18 Parameters for ACL Configuration (Continued)

Item	Description	
ACL Type	The options include IP, IP+Mac and IP +Mac+Vid. Modifying ACL type will delete all the existing ACL rules.	
Port	The number of the LAN port(s) subject to the ACL rule. The options include ALL and 1 to 4.	
IP	The IP address of the accessed user device.	
Mac	The Mac address of the accessed user device.	
VLAN ID	The VLAN ID of the accessed LAN port; the value ranges from 1 to 4095.	

4.4.6 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 4.34.



Security » DDOS » DDOS

In this page,you could enable/disable DDOS.

DDOS: ● Enable ○ Disable *

Figure 4.34 DDOS

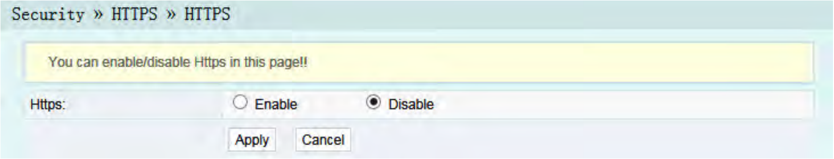
2. Select to **Enable** or **Disable** the anti-dos attack function as required.

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

4.4.7 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 4.35.


Security » HTTPS » HTTPS

You can enable/disable Https in this page!!

Https: ○ Enable ● Disable

Figure 4.35 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.

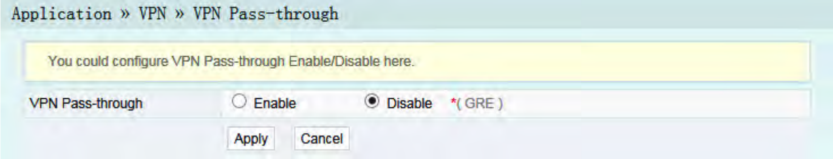
4.5 Application

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

4.5.1 VPN

Set whether to enable the VPN transparent transmission channel.

1. Select **Application** in the navigation bar and select **VPN** in the left link bar to open the VPN transparent transmission configuration tab, as shown in Figure 4.36.



Application » VPN » VPN Pass-through

You could configure VPN Pass-through Enable/Disable here.

VPN Pass-through ○ Enable ● Disable *(GRE)

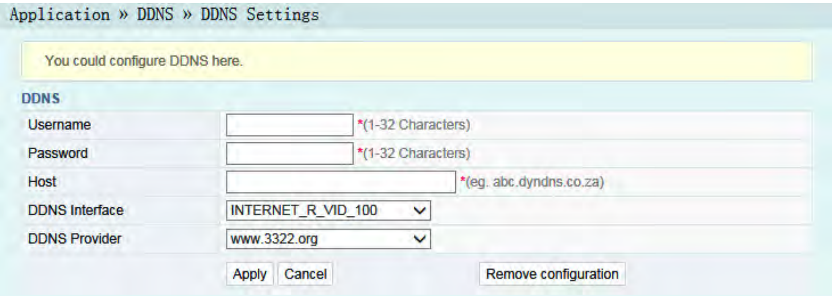
Figure 4.36 VPN Transparent Transmission

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

4.5.2 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 4.37.



Application » DDNS » DDNS Settings

You could configure DDNS here.

DDNS

Username	*(1-32 Characters)
Password	*(1-32 Characters)
Host	*(eg. abc.dyndns.co.za)
DDNS Interface	INTERNET_R_VID_100
DDNS Provider	www.3322.org

Figure 4.37 DDNS Settings

2. Configure parameters relevant to DDNS according to the requirement. Table 4.19 describes the parameters.
3. Click **Apply** to apply and save the configuration.

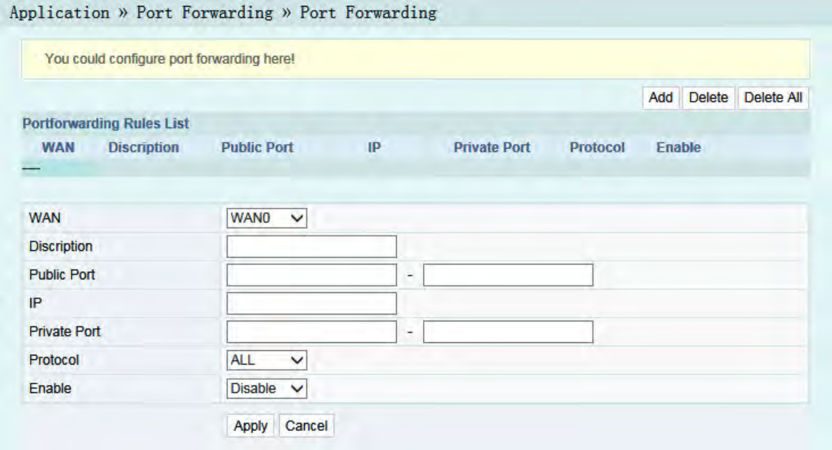
Table 4.19 Parameters for DDNS Settings

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.
DDNS Interface	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.

4.5.3 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 4.38.



Application » Port Forwarding » Port Forwarding

You could configure port forwarding here!

Portforwarding Rules List

WAN	Discription	Public Port	IP	Private Port	Protocol	Enable

WAN	WAN0	
Discription		
Public Port		-
IP		
Private Port		-
Protocol	ALL	
Enable	Disable	

Figure 4.38 Port Forwarding

2. Configure parameters relevant to port forwarding according to the requirement. Table 4.20 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.20 Parameters for Port Forwarding

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

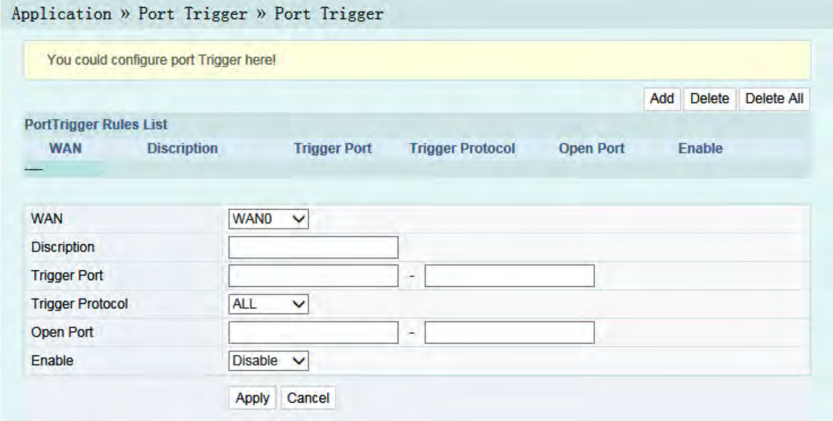
Table 4.20 Parameters for Port Forwarding (Continued)

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.

4.5.4 Port Triggering

Port triggering means that when the corresponding port at the LAN side sends messages, the ONU will automatically enable the designated port at the WAN side and map the port to the corresponding port on the host that sends the messages at the LAN side. In this way, normal communication can be guaranteed.

1. Select **Application** in the navigation bar and select **Port Trigger** in the left link bar. Click **Add** to open the port triggering configuration tab, as shown in Figure 4.39.



Application » Port Trigger » Port Trigger

You could configure port Trigger here!

PortTrigger Rules List

WAN	Discription	Trigger Port	Trigger Protocol	Open Port	Enable

WAN	WAN0
Discription	
Trigger Port	-
Trigger Protocol	ALL
Open Port	-
Enable	Disable

Figure 4.39 Port Triggering

2. Configure parameters relevant to port triggering according to the requirement. Table 4.21 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.21 Parameters for Port Triggering

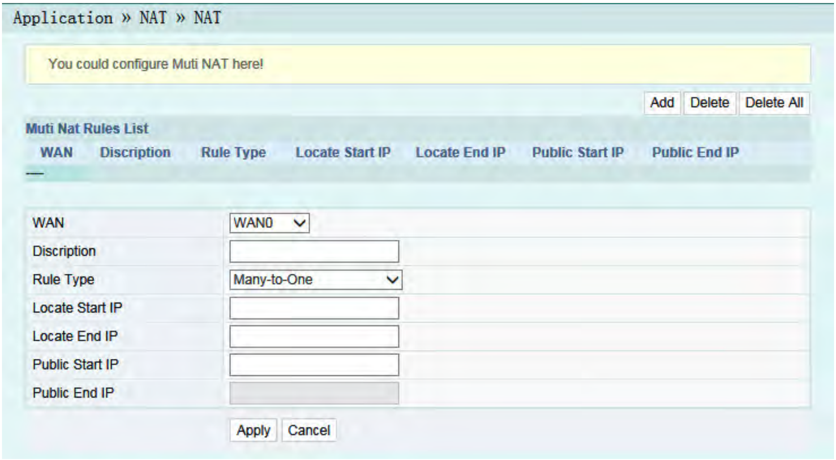
Item	**Description**
WAN	The corresponding WAN connection bound with the port triggering rule.
Description	The port triggering rule name.
Trigger Port	The range of destination port for the port triggering data packets. If only one port exists, enter the same port number.
Trigger Protocol	The protocol type for the port triggering data packets. The options include ALL, TCP and UDP.
Open Port	The range of destination port for the opened data packets. If only one port exists, enter the same port number.
Enable	Enables or disables the rule.

4.5.5 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 4.40.



Application » NAT » NAT

You could configure Muti NAT here!

Muti Nat Rules List

WAN	Discription	Rule Type	Locate Start IP	Locate End IP	Public Start IP	Public End IP
—						

WAN	WAN0
Discription	
Rule Type	Many-to-One
Locate Start IP	
Locate End IP	
Public Start IP	
Public End IP	

Figure 4.40 NAT

2. Configure relevant parameters according to the requirement. Table 4.22 describes the parameters.
3. Click **Apply** to apply and save the configuration.

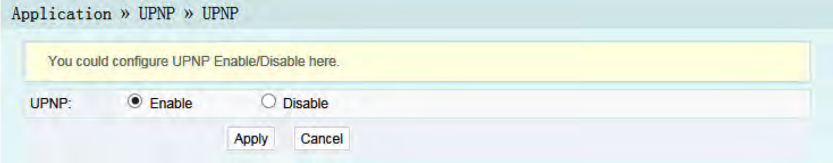
Table 4.22 Parameters for NAT Configuration

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.

4.5.6 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 the PC, the port mapping table will be generated on the ONU automatically using the UPnP protocol, so that the operation can be sped up.

1. Select **Application** in the navigation bar and select **UPNP** in the left link bar to open the UPNP configuration tab, as shown in Figure 4.41.


Application » UPNP » UPNP

You could configure UPNP Enable/Disable here.

UPNP: ● Enable ○ Disable

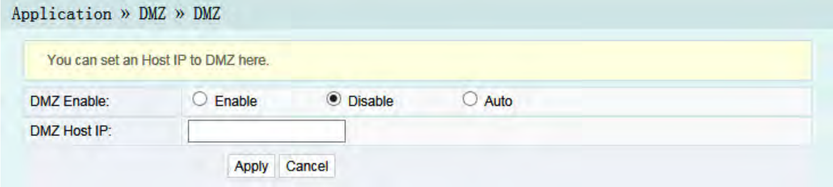
Figure 4.41 UPnP

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

4.5.7 DMZ

When the ONU 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 ONU will forward all the IP packets from the WAN to the designated DMZ host.

1. Select **Application** in the navigation bar and select **DMZ** in the left link bar to open the DMZ configuration tab, as shown in Figure 4.42.


Application » DMZ » DMZ

You can set an Host IP to DMZ here.

DMZ Enable: ○ Enable ● Disable ○ Auto

DMZ Host IP:

Figure 4.42 DMZ

2. Configure relevant parameters according to the requirement. Table 4.23 describes the parameters.
3. Click **Apply** to apply and save the configuration.

Table 4.23 Parameters for DMZ Configuration

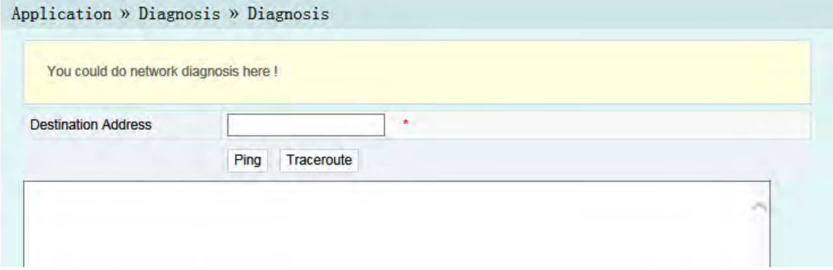
Item	Description
DMZ Enable	Enables or disables the DMZ function. The options include Enable, Disable and Auto. If Enable is selected, the DMZ host IP address should be set. If Auto is selected, the DMZ host uses the first IP address allocated by DHCP.
DMZ Host IP	The host IP address of the DMZ.

4.5.8 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 4.43.



Application » Diagnosis » Diagnosis

You could do network diagnosis here !

Destination Address *

Figure 4.43 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, device management and log query in the Web GUI.

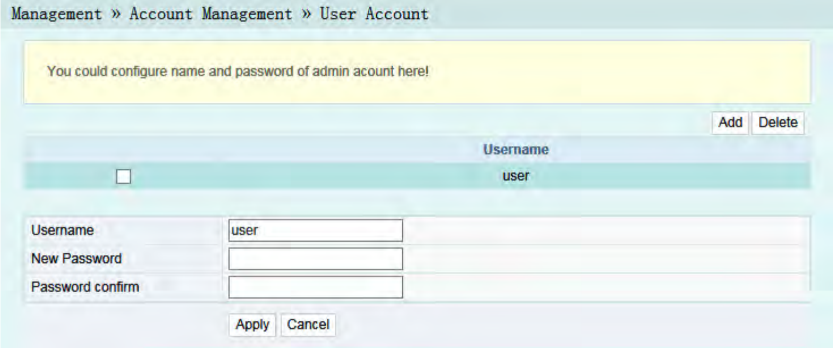
4.6.1 User Management

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 4.44.



Management » Account Management » User Account

You could configure name and password of admin acount here!

	Username
□	user

Username	user
New Password	
Password confirm	

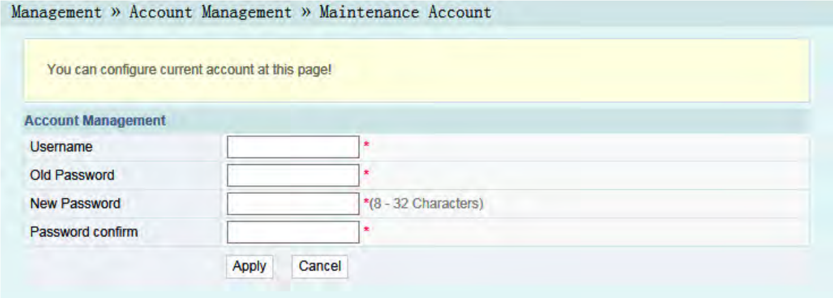
Figure 4.44 User Account Management

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 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 tab, as shown in Figure 4.45.



Management » Account Management » Maintenance Account

You can configure current account at this page!

Account Management

Username	*
Old Password	*
New Password	*(8 - 32 Characters)
Password confirm	*

Figure 4.45 Maintenance Account Management

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

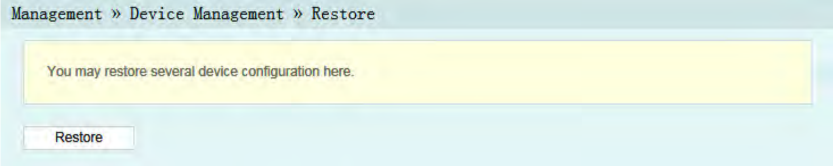
4.6.2 Device Management

The ONU provides multiple device management functions such as configuration restoring, local upgrade, configuration backup, FTP client end, FTP server, device reboot and NTP time calibration.

4.6.2.1 Restoring the Configuration Data

Restore the configuration of the ONU to the factory configuration, such as Web login username and password, and wireless network SSID and password.

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 4.46.



Management » Device Management » Restore

You may restore several device configuration here.

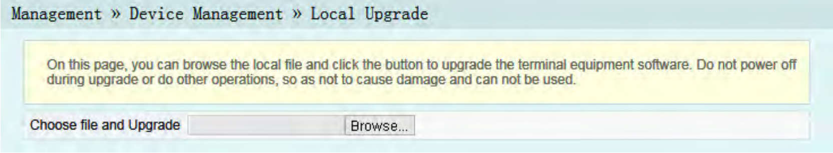
Figure 4.46 Configuration Restoring

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

4.6.2.2 Local Upgrade

Select the local file and upgrade the ONU 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 tab, as shown in Figure 4.47.



Management » Device Management » Local Upgrade

On this page, you can browse the local file and click the button to upgrade the terminal equipment software. Do not power off during upgrade or do other operations, so as not to cause damage and can not be used.

Choose file and Upgrade

Figure 4.47 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 ONU 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.

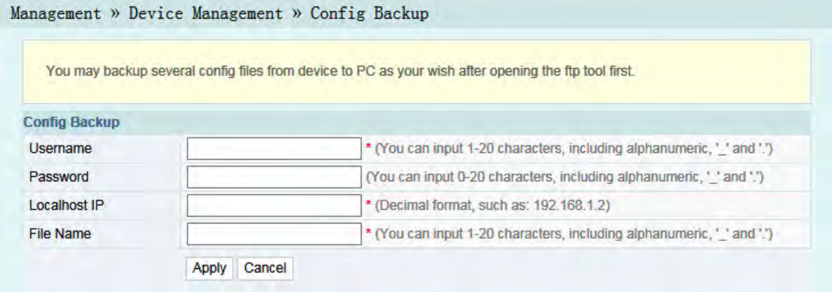
Tip:

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

4.6.2.3 Configuration Backup

Back up and save the ONU configuration files for the later restoring. 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 restoring tab, as shown in Figure 4.48.



Management » Device Management » Config Backup

You may backup several config files from device to PC as your wish after opening the ftp tool first.

Config Backup

Username		* (You can input 1-20 characters, including alphanumeric, '_' and '.')
Password		(You can input 0-20 characters, including alphanumeric, '_' and '.')
Localhost IP		* (Decimal format, such as: 192.168.1.2)
File Name		* (You can input 1-20 characters, including alphanumeric, '_' and '.')

Figure 4.48 Configuration Backup

2. Configure parameters relevant to file backup. Table 4.24 describes the parameters.
3. Click **Apply** to save the configuration backup file.

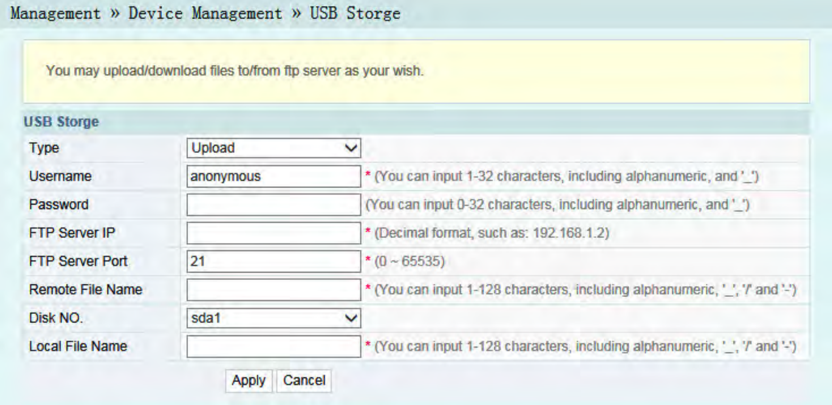
Table 4.24 Parameters for Configuration Backup

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

4.6.2.4 FTP Client End

The ONU serves as the FTP client end. Users can upload files to the FTP server or download files from the FTP server.

1. Select **Management** in the navigation bar. Select **Device Management→Config Backup** from the left link bar to open the FTP client end tab, as shown in Figure 4.49.



Management » Device Management » USB Storge

You may upload/download files to/from ftp server as your wish.

USB Storge

Type	Upload	
Username	anonymous	* (You can input 1-32 characters, including alphanumeric, and '_')
Password		(You can input 0-32 characters, including alphanumeric, and '_')
FTP Server IP		* (Decimal format, such as: 192.168.1.2)
FTP Server Port	21	* (0 ~ 65535)
Remote File Name		* (You can input 1-128 characters, including alphanumeric, '_', '/' and '-')
Disk NO.	sda1	
Local File Name		* (You can input 1-128 characters, including alphanumeric, '_', '/' and '-')

Figure 4.49 FTP Client End

2. Configure parameters relevant to the FTP client end. Table 4.25 describes the parameters.
3. Click **Apply** to save and apply the configuration.

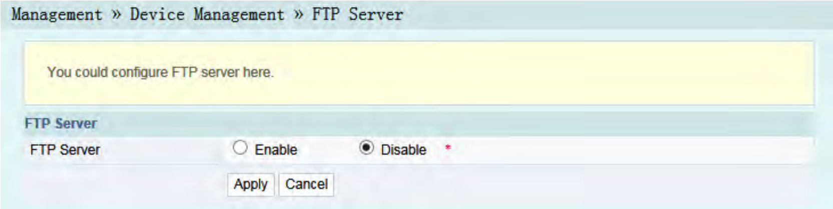
Table 4.25 Parameters for the FTP Client End

Item	**Description**
Type	Select to upload or download.
Username	The FTP server username.
Password	The FTP server password.
FTP Server IP	The FTP Server IP address.
FTP Server Port	The FTP server port.
Remote File Name	The name of file saved in the FTP server.
Disk NO.	The disk number of the USB port connected to the ONU.
Local File Name	The name of file saved locally.

4.6.2.5 FTP Server

With the FTP server function of the ONU enabled, users can access the ONU resources via the FTP client end on the PC.

1. Select **Management** in the navigation bar. Select **Device Management→FTP Server** from the left link bar to open the FTP server configuration tab, as shown in Figure 4.50.



Management » Device Management » FTP Server

You could configure FTP server here.

FTP Server

FTP Server ○ Enable ● Disable *

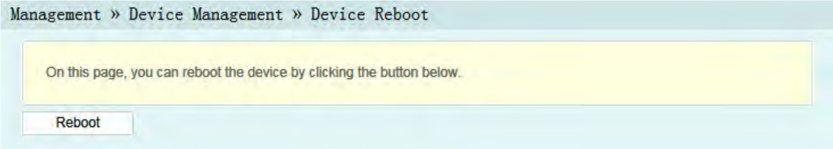
Figure 4.50 FTP Server

2. Enable or disable the FTP server function according to the requirement.Select **Enable** and then enter the **Username** and **Password** for connection with the FTP server.

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

4.6.2.6 Device Reboot

1. Select **Management** in the navigation bar. Select **Device Management→Device Reboot** from the left link bar to open the device reboot tab, as shown in Figure 4.51.



Management » Device Management » Device Reboot

On this page, you can reboot the device by clicking the button below.

Figure 4.51 Device Reboot

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

Caution:

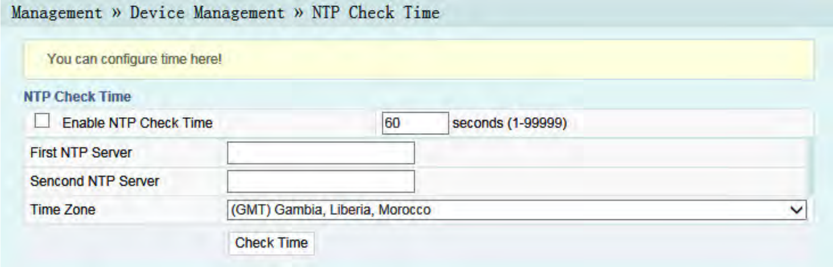
Save the configuring data before rebooting the device to prevent loss of the configuration data.

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

4.6.2.7 NTP Time Calibration

Users can obtain the precise time by connecting the ONU 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 FTP client end tab, as shown in Figure 4.52.



Management » Device Management » NTP Check Time

You can configure time here!

NTP Check Time

☐ Enable NTP Check Time 60 seconds (1-99999)

First NTP Server

Sencond NTP Server

Time Zone (GMT) Gambia, Liberia, Morocco

Figure 4.52 NTP Time Calibration

2. Configure relevant parameters relevant to the NTP time calibration. Table 4.26 describes the parameters.
3. Click **Check Time** to save and apply the configuration.

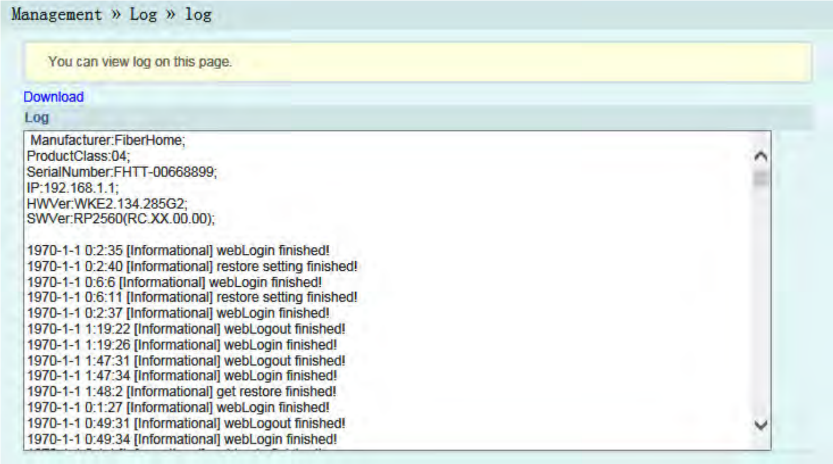
Table 4.26 Parameters for NTP Time Calibration

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.
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.

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.

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 4.53.



```
 Manufacturer:FiberHome;
ProductClass:04;
SerialNumber:FHTT-00668899;
IP:192.168.1.1;
HWVer:WKE2.134.285G2;
SWVer:RP2560(RC.XX.00.00);

1970-1-1 0:2:35 [Informational] webLogin finished!
1970-1-1 0:2:40 [Informational] restore setting finished!
1970-1-1 0:6:6 [Informational] webLogin finished!
1970-1-1 0:6:11 [Informational] restore setting finished!
1970-1-1 0:2:37 [Informational] webLogin finished!
1970-1-1 1:19:22 [Informational] webLogout finished!
1970-1-1 1:19:26 [Informational] webLogin finished!
1970-1-1 1:47:31 [Informational] webLogout finished!
1970-1-1 1:47:34 [Informational] webLogin finished!
1970-1-1 1:48:2 [Informational] get restore finished!
1970-1-1 0:1:27 [Informational] webLogin finished!
1970-1-1 0:49:31 [Informational] webLogout finished!
1970-1-1 0:49:34 [Informational] webLogin finished!
```

Figure 4.53 Log

2. View or download the saved information according as needed.

5 Handling Common Problems

The following introduces how to handle common router faults.

5.1 The Power Indicator LED Remaining Off

Handle 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.

5.2 The PON Indicator LED Remaining Off

Handle 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 ONU has obtained the ISP authorization.
4. Check whether the optical interface is normal; if not, replace the device.

5.3 The LOS Indicator LED Keeping Blinking

Handle 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 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 device is faulty.

5.4 LAN Indicator LED Remaining Off

Handle 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).

5.5 Failing to Detect ONU Using Wi-Fi

Handle according to the procedures below.

1. Check whether the wireless function is disabled for the ONU and whether the SSID is set to **Hidden** so that the network is unavailable.
2. Check whether the network card drive of the computer is installed normally and whether the WLAN function of the wireless terminal (such as computer and telephone) is enabled.
3. Adjust the position of the ONU to reduce the barriers on the wireless channel (such as walls) and make sure the distance

between the ONU and the wireless terminal is within the required range.

Appendix A 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
Other	TR-069	CPE WAN Management Protocol

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:

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 troubleshooting □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.

FiberHome Telecommunication Technologies Co., Ltd.

Address: No. 88 Youkeyuan Rd., Wuhan, Hubei, China
Zip code: 430074
Website: www.fiberhomegroup.com