

4G/5G ODU

User Manual

4G/5G ODU

User Manual

Version: 4G/5G ODU-15-12-100

We are enthusiastic for providing tech support in every way. You can get in touch with local dealer as well as contact to Customer Service Department directly.

Preface

Version statement

This Manual is provided for 4G/5G ODU, the software version must be at least 1.10.

Brief Introduction

This manual provides technical information on how to configure and operate application for your 4G/5G ODU unit.

Intended Audience

System administrators.

Network engineers.

Maintenance technicians.

Style Convention

Table-1 Style convention used in this manual

Style	meanings
\	Multi-level catalogs or menus are separated by '\ ' character. For instance "file\new\directory" means the menu item "directory" in menu "new" which in turn in the menu "file".
	Used to highlight important area in diagrams.
<>	Indicates the input data from operating terminal.
【】	Indicates one parameter configuration or a function.
{ XX XX }	Indicates a syntax of CLI command options, multiple command options in one "{ }", separated by " ", means exclusive single selection.
<i>host</i> (italic)	Indicates user specified parameters. e.g. for command: tftp host {get put} {sys cfg} filename The host and filename should be replaced by user specified real parameters, such as: tftp 138.0.0.1 get sys sysfile.bin

Table-2 Convention for Mouse Operation

Operation	Meanings
Click	Press and release a mouse button quickly
Double click	Quickly press and release a mouse button twice
Drag	Press a mouse button and move the mouse

Table-3 Convention For Keyboard Operation

Style	Meanings
Ctrl + C	“+” means an operation which presses down several keys in the keyboard in the same time. E.g. “Ctrl + C” means press down the key of “Ctrl” and “C” in the same time.

Content

1	OVERVIEW	1
2	PRODUCT INTRODUCTION	2
2.1	APPEARANCE.....	2
2.2	HARDWARE INTERFACE	2
2.3	FEATURES	2
2.4	TECHNICAL INDEX	3
2.5	WORKING ENVIRONMENT.....	3
3	CONFIGURATION.....	4
3.1	LOGIN.....	4
3.2	HOME.....	4
4	NETWORK	5
4.1	NETWORK MANAGEMENT SUMMARY	5
4.2	LAN PORT CONFIGURATION	6
4.3	WLAN CONFIGURATION.....	7
4.3.1	Basic Settings	7
4.3.2	Security	8
4.3.3	Advanced Settings.....	9
4.3.4	Client Info	9
4.3.5	MAC Filtering	10
4.4	MOBILE DATA	11
4.4.1	Basic settings.....	11
4.4.2	Advanced Parameters	12
4.4.3	Status	13
4.5	IPv6	14
5	DATA SERVICE	16
5.1	SERVICE STATUS.....	16
5.2	DHCP SERVER.....	17
5.2.1	Static Address Assign	17
5.2.2	DHCP Relay.....	18
5.3	NAT.....	18
5.3.1	Port Forwarding Settins	19
5.3.2	DMZ	20
5.4	FIREWALL CONFIG.....	21
5.4.1	Attack Defense.....	21
5.4.2	Service Type	23
5.4.3	Internet Access Control.....	24
5.4.4	Management Access Control.....	26
5.4.5	Internet Filter Strategy	29
5.4.6	IP&MAC Binding	31

5.5	QoS	32
5.5.1	QoS Basic Settings	32
5.5.2	DDNS	33
5.6	VPN	34
5.6.1	PPTP Server	34
5.6.2	L2TP Server	34
5.6.3	IPSec.....	35
5.7	ROUTING.....	40
5.7.1	Static Route.....	40
5.7.2	Policy Route	40
5.8	MULTICAST	41
6	SYSTEM.....	42
6.1	TIME MANAGEMENT	42
6.2	SYSTEM MANAGEMENT	43
6.3	REBOOT	44
6.4	BACKUP/RESTORE	44
6.5	DIAGNOSIC	44
6.5.1	Ping	44
6.5.2	Traceroute	45
6.5.3	TcpDump	45
6.6	USER MANAGEMENT.....	46
6.7	SYSTEM LOG.....	47
6.7.1	Log Config.....	47
6.7.2	Log Diaplay	47
6.8	TR069.....	48
6.9	SNMP	49
7	APPLY.....	53

4G/5G ODU USER MANUAL

1. Overview

4G/5G ODU designed for those who want to achieve high speed internet access and convenient management. In addition to its practical features and easy operation, it provides multiple management functions which covers system, DHCP server, DMZ host, firewall and static routing, etc.

4G/5G ODU can provide different internet accesses for different users which means some staff's access could set to be some designated websites or some specified operations while the others are not subject to this limit.

4G/5G ODU provides a clear and easily understandable configuration interface and it achieves its full function with no need for any other software.

2. Product Introduction

2.1 Appearance



Figure2-1 Appearance

2.2 Hardware Interface

- 2 x 1000 Mbps Ethernet Port
- Power: 48V 0.32A

2.3 Features

- Support PPPoE, DHCP and static IP address
- Support NAT,NAPT, static address mapping and port mapping(virtual server)
- VPN (PPTP/L2TP/IPsec)
- Support IPv6 protocol stack
- Support 802.11b/g/n and Mixed mode(optional) for WIFI,4 SSID
- Support VLAN division, based on physical port, SSID or IP address segment
- Support DHCP Server, DHCP Relay
- Support LTE

4G/5G ODU USER MANUAL

2.4 Technical Index

- 2000 new connections per second
- Maximum current connections:2000
- 5 IPsec VPN tunnels at least
- IPsec VPN tunnel throughput: 6Mbps
- Support 15000 routes
- Support SNMP、TR069 Protocol
- CLI
- Support graphical user interface management based on Web page

2.5 Environmental

Environmental requirements include power supply, storage temperature, working temperature and humidity.

- Power: 48V 0.32A
- Storage Temperature: -40°C - 70°C
- Long Time Working Temperature: -10°C - 50°C
- Short Time Working Temperature: -15°C - 60°C
- Humidity: 5% - 95% RH, No Coagulation

3. Configuration

3.1 Login

The Web interface is ready about one minute after the device power on. The default LAN IP address is 192.168.100.1(you can also access the Web interface via WAN port). Enter IP address in the address bar of web browser and then press ENTER, then it jumps to the Login interface as Figure 3-1 shows. Choose languages: English.



The screenshot shows the login page of the ODU web interface. At the top, there is a dark blue header with the word "Login" in yellow. Below the header, the text "ODU" is centered in a large, bold, black font. Underneath "ODU", there are three input fields: "Username", "Password", and "Language". The "Language" field is a dropdown menu with "English" selected and a downward arrow. Below these fields is a "Login" button.

Figure 3-1 Login Interface

3.2 Home

When logged in, current status information will be displayed: Serial Number, Software Version, CPU Usage and IP addresses.

4G/5G ODU USER MANUAL

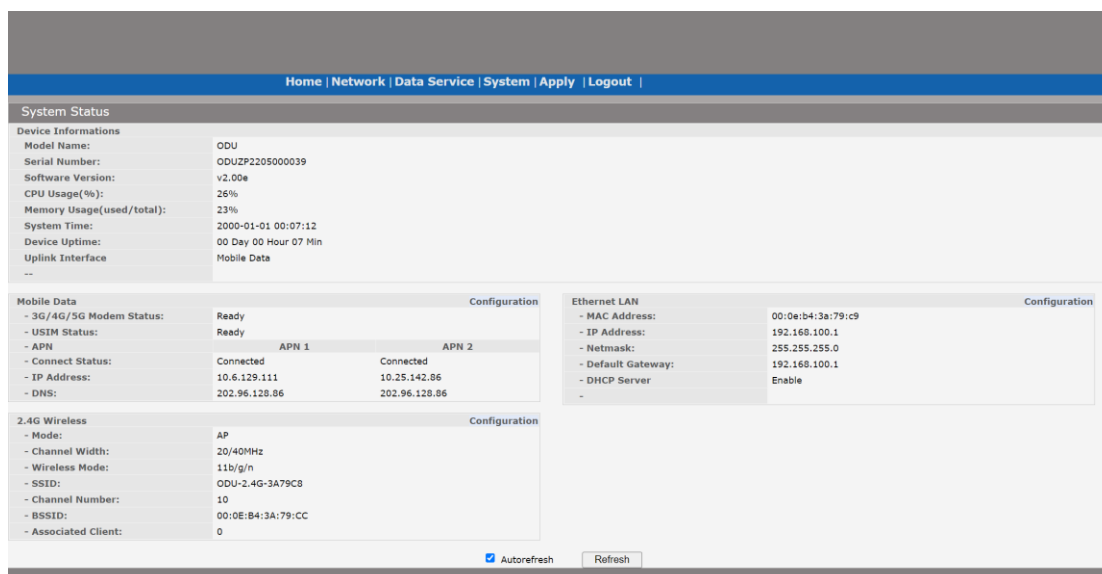


Figure 3-2 Home

4. Network

4.1 Network Management Summary

“Network” contains information of WAN port, LAN ports, VLAN ,LTE and IPv6.As shown in Figure 4-1.

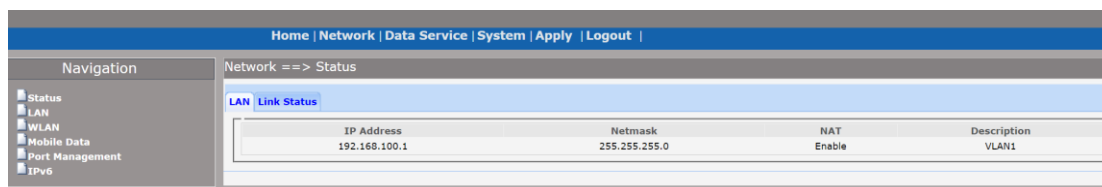


Figure 4-1 Network

“Network==>Status” shows the status of WAN port, LAN ports and link status. As shown in figure 4-2、figure 4-3.

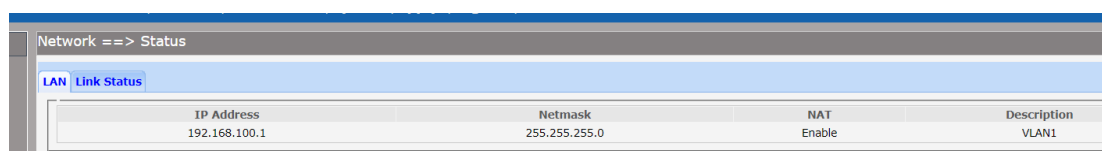
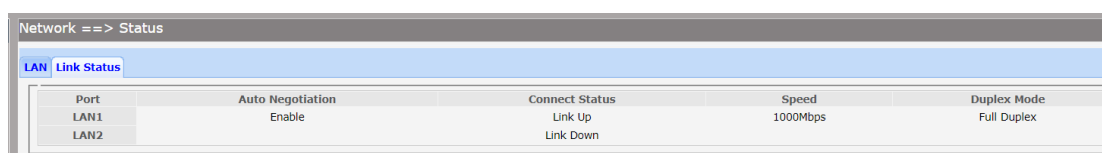


Figure 4-2 LAN port(s)



4G/5G ODU USER MANUAL

Figure 4-3 Link Status

4.2 LAN Port Configuration

Start LAN Port configuration by “Network==>LAN”, as shown in Figure 4-4.

Network ==> LAN

Interface Name	IP	Netmask	NAT	VID	LAN Bind	WAN Bind
VLAN1	192.168.100.1	255.255.255.0	Enable	--	1,2	D

Total 1 Pages, 1 Rows

WAN Bind Note: D(DATA); V(VOICE); M(MGMT); O1(OTHER1); O2(OTHER2);

AddDel

Port	Route/Bridge	VLAN ID List	Note Message
LAN1	Route		Route:route to WAN. Transparent bridge:not modify the packets. Tagged bridge:The first one is the default VID, the untag frame out from the WAN port with default VID; For the tagged frame, passed through the WAN port
LAN2	Route		Promisc Mode:Tagged packets in bridge mode, untagged packets in route mode,must 13 VIDs supported. (The vids' count should less than 13. e.g. 8,10,20-22,203).

SaveRefresh

Figure 4-4 LAN Ports

Click “VLAN1” to configure VLAN1 interface. As shown in Figure 4-5. Set IP address, “Netmask”, “NAT” and “DHCP” according to actual situation.

Network ==> LAN==> Static IP

Interface Name

VLAN1

IP Address

192.168.100.1

Netmask

255.255.255.0

NAT

☐ DATA

☐ DATA(specify Src IP)

☒ ANY_WAN

☐ APN1

☐ APN2

☐ DATA VPN

Enable DHCP Server

☒

Start IP

192.168.100.100

End IP

192.168.100.200

Netmask

255.255.255.0

Gateway

192.168.100.1

Primary DNS

192.168.100.1

Secondary DNS

8.8.8.8

Lease Time(Second)

86400

Option43

☐ Enable

☒ SubOption

Option42

☐ Enable

Address1

Address2

+Advanced Parameter

Save

Return

Figure 4-5 Interface Configuration

As shown in Figure 4-6, “Advanced Parameters” determines the binding relations between LAN ports and WAN Subinterfaces.

4G/5G ODU USER MANUAL

[-Advanced Parameter](#)

LAN Port	☒ LAN1	☒ LAN2
WAN Subinterface	☒ DATA	☐ VOICE ☐ MGMT ☐ OTHER1 ☐ OTHER2

Save Return

Figure 4-6 Advanced Parameter



Warning: IP addresses of WAN port and LAN ports mustn't be set to be in the same segment. And new IP address is only valid after reboot.

4.3 WLAN Configuration

Wi-Fi is a WLAN (Wireless Local Area Network) technology. It provides short-range wireless high-speed data connections between mobile data devices (such as laptops, PDAs or phones) and nearby Wi-Fi access points. 4G/5G ODU supports 4 SSID and WPS.

4.4.1 Basic settings

Start WLAN configuration by "Network==>WLAN==>Basic Settings".

Home | Network | Data Service | System | Apply | Logout |

Navigation: Status, LAN, WLAN, Mobile Data, Port Management, IPv6

Network ==> WLAN

Basic Settings | Security | WDS | Advanced Settings | Clients Info | MAC Filtering

Enable WiFi: ☒
 Enable Radio: ☒
 Channel: AutoSelect
 Wireless Mode: 11b/g/n
 Channel Width: 20/40MHz

Enable	SSID Name	Bind Interface	Enable Broadcast	Isolated	LAN Isolated	Max Client
☒	ODU-2.4G-3A79C8	VLAN1	☒	☐	☐	16
☐	ODU-2.4G-1-3A79C8	VLAN1	☒	☐	☐	16
☐	ODU-2.4G-2-3A79C8	VLAN1	☒	☐	☐	16
☐	ODU-2.4G-3-3A79C8	VLAN1	☒	☐	☐	16

Save Refresh

Figure 4-7 Basic Settings

The following items are displayed in Figure 4-7:

- **Enable WiFi:** Enable or disable the WIFI AP function globally.
- **Channel:** This field determines which operating frequency will be used. The default channel is set to AutoSelect, so the AP will choose the best channel automatically. It is not

4G/5G ODU USER MANUAL

necessary to change the wireless channel unless you notice interference problems with another nearby access point.

► **Wireless Mode:** Select the desired mode.

11b: Select if all of your wireless clients are 802.11b.

11g: Select if all of your wireless clients are 802.11g.

11n: Select only if all of your wireless clients are 802.11n.

11b/g: Select if you are using both 802.11b and 802.11g wireless clients.

11b/g/n: Select if you are using a mix of 802.11b, 11g and 11n wireless clients.

► **Channel Width:** Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients. If you choose 11n or 11b/g/n Wireless mode, this configuration is required. Two values of width are provided: 20MHz and 20/40MHz.

► **SSID:** is used to identify an 802.11 (Wi-Fi) network and it's discovered by network sniffing/scanning. 4G/5G ODU provides up to four SSID which supports up to 32 clients in total.

4.4.2 Security

Choose the menu "Network==>WLAN==>Security" to load the Security page. There are nine wireless security modes supported by the device: Open WEP, Shared WEP, WEP Auto, WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK, WPA, WPA2 and WPAWPA2. If you do not want to use wireless security, select "Disable", but it's strongly recommended to choose one of the following modes to enable security.

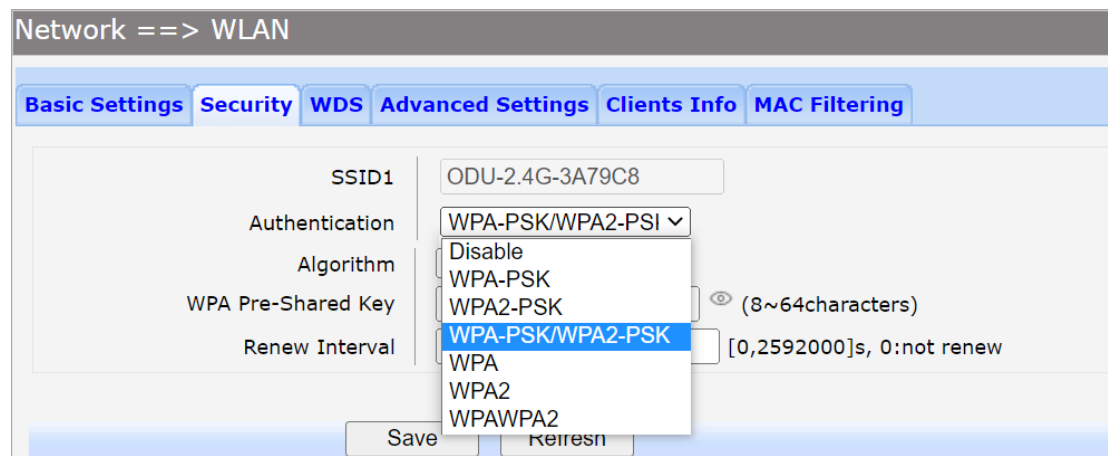


Figure 4-8 Security

Following items are displayed as shown in Figure 4-8:

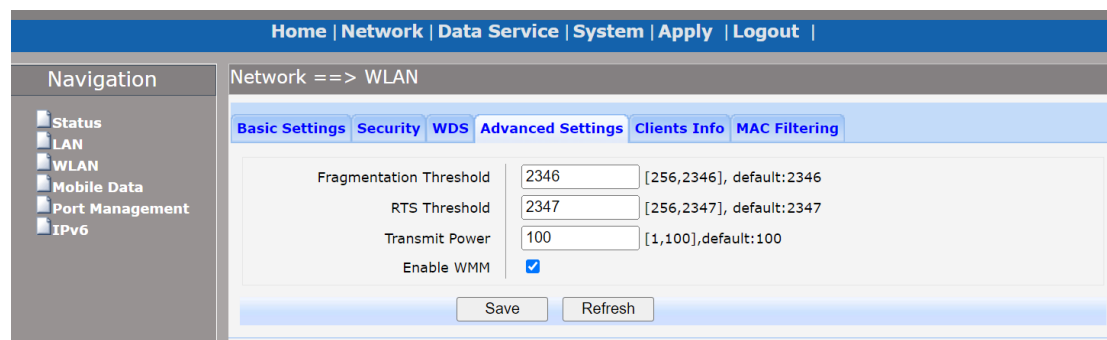
- **SSID:** The SSID enabled in WLAN→Basic Settings page. Read only
- **Authentication:** The authentication type selected: WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK.
- **Algorithm:** When WPA2-PSK or WPAPSK/WPA2PSK is set as the Authentication Type, you can select either TKIP, or AES or TKIP/AES as Encryption. When WPA-PSK is set as the Authentication Type, you can select either TKIP or AES as Encryption.

4G/5G ODU USER MANUAL

- WPA Pre-Shared Key: You can enter ASCII characters between 8 and 64 characters.
- Renew Interval: Specify the group key update interval in seconds. Enter 0 to disable the update.

4.4.3 Advanced Settings

Figure 4-11 shows content of “Network==>WLAN==>Advanced Settings”.



The screenshot shows the 'Advanced Settings' tab for WLAN. It includes a navigation menu on the left with options like Status, LAN, WLAN, Mobile Data, Port Management, and IPv6. The main content area has tabs for Basic Settings, Security, WDS, Advanced Settings (selected), Clients Info, and MAC Filtering. The settings include:

- Fragmentation Threshold: 2346 (range [256,2346], default:2346)
- RTS Threshold: 2347 (range [256,2347], default:2347)
- Transmit Power: 100 (range [1,100], default:100)
- Enable WMM: ☒

Buttons for 'Save' and 'Refresh' are at the bottom.

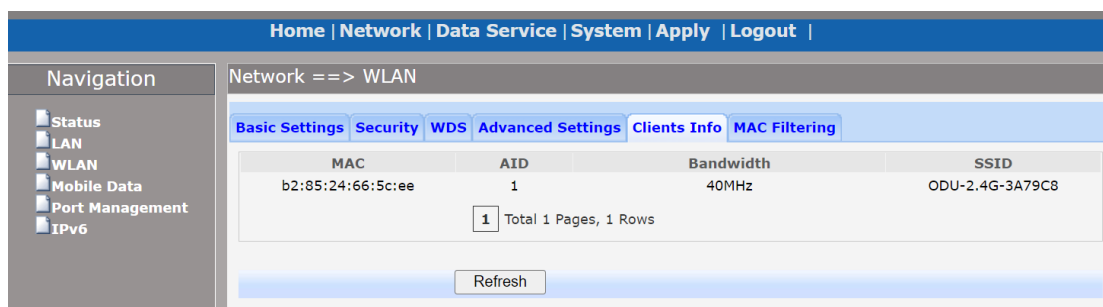
Figure 4-11 WLAN Advanced Settings

Following items are displayed in Figure 4-11:

- **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.
- **Transmit Power:** Here you can specify the transmit power of device. 100 is the default setting and is recommended.
- **Enable WMM:** Enable or disable the WIFI WMM function globally. WMM function can guarantee the packets with high-priority messages, being transmitted preferentially. It is strongly recommended enabled.

4.4.4 Clients Info

Choose the menu “Network==>WLAN==>Clients Info” to load the following page. As shown in Figure 4-12.



The screenshot shows the 'Clients Info' tab for WLAN. It includes the same navigation menu as Figure 4-11. The main content area has tabs for Basic Settings, Security, WDS, Advanced Settings, Clients Info (selected), and MAC Filtering. It displays a table with the following data:

MAC	AID	Bandwidth	SSID
b2:85:24:66:5c:ee	1	40MHz	ODU-2.4G-3A79C8

Below the table, it shows '1 Total 1 Pages, 1 Rows' and a 'Refresh' button.

Figure 4-12 Clients Info

4G/5G ODU USER MANUAL

4.4.5 MAC Filtering

You can control the wireless access by configuring the Wireless MAC Filtering function. Choose the menu “Network→WLAN→MAC” **Filtering** to load the following page as shown in Figure 4-13.

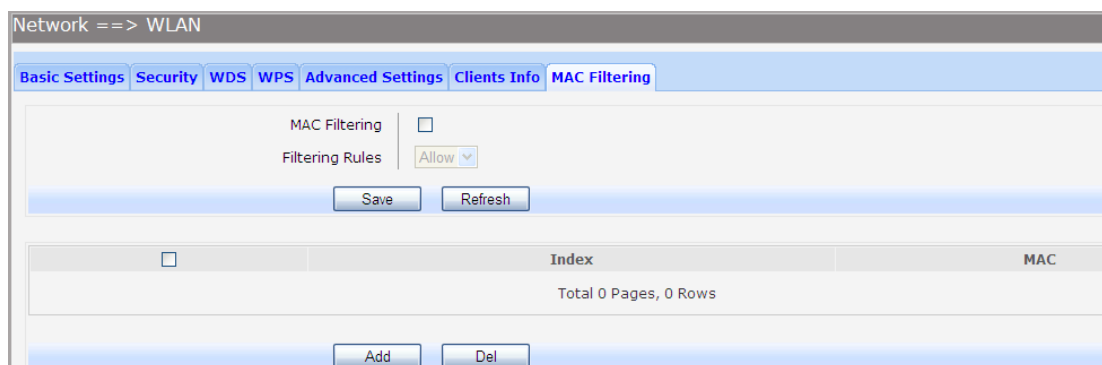


Figure 4-13 MAC filtering

The following items are displayed:

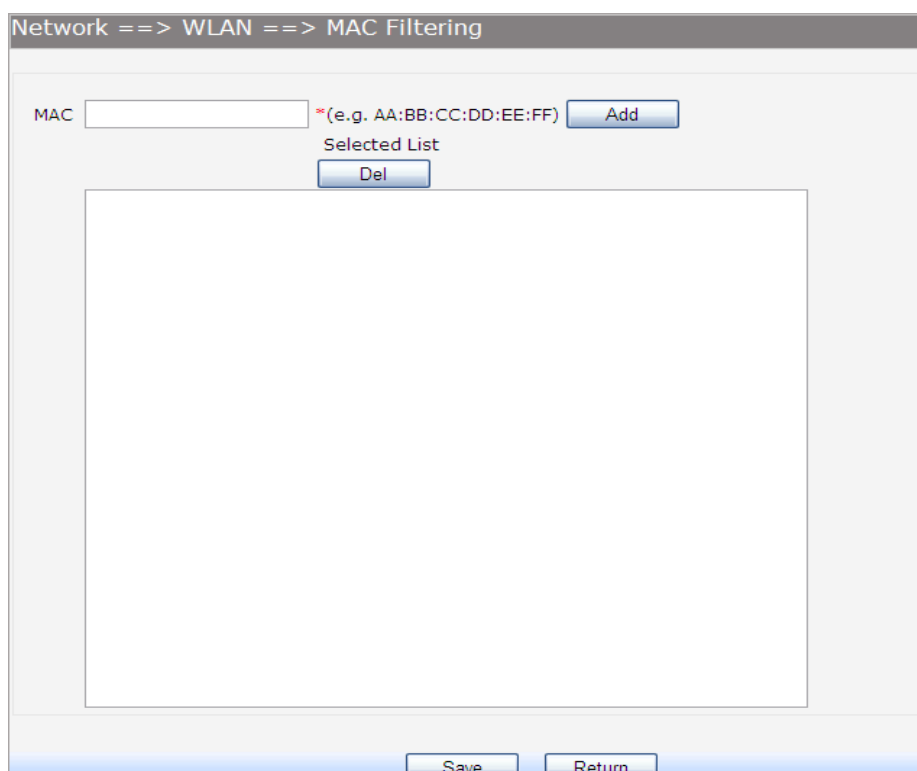
► **MAC Filtering:** Enable or disable the Wifi MAC filtering function globally. ►

Filtering Rules: Two MAC filtering rules are provided:

Allow: allow the stations specified by entries in the list to access.

Deny: deny the stations specified by entries in the list to access.

To delete Wireless MAC Address filtering entries, select the entries and click the **Del** button. To Add a Wireless MAC Address filtering entry, click the **Add** button.



4G/5G ODU USER MANUAL

Figure4-14 MAC Filtering Table

4.4 Mobile Data

Typically, LTE Modem is used as uplink port as a backup of WAN. Insert LTE Modem into USB port, after dialing successful, LTE Modem will serve as a backup uplink usage.

4.5.1 Basic settings

Choose the menu **Network**→**Mobile Data** to load the following page.

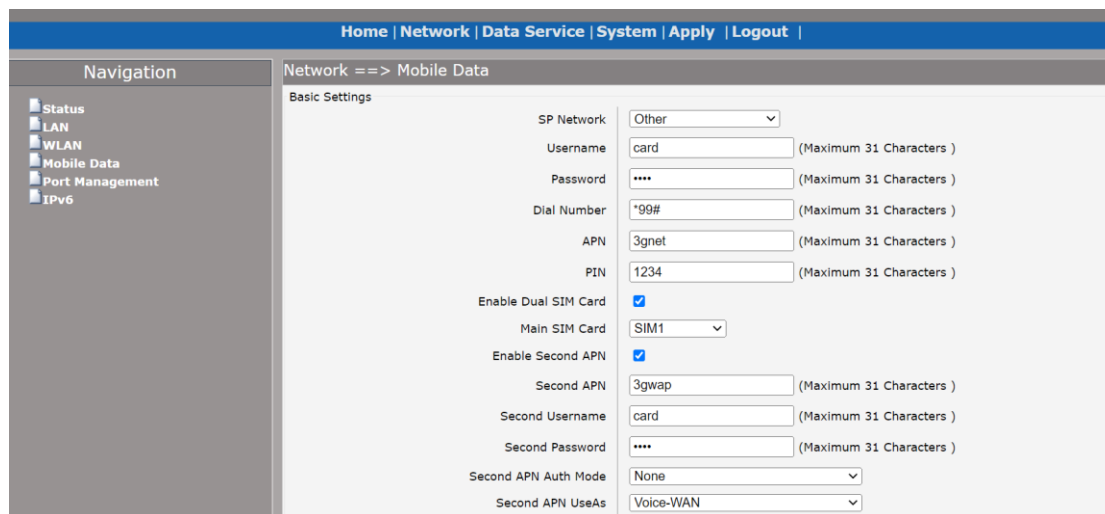


Figure 4-15 LTE Basic settings

The following items are displayed in Figure 4-15:

- ▶ **SP Network:** Other or Swisscom. If it is not the target user, you need to select the other.
- ▶ **Username:** LTE network dial-up username.
- ▶ **Password:** LTE network dial-up password.
- ▶ **Dial Number:** LTE network dial numbers.
- ▶ **APN:** LTE network access APN.
- ▶ **PIN:** LTE networks need to use dial-up PIN code, if not, set to empty.
- ▶ **Enable Dual SIM Card:** Enable or Disabled dual SIM card
- ▶ **Main SIM Card:** Select a card as main SIM card
- ▶ **Enable Second APN:** If there's a second APN, enable it
- ▶ **Second APN:** LTE network access second APN
- ▶ **Second Username:** LTE network dial-up second username.
- ▶ **Second Password:** LTE network dial-up second password.
- ▶ **Second APN Auth Mode:** Select the auth mode for second APN. Selectable: Pap, Chap, Chav2

4G/5G ODU USER MANUAL

► **Second APN UseAs:** Select Voice-WAN or Mgmt-WAN.

4.5.2 LTE Advanced Parameters

Choose the menu **Network→Mobile Data→Advanced Parameters** to load the following page.:

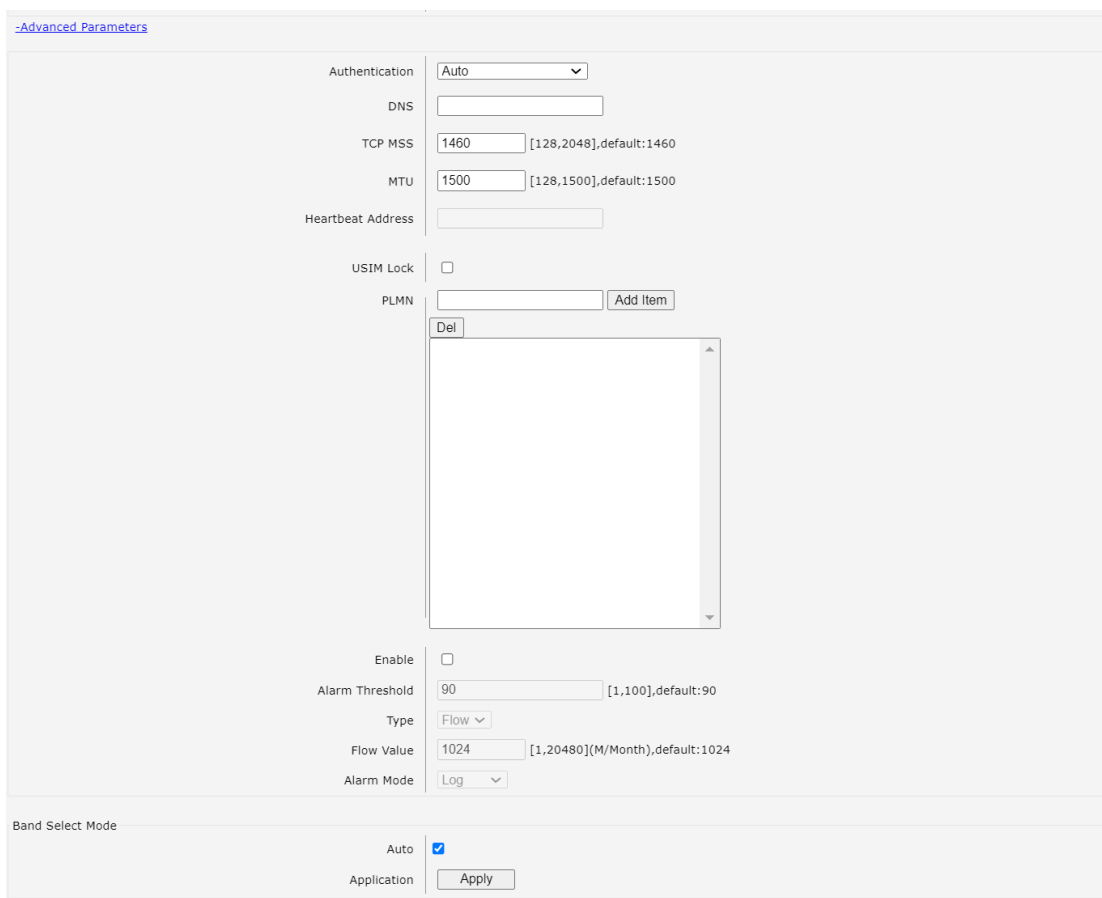


Figure 4-16 LTE Advanced Parameters

The following items are displayed in Figure 4-16:

- **Band Select Mode:** Choose FDD-LTE/TDD-LTE
- **Application:** Apply

4G/5G ODU USER MANUAL

4.5.3 Status

Status		
Modem Status	Ready	
SIM Card Status	Ready	
Operation Name	CHN-CT	
Signal Quality	-77dBm	
Connection Status	Connected	
Connect Time	00:03:38	
Uplink Current Speed	72 bps	
Downlink Current Speed	0 bps	
Uplink/Downlink Traffic	6.0 KB/ 0.0 B	
RSSI	N/A	
RSRP	-77 dBm	
RSRQ	-11 dB	
IMSI	460110403568492	
PCI	877	
Cell Id	75894D087	
Connected band	78	
PLMN	46011	
Connected Network Type	5G SA	
IMEI	869814060013756	
TAC	752A14	
Earfcn	627264	
DL Bandwidth	100 MHz	
Connected APN	3gnet	

Figure 4-17 LTE Status

The following items are displayed in Figure 4-17:

- ▶ **Modem Status:** Indicates whether to insert LTE module.
- ▶ **SIM Card Status:** Indicates whether to insert LTE modem in the SIM card, the ready state means the SIM card is detected.
- ▶ **Operation Name:** LTE modem Product Type.
- ▶ **Signal Quality:** Signal quality of LTE Modem, up to 31.
- ▶ **Connection Status:** Connected or disconnected.
- ▶ **Connect Time:** Connected time.
- ▶ **Uplink Current Speed:** Speed of uplink.
- ▶ **Downlink Current Speed:** Speed of downlink.
- ▶ **Uplink/Downlink Traffic:** Traffic of Up/Downlink.
- ▶ **RSSI:** Received Signal Strength Indication.
- ▶ **RSRP:** Reference Signal Receiving Power.
- ▶ **RSRQ:** Reference Signal Receiving Quality.
- ▶ **IMSI:** International Mobile Subscriber Identification Number.

4G/5G ODU USER MANUAL

- ▶ **PCI:** Physical Cell Identifier.
- ▶ **Cell Id:** Cell Identifier.
- ▶ **Connected band:** The band that connected.
- ▶ **PLMN:** Public Land Mobile Network.
- ▶ **Connected Network Type:** Connected Network Type.
- ▶ **IMEI:** International Mobile Equipment Identity.
- ▶ **TAC:** Tracking Area Code
- ▶ **Earfcn:** E-UTRA Absolute Radio Frequency Channel Number
- ▶ **DL Bandwidth:** Download Bandwidth
- ▶ **Connected APN:** The APN now connecting

4.5 IPv6

Choose the menu **Network**→**IPv6** to load the following two pages.

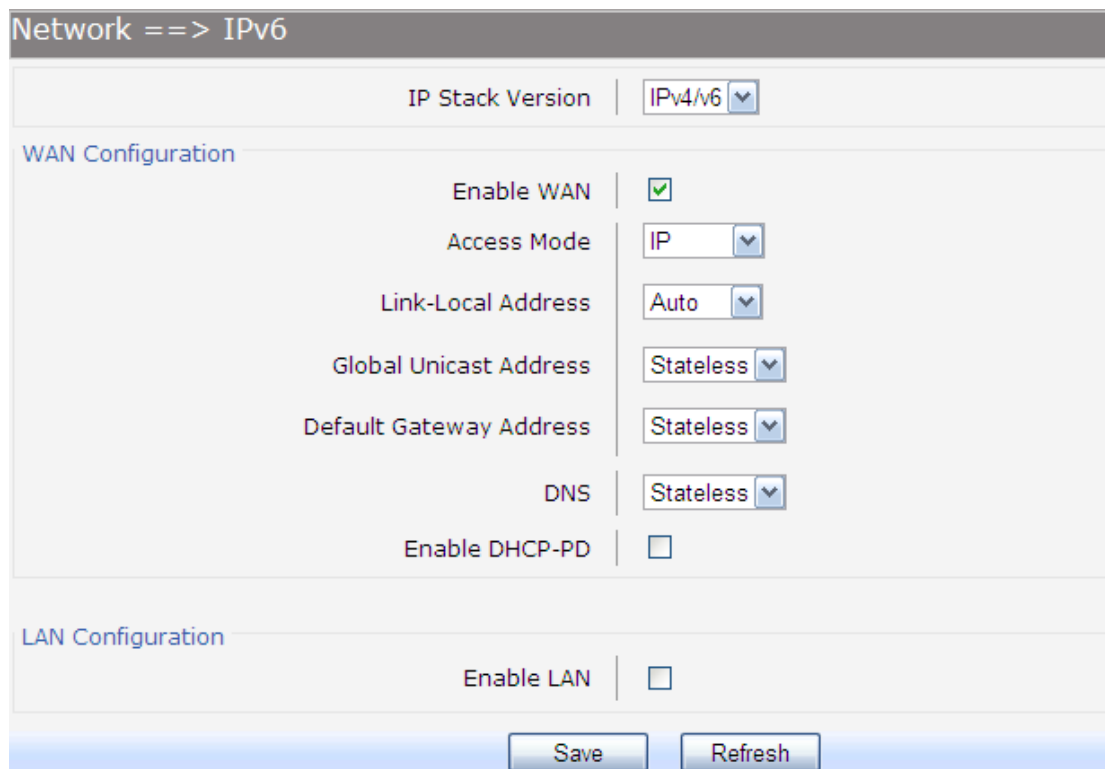


Figure 4-18 IPv6 WAN Configuration

The following items are displayed in Figure 4-18:

- ▶ **IP Stack Version:** Choose the IP stack version to use. Provides the following three types: IPv4, IPv6, IPv4/v6.

WAN Configuration

- ▶ **Enable WAN:** If IPv6 or IPv4/v6 is chosen, select this to enable IPv6 stack on WAN.
- ▶ **Access Mode:** Select access mode of WAN: IP or PPP.
- ▶ **Link-Local Address:** Select type of Link-Local address: Auto or Manual. If Manual is selected, you should specify address manually.
- ▶ **Global Unicast Address:** Stateless, Manual, DHCPv6. If Manual is selected, you

4G/5G ODU USER MANUAL

should specify address manually.

- **Default Gateway Address:** Stateless,Manual. If Manual is selected, you should specify address manually.
- **DNS:** Stateless,Manual,DHCPv6. If Manual is selected, you should specify DNS manually.
- **Enable DHCP-PD:** Whether to enable DHCP-PD(prefix delegation) on WAN.

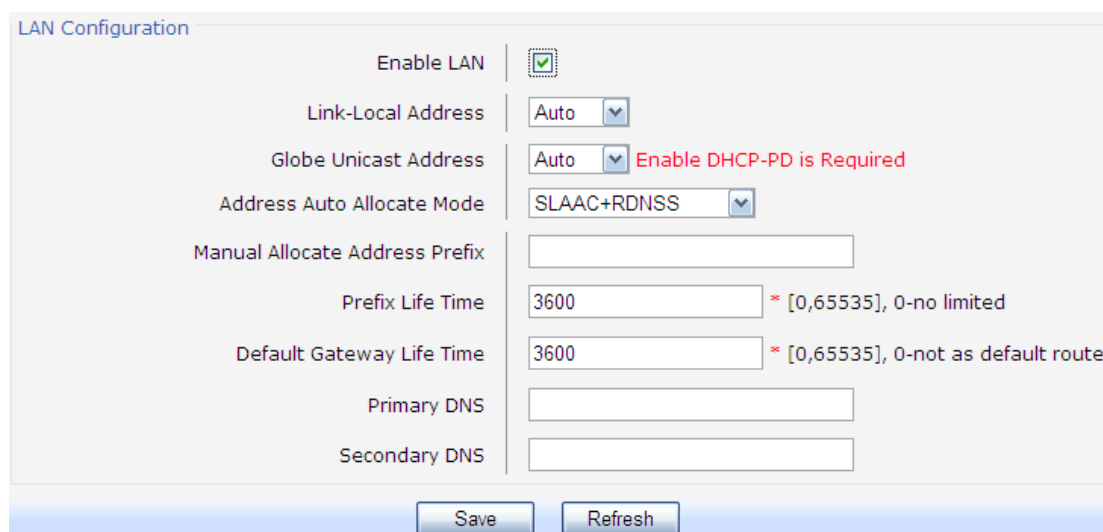


Figure 4-19 IPv6 LAN Configuration

LAN Configuration as shown in Figure 4-19:

- **Enable LAN:** If IPv6 or IPv4/v6 is chosen, select this to enable IPv6 stack on LAN.
- **Link-Local Address:** Select type of Link-Local address: Auto or Manual. If Manual is selected, you should specify address manually.
- **Global Unicast Address:** Manual,Auto. If Manual is selected, you should specify address manually.
- **Address Auto Allocate Mode:** SLAAC+RDNSS(Recursive DNS Server) SLAAC(Stateless address autoconfiguration)+DHCPv6 DHCPv6
- **Manual Allocate Address Prefix:** Configure the manual allocate address prefix. ►
- Prefix Life Time:** Enter the life time of prefix.
- **Default Gateway Life Time:** Enter the life time of default gateway.
- **Primary DNS:** Enter the primary DNS address.
- **Secondary DNS:** Enter the secondary DNS address.

4G/5G ODU USER MANUAL

5. Data Service

4G/5G ODU has many powerful data functions, it provides data services of DHCP server, QoS, DDNS, L2TP, PPTP, IPSec, DMZ, PAT, firewall, LTE modem, ALG, etc.

5.1 Service Status

Check the Data service status at “Data Service==>Status”. The Status includes Service State, ARP Table, Route Table and Net State, all of which shows the read-only data information. As show in the following four figures.

Data Service ==> Status

Service State ARP Table Route Table Net State

Enable WiFi	☒	Enable Internet Web Access	☒
Enable QoS	☐	Enable UPnP	☒
Enable DDNS	☐	Enable Port Mirror	☐
Enable DMZ	☐	Enable MAC Filter	☐
Enable L2TP Server	☐	Enable Access Control	☐
Enable PPTP Server	☐	Enable ARP Attack Defense	☐

Figure 5-1 Service State

Data Service ==> Status

Service State ARP Table Route Table Net State

IP Address	Flag	HW Address	Interface
192.168.100.90	0x2	74:d4:35:49:5b:7c	br0

1 Total 1 Pages, 1 Rows

Figure 5-2 ARP Table

Data Service ==> Status

Service State ARP Table Route Table Net State

Index	interface
1	from all lookup local
2	from all lookup 1
3	from all fwmark 0x3e8 lookup 2
4	from all fwmark 0x3e9 lookup 3
5	from all fwmark 0x3ea lookup 4
6	from all fwmark 0x3eb lookup 5
7	from all fwmark 0x3ec lookup 6
8	from all lookup main
9	from all lookup default

1 Total 1 Pages, 9 Rows

Figure 5-3 Route Table

4G/5G ODU USER MANUAL

Data Service ==> Status

Service State ARP Table Route Table Net State			
Protocol	Local Address	Foreign Address	State
TCP	0.0.0.0:8099	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:9443	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:9100	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:80	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:53	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:22	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:23	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:24	0.0.0.0:0	TCP_LISTEN
TCP	192.168.100.1:80	192.168.100.1:15158	TCP_ESTABLISHED
TCP	192.168.100.1:80	192.168.100.1:15087	TCP_TIME_WAIT
TCP	192.168.100.1:80	192.168.100.1:15157	TCP_ESTABLISHED
TCP	192.168.100.1:80	192.168.100.1:15159	TCP_ESTABLISHED
TCP	192.168.100.1:80	192.168.100.1:15161	TCP_ESTABLISHED
TCP	192.168.100.1:80	192.168.100.1:15156	TCP_ESTABLISHED
TCP	192.168.100.1:80	192.168.100.1:15094	TCP_TIME_WAIT
TCP	192.168.100.1:80	192.168.100.1:15160	TCP_ESTABLISHED
UDP	169.254.254.1:1025	169.254.254.1:0	
UDP	0.0.0.0:53	0.0.0.0:0	
UDP	0.0.0.0:67	0.0.0.0:0	
UDP	0.0.0.0:50000	0.0.0.0:0	

Total 2 Pages, 24 Rows

Figure 5-4 Net State

5.2 DHCP Server

5.2.1 Static Address Assign

Choose the menu **Data Service→DHCP Server→Static Address Assign**, and then you can view and add address which is assigned for clients(As shown in Figure 5-5). When you specify a static IP address for a client on the LAN, that client will always receive the same IP address each time when it accesses the DHCP server. The Reserved IP addresses should be assigned to the devices that require permanent IP settings.

Data Service ==> DHCP Server

Static Address Assign Status DHCP Relay					
☐	Index	IP	Netmask	MAC	Description
Add Del					

Figure 5-5 Static Address Assign

Click the Index in the entry you want to modify. If you want to delete the entry, select it and click the “Del”. Click the “Add” button to add a new entry.

Data Service ==> DHCP

Client IP Address	192.168.0.30	* For example: 192.168.0.30
Client Mask	255.255.0.0	* For example: 255.255.0.0
Client MAC	01:02:03:04:05:06	* For example: 01:02:03:04:05:06
Description	Client1	

Figure 5-6 Add Static DHCP Address

4G/5G ODU USER MANUAL

5.2.2 DHCP Relay

Start DHCP Relay by “Data Service==>DHCP Server==>DHCP Relay”.

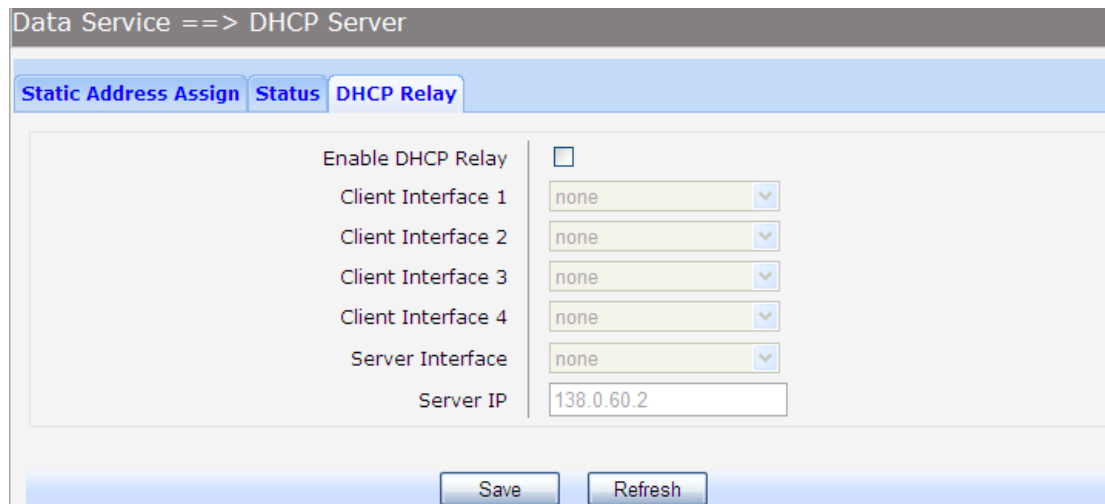


Figure 5-7 DHCP Relay

The following items are displayed in Figure 5-7:

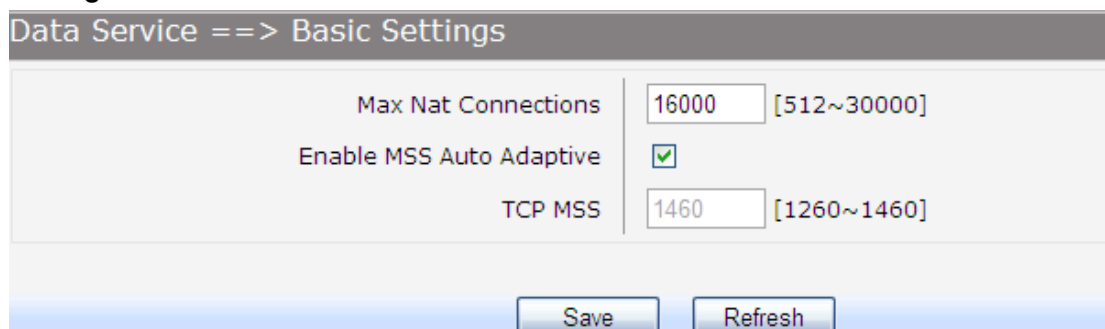
- ▶ **Enable DHCP Relay:** Enable or disable DHCP Relay.
- ▶ **Client Interface:** The interface to listen for DHCP client requests. Up to four interfaces can be selected.
- ▶ **Server Interface:** Choose the interface which connects DHCP server.
- ▶ **Server IP:** Configure the DHCP server IP address.

5.3 NAT Config

Network Address Translation (NAT) is a network protocol used in IPv4 networks that allows multiple devices to connect a network protocol using the same public IPv4 address. NAT was originally designed in an attempt to help conserve IPv4 addresses. NAT modifies the IP address information in IPv4 headers while in transit across a traffic routing device.

Basic settings

Start NAT Basic settings by **Data Service==>NAT Config==>Basic settings**



4G/5G ODU USER MANUAL

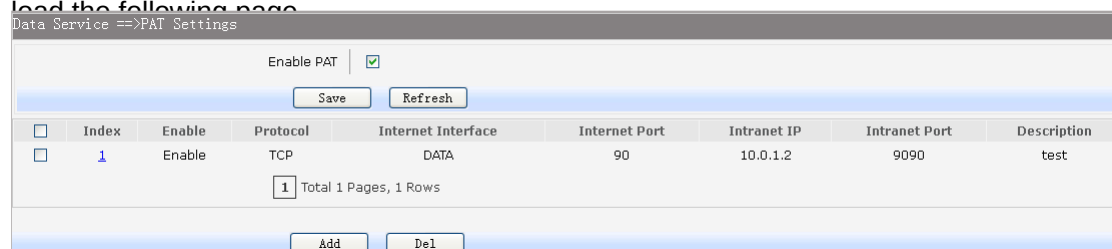
Figure 5-8 NAT Basic Settings

The following items are displayed in Figure 5-8:

- ▶ **Max Nat Connections:** Specify the maximum number of NAT connections.
- ▶ **Enable MSS Auto Adaptive:** Enable or disable auto adaptive the value of MSS(Maximum Segment Size).
- ▶ **TCP MSS:** If Enable MSS Auto Adaptive is not selected, configure this to specify the maximum segment size of the TCP protocol.

5.3.1 Port Forwarding Settings

Several internal addresses can be NATed to only one or a few external addresses by using a feature called overload, which is also referred to as PAT. PAT is a subset of NAT functionality, where it maps several internal addresses to a single external address. PAT statically uses unique port numbers on a single outside IP address to distinguish between the various translations. Choose the menu **Data Service**→**NAT Config**→**PAT Settings** to load the following page.



Data Service ==> PAT Settings

Enable PAT ☒

Save Refresh

☐	Index	Enable	Protocol	Internet Interface	Internet Port	Intranet IP	Intranet Port	Description
☐	1	Enable	TCP	DATA	90	10.0.1.2	9090	test

1 Total 1 Pages, 1 Rows

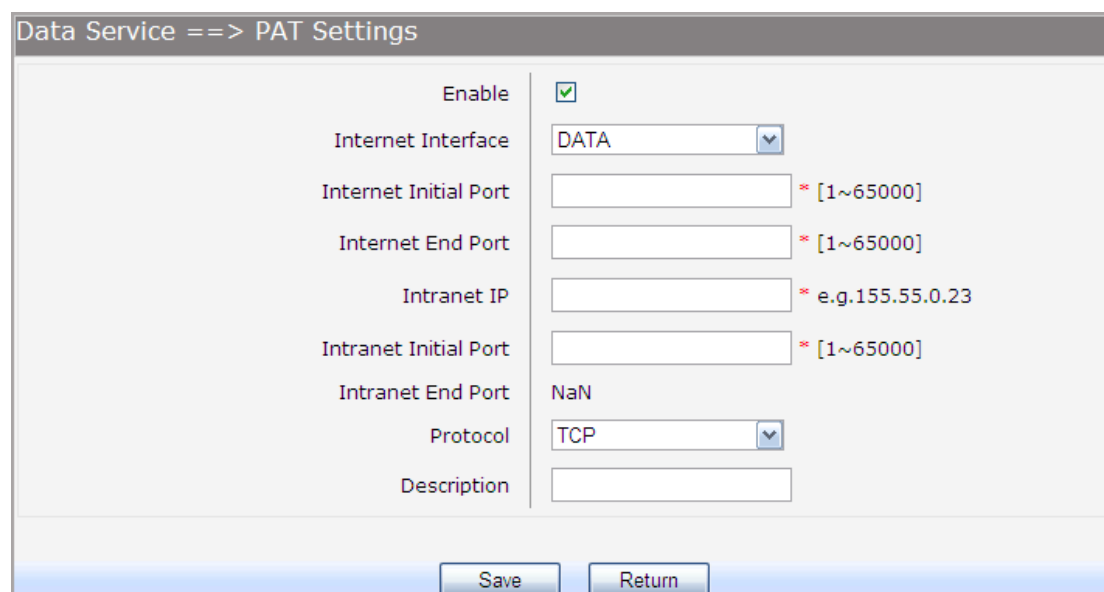
Add Del

Figure 5-9 PAT Basic settings

The following items are displayed in Figure 5-9:

- ▶ **Enable PAT:** Enable or disable PAT globally.

Click the Index in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.



Data Service ==> PAT Settings

Enable ☒

Internet Interface DATA

Internet Initial Port [1~65000]

Internet End Port [1~65000]

Intranet IP e.g.155.55.0.23

Intranet Initial Port [1~65000]

Intranet End Port NaN

Protocol TCP

Description

Save Return

Figure 5-10 Add PAT

The following items are displayed in Figure 5-10:

- ▶ **Enable:** Enable or disable this PAT entry.

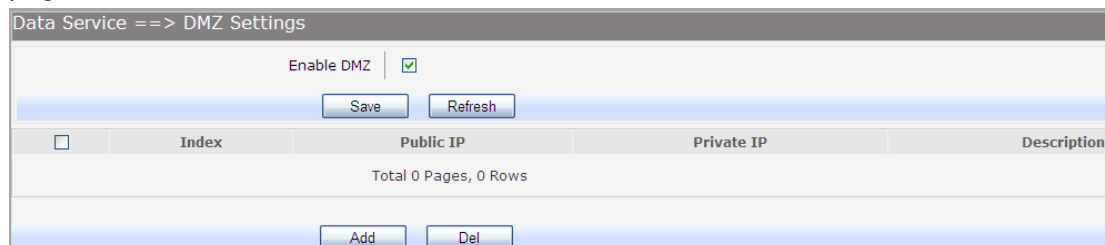
4G/5G ODU USER MANUAL

- **Internet Port:** Enter the service port provided for accessing external network. All the requests from internet to this service port will be redirected to the specified server in local network.
- **Intranet Port:** Specify the service port of the LAN host as virtual server.
- **Intranet IP:** Enter the IP address of the specified internal server for the entry. All the requests from the internet to the specified LAN port will be redirected to this host.
- **Protocol:** Specify the protocol used for the entry.
- **Internet Interface:** Specify the interface to receive requests from the internet for the entry.
- **Description:** Enter a name for Virtual Server entry.

5.3.2 DMZ

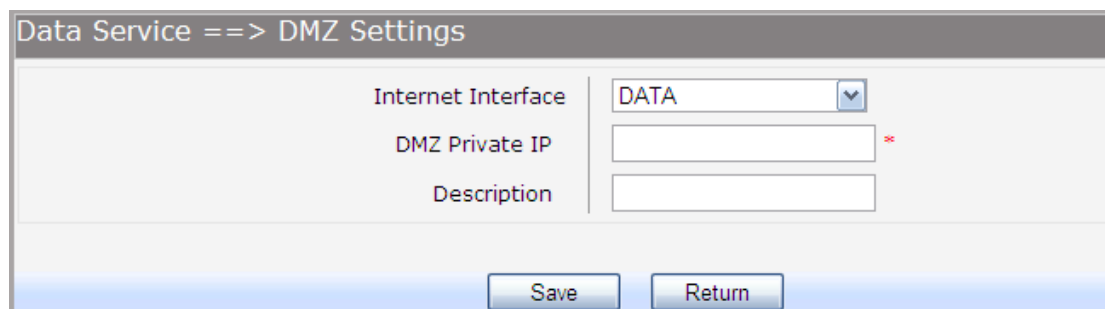
In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical network that contains and exposes an organization's external-facing services to a larger and insecure network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

Choose the menu “Data Service→NAT Config→DMZ Settings” to load the following page.



The screenshot shows the "Data Service ==> DMZ Settings" page. At the top, there is a checkbox for "Enable DMZ" which is checked. Below it are "Save" and "Refresh" buttons. A table with columns "Index", "Public IP", "Private IP", and "Description" is shown, but it is empty. Below the table, it says "Total 0 Pages, 0 Rows". At the bottom, there are "Add" and "Del" buttons.

Figure5-11 Existed DMZ



The screenshot shows the "Data Service ==> DMZ Settings" page with the "Add DMZ" form. It includes fields for "Internet Interface" (set to "DATA"), "DMZ Private IP" (with a red asterisk indicating a required field), and "Description". At the bottom, there are "Save" and "Return" buttons.

Figure 5-12 Add DMZ

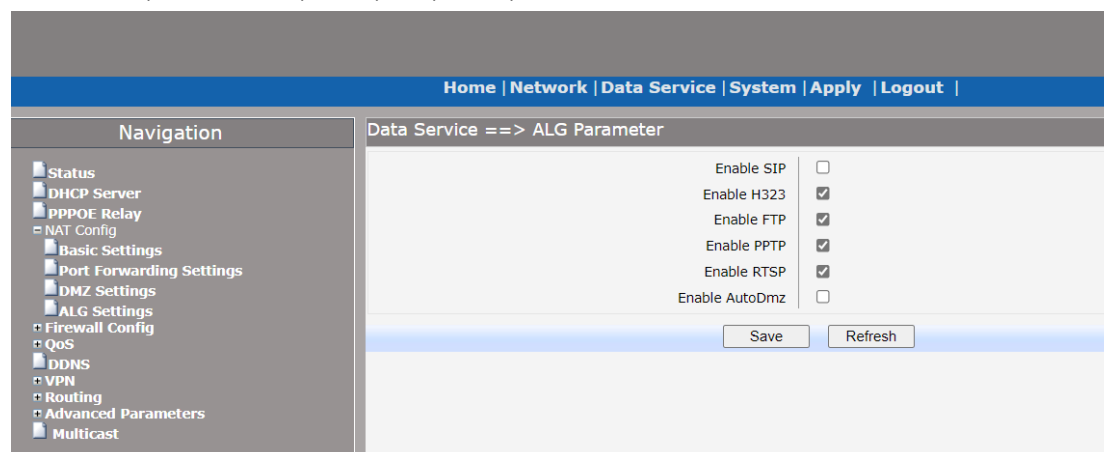
The following items are displayed in Figure 5-12:

- **Internet Interface:** The interface for this DMZ entry.
- **DMZ Private IP:** The private IP address for this DMZ entry.
- **Description:** Enter a description string for this DMZ entry

4G/5G ODU USER MANUAL

5.3.3 ALG Settings

Application Layer Gateway technology can allow some application traffic passthrough the firewall,such as SIP,H323,FTP,PPTP,RTSP.



5.4 Firewall Config

With Attack Defense function enabled, the device can distinguish the malicious packets and prevent the port scanning from external network, so as to guarantee the network security. Configure this for abnormal packets defense and flood attack defense. Flood attack is a commonly used DoS (Denial of Service) attack, including TCP SYN, UDP, ICMP, and so on.

5.4.1 Attack Defense

Choose the menu “**Data Service→Firewall Config→Attack Defense**” to load the following page shown in Figure 5-13.

4G/5G ODU USER MANUAL

Data Service ==> Attack Defense

Generic Downstream Access Control

Enable Broadcast Storm Defense	☐
Enable Block Ping	☐
Enable TCP SYN Flood Defense	☐ 50 [1~1000](packets/second)
Enable UDP Flood Defense	☐ 50 [1~1000](packets/second)
Enable ICMP Defense	☒ 50 [1~1000](packets/second)
Enable ARP Attack Defense	☐
Enable Port Scan Defense	☐
Enable Land Based Defense	☐
Enable Ping Of Death Defense	☐
Enable Teardrop Defense	☐
Enable Fraggle Defense	☐
Enable Smurf Defense	☐
Enable Reject Direct IP call	☐
Enable Filter Invaoid Packet	☐

Save Refresh

Figure 5-13 Attack Defense

The following items are displayed in Figure 5-13:

- ▶ **Enable Broadcast Storm Defense:** Enable or disable Broadcast Storm Defense.
- ▶ **Enable Block Ping:** Enable or disable Block Ping function.
- ▶ **Enable TCP SYN Flood Defense:** Enable or disable TCP SYN Flood Defense.
- ▶ **Enable UDP Flood Defense:** Enable or disable UDP Flood Defense.
- ▶ **Enable ICMP Defense:** Enable or disable ICMP Defense.
- ▶ **Enable ARP Attack Defense:** Enable or disable ARP Attack Defense.
- ▶ **Enable Port Scan Defense:** A port scanner is a software application designed to probe a server or host for open ports. Check the box to prevent port scanning.
- ▶ **Enable Land Based Defense:** The Land Denial of Service attack works by sending a spoofed packet with the SYN flag - used in a "handshake" between a client and a host - set from a host to any port that is open and listening. If the packet is programmed to have the same destination and source IP address, when it is sent to a machine, via IP spoofing, the transmission can fool the machine into thinking it is sending itself a message, which, depending on the operating system, will crash the machine. Check the box to enable Land Based Defense.
- ▶ **Enable Ping Of Death Defense:** Ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. Check the box to enable Ping of Death Defense.

4G/5G ODU USER MANUAL

- **Enable Teardrop Defense:** Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Check the box to enable Teardrop Defense.
- **Enable Fraggle Defense:** A fraggle attack is a variation of a Smurf attack where an attacker sends a large amount of UDP traffic to ports 7 (echo) and 19 (chargen) to an IP Broadcast Address, with the intended victim's spoofed source IP address. Check the box to enable Fraggle Defense.
- **Enable Smurf Defense:** The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Check the box to enable Smurf Defense..

5.4.2 Service Type

Service Type defines the entry with protocol and port range, which can be chosen in Internet Access-Ctrl page.

Choose the menu “Data Service→Firewall Config→Service Type” to load the following page. Figure 5-13 shows the existed service type. Click the Index in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add**

Data Service ==> Service Type

☐	Index	Name	Protocol	Port Range	Description
☐	1	type1	TCP	1000--2000	test

1 Total 1 Pages, 1 Rows

Add Del

Figure 5-14 Existed Service Type

Data Service ==> Firewall

Name		*
Protocol	UDP	
Port Range	1 -- 65535	* [1~65535]
Description		

Save Return

Figure 5-15 Add Service Type

The following items are displayed in Figure 5-15:

- **Name:** Name of this entry, it will be list in Internet Access-Ctrl page.
- **Protocol:** Select the protocol for this entry. Four types are provided: TCP, UDP, ICMP and ALL.
- **Port Range:** Configure the port range for this entry.
- **Description:** Enter a description string for this entry

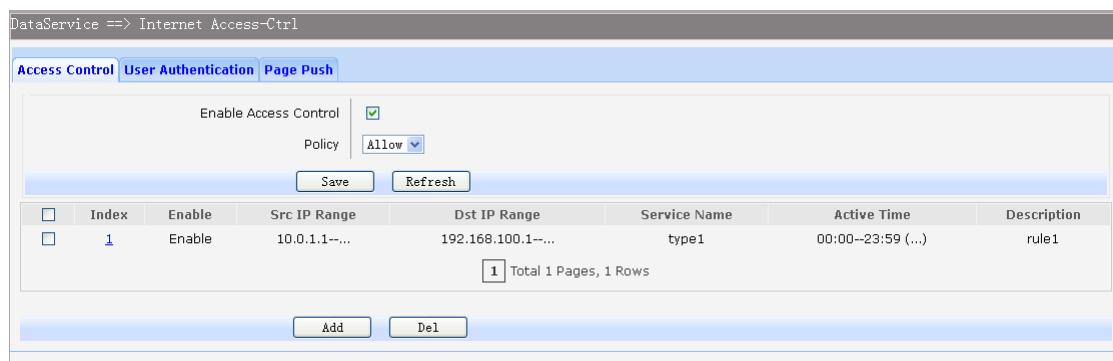
4G/5G ODU USER MANUAL

5.4.3 Internet Access Control

Each sub-page under this page is used to control Internet access.

5.4.3.1 Access Control

This sub-page is used to control Internet access through IP, port, and time. Choose the menu “**Data Service**→**Firewall Config**→**Internet Access-Ctrl**→**Access Control**” to load the following page.



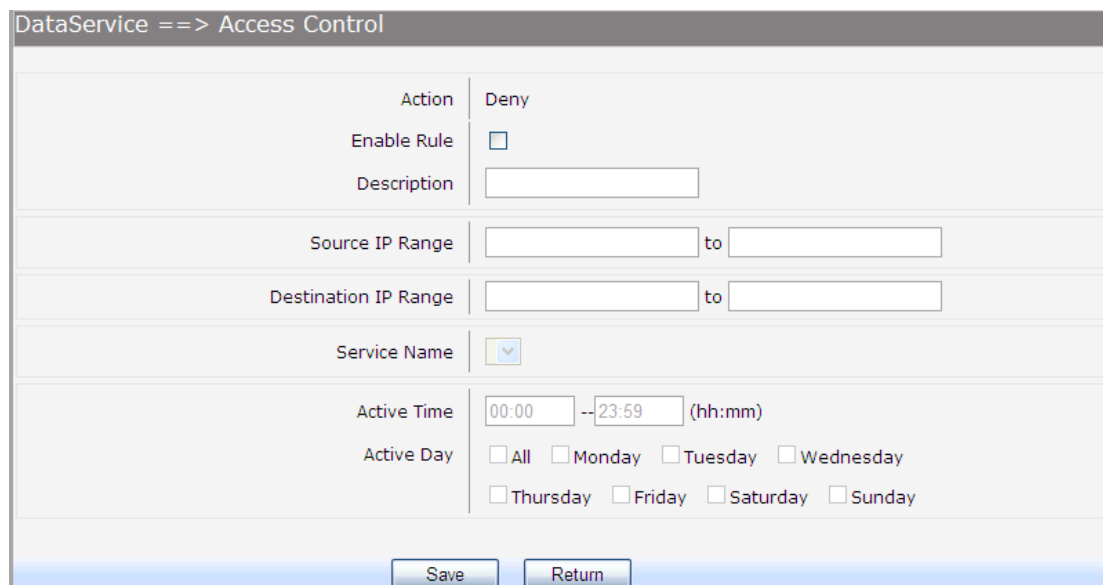
The screenshot shows the 'Access Control' configuration page. At the top, there are tabs: 'Access Control', 'User Authentication', and 'Page Push'. Below the tabs, there is a section for 'Enable Access Control' with a checked checkbox and a 'Policy' dropdown set to 'Allow'. There are 'Save' and 'Refresh' buttons. Below this is a table with the following columns: Index, Enable, Src IP Range, Dst IP Range, Service Name, Active Time, and Description. The table contains one row with Index 1, Enable checked, Src IP Range 10.0.1.1-..., Dst IP Range 192.168.100.1-..., Service Name type1, Active Time 00:00--23:59 (...), and Description rule1. Below the table, there are 'Add' and 'Del' buttons.

Figure 5-16 Access Control

The following items are displayed in Figure 5-16:

- **Enable Access Control:** Enable or disable access control from WAN.
- **Policy: Default policy of access control:** Allow or Deny. If Allow is selected, all packets will be allowed except the entries list on this page. If Deny is selected, all packets will be denied except the entries list on this page.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry (As shown in Figure 5-17).



The screenshot shows the 'Add Access Control' configuration page. It has a title bar 'DataService ==> Access Control'. The page is divided into several sections: 'Action' with a 'Deny' dropdown; 'Enable Rule' with an unchecked checkbox; 'Description' with a text input field; 'Source IP Range' with two text input fields separated by 'to'; 'Destination IP Range' with two text input fields separated by 'to'; 'Service Name' with a dropdown menu; 'Active Time' with two time input fields (00:00 and 23:59) and '(hh:mm)' label; and 'Active Day' with checkboxes for All, Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday. At the bottom, there are 'Save' and 'Return' buttons.

Figure 5-17 Add Access Control

The following items are displayed in Figure 5-17:

4G/5G ODU USER MANUAL

- ▶ **Action:** The policy of this entry, Allow or Deny. It is the inverse of **Policy**. Read only.
- ▶ **Enable Rule:** Enable or disable this rule.
- ▶ **Description:** Enter a description string for this rule
- ▶ **Source IP Range:** Enter the source IP range in dotted-decimal format (e.g. 192.168.1.23).
- ▶ **Destination IP Range:** Enter the destination IP range in dotted-decimal format (e.g. 192.168.1.23).
- ▶ **Service Name:** Choose a service type that defined in **Service Type** page.
- ▶ **Active Time:** Specify the time range for the entry to take effect.
- ▶ **Active Day:** Specify the day range for the entry to take effect.

5.4.3.2 User Authentication

This sub-page is used to control Internet access through username and password. Choose the menu **Data Service**→**Firewall Config**→**Internet Access-Ctrl**→**User Authentication** to load the following page.

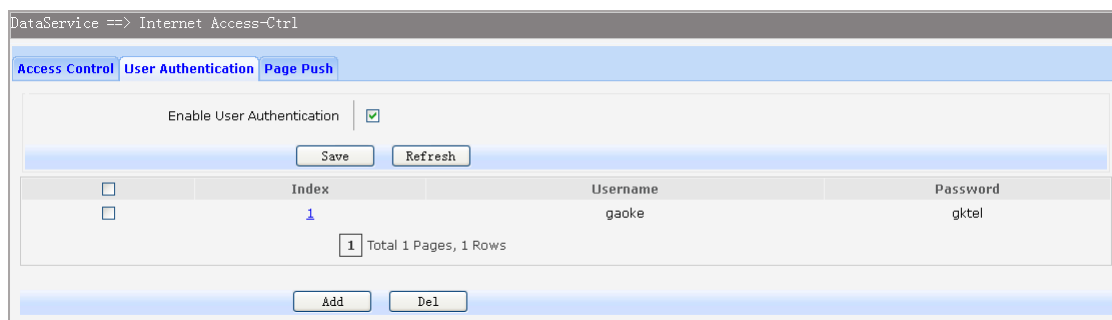
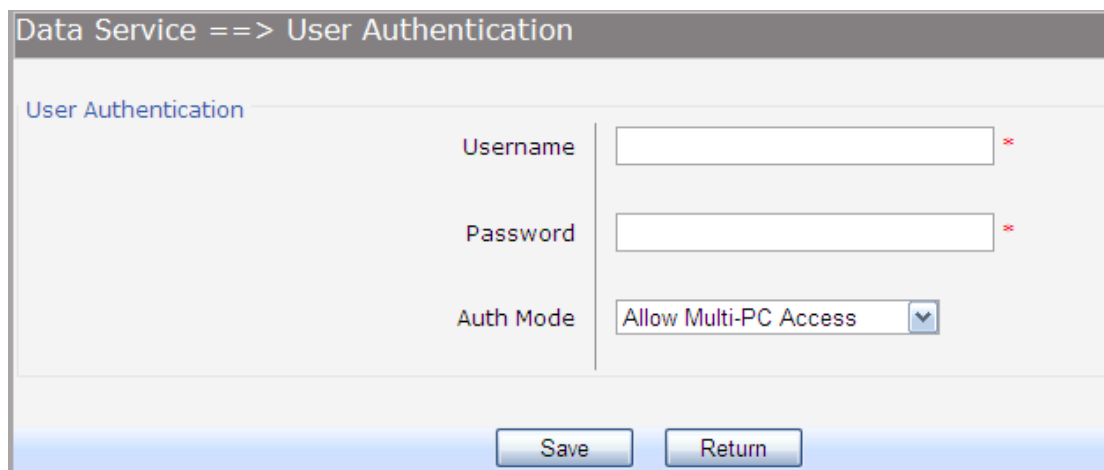


Figure 5-18 User Authentication

The following items are displayed in Figure 5-18:

▶ **Enable User Authentication:** Enable or disable user authentication globally. If enabled, only the following list of users and passwords can access the Internet. Press **Save** button if you have modified this parameter.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.



4G/5G ODU USER MANUAL

Figure 5-19 Add User Authenticaiton

The following items are displayed in Figure 5-19:

- **Username:** Enter the username of this entry.
- **Password:** Enter the password of this entry.
- **Auth Mode:** Choose the authentication mode of this entry. Provides four modes:
 - Allow Multi-PC Access:** Allows multiple computers to access the Internet using this account.
 - Allow One PC Access:** Only allows one computer to access the Internet using this account.
 - Allow Special IP Access:** Allowing only specified IP computer uses this account to access the Internet.
 - Allow Special MAC Access:** Allowing only specified MAC computer uses this account to access the Internet

5.4.3.3 Page Push

HTTP Page push is a mechanism for sending unsolicited (asynchronous) data from web server to a web browser. When accessing the Internet for the first time, the specified HTTP page will be pushed to the browser when enabled.

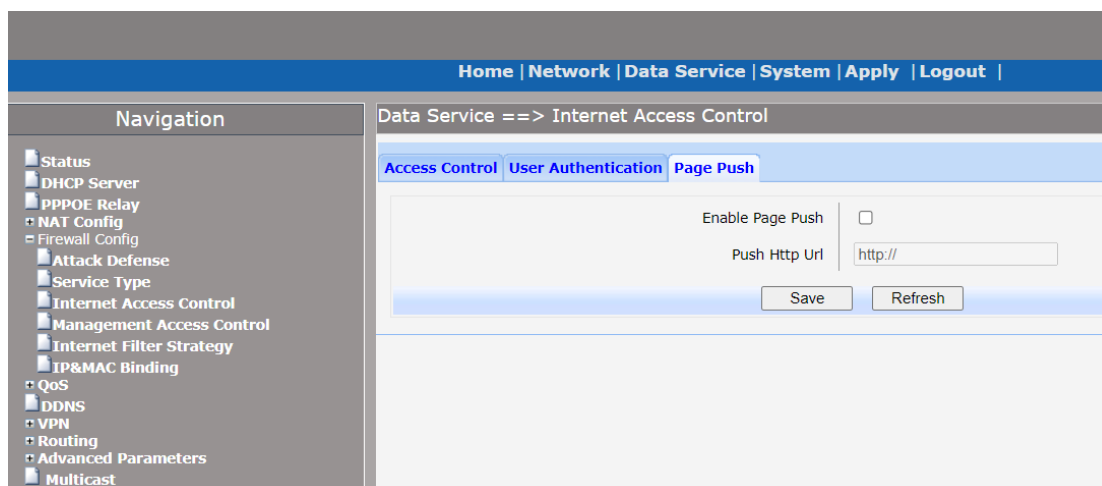


Figure 5-20 Page Push

The following items are displayed in Figure 5-20:

- **Enable Page Push:** If enabled, push specified HTTP page to the browser when accessing the Internet for the first time.
- **Push Http Url:** Specifies the HTTP URL of the page you want to push.

5.4.4 Management Access Control

5.4.4.1 WEB

Choose the menu “Data Service→Firewall Config→Management Access Control→WEB” to load the following page.

4G/5G ODU USER MANUAL

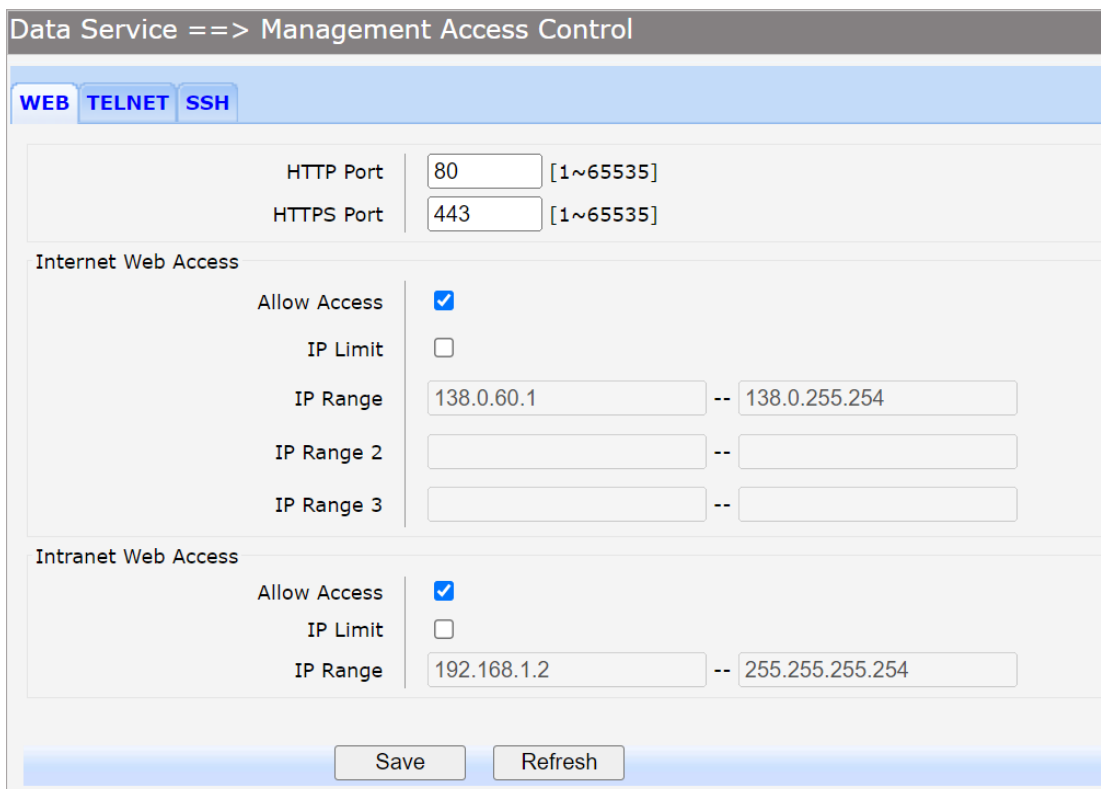


Figure 5-21 Web

The following items are displayed in Figure 5-21:

- **HTTP Port:** Port used with HTTP access device.

HTTP: Hypertext Transfer Protocol.

- **HTTPS Port:** Port used with HTTPS access device.

HTTPS: it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol.

Internet Web Access:

- **Allow Access:** If enabled, allow user to access the device from the Internet via WEB.

- **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via WEB.

- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access to the device from the Internet via WEB.

Intranet Web Access:

- **Allow Access:** If enabled, allow user to access the device from the Intranet via WEB.

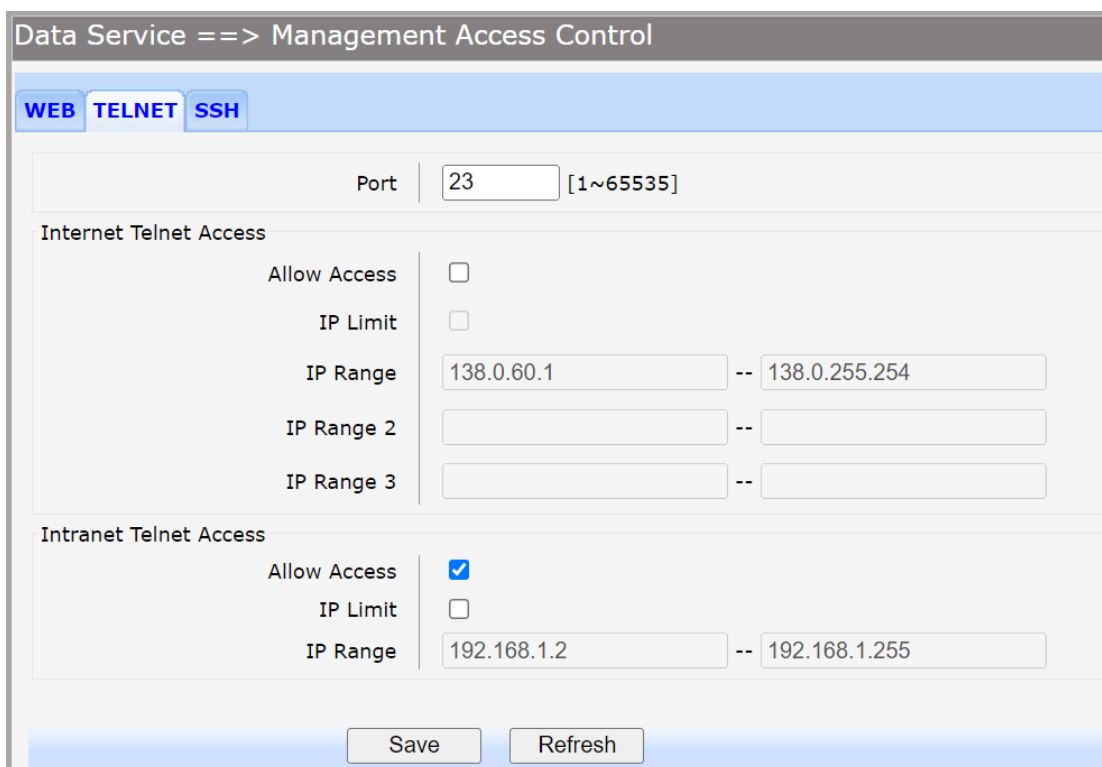
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via WEB.

- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access the device from the Intranet via WEB.

5.4.4.2 TELNET

Choose the menu “Data Service→Firewall Config→Management Access Control→TELNET” to load the following page.

4G/5G ODU USER MANUAL



Data Service ==> Management Access Control

WEB TELNET SSH

Port: 23 [1~65535]

Internet Telnet Access

Allow Access: ☐

IP Limit: ☐

IP Range: 138.0.60.1 -- 138.0.255.254

IP Range 2: --

IP Range 3: --

Intranet Telnet Access

Allow Access: ☒

IP Limit: ☐

IP Range: 192.168.1.2 -- 192.168.1.255

Save Refresh

Figure 5-22 Telnet

The following items are displayed in Figure 5-22:

► **Port:** Port when using telnet tools access device.

Internet Web Access:

► **Allow Access:** If enabled, allow access to the device from the Internet via telnet.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via telnet

► **IP Range:** If IP Limit enabled, specifies the IPv4 address range that only allow access to the device from the Internet via telnet.

Intranet Web Access:

► **Allow Access:** If enabled, allow access to the device from the Intranet via telnet. ► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via telnet

► **IP Range:** If IP Limit enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via telnet.

5.4.4.3 SSH

Choose the menu “Data Service→Firewall Config→Management Access Control→SSH” to load the following page.

4G/5G ODU USER MANUAL

Data Service ==> Management Access Control

WEB TELNET SSH

Port [1~65535]

Internet SSH Access

Allow Access ☐

IP Limit ☐

IP Range --

IP Range 2 --

IP Range 3 --

Intranet SSH Access

Allow Access ☒

IP Limit ☐

IP Range --

Figure 5-23 SSH

The following items are displayed in Figure 5-23:

- **Port:** Port when using SSH tools access device.

Internet Web Access:

- **Allow Access:** If enabled, allow access to the device from the Internet via SSH.
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via SSH
- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via SSH.

Intranet Web Access:

- **Allow Access:** If enabled, allow access to the device from the Intranet via SSH.
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via SSH
- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via SSH.

5.4.5 Internet Filter Strategy

5.4.5.1 URL Filter

Choose the menu “Data Service→Firewall Config→Internet Filter Strategy→URL Filter” to load the following page.

4G/5G ODU USER MANUAL

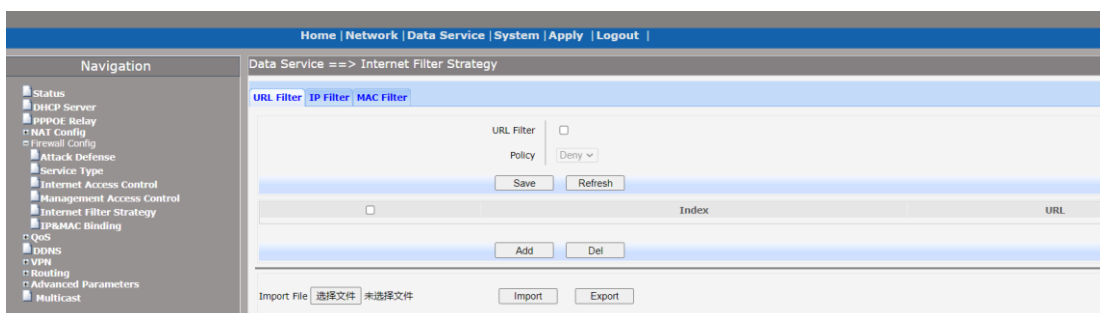


Figure 5-24 URL Filter

The following items are displayed in Figure 5-24:

- **URL Filter:** If enabled, packet filtering is enabled by URL.
- **Policy:** The policy for filtering web page, Deny and Allow. You can export all the URLs as a file. Of course, you can also import a file.

5.4.5.2 IP Filter

Choose the menu “Data Service→Firewall Config→Internet Filter Strategy→IP Filter” to load the following page.

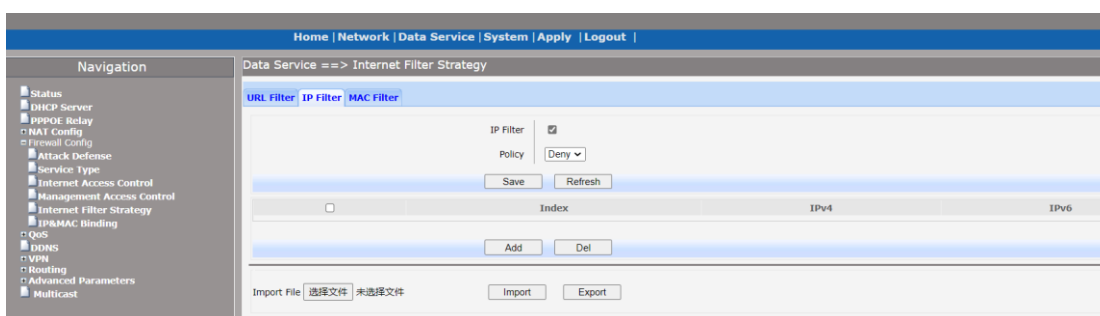


Figure 5-25 IP Filter

The following items are displayed in Figure 5-25:

- **IP Filter:** If enabled, packet filtering is enabled by IP address.
- **Policy:** The policy for IP address list. Deny and Allow. You can export all the IP addresses as a file. Of course, you can also import a file.

5.4.5.3 MAC Filter

Choose the menu “Data Service→Firewall Config→Internet Filter Strategy→MAC Filter” to load the following page.

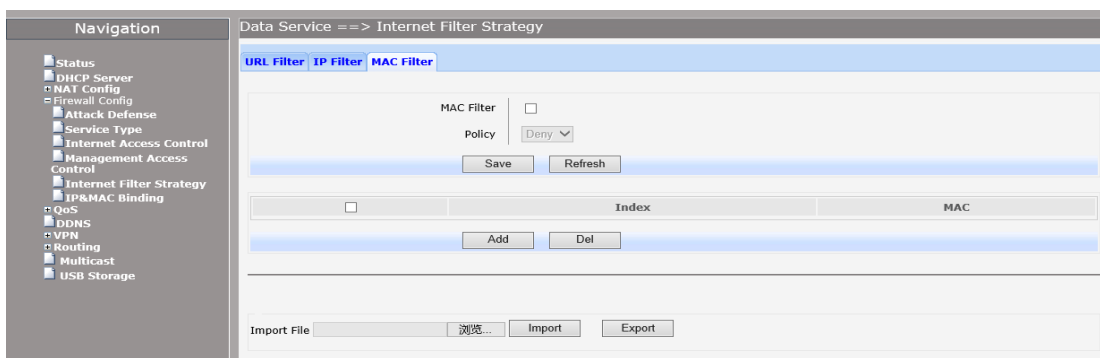


Figure 5-26 MAC Filter

4G/5G ODU USER MANUAL

The following items are displayed in Figure 5-26:

- **IP Filter:** If enabled, packet filtering is enabled by MAC.
- **Policy:** The policy for MAC list. Deny and Allow. You can export all the MAC addresses as a file. Of course, you can also import a file.

If you want to delete an entry, select it and click the **Del**. Click the **Add** button to add a new entry. There are two ways to add MAC:

Artificial designated MAC: You can manually enter a MAC.

Using Studying MAC: You can choose one or more MAC devices learned.

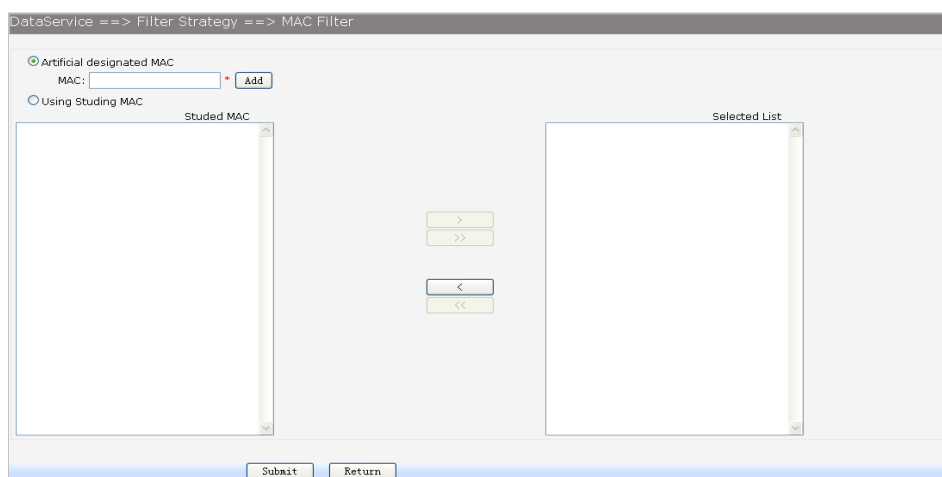


Figure 5-27 Add MAC Filter

5.4.6 IP&MAC Binding

Choose the menu “**Data Service→Firewall Config→IP&MAC Binding**” to load the following page as shown in Figure 5-28. There are two ways to add a binding entry: You can manually enter a pair of IP and MAC, and then press **Add Item**. Alternatively you can select a pair of IP and MAC in **Scan List** that device learned.

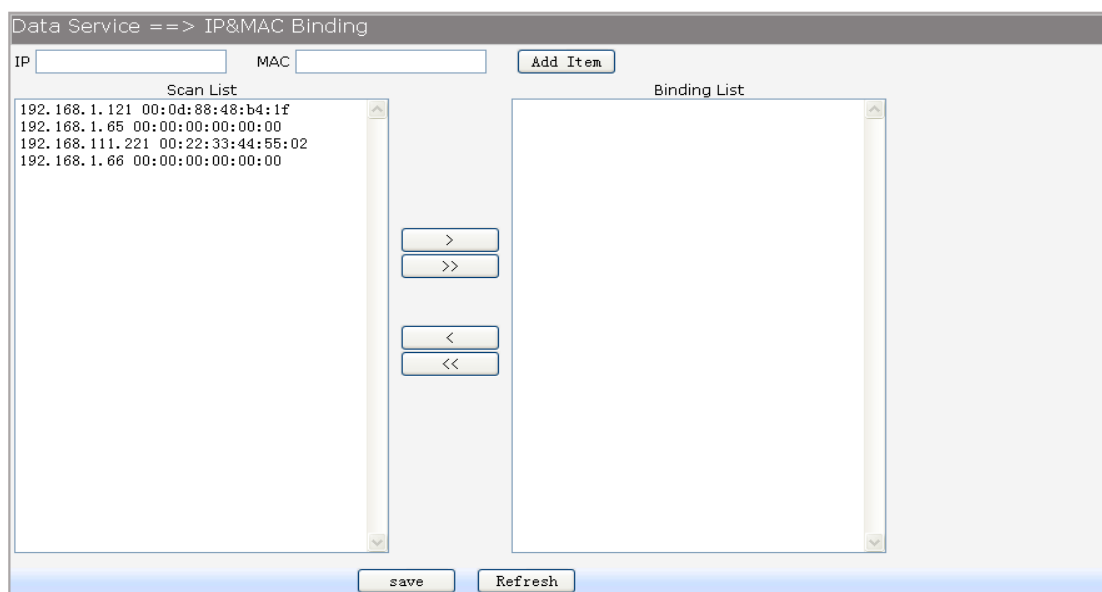


Figure 5-28 IP&MAC Binding

4G/5G ODU USER MANUAL

5.5 QoS

QOS feature is enabled by default, based on 802.1P, strict priority scheduling mode. The device supports four priority queues, when QOS feature enabled.

5.5.1 QoS Basic Settings

Choose the menu “**Data Service→QoS→Basic Settings**” to load the following page.

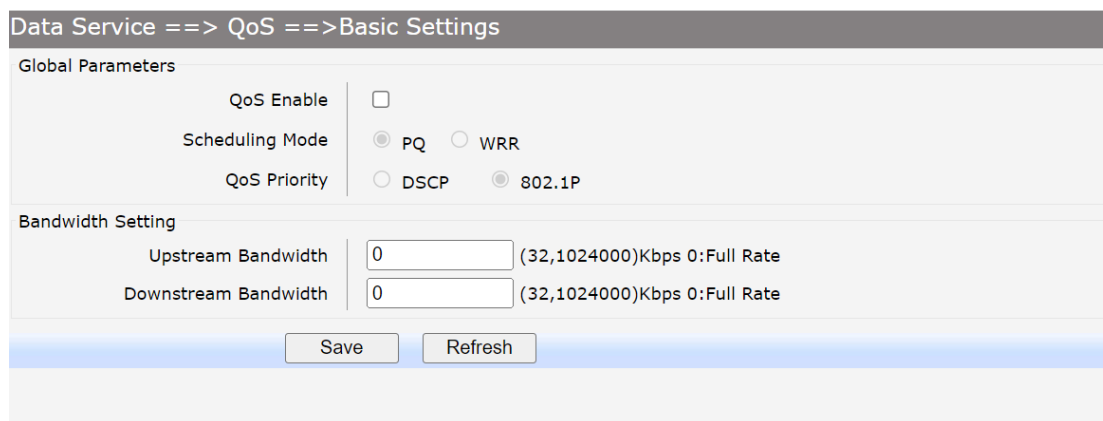


Figure 5-29 QoS Basic Settings

The following items are displayed in Figure 5-29:

Global Parameters

► **Qos Enable:** Enable or disable QoS functionality.

► **Scheduling Mode:**

PQ: PQ means strict priority, that is, when congestion occurs, first sending packets of high priority queue.

WRR: All queues use weighted fair queuing scheme which is defined in Weight Ratio ►

Qos Priority:

DSCP: When you select DSCP value, corresponding to the following relationship.

DSCP priority value	Priority queue (queue 3 highest priority)
0-15	Queue 0
16 ~ 31	Queue 1
32 to 47	Queue 2
48 ~ 63	Queue 3

802.1P: Select the queue classification mode, when selecting 802.1P mode, depending on the value of 802.1p priority classification into different queues, corresponding to the following relationship.

4G/5G ODU USER MANUAL

801.1p priority value	Priority queue (queue 3 highest priority)
0 to 1	Queue 0
2.3	Queue 1
4.5	Queue 2
6-7	Queue 3

Bandwidth Setting

- **Upstream Bandwidth:** Configure the bandwidth of upstream.
- **Downstream Bandwidth:** Configure the bandwidth of downstream.

5.5.2 DDNS

Choose the menu “**Data Service→QoS→DDNS**” to load the following page.

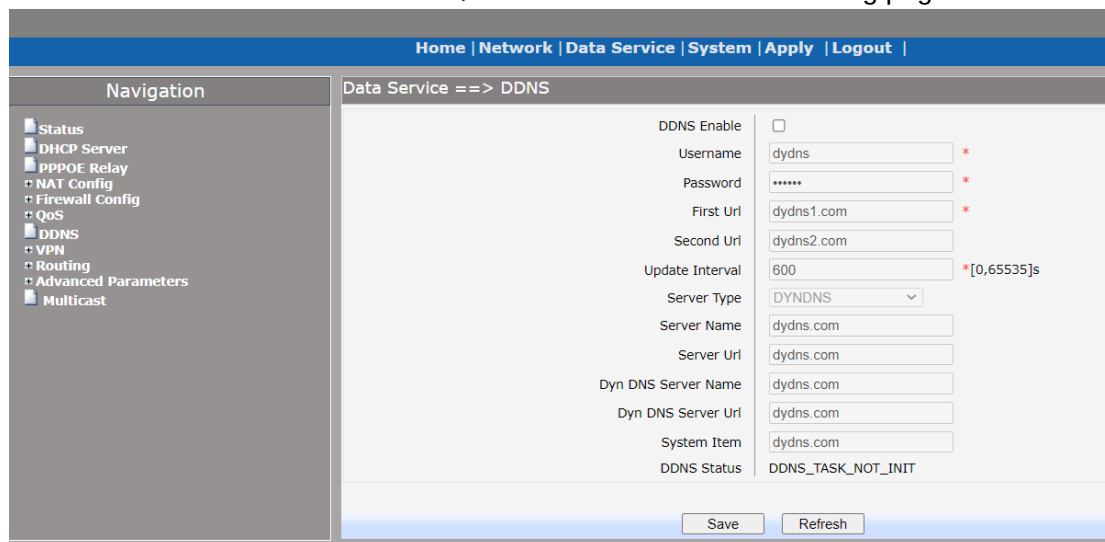


Figure 5-30 DDNS

The following items are displayed in Figure 5-30:

- **DDNS Enable:** Active or inactive dynamic DNS service.
- **Username:** Enter account name of your DDNS account.
- **Password:** Enter password of your DDNS account.
- **First Url:** First domain name that you registered your DDNS service provider.
- **Second Url:** First domain name that you registered your DDNS service provider. ►
- Update Interval:** How often, in seconds, the IP is updated.
- **Server Type:** optional DDNS server type, can select from pull-down list:
 - DYNDNS:** For dyndns.org
 - FREEDNS:** For freedns.afraid.org
 - ZONE:** For zoneedit.com
 - NOIP:** For no-ip.com **3322:** For 3322.org
 - CUSTOM:** For custom self-defined DDNS server type.
- **Server Name:** If CUSTOM is selected, specify server name of the device.
- **Server Url:** If CUSTOM is selected, specify server URL of the device.

4G/5G ODU USER MANUAL

- **Dyn DNS Server Name:** If CUSTOM is selected, specify dyndns DNS server name of custom self-defined.
 - **Dyn DNS Server Url:** If CUSTOM is selected, specify dyndns DNS server URL of custom self-defined.
 - **System Item:** If CUSTOM is selected, specify system item of custom self-defined. ►
- DDNS Status:** Display the status of DDNS service. Read only.

5.6 VPN

5.6.1 PPTP Server

Choose the menu “**Data Service→VPN→PPTP Server**” to load the following page.

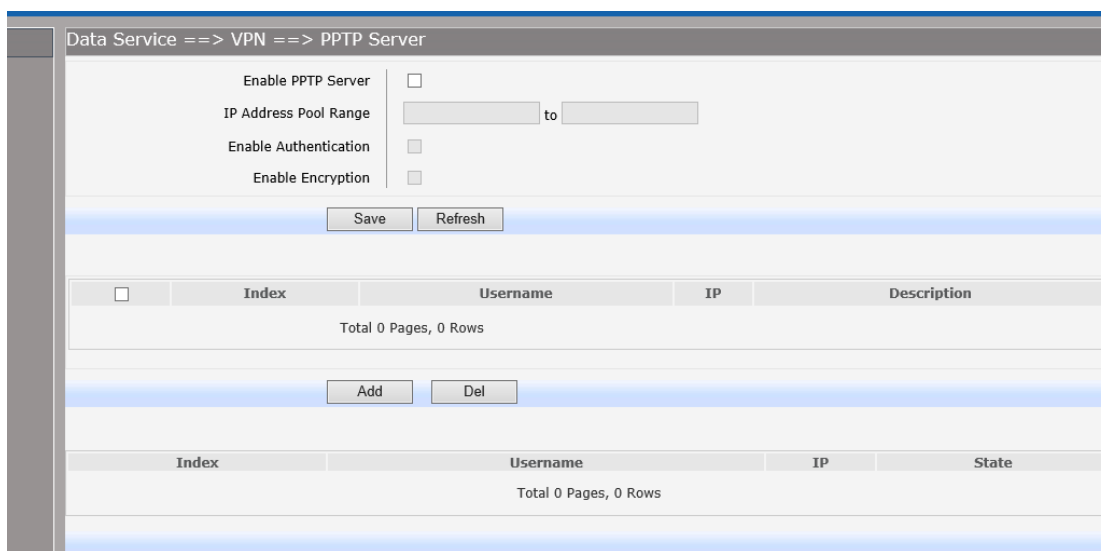


Figure 5-31 PPTP Server

The following items are displayed in Figure 5-31:

- **Enable PPTP Server:** Enable or disable the PPTP server function globally.
- **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- **Enable Authentication:** Specify whether to enable authentication for the tunnel. ►
- **Enable Encryption:** Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.

5.6.2 L2TP Server

Choose the menu “**Data Service→VPN→L2TP Server**” to load the following page.

4G/5G ODU USER MANUAL

Data Service ==> VPN ==> L2TP Server

☐ Enable L2TP Server
 Local IP:
 IP Address Pool Range: to
 Enable Authentication: ☒ Auth Secret: (1-127 Characters)
 Enable Debug: ☐

☐	Index	Username	IP	Description
Total 0 Pages, 0 Rows				

Index	Username	IP	State
Total 0 Pages, 0 Rows			

Figure 5-32 L2TP Server

The following items are displayed in Figure 5-32:

- ▶ **Enable L2TP Server:** Enable or disable the L2TP server function globally.
- ▶ **Local IP:** Enter the local IP address of L2TP server.
- ▶ **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- ▶ **Enable Authentication:** Specify whether to enable authentication for the tunnel. If enabled, enter the authentication secret.
- ▶ **Enable Debug:** Specify whether to enable the debug for L2TP.

5.6.3 IPsec

5.6.3.1 IKE Safety Proposal

Choose the menu “**Data Service→VPN→IPsec→IKE Safety Proposal**” to load the following page.

Data Service ==> VPN ==> IPsec

[IKE Safety Proposal](#) [IKE Safety Policy](#) [IPsec Safety Proposal](#) [IPsec Safety Policy](#)

☐	Index	Proposal Name	Encryption Algorithm	Auth Algorithm	DH Group
Add Del					

Figure 5-33 IKE Safety Proposal

The following items are displayed in Figure 5-34:

- ▶ **Proposal Name:** Specify a unique name to the IKE proposal for identification and management purposes. The IKE proposal can be applied to IPSEC proposal.
- ▶ **Encryption Algorithm:** Specify the encryption algorithm for IKE negotiation. Options include: **DES:** DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a

4G/5G ODU USER MANUAL

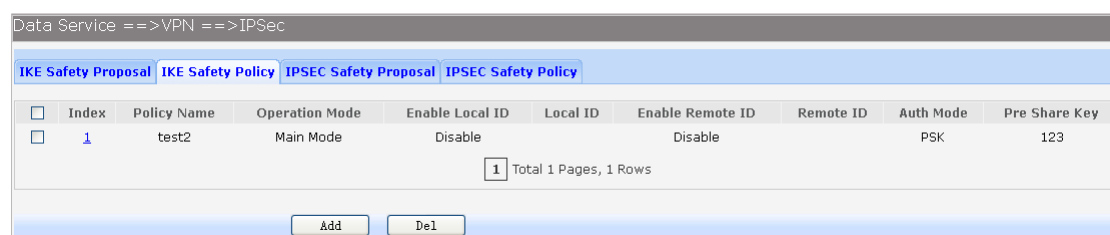
56-bit key. **3DES**: Triple DES, encrypts a plain text with 168-bit key. **AES**: Uses the AES algorithm for encryption.

► **Auth Algorithm**: Select the authentication algorithm for IKE negotiation. Options include: **MD5**: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest. **SHA1**: SHA1 (Secure Hash Algorithm) takes a message less than 2^{64} (the 64th power of 2) in bits and generates a 160-bit message digest.

► **DH Group**: Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits. Options include **DH 768 modp**, **DH 1024 modp** and **DH 1536 modp**.

5.6.3.2 IKE Safety Policy

Choose the menu “**Data Service**→**VPN**→**IPsec**→**IKE Safety Policy**” to load the following page.



☐	Index	Policy Name	Operation Mode	Enable Local ID	Local ID	Enable Remote ID	Remote ID	Auth Mode	Pre Share Key
☐	1	test2	Main Mode	Disable		Disable		PSK	123

1 Total 1 Pages, 1 Rows

Add Del

Figure 5-34 IKE Safety Policy

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

4G/5G ODU USER MANUAL

Data Service ==> VPN==>IPSec ==> IKE Policy

Policy Name	* (Maximum 128 Characters)
Operation Mode	☐ Challenge Mode ☒ Main Mode
Enable Local ID	☐ (Maximum 256 Characters)
Enable Remote ID	☐ (Maximum 256 Characters)
Auth Mode	PSK
Pre Share Key	* (Maximum 255 characters)
NAT-T	☒ off ☐ on ☐ force
NAT-T Keep-alive	20 (Second, 0s means disable keep-alive packets)
DPD Delay	0 * (Second, 0s means disable DPD)
DPD Retry	5 * (Second)
DPD Max Retries	5 *
Enable Safety Proposal1	☐
Enable Safety Proposal2	☐
Enable Safety Proposal3	☐
Enable Safety Proposal4	☐

Save Return

Figure 5-35 Add or Modify IKE Safety Policy

The following items are displayed in Figure 5-35:

► **Policy Name:** Specify a unique name to the IKE policy for identification and management purposes. The IKE policy can be applied to IPSEC policy.

► **Operation Mode:** Select the IKE Exchange Mode in phase 1, and ensure the remote VPN peer uses the same mode.

Main: Main mode provides identity protection and exchanges more information, which applies to the scenarios with higher requirement for identity protection.

Challenge: Challenge Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirement for identity protection.

► **Enable Local ID:** If enabled, enter a name for the local device as the ID in IKE negotiation.

► **Enable Remote ID:** If enabled, enter the name of the remote peer as the ID in IKE negotiation.

► **Auth Mode:** Select the authentication mode for this IKE policy entry.

PSK:

Certificate:

► **Pre Share Key:** Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.

► **NAT-T:** Select off, on or force

► **NAT-T Keep-alive:** Specify the keep-alive interval

► **DPD Delay:** Specify the delay for DPD

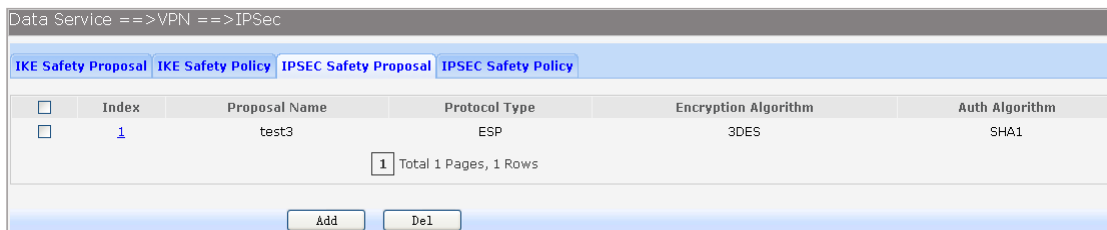
► **DPD Retry:** Specify retry interval for DPD

4G/5G ODU USER MANUAL

- **DPD Max Retries:** Specify maximum retry time for DPD
- **Enable Safety Proposal:** Select the Proposal for IKE negotiation phase 1. Up to four proposals can be selected.

5.6.3.3 IPSEC Safety Proposal

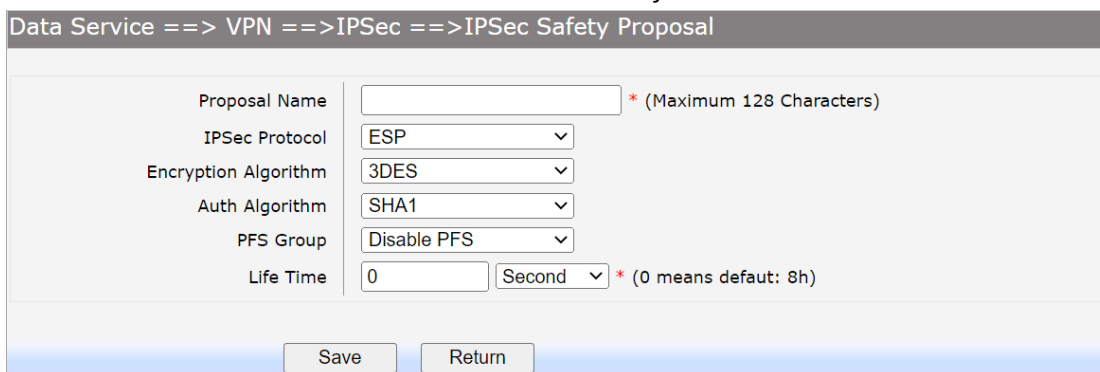
Choose the menu “**Data Service**→**VPN**→**IPsec**→**IPSEC Safety Proposal**” to load the following page.



Data Service ==>VPN ==>IPSec					
IKE Safety Proposal IKE Safety Policy IPSEC Safety Proposal IPSEC Safety Policy					
☐	Index	Proposal Name	Protocol Type	Encryption Algorithm	Auth Algorithm
☐	1	test3	ESP	3DES	SHA1
1 Total 1 Pages, 1 Rows					
Add Del					

Figure 5-36 IPSEC Safety Proposal

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.



Data Service ==> VPN ==>IPSec ==>IPSec Safety Proposal	
Proposal Name	* (Maximum 128 Characters)
IPSec Protocol	ESP ▼
Encryption Algorithm	3DES ▼
Auth Algorithm	SHA1 ▼
PFS Group	Disable PFS ▼
Life Time	0 Second * (0 means default: 8h)
Save Return	

Figure 5-37 Add IPSEC Safety Proposal

The following items are displayed in Figure 5-37:

- **Proposal Name:** Specify a unique name to the IPSEC Proposal for identification and management purposes. The IPSEC proposal can be applied to IPSEC policy.
- **IPSec Protocol:** Select the security protocol to be used. Options include: **AH:** AH (Authentication Header) provides data origin authentication, data integrity and anti-replay services.

ESP: ESP (Encapsulating Security Payload) provides data encryption in addition to origin authentication, data integrity, and anti-replay services.

ESP+AH: Both ESP and AH security protocol.

- **Encryption Algorithm:** Select the algorithm used to encrypt the data for ESP encryption. Options include:

DES: DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key. The key should be 8 characters.

3DES: Triple DES, encrypts a plain text with 168-bit key. The key should be 24 characters.

AES: Uses the AES algorithm for encryption. The key should be 16 characters.

- **Auth Algorithm:** Select the algorithm used to verify the integrity of the data. Options include:

4G/5G ODU USER MANUAL

MD5: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.

SHA: SHA (Secure Hash Algorithm) takes a message less than the 64th power of 2 in bits and generates a 160-bit message digest.

► **PFS Group:** Select PFS group parameters. Selectable: Disable PFS, DH 1536 modp, DH 1024 modp, DH 768 modp.

► **Life Time:** Specify the life time.

5.6.3.4 IPSEC Safety Policy

Choose the menu “**Data Service**→**VPN**→**IPsec**→**IPSEC Safety Policy**” to load the following page.

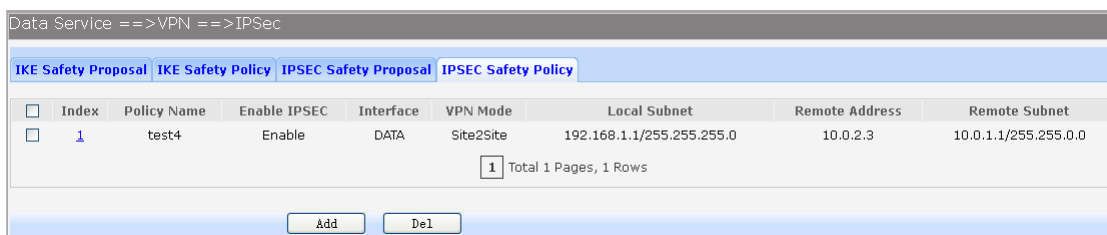


Figure 5-38 IPSEC Safety Policy

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

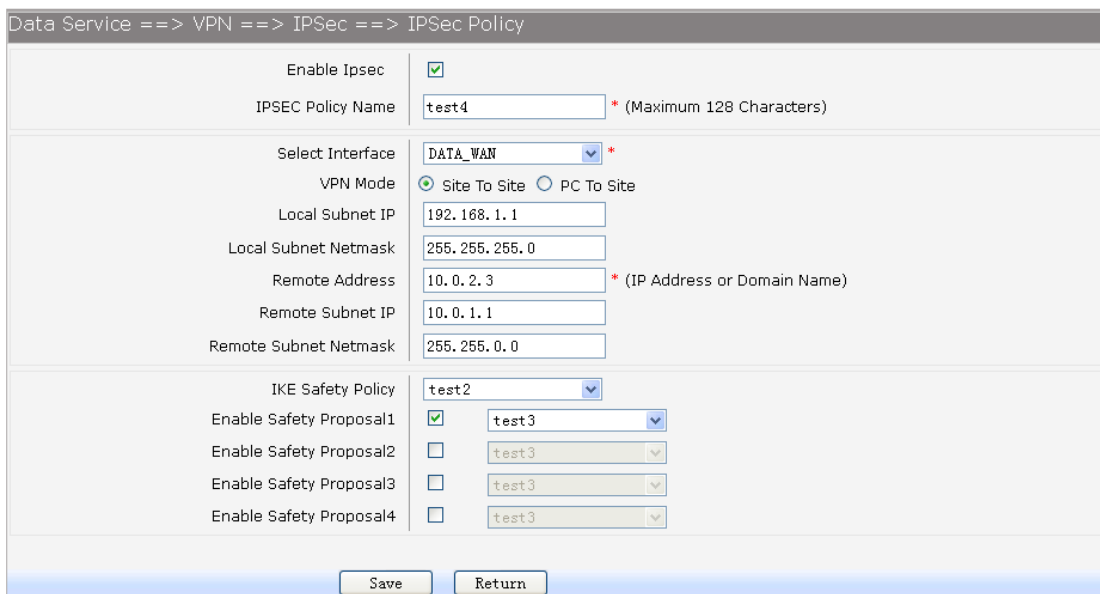


Figure 5-39 Add or Modify IPSEC Safety Policy

The following items are displayed in Figure 5-39:

- **Enable Ipsec:** Enable or disable this IPSEC entry.
- **IPSEC Policy Name:** Specify a unique name to the IPSEC policy.
- **Select Interface:** Specify the local WAN port for this Policy.
- **VPN Mode:** Select the network mode for IPSEC policy. Options include:
 - Site To Site:** Select this option when the client is a network.
 - PC to Site:** Select this option when the client is a host.
- **Local Subnet IP & Local Subnet Netmask:** Specify IP address range on your local

4G/5G ODU USER MANUAL

LAN to identify which PCs on your LAN are covered by this policy.

► **Remote Address:** If PC to Site is selected, specify IP address on your remote network to identify which PCs on the remote network are covered by this policy.

► **Remote Subnet IP & Remote Subnet Netmask:** Specify IP address range on your remote network to identify which PCs on the remote network are covered by this policy.

► **IKE Safety Policy:** Specify the IKE policy. If there is no policy selection, add new policy on VPN→IPSec→IKE Safety Policy page.

► **Enable Safety Prososal: If enabled,** Select IPSEC Proposal. If there is no policy selection, add new IPSEC proposal on VPN→IPSec→IPSEC Safety Proposal page. Up to four IPSEC Proposals can be selected.

5.7 Routing

5.7.1 Static Route

5.7.1.1 IPv4

Choose the menu “**Data Service→Routing→Static Route→IPv4**” to load the following page.

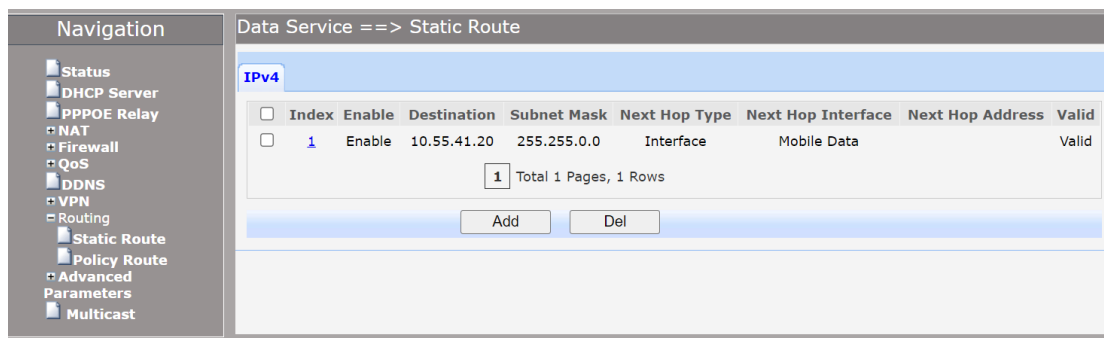


Figure 5-40 IPv4 Static Route

The following items are displayed in Figure 5-40:

- **Enable:** Select it to add and modify the current route. Conversely, disable the current route.
- **Destination IP:** Enter the destination host the route leads to.
- **Netmask:** Enter the Subnet mask of the destination network.
- **Next Hop Type:** Include **Next Hop Interface** and **Next Hop Address**(see following option)
- **Next Hop Interface:** Specify the interface of next hop for current route
- **Next Hop Address:** Specify the address of next hop for current route
- **Valid:** Show the status of current route.

5.7.2 Policy Route

Choose the menu “**Data Service→Routing→Policy Route**” to load the following page.

4G/5G ODU USER MANUAL

Data Service ==> Policy Route

☐	Index	Enable	Src IP Range	Dst IP Range	Dst Port Range	Next Hop	Active Time
☐	1	YES	192.168.1.100-192.168.1.200	210.10.10.3-210.10.10.50	1000-2000	DATA	TimeInfo

1 Total 1 Pages, 1 Rows

Add Del

Figure 5-42 Policy Route

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

DataService ==> Policy Route

Enable Policy Route ☐

Protocol

Source IP to

Destination IP to

Destination Port to [0~65535]

Active Time -- (hh:mm)

Active Day ☐ All ☐ Monday ☐ Tuesday ☐ Wednesday
☐ Thursday ☐ Friday ☐ Saturday ☐ Sunday

Save Return

Figure 5-43 Add or Modify Policy Route

Following items are displayed in Figure 5-43:

- ▶ **Enable PoliceRoute:** Enable or disable the entry
- ▶ **Source IP:** Enter IP address or IP range of source in the rule entry.
- ▶ **Destination IP:** Enter IP address or IP range of destination in the rule entry.
- ▶ **Destination Port:** Specify port or port range of destination in the rule entry.
- ▶ **Active Time:** Specify the active time range for the rule entry.
- ▶ **Active Day:** Specify the active days for the rule entry.

5.8 Multicast

Choose the menu “**Data Service→Multicast**” to load the following page.

Home | Network | Data Service | System | Apply | Logout |

Navigation

- Status
- DHCP Server
- PPPOE Relay
- NAT
- Firewall
- QoS
- DDNS
- VPN
- Routing
- Advanced Parameters
- Multicast

Data Service ==> Multicast

Multicast Mode

Quick Leave ☐

IGMP Version

Upstream Interface

Specify ports to play IPTV video LAN1 ☒ LAN2 ☒

IGMP messages source address is 0.0.0.0 ☐

Save Refresh

Figure 5-44 Multicast

4G/5G ODU USER MANUAL

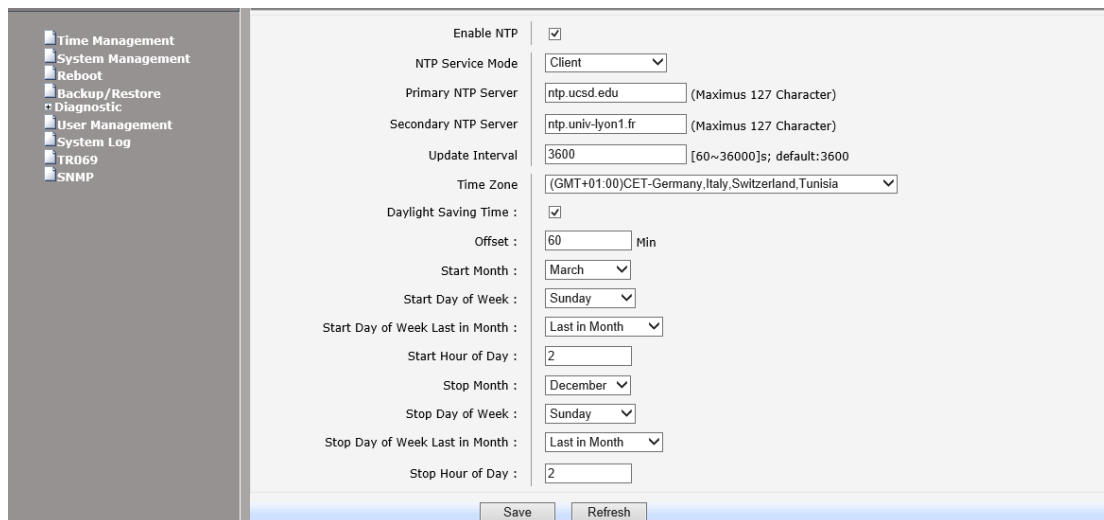
The following items are displayed in Figure 5-44:

- **Multicast Mode:** Enable or disable the IGMP proxy function globally. Currently, IGMP proxy is mainly used for IPTV.
- **IGMP Version:** Enable or IGMP V2 or IGMP V3.
- **QuickLeave:** Enable or disable IGMP quickleave function.
- **Specify ports to play IPTV video:** Enable this if you want to specify LAN port(s) to play IPTV video.
- **LAN1:** Enable or disable LAN1 to play IPTV video.
- **LAN2:** Enable or disable LAN2 to play IPTV video.
- **IGMP messages source address is 0.0.0.0:** Enable or Disable IGMP messages source address is 0.0.0.0

6 System

6.1 Time Management

Choose the menu “**Data Service→Time Management**” and select **Manual Configuration** to load the following page.



The screenshot displays the 'Time Management' configuration page. On the left is a sidebar menu with options: Time Management, System Management, Reboot, Backup/Restore, Diagnostic, User Management, System Log, TR069, and SNMP. The main area contains the following settings:

- Enable NTP:** ☒
- NTP Service Mode:** Client (dropdown)
- Primary NTP Server:** ntp.ucsd.edu (Maximus 127 Character)
- Secondary NTP Server:** ntp.univ-lyon1.fr (Maximus 127 Character)
- Update Interval:** 3600 [60~36000]s; default:3600
- Time Zone:** (GMT+01:00)CET-Germany,Italy,Switzerland,Tunisia (dropdown)
- Daylight Saving Time:** ☒
- Offset:** 60 Min
- Start Month:** March (dropdown)
- Start Day of Week:** Sunday (dropdown)
- Start Day of Week Last in Month:** Last in Month (dropdown)
- Start Hour of Day:** 2
- Stop Month:** December (dropdown)
- Stop Day of Week:** Sunday (dropdown)
- Stop Day of Week Last in Month:** Last in Month (dropdown)
- Stop Hour of Day:** 2

At the bottom are 'Save' and 'Refresh' buttons.

Figure 7-1 Time Management

The following items are displayed in Figure 7-1:

- **Enable NTP:** Enable or disable NTP service.
- **NTP Service Mode:** Specify CPE role as NTP Client or both Client and Server.
- **Primary NTP Server:** Specify the primary NTP server for role as NTP client.
- **Second NTP Server:** Specify the second NTP server for role as NTP client.
- **Time Zone:** Enter the local time zone.
- **Update Interval:** Specify update interval for role as NTP client.
- **Daylight Saving Time:** Enable or disable the Daylight Saving Time(DST).
- **Offset:** Enter the offset of DST.
- **Start Month:** Specify the start month of DST, range from 1 to 12 in one year.

4G/5G ODU USER MANUAL

- ▶ **Start Day of Week:** Specify the start weekday of DST, range from Sunday to Saturday.
- ▶ **Start Day of Week Last in Month:** Specify the order of start weekday in the month from pull-down list as following:
 - First in Month
 - Second in Month
 - Third in Month
 - Fourth in Month
 - Last in Month
- ▶ **Start Hour of Day:** Specify the start hour of DST, range from 0 to 23 in one day.
- ▶ **Stop Month:** Specify the end month of DST, range from 1 to 12 in one year.
- ▶ **Stop Day of Week:** Specify the end weekday of DST, range from Sunday to Saturday.
- ▶ **Stop Day of Week Last in Month:** Specify the order of end weekday in the month, similar as **Start Day of Week Last in Month**.
- ▶ **Stop Hour of Day:** Specify the end hour of DST, range from 0 to 23 in one day.

6.2 System Management

Choose the menu “**Data Service**→**System Management**” and select **Manual Configuration** to load the following page.

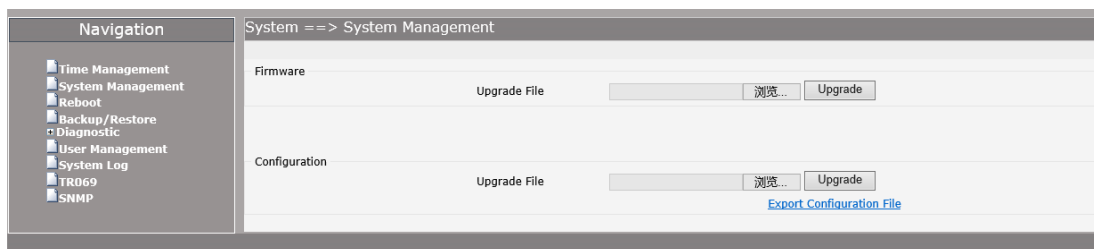


Figure 7-2 System Management

Firmware upgrade via WEB interface:

- 1) Choose menu “Firmware-Upgrade”, then select the right firmware file, click **Upgrade**, wait a few minutes for firmware downloading and programming.
- 2) Choose menu “Reboot”, then click **Reboot** button to reset the device.

Configuration updating via WEB:

- 1) Choose menu “Configuration-Upgrade”, then select the right configuration file, click **Upgrade**, wait a few seconds for downloading and programming.
- 2) Choose menu “Reboot”, then click **Reboot** button to reset the device.

Configuration exporting via WEB interface:

Click the “**Export Configuration File**” to export the configuration file.

4G/5G ODU USER MANUAL

6.3 Reboot

Choose menu **“System Reboot”**, then click **Reboot** button to reset the device.

6.4 Backup/Restore

Choose the menu **“System→Backup/Restore”** to load the following page.

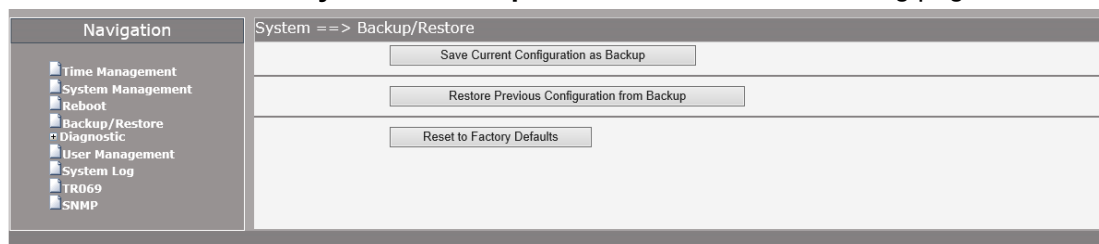


Figure 7-3 Back/Restore

The following items are displayed on this screen:

- **Save Current Configurations as Backup:** Save current parameters as customer default parameters.
- **Restore Previous Configurations from Back:** To reset to customer default parameters.
- **Reset to Factory Defaults:** To reset to factory parameters.

6.5 Diagnostic

6.5.1 Ping

Choose menu **“System Diagnostic Ping”**, and then you can use **Ping** function to check connectivity of your network in the following screen.

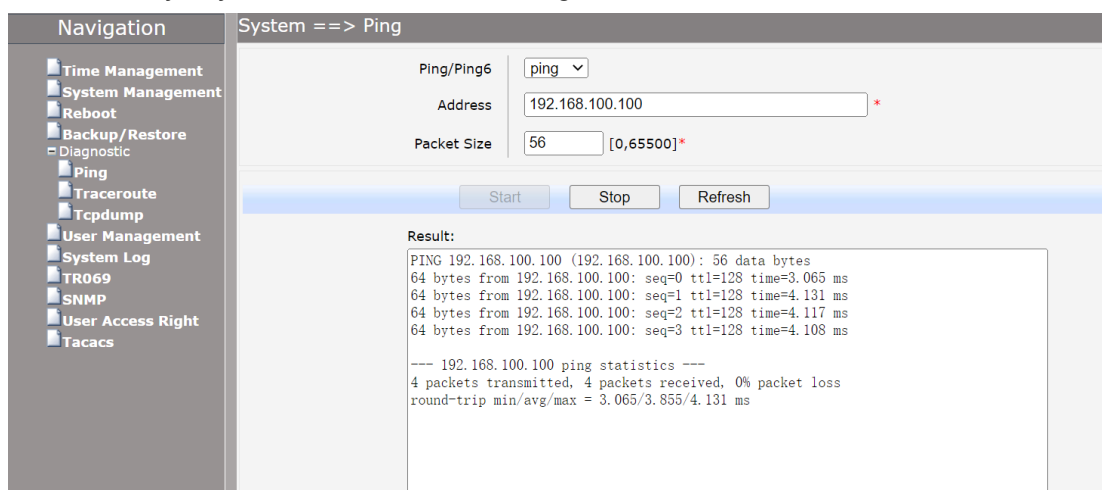


Figure 7-4 Ping

The following items are displayed on this screen:

- **Ping:** Enter the IP Address or Domain Name of the PC whose connection you

4G/5G ODU USER MANUAL

wish to diagnose.

► **Packet Size:** Specify the Ping packet size.

► **Result:** This page displays the result of diagnosis.

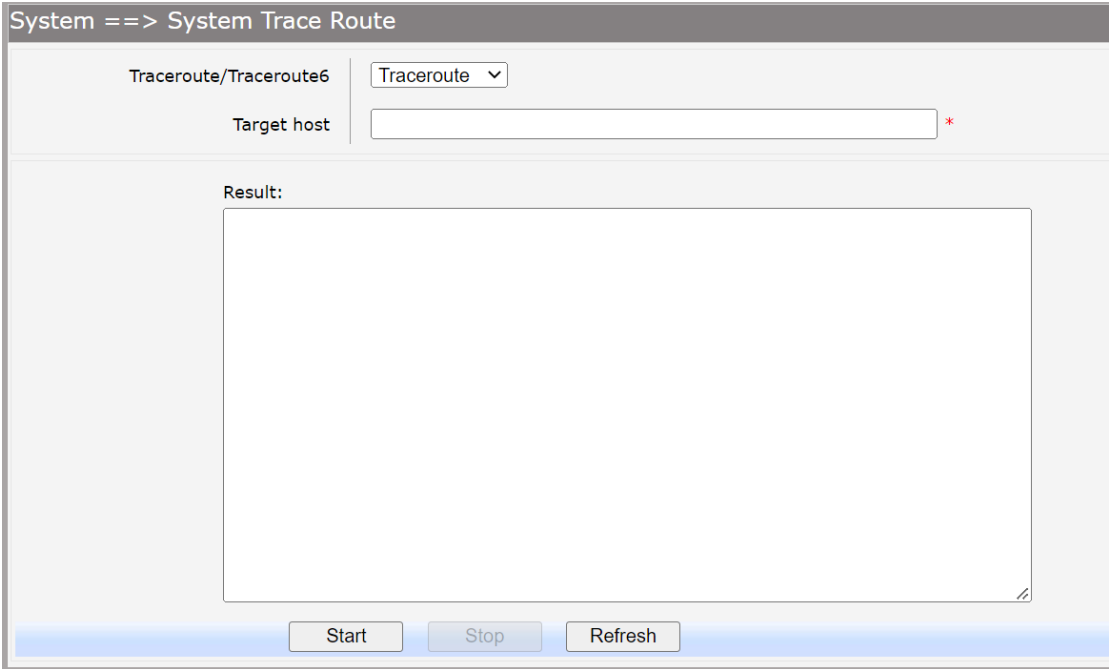
Click **Start** button to check the connectivity of the Internet.

Click **Stop** button to stop sending the Echo Request messages.

Click **Refresh** button to refresh the web page.

6.5.2 Traceroute

Choose the menu “**System→Diagnostic→Traceroute**” to load the following page.



The screenshot shows a web browser window titled "System ==> System Trace Route". Inside the window, there is a section labeled "Traceroute/Traceroute6" with a dropdown menu currently set to "Traceroute". Below this is a text input field labeled "Target host" with a red asterisk indicating it is required. A large empty box labeled "Result:" is positioned below the input field. At the bottom of the interface are three buttons: "Start", "Stop", and "Refresh".

The following items are displayed on this screen:

► **Target host:** Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.

► **Result:** This page displays the result of diagnosis.

Click **Start** button to check the connectivity of the Internet.

Click **Stop** button to stop sending the messages.

Click **Refresh** button to refresh the web page.

6.5.3 TcpDump

Choose the menu “**System→Diagnostic→Tcpdump**” to load the following page.

4G/5G ODU USER MANUAL

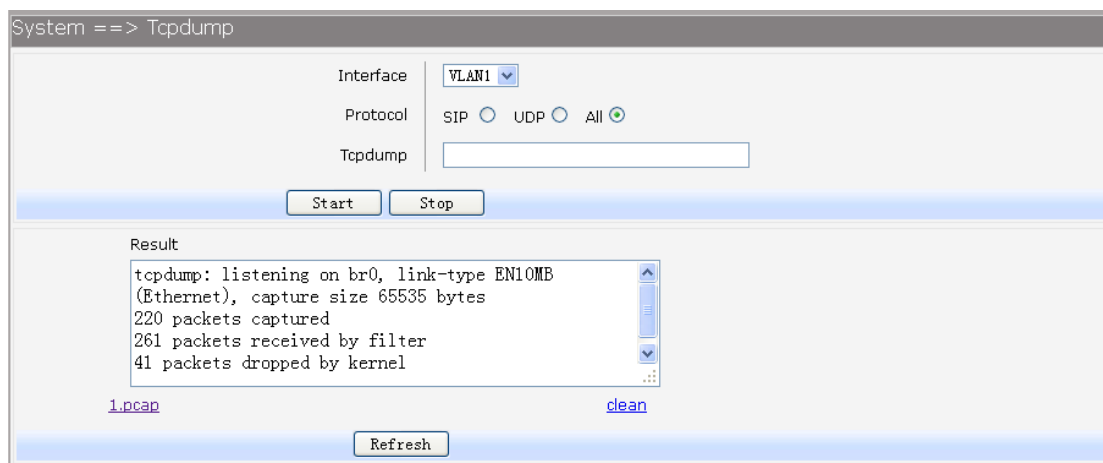


Figure 7-5 TcpDump

The following items are displayed in Figure 7-5:

- **Interface:** By selecting the interface, only packets through this interface will be captured.
- **Protocol:** By selecting the protocol, only packets of this protocol will be captured.
- **Tcpdump:** Enter some options of tcpdump(e.g. -n -s0 -c 100)
- **Result:** This page displays the result of capture packets.

Click **Start** button to capture the packets which correspond to the configuration requirement.

Click **Stop** button to stop capturing the packets.

Click **"*.pcap"** to open or download the capture packets file.

Click **"clean"** to delete all the packets file.

Click **Refresh** button to refresh the web page.

6.6 User Management

To change the factory default user password of the device, choose the menu **"System→User Management"** to load the following page

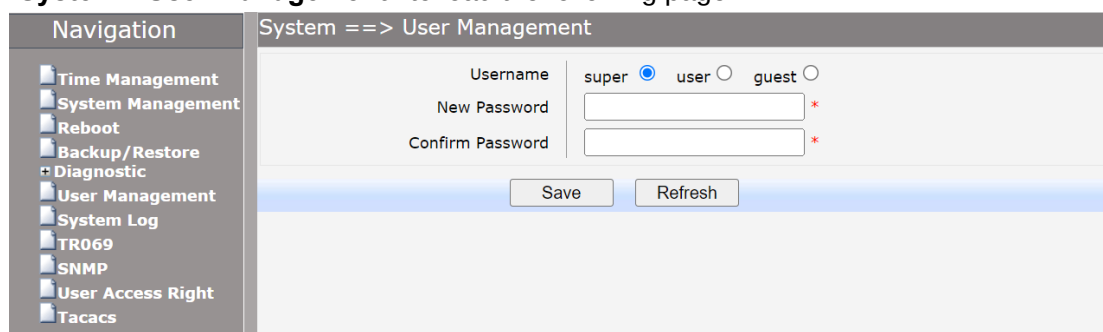


Figure 7-6 User Management

The following items are displayed in Figure 7-6:

- **Username:** You can select the user with different permissions. However, selecting the user whose permission is higher than your permission is forbidden.
- **New Password:** Enter the new password for specified user, not more than 32

4G/5G ODU USER MANUAL

characters, and the space is not supported.

► **Confirm Password:** Enter the new password again to confirm for specified user, not more than 32 characters, and the space is not supported. Click the **Save** button when finished.

6.7 System Log

7.7.1 Log Config

Choose the menu “**System→System Log→Log Config**” to load the following page.

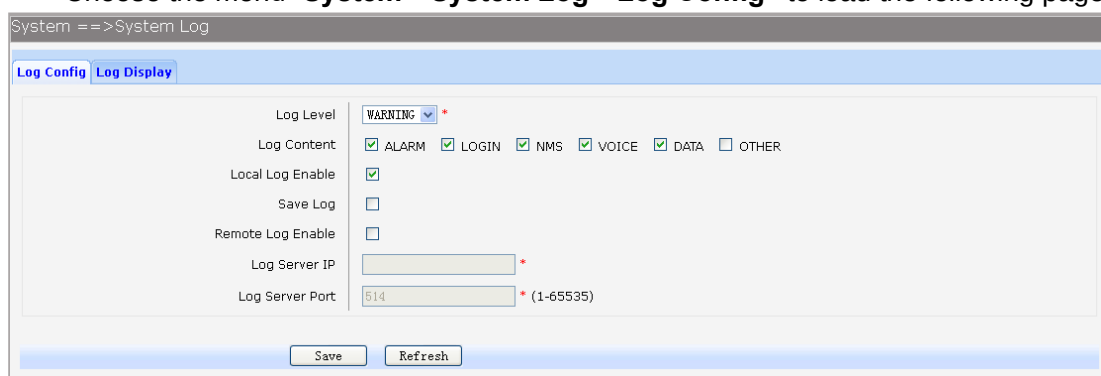


Figure 7-7 Log Config

The following items are displayed in Figure 7-7:

- **Log Level:** By selecting the log level, only logs of this level will be shown.
- **Log Content:** By selecting the log content, only logs of selected content will be shown.
- **Local Log Enable:** Check this box to enable local log function.
- **Save Log:** If **Local Log Enable** is selected, Check this box to enable saving logs to memory file.
- **Remote Log Enable:** Check this box to enable remote log function, the logs will be send to the Log Server.
- **Log Server IP:** Enter the IP address of the Log Server.
- **Log Server Port:** Enter the port that Log service used. Click the **Save** button when finished.

7.7.2 Log Display

Choose the menu “**System→System Log→Log Display**” to load the following page.

4G/5G ODU USER MANUAL

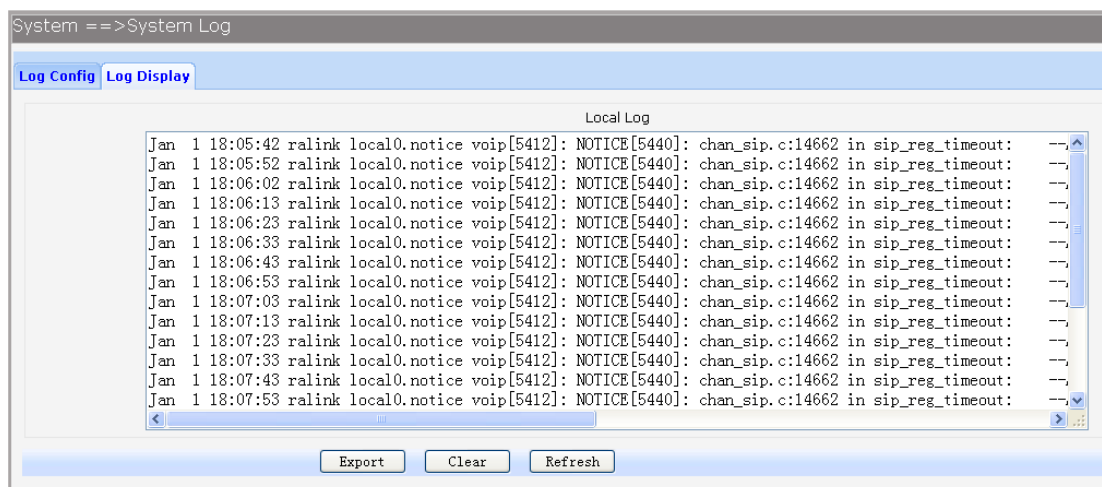


Figure 7-8 Log Display

Click the **Export** button to export all the local logs as a file.

Click the **Clear** button to clear all the local logs from the device permanently, not just from the page.

Click **Refresh** button to refresh the web page.

6.8 TR069

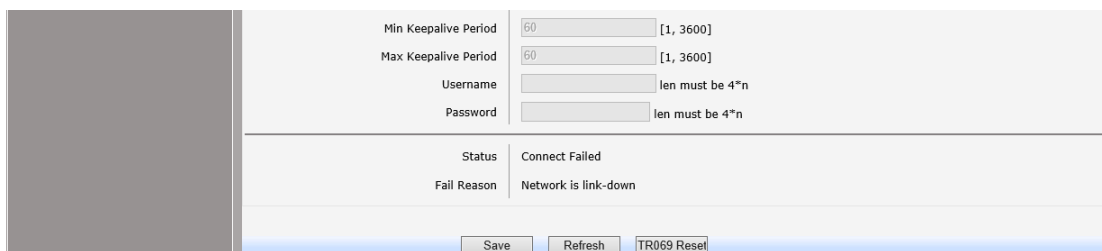
TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bi-directional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

Choose the menu **System**→**TR069** to load the following page.

- Time Management - System Management - Reboot - Backup/Restore - Diagnostic - User Management - System Log TR069 - SNMP	Serial Number	1111111111111111
	Please operating [TR069 Reset] button after modifying tr069 parameter and saving	
	Enable	☒
	ACS URL	http://10.250.0.10:8080/ACS-server/ACS
	Scheduler Send Inform	☐ 3600 (1,4294967295)s
	TR069 Account	000EB4-R3621-000EB40
	TR069 password	*****
	Connection Request Auth	☐
	Connection Request Username	cpe
	Connection Request Password	***
CPE Server Name	cpe	
CPE Port	8099	
Enable Stun	☐	
Server Address		
Server Port	3478	[1, 65535]
Client Port	1600	[1, 65535]

Figure 7-9 TR069

4G/5G ODU USER MANUAL



Min Keepalive Period	60	[1, 3600]
Max Keepalive Period	60	[1, 3600]
Username		len must be 4*n
Password		len must be 4*n
Status	Connect Failed	
Fail Reason	Network is link-down	
Save Refresh TR069 Reset		

Figure 7-10 TR069

The following items are displayed in Figure 7-9 and Figure 7-10:

- ▶ **Serial Number:** The serial number of device. Read only.
 - ▶ **Enable:** Enable or disable the TR069 function globally.
 - ▶ **ACS URL:** Input ACS Address: IP or domain name.
 - ▶ **Schedular Send Inform:** Whether or not the CPE must periodically send CPE information to Server using the Inform method call. Enter the duration in seconds of the interval if enabled.
 - ▶ **TR069 Account:** Username used to authenticate the CPE when making a connection to the ACS.
 - ▶ **TR069 password:** Password used to authenticate the CPE when making a connection to the ACS.
 - ▶ **Connection Request Auth:** Whether to authenticate an ACS making a Connection Request to the CPE.
 - ▶ **Connection Request Username:** Username used to authenticate an ACS making a Connection Request to the CPE.
 - ▶ **Connection Request Password:** Password used to authenticate an ACS making a Connection Request to the CPE.
 - ▶ **CPE Server Name:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
 - ▶ **CPE Port:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
 - ▶ **Status:** Connection Status when CPE making a connection to the ACS. Read only.
 - ▶ **Fail Reason:** Show reason for the failure when CPE making a connection to the ACS. Read only.
- Click the **Save** button when finished.
- Click **Refresh** button to refresh the web page.

6.9 SNMP

You can configure the SNMP parameters and view the registration status of SNMP. Choose the menu **"System→SNMP"** to load the following page.

4G/5G ODU USER MANUAL

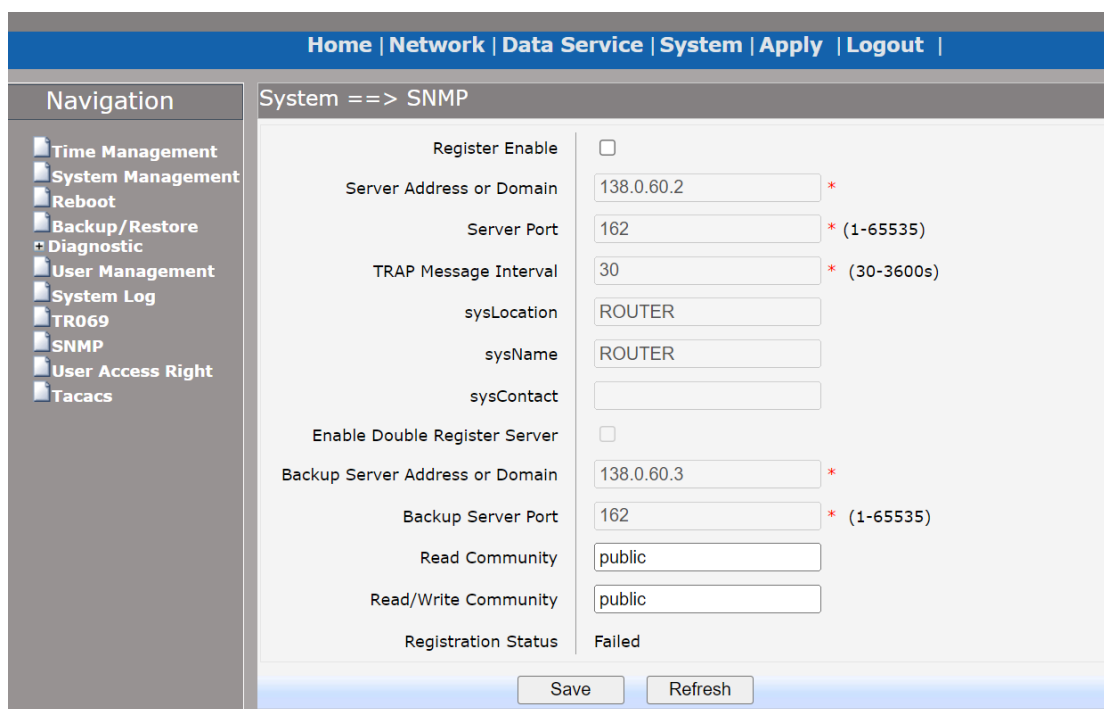


Figure 7-11 SNMP

The following items are displayed in Figure 7-11:

- ▶ **Register Enable:** Check this box to enable SNMP register.
 - ▶ **Server Address or Domain:** Enter the IP address or domain name of register server.
 - ▶ **Server Port:** Enter the port of Register Server.
 - ▶ **TRAP Message Interval:** Set the sending interval between TRAP messages.
 - ▶ **Regional Identity:** Set the identity of regional.
 - ▶ **Device Identifier:** Set the identifier of device.
 - ▶ **Enable Double Register Server:** Check this box to enable backup Register Server.
 - ▶ **Backup Server Address or Domain:** Enter the IP Address or Domain Name of Backup Register Server.
 - ▶ **Backup Server Port:** Enter the port of Backup Register Server.
 - ▶ **Community:** Set the community of SNMP.
 - ▶ **Registration Status:** The status of registration. Read only.
- Click the **Save** button when finished.
- Click **Refresh** button to refresh the web page.

6.10 User Access Right

You can customize the user's access right here.

4G/5G ODU USER MANUAL

Home | Network | Data Service | VoIP Service | System | Apply | Logout |

Navigation: Time Management, System Management, Reboot, Backup/Restore, Diagnostic, User Management, System Log, TR069, SNMP, User Access Right

System ==> User Access Right

☐	Index	Username	Access Detail
☐	1	user	detail
☐	2	guest	detail

Add Del

Enable ☐

Radius Server IP: 1.1.1.1

Radius Server Port: 1812 [0-65535], default: 1812

Radius Shared Secret: *****

Save Refresh

Add:

Home | Network | Data Service | VoIP Service | System | Apply | Logout |

Navigation: Time Management, System Management, Reboot, Backup/Restore, Diagnostic, User Management, System Log, TR069, SNMP, User Access Right

System ==> User Management

User Account

User Role: NULL

User Name: 111

New Password: **

Confirm Password: ***

Save Reset Return

► **User Role:** NULL.

► **User Name:** User's name.

► **New Password:** Set your password of this user.

► **Confirm Password:** Confirm your setting password.

Enter "Detail", you can choose the specific rights.

Home | Network | Data Service | VoIP Service | System | Apply | Logout |

Navigation: Time Management, System Management, Reboot, Backup/Restore, Diagnostic, User Management, System Log, TR069, SNMP, User Access Right

System ==> WebAccessSetting

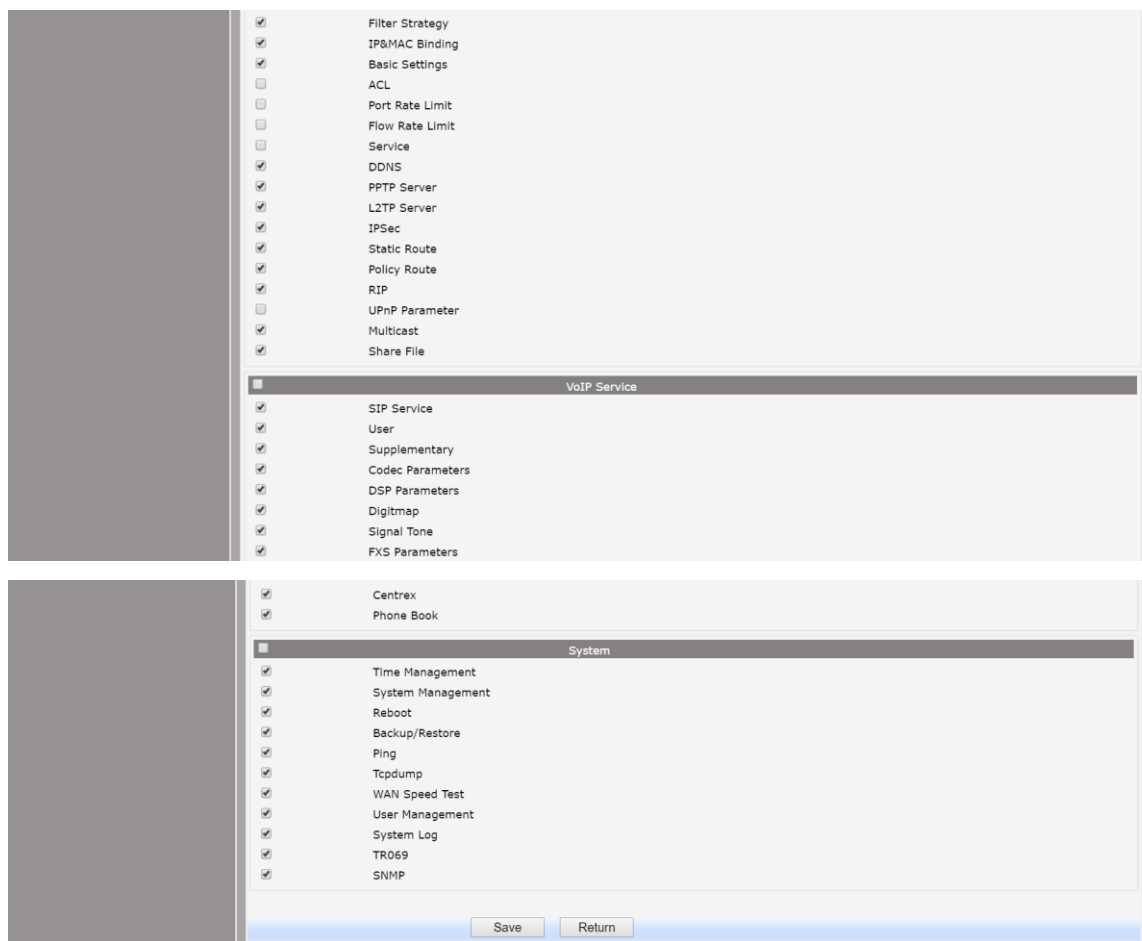
Network

- ☒ Status
- ☒ WAN
- ☒ LAN
- ☒ WLAN
- ☒ 3G Modem
- ☐ PortMirror
- ☒ IPv6

Data Service

- ☒ Status
- ☒ DHCP Server
- ☒ NAT Basic-Settings
- ☒ PAT Settings
- ☒ DMZ Settings
- ☐ ALG Settings
- ☒ Attack Defense
- ☒ Service Type
- ☒ Internet Access-Ctrl
- ☒ Management Access-Ctrl

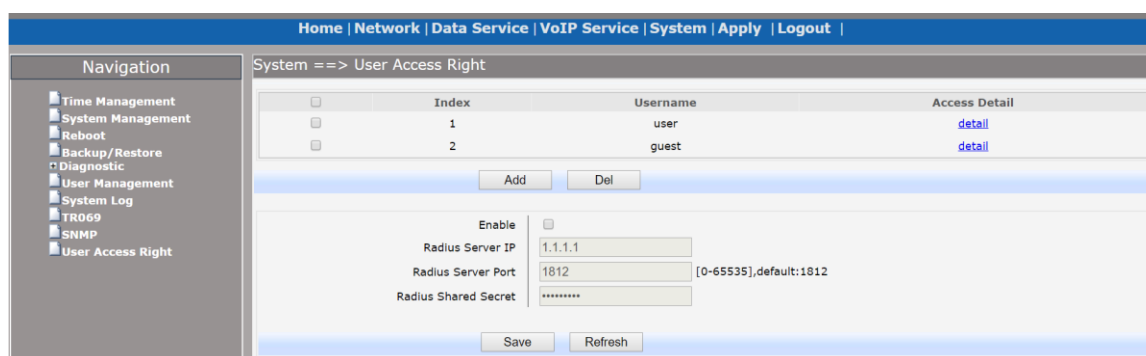
4G/5G ODU USER MANUAL



The screenshot displays the configuration interface for the 4G/5G ODU. It features a sidebar with a list of services, each with a checkbox. The 'VoIP Service' section is expanded, showing sub-options like SIP Service, User, Supplementary, Codec Parameters, DSP Parameters, Digitmap, Signal Tone, and FXS Parameters. Below this, the 'System' section is also expanded, showing options like Time Management, System Management, Reboot, Backup/Restore, Ping, Tcddump, WAN Speed Test, User Management, System Log, TR069, and SNMP. At the bottom, there are 'Save' and 'Return' buttons.

6.10.1 Radius

Set Radius Server here:



The screenshot shows the 'Radius' configuration page. The top navigation bar includes links for Home, Network, Data Service, VoIP Service, System, Apply, and Logout. The left sidebar shows a tree view with 'User Access Right' selected. The main content area is titled 'System ==> User Access Right'. It contains a table with columns for Index, Username, and Access Detail. Below the table are 'Add' and 'Del' buttons. Further down, there are fields for 'Enable' (a checkbox), 'Radius Server IP' (1.1.1.1), 'Radius Server Port' (1812), and 'Radius Shared Secret' (a masked password field). 'Save' and 'Refresh' buttons are at the bottom.

- ▶ **Enable:** Enable Radius.
- ▶ **Radius Server IP:** Radius Server IP.
- ▶ **Radius Server Port:** Radius Server Port.
- ▶ **Radius Shared Secret:** Set Radius server Shared password.

4G/5G ODU USER MANUAL

7 Apply

Follow the prompts, Some parameters take effect only after clicking the button of “**Apply**”.

