InHandNetworks 5G ODU 2000 Series

User Manual

V1.1—2023.05

InHand Networks
Global Leader in Industrial IoT
www.inhandnetworks.com

Declaration

Thank you for choosing our product. Before using this product, please read this manual carefully.

The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.

Due to continuous updating, InHand cannot promise that the contents are consistent with the actual product information, and does not assume any disputes caused by inconsistency of technical parameters. The information in this document is subject to change without notice. InHand reserves the right of final change and interpretation.

©2023 InHand Networks. All rights reserved.

Conventions

Symbol	Indication
1 1	Button name, for example, ‘click Save button’.
“”	Indicates a window name or menu name, for example, the pop-up window “New User”.
>>	A multi-level menu is separated by the double brackets “>>”. For example, the multi-level menu File >> New >> Folder indicates the menu item [Folder] under the sub-menu [New], which is under the menu [File].
Cautions	Please be careful of the contens under Cautions, improper action may result in loss of data or device damage.
Note	Note contain detailed descriptions and helpful suggestions.

Technical Support

Email: support@inhandnetworks.com

URL: www.inhandnetworks.com

CONTENTS

1 Overview 1

2 Hardware 3

2.1 Indicator Description 3

2.2 Restoring to Default Settings via the Reset Button 4

3 Default Settings 5

4 Login and Access to Internet 6

4.1 Connect via Mobile Phone 6

4.2 Connect via PC 8

5 Web Configuration 11

5.1 Dashboard 11

5.2 Status 12

5.2.1 Link Monitor 12

5.2.2 Cellular Signal 12

5.2.3 Clients 13

5.2.4 VPN 13

5.2.5 Events 13

5.2.6 Logs 14

5.3 Internet 14

5.3.1 Uplink Table 14

5.3.2 Uplink Setting 16

5.4 Local Network 18

5.5 Wi-Fi 19

5.6 VPN 20

5.6.1 IPSec VPN 20
5.6.2 L2TP VPN 22
5.7 Security 25
5.7.1 Firewall 25
5.7.2 Policy-Based Routing 28
5.7.3 Traffic Shaping 29
5.8 Services 32
5.8.1 DHCP server 32
5.8.2 DNS server 32
5.8.3 Fixed Address List 32
5.8.4 Static Routes 33
5.8.5 Passthrough Settings 33
5.9 System 34
5.9.1 Change the Password 34
5.9.2 Cloud Management 34
5.9.3 Remote Access Control 35
5.9.4 System Clock 36
5.9.5 Device Options 36
5.9.6 Configuration Management 37
5.9.7 Device Alarms 37
5.9.8 Tools 38
5.9.9 Log Server 40
5.9.10 Other Settings 40

1 Overview

5G cellular greatly enhances the flexibility and convenience of the network at any time and anywhere, which means enterprises can easily build a 5G network in just a few minutes to improve the competitiveness of digital business development. The cloud-managed 5G ODU 2000 series, combined with InCloud Manager SaaS service, provides global customers with high-speed, convenient, and secure 5G efficient networks.

5G ODU is a key part of the cellular gateway series launched by InHand for WAN, which can instantly deploy ultra-high speed 5G network by having gigabit cellular uplink without waiting on broadband; supporting dual SIM card switch network; adapting to the harsh environment. 5G ODU can provide a better and more stable network.

Combined with InCloud Manager, 5G ODU forms a cloud-managed network solution, providing global customers with high-speed and secure network access, and simple and convenient network management services to empower your core business.

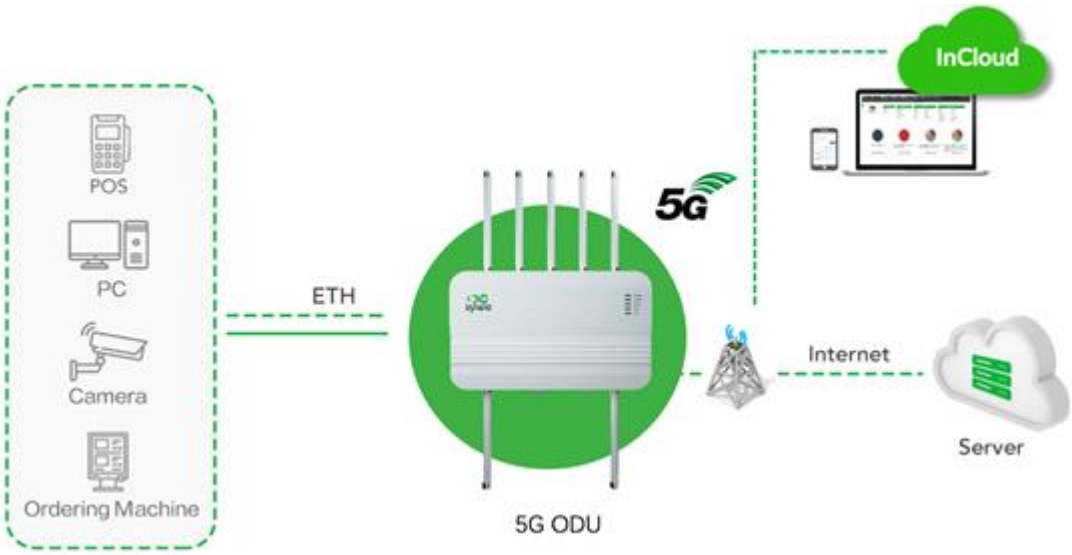


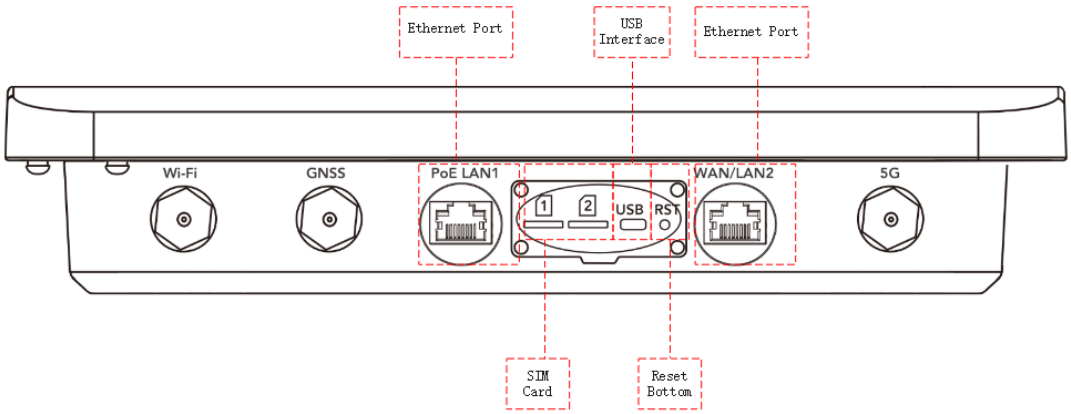
Fig. 1 Application case

2 Hardware

2.1 Indicator Description

ODU2002 Indicator Light	LED status and definition
System	Off --- Power off Steady in red --- System starting Blink in red --- System error Steady in green --- System working
Cellular	Off --- Cellular disable Steady in blue --- 4G dialed up Steady in green --- 5G dialed up Blink in red --- Connection error
Signal	Off --- Connection error Steady in red --- Signal value ≤9 Steady in blue --- 10≤Signal level≤19 Steady in green --- Signal level ≥ 20
LAN	Off --- Connection error Steady in green --- LAN port connected Blink in green --- LAN port data transmitting
WAN	Off --- Connection error Steady in green --- WAN port connected Blink in green --- WAN port data transmitting

2.2 Restoring to Default Settings via the



Reset Button

To restore to default settings by the reset button, please perform the following steps:

1. When the unit power ON, press and hold the reset button for 5-10 seconds.
2. When System LED is steady on blue, release RESET button, system LED will blink in blue, and press the RESET button again.
3. When System LED is steady on blue, release the RESET button. The unit has been restored to default settings and will start up normally later.

3 Default Settings

No.	Function	Default Settings
1	**Cellular**	– SIM1 enabled.
2	**Wi-Fi**	– Wi-Fi 2.4G AP mode enabled, SSID: ODU2002-followed with the last 6 letters of the MAC address. – Auth Method is WPA2-PSK. – Password is the last 8 letters of serial number.
3	**Ethernet**	– PoE LAN1 enabled, IP address: 192.168.1.1, Netmask: 255.255.255.0. DHCP server enabled, 192.168.1.2~ 192.168.1.254. – WAN/LAN2 enabled as WAN, DHCP client mode.
4	**Management Services**	– HTTPS(443) enabled. – Disable HTTPS/SSH/ping from cellular/WAN interface.
5	**Username and password**	– **adm/123456**

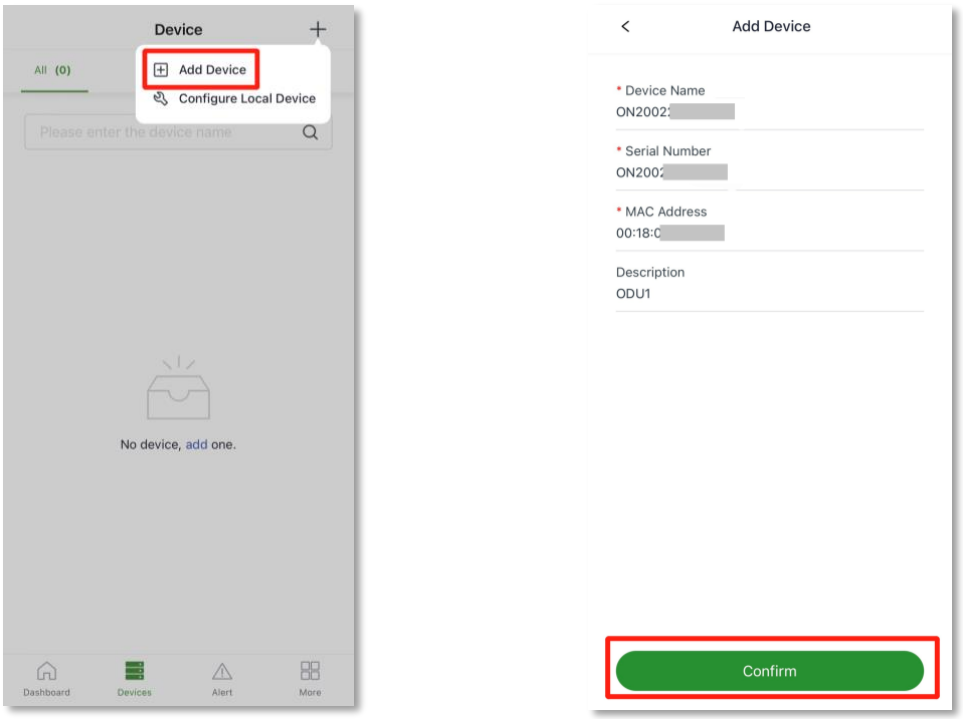
4 Login and Access to Internet

Before power on, please insert the SIM card and connect the 5G antenna to the device. Or connect Ethernet cable to WAN/LAN2 interface.

4.1 Connect via Mobile Phone

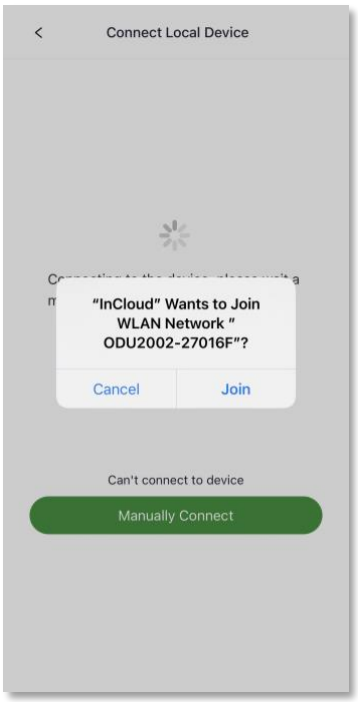
Step 1: Install InCloud APP by scan following QR code in mobile phone.

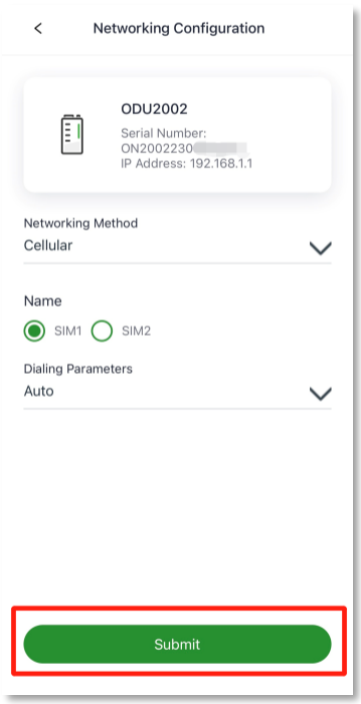
Step 2: Click the "Device" directory below to enter the [Device] page, click the menu button in the upper right corner, and select [Add Device]. Scan the QR code on the ODU to add device.



Step 3: After scanning the code successfully, configure the name, serial number, and description information of the device.

Step 4: If ODU cannot connect to Internet, click "Configure local device" in [Device] page, scan the QR code on the device again and then configure the device to connect to the Internet. Mobile phone will connect to ODU’ s Wi-Fi after scanning the QR code in "Configure local device".



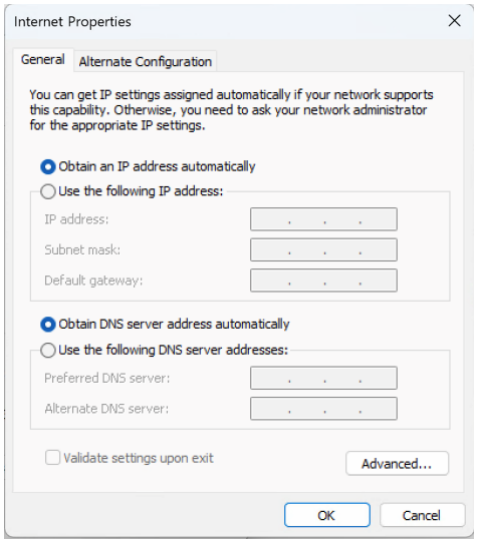


4.2 Connect via PC

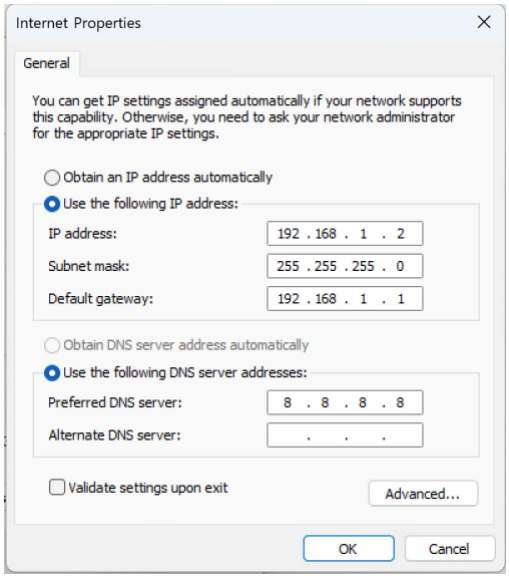
Step 1: Connect PoE LAN1 interface on ODU and PC with Ethernet cable.

Step 2: Set the IP of the PC via DHCP or fixed IP address, the PC IP address and ODU address should be in the same segment.

Use DHCP to obtain the address automatically (recommended). The DHCP server function is enabled by default on the LAN port of ODU.

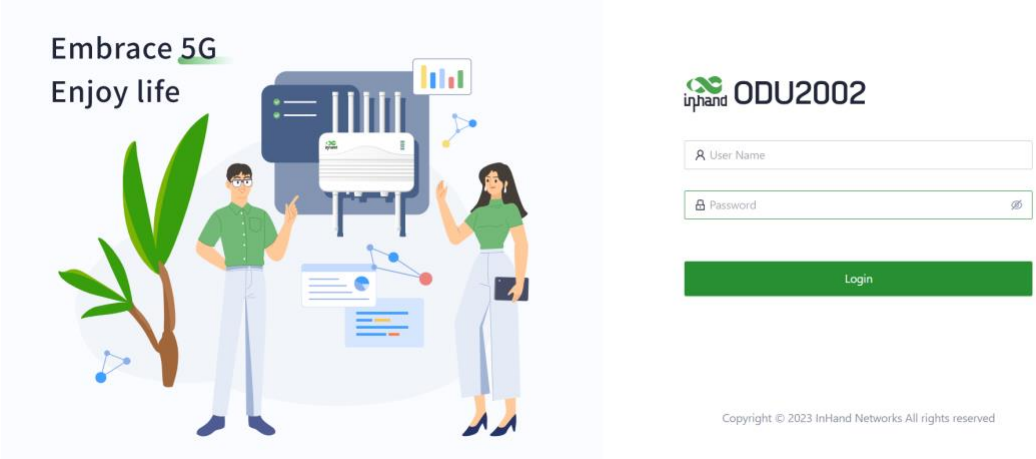


Use a fixed IP address, the PC and the device must be in the same segment. On PC side, the IP address needs to be configured as any address in 192.168.1.2~192.168.1.254, the gateway should be 192.168.1.1, the subnet mask should be 255.255.255.0, and the DNS server should be 8.8.8.8 or operator DNS server address.



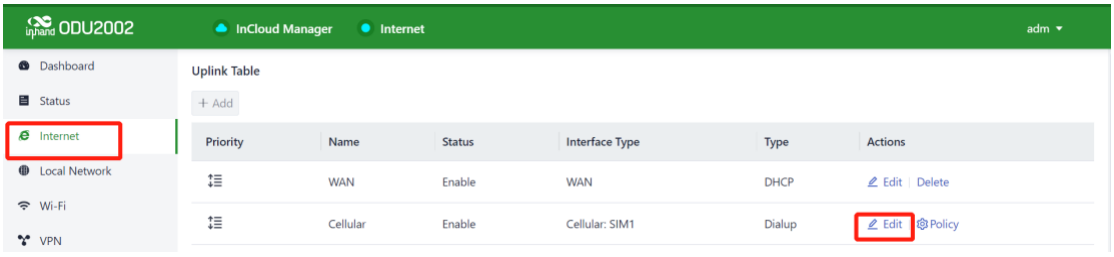
Step 3: Open a browser and enter the device's default address 192.168.1.1 in the browser address bar. After entering the username and password (default: adm/123456), enter the device's WEB management interface. If the page

prompts that the webpage is not secure, open the hidden or advanced options and select "Proceed to website".



Step 4: Check the network status in the "Interface Status" in "Dashboard". The device connects to the Internet successfully if the "Cellular" or "WAN" icon turns green. Click corresponding icon to view interface information such as signal strength, IP address, and traffic consumption.

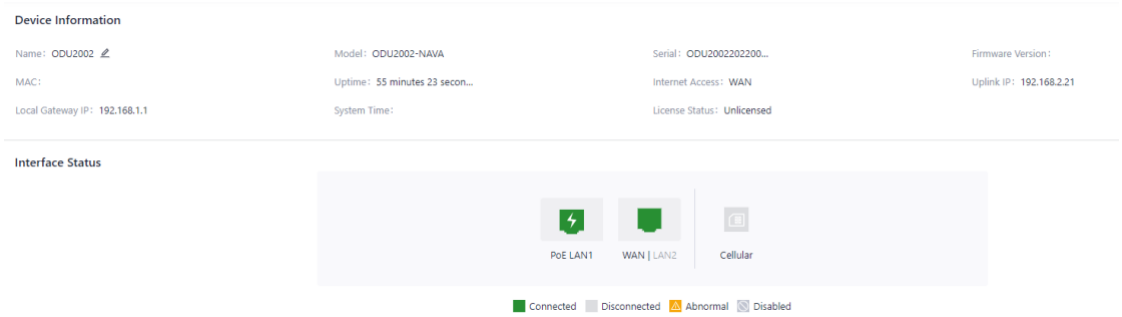
Step 5: If ODU cannot connect to network, click "Internet" on the left navigation bar, click the edit button behind the "Cellular" or "WAN" to set up network parameters. The device enables the dial-up function and WAN by default, please wait for a few minutes to go online, and re-enable the dial-up if it is not dialed.



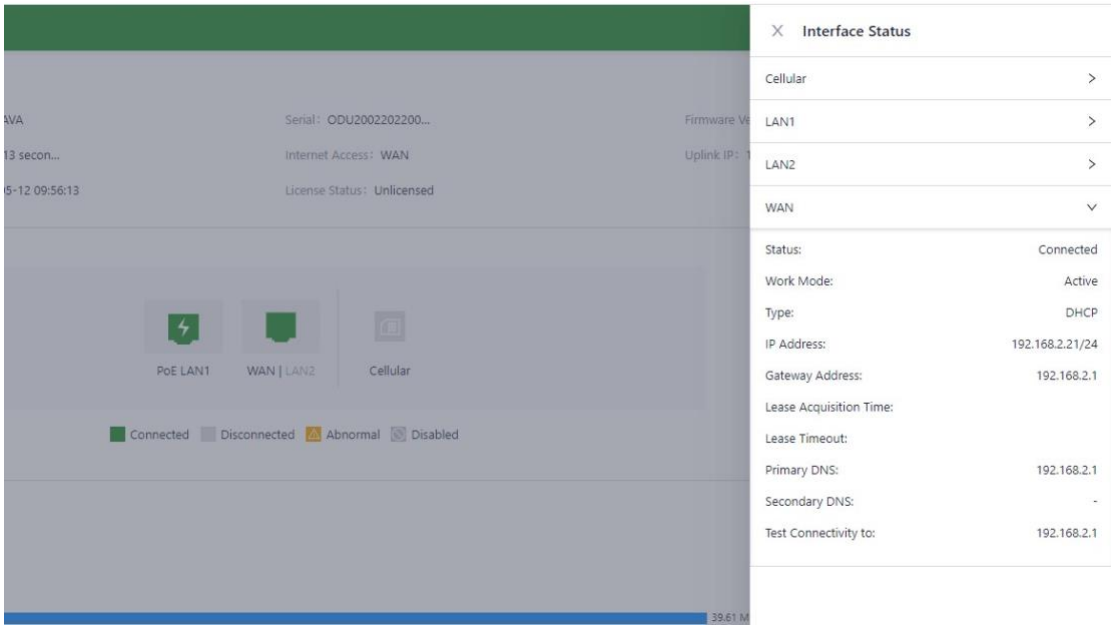
5 Web Configuration

5.1 Dashboard

Click "Dashboard" in the left menu, and check Device Information, Interface Status, Traffic Statistics and Wi-Fi information of the device.



Click interface icon in Interface Status, and check detailed information of the interface in the right menu.

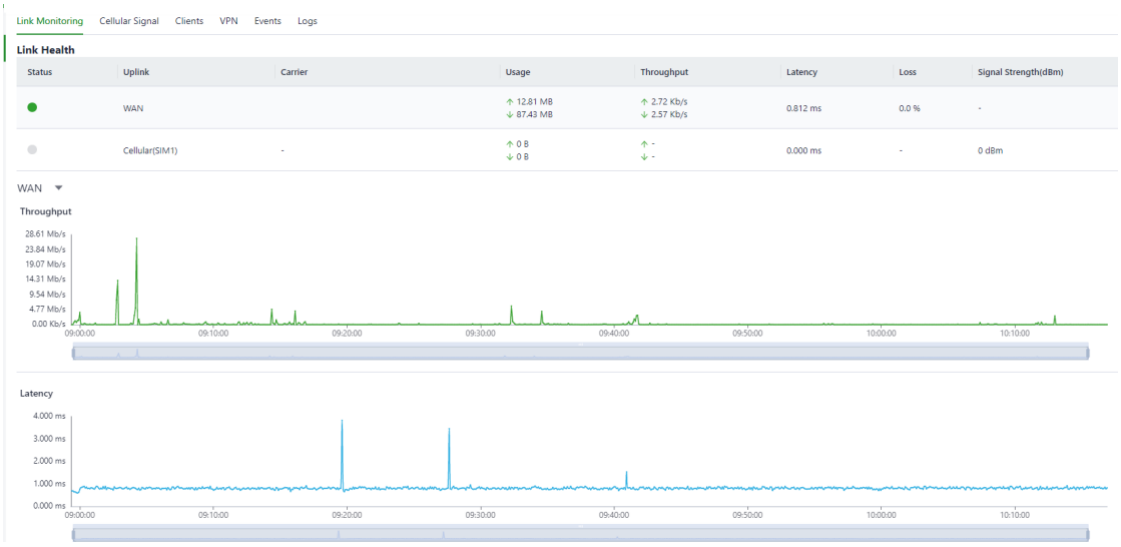


5.2 Status

Click "Status" in the left menu, check link status, signal, log and other information of the device.

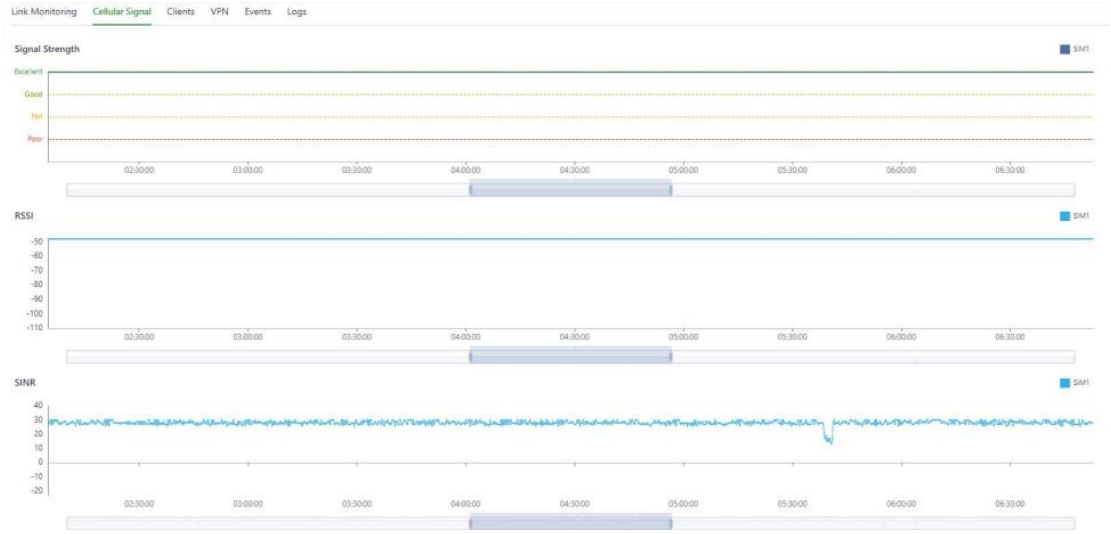
5.2.1 Link Monitor

The Link Monitor page displays the health of each uplink, as well as the throughput, latency and packetloss rate on each uplink interface.



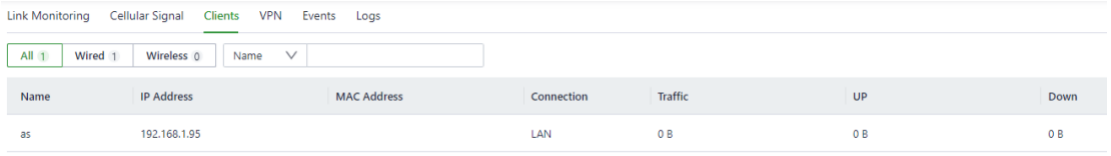
5.2.2 Cellular Signal

The Cellular Signal page displays the SIM card signal strength on the cellular interface, as well as other parameters such as RSSI, SINR, and RSRP.



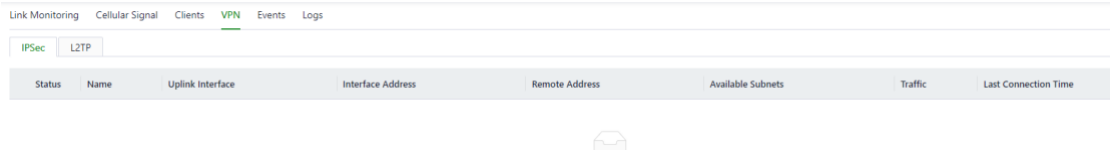
5.2.3 Clients

The Clients page displays details about each client connected to ODU, such as device name, IP address, MAC address, traffic statistics, and online duration.



5.2.4 VPN

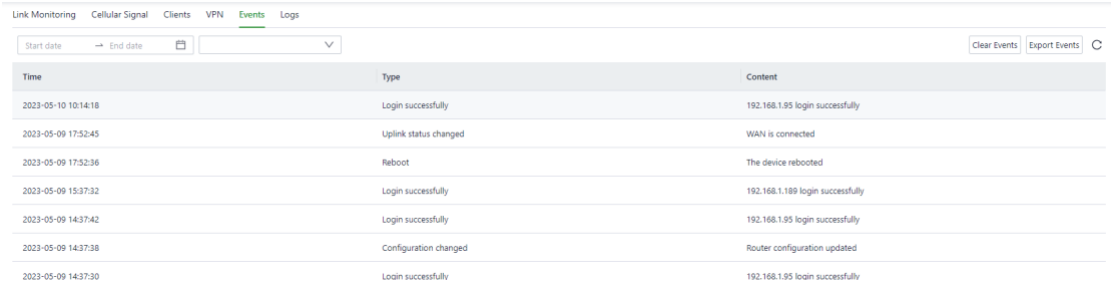
Check the status and the traffic consume of the VPN in ODU in VPN page.



5.2.5 Events

ODU will record event log like user login, configuration changed, link changed, reboot and other events in Events page,

By selecting start data, end date and event type, narrow the scope of retrieval and view a certain type of event.



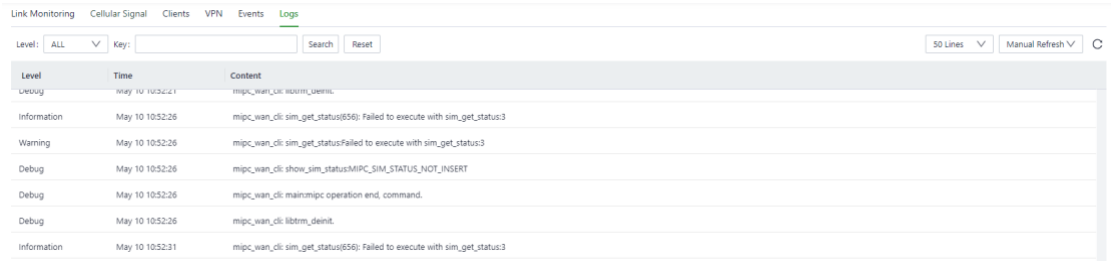
5.2.6 Logs

Check the logs recorded during operation of the device, which can be used for trouble shooting when the ODU can not work properly.

Clear Logs: clear current running logs.

Download Logs: download running logs.

Download Diagnostic Logs: download log information for trouble shooting, it contains system running logs, device information, and device configuration.



5.3 Internet

Click “Internet” in the left menu to check and configure the uplink interfaces and multi-link work mode of ODU.

Please exercise caution when changing Internet settings and may cause network interruption.

5.3.1 Uplink Table

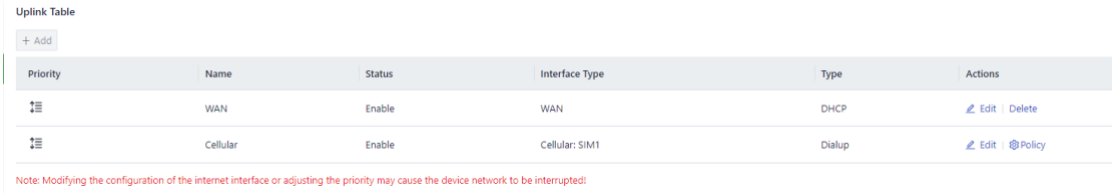
Check and edit WAN and Cellular interface in Uplink Table. It supports to edit cellular threshold policy in this page, and drag icons in the Priority column to reprioritize the interfaces.

Notes:

If delete WAN interface in this page, WAN/LAN2 port will work as LAN.

WAN/LAN2 port will change back to WAN if add WAN interface again.

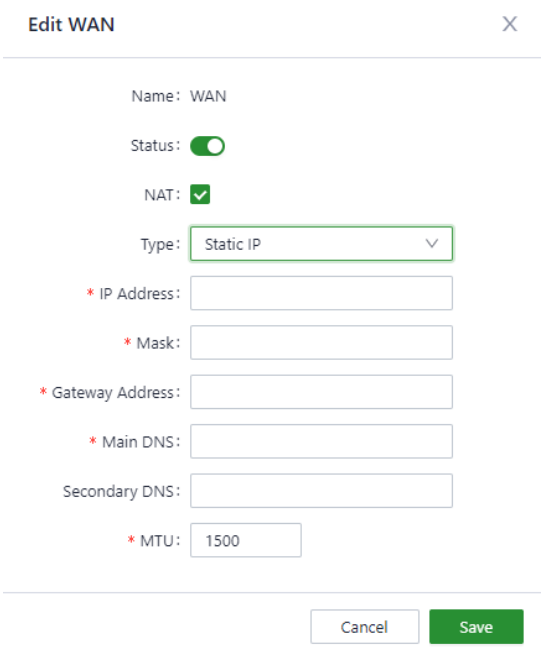
When delete WAN, all configuration on this interface like the static routes, inbound and outbound rules, port forwarding etc. will be removed.



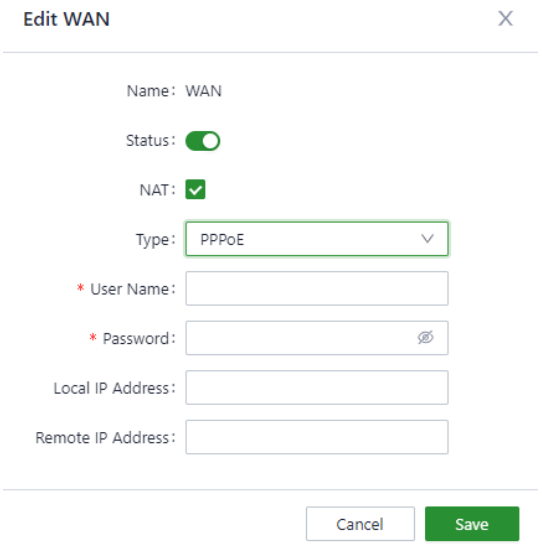
ODU supports three types of WAN interface:

DHCP: The DHCP service is enabled on the WAN interface by default. Therefore, ODU can connect to the Internet immediately if connect WAN interface to upstream network device which enables DHCP server.

Static IP: Manually assign an IP address obtained from the carrier or upstream network device.

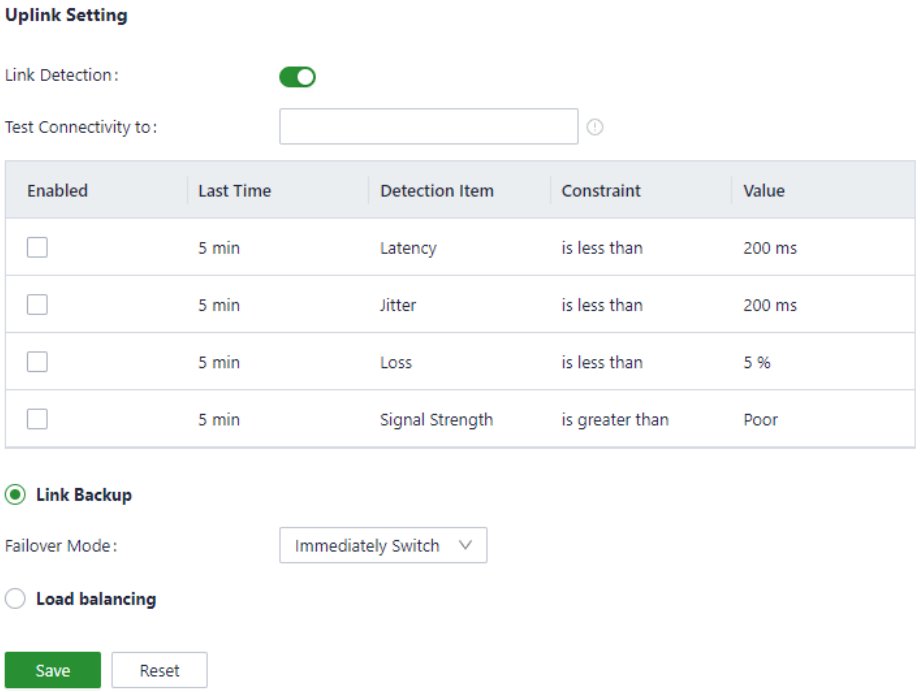


PPPoE: Set the PPPoE service on WAN so that ODU can dial up to the Internet through the broadband service.



5.3.2 Uplink Setting

Configure link detection items and optimal forwarding mode for uplink interfaces.



Link detection is enabled by default. In the private network environment, please manually configure the address in "Test Connectivity to" or disable link detection function to prevent the cellular interface from working abnormally.

If detection function is disabled, it will not display latency, jitter, packet loss rate, or signal strength in Status page.

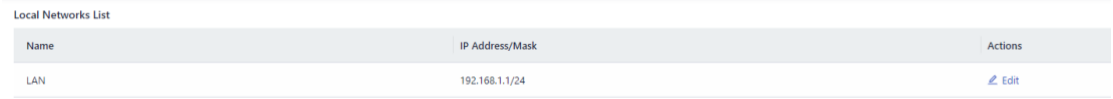
If the "Test Connectivity to" address is empty, system will detect the primary DNS server address obtained by each interface, otherwise, system will use this address as the detection address for all uplink interfaces.

In **Link Backup** mode, ODU will monitor enabled items and trigger a link switch when any item exceeds the threshold. If there is no item enabled, link switch will only be triggered based on priority and connectivity of the links.

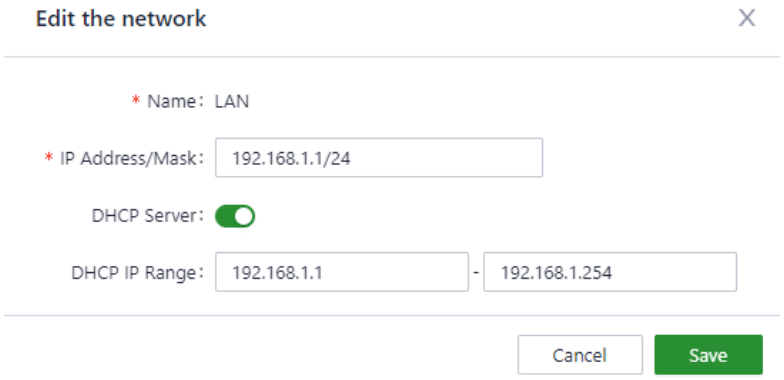
In **Load Balancing** mode, ODU will distribute data traffic to all available links.

5.4 Local Network

Check and configure LAN of the device in Local Network page.

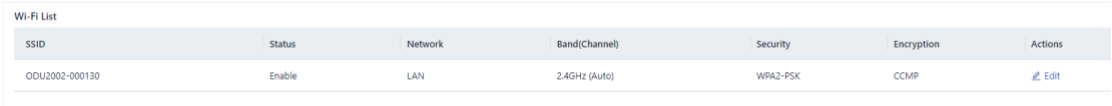


Edit the network: Click the Edit button on the right to edit LAN IP, enable/disable DHCP server and change the range of DHCP address.

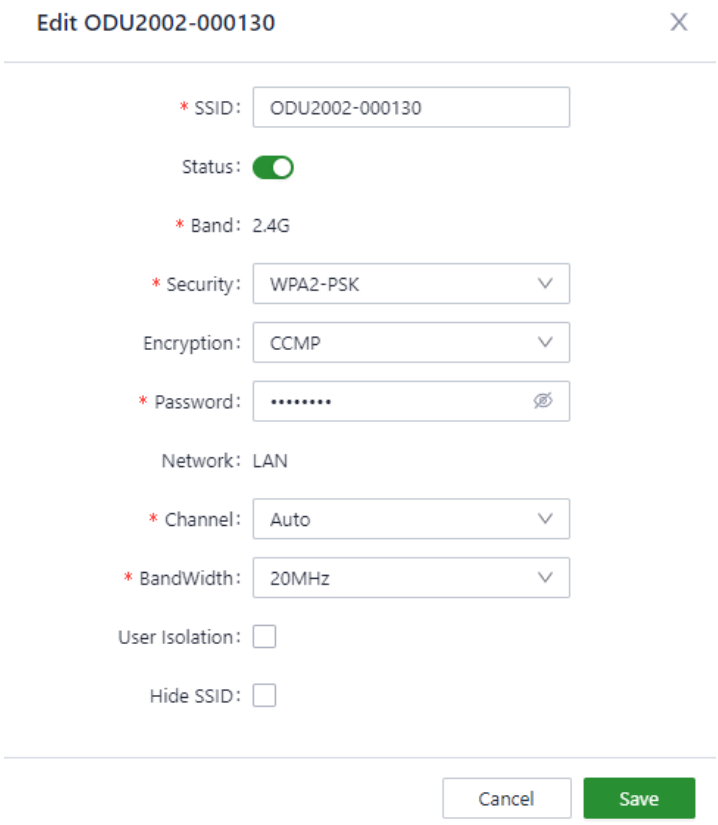


5.5 Wi-Fi

Configure ODU to serve as Wi-Fi AP to provide SSID for wireless network access.



Edit Wi-Fi: Click Edit button on the right, configure SSID, password or other parameters of this Wi-Fi.



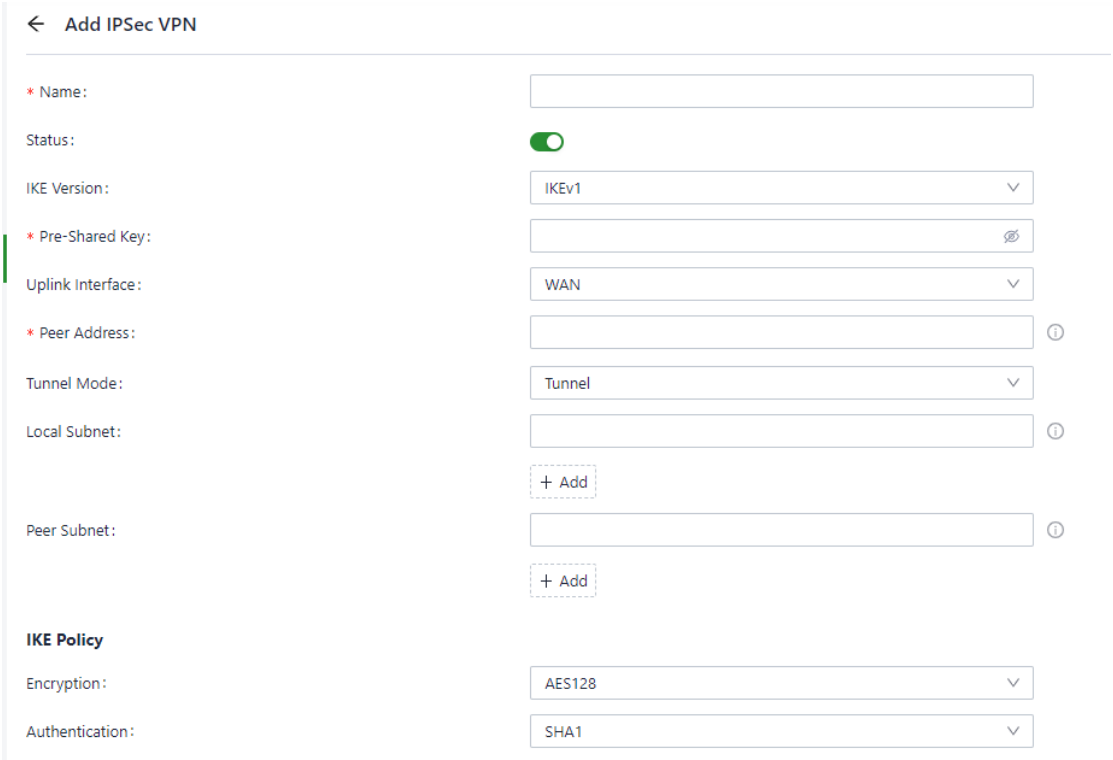
5.6 VPN

VPN is intended to establish a private network on the public network for encrypted communication. A VPN router enables remote access by encrypting data packets and converting the destination address of data packets. VPN can be realized by a server, hardware, or software. Compared with the traditional DDN private line or frame relay, VPN provides a more secure and convenient remote access solution.

5.6.1 IPSec VPN

IPsec is a group of open network security protocols developed by IETF. At the IP layer, data source authentication, data encryption, data integrity, and anti-replay functions are used to ensure the security of data transmission between communication parties on the Internet, which reduces the risk of leakage and eavesdropping, ensures the integrity and confidentiality of data, and the security of service transmission for users.

In IPSec VPN page, click Add button on the left to build a new IPSec tunnel.



The following parameters must be set in IPSec tunnel

Name: specify the name of the IPSec VPN created on the device, which is used for local VPN management.

IKE Version: specify the version of the IKE protocol used on ODU, IKEv1 or IKEv2.

Pre-Shared Key: specify the authentication key for IKE negotiation, which must be consistent on both sides.

Uplink Interface: specify the local uplink interface used to establish the IPSec VPN tunnel.

Peer Address: specify the IP address of the peer device.

Notes: The peer IP address must be set to 0.0.0.0 if working as IPSec server.

Tunnel Mode: specify the IP packet encapsulation mode on the IPSec VPN tunnel, which can be tunnel mode or transmission mode.

Local Subnet: specify the IP address segment of the traffic to be sent out by the ODU through IPSec VPN tunnel.

Peer Subnet: specify the IP address segment used for communication on the other end of the IPSecVPN tunnel.

IKE Policy:

Encryption: specify the encryption algorithm for IKE.

Authentication: specify the authentication algorithm for IKE.

DH Groups: specify the DH key exchange mode.

Lifetime: specify the lifetime of the IKE SA. The default value is 86400 seconds. **IPSec Policy:**

Security Protocol: specify the security protocol used for ERP.

Encryption: specify the encryption algorithm the ESP protocol.

Authentication: specify the authentication algorithm for ESP.

PFS Groups: specify the Perfect Forward Secrecy (PFS) mode, which improves the communication security through an additional key exchange in Phase 2 negotiation.

Lifetime: specify the lifetime of the IPSec SA. The default value is 86400 seconds.

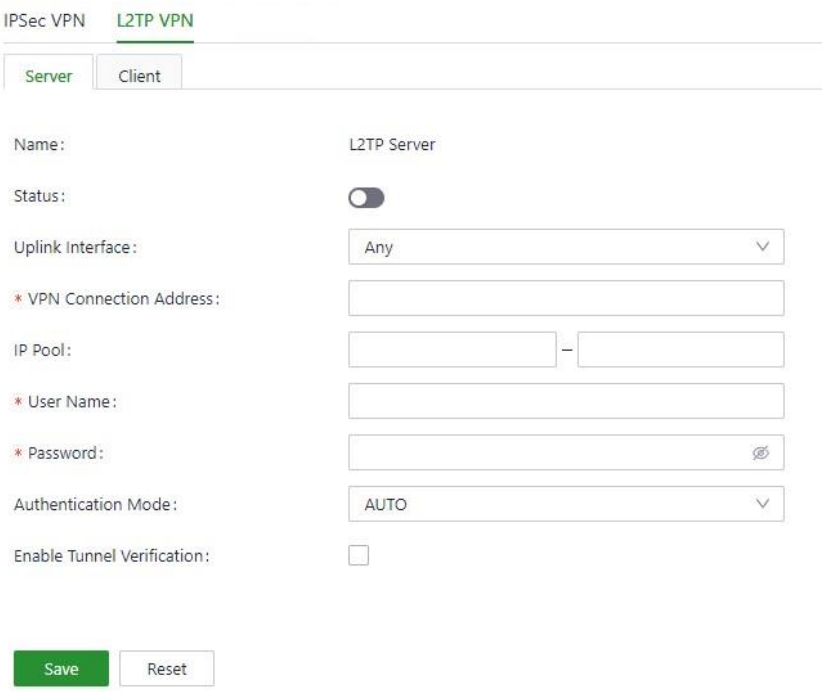
5.6.2 L2TP VPN

Layer 2 Tunneling Protocol (L2TP) is a tunnel protocol for virtual private dial networks (VPDNs). This protocol establishes a tunnel from a remote site to the headquarters of an enterprise over a public switched telephone network (PSTN) or integrated services digital network (ISDN) through Point-to-Point Protocol

(PPP) negotiation. This tunnel allows remote users to connect to the intranet of the enterprise in a secure way.

5.6.2.1 Server

Generally, L2TP server is deployed at the headquarters of an enterprise to provide remote access for employees. On the VPN page, choose L2TP VPN > Server to display the L2TP server configuration.



Name: the name of the L2TP server, cannot be changed.

Status: enable or disable L2TP server. This function is disabled by default.

Uplink Interface: specify the uplink interface used to establish a tunnel from L2TP server.

VPN Connection Address: specify the gateway address for the L2TP client.

IP Pool: System will assign an IP address to the L2TP client from the specified IP address pool.

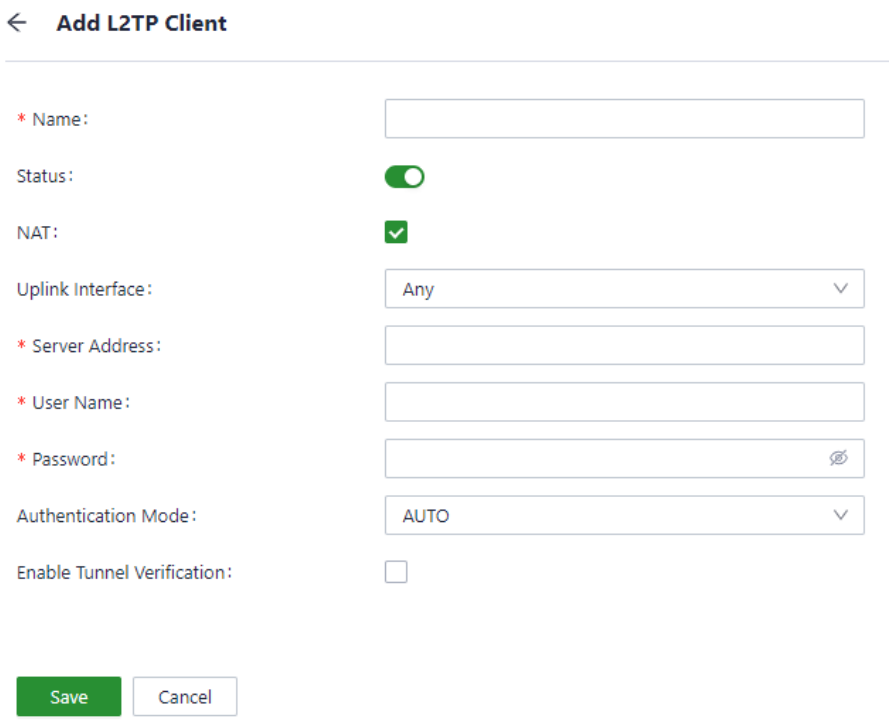
User Name/Password: specify the user name and password for L2TP negotiation, which must be consistent on both ends of the tunnel.

Authentication Mode: specify the authentication mode for the L2TP tunnel.

Enable Tunnel Authentication: Please make sure both ends of the tunnel are configured with the same user name and password if enable this option.

5.6.2.2 Client

Click Add button on the left to configure L2TP client parameters and establish a tunnel with remote L2TP server.



Name: specify the local name of L2TP client tunnel.

Status: enable or disable L2TP client tunnel.

NAT: enable or disable NAT for packets forwarded by the ODU for the LAN device.

Uplink Interface: specify the uplink interface used to establish L2TP tunnel.

Server Address: specify the IP address used by the remote L2TP server.

User Name/Password: specify the user name and password for L2TP negotiation, which must be consistent on both ends of the tunnel.

Authentication Mode: specify the authentication mode for the L2TP tunnel.

Enable Tunnel Verification: Please make sure both ends of the tunnel are configured with the same server name and verification key if enable this option.

5.7 Security

Click "Security" in the left menu to enter Security page, and configure advanced security features including firewall, policy-basedrouting, and traffic shaping.

5.7.1 Firewall

Set inbound or outbound rules, port forwarding and MAC address filter in firewall.

5.7.1.1 Inbound/Outbound Rules

User can set rules to control data traffic based on interface. For example:

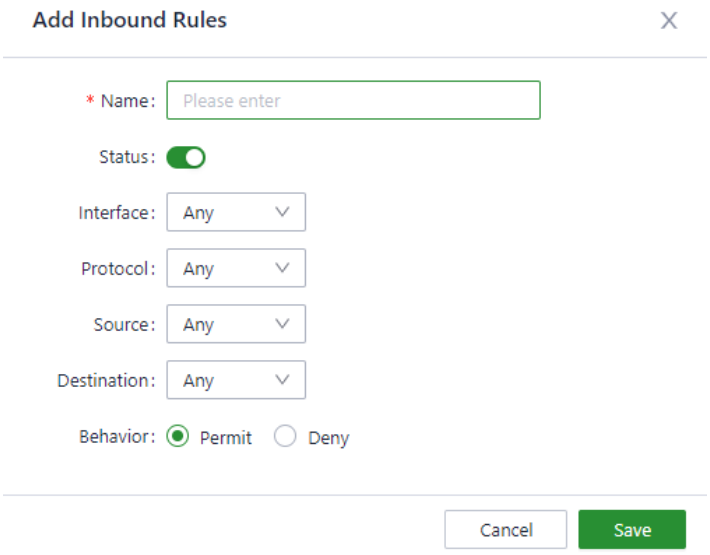
User can use inbound rules to forbid some of IP addresses to access to router when under attack from such IP.

User can use outbound rules to forbid some client devices to access to public network.

Outbound rules: Inside network access to outside network, allow all data by default.

InBound rules: Outside network access to inside network, forbid all data by default.

Click Add button in the left to add a new rule.



Name: set the local identifier of the inbound rule.

Status: enable or disable the rule.

Interface: set the traffic forwarding interface. For an outbound rule, select the interface from which traffic is sent out. For an inbound rule, select the interface on which traffic is received.

Protocol: set the protocol type of packets to be matched, supports **Any**, **TCP**, **UDP**, **ICMP**, and **Custom**.

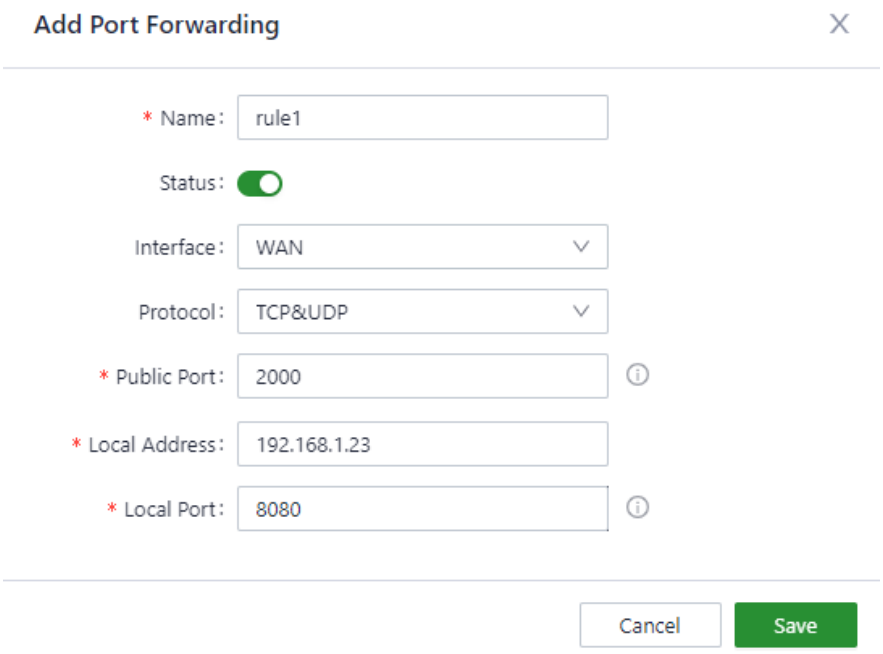
Source: set the source IP address of packets to be matched, supports IP address or retain the default option **Any**.

Destination: set the destination IP address of packets to be matched, supports entering an IP address or retain the default option **Any**.

5.7.1.2 Port Forwarding

When outside network accesses to specific ports of the ODU, system will transfer this data to corresponding ports of inside device according to relevant port forwarding rules. So that the service deployed in LAN will be available in public network, and the same public IP address can be used to access to plenty of services by using multiple port forwarding rules.

For example, after set port forwarding rules like below, when users from public network try to access to ODU’ s port 2000 on WAN, system will transfer request to 192.168.1.23:8080 in LAN.



Name: set the local identifier of the port forwarding rule.

Status: enable or disable the port forwarding rule.

Interface: set the uplink interface that provides port mapping for internal clients. This interface must have a public IP address.

Protocol: set the protocol type to which port mapping is applied. **TCP**, **UDP**, and **TCP&UDP**.

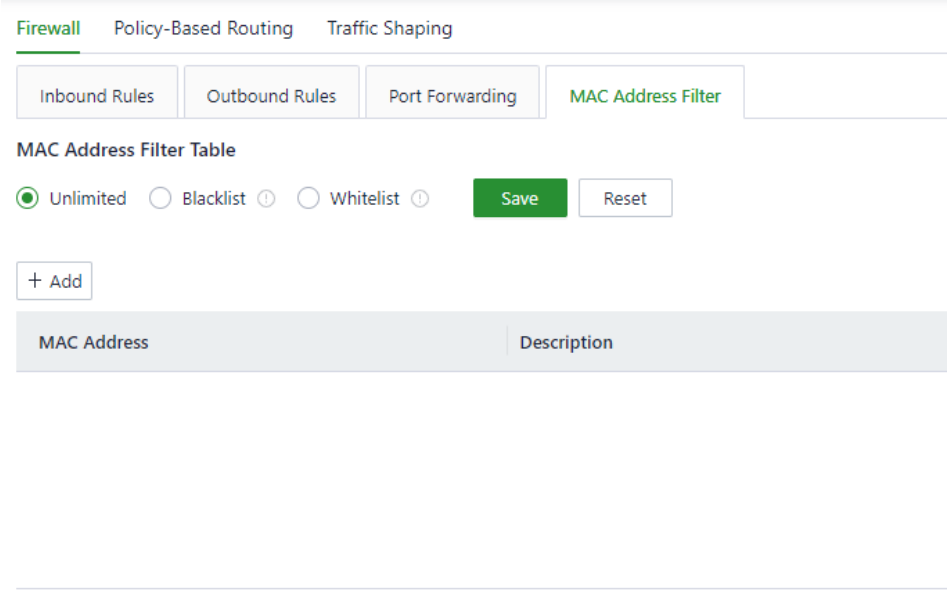
Public Port: set the protocol port on the uplink interface to be mapped.

Local Address: set the IP address of the target client that external users need to access.

Local Port: set the protocol port that external users need to access on the target client.

5.7.1.3 MAC Address Filter

Configure MAC address filter rules for LAN devices to allow or forbid LAN devices to access to Internet.



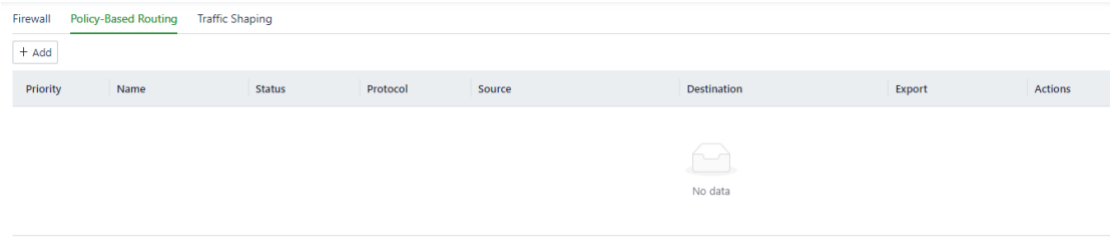
Blacklist: Devices in the blacklist will not be able to access the Internet.

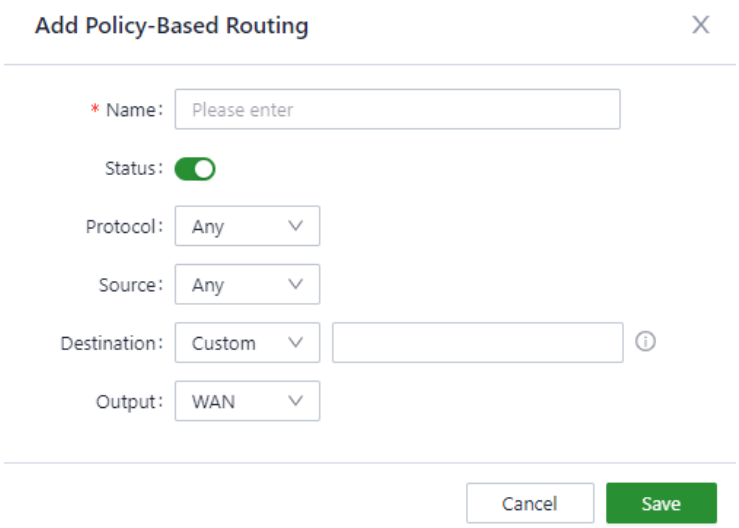
Whitelist: Only devices in the whitelist are allowed to access the Internet.

5.7.2 Policy-Based Routing

Policy-based routing (PBR) allows ODU to forward different data flows through different links based on configured policies. This feature enables flexible route selection and control, thus improving the link utilization and

reducing operational cost of the enterprise. Choose **Security** > **Policy-based Routing** and click **Add** to add a PBR rule.





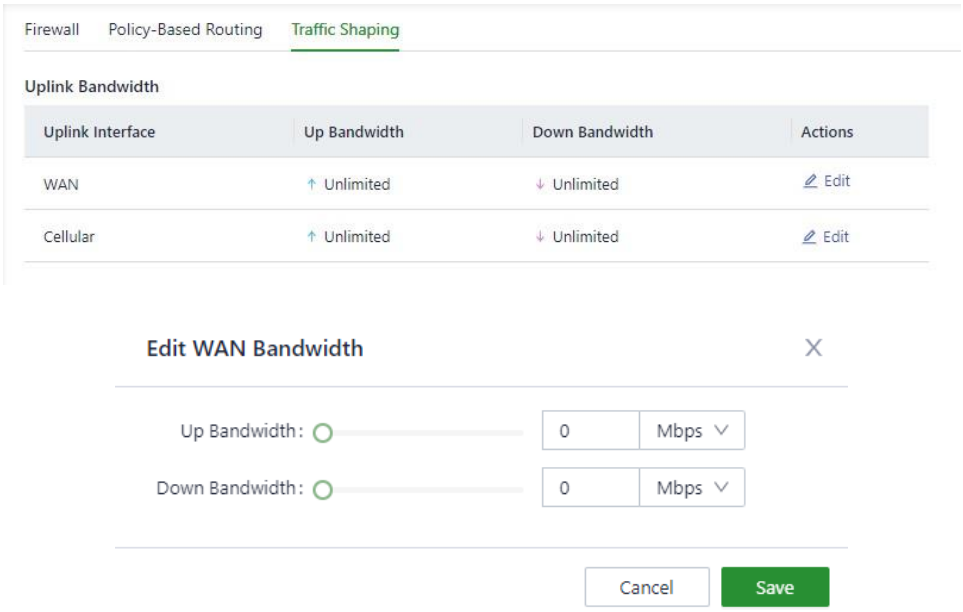
Notes:

The source and destination addresses of the PBR cannot be set as **Any** at the same time.

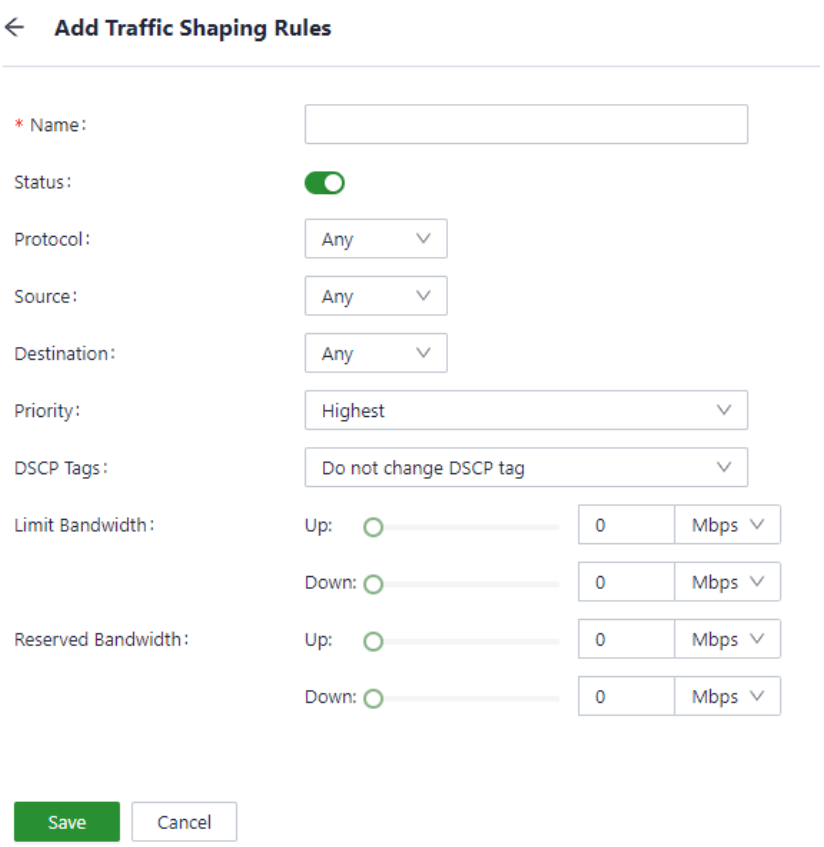
5.7.3 Traffic Shaping

Create shaping policies to apply per-user controls on a per-protocol basis to optimize the network. This function can also reduce bandwidth for recreational traffic, and prioritize bandwidth for critical business traffics.

Choose **Security** > **Traffic Shaping** and click **Edit** to modify the bandwidth of the uplink interfaces.



Click **Add** to create a new traffic shaping rule. Traffic shaping policies consist of a series of rules that are performed in order, which is similar to custom firewall rules. There are two main components to each rule: the type of traffic to be limited or shaped (rule definition), and how that traffic should be limited or shaped (rule actions).



Notes:

Traffic forwarding priority for unmatched rules is medium.

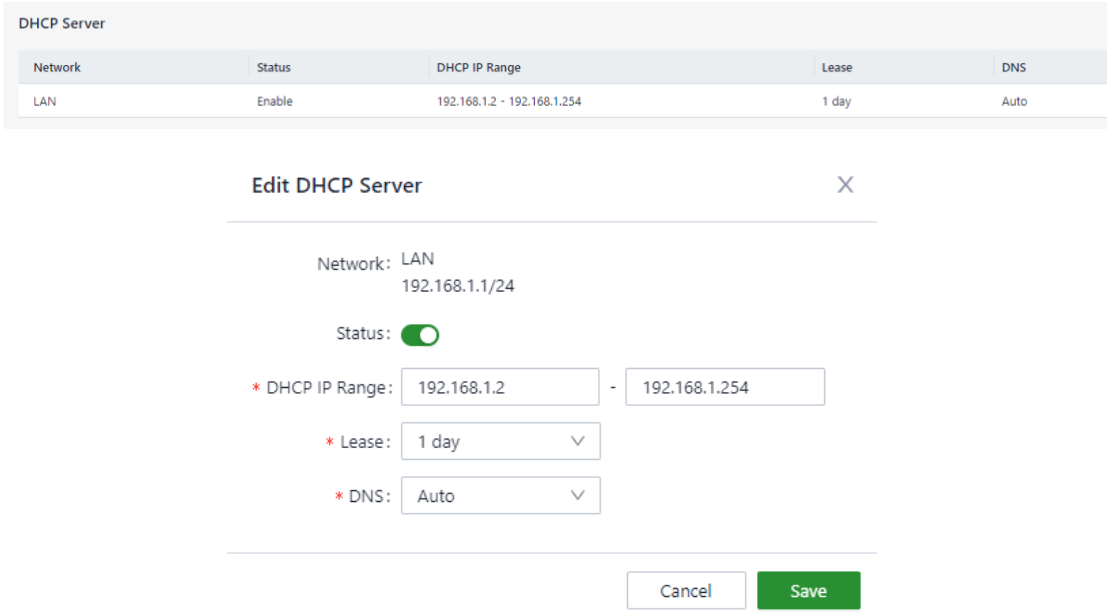
When Limit Bandwidth is set to 0, system will not limit the bandwidth.

The value of Reserved Bandwidth should not be greater than the Limit Bandwidth.

5.8 Services

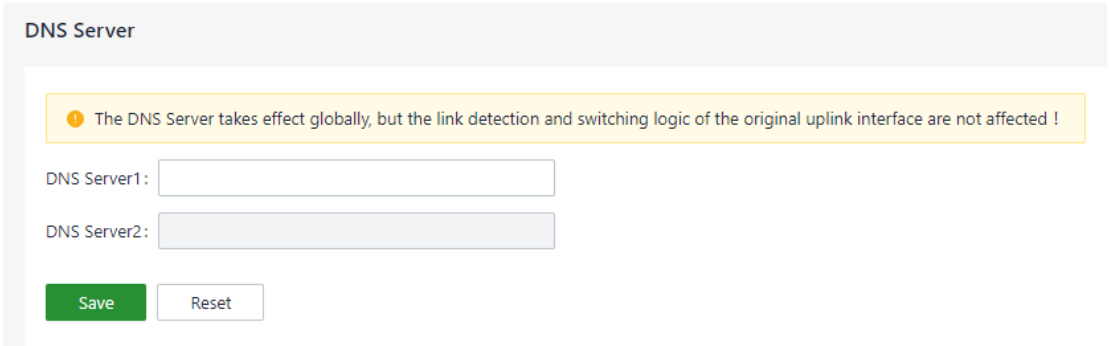
5.8.1 DHCP server

DHCP implements dynamic IP address allocation in a client/server model. The LAN device sends a request to ODU, and ODU replies with an IP address assigned to the client.



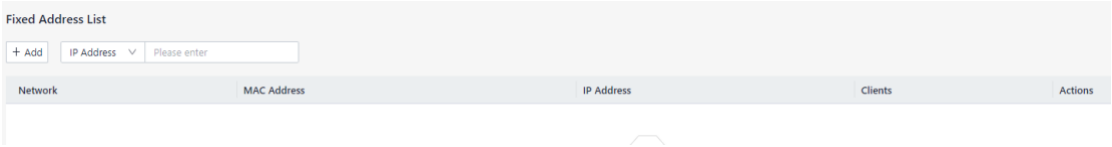
5.8.2 DNS server

Set global DNS server for ODU. System will use DNS server in this page if the original DNS server from uplink interface cannot work.



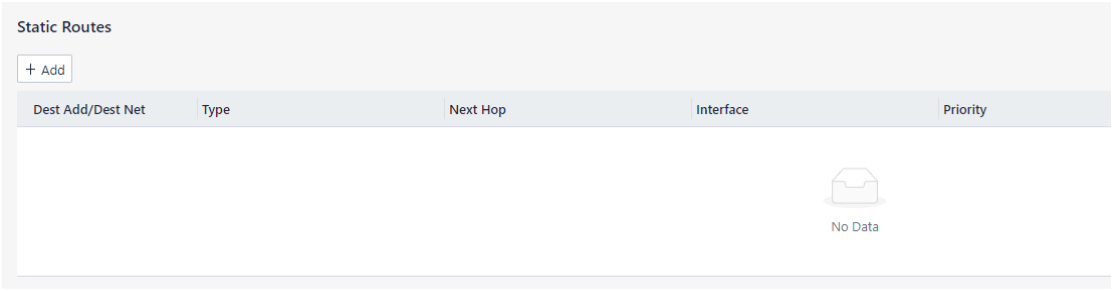
5.8.3 Fixed Address List

ODU is able to distribute IP address based on client device’ s MAC address by using fixed address list. Distributed IP address should in the range of IP address of the local network.



5.8.4 Static Routes

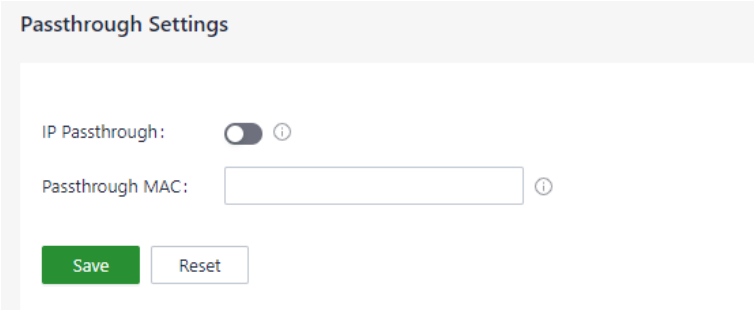
Configure static routes to forward data by specific route or interface. This list will only display the rules created by user, and will not show the routes created automatically after modifying WAN or LAN interface.



Static routes to the same destination IP address or network cannot have the same next-hop address, outbound interface, or priority.

5.8.5 Passthrough Settings

Configure IP passthrough to transparently forward data from uplink interface to one client device.



Notes:

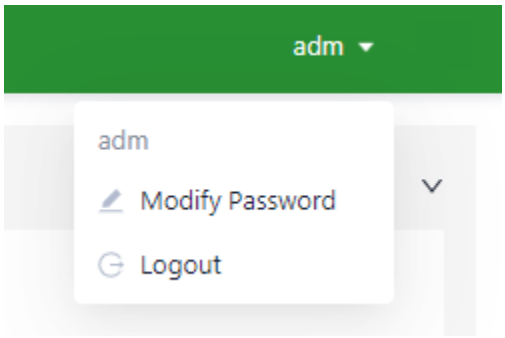
After the IP Passthrough mode is enabled, only one client can access to Internet, and Static routing, VPN, Port Forwarding and Policy-Based Routing functions will not work.

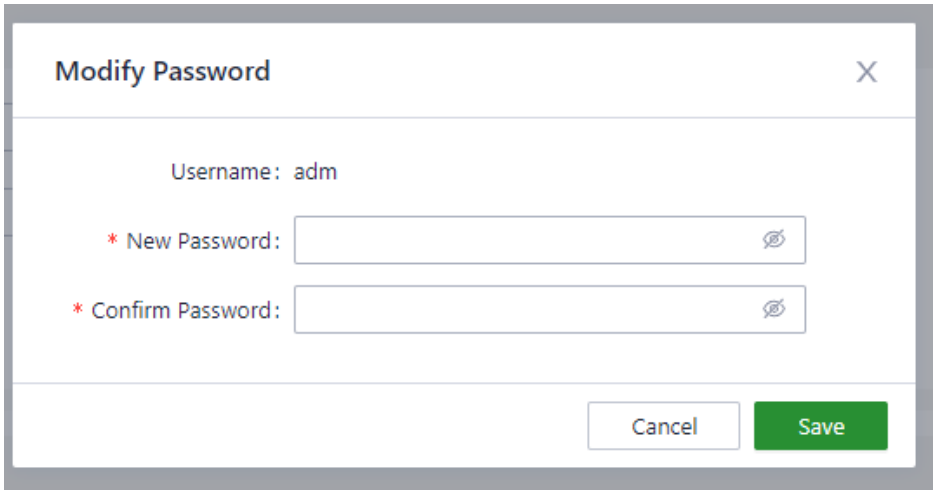
The inbound rule needs to be released when accessing the client device.

5.9 System

5.9.1 Change the Password

The default username and password of ODU is adm/123456. Please change the password for securiry after first login. Click “adm” on the top right of the web page, click **Modify Password** in the menu to change the password.

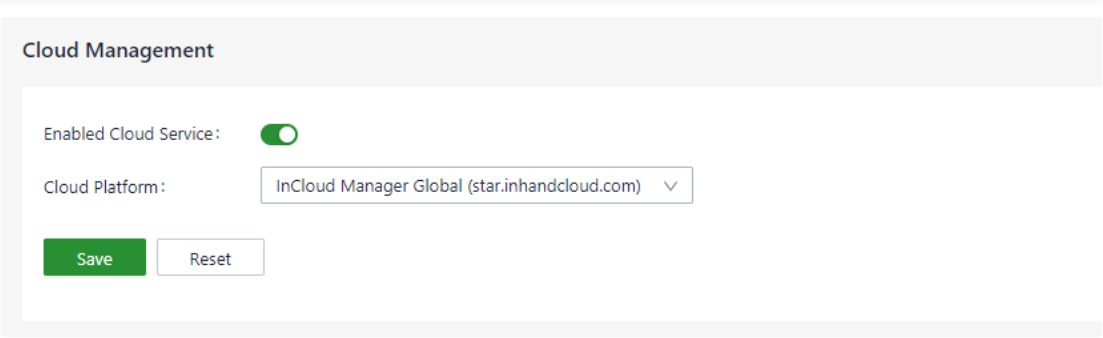




5.9.2 Cloud Management

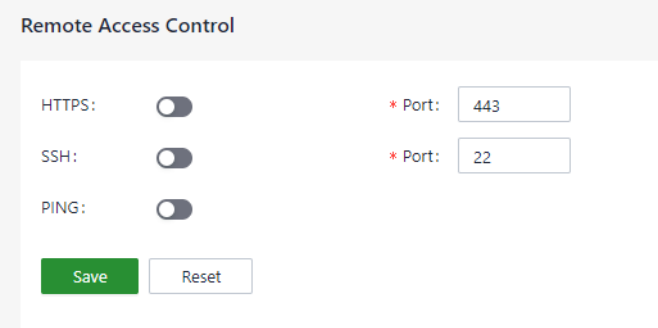
InCloud Manager (star.inhandcloud.com) is a cloud platform developed by InHand to help enterprises accelerate network deployment, simplify network maintenance, and improve service experience. This platform provides zero touch deployment, intelligent maintenance and security features to create good service experiencefor users. Users can log in to the platform to manage the devices temotely, perform batch configuration, and monitor traffic on the devices.

ODU connects to InCloud Manager automatically. User can select which InHand platform to connect to in this page, and also disable InCloud Manager in this page.



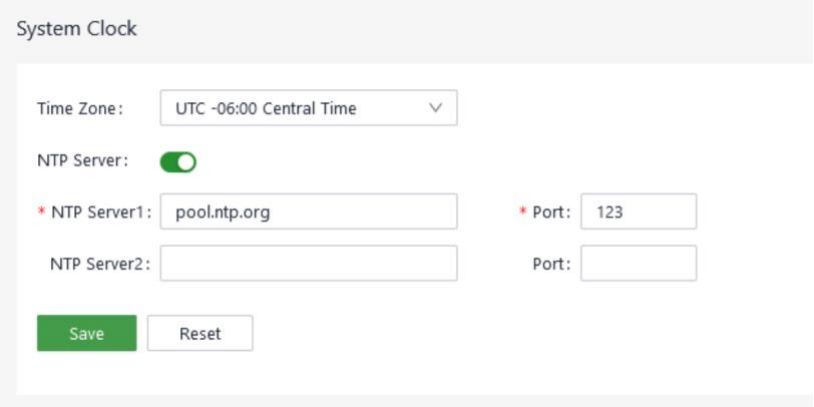
5.9.3 Remote Access Control

User can allow or forbid public network to access to ODU and which port for public network to access to ODU in this page. The rules in this page will not influence LAN device to access to ODU. ODU supports HTTPS when access to its web configuration page.



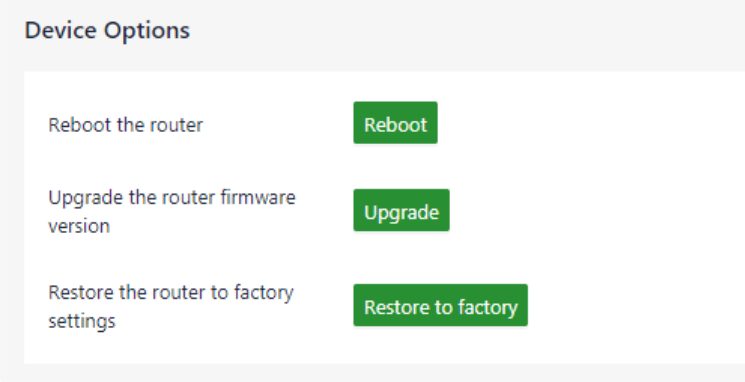
5.9.4 System Clock

Select a time zone for the system and enable the NTP server to synchronize time with the target NTP server.



5.9.5 Device Options

Reboot, upgrade firmware or reset ODU to default factory settings in this page.



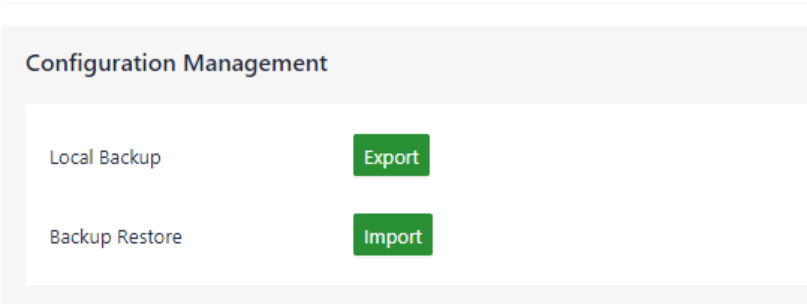
Notes:

Before upgrading the firmware, please make sure the new firmware is obtained froman official source.

If the ODU is connected to InCloud Manager, the platform will synchronizes the settings before restore to factory settings. The ODU will only clear historical data.

5.9.6 Configuration Management

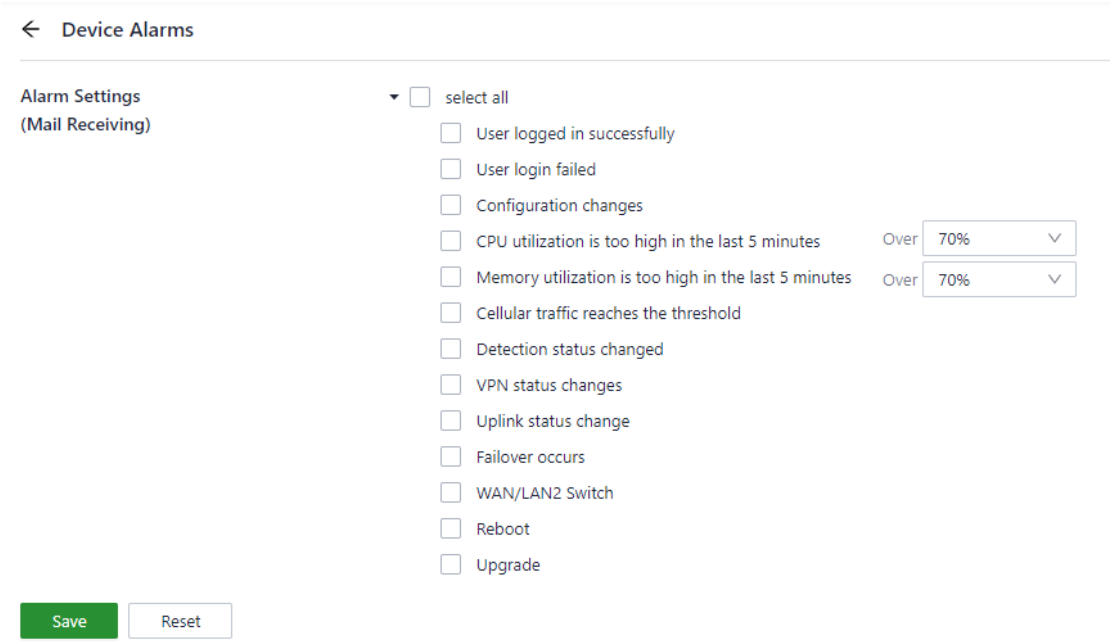
User can export system configuration to local PC as backup, and import the configuration to device to restore the configuration.



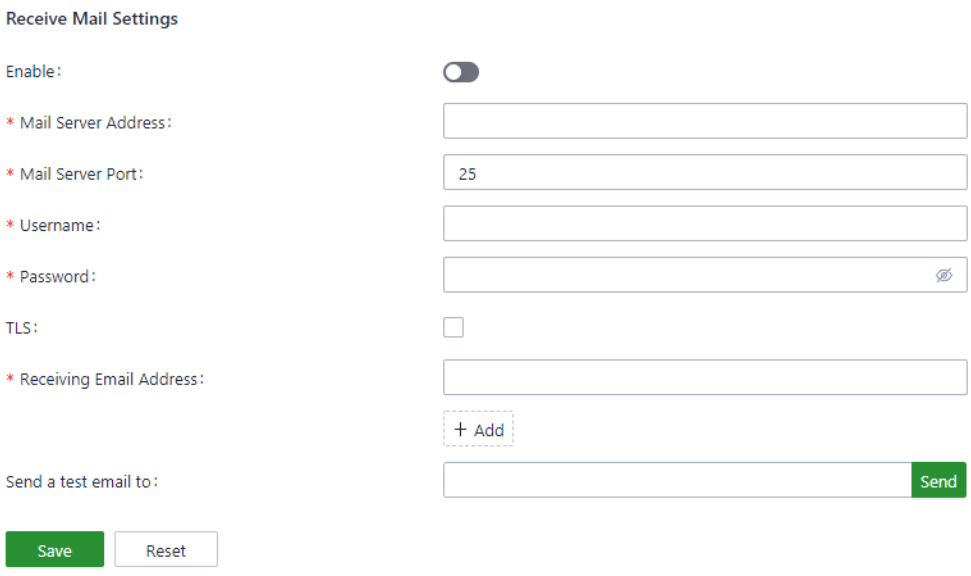
5.9.7 Device Alarms

When user needs to pay attention to some of events that may occur on the device, user can select corresponding alarm events and set an email address for alarm email. ODU will send out alarm if a selected event occurs, and record unselected events in log.

ODU supports recording and alarming following events at present:



After configure mail server address, port, username and password, ODU will send alarm email through this email. Configure Receiving Email Address and send a test email to this address to check the correctness of the configuration above.

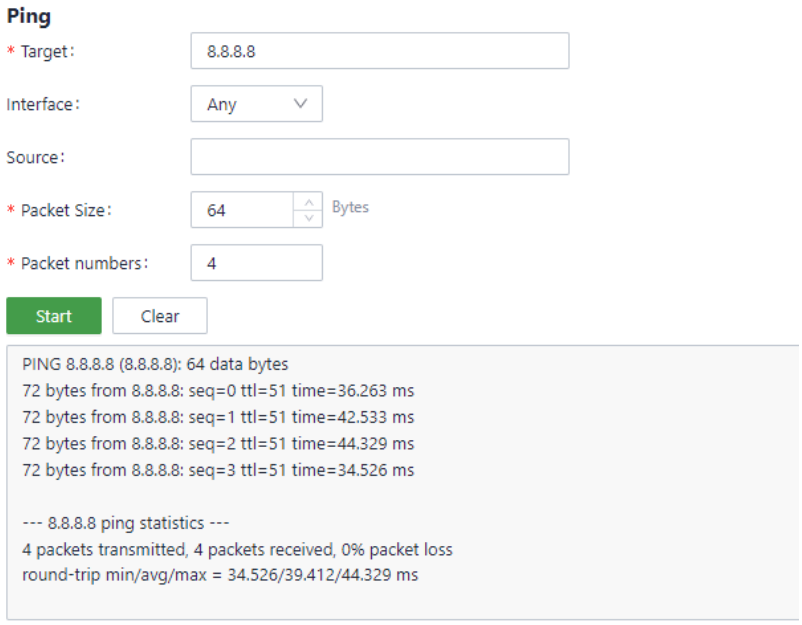


5.9.8 Tools

5.9.8.1 Ping

Use ICMP protocol to check the connectivity between source address (ODU itself if **Source** is blank) and other IP address or domain name in **Target**.

Enter IP address or domain name in **Target**, and click **Start** to start ping.



5.9.8.2 Traceroute

Enter target IP address or domain name, select interface, and click "Start" to test and trace the link situation from ODU to the target.

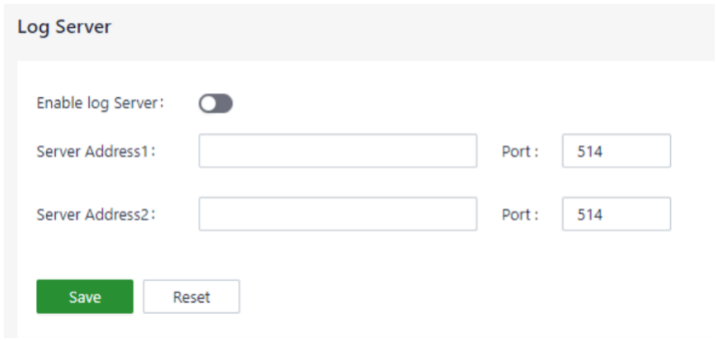
5.9.8.3 Capture

User can use this feature to catch the data forwarding through specified interfaces.

By selecting options in the Output drop-downlist, user can view information about the captured data packets or export the information to PC.

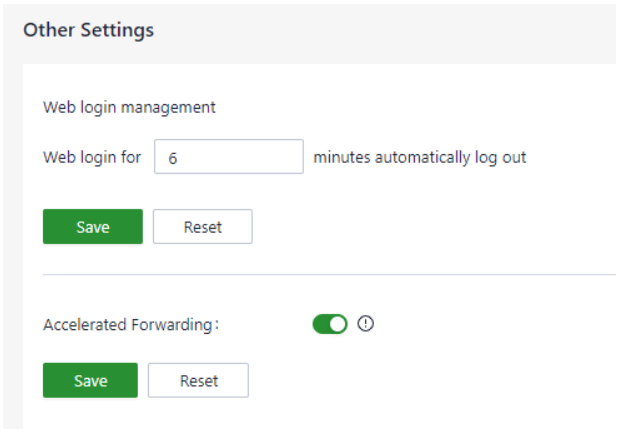
5.9.9 Log Server

Set a remote log server and ODU will upload system logs to this remote log server.



5.9.10 Other Settings

Set web login timeout, enable or disable accelerated forwarding and configure other system settings in this page.

Notes:

Cellular forwarding speed will be significantly increased after enabling Accelerated Forwarding, but other functions like traffic shaping or IPSec will not take effort.