Edge Router

User Manual

V1.0—2021.05

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.

ER800 series include several model numbers, like ER805. This user manual is applied for all the ER800 series.

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

InHand ER800 Edge Router is a new generation edge router launched by InHand Networks. With 4G wireless network and a variety of broadband services, this product can provide Internet access for all industries of IoT. The product adopts SD-WAN technology to provide uninterrupted data communication link experience for industry applications.

ER800, with its perfect security and agile wireless link services, realizes the networking of a variety of IoT devices, can help enter enterprises to realize informatization and digitization.

2 Hardware

2.1 Indicator Description

ER800 Indicator	LED Status and Definition
System	Steady off --- Power off. Blinking in blue --- System starting. Steady in blue --- System operates properly. Blinking in red --- System faults. Blinking in green --- System upgrading.
Network Status	Blinking in red --- Network connection lost. Blinking in green --- Cellular network connecting. Steady in green --- Cellular network connected. Blinking in blue --- Ethernet network connecting. Steady in blue --- Ethernet network connected.
Wi-Fi 2.4G	Steady off --- Disabled. Steady in green --- Wi-Fi 2.4G connecting. Blinking in green --- Wi-Fi 2.4G working properly.
Wi-Fi 5G	Steady off --- Disabled. Steady in blue --- Wi-Fi 2.4G connecting. Blinking in blue --- Wi-Fi 2.4G working properly.

Note: If both cellular network and ethernet network are working properly, Network Status Indicator will be in blue. And it will show the color of the connecting network if another network is not connected. If either two network are not connected, this indicator will be in red.

2.2 Restoring to Default Settings via the Reset Button

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

1. Press the RESET button within 10 seconds after power on the device.
2. System indicator will be steady on after blinking for about 1 minute.
3. Release RESET button, System indicator will blink, and press the RESET button again.
4. When System indicator blinks slowly, release the RESET button. The device has been restored to default settings and will start up normally later.

3 Default Settings

No.	Function	Default Settings
1	**Cellular**	– Dual SIM card enabled, use SIM1 by default.
2	**Wi-Fi**	– Wi-Fi 2.4G AP mode enabled, SSID: ER800- followed with 6 numbers. – Wi-Fi 5G AP mode enabled, SSID: ER800-5G- followed with 4 numbers. – Auth Method is WPA2-PSK. – Both WPA/WPA2 PSK keys in two mode are the last 8 letters in serial number.
3	**Ethernet**	– 4 LAN are enabled. – IP Address: 192.168.2.1 – Netmask: 255.255.255.0 – DHCP server enabled, IP address is 192.168.2.2 to 192.168.2.100, can provide IP address for downstream devices automatically.
4	**Management Services**	– HTTP(80) and HTTPS(443) are enabled. – Telnet is disabled. – SSH is disabled. – Only allow HTTPS to access from cellular network.
5	**Username and password**	– **adm/123456** (super administrator)

4 Login and Network Access

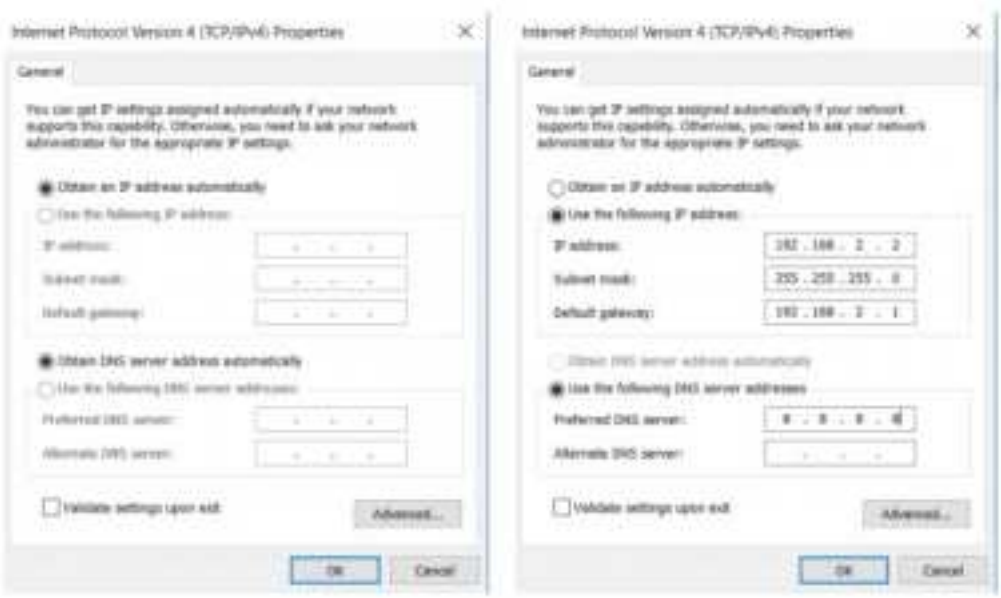
4.1 Network Access via Ethernet

Step 1: Connect power and Ethernet cable to ER800, connect WAN port to public network, and one of LAN to PC.

Step 2: Configure PC to be in the same network segment as the IP address of the router.

(1) Enable PC to obtain an IP address from DHCP automatically (recommended).

(2) Configure a fixed IP address in the same network segment as the router for PC. The IP address should be one of the address in 192.168.2.2~192.168.2.254, Subnet mask should be 255.255.255.0, and Default gateway should be 192.168.2.1. DNS server should be 8.8.8.8 or the address of ISP’ s DNS server.

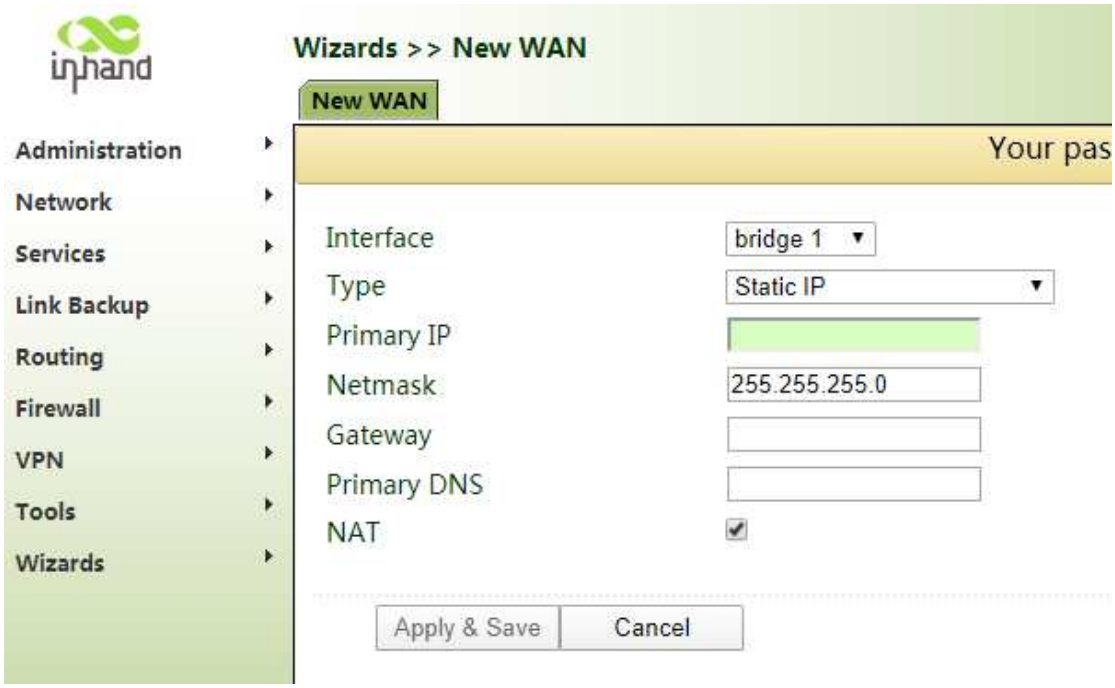


Obtain an IP address automatically/manually

Step 3: Access to the default IP address 192.168.2.1 in a browser, enter username and password(adm/123456 by default) in pop-up window and then access to router' s WEB management page. If the browser alarms the connection is not private, show advanced, and proceed to access to the address.

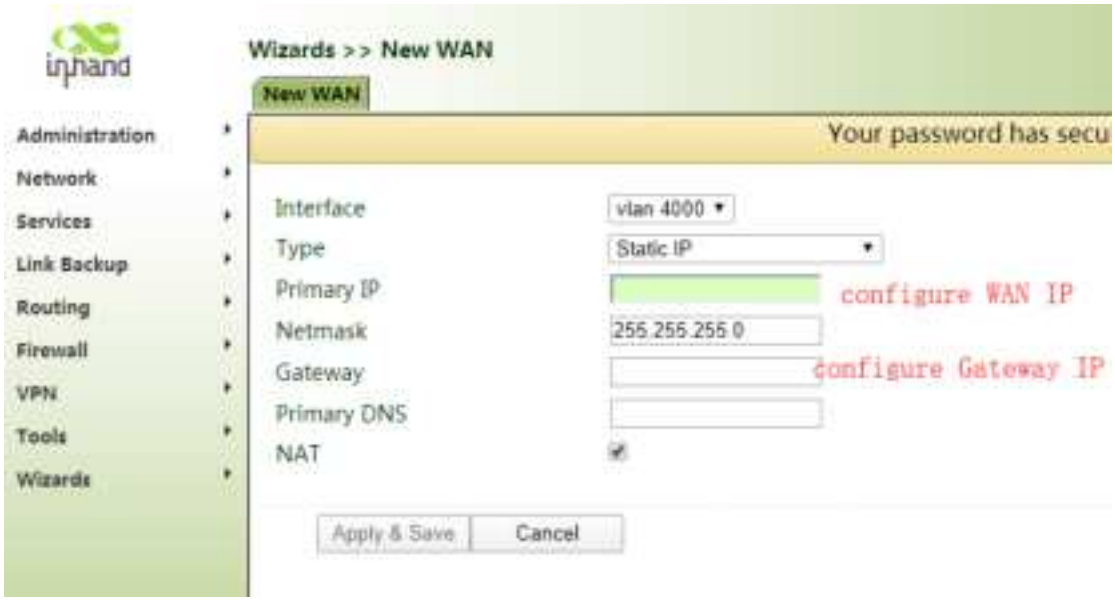
Login to device' s WEB management page

Step 4: Create a WAN port in "Wizards >> New WAN" in the left menu. Configure an IP address for WAN port and let the router connect to Internet.



There are there types to obtain IP address: Dynamic DHCP (recommend). Static IP (Click Apply & Save after configure manually) and ADLS Dialup (Click Apply & Save after configure manually).

Obtain IP address by Dynamic Address (DHCP)



Obtain IP address by Static IP

Step 5: Check the connectivity in “Tools >> Ping”.


Tools >> Ping
Ping
Administration
Network
Services
Link Backup
Routing
Firewall
VPN
Tools
Wizards
Your password has security risk.
Host
8.8.8.8
Ping
Ping Count
4
Packet Size
32
Bytes
Expert Options
PING 8.8.8.8 (8.8.8.8): 32 data bytes
40 bytes from 8.8.8.8: seq=0 ttl=105 time=267.330 ms
40 bytes from 8.8.8.8: seq=1 ttl=105 time=265.803 ms
40 bytes from 8.8.8.8: seq=2 ttl=105 time=265.234 ms
40 bytes from 8.8.8.8: seq=3 ttl=105 time=264.598 ms
--- 8.8.8.8 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 264.598/265.741/267.330 ms

4.2 Network Access via SIM card

Step 1: Insert the SIM card when device is power off. Connect 2 4G antennas to the router, and connect PC to router. Then power on.

Note:

When insert or plug out SIM card, please unplug the power cable to prevent data loss or damage the router.
ER800 supports 4 antennas (2 WLAN antenna and 2 WWAN antennas), please connect all antennas to obtain high communication quality.

Step 2: Open a browser and access to router’ s WEB management page. (refer to 4.1)

Step 3: Click “Network >> Cellular”, set profile. The device enables the cellular by default, it will connect to Internet within a few minntes. If the device cannot connect to Internet, please disable and restart dialup. (If you use a private network SIM card, you also need to configure APN parameter)

Step 4: Check the dialup status in "Status", if it shows Connected and there is IP address and other dialup parameters, the router has connected to Internet by SIM card.


Network >> Cellular
Status
Cellular
Modem
Active SIM
SIM 1
IMEI Code
353593090129021
IMSI Code
460110923582245
ICCID Code
89860318040283846651
Signal Level
(29 asu -55 dBm)
RSRP
-85 dBm
RSRQ
-15 dB
Register Status
registered
Operator
CHN-CT
Network Type
4G
LAC
9B11
Cell ID
9D54212
Network
Status
Connected
IP Address
10.65.120.18
Netmask
255.255.255.252
Gateway
10.65.120.17
DNS
61.139.2.69 218.6.200.139
MTU
1500

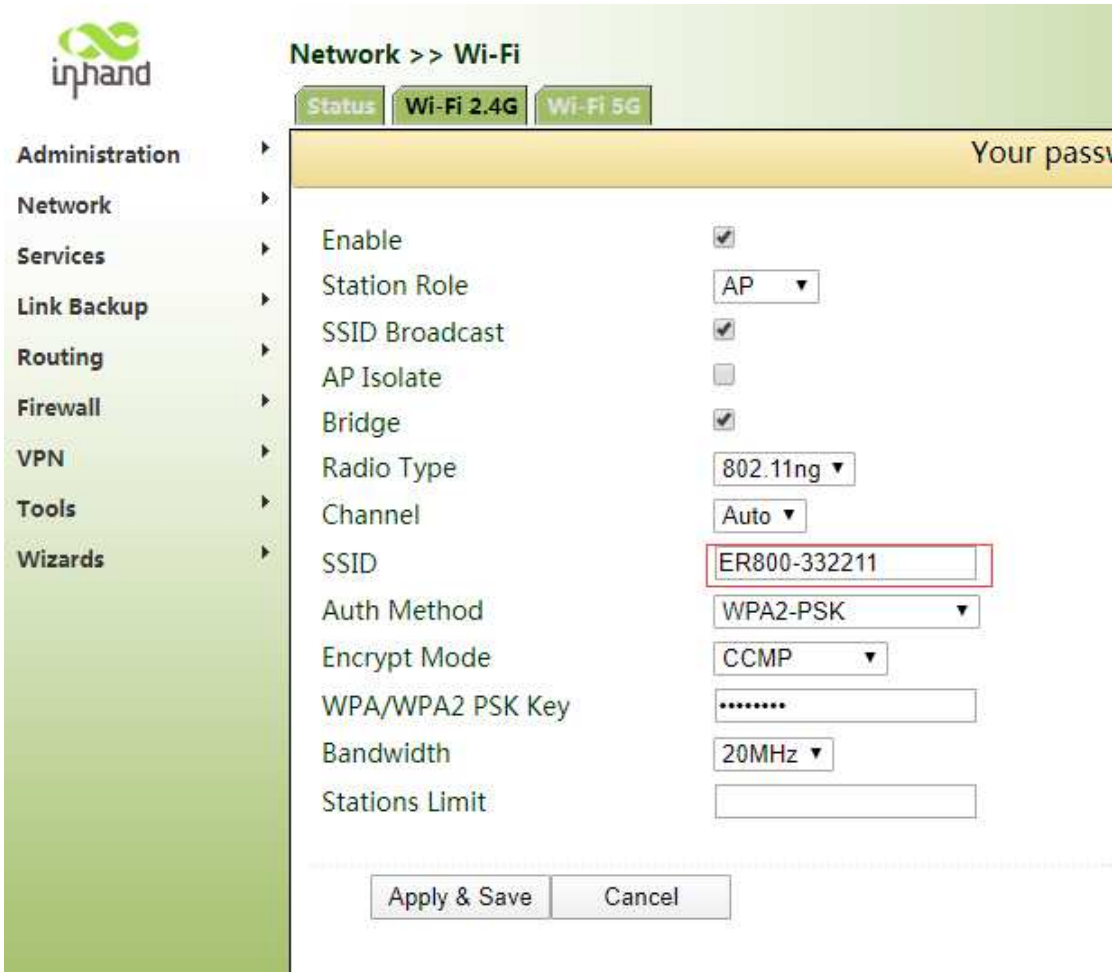
4.3 Network Access via Wi-Fi

Step 1: Connect Wi-Fi antenna, and connect PC to the device. Access to router’ s WEB management page. (refer to 4.1)

Step 2: Choose the frequent band of Wi-Fi. ER800 supports 2.4G and 5G Wi-Fi. These two Wi-Fi can work at the same time. You can check Wi-Fi status in “Network >> Wi-Fi”.

Step 3: Set Station Role in "Wi-Fi 2.4G" or "Wi-Fi 5G": AP or Client.

AP mode (default mode): ER800 acts as an accsess point to radiate wireless signals, and other terminal devices can connect this device to access the Internet. It is necessary to ensure that ER800 itself has been connected to the Internet through wired or dialup mode. AP mode supports setting SSID name and encryption authentication mode, and terminal devices will need to input password when connecting.

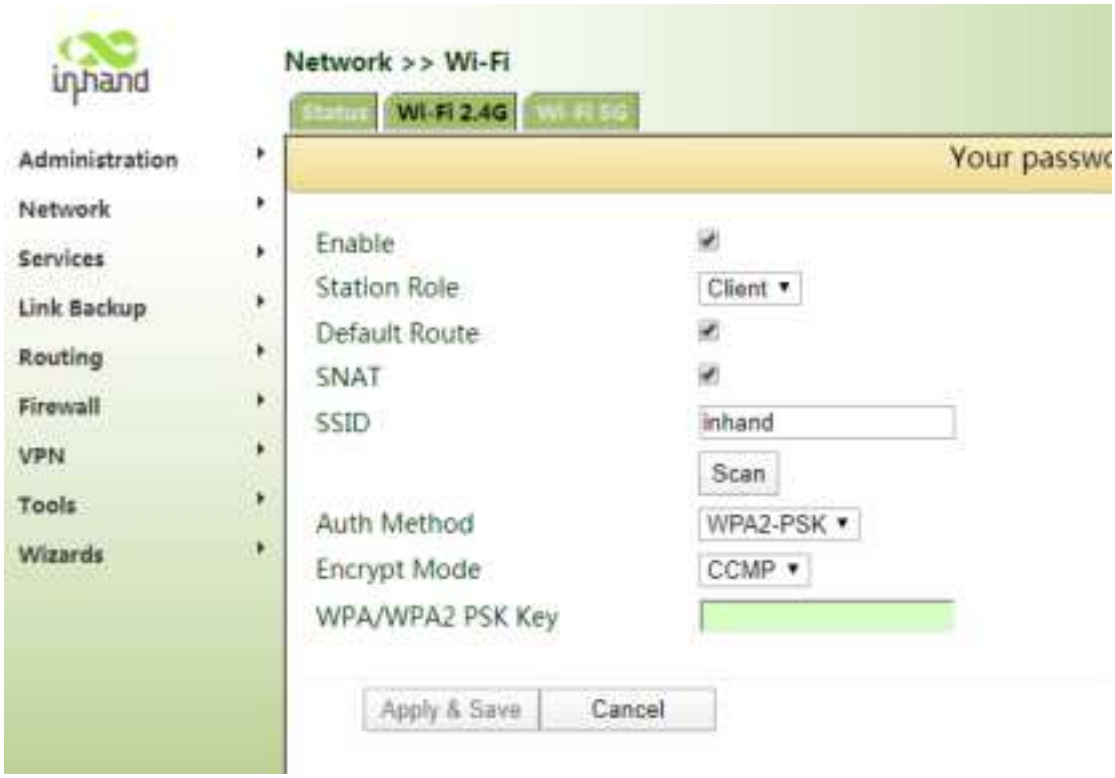


Client mode: ER800 connects to other AP Wi-Fi device to access the Internet.

1. Select Station Role to Client and save.

2. Click Scan to scan available AP, and click Connect to choose one of AP.

3. Configure Wi-Fi parameters and save. Then check the connection status in "Status".


Network >> Wi-Fi
Wi-Fi 2.4G
Administration
Network
Services
Link Backup
Routing
Firewall
VPN
Tools
Wizards
Enable
Station Role
Client
Default Route
SNAT
SSID
inhand
Scan
Auth Method
WPA2-PSK
Encrypt Mode
CCMP
WPA/WPA2 PSK Key
Apply & Save
Cancel

5 Network Management

In parameter settings, a green text box indicates a mandatory parameter, and a pure white text box indicates an optional parameter.

5.1 Network

5.1.1 Bridge port

A bridge port is intended to connect two different physical LANs over a bridge, enable storage and forwarding across LANs at the link layer.

Method for modifying the IP address of a bridge port and bridge members:

1. Click "Network >> Bridge" and select "Bridge". Choose a bridge and click Modify.

2. Modify the IP address of the bridge port or bridge members. Among the bridge members, dot11radio and dot11radio2 are Wi-Fi 2.4G and Wi-Fi 5G port respectively.

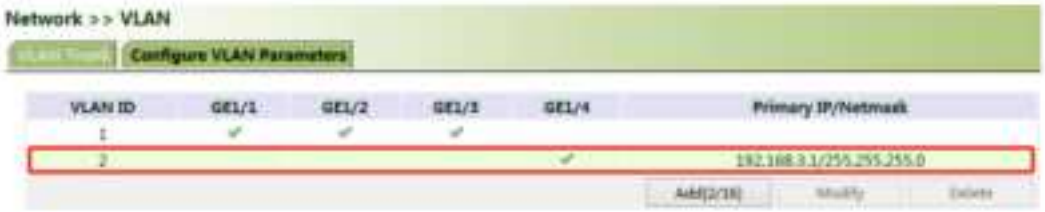
5.1.2 VLAN Port

A virtual LAN (VLAN) comprises a group of logical devices and users. These devices and users are not limited by physical locations, but can be organized base on functions, departments, applications, and other factors. They communicate with each other as if they are in the same network segment, which contributes to the name of VLAN.

Method for adding a port of VLAN2:

1. Click "Network >> VLAN >> Configure VLAN parameters >> Add". Set the virtual IP address of the port of VLAN 2 and select the member port of VLAN 2 as required. Click Apply & Save.

2. Return to the VLAN list. The port of VLAN 2 has been added successfully.



Currently, VLAN ports of the device support two link types: access and trunk. An access port belongs to only one VLAN and is generally connected to a computer. A trunk port can be used for multiple VLANs and can receive messages from or send messages to multiple VLANs. It can be connected to a switch or a user's computer. You can select the link type as required on the "VLAN Trunk" page.

5.1.3 ADSL Dialup (PPPoE)

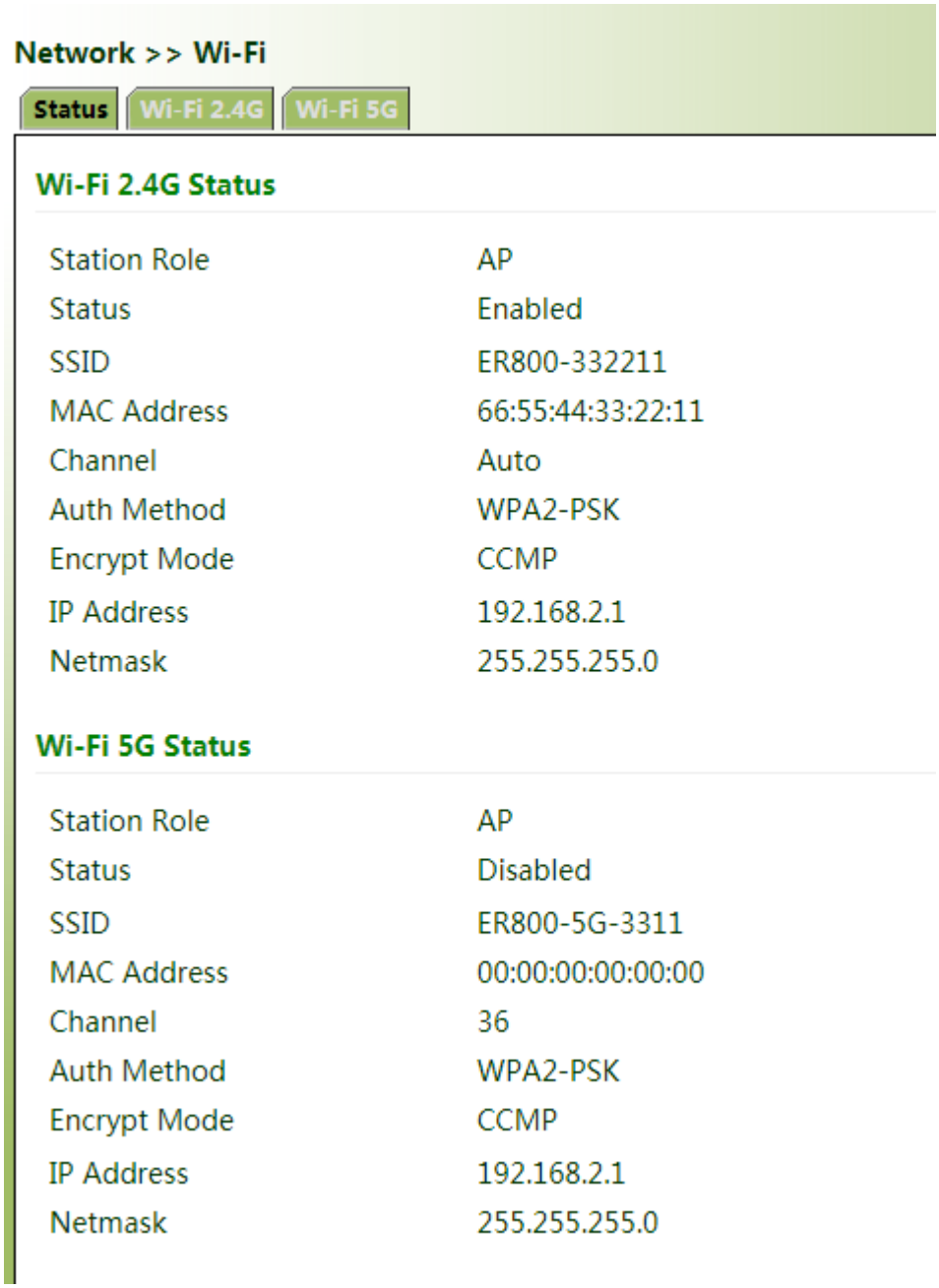
Method for connecting ER800 to a PPPoE server:

1. Click "Network > > ADSL Dialup (PPPoE)", select the interface for connecting to the PPPoE server in the "Dial Pool" bar, and click Add.

2. Enter the user name, password, and pool ID of the PPPoE server in the "PPPoE List" bar. The pool ID must be the same as that in the "Dial Pool" bar. Click Add, and then click Apply & Save.

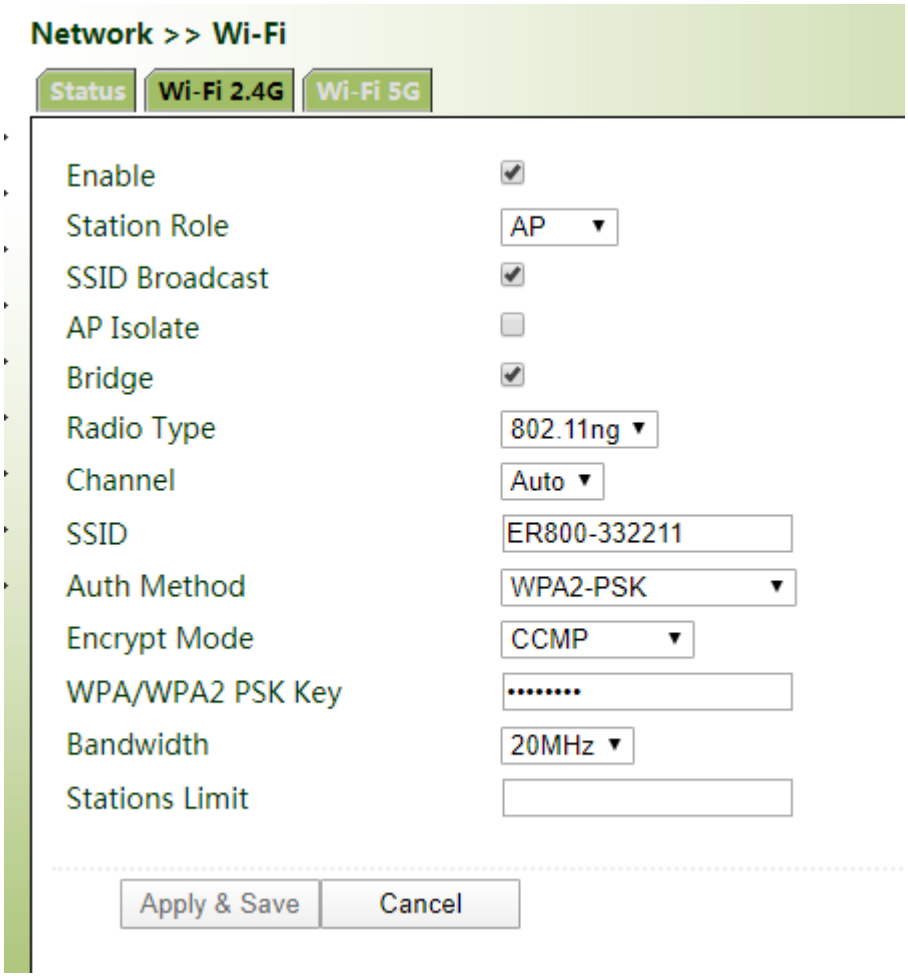
5.1.4 Wi-Fi

ER800 can be used as an AP or a client. When it is used as an AP, other users can access the Internet through the router via Wi-Fi. When it is used as a client, the router connects to an AP for Internet access. The Status bar shows router’s current Wi-Fi connection status.



Method for providing network access service for wireless terminals when the router is used as an AP:

Click "Wi-Fi >> Wi-Fi 2.4 or Wi-Fi 5G" and select "AP" for "Station Role". Enter the SSID, authentication method, and key consistent with those of the wireless AP. Click Apply & Save.



Method for connecting to an AP for Internet access when ER800 is used as a client:

Select "Client", enter Wi-Fi SSID and key, and click Apply & Save. Or select "Client", click Apply & Save, then click Scan to choose the AP you want.

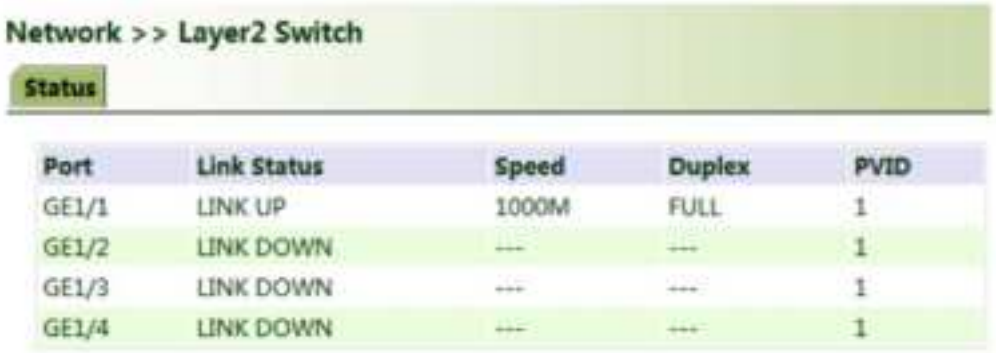
5.1.5 Loopback Port

Method for adding Multi-IP Settings:

Click "Network >> Loopback >> Multi-IP Settings", configure any IP address for the router, click Add, and then click Apply & Save.

5.1.6 Layer 2 Switch

Check the network connection status of GE1 to GE4. LINK UP indicates that the network is connected. LINK DOWN indicates that the network is disconnected.



5.2 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.

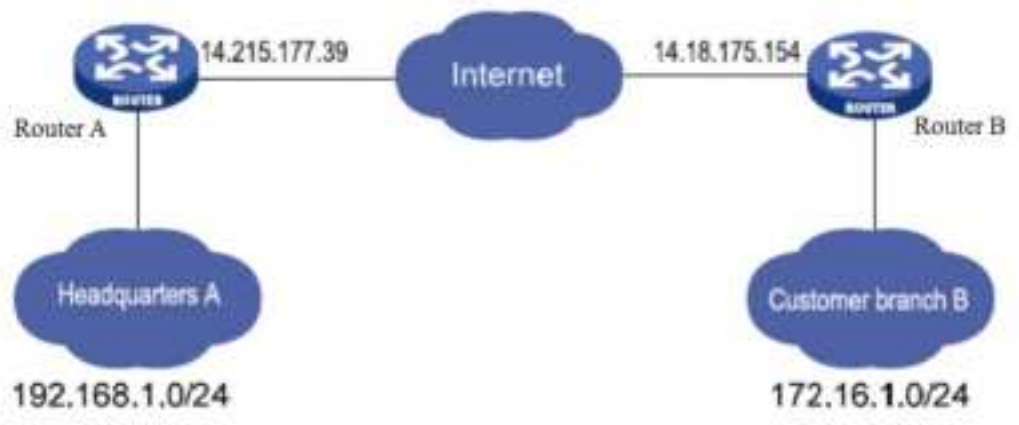
A common VPN application scenario: An employee on a business trip wants to access to the enterprise's intranet. The employee connects to enterprise's VPN server and then accesses to enterprise's intranet through the VPN server. Communication data between the VPN server and the client is encrypted and can be regarded as being transmitted on a dedicated data network. This ensures data security.

5.2.1 IPsec

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. This reduces the risk of leakage and eavesdropping, ensures the integrity and confidentiality of data, and the security of service transmission for users.

Scenario: Data is transmitted between the subnet (192.168.1.0/24) of headquarters A and the subnet (172.16.1.0/24) of customer branch B through router A and router B. The transmission channels between router A and router B

are encrypted over IPsec, which protects the security of data transmission between headquarters A and customer branch B.



Method for encrypting the transmission channels between router A and router B over IPcec:

Parameter settings:

Router A	
Set IKEv1/v2 Parameters	
ID	Custom
Encryption algorithm	AES128
Hash algorithm	SHA1
Diffie-Hellman key exchange	Group2
Lifecycle	86400
IPsec Policy	

Router B	
Set IKEv1/v2 Parameters	
ID	Custom
Encryption algorithm	Same as that of Router A
Hash algorithm	
Diffie-Hellman key exchange	
Lifecycle	
IPsec Policy	

Name	Custom
Encapsulation	ESP
Encryption algorithm	AES128
Authentication method	SHA1
IPsec mode	Tunnel mode
IPsec tunnel configuration	
Peer address	Address where router B establiches the IPsec service
Interface	Interface for establishing the IPsec service
IKE version	IKE version used
Authentication method	Shared key
Local subnet	IP address of the subnet of router A
Peer subnet	IP address of the subnet of router B

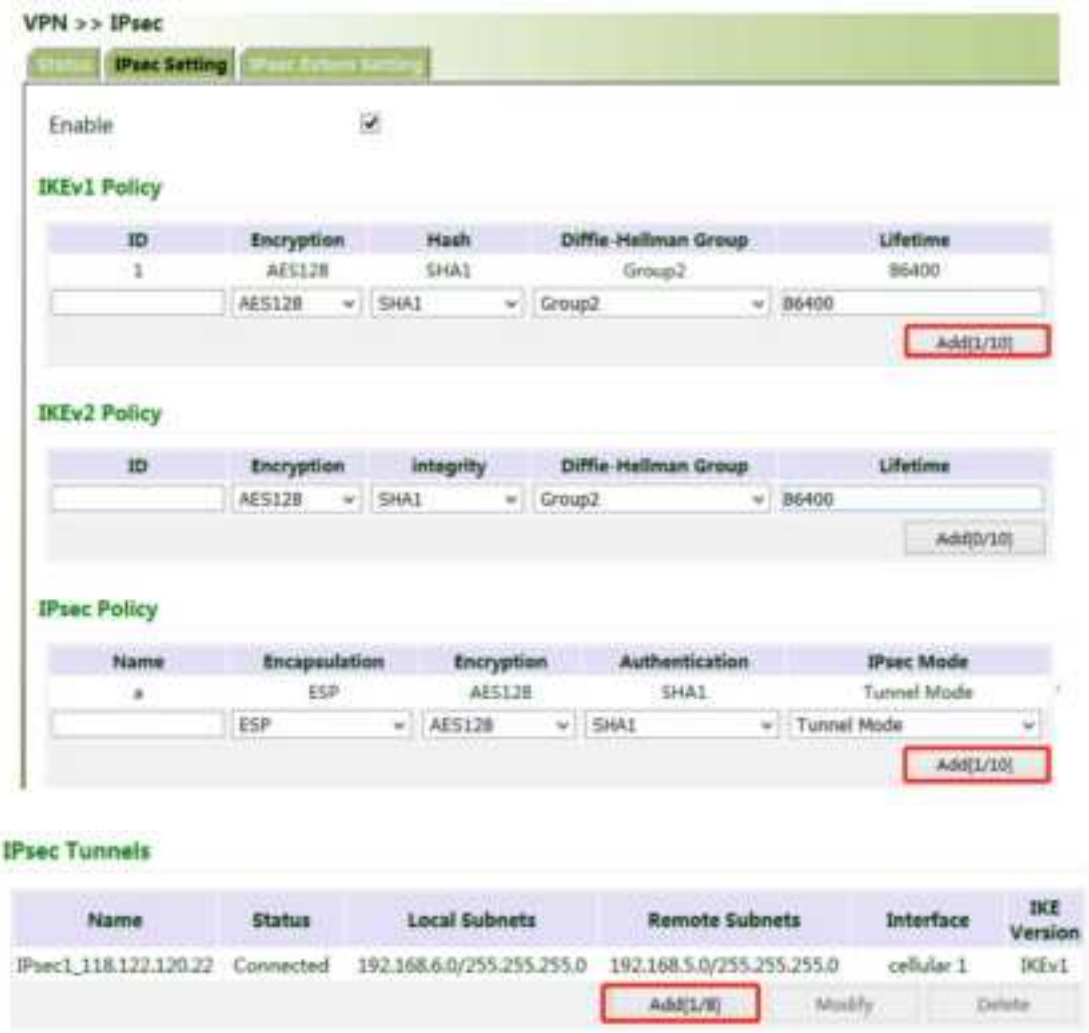
Name	Custom
Encapsulation	Same as that of Router A
Encryption algorithm	
Authentication method	
IPsec mode	
IPsec tunnel configuration	
Peer address	Address where router A establishes the IPsec service
Interface	Interface for establishing the IPsec service
IKE version	Same as that of router A
Authentication method	
Local subnet	IP address of the subnet of router B
Peer subnet	IP address of the subnet of router A

Detailed configuration steps:

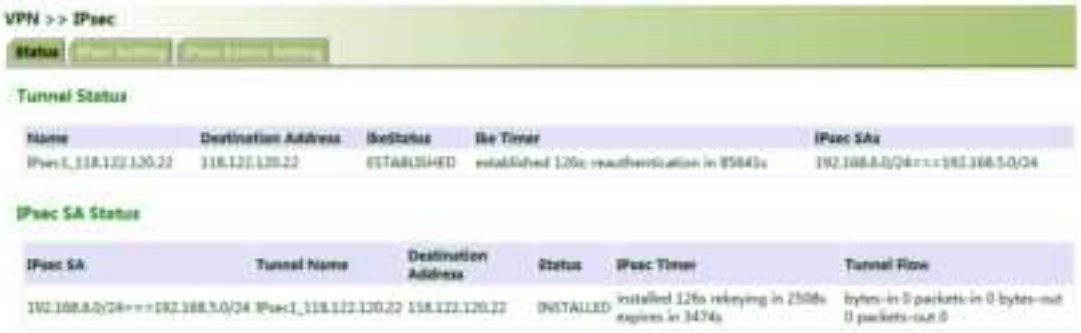
1. Configure router A and router B.

(1) Add IKE and IPsec policies, and click Apply & Save.

(2) Add IPsec tunnels and click Apply & Save.



2. Access the IPsec Status page. The IPsec VPN is established successfully if the page is shown as below.



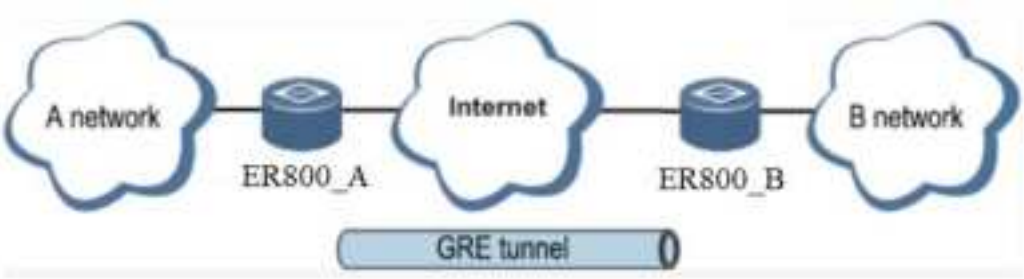
Note:

The IPsec profile does not need to be configured when establish an IPsec VPN, but needs to be configured when establish a DM VPN.

5.2.2 GRE

Generic Routing Encapsulation (GRE) protocol can be used to encapsulate datagrams of some network layer protocols, so that these encapsulated datagrams can be transmitted on the IPv4 network.

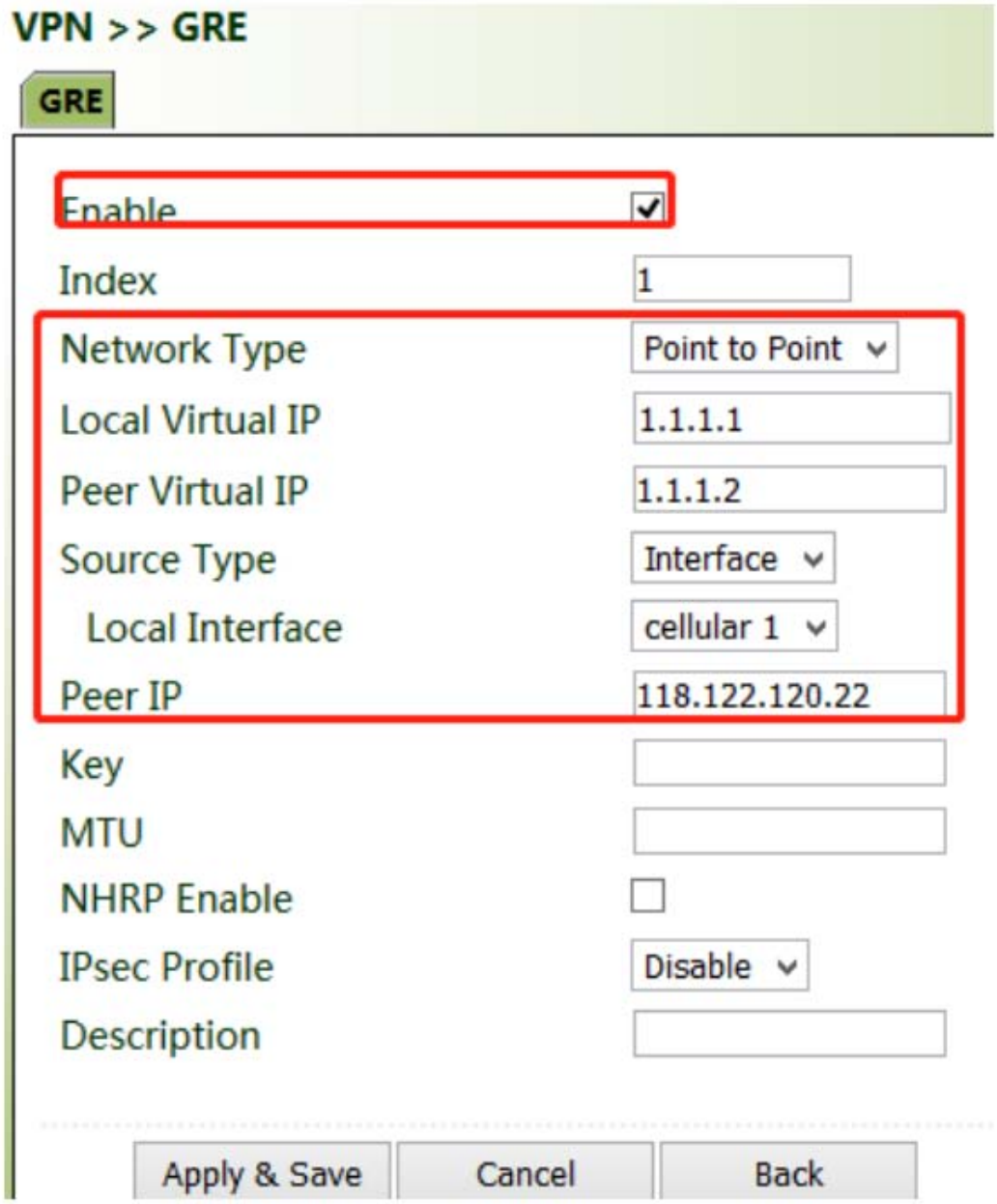
Scenario: GRE is enabled for ER800_A and ER800_B through the public network.



Method for enabling GRE for transmission channels of ER800_A and ER800_B:

1. Click "VPN >> GRE" and then click Add.

2. Set "Index" as required. Select "Point to Point" or "Subnet" for "Network Type". Set "Local Virtual IP" and "Peer Virtual IP", ensuring that they are on the same network segment. Enter the source and peer IP addresses or interfaces and the key. Click Apply & Save.



3. Set ER800_B in the same way. The virtual and peer IP addresses of ER800_B must correspond to those in ER800_A, and the key must be the same as that of ER800_A.

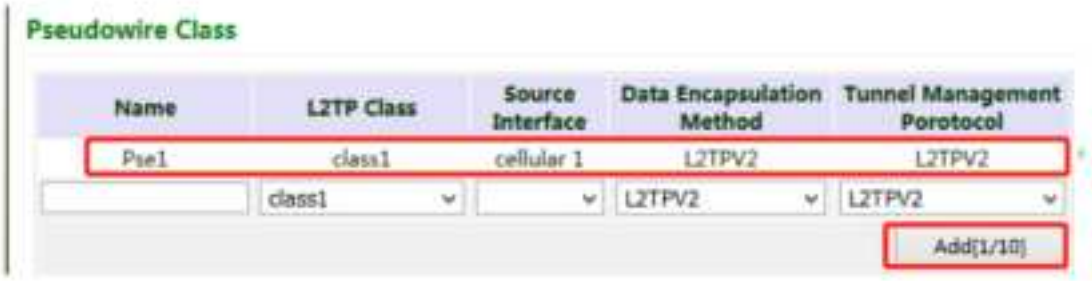
5.2.3 L2TP

The Layer 2 Tunneling Protocol (L2TP) is an industrial-standard Internet tunneling protocol used to encrypt network data streams.

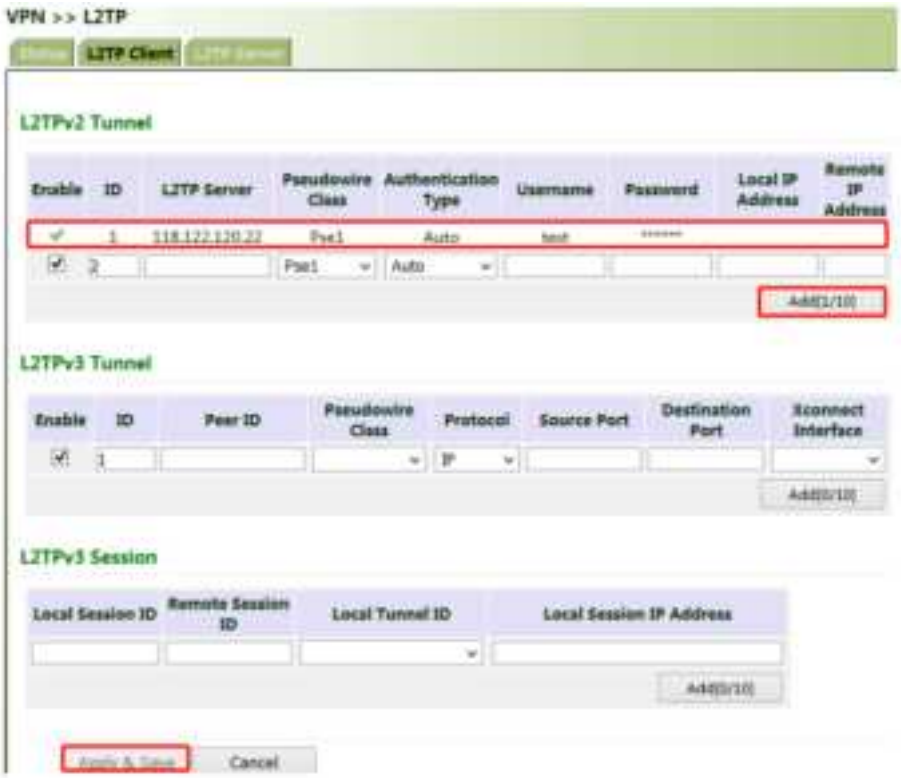
Method for setting a L2TP client in ER800:

1. Click "VPN >> L2TP >> L2TP Client >> L2TP Class", enter a name of an L2TP class, and click Add.

2. Configure the pseudowire class: Enter a name of any pseudowire class. "L2TP Class" is the same as that on the "L2TP Class" page. Set "Source Interface" to the interface connecting to the server. Select L2TPV2 for "Protocol" and click Add.



3. Set L2TPV2 tunnel parameters: Enter the server's domain name or IP address for "L2TP Server". "Pseudowire Class" is the same as that on the "Pseudowire Class" page. Enter the user name and password created on the server. Set other parameters as required. Click Apply & Save.



4. After gateway A and gateway B are configured, access the L2TP status page to view the L2TP connection status.

5.2.4 OpenVPN

Based on the application-layer VPN of the OpenSSL library, OpenVPN supports multiple authentication methods such as the certificate, key, and user name/password. Compared with traditional VPN, it is simpler and easier to use.

Authentication methods:

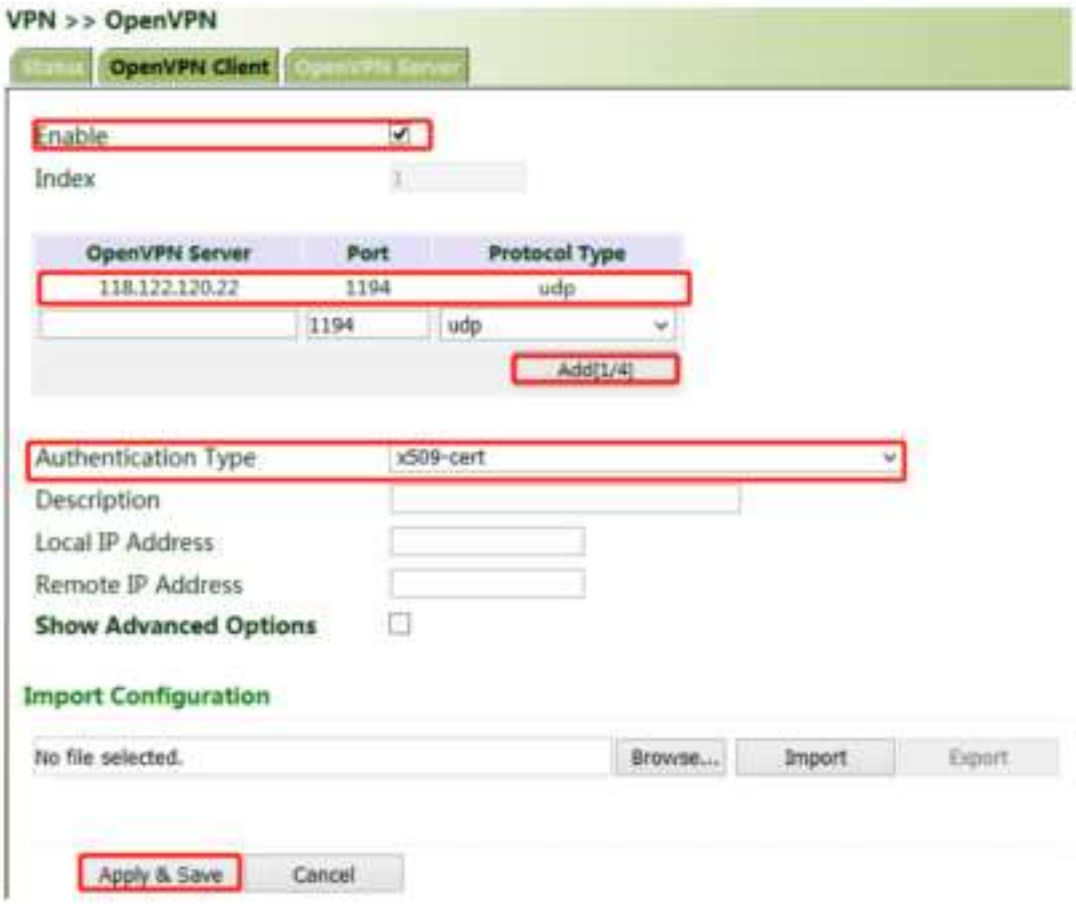
Authentication methods	Operation on the web page
None	No authentication is required.
User	Enter the user name and password created on the

name/password	OpenVPN server, import the CA certificate, public key, and private key for authentication in "VPN >> Certificate Management".
Pre-shared key	Enter the pre-shared key created on the OpenVPN server.
Digital certificate	Import the CA certificate, public key, and private key for authentication in "VPN >> Certificate Management".
Digital certificate/user name/password	Enter the user name and password created on the OpenVPN server, import the CA certificate, public key, and private key for authentication in "VPN >> Certificate Management".
Digital certificate/TLS authentication	Enter the pre-shared key created on the OpenVPN server, import the CA certificate, public key, and private key for authentication in "VPN >> Certificate Management".
Digital certificate/TLS authentication/user name/password	Enter the pre-shared key, user name and password created on the OpenVPN server, import the CA certificate, public key, and private key for authentication in "VPN >> Certificate Management".

Method for setting OpenVPN client on ER800 when connecting to an OpenVPN server:

OpenVPN can be configured manually, or by importing config file. In the following example, the authentication type is a digital certificate.

1. Set the OpenVPN parameters for the gateway as shown in the figure below, ensuring that the network parameters at both ends of the tunnel are consistent. Click Apply & Save.



2. Select digital certificate in "Authentication Type", import the CA certificate, public key, and private key in "VPN >> Certificate Management".

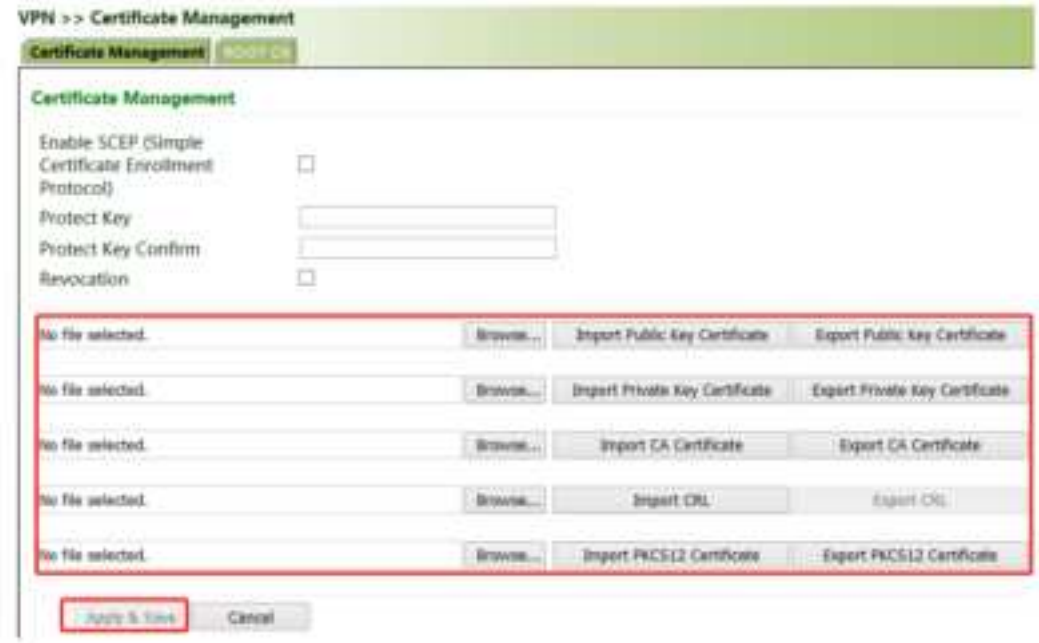
3. Click Apply & Save. Return to the "Status" page and view the tunnel status.

5.2.5 Certificate Management

Certificates used for IPsec and OpenVPN services can be imported or exported in this page.

Method for importing certificates:

Click "VPN >> Certificate Management >> Browse", select the certificate obtained from the certificate server, click Import XX Certificate, and then click Apply & Save.



If there is no local certificate available, check "Enable SCEP (Simple Certificate Enrollment Protocol)" to apply for a certificate online.

Method for applying a certificate for the router online:

1. Click "VPN >> Certificate Management". Check "Enable SCEP (Simple Certificate Enrollment Protocol)" and "Force to re-enroll". Enter the certificate protection key and confirm it. Enter the URL of the certificate server, certificate name, and FQDN. Click Apply & Save.

2. After the server issues the certificate, check the application status. If the application status is "Completion", certificate application succeeds.

5.3 Service

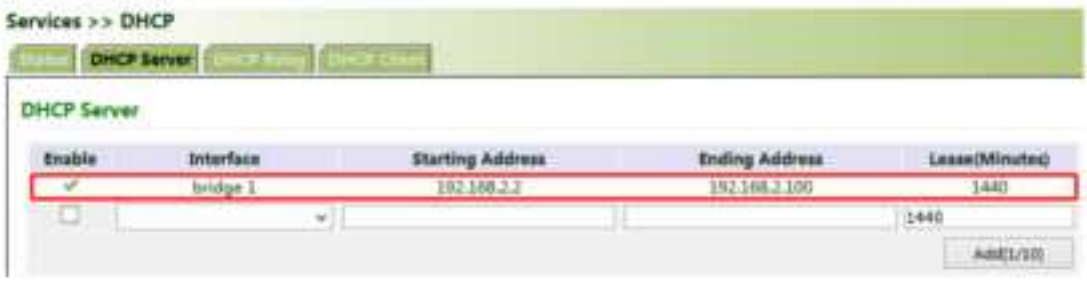
5.3.1 DHCP (Automatic IP Address Allocation)

DHCP uses client/server communication mode. The client submits a configuration application to the server, and the server returns the IP address assigned to the client, in this way, DHCP realizes the dynamic configuration of the IP address.

DHCP server and DHCP forwarding function are mutually exclusive.

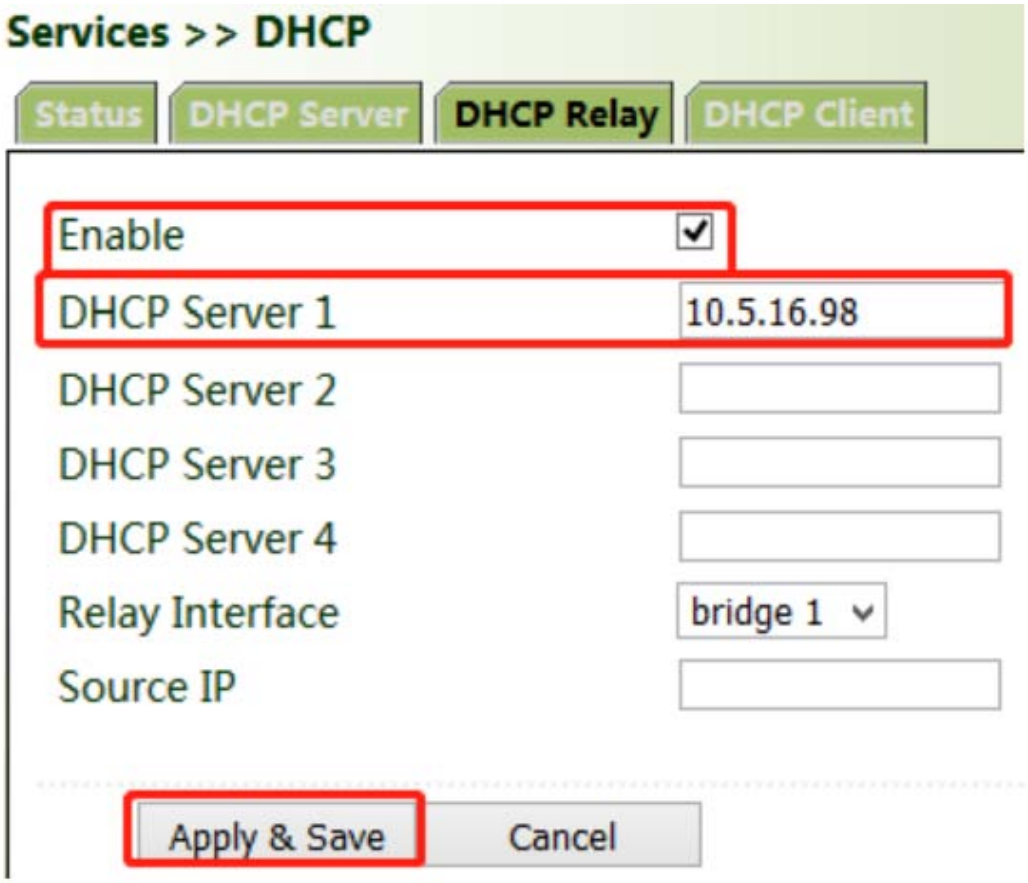
Method for setting DHCP server in ER800:

Click "Services >> DHCP". In the "DHCP Server" bar, check "Enable", select an interface, set the start and end IP addresses, click Add, and then click Apply & Save.



Method for enabling DHCP forwarding in ER800:

Click "Services >> DHCP >> DHCP Relay", check "Enable", enter the server address, select the gateway interface, and click Apply & Save.



5.3.2 DNS

Domain name service (DNS) is a distributed network directory service mainly used for mutual conversion between a domain name and an IP address.

Method for enabling the DNS server in ER800:

Click "Services >> DNS >> DNS Server", enter the address of the DNS server, and click Apply & Save.

Method for enabling DNS forwarding in ER800:

As a DNS agent, the router forwards DNS requests and response messages between DNS client and DNS server, and provides domain name resolution for client.

IF the router enables DHCP service, DNS forwarding will be enabled by default and cannot be disabled.

Click "Services >> DNS >> DNS Relay", check "Enable DNS Relay", set the mapping between the domain name and the IP address, click Add, and then click Apply & Save. After the settings are completed, when a DNS client on the LAN requests a host domain name in the list, the DNS agent server will return the corresponding IP address to the client.

5.3.3 DDNS

Dynamic domain name server (DDNS) maps the dynamic IP address of the router to a fixed DNS. Each time a user connects to the Internet, the client program will transmits the dynamic IP address of the host to the server program on the server host. The server program provides the DDNS service and realizes dynamic domain name resolution. In this way, you can access the Internet by entering the domain name, even if the IP address is changed.

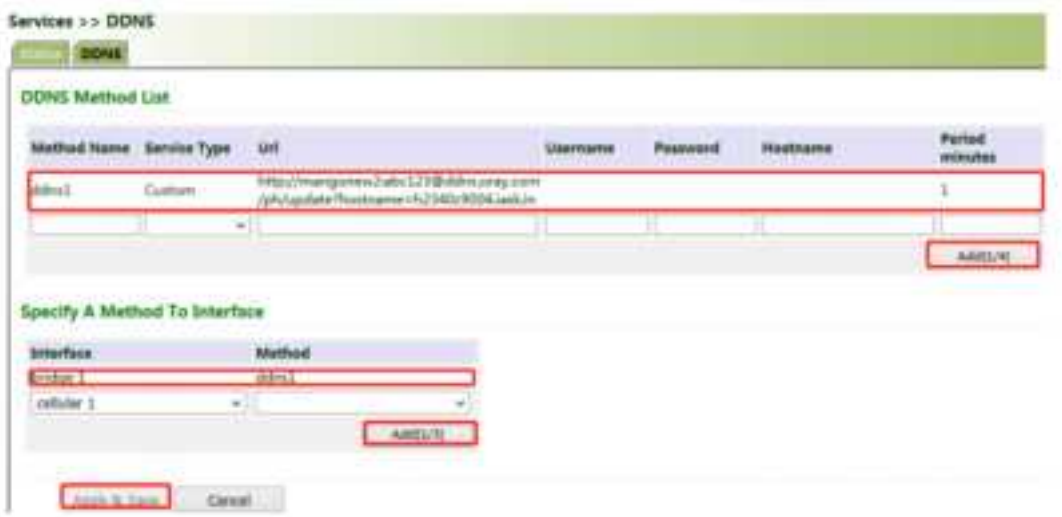
Method for enabling the DDNS in ER800:

1. If use Custom service, set "Method Name" as required, select "Custom" for "Service Type", and enter the DDNS expression "http://user name:password@ddns.oray.com/ph/update?hostname=host name" of the server for "Url". This expression is only for reference. The real URL is provided by the service provider (usually available on the official website of the service provider). Click Add.

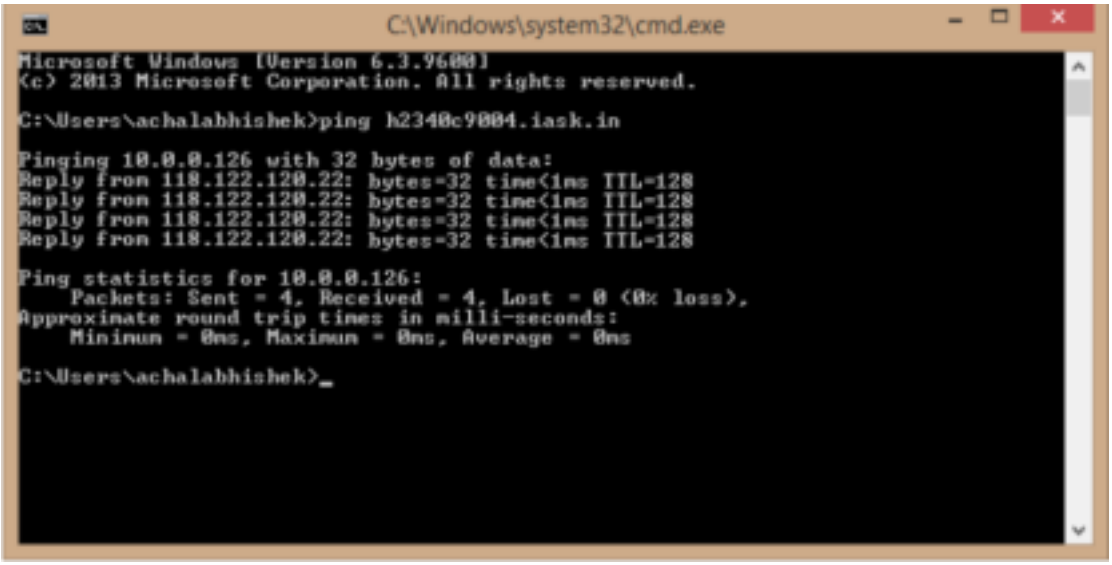
If use a common domain name server, set "Method Name" and "Service Type" as required, enter the user name, password, and host name obtained from the server, and click Add.

If select as "Disable", the DDNS service will not enable.

2. Select the rotuer interface, enter the name of the DDNS method, click Add, and then click Apply & Save.



3. Wait several minutes after the DDNS settings are applied and saved. Then ping the host name (domain name) of the domain name server to check the stauts of application to the DDNS service.



5.3.4 SMS

The router can restart or manual dialup via SMS messages, and some of routers can send alarm information to the SMS whitelist.

Method for controlling ER800 to restart and manual dialup via SMS:

When the cellular selects in SMS activation mode, click "Services >> SMS" and check "Enable". In the "SMS Access Control" bar, set "ID" as required, select "permit" for "Action", enter the phone number, and click Apply & Save. When you activate the dialup port via SMS, after the configuration is completed, you can restart the router by sending **reboot** to router’ s SIM card number from the mobile phone in whitelist, or send **cellular 1 ppp up/down** to make the router redial or stop dialup.

5.3.5 QoS

Quality of Service (QoS) is a network security mechanism that allows a network to provide better services for designated network communication by using various basic technologies. It is a technology for solving network delays and blocking problem.

Method for setting the maximum egress bandwidth in ER800 via QoS:

Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the egress maximum bandwidth, click Add, and then click Apply & Save.

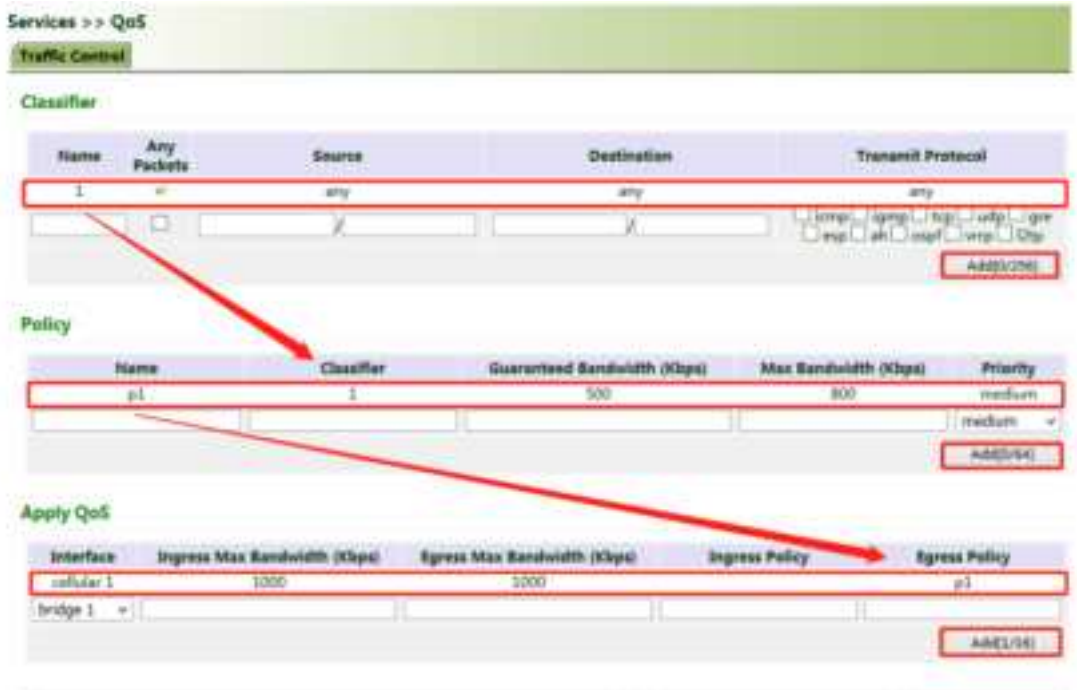
Method for applying the ingress and egress policies in ER800 via QoS:

1. Add a network link classifier. Click "QoS >> Traffic Control >> Classifier", check "Any Packets", set the source and destination addresses of the link, select

transmit protocols for QoS control, and click Add.

2. Set transmission policies. Click "QoS >> Traffic Control >> Policy", enter a custom policy name for "Name", enter the classifier name for "Classifier", set the guaranteed bandwidth, maximum bandwidth, and policy priority, and click Add.

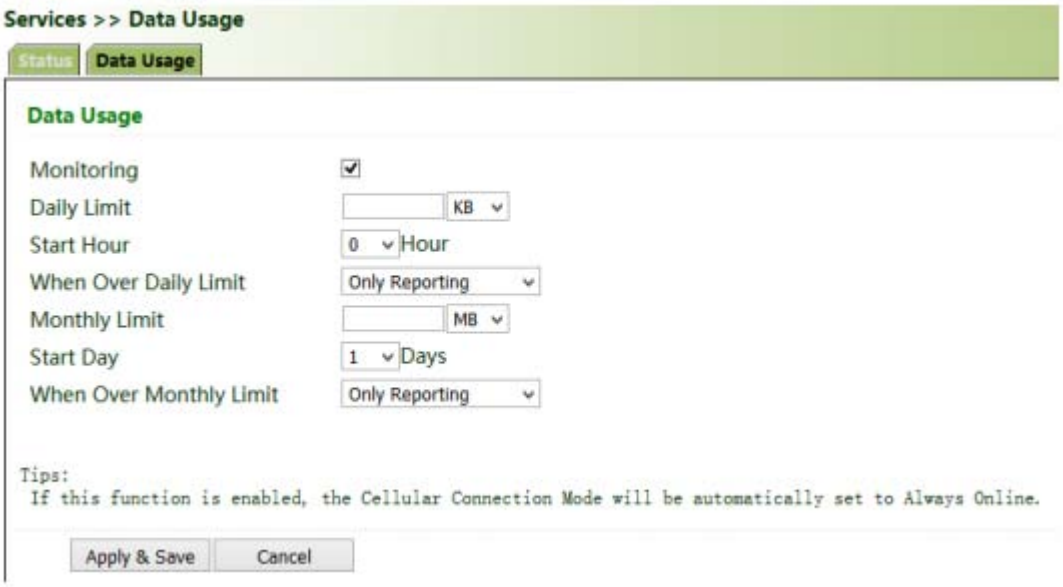
3. Click "QoS >> Traffic Control >> Apply QoS", select the gateway interface, enter the policy name for "Ingress Policy" and "Egress Policy", click Add, and then click Apply & Save.



5.3.6 Traffic Control

Method for enabling traffic control in ER800:

Click "Services >> Traffic Control", enable traffic control, set traffic control parameters, and click Apply & Save. After the settings are completed, the system generates an alarm, stops forwarding, or disables the interface when the traffic exceeds the limit according to the settings on this page.


Services >> Data Usage
Status
Data Usage
Data Usage
Monitoring
Daily Limit
KB
Start Hour
0
Hour
When Over Daily Limit
Only Reporting
Monthly Limit
MB
Start Day
1
Days
When Over Monthly Limit
Only Reporting
Tips:
If this function is enabled, the Cellular Connection Mode will be automatically set to Always Online.
Apply & Save
Cancel

5.4 Firewall

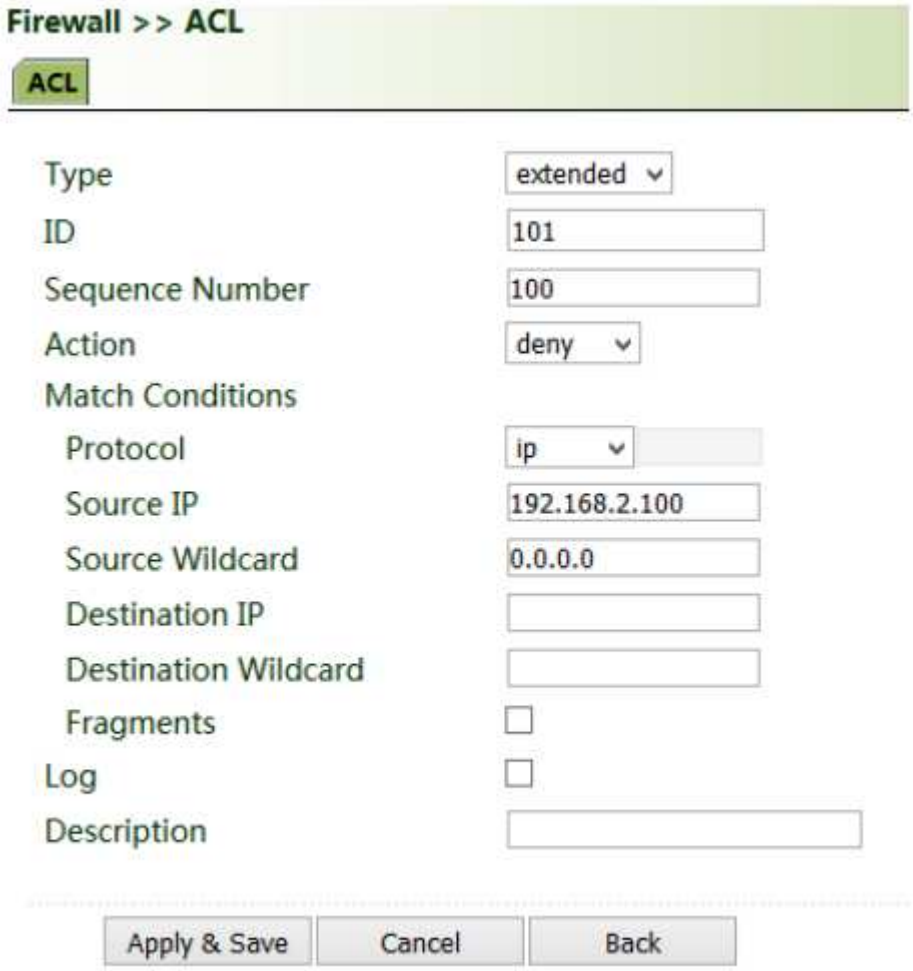
5.4.1 ACL

Access control list (ACL) is an access control technology based on packet filtering. It can pass or discard the packets on the interface based on preset conditions.

Scenario: All devices in the LAN (bridge 1) can access the Internet, except the device with IP address 192.168.2.100.

Method for setting in ER800:

1. Click "Firewall >> ACL >> Add". Enter the ID and sequence number. A smaller sequence number indicates a higher priority. Select "deny" for "Action". Set "Source IP" to "192.168.2.100" and "Source Wildcard" to "0.0.0.0". Leave "Destination IP" empty, which indicates 0.0.0.0/0, that is, all IP addresses. Click Apply & Save.



2. Return to the ACL page, add the rule with the ID you set before to the management rule of bridge 1, and click Add. Then click Apply & Save.

5.4.2 NAT

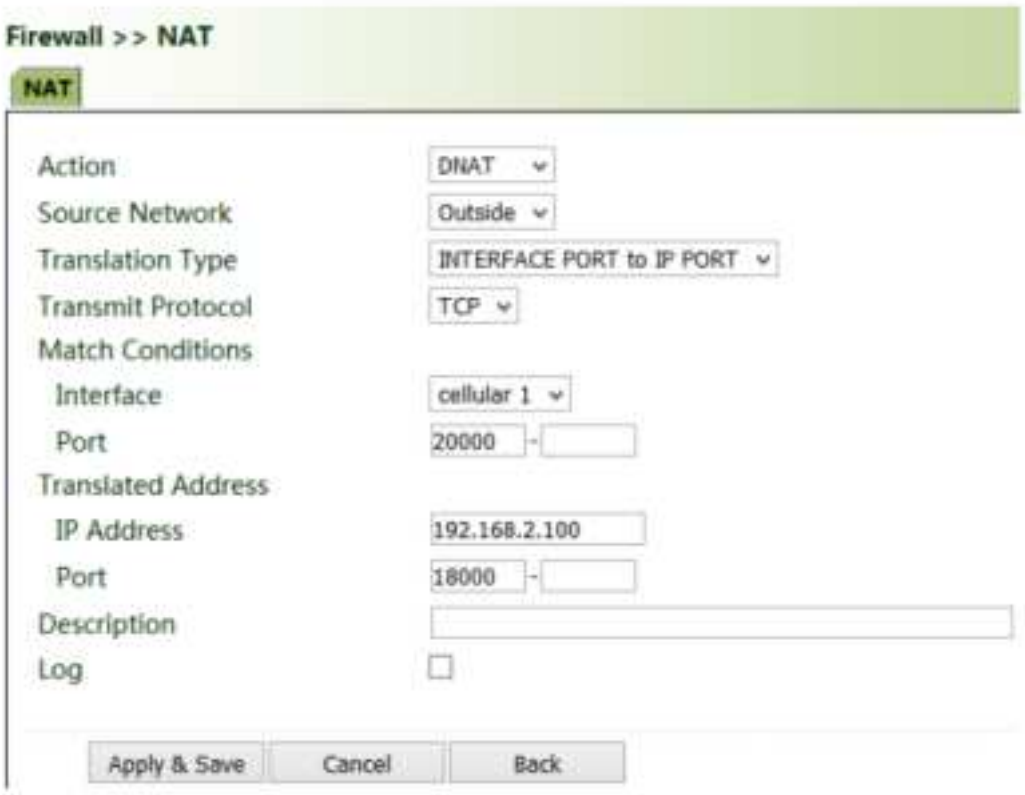
Network address translation (NAT) can be used when some hosts on a private network have been assigned with local IP addresses (that is, private IP addresses used only on the private network), but expect to communicate with hosts on the Internet (without encryption).

Scenario: A user expects to access a camera on the LAN of the device through the public network. The camera’ s address is 192.168.2.100, and the opens port 18000 to provide video service.

1. Click "Firewall >> NAT", and select "DNAT" for "Action", and "Outside" for "Source Network". Select "IP PORT to IP PORT" or "INTERFACE PORT to IP PORT" for "Translation Type". The public IP address obtained through cellular is not fixed, so "INTERFACE PORT to IP PORT" is more convenient. Select "TCP" for "Transmit Protocol" because video service is transmitted over TCP. Select "cellular 1" (dialup interface for the cellular network) for "Interface" and set

"Port" to "20000". Set "IP Address" and "Port" under "Translated Address" to "192.168.200" and "18000" respectively. Click Apply & Save.

The router will redirect the TCP service destined for port 20000 of the cellular 1 interface to the internal IP address 192.168.2.100 and port 18000.

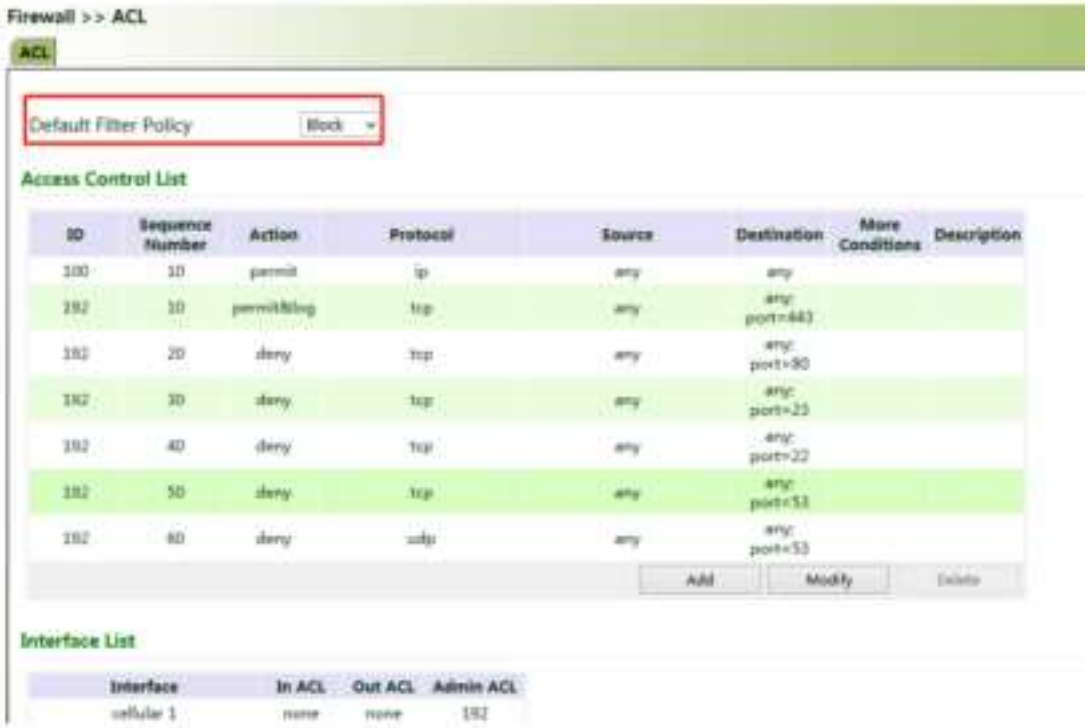


5.4.3 MAC-IP Binding

After MAC-IP binding, downstream devices can access the public network through the router only by using the IP address bound to the MAC address of the device.

Method for binding the device’s MAC address and IP address:

1. Click "Firewall >> ACL" and select "Block" for "Default Filter Policy".



2. Click "Firewall >> MAC-IP Binding", check "Enable", enter the MAC address and IP address of the connected device, click Add, and click Apply & Save.

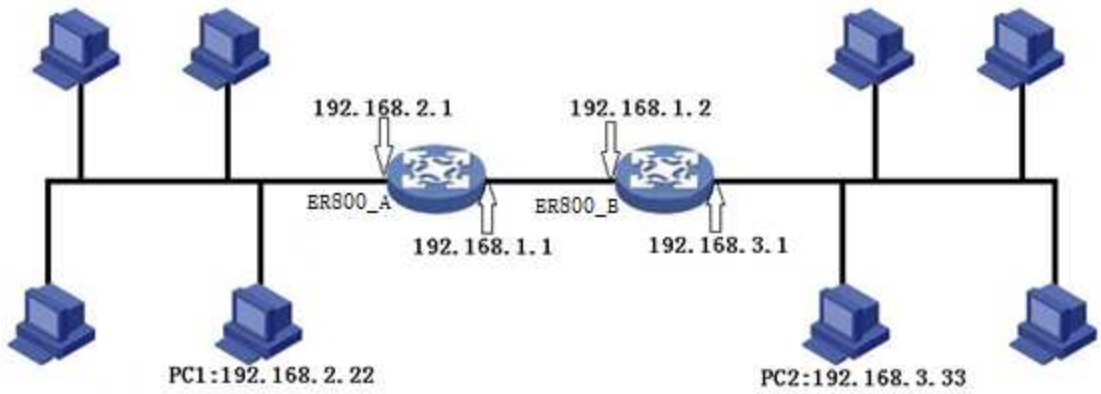
5.5 Routing

5.5.1 Static Routing

Set the destination network, subnet mask, and interface or gateway as required.

5.5.2 Dynamic Routing

Scenario: Enable dynamic routing between two LANs for mutual communication between them. The topology is shown below.

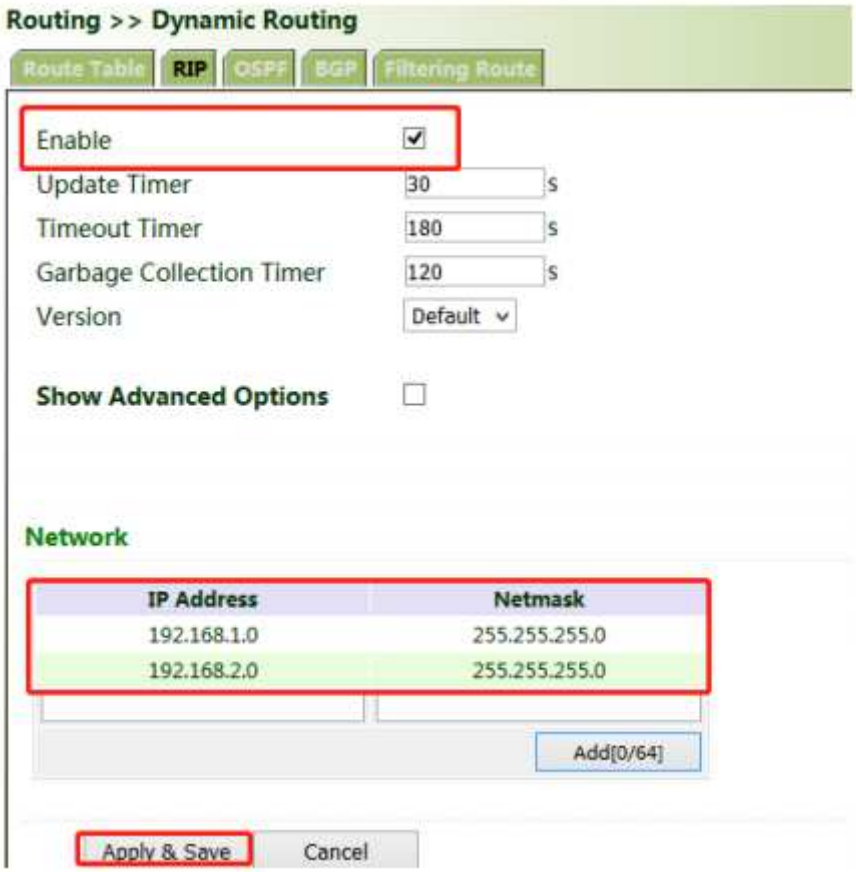


5.5.2.1 RIP

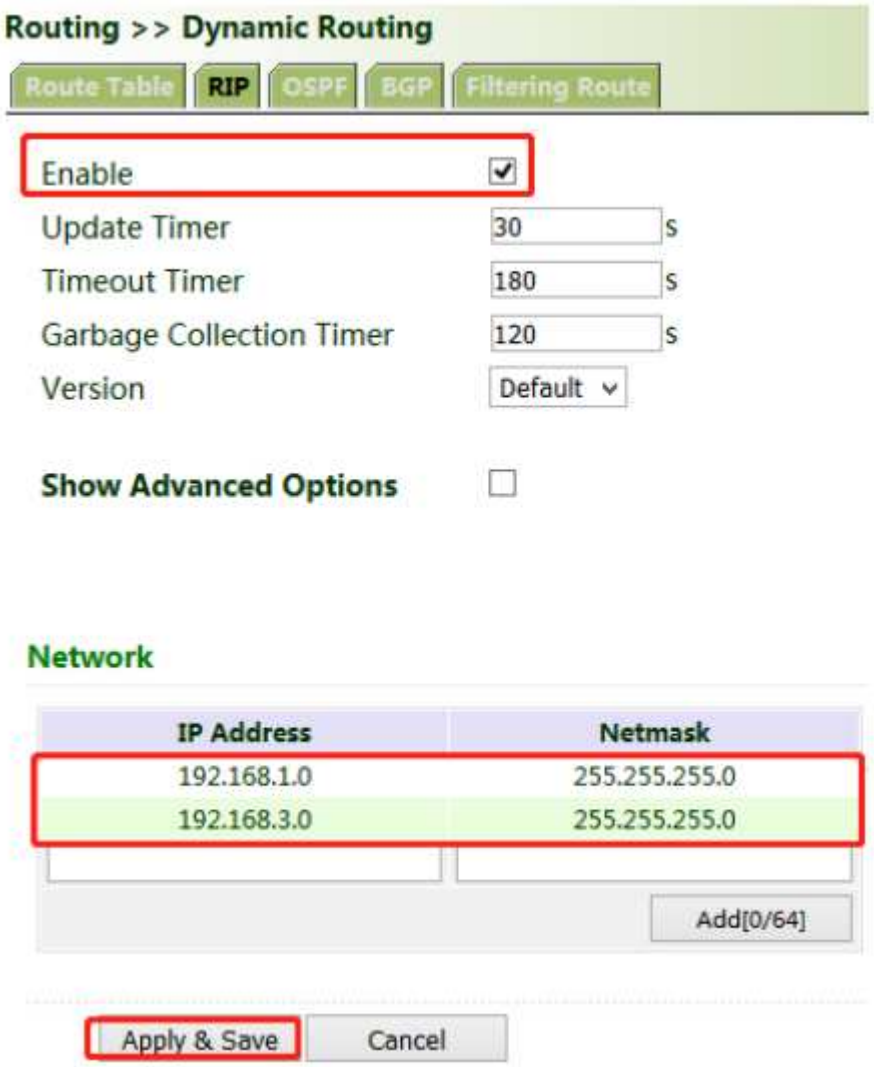
Routing Information Protocol (RIP) is a simple internal dynamic routing protocol mainly used on small-scale networks.

Method for enabling dynamic routing between ER800_A and ER800_B over RIP in the scenarie:

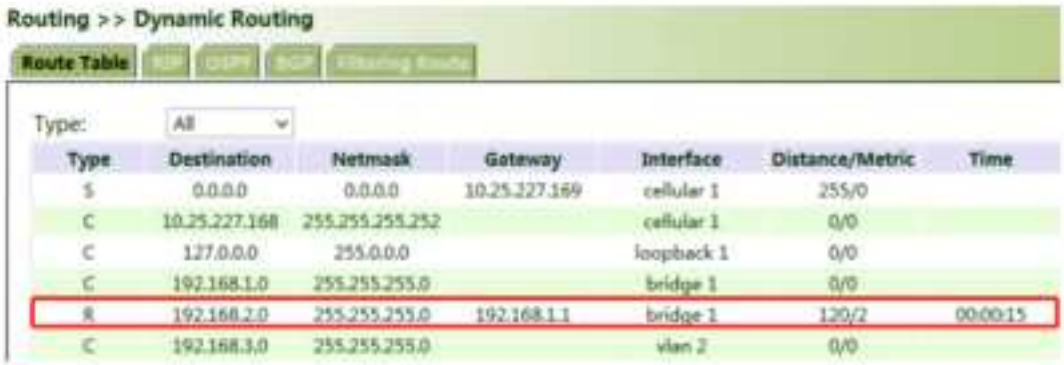
1. Configure ER800_A. Click "Routing >> Dynamic Routing >> RIP", check "Enable", and configure ER800_A in the "Network" bar to announce the routing entry of ER800_A.



2. Configure ER800_B.



3. After the configuration is completed, check whether PC 1 can communicate to PC 2. If yes, the dynamic route has been added successfully.



5.5.2.2 OSPF

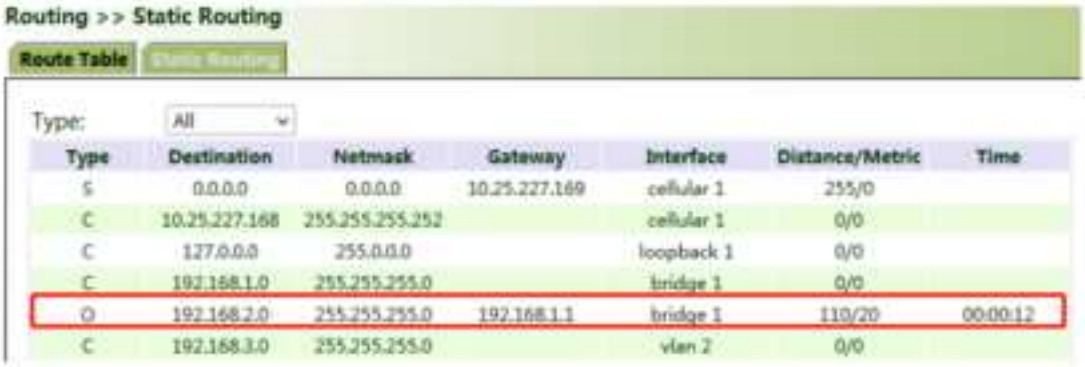
Open Shortest Path First (OSPF) protocol is a link-status-based internal gateway protocol mainly used in large-scale networks.

Method for enabling dynamic routing between ER800_A and ER800_B over OSPF in the scenarie:

1. Configure ER800_A. Click "Routing >> Dynamic Routing >> OSPF", check "Enable", enter a valid IP address for "Router ID", and configure ER800_A in the "Network" bar to announce the routing entry of ER800_A.

2. Configure ER800_B.

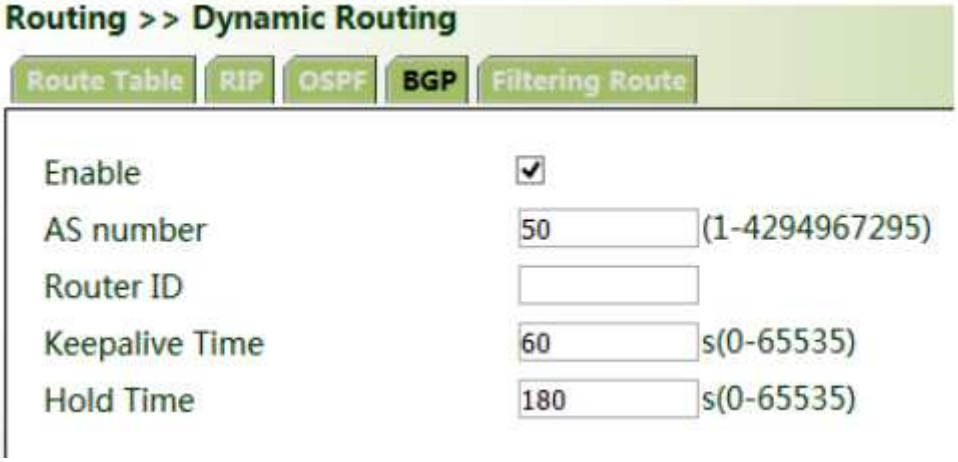
3. After the configuration is completed, check whether PC 1 can communicate to PC 2. If yes, the dynamic route is added successfully.



5.5.2.3 BGP

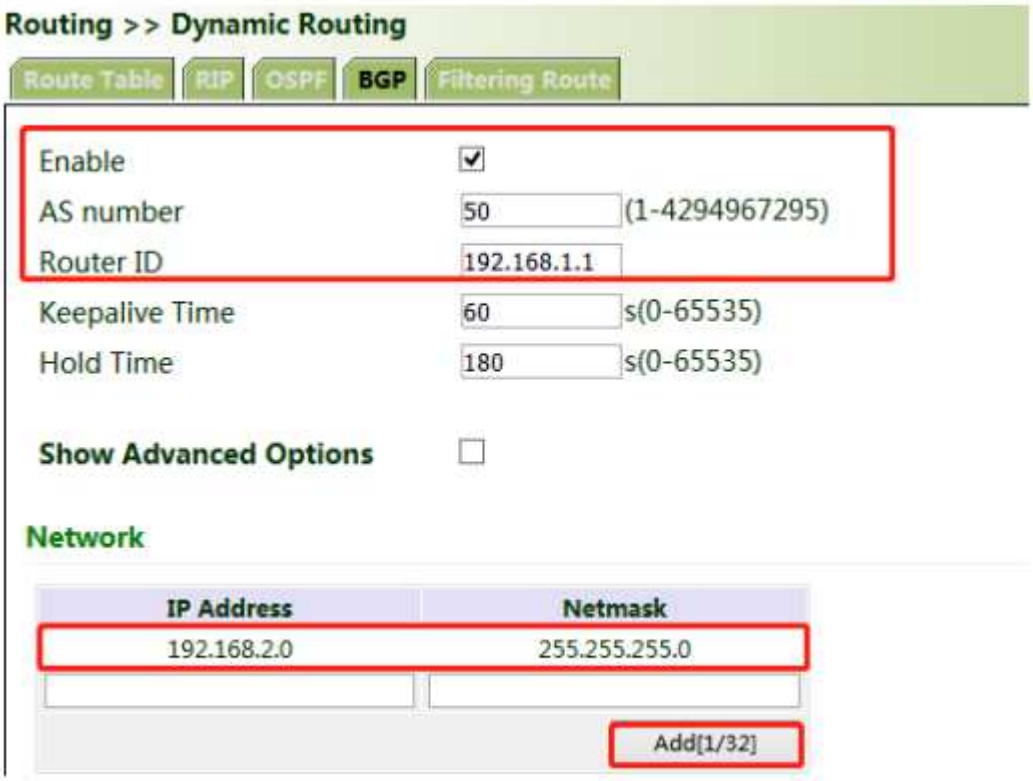
Method for enabling dynamic routing between ER800_A and ER800_B over BGP in the scenarie:

1. Configure ER800_A. Click "Routing >> Dynamic Routing >> BGP", check "Enable", and set "AS number" as required.



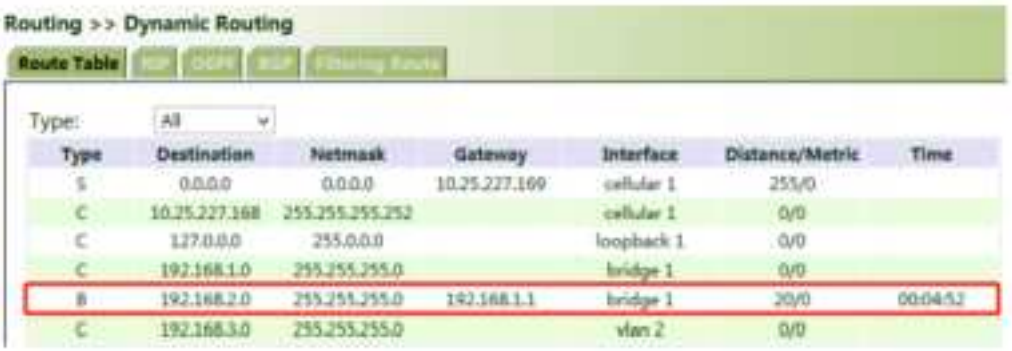
2. In the "Neighbor" bar, click Add, enter ER800_B’ s IP address 192.168.1.2, set "AS number" as required, and click Apply & Save.

3. Enter a valid IP address for "Router ID", configure ER800_A in the "Network" bar, and click Add to announce the routing entry of ER800_A. Then click Apply & Save.



4. Configure ER800_B. The parameters are the same as or corresponding to those of in ER800_A.

5. After the configuration is completed, check whether PC 1 can communicate to PC 2. If yes, the dynamic route is added successfully.


Routing >> Dynamic Routing
Route Table
Type: All
Type Destination Netmask Gateway Interface Distance/Metric Time
S 0.0.0.0 0.0.0.0 10.25.227.169 cellular 1 255/0
C 10.25.227.168 255.255.255.252 cellular 1 0/0
C 127.0.0.0 255.0.0.0 loopback 1 0/0
C 192.168.1.0 255.255.255.0 bridge 1 0/0
R 192.168.2.0 255.255.255.0 192.168.1.1 bridge 1 20/0 00:04:52
C 192.168.3.0 255.255.255.0 vlan 2 0/0

5.6 Link Backup

5.6.1 SLA

Service level agreement (SLA) is used to detect whether the router is disconnected with ISP.

Method for adding an SLA entry in ER800:

Click "Link Backup >> SLA >> Add", enter the detected IP address for "Destination Address", set other parameters as required, click Add, and then click Apply & Save.

Timeout (ms) indicates the duration for determining a detection failure.

Consecutive indicates the number of detection failures resulting in a link failure.

5.6.2 Track

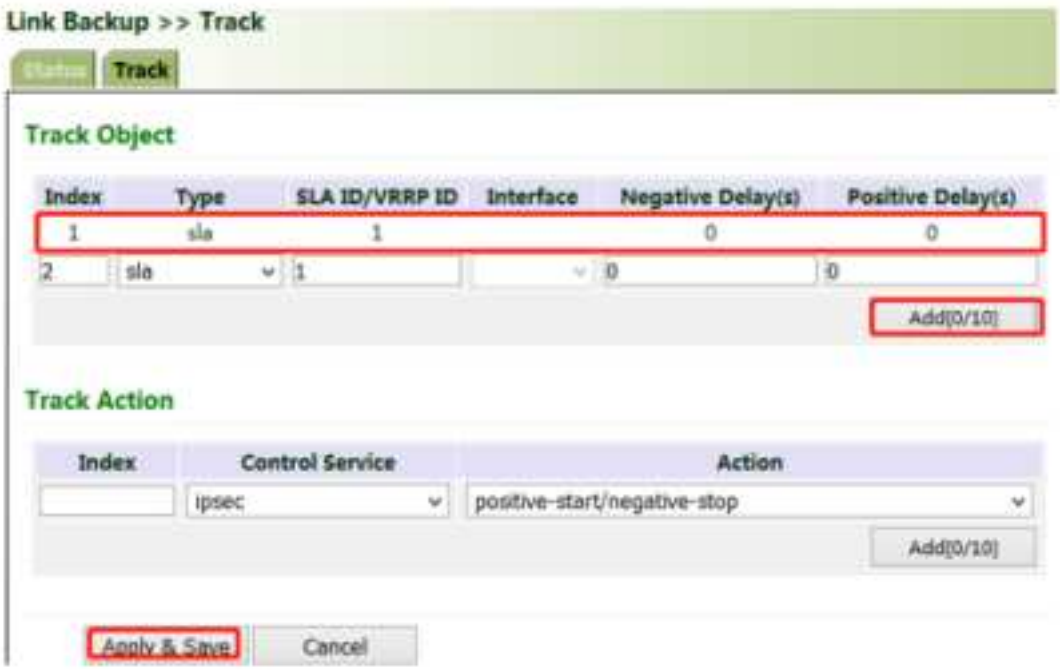
At present, track module can be used with following application modules: VRRP, static routing, and interface backup. If detection succeeds, the corresponding track entry will be in Positive state. If detection fails, the corresponding track entry will be in Negative state.

Method for adding a track entry in ER800:

Click "Link Backup >> Track >> Track", set "Index" as required, select "SLA", "Interface", or "VRRP" for "Type", set "SLA/VRRP ID" based on the ID in the SLA list, set "Negative Delay (s)" and "Positive Delay (s)" as required, click Add, and then click Apply & Save.

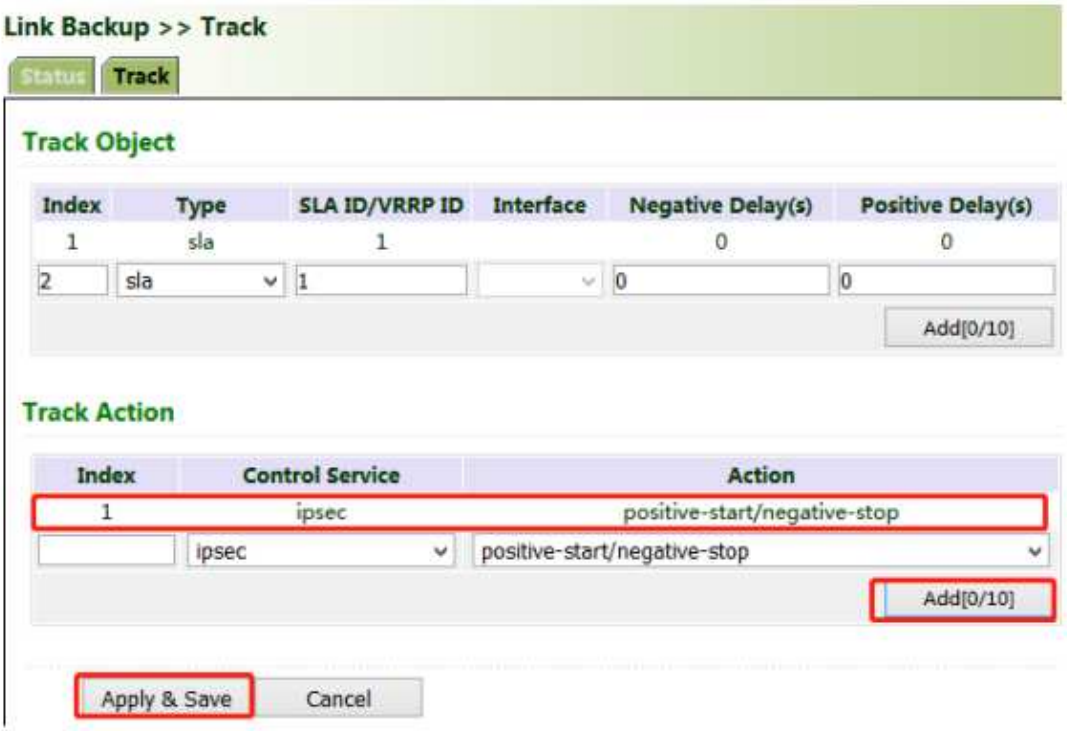
Negative Delay (s): Before switching in case of an abnormal state, system will delay for some time based on the Negative Delay setting (0 indicates switching immediatly).

P**ositive Delay (s)**: When a failure is recovered, system will delay for some time based on the Positive Delay setting before switch back to formar link(0 indicates immediate switching).



Method for adding an IPsec track entry in ER800:

Click "Link Backup >> Track >> Track" and set "Index" as required. "positive-start/negative-stop" means starting the IPsec service when the track detection state is Positive and stopping the IPsec service when the track detection state is Negative.



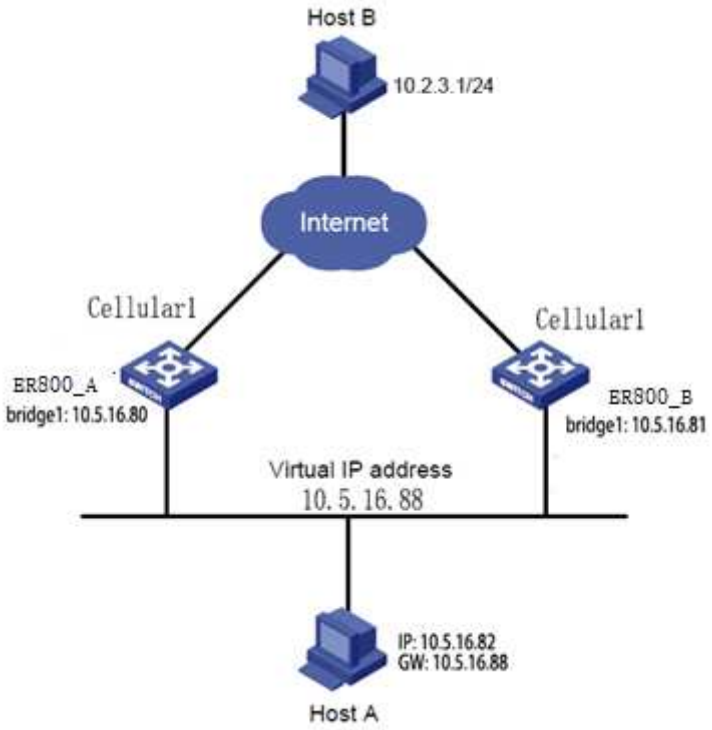
5.6.3 VRRP

Scenario: Multiple routers connect to one network at the same time. Router A acts as the host, and router B acts as a backup for router A. When router A fails, router B temporarily replaces router A as the host.

1. Information of the VRRP backup group:

- Backup group ID is 1.
- The IP address of the virtual router in backup group is 10.5.16.88.
- Router A acts as the master router.
- Router B acts as a backup router.

2. Network Diagram



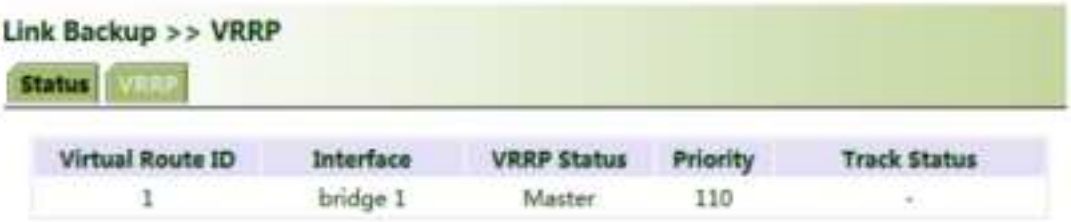
Router	Ethernet port connected to host A	IP address of the port connected to host A	Priority	Work mode
ER800_A	bridge1	10.5.16.80	110	Preemption
ER800_B	bridge1	10.5.16.81	100	Preemption

Method for configuring ER800_A as the master router and ER800_B as a backup router:

1. Configure ER800_A.

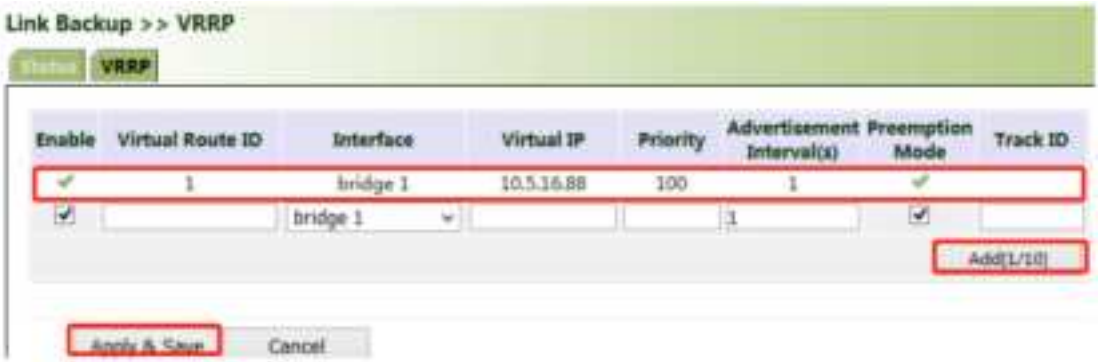
Click "Link Backup >> VRRP", set "Virtual Route ID" as required, select the interface of ER800_A, enter the virtual IP address, set the interface priority to 110, and click Add.

Click "Link Backup >> VRRP >> Status" to check the status of VRRP.



2. Configure ER800_B.

Click "Link Backup >> VRRP", set the interface priority to 100, and click Add.



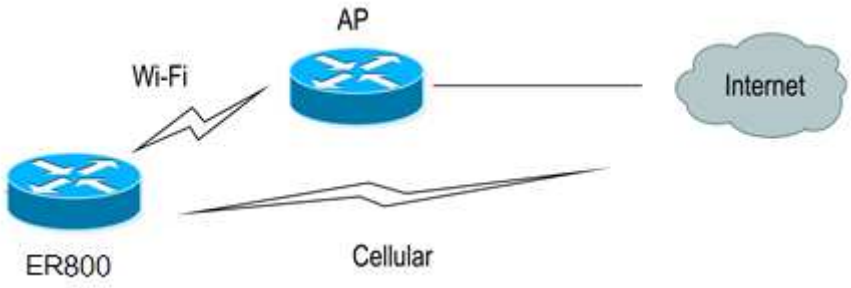
Click "Link Backup >> VRRP >> Status" to check the status of VRRP.

ER800_A performs router functions under normal circumstances. When ER800_A shuts down or fails, ER800_B performs router functions. Preemption mode is intended to enable ER800_A to continue to act as the master router

after it recovers.

5.6.4 Interface Backup

Scenario: VG710 accesses to the Internet via Wi-Fi, and an interface backup allows ER800 to access to the Internet through cellular when Wi-Fi is down. The topology is shown as below.

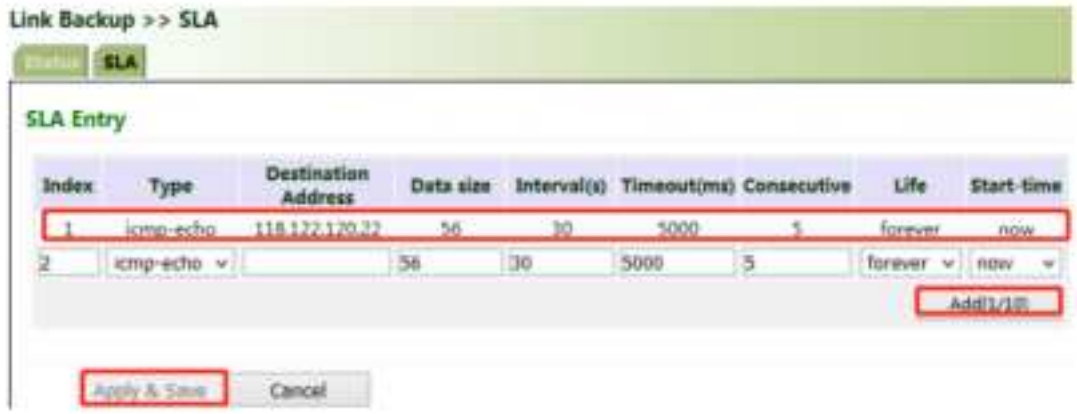


Method for creating an interface backup in ER800:

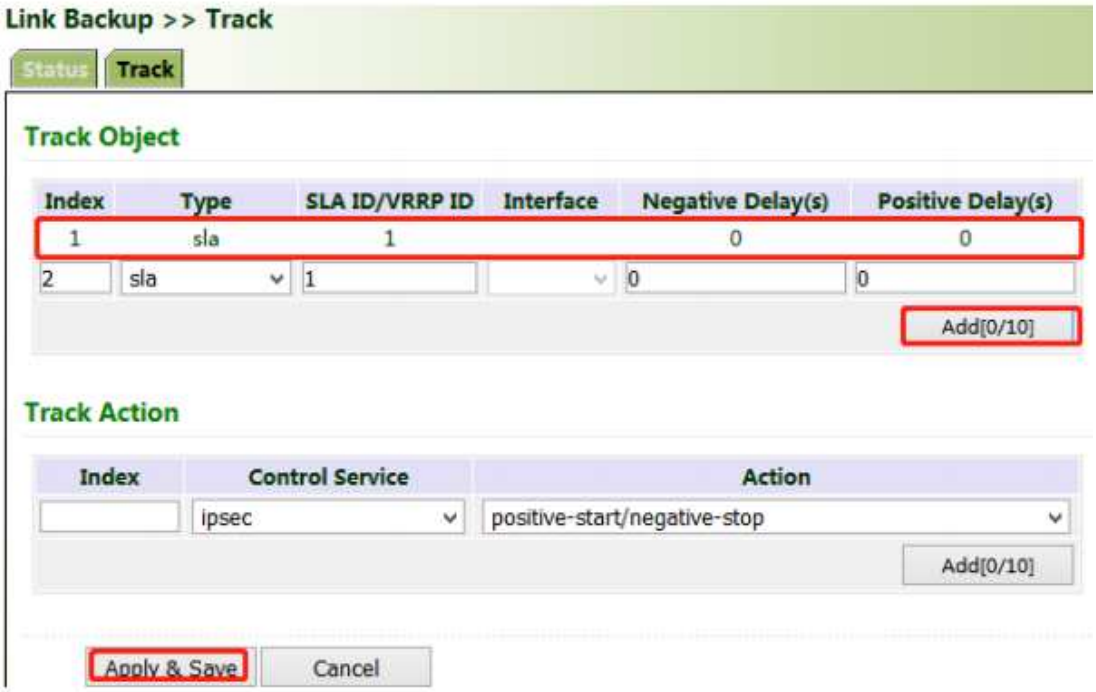
1. Configure ER800 to access to the Internet via Wi-Fi.

2. Click "Link Backup >> SLA >> SLA", add an ICMP detection entry. Set the IP address to the host address that can be detected over ICMP on the public or

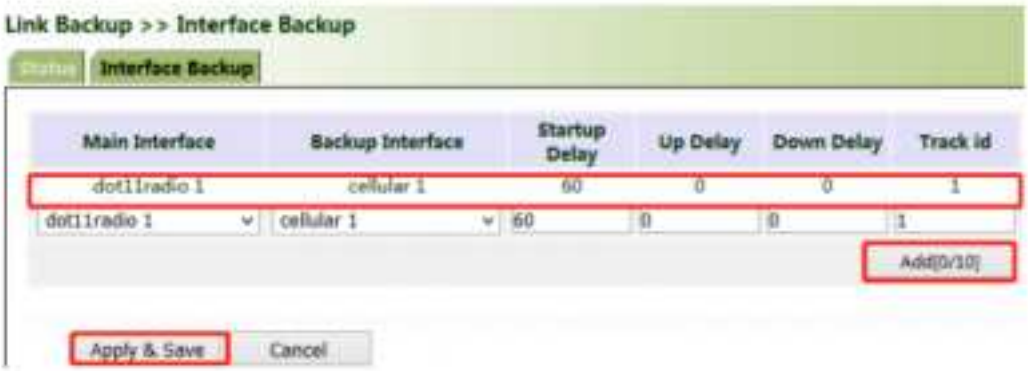
private network, for example, the public IP address 118.122.120.22. Click Apply & Save.



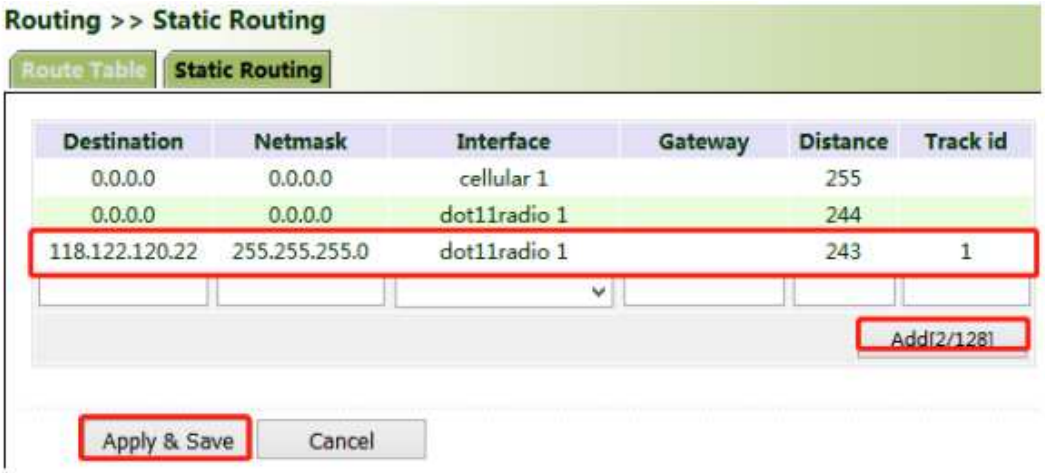
3. Click "Link Backup >> Track >> Track", add a track entry. Select "SLA" for "Type" and "dot11radio1" for "Interface", click Add, and then click Apply & Save.



4. Click "Link Backup >> Interface Backup", select "dot11radio1" for "Main Interface" and "cellular 1" for "Backup Interface", and click Apply & Save.



5. Click "Routing >> Static Routing", and add two routes for network access through the "dot11radio1" and "cellular 1" interfaces. A smaller value of "Distance" indicates a higher priority.



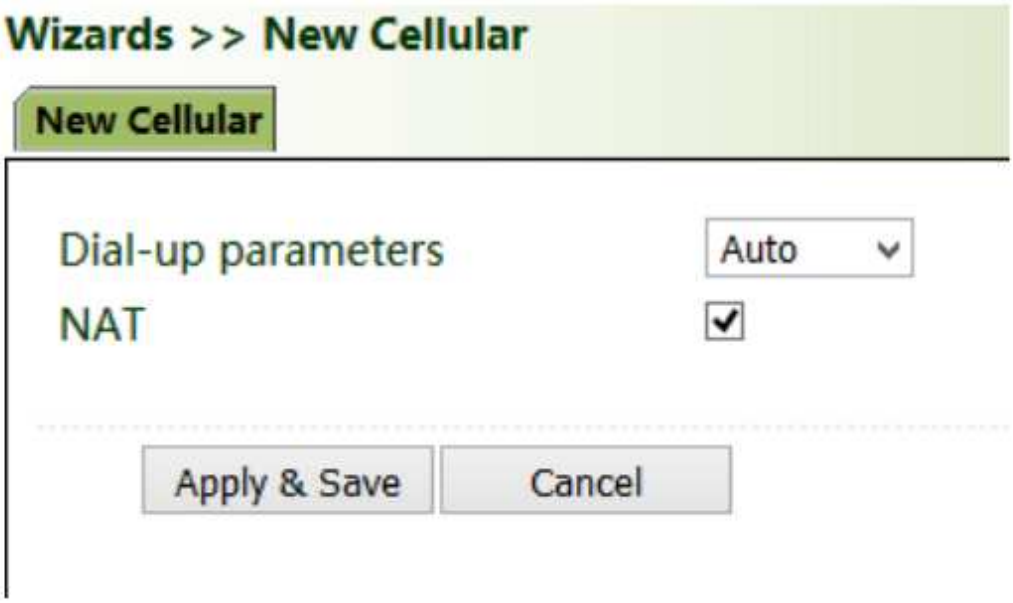
6. Trigger a Wi-Fi failure. According to the preset link detection policy, ER800 accesses tp the Internet through dial-up via the cellular port, and when Wi-Fi recovers, it will switch back to Wi-Fi immediately.

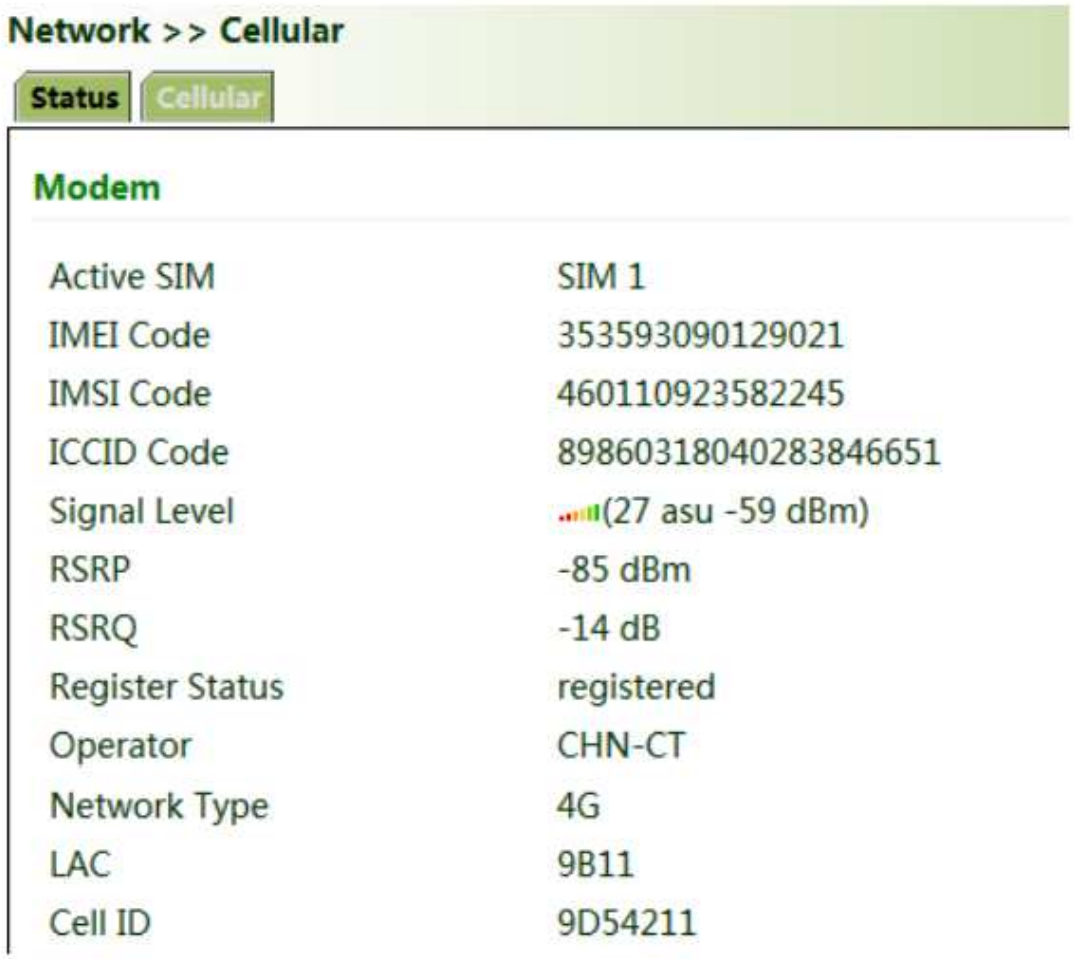
5.7 Wizards

Wizards module incorporates some common communication parameters, simplifies the operations.

5.7.1 New Cellular

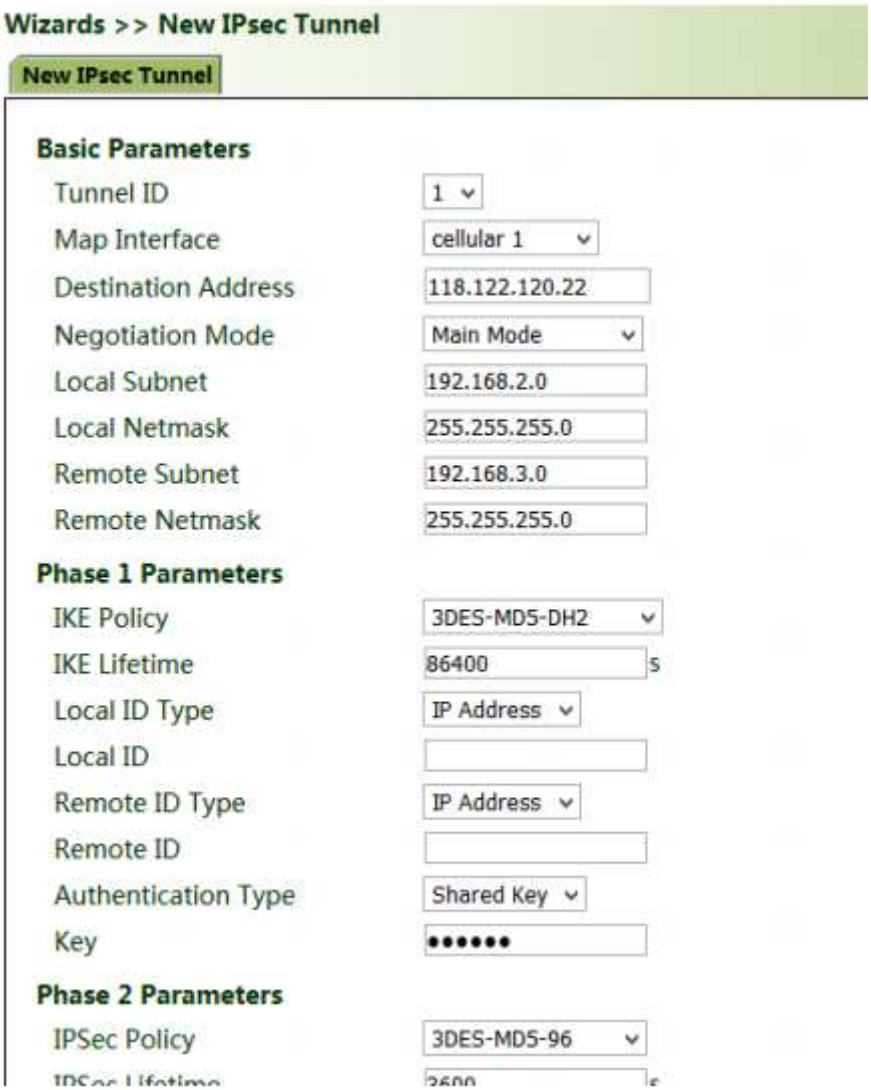
After insert a common network interface card, click "Wizards >> New Cellular >> Apply & Save", then access to the status page to check the network connection status of the device.





5.7.2 New IPsec Tunnel

Click "Wizards >> New IPsec Tunnel", set "Map Interface" to an interface ("bridge": bridge interface; "cellular": dialup interface; "dot11radio": Wi-Fi interface) for which you want to establish a tunnel, enter the peer IP address for "Destination Address", and enter the subnet IP addresses and masks at both ends of the tunnel. In Phase 1, enter the IDs at both ends of the tunnel and the connection key, and click Apply & Save.

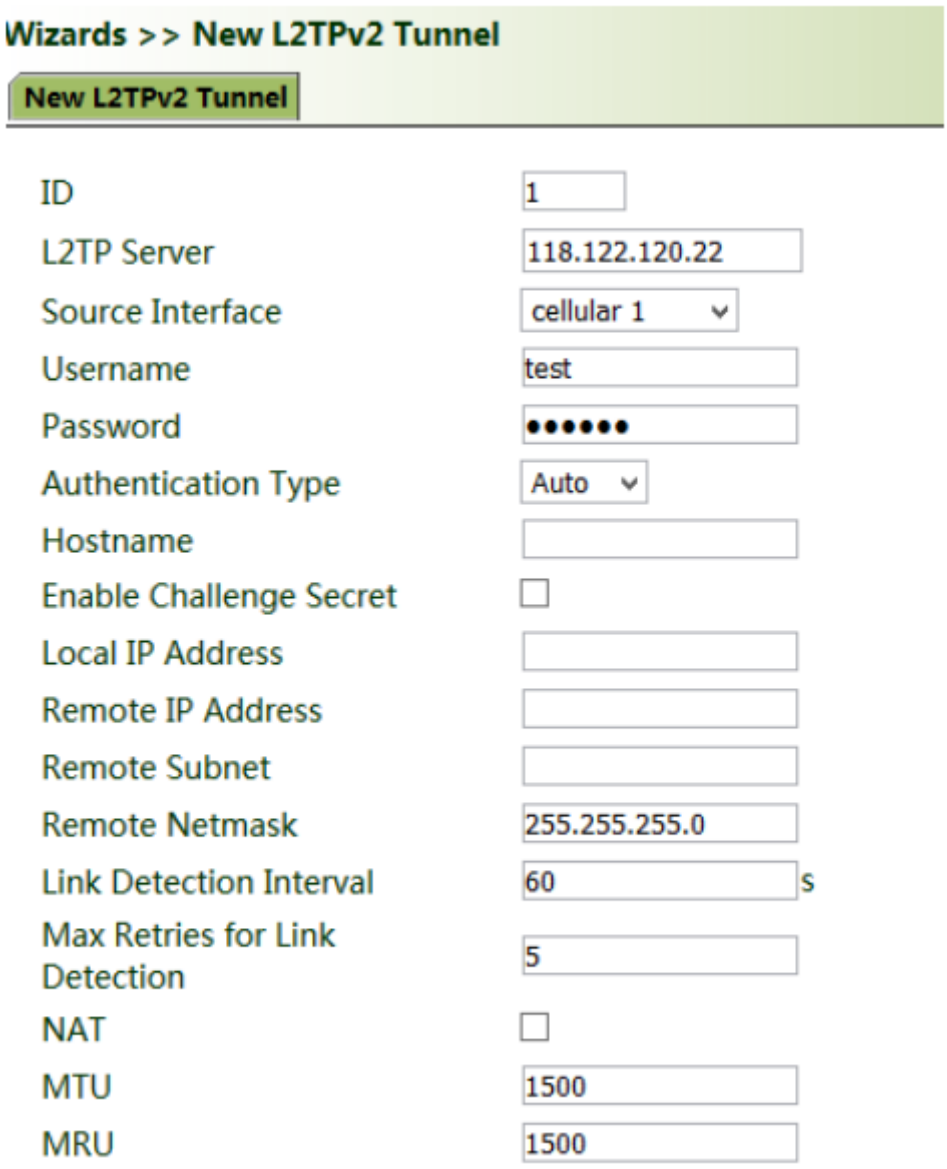


5.7.3 IPsec Experts Configuration

This function is only for specific users. Please contact our technical support.

5.7.4 New L2TPv2 Tunnel

Set the parameters of the L2TP server and the local/remote address. Click Apply & Save.



5.7.5 New Port Mapping

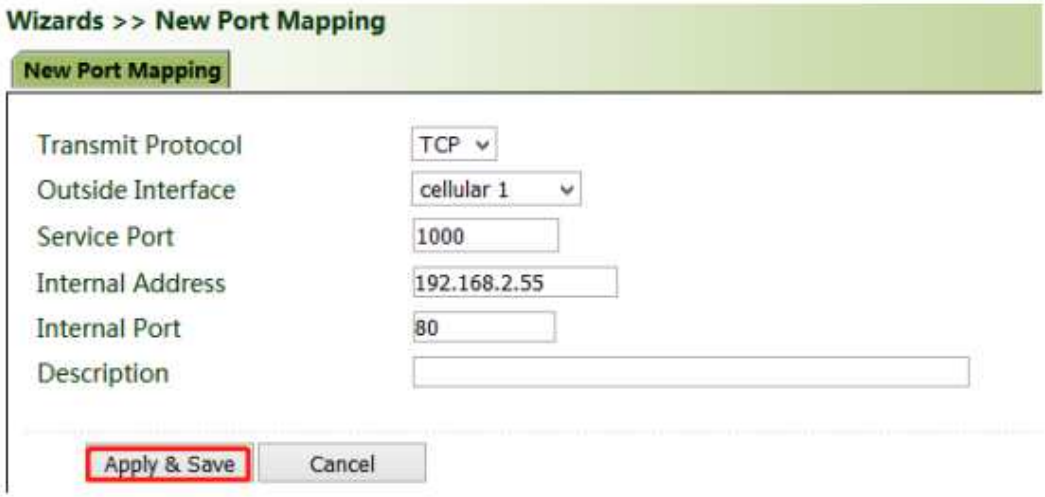
Port mapping is to map a host' s port on the intranet to a port on the extranet. When a user accesses the port on the extranet, the server will automatically map the request to the internal machine on the corresponding port.

Scenario: Users on the extranet cannot directly access to a web server in the intranet. In this case, a port mapping in the router can automatically transfers

the data to port 80 of the web server in the intranet when a user on the extranet accesses port 1000 via the cellular interface of the router.

Method for creating a port mapping in ER800:

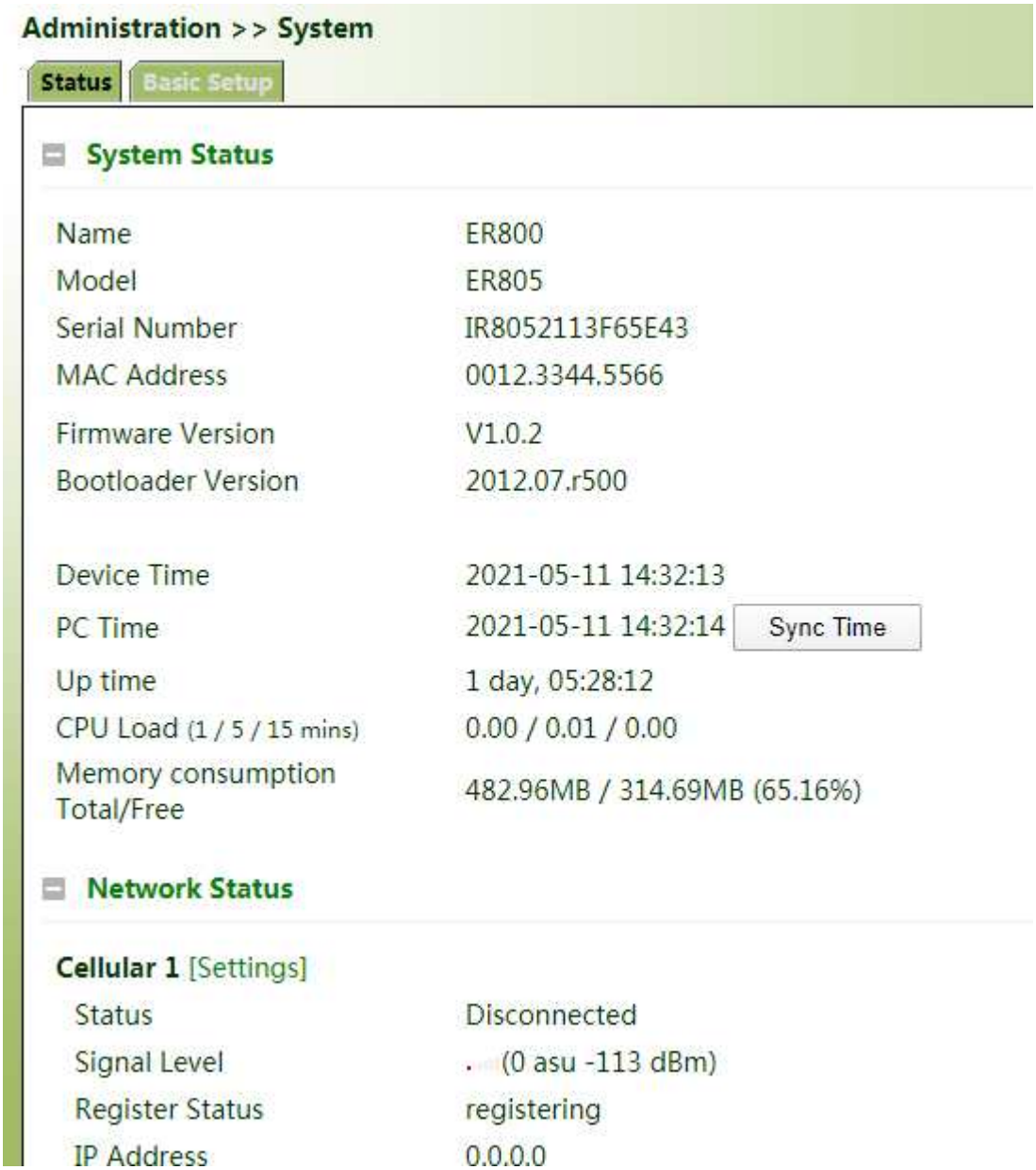
Click "Wizards >> New Port Mapping". Enter the interface for "Outside Interface", port for "Service Port", IP address of the internal host for "Internal Address", and port ID of the internal host for "Internal Port". Click Apply & Save.



6 System Management

6.1 System

Click "Administration >> System >> Status" to check the current system and network status of the device.



Click "Basic Setup" to modify the system language and device name.


Administration >> System
Status
Basic Setup
Language
English
Device Name
ER800
Apply & Save
Cancel

6.2 System Time

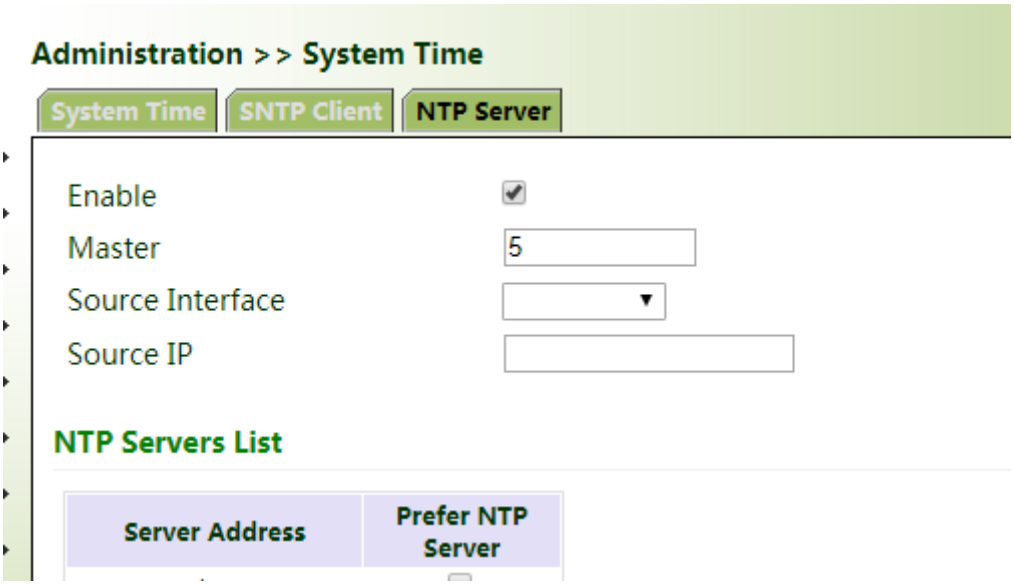
To ensure the coordination between the router and other devices, please set the system time accurately.

Synchronize system time manually:

Click "Administration >> System Time >> System Time >> Sync Time" to ensure consistency between the router time and PC time.

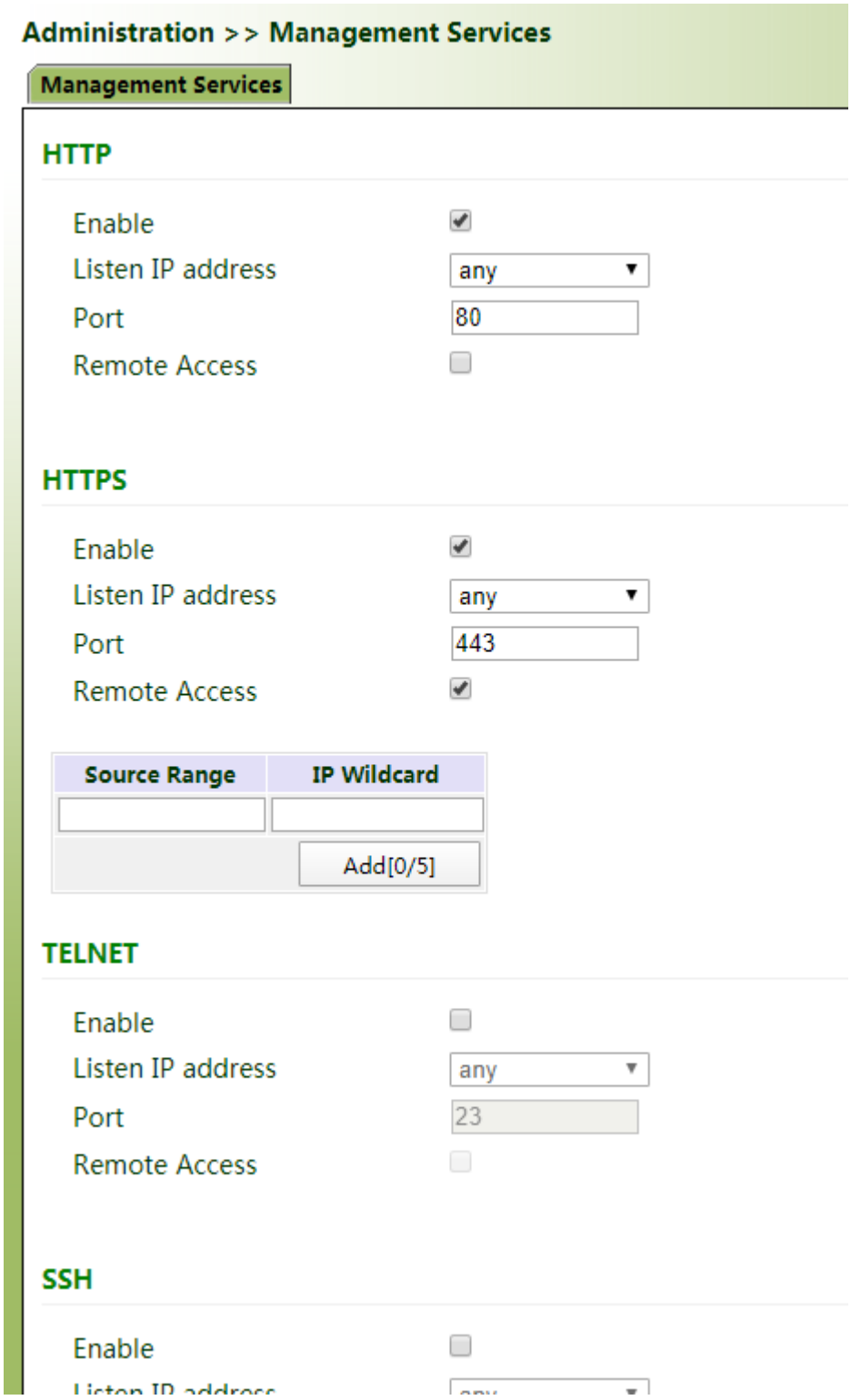
Synchronize system time automatically:

Click "Administration >> System Time >> SNTP Client or NTP Server" and check "Enable" to synchronize the time between the router and SNTP or NTP server. After NTP is enabled, the router can synchronize time for all devices in the LAN.


Administration >> System Time
System Time
SNTP Client
NTP Server
Enable
Master
5
Source Interface
Source IP
NTP Servers List
Server Address
Prefer NTP Server

6.3 Management Services

When need to access to router the via HTTP, HTTPS, TELNET, or SSH, click "Administration >> Management Services", enable the services, and click Apply & Save.


Administration >> Management Services
Management Services
HTTP
Enable
Listen IP address
any
Port
80
Remote Access
HTTPS
Enable
Listen IP address
any
Port
443
Remote Access
Source Range
IP Wildcard
Add[0/5]
TELNET
Enable
Listen IP address
any
Port
23
Remote Access
SSH
Enable

6.4 User Management

Click "Administration >> User Management" and create users, modify passwords, or delete users on the user management page.

Superuser and common user:

- Superuser: System will only create one superuser by default, with user name of **adm** and default password of **123456**. It has full access rights for function.

Note: You cannot delete the superuser, but can modify its password.

- Common user: Created by superuser, can check and modify router configurations.

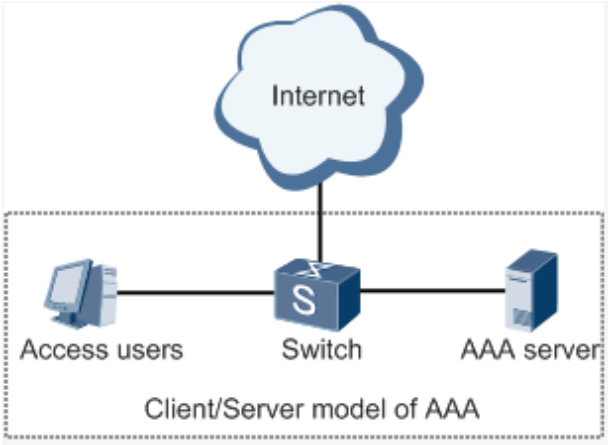
6.5 AAA

AAA is a security management mechanism for access control in network security, which provides three security services: authentication, authorization, and accounting.

- Authentication: Verify whether a user has the right to access.
- Authorization: Authorize a user to use specific services.
- Accounting: Record a user’ s network resource usage.

You can use only one or two of the security services provided by AAA. For example, if a company only expects to authenticate employees when they access to specific resources, the network administrator only needs to configure the authentication server. However, if a company expects to record the network usage of employees, the accounting server must be configured.

AAA usually works in client/server structure, which is highly scalable and convenient for centralized management of user information. as shown in the figure below.



Note: **Radius、Tacacs+ and LDAP** indicate authentication and authorization servers. **Local** indicates the local user name and password of the router.

6.5.1 Radius

Remote Authentication Dial in User Service (Radius) is a distributed information exchange protocol based on client/server structure. It protects the network from unauthorized access, and is usually used in various network environments that requires high security and allows remote user access.

Method for enabling Radius server in ER800:

Click "Administration >> AAA >> Radius". In "Server List", enter server address (domain name/IP address), port, and authentication key, click Add, and then click Apply & Save.

6.5.2 Tacacs+

Terminal Access Controller Access Control System + (Tacacs+) protocol is similar to Radius. It uses client/server mode for communication between the network access server (NAS) and the Tacacs+ server. However, Tacacs+ bases on TCP, and Radius bases on UDP. Tacacs+ protocol is mainly used for AAA's end users, Point-to-Point Protocol (PPP) and virtual private dial-up network

(VPDN) access users. Its typical application is to authenticate, authorize, and perform accounting for end users who need to login the device. As a Tacacs+ client, the device sends user name and password to the Tacacs+ server for verification. After authentication and authorization, the user can login the device for operations.

Method for enabling Tacacs+ server in ER800:

Click "Administration >> AAA >> Tacacs+". In "Server List", enter server address (domain name/IP address), port, and authentication key, click Add, and then click Apply & Save.

6.5.3 LDAP

The main advantage of Lightweight Directory Access Protocol (LDAP) lies in its quick response to users' search operations. For example, there will be massive user authentication operations perform concurrently. It will be inefficient if use database, because database is divided into various tables and will synthesise and filter in every searching. LDAP is equivalent to one table, and requires only user name, password, and some other parameters, which is quite simple. It can meet the authentication requirement regarding the efficiency and structure.

Method for enabling LDAP server in ER800:

Click "Administration >> AAA >> LDAP". In "Server List", enter any name for "Name", enter server address (domain name/IP address) and port, and enter the base DN obtained from the server. Set user name and password for accessing the server. Select "None", "SSL", or "StartTLS" for "Security". Click Add, and then click Apply & Save.

6.5.4 AAA

Authentication methods:

- No authentication (**none**): No validity check is performed.
- Local authentication (**local**): User information is configured on the NAS. Local authentication is fast, which can reduce the operational costs, but the information storage amount is limited by hardware.
- Remote authentication: User information is configured on the authentication server. Remote authentication is supported over Radius, Tacacs+, and LDAP.

Authorization method:

- No authorization (**none**): No authorization is performed for users.

- Local authorization (**local**): Authorization is performed based on the properties configured by the NAS for the local account.
- Tacacs+ authorization: Users are authorized by the Tacacs+ server.
- Authorization after successful Radius authentication: Authorization is bound to authentication, and cannot be performed independently over Radius. Radius
- LDAP authorization

Method for enabling authentication and authorization in ER800:

Click "Administration >> AAA >> AAA Settings". 1, 2, and 3 are corresponding to Radius, Tacacs, ad LDAP respectively. Authentication entries 1, 2, and 3 must be corresponding to authorization entries 1, 2, and 3 respectively. If all of radius, tacacs+, and local are set, the priority sequence will be as follows: 1 > 2 > 3.

6.6 Configuration Management

Method for importing configurations:

Click "Administration >> Config Management >> Config Management >> Browse", select a configuration file, and click Import to import the configuration file to the router.

Method for backing up current running configurations to the PC (common):

Click Backup running-config.

Method for restoring default configurations:

Click Restore default configuration and then click OK.

6.7 SNMP

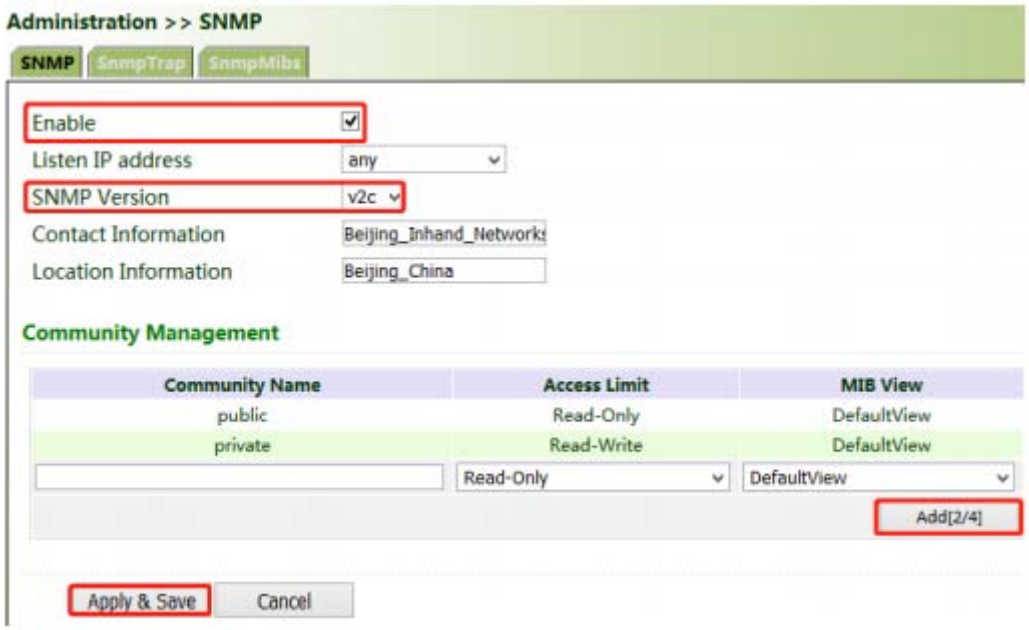
6.7.1 SNMP

At present, the SNMP Agent in ER800 supports SNMPv1, SNMPv2c, and SNMPv3.

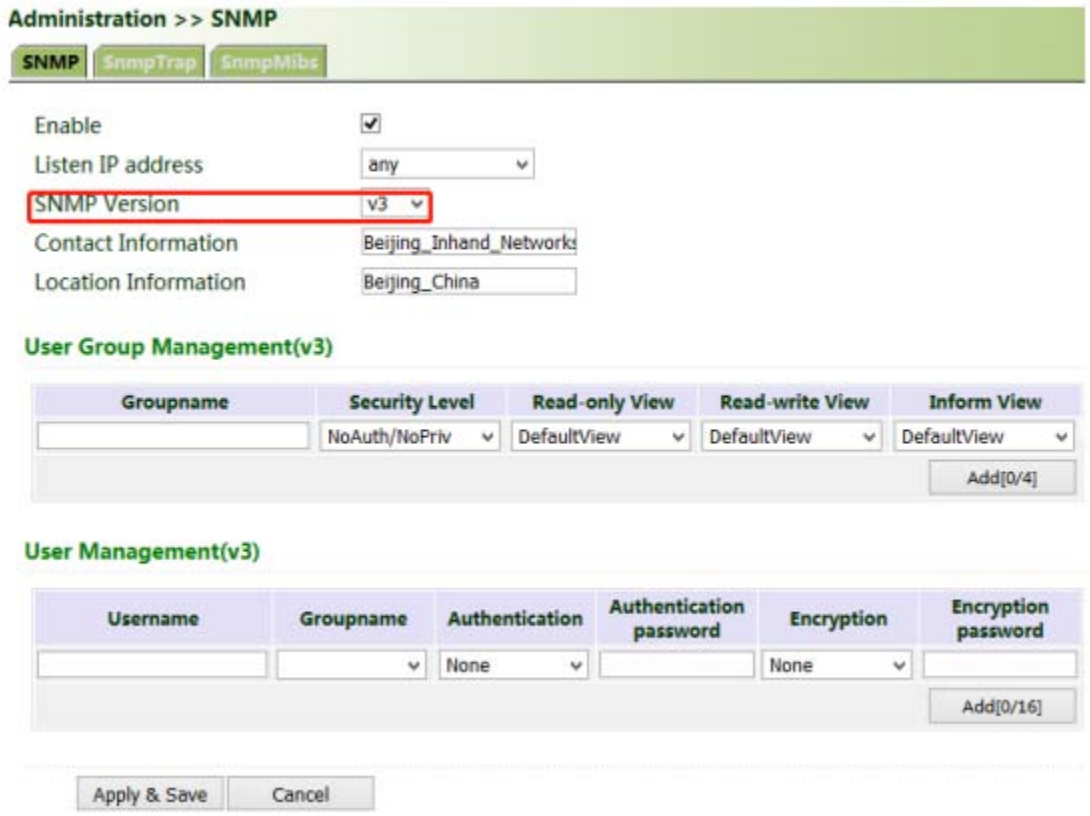
- SNMPv1 and SNMPv2c use community names for authentication.
- SNMPv3 uses user names and passwords for authentication.

Method for enabling SNMP in ER800:

Click "Administration >> SNMP >> SNMP", check "Enable", select "v1c" or "v2c" for "SNMP Version", and click Apply & Save.



If use v3c, you need also to configure corresponding user and user group. Enter any name for "Groupname", select a security level, and click Add. Enter any name for "Username", select the new group name for "Groupname", set "Authentication" and "Authentication password", click Add, and then click Apply & Save.

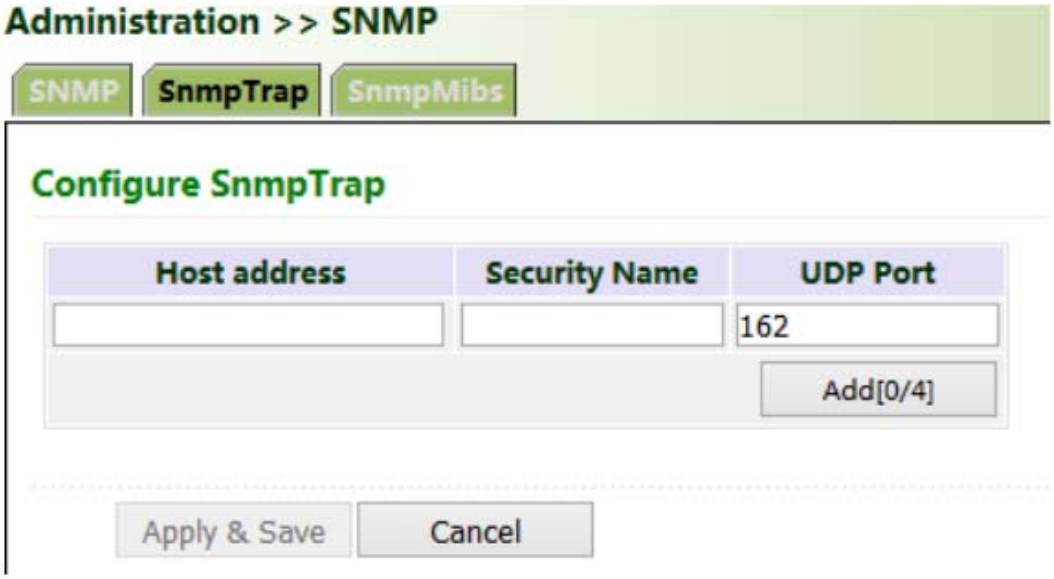


6.7.2 SNMP Trap (Alarm)

SNMP trap is a type of entrance. When this entrance is reached, the SNMP managed devices will actively notify the NMS, instead of waiting for the polling of NMS. In a SNMP-enabled network, the agents on managed devices can report errors to the NMS anytime, without waiting for the polling from NMS. The errors are reported to the NMS through traps.

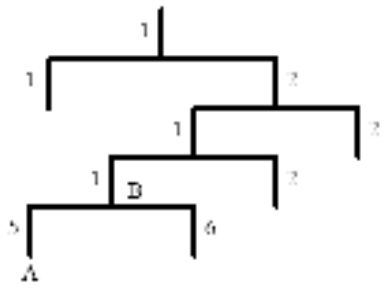
Method for enabling SnmpTrap in ER800:

Click "Administration >> NMP >> SnmpTrap". Enter IP address of the NMS. Enter the corresponding group name when v1c or v2c is selected, or the corresponding user name when v3c is selected, ensuring that the name consists of 1–32 characters. By default, the UDP port ID ranges from 1 to 65535.



6.7.3 SnmpMibs

In SNMP messages, management variables are used to describe the managed objects in the device. SNMP uses a hierarchical naming scheme to identify the managed objects uniquely. The entire hierarchical structure is like a tree. Nodes of the tree represent the managed objects. As shown in the figure below, each node can be uniquely identified by a path starting from the root.

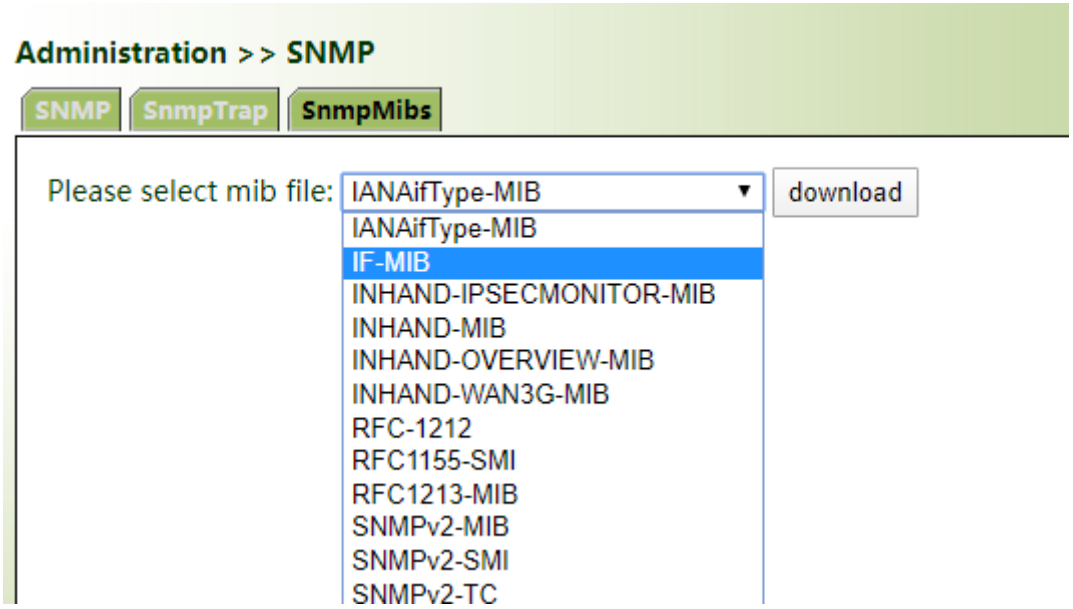


Management information base (MIB) is used to describe the hierarchical structure of the tree. It is a set of standard variable definitions for the monitored network device. In the above figure, managed object B can be

uniquely determined by a string of numbers {1.2.1.1}, which named object identifier (OID) of this managed object.

Method for downloading a SnmpMibs file to the PC:

Click "Administration >> SNMP >> SnmpMibs", select a folder, and click download to download it to the PC. Find the folder on the PC and import it to NMS.



6.8 Alarm

The alarm function allows users to identify router' s abnormalities in time. When an abnormality occurs, the router will report an alarm. You can select system-defined abnormalities and choose an appropriate notification way to obtain the abnormality information. All alarms are recorded in alarm logs so that users can identify abnormalities and perform troubleshooting in time.

Alarm states:

- Raise: indicates that the alarm has been generated but not been confirmed.
- Confirm: indicates that the alarm cannot be solved currently.
- All: indicates all generated alarms.

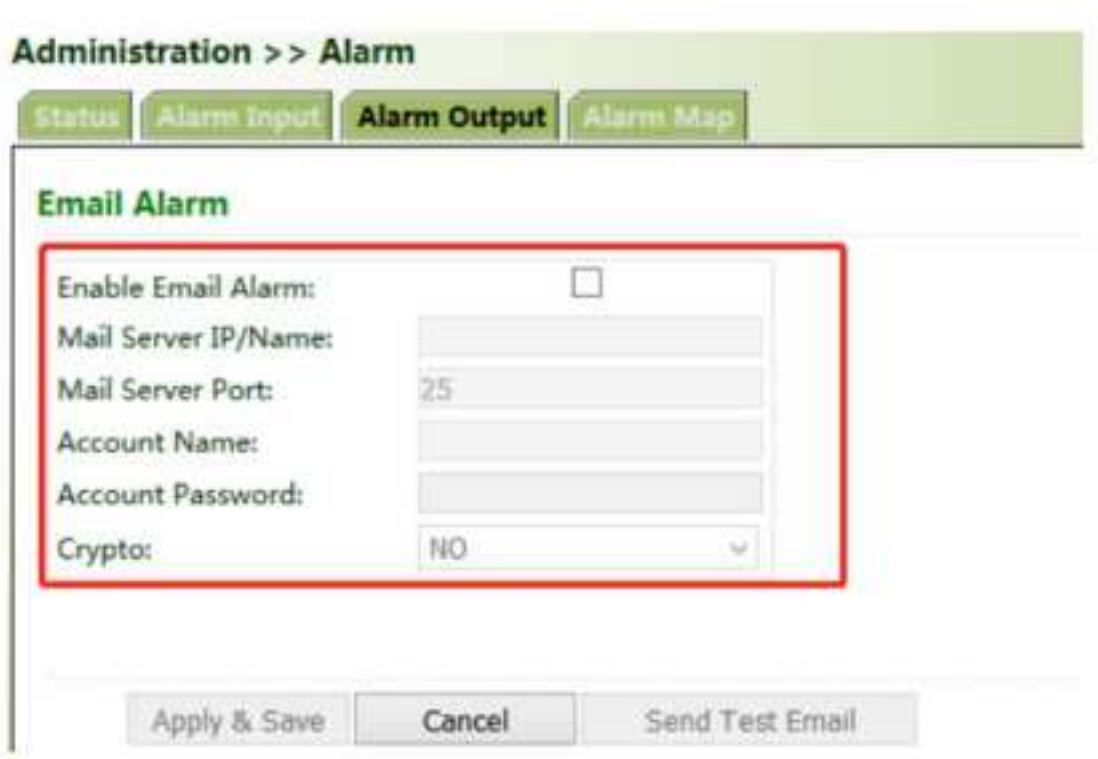
Alarm levels:

- EMERG: The device undergoes a serious error that causes a system reboot.
- CRIT: The device undergoes an unrecoverable error.
- WARN: The device undergoes an error that affects system functions.
- NOTICE: The device undergoes an error that affects system performance.
- INFO: A normal event occurs.

1. Status: Click "Administration >> Alarm >> Status" and view all alarms generated in the system since power-on.

2. Alarm Inputs: Select an alarm type as required. When this item is abnormal, an alarm is generated.

3. Alarm Output: When an alarm is generated, the system will send the alarm content to the destination email address automatically. Set the sender mail address in "Email Alarm" and the receiver mail address in "Mail Address". "Mail Server IP/Name" can be searched in the Internet.



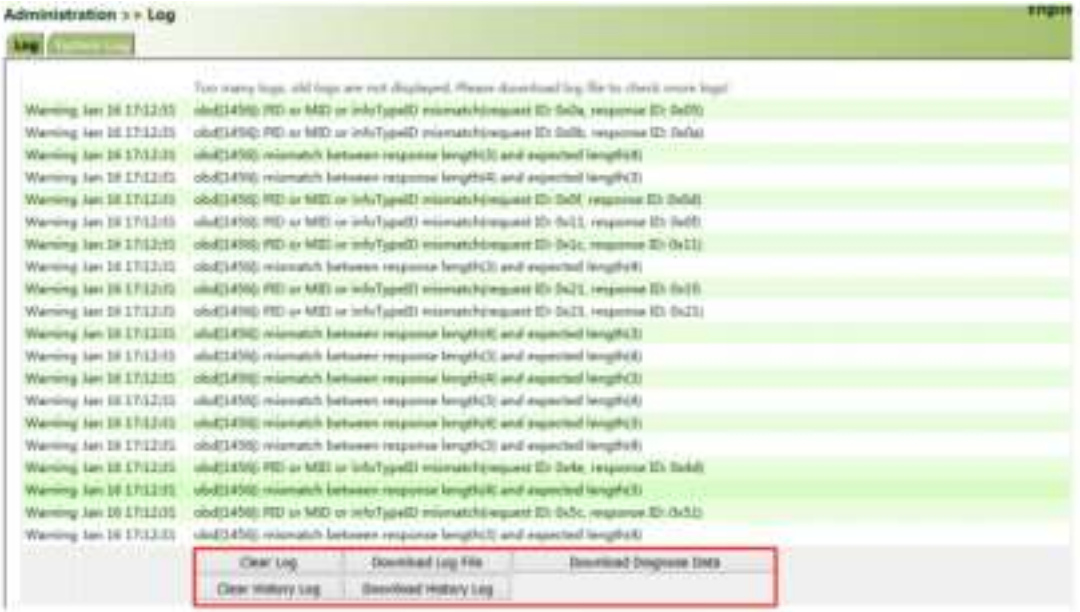
4. Alarm Map: Alarms can be received in two ways: command line interface (CLI) (console interface) and Email. Some devices support SMS alarms. Please enable and set the email address on the "Alarm Output" page.

6.9 System Logs

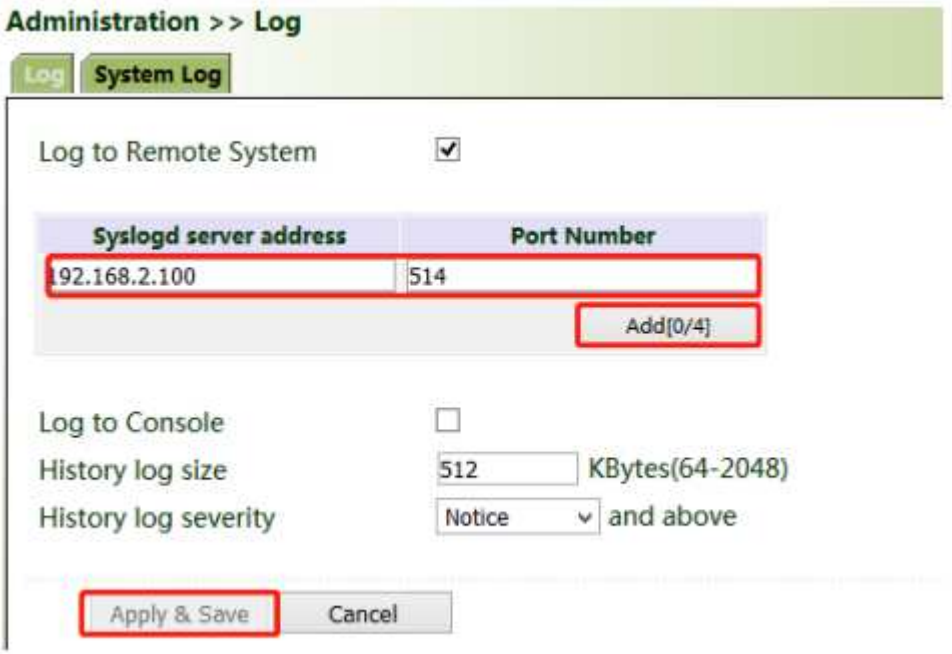
Method for checking system logs:

Click "Administration >> System Log" to view system logs.

This page also provides the following operations: "Clear Log", "Download Log File", "Download Diagnose Data", "Clear History Log", and "Download History Log". History logs are those stored for extended time as specified on the "System Log" page. The diagnose data file is encrypted, you need to decrypt the file with the decryption tool provided by InHand.

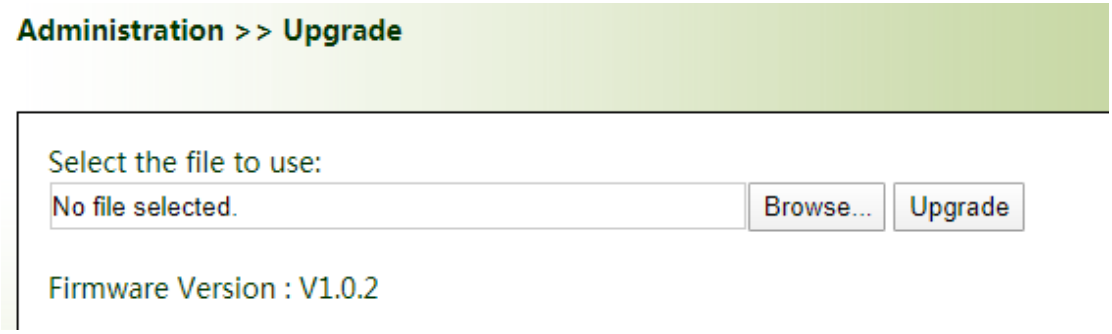


The storage space of the router is limited (512 KB by default). To save all the logs, you need to use a remote log server (for example, Kiwi Syslog Daemon). Set the address and port of the log server on the web page. The router will upload all the system logs to the remote log server.



6.10 System Upgrade

Click "Administration >> Upgrade >> Browse", select an upgrade file, and click Upgrade. Then restart the system after the upgrade is completed.



Note:

During the software upgrade, do not perform any operation on the web page; otherwise, the software upgrade may be interrupted.

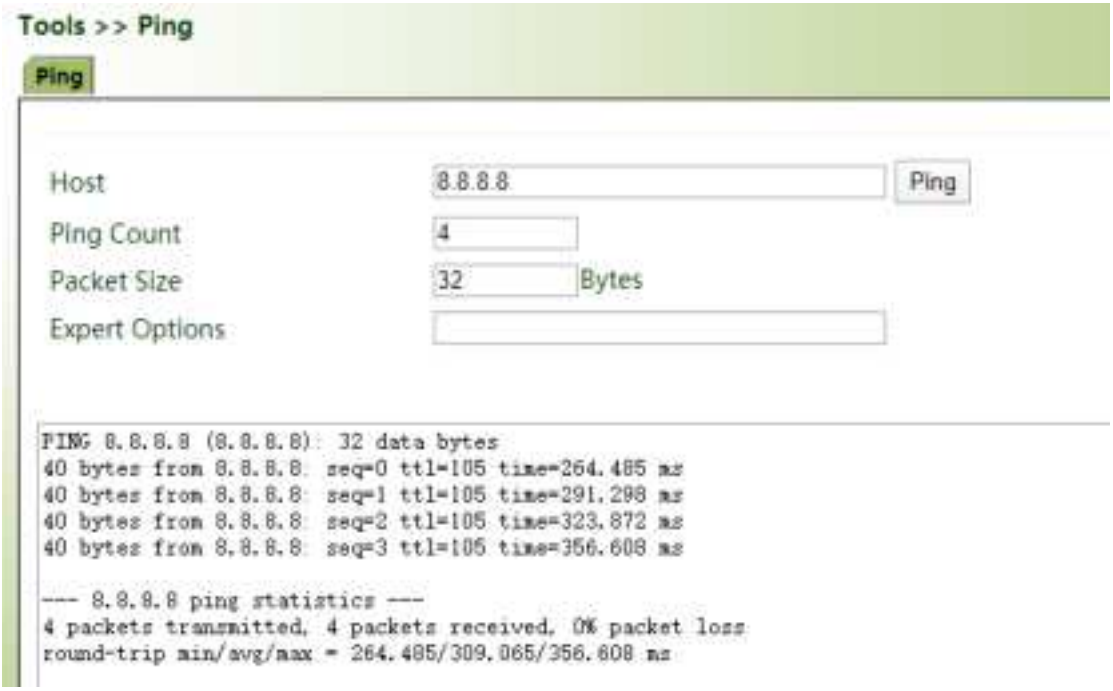
6.11 System Reboot

Click "Administration >> Reboot >> OK" to reboot the system.

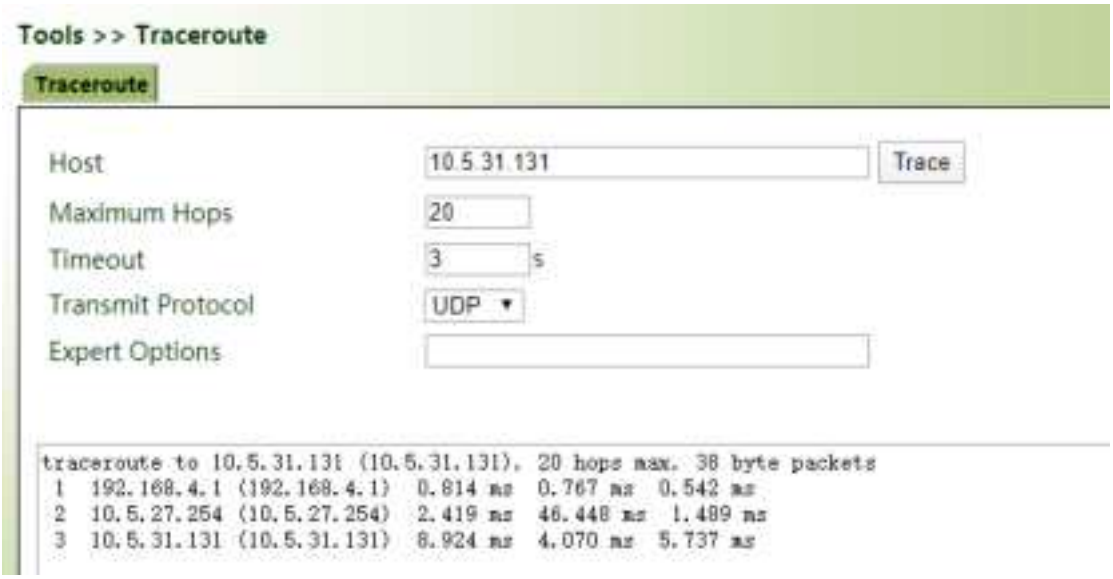
7 Diagnostic Tools

Diagnostic tools are used to detect the network connection of the router: Ping, Traceroute, Tcpdump, and Link Speed Test.

Ping: It is used to detect the external network connection of the device. Enter any common website for "Host" and click Ping. If data transmission occurs, the network is connected properly.

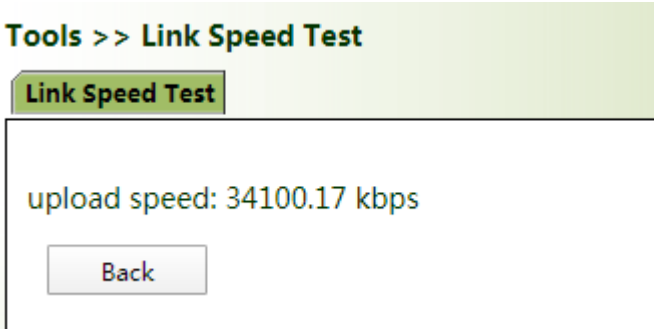


Traceroute: Enter the IP address of the peer host and click "Trace" to detect the route connection.



Tcpdump: Select an interface ("any" or "bridge1"), set "Capture Number", and click Start Capture, Stop Capture and finally Download Capture File.

Link Speed Test: Upload and download files to test the link speed.



Note:

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

FCC Warning

✧ Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

✧ —Reorient or relocate the receiving antenna.

✧ —Increase the separation between the equipment and receiver.

✧ —Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

✧ —Consult the dealer or an experienced radio/TV technician for help.

✧ FCC Caution

✧ This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

✧ The user manual or instruction manual for an intentional or unintentional radiator shall caution the user that changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment. In cases where the manual is provided only in a form other than paper, such as on a computer disk or over the Internet, the information required by this section may be included in the manual in that alternative form, provided the user can reasonably be expected to have the capability to access information in that form.

✧ **RF Exposure Statement**

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

✧ EUT configuration:

(FCC ID: 2AANYER805 contains FCC ID: XMR201807EP06A, IC: 11594A-ER805 contains IC: 10224A-201807EP06A)

ISED statement

This device complies with Innovation, Science and Economic Development Canada license-exempt RSS standard(s). Operation is subject to the following two conditions:

(1) This device may not cause interference, and

(2) This device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d' Innovation, science et développement économique au Canada applicables aux appareils radio exempts de licence.

L'exploitation est autorisée aux deux conditions suivantes:

(1) l'appareil ne doit pas produire de brouillage, et

(2) l'utilisateur de l'appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d'en compromettre le fonctionnement.

ISED RF Exposure Statement

This equipment must be installed and operated in accordance with provide instructions and the antenna used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operation in conjunction with any other antenna or transmitter. End-users and installers must be provided with antenna installation instructions and transmitter operating conditions for satisfying RF exposure compliance.

ce matériel doit être installé et exploité conformément à des instructions et l'antenne utilisée pour cet émetteur doit être installé pour fournir une distance d'au moins 30 cm de toutes les personnes et ne doit pas être installé ou opération conjointement avec toute autre antenne ou transmitter.les utilisateurs finals et les installateurs doivent fournir des instructions d'installation et d'antennes - conditions relatives à l'exposition aux champs rf de conformité.

This radio transmitter [IC: 11594A-ER805] has been approved by Innovation, Science and Economic Development Canada to operate with the antenna types listed below, with the maximum permissible gain indicated. Antenna types not included in this list that have a gain greater than the maximum gain indicated for any type listed are strictly prohibited for use with this device.

Cet émetteur radio [IC: 11594A-ER805] a été approuvé par le Ministère canadien de l'innovation, de la science et du développement économique et peut fonctionner avec le type d'antenne indiqué ci - dessous et indiquer un gain maximal autorisé.Le gain d 'un type d' antenne qui ne figure pas dans cette liste est supérieur au gain maximal de tout type énuméré et est strictement interdit d 'utilisation avec le dispositif.

Antenna Information:

Antenna	Manufacturer	Model Number	Antenna Gain (Max)	Impedance (ohm)	Antenna Connector	Antenna Type
Wi-Fi Ant. 1 Wi-Fi Ant. 2	SHENZHEN GUYOU TECHNOLOGY CO.LTD	GY-XPF-BCL2.5-GJG22	2.72 dBi 2412-2462MHz 0.21 dBi 5150-5250MHz 0.02 dBi 5725-5850MHz	50	RP-SMA(male)	Monopole
LTE Main Ant LTE Diversity Ant.	SHENZHEN GUYOU TECHNOLOGY CO.LTD	GY-XPL-BDL2-AJG30	0 dBi	50	SMA-J(male)	Monopole