IP3012L Industrial Communication Server

User’s Manual

IP3012L User's Manual

Copyright Notice

Trademarks

InHand is a registered trademark of InHand Networks. Other registered marks cited in this manual represented their respective companies.

Disclaimer

Information in this document is subject to change without notice and does not represent an obligation on the part of InHand Networks.

This user manual may include intentional technical or typographical errors. Changes are periodically made to the manual to correct such errors, and these changes are not informed in new editions.

Technical Support Contact Information

InHand Networks

support@inhandnetworks.com

Table of Contents

1. IP3012L Introduction

This Chapter includes:

- Overview
- Features

1.1 Overview

IP3012L is a dedicated vehicle Wi-Fi router with embedded NGINX web server and local storage SSD. With IP3012L and the Rainbow Wi-Fi cloud, motor coach operators may easily setup an advanced Wi-Fi operating system which provides device management, content management, vehicle location management, visitor management, statistical reports, and other features. Travelers simply connect to the Wi-Fi hotspot provided by IP3012L to surf Internet, and to enjoy local services such as VOD movies and interactive games provided by operators. By deploying the Rainbow Wi-Fi cloud, motor coach operators may easily remotely manage thousands of IP3012L devices, no matter changing visitor policy or updating media content deployed in IP3012L.

The IP3012L is a portal into the mobile internet and a step forward in providing value-added services to travelers.

1.2 Features

- **Advanced Wi-Fi**
  - Support dual band 2.4GHz and 5.8GH, fully compliance with IEEE802.11 ac/a/b/g/n standards.
  - With 2X2 MIMO technology enabled, Wi-Fi connection bandwidth can reach as high as 1.2Gbps, brings amazing multi-user performance.
- **High-speed 4G Access**
  - Integrating up to 4G cellular module, IP3012provides FDD-LTE access, with 100Mbps uplink and 50Mbps downlink.
  - Quad Band LTE: 700/850/AWS (1700/2100)/1900 MHz; FDD-Band (17,5,4,2); Tri Band UMTS (WCDMA): 850/AWS (1700/2100)/1900 MHz; FDD-Band (5,4,2) Quad Band

GSM/GPRS/EDGE: 850/900/1800/1900 MHz

- **GPS**
  - With GPS enabled, IP3012 provides vehicle location, speed/course over ground and track information.
- **Powerful Web Portal**
  - When visitors connect to the Wi-Fi hotspot provided by IP3012L, a greeting splash page pops up, providing local media services and user authentication.
- **Built-in Web Server**
  - Embed reliable NGINX web server, enabling local media services.
  - Support PHP, enabling dynamic page content.
- **Local Storage**
  - Support SSD up to 1TB, tolerating vibration from vehicle.
  - Local storage may be used to store local web content, movies, music, apps, etc. to accelerate local access and to save internet bandwidth.
- **Content Update Mechanism**
  - Inremote synchronization mode, locally stored contents may sync with the cloud.
  - Inlocal synchronization mode, content may be updated via SD card or FTP.
  - Both modes may be hybrid to enable even more flexible operation.
- **Visitor Behavior Management**
  - Support visitor authentication by SMS or social accounts.
  - Support QoS to limit per-user bandwidth and traffic, preventing overages and protecting latency-sensitive traffic.
  - Support web sites blacklist and whitelist.
- **Cloud Management**
  - Support the Rainbow Wi-Fi cloud, enabling device management, content management, vehicle location management, visitor management, statistical reports, and other features.
  - Support CLI, web UI and SNMPv3.
- **High Reliability**
  - With dedicated vehicle power module inside, IP3012L tolerates power voltage dips,

overruns, short and other failures. Support automatically power control with ACC signal to protect SSD and vehicle battery.

- Fanless cooling design to simplify installation.
- Support link quality inspection and auto-recovery to ensure reliable LTE access.

- **Robust Security**
  - Support IPSec VPN, DMVPN, L2TP, SSL VPN, and CA certification to ensure data security.
  - Support powerful firewall functions such as Stateful Packet Inspection (SPI), Access Control List (ACLs), DoS attack prevention, etc.
  - Support AAA, TACACS, Radius, local authentication, and multi levels user authority to ensure secure management.

2. Establish Network Connection

This chapter mainly contains the following contents:

- Establish Network Connection
- Confirm that the connection between supervisory PC and router
- Cancel the Proxy Server

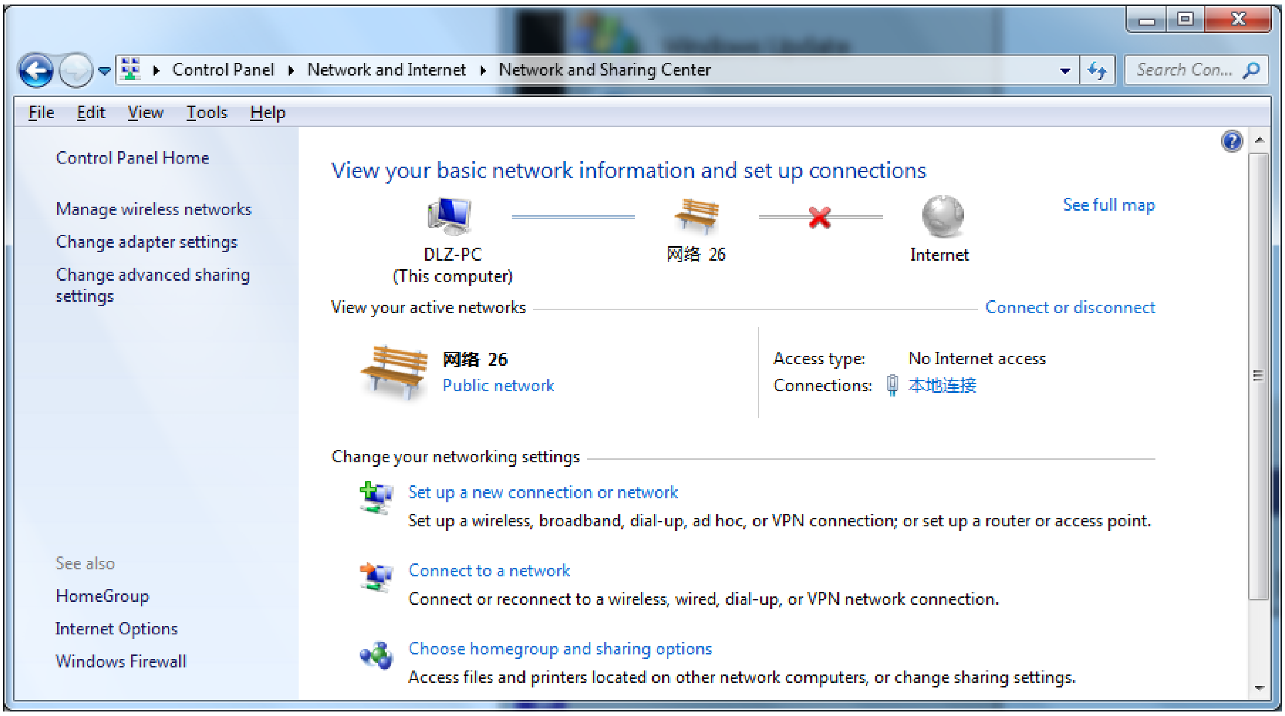
After completing the hardware installation, before to log in the Web set-up page, you need to ensure that the management of the Ethernet card installed on your computer.

2.1 Establish Network Connection

2.1.1 Automatic acquisition of IP address (recommended)

Please set the supervisory computer to "automatic acquisition of IP address" and "automatic acquisition of DNS server address" (default configuration of computer system) to let the router automatically assign IP address for supervisory computer.

1) Open “Control Panel”, double click “Network and Internet” icon, enter “Network and Sharing Centers”



View your basic network information and set up connections

View your active networks

网络 26
Public network

Access type: No Internet access
Connections: 本地连接

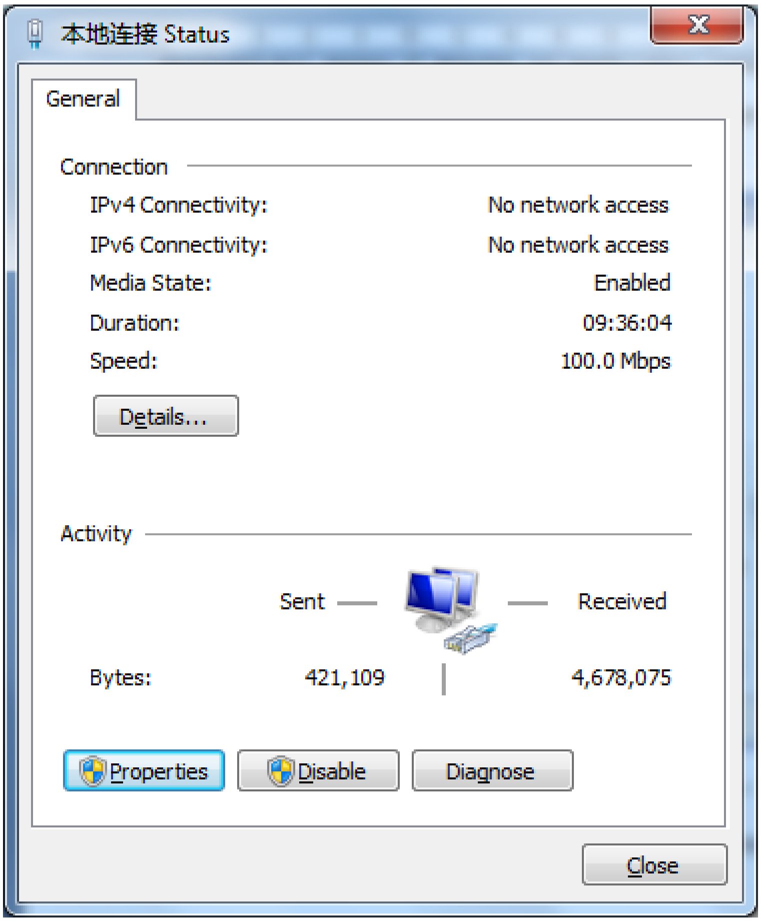
Change your networking settings

Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

2) Click the button <Local Connection> to enter the window of "Local Connection Status”



本地连接 Status

General

Connection

IPv4 Connectivity: No network access

IPv6 Connectivity: No network access

Media State: Enabled

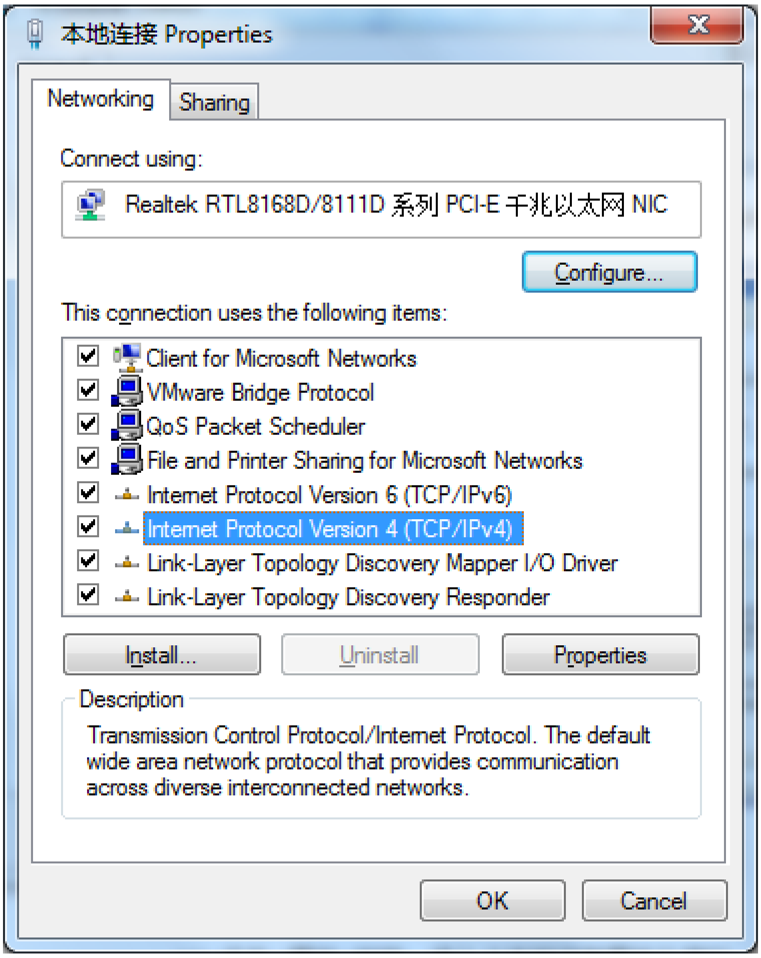
Duration: 09:36:04

Speed: 100.0 Mbps

Activity

	Sent	Received
Bytes:	421,109	4,678,075

3) Click <Properties>to enter the window of "Local Connection Properties”, as shown below.



本地连接 Properties

Connect using:

Realtek RTL8168D/8111D 系列 PCI-E 千兆以太网 NIC

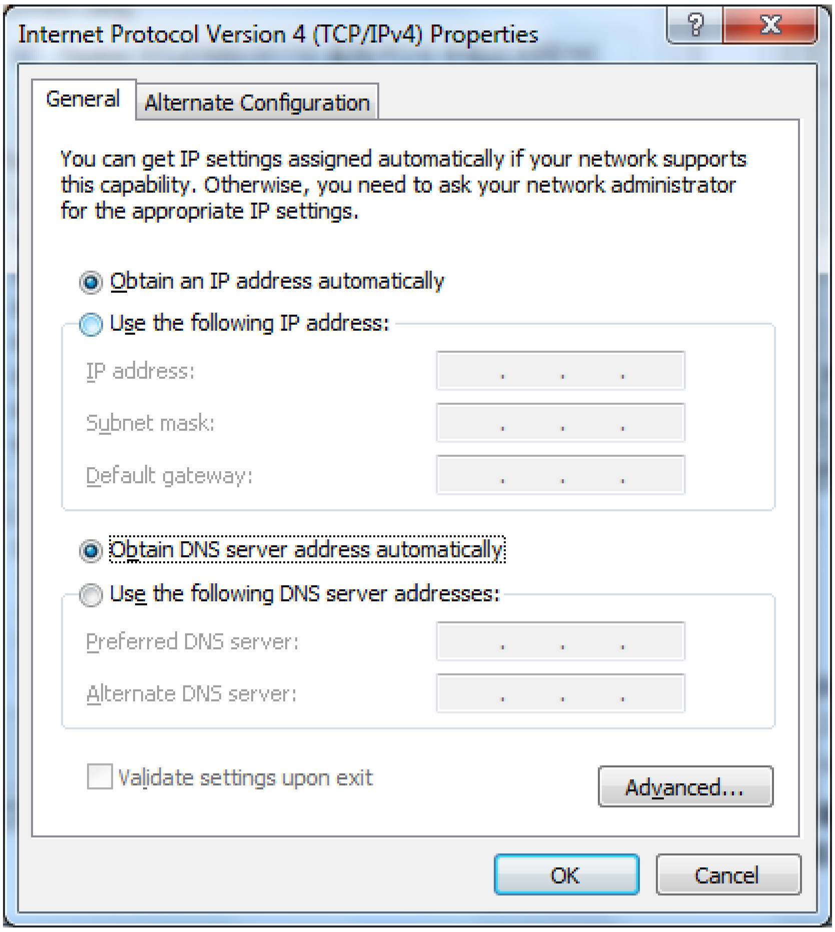
This connection uses the following items:

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

Description

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

4) Select "Internet Portocol Version 4(TCP/IPv4)", click <Properties> to enter "Internet Portocol Version 4 (TCP/IPv4)Properties" page. Select "Obtain an IP address automatically" and "Obtain DNS Server address automatically", then click <OK> to finish setting, as shown below.



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

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

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

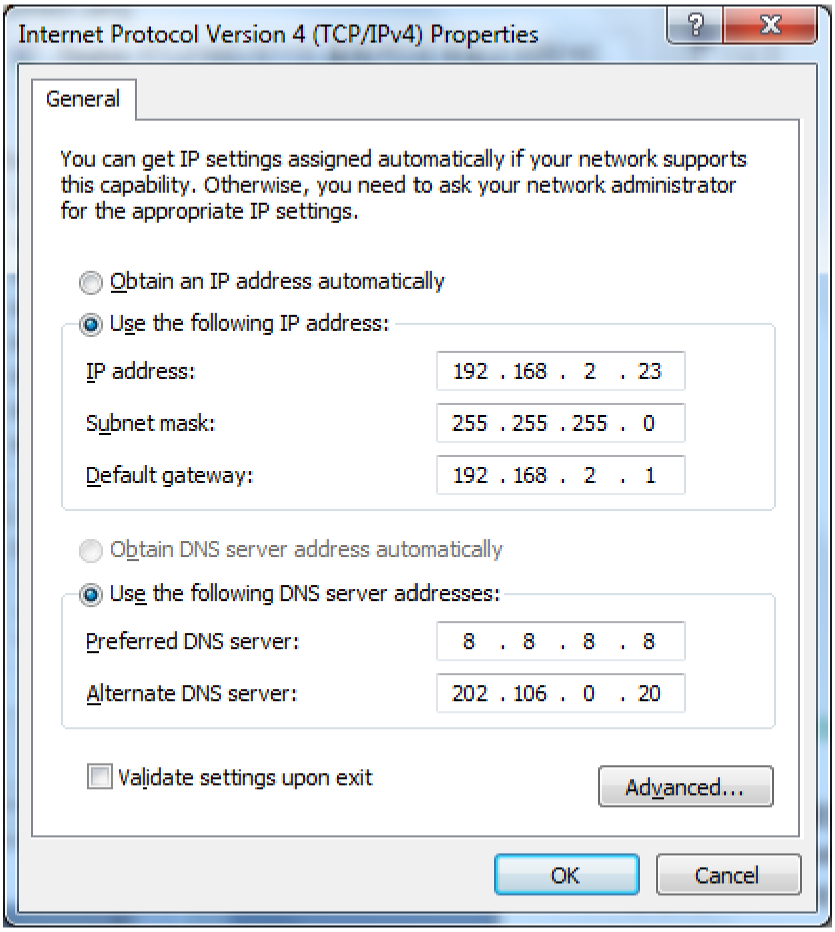
Alternate DNS server: . . .

□ Validate settings upon exit

2.1.2 Set a static IP address

Set computer management IP address and deviece FE port IP address on the same network segment (device FE port initial IP address: 192.168.2.1, Subnet Mask: 255.255.255.0). The following FE1/1 port connected to a computer and management provided in Windows XP system described as an example.

Enter “Internet Portocol (TCP/IP) Properties” page, select “Use the following IP address”, type IP address (arbitrary value between 192.168.2.2～192.168.2.254), Subnet Mask (255.255.255.0), and Defafult Gateway (192.168.2.1), then click <OK>to finish setting, as shown Figure 2-5.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

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

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 2 . 23

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 2 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8

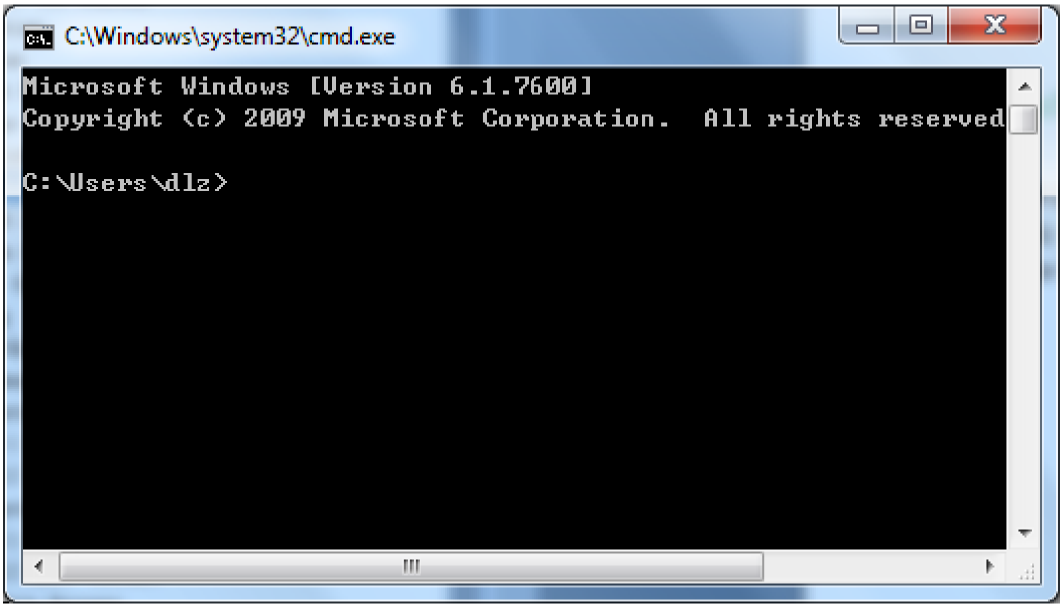
Alternate DNS server: 202 . 106 . 0 . 20

□ Validate settings upon exit

Figure 2-5 Internet Portocol (TCP/IP) Properties

2.2 Confirm that the network between the supervisory PC and router is connected

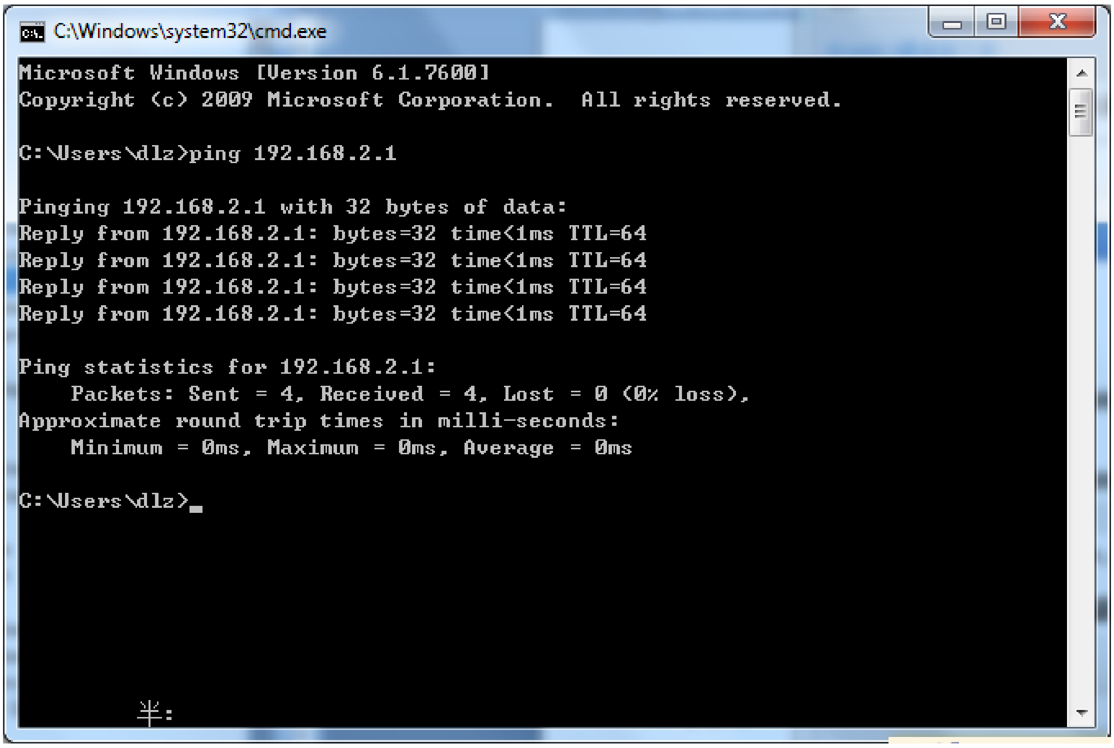
1) Click the lower left corner of the screen <Start> button to enter the "Start" menu, select "Run" pop-up "Run" dialog box, shown in Figure 2-6.



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved

C:\Users\dlz>
```

Figure 2-6 Run

2) Enter "ping 192.168.2.1 (IP address of router; it is the default IP address), and click the button <OK>. If the pop-up dialog box shows the response returned from the router side, it indicates that the network is connected; otherwise, check the network connection, shown in Figure 2-7.



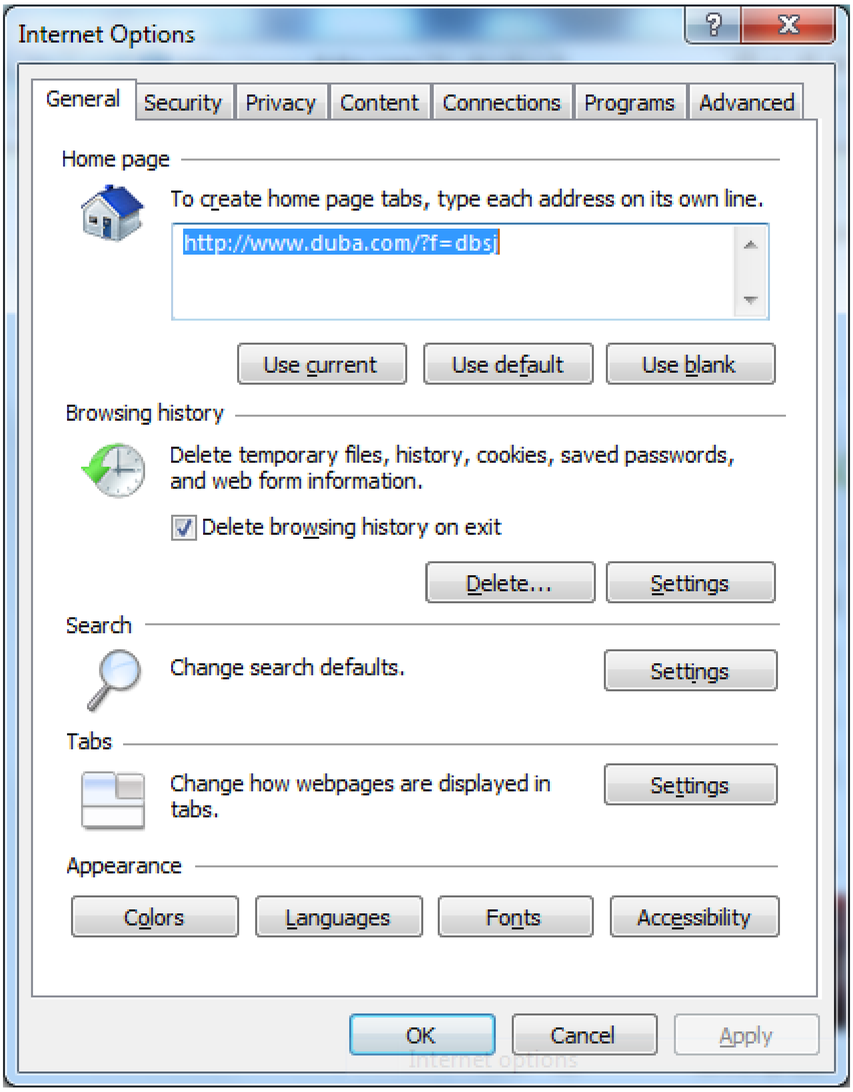
```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\dlz>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64
Reply from 192.168.2.1: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\dlz>_
```

Figure 2-7 Command Prompt

2.3 Cancel the Proxy Server

If the current supervisory computer uses a proxy server to access the Internet, it is required to cancel the proxy service and the operating steps are as follows:

1) Select [Tools/Internet OPtions] in the browser to enter the window of [Internet Options], shown in Figure 2-8.



Internet Options

Home page

To create home page tabs, type each address on its own line.

http://www.duba.com/?f=dbsj

Browsing history

Delete temporary files, history, cookies, saved passwords, and web form information.

☑ Delete browsing history on exit

Search

Change search defaults.

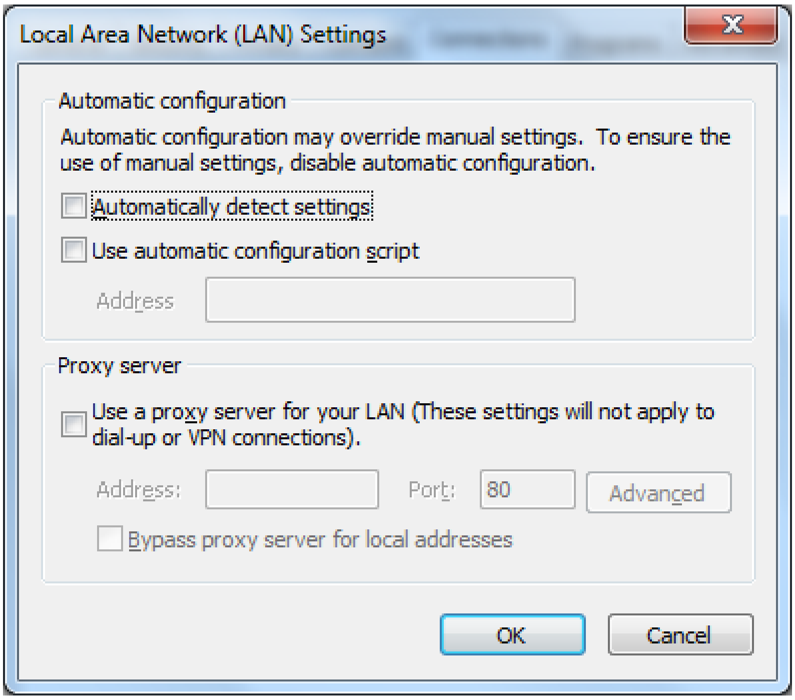
Tabs

Change how webpages are displayed in tabs.

Appearance

Figure 2-8 Internet OPtions

2）Select the tab”Connect” and click the button<LAN Setting(L)> to enter the page of “LAN Setting”.Please confirm if the option”Use a Proxy Server for LAN” is checked;if it is checked,please cancel and click the button<OK>, shown in Figure 2-9.



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address

Proxy server

□ Use a proxy server for your LAN (These settings will not apply to dial-up or VPN connections).

Address: Port: 80

□ Bypass proxy server for local addresses

Figure 2-9 LAN Setting

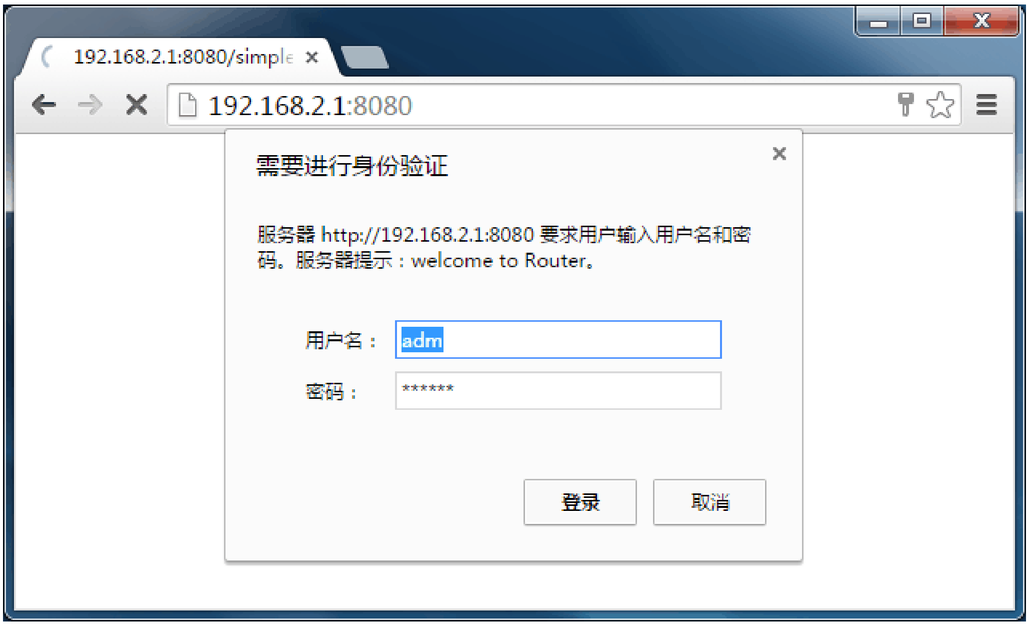
3. Web Configuration

This chapter includes the following parts:

- Login/out Web Configuration Page
- Management
- Network
- Link Backup
- Routing
- Tools
- Installation Guide
- Personalization Features
- Firewall
- Qos
- VPN

3.1 Login the Web Setting Page of Router

Run the Web browser, enter “http://192.168.2.1:8080” in the address bar, and press Enter to skip to the Web login page, as shown in Figure 3-1. Enter the “User Name” (default: adm) and “Password” (default: 123456), and click button <OK> or directly press Enter to enter the Web setting page.



需要进行身份验证

服务器 http://192.168.2.1:8080 要求用户输入用户名和密码。服务器提示：welcome to Router。

用户名：adm

密码：******

Figure 3-1 Login Router

After entering the Web Setting page, click the "Advanced Configuration" web interface, the pop-up dialog box, enter "User Name" (default: adm) again and "Password" (default: 123456), then enter the parameter configuration interface start parameter settings. Advanced configuration is shown in 3.2~3.11.

Instruction

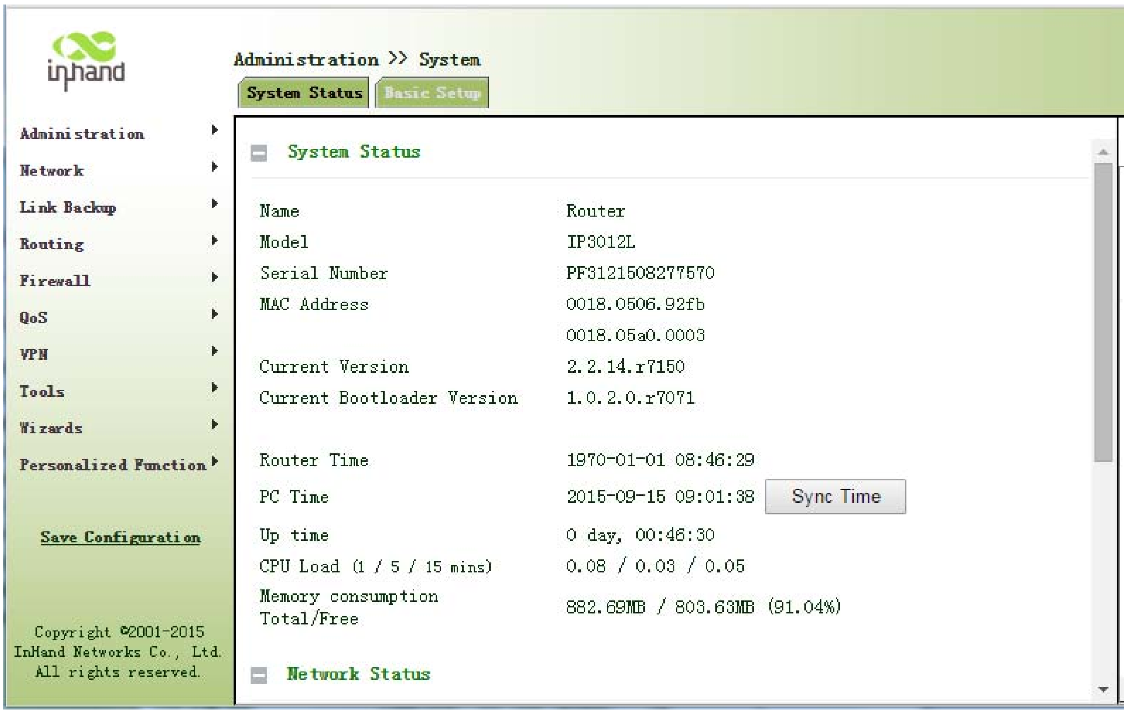
- At the same time, the router allows up to four users to manage through the Web setting page. When multi-user management is implemented for the router, it is suggested not to conduct configuration operation for the router at the same time; otherwise it may lead to inconsistent data configuration.
- For security, you are suggested to modify the default login password after the first login and safe keep the password information.

3.2 Management

3.2.1 System

3.2.1.1 System Status

From the left navigation panel, select Administration/System, then enter “System Status” page. On this page you can check system status and network status, as shown in Figure 3-2. In system status, by clicking <Sync Time>you can make the time of router synchronized with the system time of the host. Click the “Set” on network status to enter into the configuration screen directly. For configuration methods, refer to Section 3.3.2.



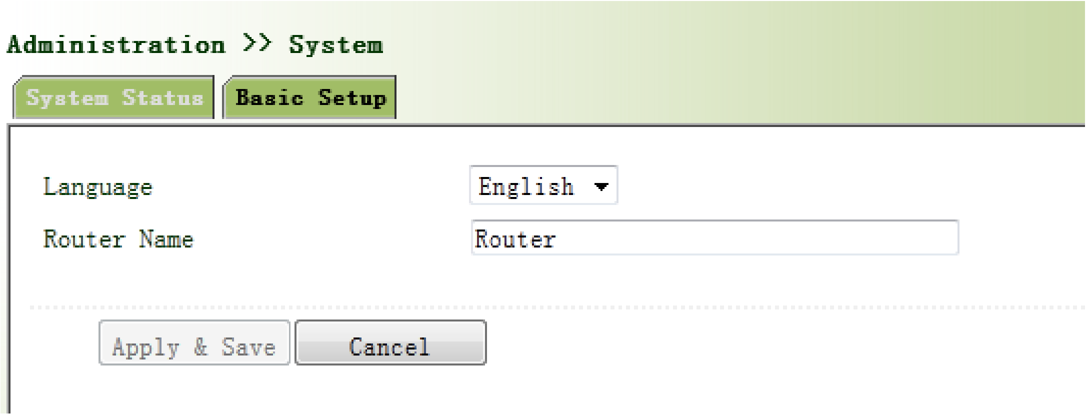
System Status

Name	Router
Model	IP3012L
Serial Number	PF3121508277570
MAC Address	0018.0506.92fb 0018.05a0.0003
Current Version	2.2.14.r7150
Current Bootloader Version	1.0.2.0.r7071
Router Time	1970-01-01 08:46:29
PC Time	2015-09-15 09:01:38
Up time	0 day, 00:46:30
CPU Load (1 / 5 / 15 mins)	0.08 / 0.03 / 0.05
Memory consumption Total/Free	882.69MB / 803.63MB (91.04%)

Figure 3-2 System Status

3.2.1.2 Basic Settings

Select Administration/System, then enter “Basic Setup” page. You can set the language of Web Configuration Page and define Router Name, as shown in Figure 3-3.



Language	English
Router Name	Router

Figure 3-3 Basic Settings

3.2.2 System Time

To ensure the coordination between this device and other devices, user is required to set the system time in an accurate way since this function is used to configure and check system time as well as system time zone.

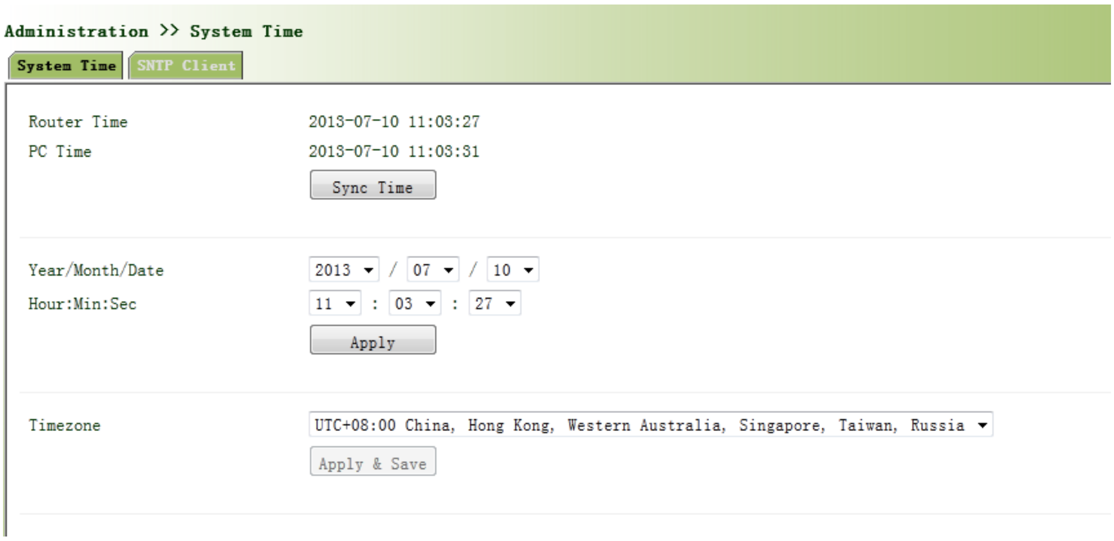
The device supports manual setting of system time and the time to pass self-synchronistic SNTP server.

3.2.2.1 System Time

Time synchronization of router with connected host could be set up manually in system time configuration part while system time is allowed to be set as any expected value after Year 2000 manually.

From the left navigation panel, select Administration/System Time, then enter “System Time” page, as shown in Figure 3-4.

By clicking <Sync Time>you can make the time of router synchronized with the system time of the host. Select the expected parameters in Year/Month/Date and Hour: Min: Sec Colum, then click <Apply & Save>. The router will immediately set the system time into expected value.



Administration >> System Time

Router Time 2013-07-10 11:03:27
PC Time 2013-07-10 11:03:31

Year/Month/Date 2013 / 07 / 10
Hour:Min:Sec 11 : 03 : 27

Timezone UTC+08:00 China, Hong Kong, Western Australia, Singapore, Taiwan, Russia

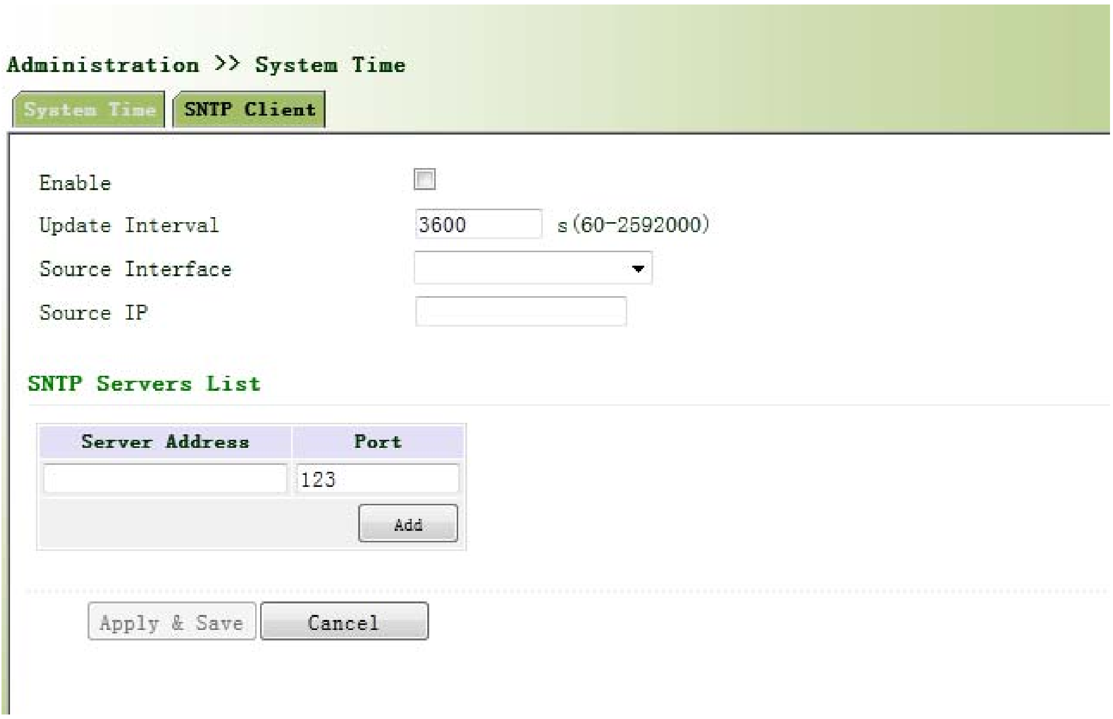
Figure 3-4 System Time

3.2.2.2 SNTP Client Port

SNTP, namely Simple Network Time Protocol, is a system for synchronizing the clocks of networked computers. In most places of the Internet today, SNTP provides accuracies of 1-50ms depending on the characteristics of the synchronization source and network paths.

The purpose of using SNTP is to achieve time synchronization of all devices equipped with a clock on network so as to provide multiple applications based on uniform time.

From the left navigation panel, select Administration/System Time, then enter “SNTP Client” page, as shown in Figure 3-5.



Administration >> System Time

Enable □

Update Interval 3600 s(60-2592000)

Source Interface

Source IP

SNTP Servers List

Server Address	Port
	123

Figure 3-5 SNTP Client Port

Page description is shown in Table 3-1.

Table 3-1 SNTP Client Port Page Description

Parameter	Description	Default
Source IP	The corresponding IP of source interface	None
SNTP Servers List		
Server Address	SNTP server address (domain name /IP), maximum to set10 SNTP server	None
Port	The service port of SNTP server	123

Attention

- Before setting a SNTP server, should ensure SNTP server reachable. Especially when the IP address of SNTP server is domain, should ensure DNS server has been configured correctly.
- If you configure a source interface and then cannot configure the source address. the opposite is also true.

Instruction

When setting multiple SNTP server, system will poll all SNTP servers until find an available SNTP server.

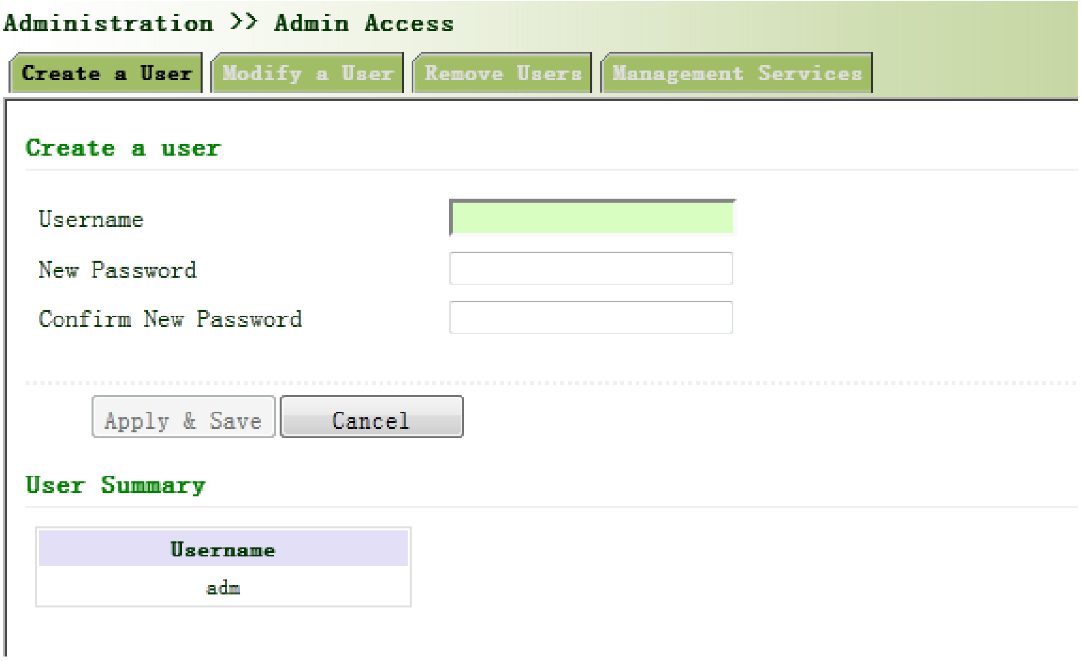
3.2.3 Admin Access

Admin Access allows the management of users which are categorized into superuser and common user.

- Superuser: only one automatically created by the system, allocated with the user name of adm and granted with all access rights to the router.
- Common user: created by superuser with the right to check rather then modify router configuration.

3.2.3.1 Create a user

Click navigation panel/Admin Access, enter “Create a user” page, Wherein the user permissions value, the higher the privilege, shown in Figure 3-6.

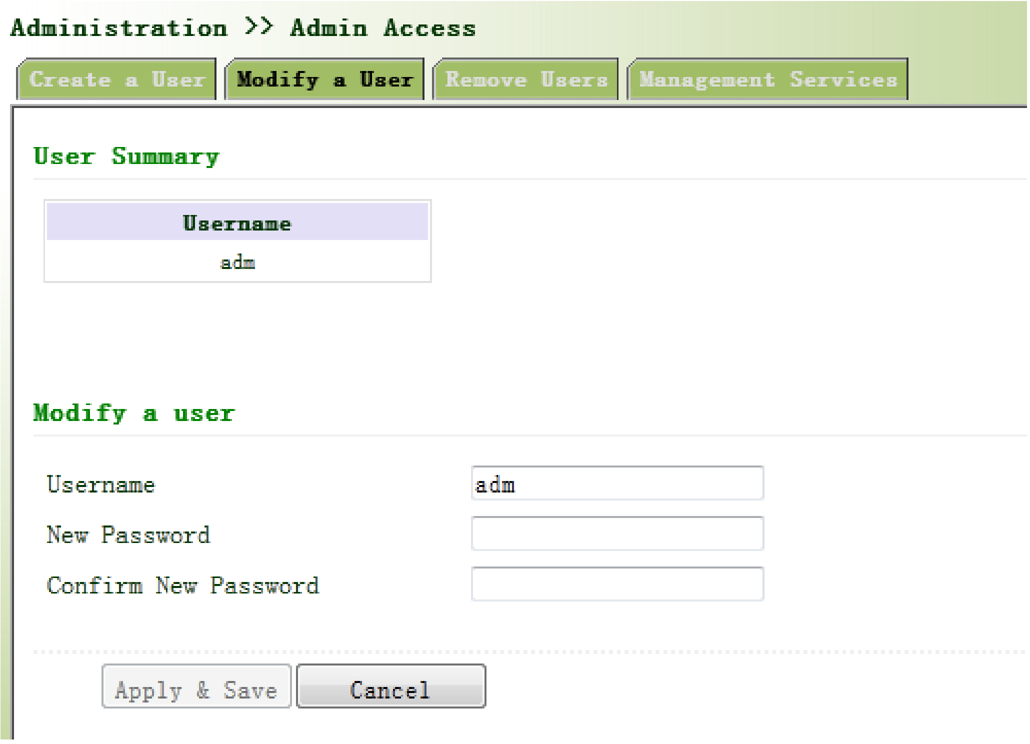


Username
adm

Figure 3-6 Create a user

3.2.3.2 Modify a User

From the left navigation panel, select Administration/Admin Access, then enter “Modify a User” page, as shown in Figure 3-7.Press the user that needs to modify in “User Summary”, after the background turns blue, enter new information in “Modify a User”.



User Summary

Username
adm

Modify a user

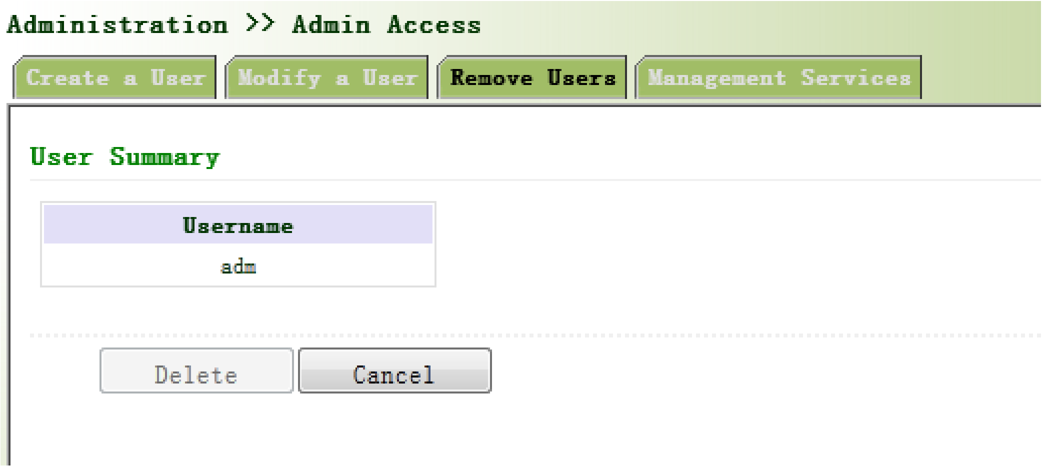
Username	adm
New Password	
Confirm New Password	

Figure 3-7 Modify a User

3.2.3.3 Remove Users

From the left navigation panel, select Administration/Admin Access, then enter “Remove Users” page, as shown in Figure 3-8.

Press the user that needs to remove in”User Summary”. After the background turns blue, press <Delete> to remove the user.



User Summary

Username
adm

Figure 3-8 Remove Users

Instruction

The super user (adm) can neither be modified nor deleted. But super user's password can be modified.

3.2.3.4 Management Service

HTTP

HTTP, shortened form of Hypertext Transfer Protocol, is used to transmit Web page information on Internet. HTTP is located as the application layer in TCP/IP protocol stack.

Through HTTP, user could log on the device to access and control it through Web.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) supports HTTP in SSL (Security Socket Layer).

HTTPS, depending on SSL, is able to improve the device's security through following aspects:

- Distinguish legal clients from illegal clients through SSL and Disable illegal clients to access the device;
- Encrypt the data exchanged between client and device to guarantee security and integrality of data transmission so as to achieve the safe management of device;
- An access control strategy based on certificate attributions is established for further control of client's access authority so as to further avoid attack for illegal clients.

TELNET

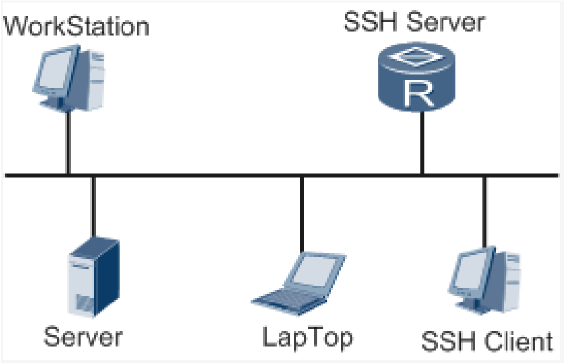
Telnet is an application layer protocol in TCP/IP protocol family, providing telnet and VT functions through Web. Depending on Server/Client, Telnet Client could send request to Telnet server which provides Telnet services. The device supports Telnet Client and Telnet Server.

SSH

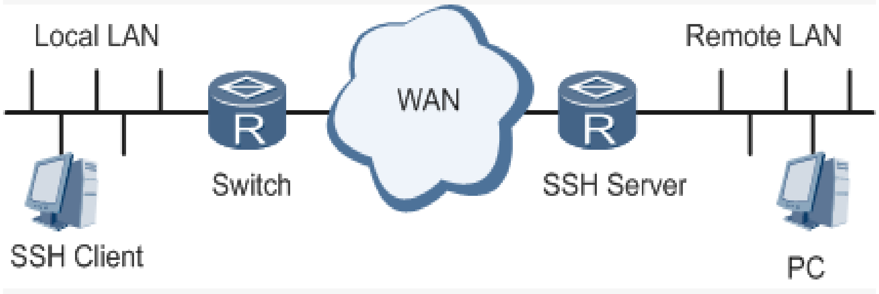
In comparison with Telnet, STelnet (Secure Telnet), based on SSH2, allows the Client to negotiate with Server so as to establish secure connection. Client could log on Server just as operation of Telnet.

Through following measures SSH will realize the secure telnet on insecure network:

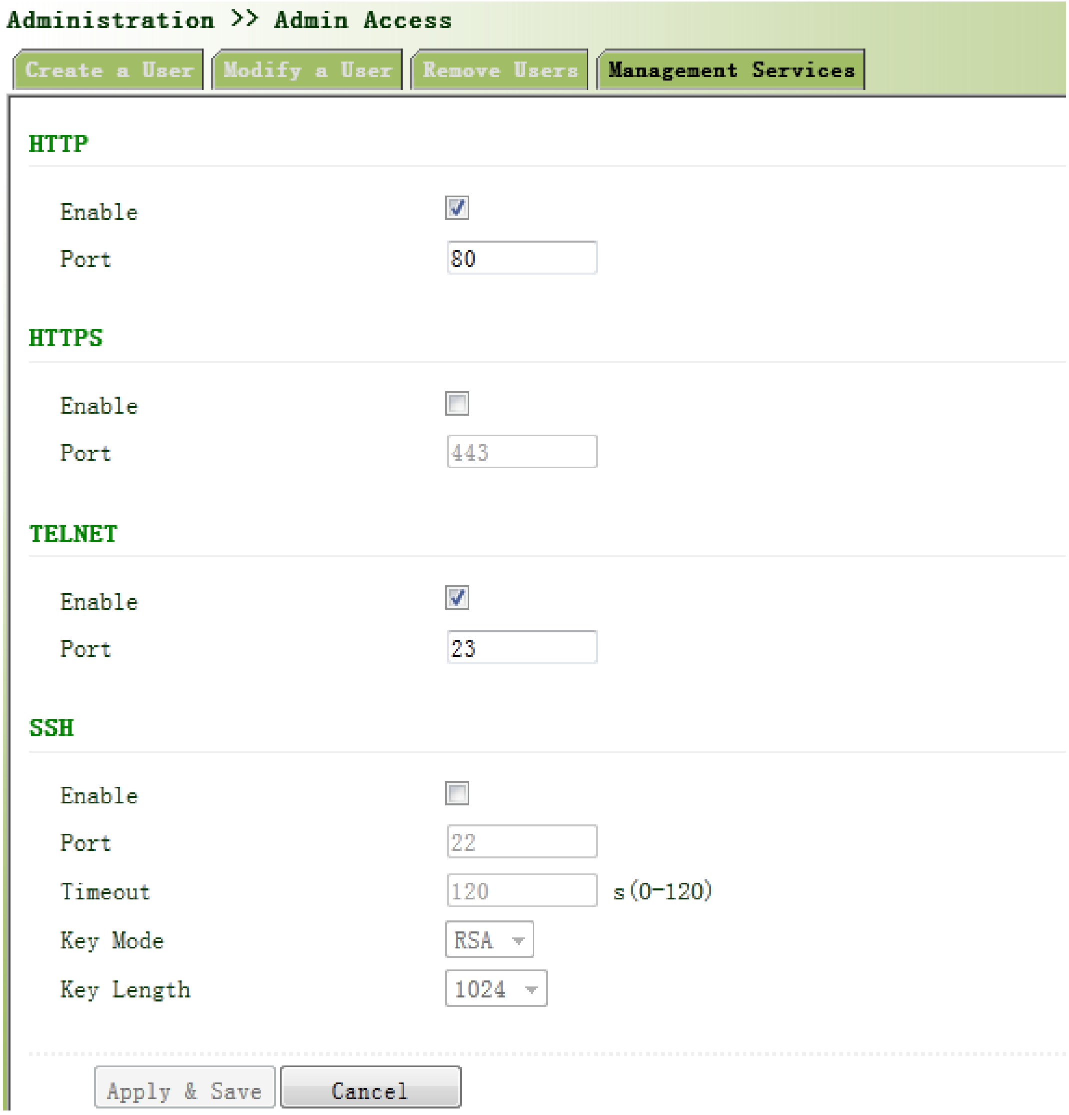
- Support RAS authentication.
- Support encryption algorithms such as DES, 3DES and AES128 to encrypt username password and data transmission.
- Local connection. A SSH channel could be established between SSH Client and SSH Server to achieve local connection. Following is a figure showing the establishment of a SSH channel in LAN:



- WAN connection. A SSH channel could be established between SSH Client and SSH Server to achieve WAN connection. Following is a figure showing the establishment of a SSH channel in WAN:



From the left navigation panel, select Administration/Admin Access, then enter “Management Service” page, as shown in Figure 3-9.



HTTP

Enable ☑

Port 80

HTTPS

Enable □

Port 443

TELNET

Enable ☑

Port 23

SSH

Enable □

Port 22

Timeout 120 s(0-120)

Key Mode RSA

Key Length 1024

Figure 3-9 Management Service

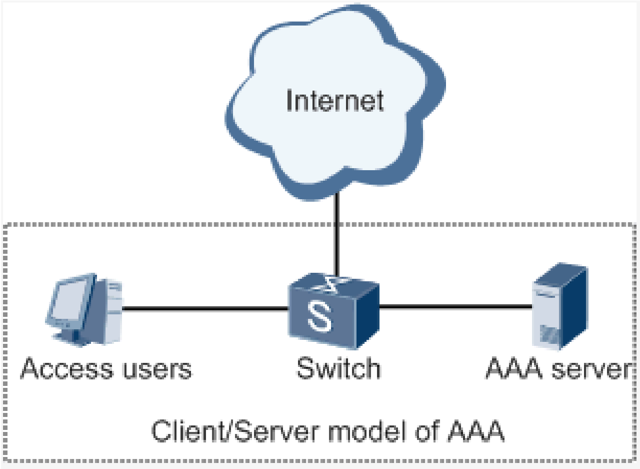
3.2.4 AAA

AAA access control is used to control visitors and corresponding services available as long as access is allowed. Same method is adopted to configure three independent safety functions. It provides modularization methods for following services:

- Authentication: verify whether the user is qualified to access to the network.
- Authorization: related with services available.
- Charging: records of the utilization of network resources.。

User may only use one or two safety services provided by AAA. For example, the company just wants identity authentication when employees are accessing to some specified resources, then network administrator only needs to configure authentication server. But if recording of the utilization of network is required, then, a charging server shall be configured.

Commonly AAA adopts "Client—Server" structure which is featured by favorable expandability and facilitates centralized management of users' information, as the following figure shows:

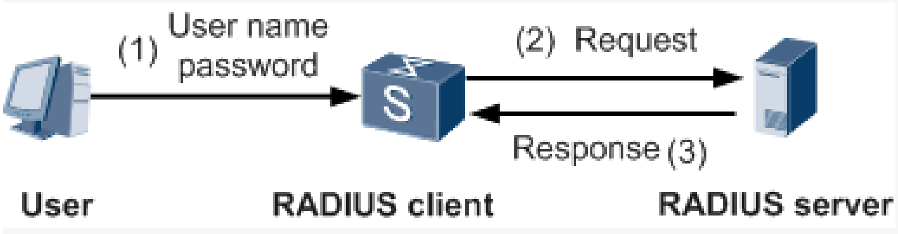


3.2.4.1 Radius

Remote Authentication Dial-in User Service (RADIUS), an information exchange protocol with a distributive Client/Server structure, could prevent the network from any disturbance from unauthorized access and is generally applied in various network environments with higher requirements on security and that permit remote user access. The protocol has defined the Radius frame format based on UDP and information transmission mechanism, confirmed UDP Port 1812 as the authentication port. Radius Server generally runs on central computer or workstation; Radius Client generally is located on NAS.

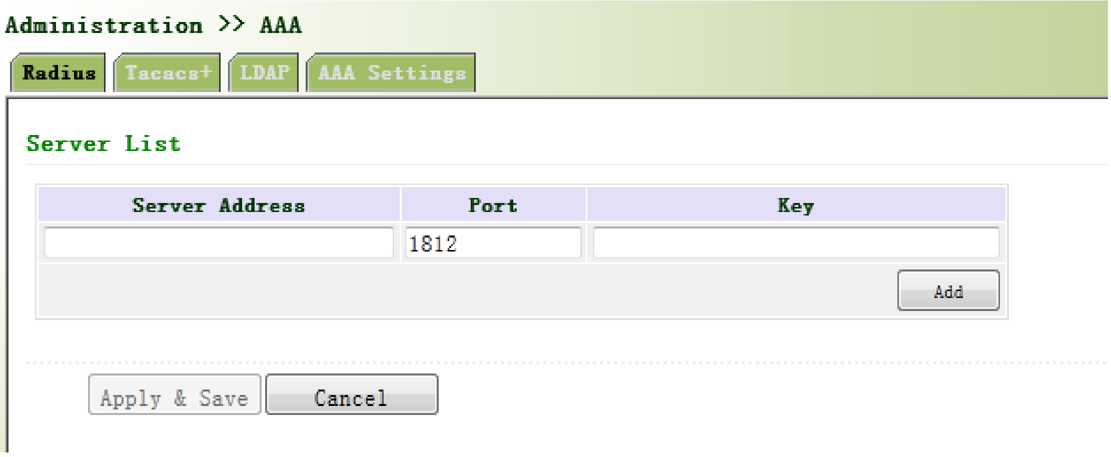
Initially Radius is designed and developed against AAA protocol of dial-in users. Along with the diversified development of user access ways, Radius also adapts itself to such changes, including Ethernet access and ADSL access. Access service is rendered through authentication and authorization.

Message flow between Radius Client and Server is shown as follows:



- User name and passport will be sent to the NAS when the user logs on it;
- Radius Client on NAS receives username and password and then sends an authentication request to Radius Server;
- Upon the reception of legal request, Radius Server executes authentication and feeds back required user authorization information to Client; For illegal request, Radius Server will feed back Authentication Failed to Client.

From the left navigation panel, select Administration/AAA, then enter “Radius” page, as shown in Figure 3-10.



Server List

Server Address	Port	Key
	1812	

Figure 3-10 Radius

Page description is shown in Table 3-2.

Table 3-2 Radius Description

Parameter	Description	Default
Server Address	Server address (domain name / IP)	None
Port	Consistent with the server port	1812
Key	Consistent with the server authentication key	None

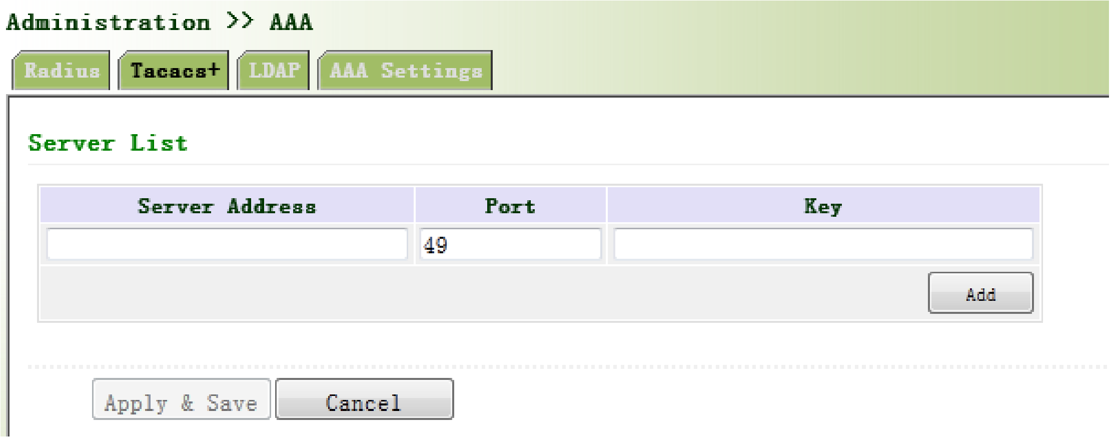
3.2.4.2 Tacacs+

Tacacs+, or Terminal Access Controller Access Control System, similar to Radius, adopts

Client/Server mode to achieve the communication between NAS and Tacacs+ Server. But, Tacacs+ adopts TCP while Radius adopts UDP.

Tacacs+ ismainly used for authentication, authorization and charging of access users and terminal users adopting PPP and VPDN. Its typical application is authentication, authorization and charging for terminal users requiring logging on the device to carry out operation. As the Client, the device will have username and password sent to Tacacs+ Server for verification. So long as user verification passed and authorization obtained, logging and operation on the device are allowed.

From the left navigation panel, select Administration/AAA, then enter "Tacacs+" page, as shown in Figure 3-11.



Server Address	Port	Key
	49	

Figure 3-11 Tacacs+

Page description is shown in Table 3-3.

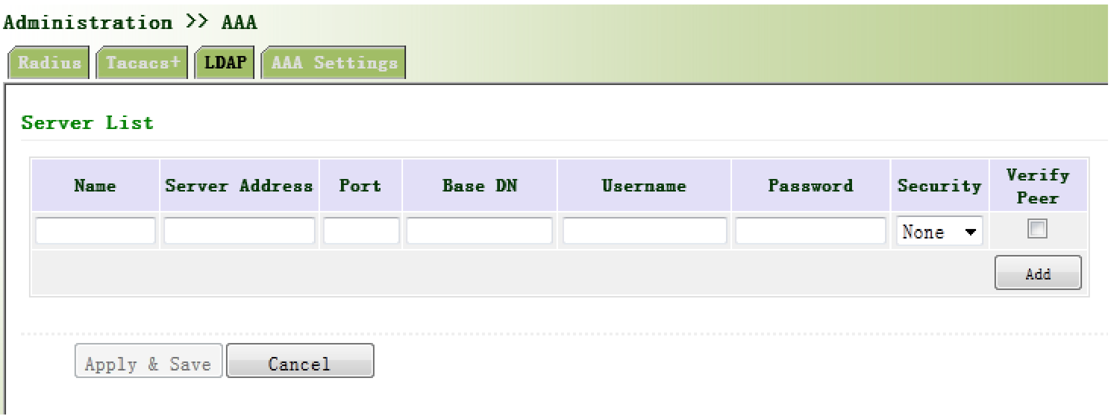
Table 3-3 Tacacs+ Description

Parameters	Description	Default
Server Address	Server address (domain name / IP)	None
Port	Consistent with the server port	49
Key	Consistent with the server authentication key	None

3.2.4.3 LDAP

One of the great advantages of LDAP is rapid response to users' searching request. For instance, user's authentication which may general a large amount of information sent as the same time. If database is adopted for this purpose, since it is divided into many tables, each time to meet such a simple requirement, the whole database has to be searched, integrated and filtered slowly and disadvantageously. LDAP, simple as a table, only requires username and command and something else. Authentication is met from efficiency and structure.

From the left navigation panel, select Administration/AAA, then enter “LDAP” page, as shown in Figure 3-12.



Server List

Name	Server Address	Port	Base DN	Username	Password	Security	Verify Peer
						None	☐

Figure 3-12 LDAP

Page description is shown in Table 3-4.

Table 3-4 LDAP Description

Parameters	Description	Default
Name	Define server name	None
Server Address	Server address (domain name / IP)	None
Port	Consistent with the server port	None
Base DN	The top of LDAPdirectory tree	None
Username	Username accessing the server	None
Password	Password accessing the server	None
Security	Encryption mod: None,SSL,StartTLS	None
Verify Peer	Verify Peer	Unopened

3.2.4.4 AAA Settings

AAA supports following authentication ways:

- None: with great confidence to users, legal check omitted, generally not recommended.
- Local: Have user’s information stored on NAS. Advantages: rapidness, cost reduction.

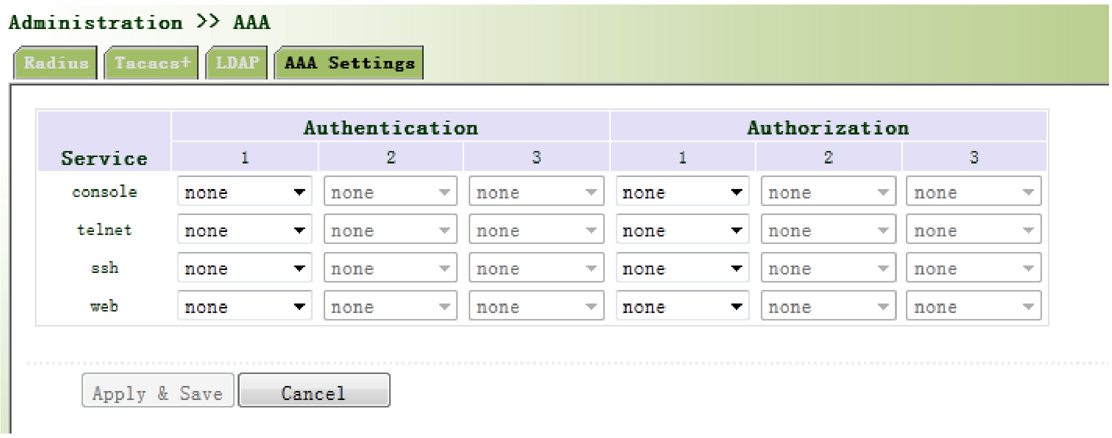
Disadvantages: storage capacity limited by hardware.

- Remote: Have user's information stored on authentication server. Radius, Tacacs+ and LDAP supported for remote authentication.

AAA supports following authorization ways:

- None: authorization rejected.
- Local: authorization based on relevant attributions configured by NAS for local user's account.
- Tacacs+: authorization done by Tacacs+ Server.
- Radius Authentication Based: authentication bonded with authorization, authorization only by Radius not allowed.
- LDAP Authorization.

From the left navigation panel, select Administration/AAA, then enter "AAA Setting" page, as shown in Figure 3-13.



Service	Authentication			Authorization		
	1	2	3	1	2	3
console	none	none	none	none	none	none
telnet	none	none	none	none	none	none
ssh	none	none	none	none	none	none
web	none	none	none	none	none	none

Figure 3-13 AAA authentication

Page description is shown in Table 3-5.

Table 3-5 AAA Settings Key Items

Key Items	Description
radius	Authentication and Authorization Server
tacacs+	Authentication and Authorization Server
ldap	Authentication and Authorization Server
local	The local username and password

Attention

Authentication 1 should be set consistently with Authorization 1; Authentication 2 should be set consistently with Authorization 2; Authentication 3 should be set consistently with Authorization 3.

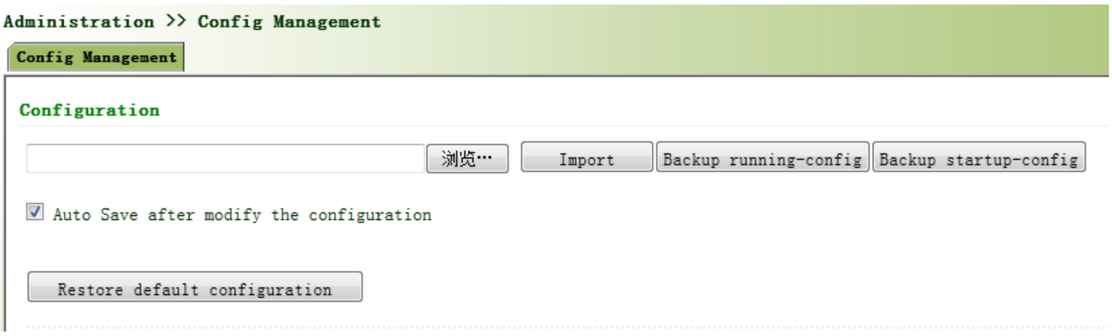
Instruction

When configure radius, Tacas+, local at the same time, priority order follow:1 >2 >3.

3.2.5 Configuration Management

Here you can back up the configuration parameters, import the desired parameters configuration backup and restore the factory settings of the router.

From the left navigation panel, select Administration/Config Management, then enter “Config Management” page, as shown in 3-14.



☑ Auto Save after modify the configuration

Figure 3-14 Configuration Management

Page description is shown in Table 3-6.

Table 3-6 Config Management Description

Parameters	Description	Default
Backup running-config	Backup running-config file to host.	None
Backup startup-config	Backup startup-config file to host.	None
Automatically save modified configuration	Decide whether to automatically save configuration after modify the configuration.	On
Restore Default Configuration	Restore factory configuration	None

Attention

When import the configuration, the system will filter incorrect configuration files, and save the correct configuration files, when system restarts, it will orderly execute theses configuration files. If the configuration files didn’t be arranged according to effective order, the system won’t enter the desired state.

Instruction

In order not to affect current system running, when performing the import configuration and restore the default configuration, need to reboot the router new configuration will take effect.

3.2.6 SNMP

Definition

SNMP, or Simple Network Management Protocol, is a standard network management protocol widely used in TCP/IP networks and provides a method of managing the device through the running the central computer of network management software. Features of SNMP:

- Simplicity: SNMP adopts polling mechanism, provides the most basic sets of features and could be used in small-scale, rapid, low cost environments. SNMP, with UDP message as the carrier, is supported by a great majority of devices.
- Powerfulness: objective of SNMP is to ensure the transmission of management information between any two points so as to facilitate administrator’s retrieval of information on any node on network and modification and troubleshooting.

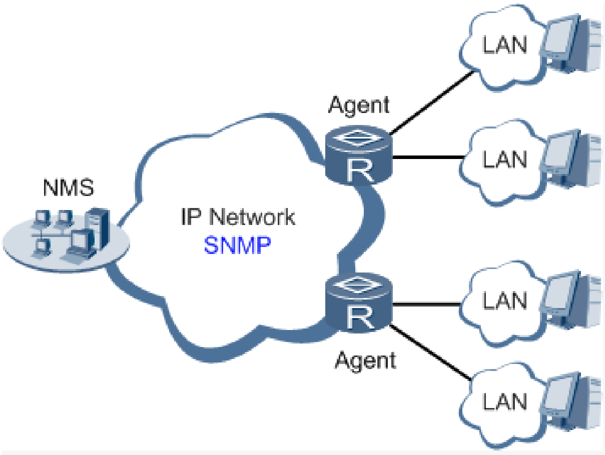
Benefits

- Network administrators could make use of SNMP to accomplish the information query, modification, troubleshooting and other jobs on any node on network to achieve higher efficiency.
- Shielding of physical differences between devices. SNMP only provides the most basic sets of features for mutual independence between administration and the physical properties, network types of devices under administration; therefore, it could realize the uniform management of different devices at a lower cost.

- Simple design, lower cost. Simplicity is stressed on addition of software/hardware, types and formats of message on devices so as to minimize the influence and cost on devices caused by running SNMP.

Application: management of device is achieved through SNMP

Administrator is required to carry out configuration and management of all devices in the same network, which are scattered, making onsite device configuration impracticable. Moreover, in case that those network devices are supplied from different sources and each source has its independent management interfaces (for example, different command lines), the workload of batch configuration of network devices will be considerable. Therefore, under such circumstances, traditional manual ways will result in lower efficiency at higher cost. At that time, network administrator would make use of SNMP to carry out remote management and configuration of attached devices and achieve real-time monitoring. Following is a figure showing how to manage devices through SNMP:



To configure SNMP in networking, NMS, a management program of SNMP, shall be configured at the Manager. Meanwhile, Agent shall be configured as well.

Through SNMP:

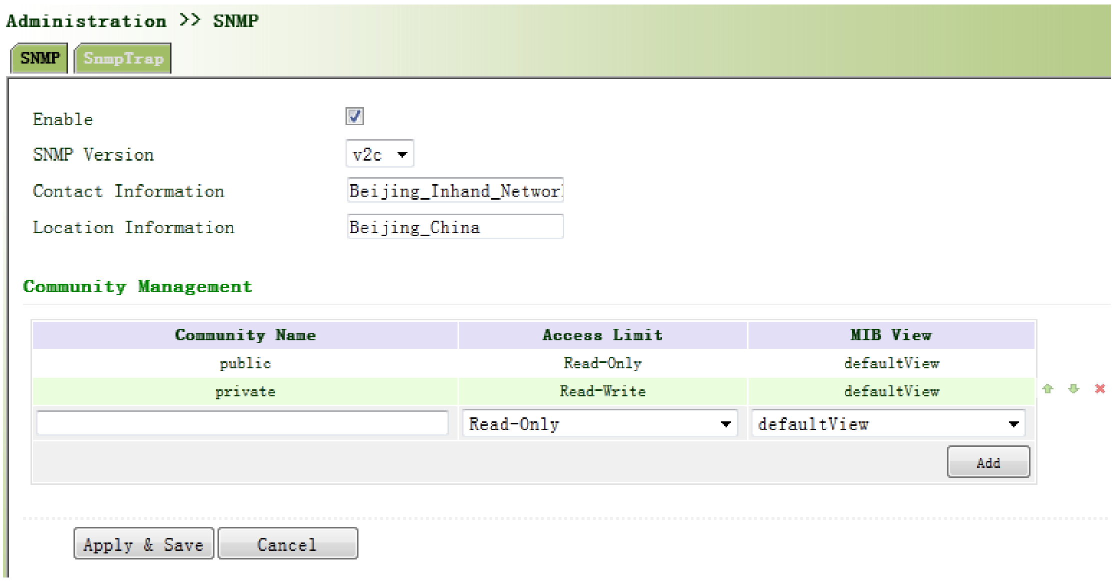
- NMS could collect status information of devices whenever and wherever and achieve remote control of devices under management through Agent.
- Agent could timely send current status information to NMS report device. In case of any problem, NMS will be notified immediately.

3.2.6.1 SNMP

SNMP agent of device supports SNMPv1, SNMPv2 and SNMPv3 at present.

- SNMPv1 and SNMPv2 adopt community name to authenticate.
- SNMPv3 adopt username and password to authenticate.

From the left navigation panel, select Administration/SNMP, then enter “SNMP” page, as shown in Figure 3-15.



Administration >> SNMP

Enable ☑
SNMP Version v2c
Contact Information Beijing_Inhand_Networ
Location Information Beijing_China

Community Management

Community Name	Access Limit	MIB View
public	Read-Only	defaultView
private	Read-Write	defaultView
	Read-Only	defaultView

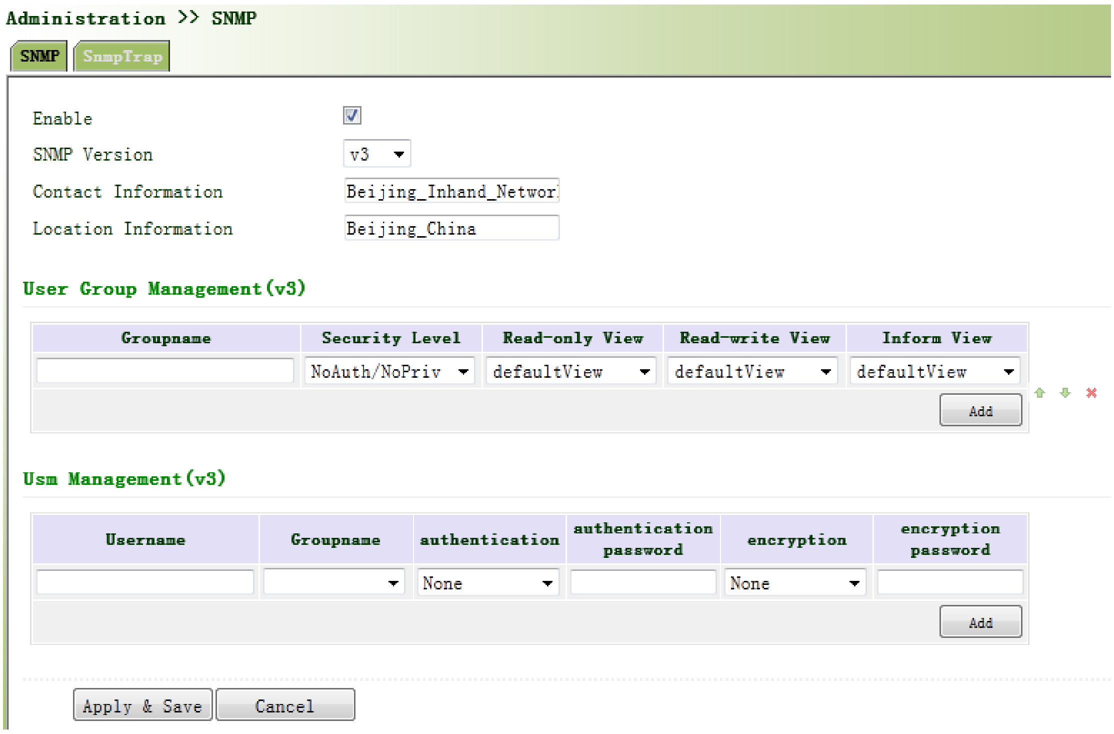
Figure 3-1 SNMPv1&SNMPv2c Settings

Page description is shown in Table 3-7.

Table 3-7 SNMP Key Items

Parameters	Description	Default
Community Name	User define Community Name	Public and private
Access Limit	Select access limit	Read-only
MIB View	Select MIB View	defaultView

When choosing SNMPv3 version, the corresponding Use and User Group should be configured. The configuration page is shown in Figure 3-16.



Enable ☑

SNMP Version v3

Contact Information Beijing_Inhand_Networ

Location Information Beijing_China

User Group Management(v3)

Groupname	Security Level	Read-only View	Read-write View	Inform View
	NoAuth/NoPriv	defaultView	defaultView	defaultView

Usm Management(v3)

Username	Groupname	authentication	authentication password	encryption	encryption password
		None		None	

Figure 3-16 SNMPv3 Setting

Page description is shown in Table 3-8.

Table 3-8 SNMPv3 Description

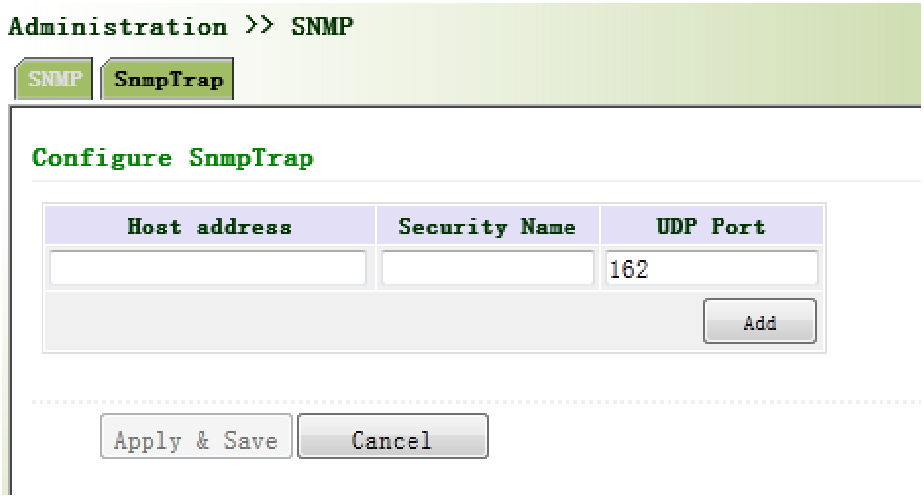
Parameters	Description	Default
Group Management		
Group name	User define, length:1-32 charaters	None
Security Level	Includes NoAuth/NoPriv, Auth/NoPriv, Auth/priv	NoAuth/NoPriv
Read-only View	Only support defaultView at present	defaultView
Read-write View	Only support defaultView at present	defaultView
Inform View	Only support defaultView at present	defaultView
User Management		
User name	User-defined user name, length: 1-32 characters	None
Group Name	Select user to join user group, first defined in the user group management table, before this, select appropriate user group	None
Authentication Mode	Select authentication mode. MD5 and SHA provides two authentication modes, “no identification" not enable authentication.	SHA
Authentication password	When only authentication mode is not "no identification", authentication password can enter. Length: 8-32 characters.	None
Encryption mode	Choose whether to use DES encryption mode	DES

Encryption Password	Only encryption mode is not "no encryption", encryption mode password can enter. Length: 8-32 characters.	None

3.2.6.2 SnmpTrap

SNMP trap: A certain port where devices under the management of SNMP will notify SNMP manager rather than waiting for polling from SNMP manager. In NMS, Agents in managed devices could have all errors reported to NMW at any time instead of waiting for polling from NMW after its reception of such errors which, as a matter of fact, are the well-known SNMP traps.

From the left navigation panel, select Administration/SNMP, then enter “SnmpTrap” page, as shown in Figure 3-17.



Configure SnmpTrap

Host address	Security Name	UDP Port
		162

Figure 3-17 SnmpTrap

Page description is shown in Table 3-9.

Table 3-9 SnmpTrap Description

Parameters	Description	Default
Host Address	Fill in the NMS IP address	None
Securtiy Name	Fill in the groupname when use the SNMP v1/v2c; Fill in the username when use the SNMP v3. Length :1-32 characters	None
UDP Port	Fill in UDP port, the default port range is 1-65535	162

3.2.7 Alarm

Alarm function is a way which is provided for users to get exceptions of device, which can make the users find and solve exceptions as soon as possible. When abnormality happened, device will send alarm. User can choose many kinds of exceptions which system defined and choose appropriate notice way to get these exceptions. All the exceptions should be recorded in alarm log so that user troubleshoot problem.

Alarm can be divided:

- Raise: Indicates the alarm occurrence has not been confirmed.
- Confirm: Alarm indicates that a user can not temporary solve.
- All: Indicates all alarms occur.

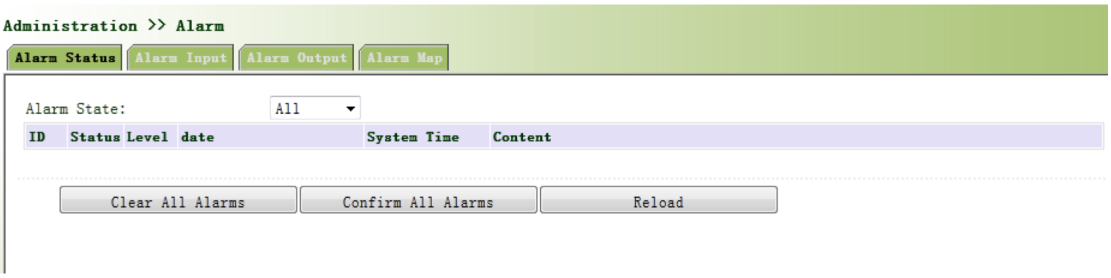
Alarm level can be divided:

- EMERG： Device occurs some faults, it could lead to the system restart.
- CRIT： Device occurs some faults which are unrecoverable.
- WARN： Device occurs some faults which could affect system function.
- NOTICE： Device occurs some faults which could affect system properties.
- INFO： Device occurs some normal events.

3.2.7.1 Alarm Status

From the left navigation panel, select Administration/Alarm, then enter “Alarm State” page, as shown in Figure 3-18. Through this page, you can check all the alrms since the router is powered.

- Click <Clear All Alarms> to set all the alarm to “clear” state.
- Click<Confirm All Alarms> to set all the alarm to “cconfirm” state.
- Click<Reload> to reload all the alarms.



Alarm State: All

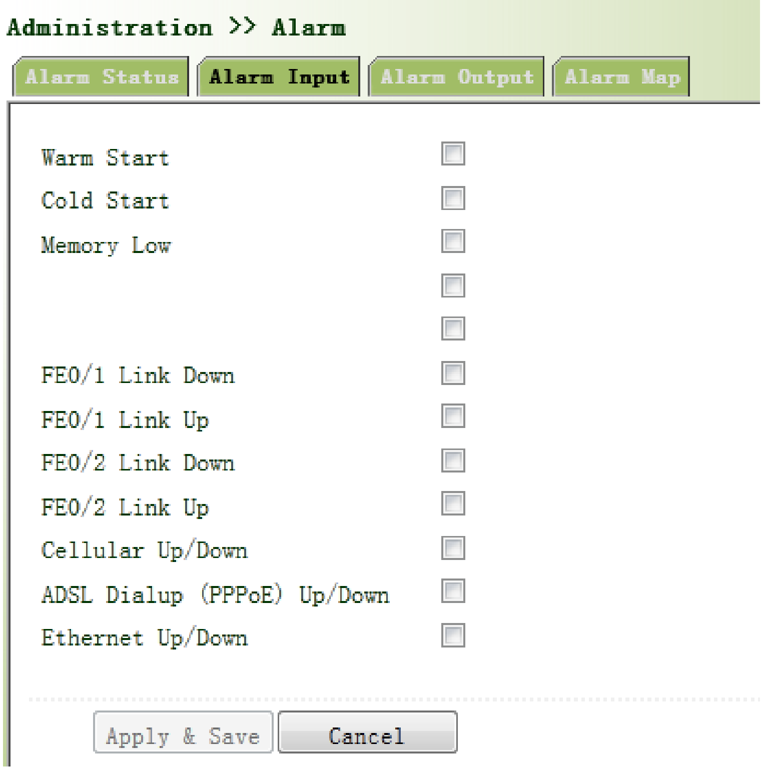
ID	Status	Level	date	System Time	Content

Figure 3-18 Alarm Status

3.2.7.2 Alarm Input

Here user could select alarm types including system alarm and port alarm. One or more than one types could be selected.

From the left navigation panel, select Administration/Alarm, then enter “Alarm Input” page, as shown in Figure 3-19.


Administration >> Alarm

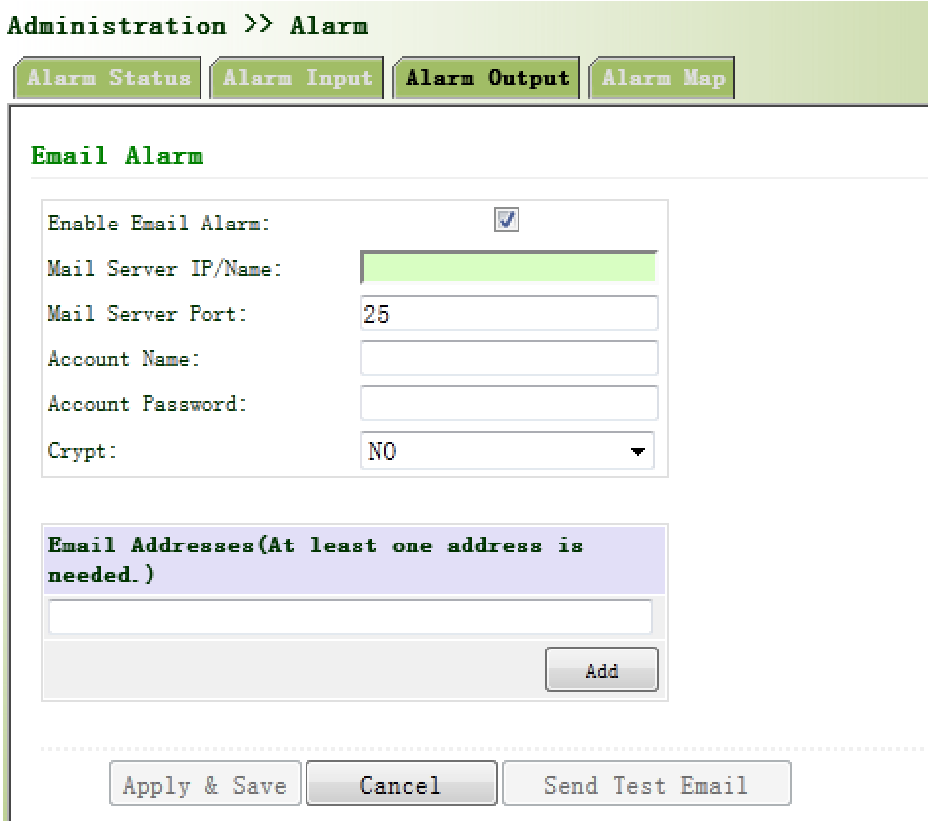
Warm Start □
Cold Start □
Memory Low □
□
□
FE0/1 Link Down □
FE0/1 Link Up □
FE0/2 Link Down □
FE0/2 Link Up □
Cellular Up/Down □
ADSL Dialup (PPPoE) Up/Down □
Ethernet Up/Down □

Figure 3-19 Alarm Input

3.2.7.3 Alarm Output

When an alarm happens, the system configured with this function will send the alarm content to intended email address from the mail address where an alarm email is sent in a form of email. Generally this function is not configured.

From the left navigation panel, select Administration/Alarm, then enter “Alarm Output” page, as shown in Figure 3-20.



Administration >> Alarm

Email Alarm

Enable Email Alarm: ☑

Mail Server IP/Name:

Mail Server Port: 25

Account Name:

Account Password:

Crypt: NO

Email Addresses(At least one address is needed.)

Figure 3-20 Alarm Output

Page description is shown in Table 3-10.

Table 3-10 Alarm Output Description

Parameters	Description	Default
Mail Server IP/Name	Set IP address of Mail Server that send alarm emails	None
Mail Server Port	Set Port of Mail Server that send alarm emails	25
Account Name	Set Email address from which alarm emails are sent	None
Account Password	Set Email password	None
Crypt	Set the crypt method	None
Email Addresses	Destination address of receiving alarm email (1-10)	None

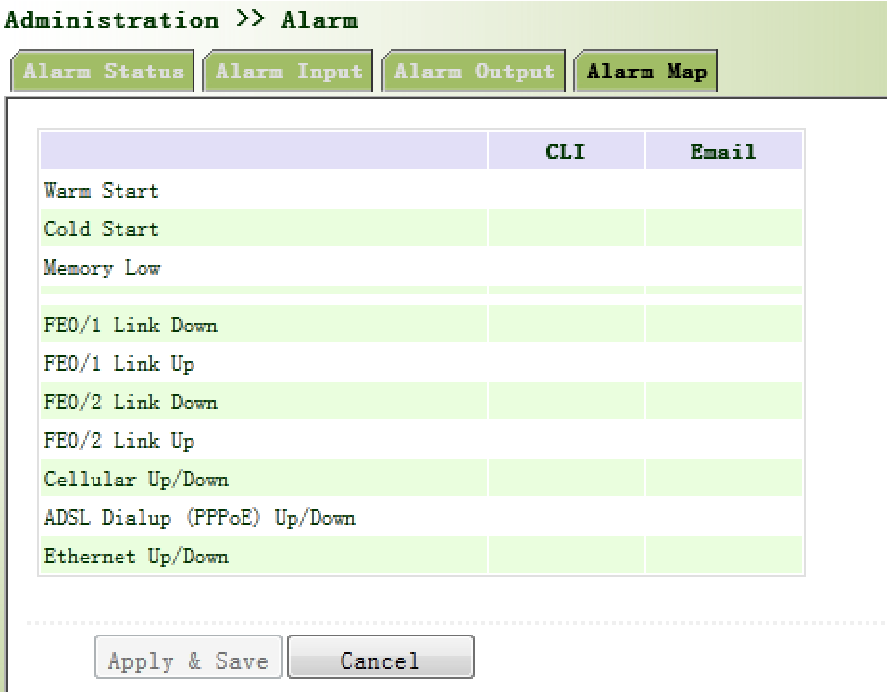
⚠ **Attention**

When the email parameters had been configured, you should click the “send test email” button so that ensure the configuration is correct. If the test email failed, it may the network configuration or mailbox configuration is not correct.

3.2.7.4 Alarm Map

Alarm Map consists of two mapping ways: CLI (console interface)and Email. In case of latter one is selected, and then alarm output shall be activated with an email address well configured.

From the left navigation panel, select Administration/Alarm, then enter “Alarm Map” page, as shown in Figure 3-21.



	CLI	Email
Warm Start		
Cold Start		
Memory Low		
FE0/1 Link Down		
FE0/1 Link Up		
FE0/2 Link Down		
FE0/2 Link Up		
Cellular Up/Down		
ADSL Dialup (PPPoE) Up/Down		
Ethernet Up/Down		

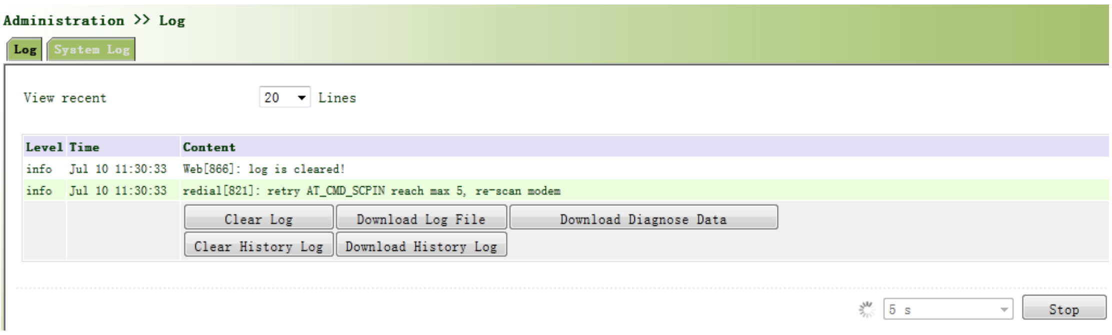
Figure 3-21 Alarm Map

3.2.8 System Log

System Log includes massive information about network and devices, including operating status, configuration changes and so on, serving as an important way for network administrator to monitor and control the operation of network and devices. System Log could provide information to help network administrator to find network problems or safety hazard so as to take more targeted measures.

3.2.8.1 System Log

From the left navigation panel, select Administration/Log, then enter “System Log” page, as shown in Figure 3-22.



View recent 20 Lines

Level	Time	Content
info	Jul 10 11:30:33	Web[866]: log is cleared!
info	Jul 10 11:30:33	redial[821]: retry AT_CMD_SCPIN reach max 5, re-scan modem

5 s

Figure 3-22 System Log

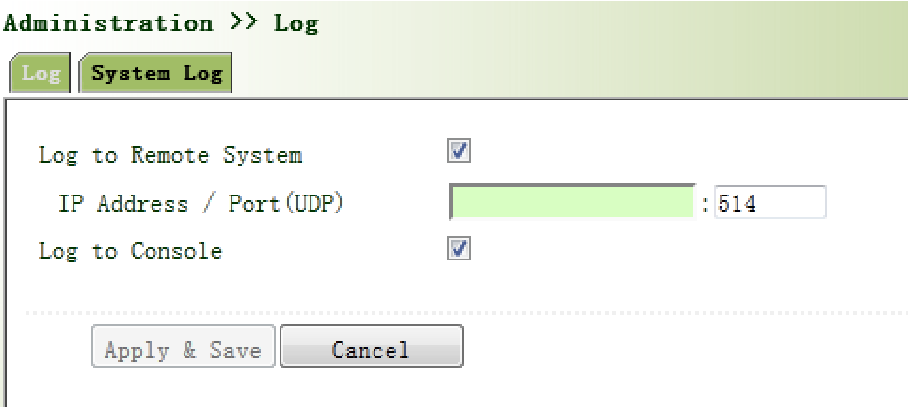
Attention

When download system log, router settings will also be downloaded.

3.2.8.2 System Log Settings

On “System Log Settings”, remote log server could be set. Router will have all system logs sent to remote log server depending on remote log software (for example: Kiwi Syslog Daemon).

From navigation panel, select Administration/Log, then enter “System Log” page, as shown in Figure 2-23.



Log to Remote System ☑

IP Address / Port(UDP) : 514

Log to Console ☑

Figure 3-23 System Log Settings

Page description is shown in Table 3-11.

Table 3-11 System Log Settings Description

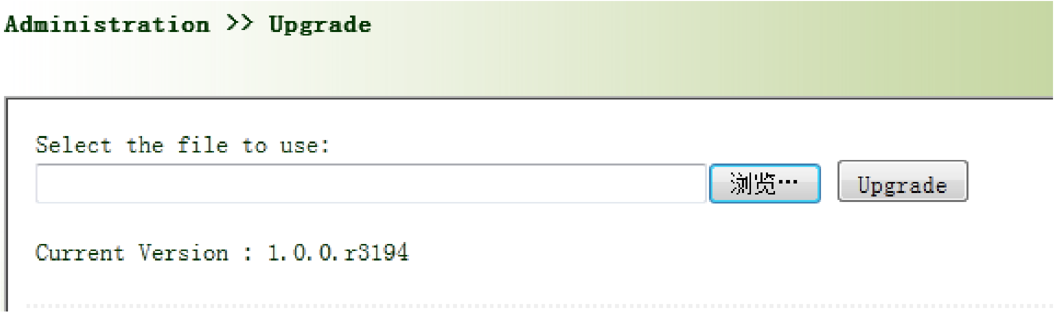
Parameters	Description	Default
Log to Remote System	Open/close remote log function	Close
IP Address/ Port(UDP)	Set remote server’s IP address/Port	None/514
Log to Console	Open/close console log function	Open

3.2.8.3 Kiwi Syslog Daemon

Kiwi Syslog Daemon is a kind of free log server software used in Windows, which could receive, record and display logs formed when powering on the host of syslog (for example, router, exchange board, Unix host). After downloading and installation of Kiwi Syslog Daemon, configure necessary parameters on “File>>Setup>>Input>>UDP”.

3.2.9 System Upgrading

From navigation panel, select Administration/Upgrade, then enter “Upgrade” page, as shown in Figure 3-24.



Administration >> Upgrade

Select the file to use:

Current Version : 1.0.0.r3194

Figure 3-24 System Upgrading

Click < Browse > to upgrade documents and then click <Upgrade> to start. The whole process takes about 1min, upon the completion of which, restart the router and new firmware takes effect.

Attention

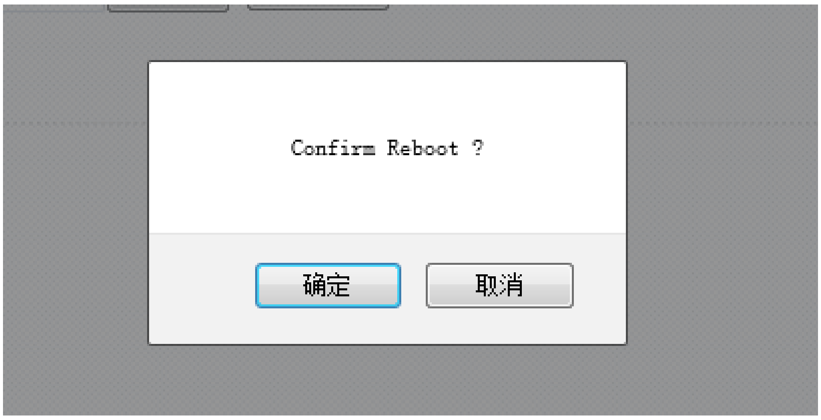
Software upgrade takes time, during which, please do no carry out any operation on Web, otherwise, interruption may take place.

Instruction

Upgrade consists of two stages: first stage: read-in of upgrade document into backup firmware zone, as described in Section of System Upgrade; second stage: copy of documents in backup firmware zone into main firmware zone, which may be executed in system reboot.

3.2.10 Reboot

From navigation panel, select Administration/Reboot, then enter “Reboot” page, as shown in Figure 3-25. Click <Yes> to reboot the system.



Confirm Reboot ?

Figure 3-25 Reboot

Attention

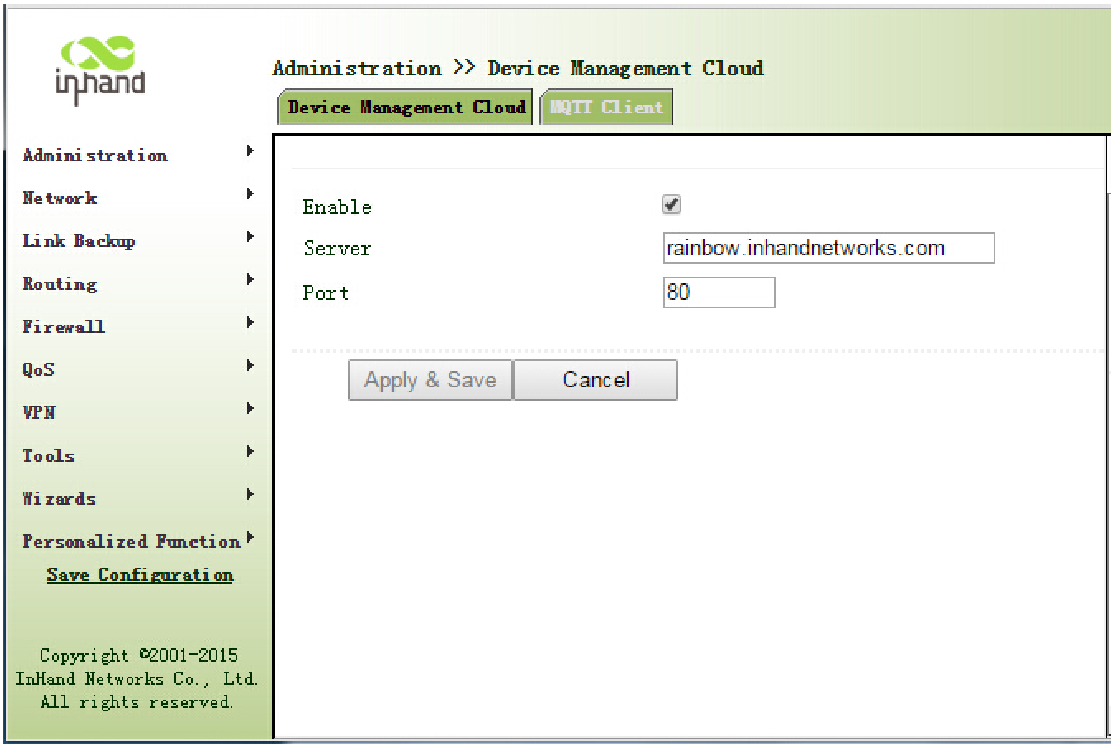
Please save the configurations before reboot, otherwise the configurations that are not saved will be lost after reboot.

3.2.11 Cloud Platform

Cloud platform is through software platform to manage devices. After enabling cloud platform, it can operate the device management through software platform that enables network-efficient running. For example, query equipment running status, update the device software, reboot the device, and send configuration parameters to the equipment, etc., may also send control or query message to the device through the cloud platform.

3.2.11.1 Cloud Platform

From navigation panel "Administration >> Device Management Cloud" menu, enter the "Cloud Platform" screen, as shown in Figure 3-26.



Enable ☑

Server rainbow.inhandnetworks.com

Port 80

Figure 3-26 Cloud Platform

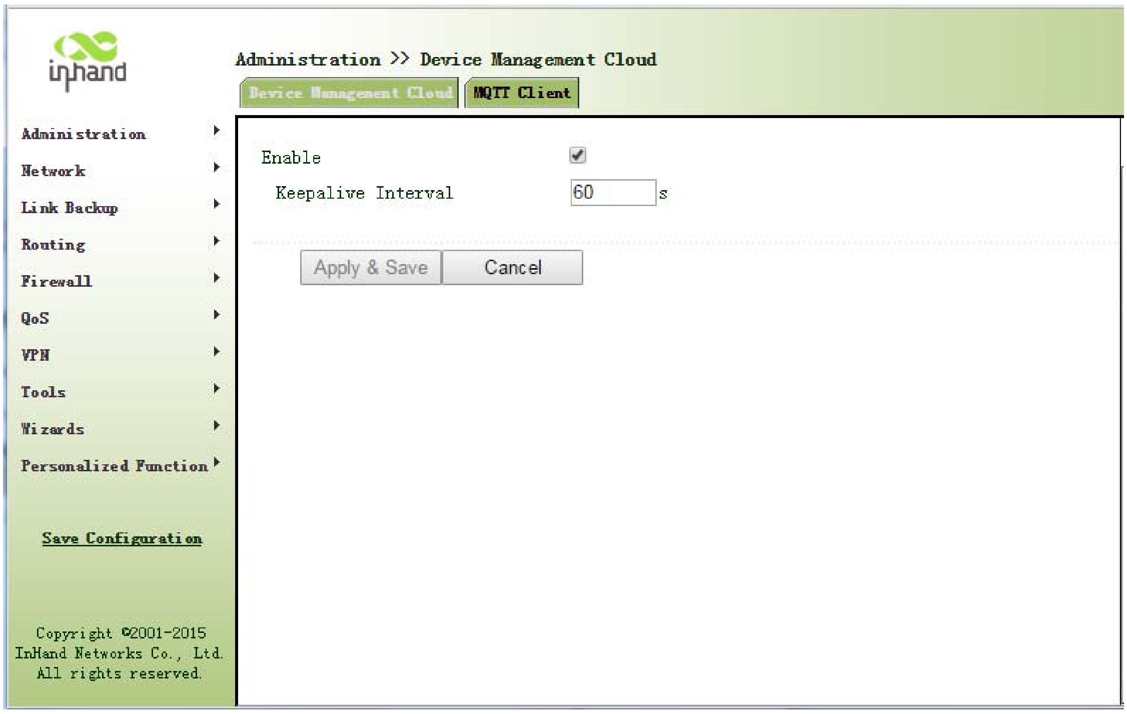
Page description is shown in Table 3-12.

Table 3-12 Cloud Platform Description

Parameters	Description	Default
Server	Set cloud platform IP address	none
Port	Setting cloud platform port number	none

3.2.11.2 MOTT Client

From navigation panel “Administration >> Device Management Cloud" menu, enter the "MOTT Client" screen, as shown below.

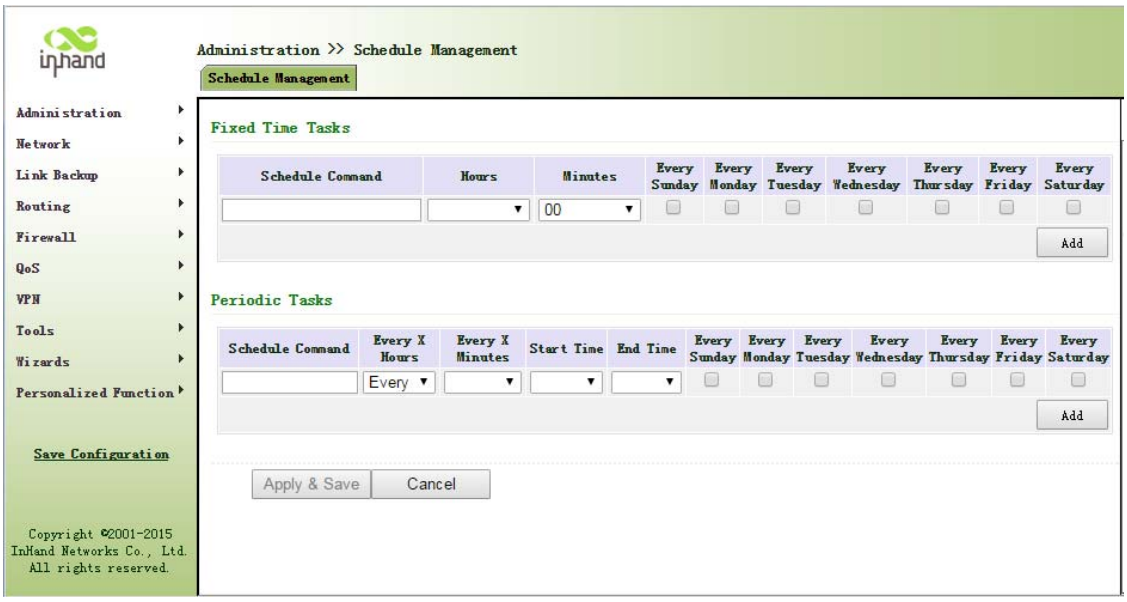


Enable ☑

Keepalive Interval 60 s

3.2.12 Scheduled Tasks

From navigation panel, select Administration>>Schedule Management, then enter "Schedule Management" page, as shown in Figure 3-27.



Fixed Time Tasks

Schedule Command	Hours	Minutes	Every Sunday	Every Monday	Every Tuesday	Every Wednesday	Every Thursday	Every Friday	Every Saturday
		00	□	□	□	□	□	□	□

Periodic Tasks

Schedule Command	Every X Hours	Every X Minutes	Start Time	End Time	Every Sunday	Every Monday	Every Tuesday	Every Wednesday	Every Thursday	Every Friday	Every Saturday
	Every				□	□	□	□	□	□	□

Figure 3-27 Schedule Management

3.3 Network

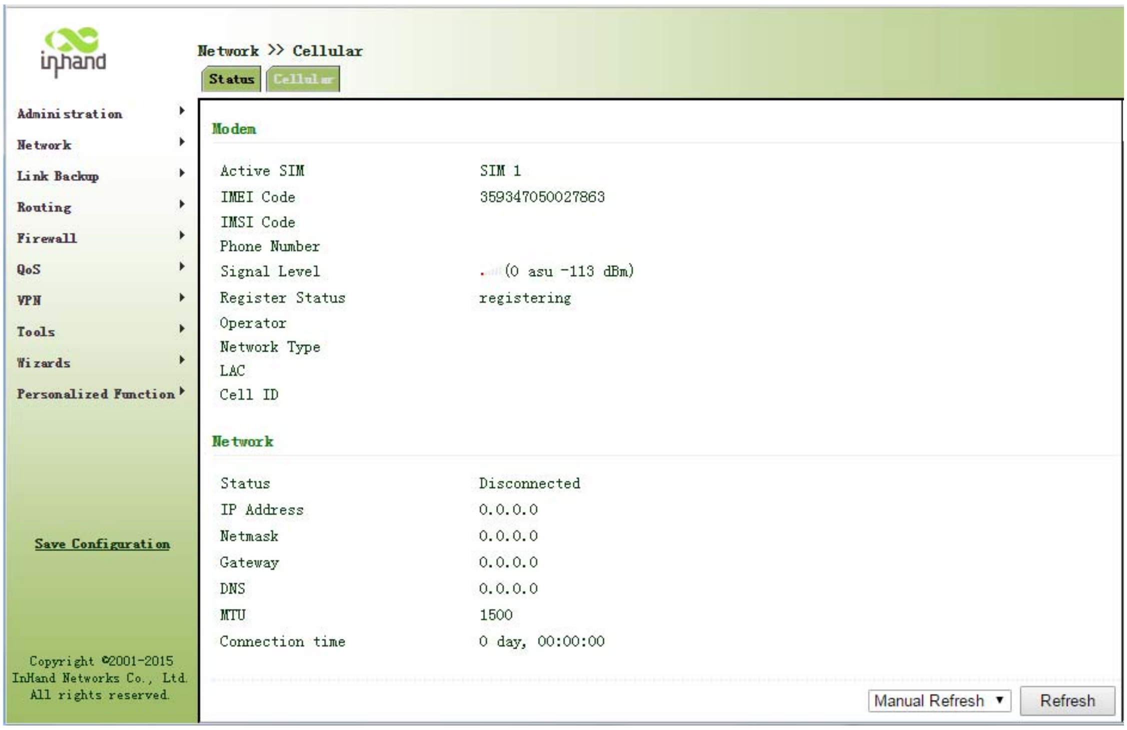
3.3.1 Cellular

SIM card dial out through Dial Interface, achieve router Wi-Fi capabilities.

Dial interface supports three connections: always-on, on-demand dialing and manual dialing.

3.3.1.1 Status

From navigation panel, select Network >> Cellular, then enter “Status” page, as shown in Figure 3-28.



Modem

Active SIM	SIM 1
IMEI Code	359347050027863
IMSI Code	
Phone Number	
Signal Level	(0 asu -113 dBm)
Register Status	registering
Operator	
Network Type	
LAC	
Cell ID	

Network

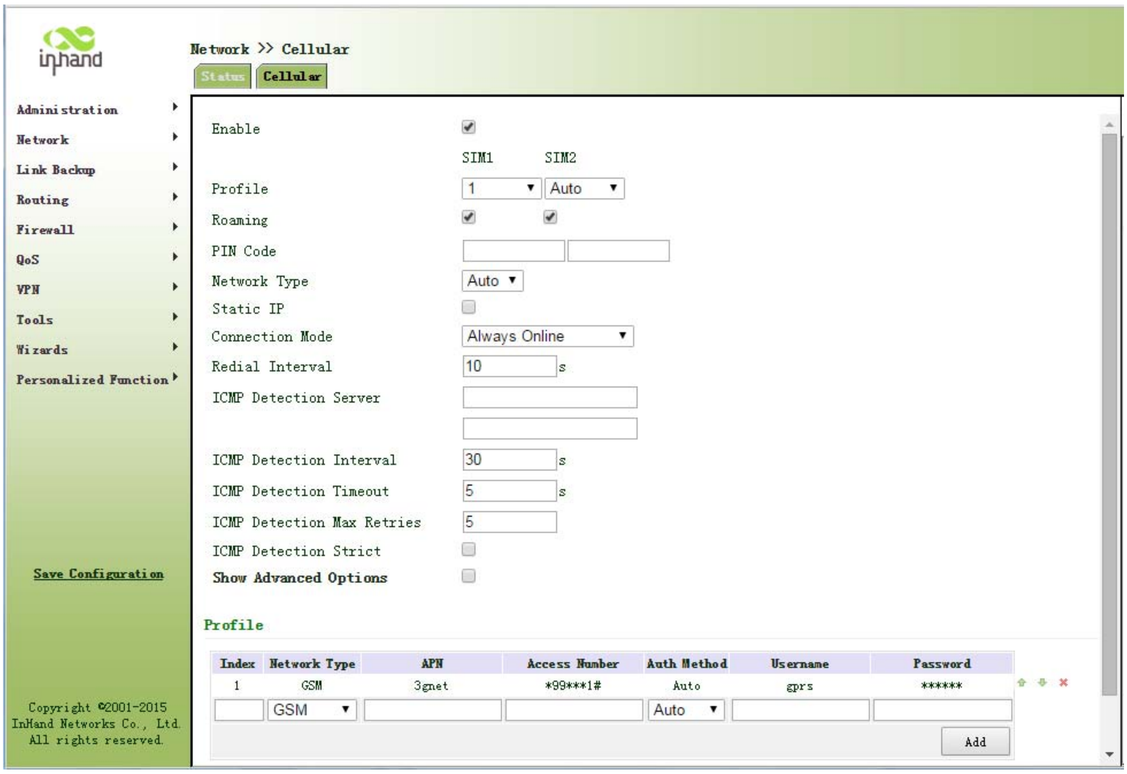
Status	Disconnected
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
Connection time	0 day, 00:00:00

Figure 3-28 Status

3.3.1.2 Cellular

In the "Cellular" page, you can complete the wireless dial configuration.

From navigation panel, select Network>>Cellular, then enter “Cellular” page, as shown in Figure 3-29-1.



Enable ☑

	SIM1	SIM2
Profile	1	Auto
Roaming	☑	☑
PIN Code		

Network Type: Auto

Static IP ☐

Connection Mode: Always Online

Redial Interval: 10 s

ICMP Detection Server:

ICMP Detection Interval: 30 s

ICMP Detection Timeout: 5 s

ICMP Detection Max Retries: 5

ICMP Detection Strict ☐

Show Advanced Options ☐

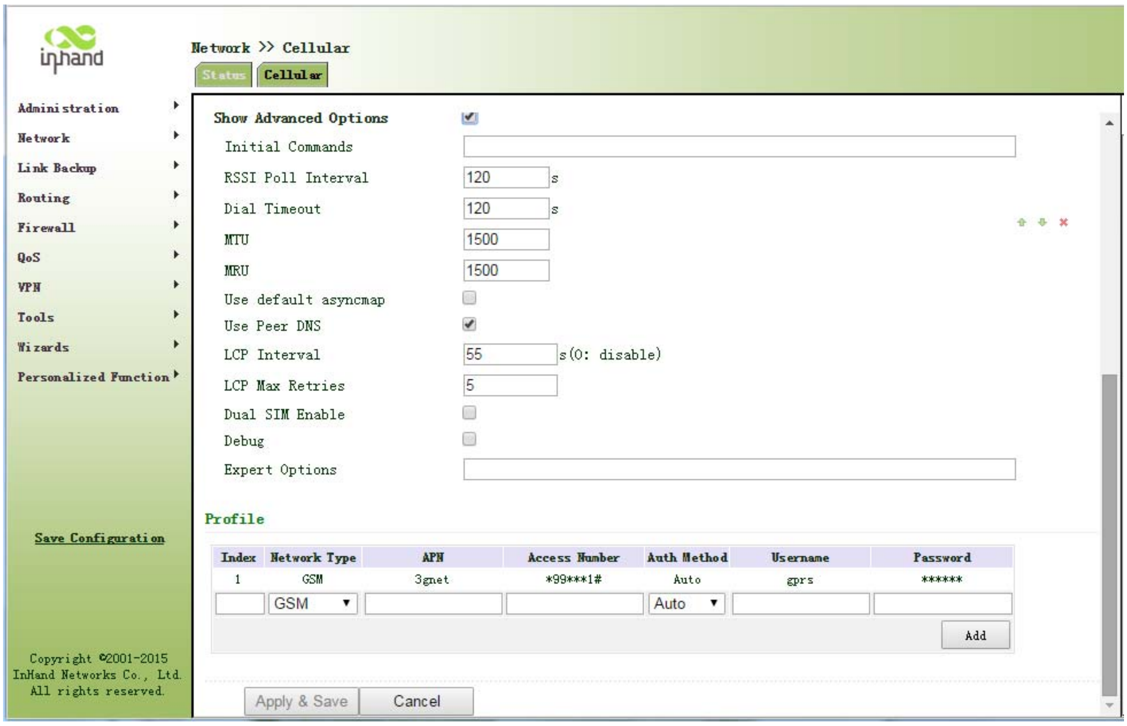
Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99***1#	Auto	gprs	******
	GSM			Auto		

Add

Figure 3-29-1 Cellular

Advanced options are shown in Figure3-29-2.



Show Advanced Options ☑

Initial Commands:

RSSI Poll Interval: 120 s

Dial Timeout: 120 s

MTU: 1500

MRU: 1500

Use default asyncmap ☐

Use Peer DNS ☑

LCP Interval: 55 s(0: disable)

LCP Max Retries: 5

Dual SIM Enable ☐

Debug ☐

Expert Options:

Profile

Index	Network Type	APN	Access Number	Auth Method	Username	Password
1	GSM	3gnet	*99***1#	Auto	gprs	******
	GSM			Auto		

Add

Figure 3-29-2 Cellular Advanced options

Page description is shown in Table 3-13.

Table 3-13 Cellular Page Description

Parameters	Description	Default
Profile	Dial policy choices, do not need to configure here	1
Roaming	Select roaming	Enable
PIN Code	SIM card PIN code	None
Network Selection Mode	Three options: Automatic, 2G and 3G	Auto
Static IP	Click Enable (Enable require operators to open related services)	Off
Connection	Alternatively always online, on-demand dial (allows data activation, phone activation, SMS activation), manual dialing	Always online
Redial Interval	when setting up the landing fails, redialing interval	10sec
ICMP detection server	Detect remote IP address	None
ICMP detection interval	Set ICMP detection interval	30sec
ICMP detection timeout	Set ICMP detection timeout	5sec
ICMP detection maximum number of retries	Set maximum number of retries when ICMP detection fails(Re-dial after reaching the maximum number)	5
ICMP strict detection	Click Enable	Off
Dial parameters		
Index	User-defined, generally in the order defined by digital.	None
Network	Mobile network type used for selecting	GSM
APN (CDMA2000 series does not set this)	Mobile operators to provide the relevant parameters (according to local operators choose)	3gnet
Dial Number	Mobile operators to provide the relevant parameters (according to local operators choose)	*99***1#
User Name	Mobile operators to provide the relevant parameters (according to local operators choose)	gprs
Password	Mobile operators to provide the relevant parameters (according to local operators choose)	******
Click Enable Show Advanced Options (the following are the relevant parameters to configure after the advanced options turn on)		
Initia Commands	Used to set advanced network parameters, generally do not need to fill in	None
RSSI Poll Interval	Set signal query interval	120sec
Dial timeout	Set dial timeout (after dialing timeout the system will redial)	120sec
MTU	Sets the maximum transmission unit in bytes	1500
MRU	Setting maximum receiving unit in bytes	1500

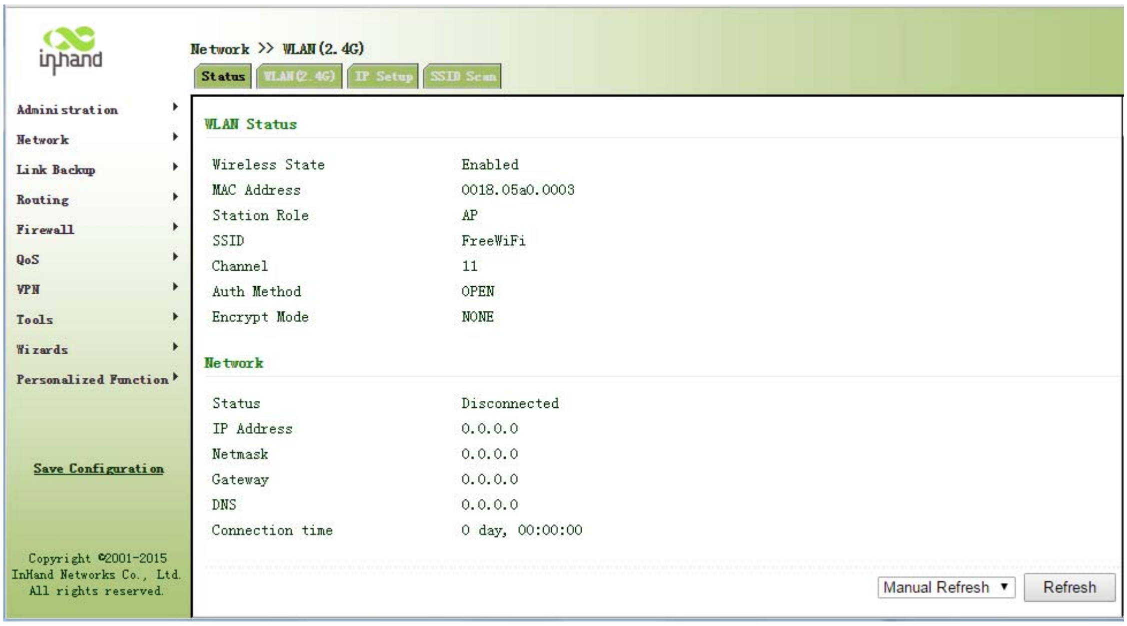
Enable default asyncmap	Click Enable default asyncmap	Disable
Use assigned DNS server	Click to enable to accept assigned DNS by mobile operators.	Enable
Connection detection interval	Set connection detection interval	55sec
Connection Detection maximum number of retries	Set maximum number of retries when connection detection fails(Re-dial after reaching the maximum number)	5
Enable debug mode	The system can print a more detailed log	Enable
Expert Options	Provide additional PPP parameters, users generally do not set	None

3.3.2 WLAN Interface（2.4G）

WLAN or Wireless LAN, is quite convenient data transmission system, which uses radio frequency (Radio Frequency; RF) technology, to replace the old out of the way of twisted copper (Coaxial) local area network composed of such a wireless local area network, can be accessed using a simple architecture allows users to through it, to "carry information technology to facilitate travel the world," the ideal state.

3.3.2.1 Status

From navigation panel, select Network/WLAN(2.4G), enter “Status” page, as shown in Figure 3-30.



WLAN Status

Wireless State	Enabled
MAC Address	0018.05a0.0003
Station Role	AP
SSID	FreeWiFi
Channel	11
Auth Method	OPEN
Encrypt Mode	NONE

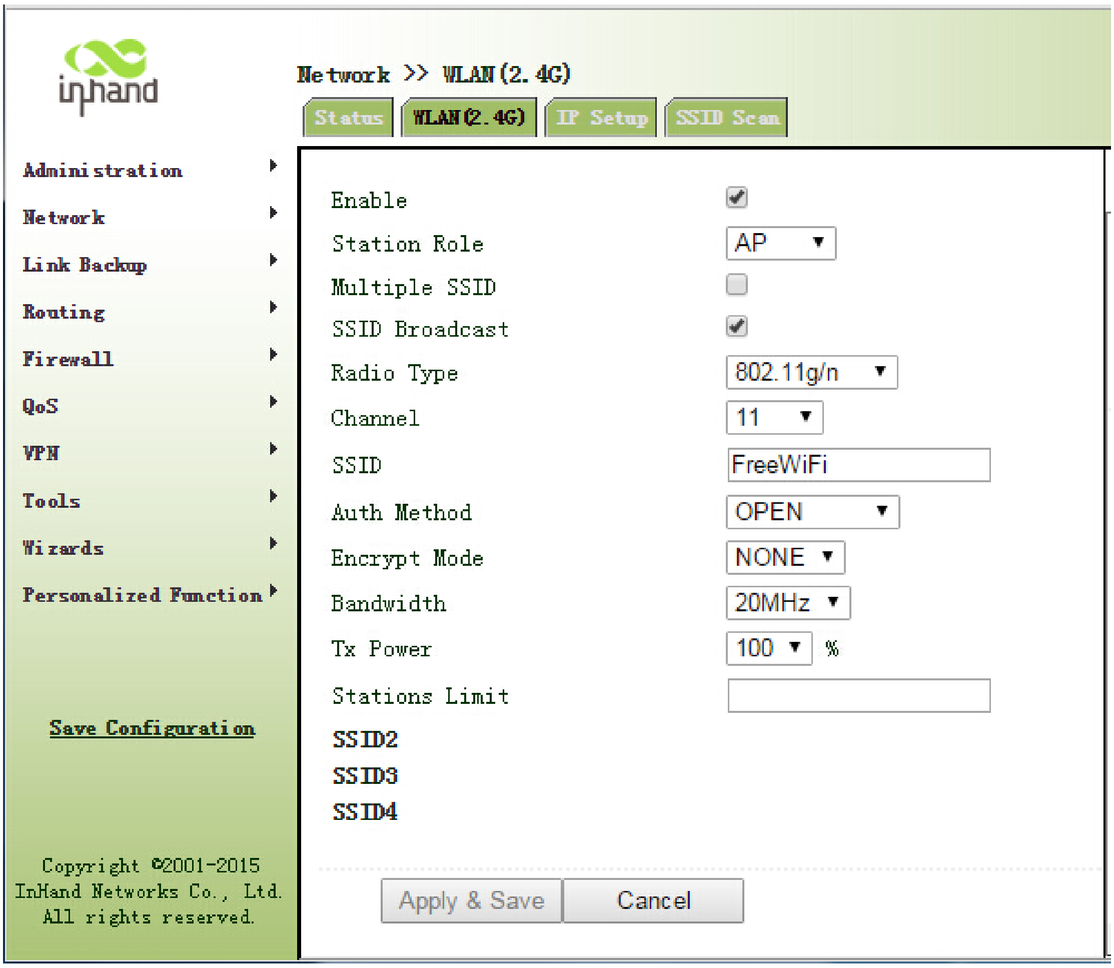
Network

Status	Disconnected
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Connection time	0 day, 00:00:00

Figure 3-30 WLAN (2.4G) Status

3.3.2.2 WLAN (2.4G)

WLAN interface has access point and client two types. From navigation panel, select "Network/WLAN (2.4G)" menu, enter "WLAN (2.4G)" page. Interface type using the "access point", as shown in Figure 3-31-a; interface type using the "client", as shown in Figure 3-31-b.



Enable	☑
Station Role	AP
Multiple SSID	□
SSID Broadcast	☑
Radio Type	802.11g/n
Channel	11
SSID	FreeWiFi
Auth Method	OPEN
Encrypt Mode	NONE
Bandwidth	20MHz
Tx Power	100 %
Stations Limit	

SSID2

SSID3

SSID4

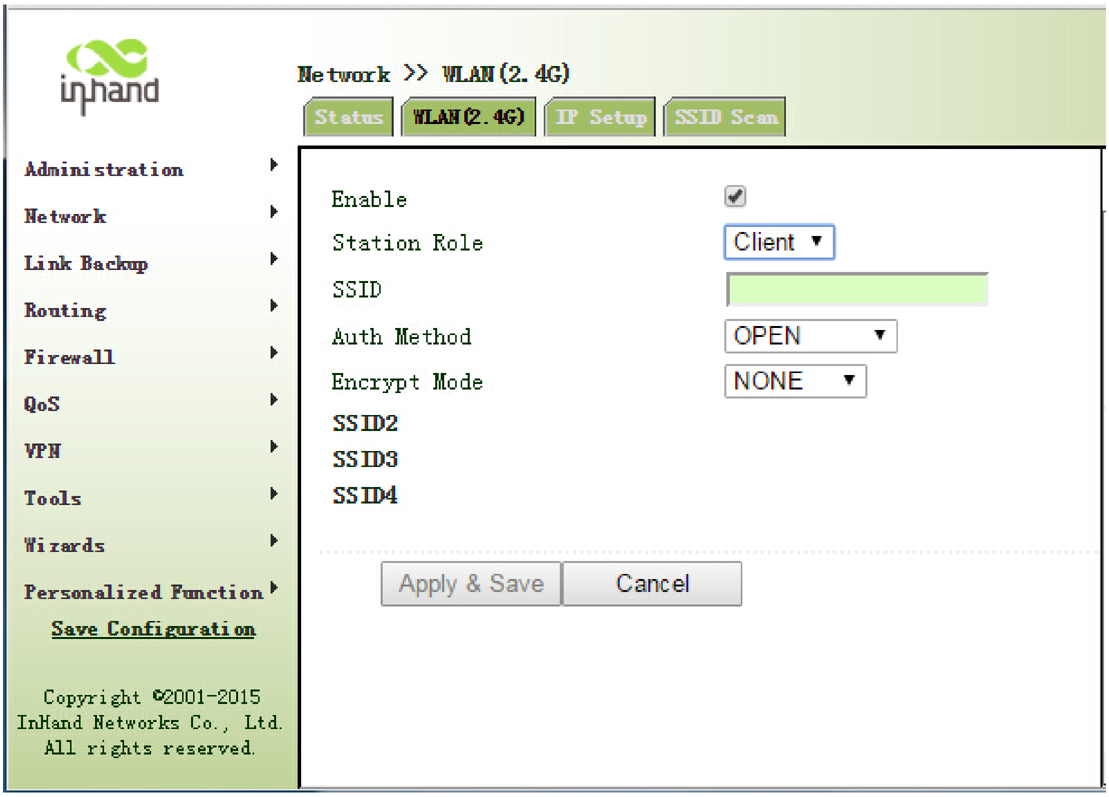
Figure 3-31-a WLAN (2.4G)- Access Point

Page description is shown in Table 3-14-a.

Table 3-14-a Access Point Description

Parameters	Description	Default
Multiple SSID	Click Enable, enabled reusable custom 3 SSID	Disable
SSID Broadcast	Open "SSID Broadcast", user can search wireless network through SSID name.	Enable
RF Type	Six types Optional: 802.11g/n,802.11g,802.11n,802.11b,802.11b/g,802.11b/g/n	802.11g/n
Channel	Select channel	11

SSID	User-defined SSID name	InPortal3000
Authentication	Four authentication modes available: Open, Shared, WPA-PSK and WPA2-PSK	Open
Encryption	According to the different authentication methods, support NONE, WEP40 and WEP104	NONE
Wireless Bandwidth	Two options: 20MHz and 40MHz	20MHz
Maximum Number of Clients	User-defined (up to 128)	None



Enable ☑

Station Role: Client

SSID:

Auth Method: OPEN

Encrypt Mode: NONE

SSID2

SSID3

SSID4

Figure 3-31-b WLAN(2.4G)- Client

Page description is shown in Table 3-14-b.

Table 3-14-b Client Interface Description

Parameters	Description	Default
SSID	Fill in the SSID name to connect	None
Authentication	SSID authentication method	Open
Encryption	SSID encryption method	NONE

When the WLAN is set as Client mode, refer to the following 3 steps:

Step 1: select "Network/Cellular" menu, enter "Cellular" page, and disable Cellular function. If the router does not have celluar module, skip this step and go to step 2.

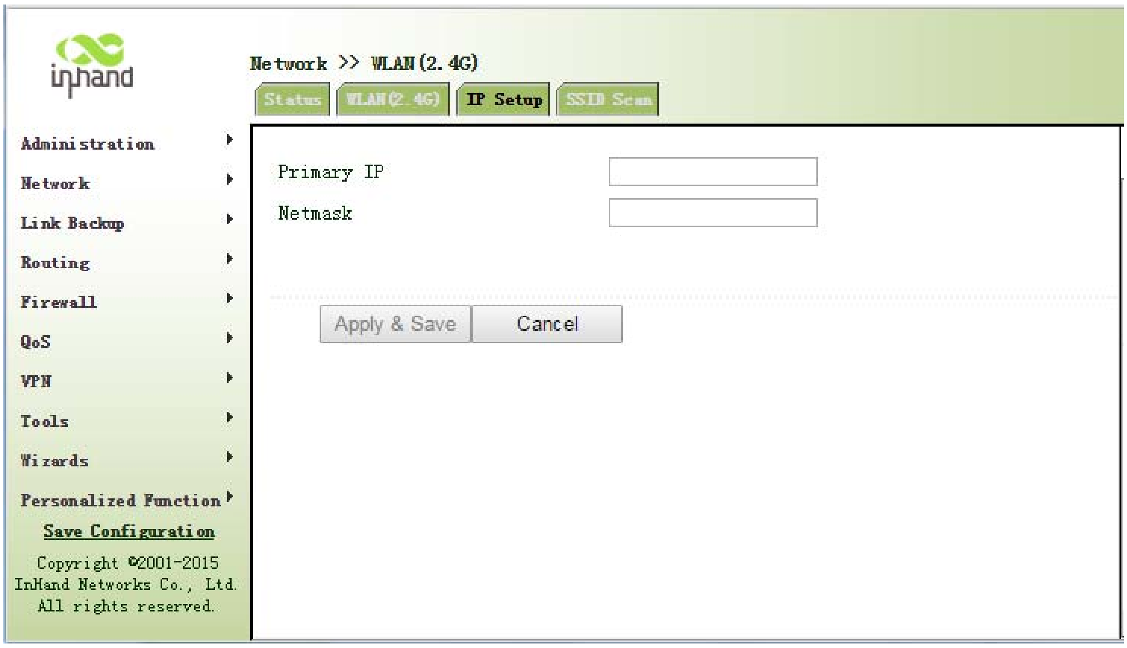
Step 2: select "Network/WLAN (2.4G)" menu, enter "WLAN (2.4G)" page and choose “Client” to configure related parameters as shown in Figure 3-31-b.

Step 2: select "Network/WLAN (2.4G)" menu, enter "IP Setup" page to configure IP parameters as shown in 3.3.2.3 IP Setup.

3.3.2.3 IP Setup

WLAN interface IP address support multiple IP, it can be set according to demand, but up to more than 10.

From navigation panel, select "Network/WLAN (2.4G)" menu, enter "IP Setup" page, as shown in Figure 3-32.



Primary IP:

Netmask:

Figure 3-32 WLAN (2.4G) IP Setup

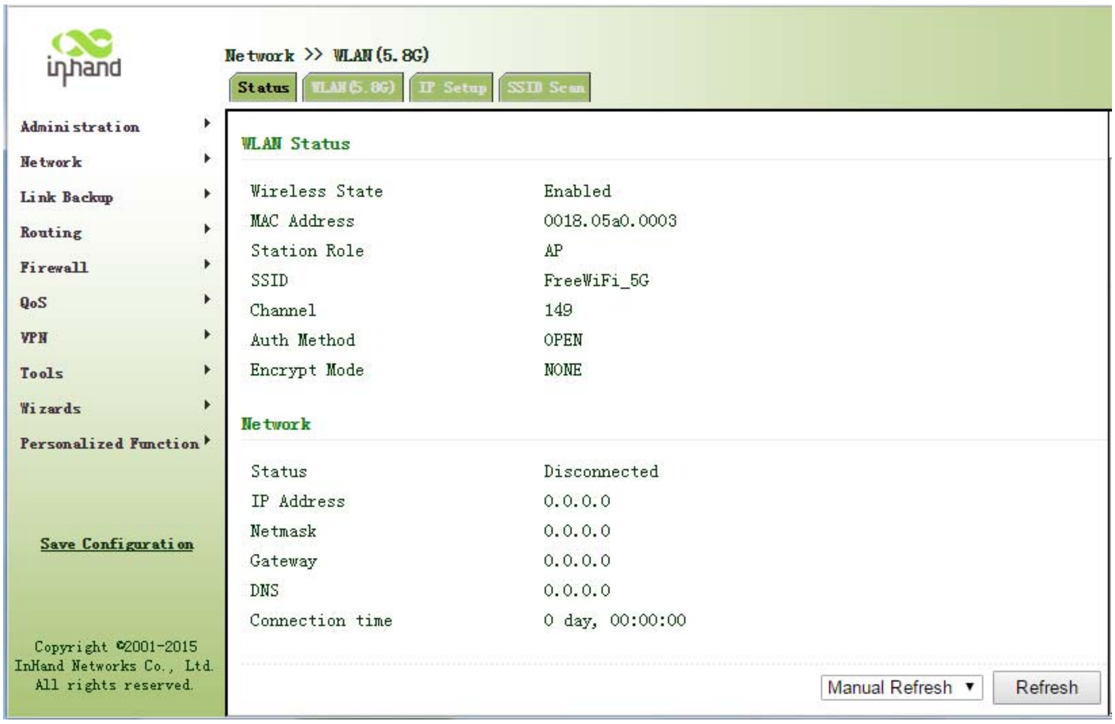
3.3.2.4 SSID Scan

WLAN interface selects client (Section 3.3.2.2WLAN Interface (2.4G)), SSID scanning function starts. From navigation panel "Network/WLAN (2.4G)" menu, enter "SSID Scan" page, will display all the available SSID names, and the display Inportal can be connected as a client state.

3.3.3WLAN Interface（5.8G）

3.3.3.1 Status

From navigation panel, select Network/WLAN (5.8G), enter “Status” page, as shown in Figure 3-34.



WLAN Status

Wireless State	Enabled
MAC Address	0018.05a0.0003
Station Role	AP
SSID	FreeWiFi_5G
Channel	149
Auth Method	OPEN
Encrypt Mode	NONE

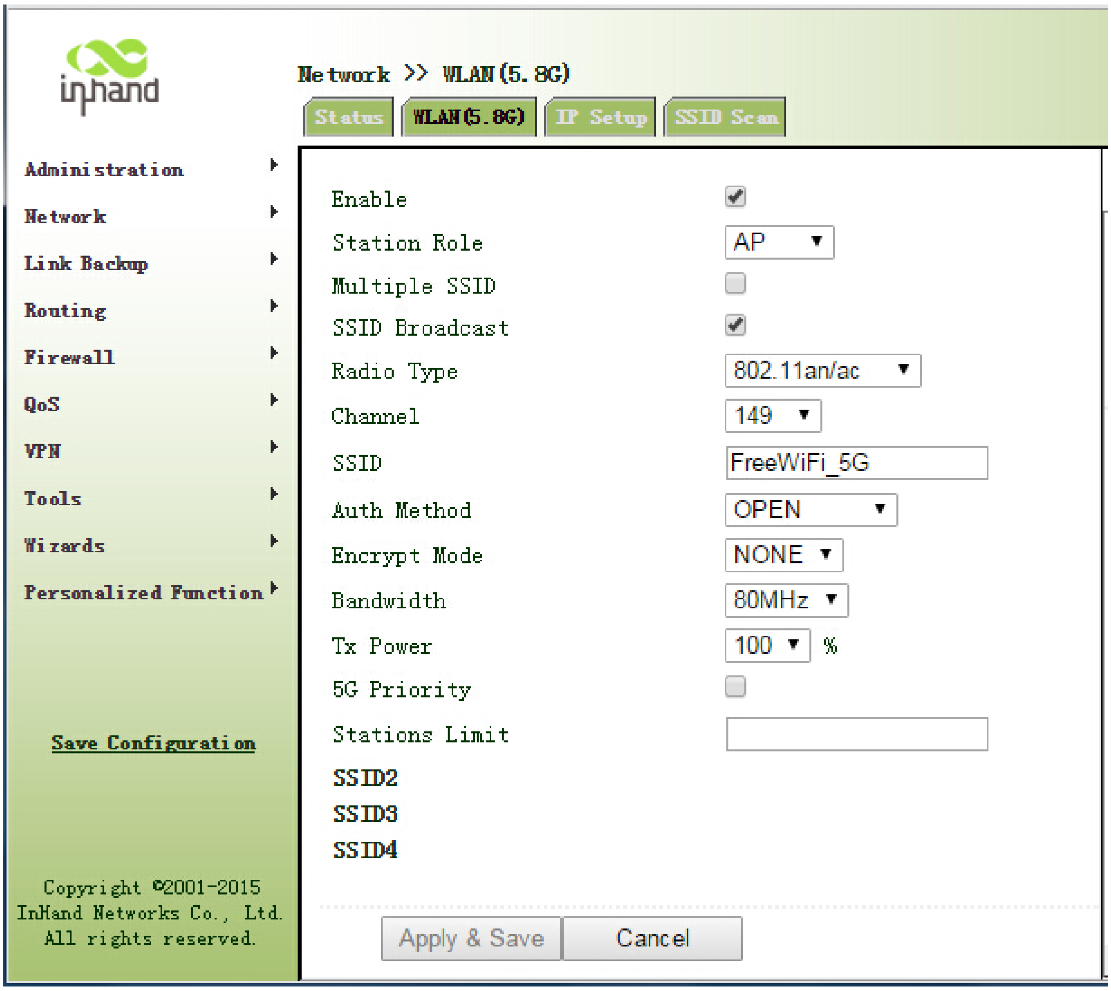
Network

Status	Disconnected
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
Connection time	0 day, 00:00:00

Figure 3-34 WLAN (5.8G) Status

3.3.3.2 WLAN（5.8G）

WLAN interface has access point and client two types. From navigation panel "Network/WLAN (5.8G)" menu, enter "WLAN (5.8G)" page. Interface type using the "access point", as shown in Figure 3-35-a; interface type using the "client", as shown in Figure 3-35-b.



Enable	☑
Station Role	AP
Multiple SSID	□
SSID Broadcast	☑
Radio Type	802.11an/ac
Channel	149
SSID	FreeWiFi_5G
Auth Method	OPEN
Encrypt Mode	NONE
Bandwidth	80MHz
Tx Power	100 %
5G Priority	□
Stations Limit	

SSID2
SSID3
SSID4

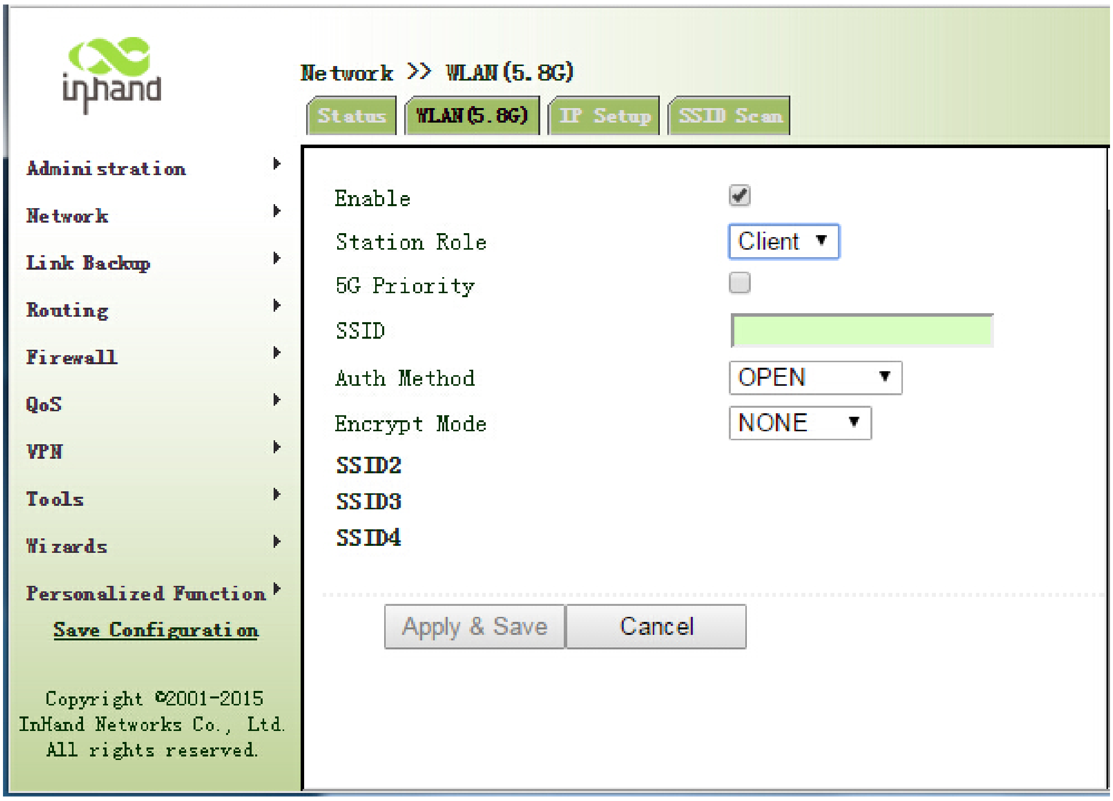
Figure 3-35-a WLAN interface (5.8G)- Acess Point

Page description is shown in Table 3-15-a.

Table 3-15-a Acess Point Description

Parameters	Description	Default
Multiple SSID	Click Enable, enabled reusable custom 3 SSID	Disable
SSID Broadcast	Open "SSID Broadcast", user can search wireless network through SSID name.	Enable
RF Type	Six types Optional: 802.11g/n,802.11g,802.11n,802.11b,802.11b/g,802.11b/g/n	802.11g/n
Channel	Select channel	11
SSID	User-defined SSID name	InPortal3000
Authentication	Four authentication modes available: Open, Shared, WPA-PSK and WPA2-PSK	Open
Encryption	According to the different authentication methods, support NONE, WEP40 and WEP104	NONE
Wireless Bandwidth	Two options: 20MHz and 40MHz	20MHz

Maximum Number of Clients	User-defined (up to 128)	None



Enable ☑

Station Role Client

5G Priority □

SSID

Auth Method OPEN

Encrypt Mode NONE

SSID2

SSID3

SSID4

Figure 3-35-b WLAN interface (5.8G)-Client

Page description is shown in Table 3-15-b.

Table 3-15-b WLAN interface (5.8G) Description

Parameters	Description	Default
5G priority	Select Enable	Disable
SSID	SSID name to connect	None
Authentication	SSID authentication method	Open
Encryption	SSID encryption method	NONE

When the WLAN is set as Client mode, refer to the following 3 steps:

Step 1: select "Network/Cellular" menu, enter "Cellular" page, and disable Cellular function. If the router does not have celluar module, skip this step and go to step 2.

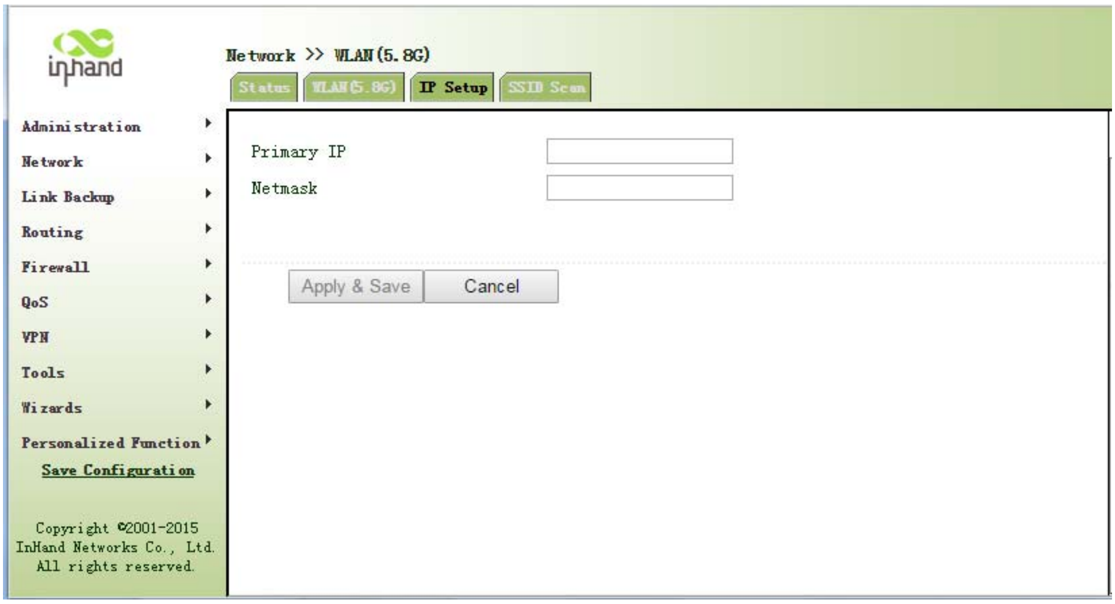
Step 2: select "Network/WLAN (5.8G)" menu, enter "WLAN (5.8G)" page and choose “Client” to configure related parameters as shown in Figure 3-35-b.

Step 2: select "Network/WLAN (5.8G)" menu, enter "IP Setup" page to configure IP parameters as shown in 3.3.3.3 IP Setup.

3.3.3.3 IP Setup

WLAN interface IP address support multiple IP, it can be set according to demand, but up to more than 10.

From navigation panel, select Network/WLAN (5.8G), enter "IP Setup" page, as shown in Figure 3-36.



Primary IP
Netmask

Figure 3-36 WLAN (5.8G) IP Setup

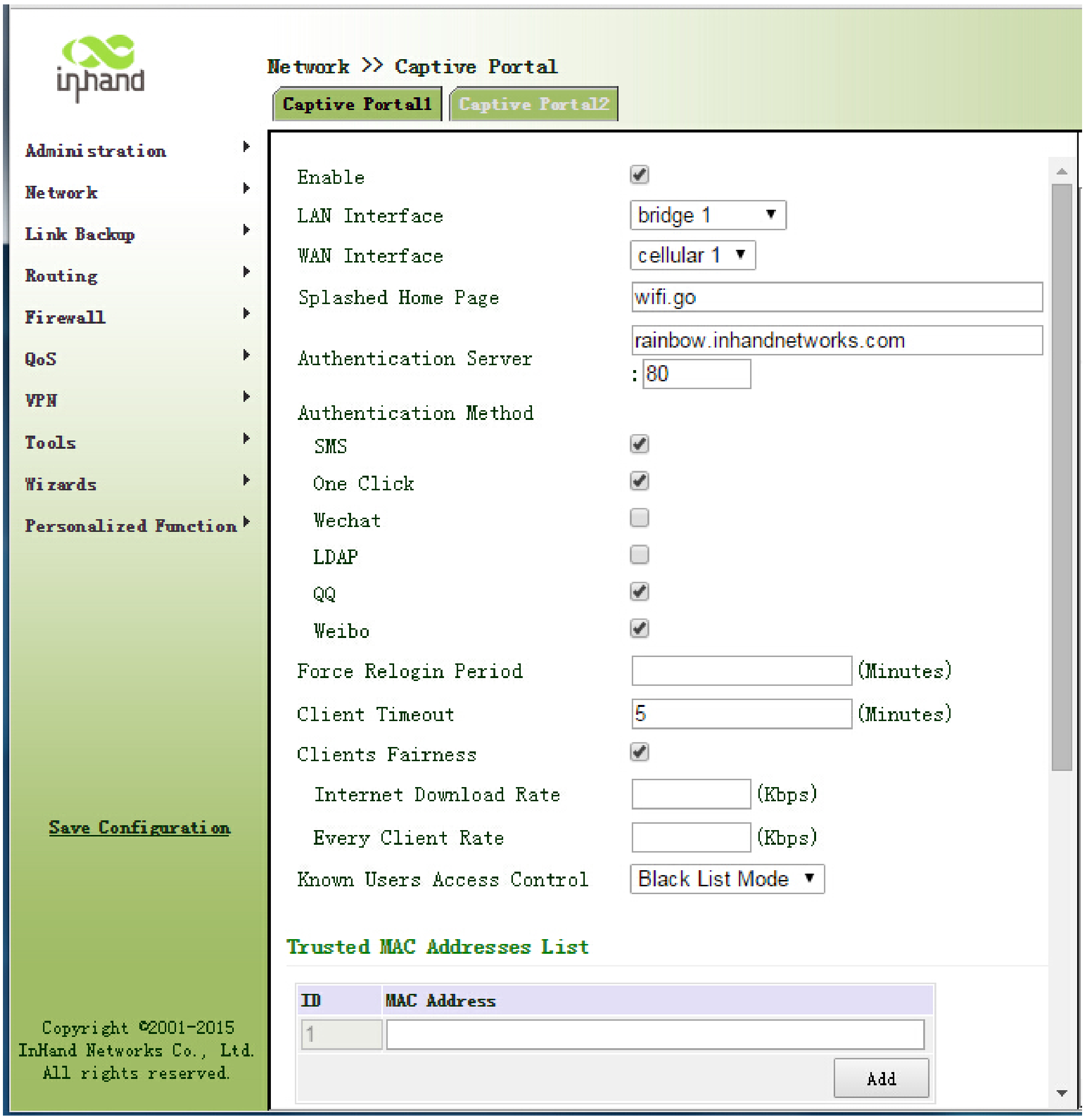
3.3.3.4 SSID Scan

WLAN interface selects client (Section 3.3.3.2WLAN Interface (5.8G)), SSID scanning function starts. From navigation panel "Network/WLAN interface (5.8G)" menu, enter "SSID Scan" page, will display all the available SSID names, and the display Inportal can be connected as a client state.

3.3.4 Captive Portal

Captive portal is Web page that user must visit and interact with before granted access to public access network. Captive portal usually offers free Wi-Fi hotspot services to Internet users in commercial centers, airports, hotel lobbies, cafes and other public places to use.

From navigation panel "Network/captive portal" menu, enter the "captive portal" page. As shown in Figure 3-38.



Network >> Captive Portal

Enable ☑

LAN Interface: bridge 1

WAN Interface: cellular 1

Splashed Home Page: wifi.go

Authentication Server: rainbow.inhandnetworks.com : 80

Authentication Method
- SMS ☑
- One Click ☑
- Wechat ☐
- LDAP ☐
- QQ ☑
- Weibo ☑

Force Relogin Period: (Minutes)

Client Timeout: 5 (Minutes)

Clients Fairness ☑
- Internet Download Rate: (Kbps)
- Every Client Rate: (Kbps)

Known Users Access Control: Black List Mode

Trusted MAC Addresses List

ID	MAC Address
1	

Copyright ©2001-2015 InHand Networks Co., Ltd. All rights reserved.

Figure 3-38 Captive Portal

Page description is shown in Table 3-16.

Table 3-16 Captive Portal Description

Parameters	Description	Default
LAN Interface	Captive portal local interface	dotllradio 1
WAN Interface	External network adapter	cellular 1
Splashed Home Page	Push Home to customers	wifi.go
Authentication Server	User authentication server IP address for user login authentication	None: 80
Force Relogin Period	Force user to re-login	None
Silent User	User automatic logoff when no flow	5

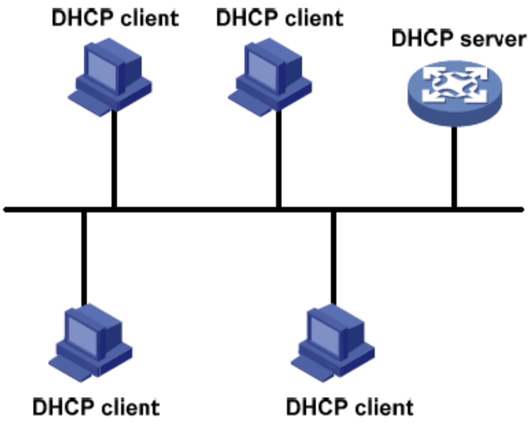
Automatic Logoff		
Client Fairness	Used in conjunction with the speed function	Enable
Speed Limit	Wifi client traffic restrictions	None
Known Users Access Control	Authenticated user access control two optionals: blacklist and whitelist mode.	Blacklist
Trusted MAC Addresses List		
ID	Serial number	None
MAC Address	MAC address authentication-free user	None
Global whitelist		
ID	Serial number	None
Domain/IP	addressor IP that can be accessed without authentication	None
Authenticated users blacklist		
ID	Serial number	None
Domain/IP	Restrict authenticated users to access network, that is can not be accessed by authenticated users to blacklist addresses or IP	None

3.3.5 DHCP service

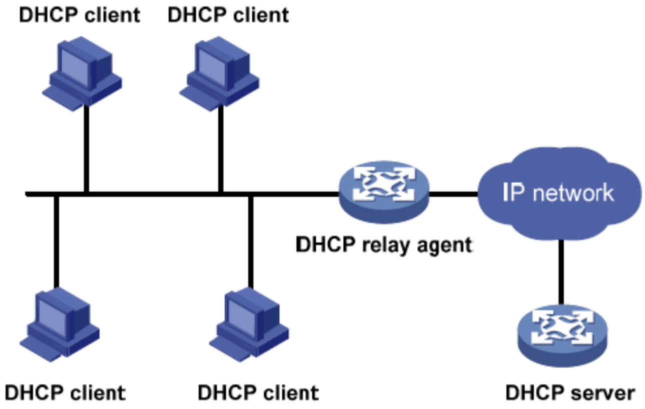
Along with the continuous expansion of network size and complication of network, number of computers often exceeds distributable IP addresses. Meanwhile, in pace with the extensive application of portable devices and wireless network, position of computer changes frequently, resulting to the frequent upgrade of IP address, leading to a more and more complicated network configuration. DHCP (Dynamic Host Configuration Protocol) is a product for such demands.

DHCP adopts Client/Server communication mode. Client sends configuration request to Server which feeds back corresponding configuration information, including distributed IP address to the Client to achieve the dynamic configuration of IP address and other information.

In typical applications of DHCP, generally one DHCP Server and a number of Clients (PC and Portable Devices) are included, as the following figure shows:

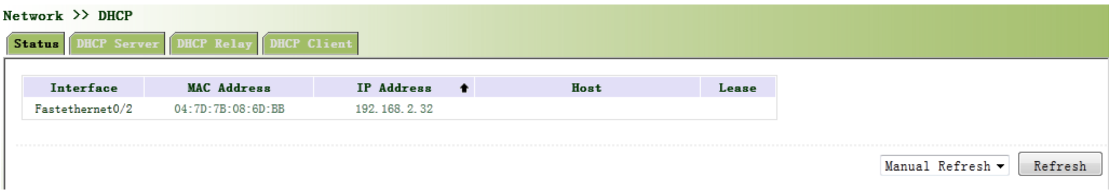


When DHCP Client and DHCP Server are in different physical network segment, Client could communicate with Server through DHCP Relay to obtain IP address and other configuration information, as the following figure shows:



3.3.5.1 Status

From navigation panel, select Network/DHCP, then enter “Status” page, as shown in Figure 3-39.



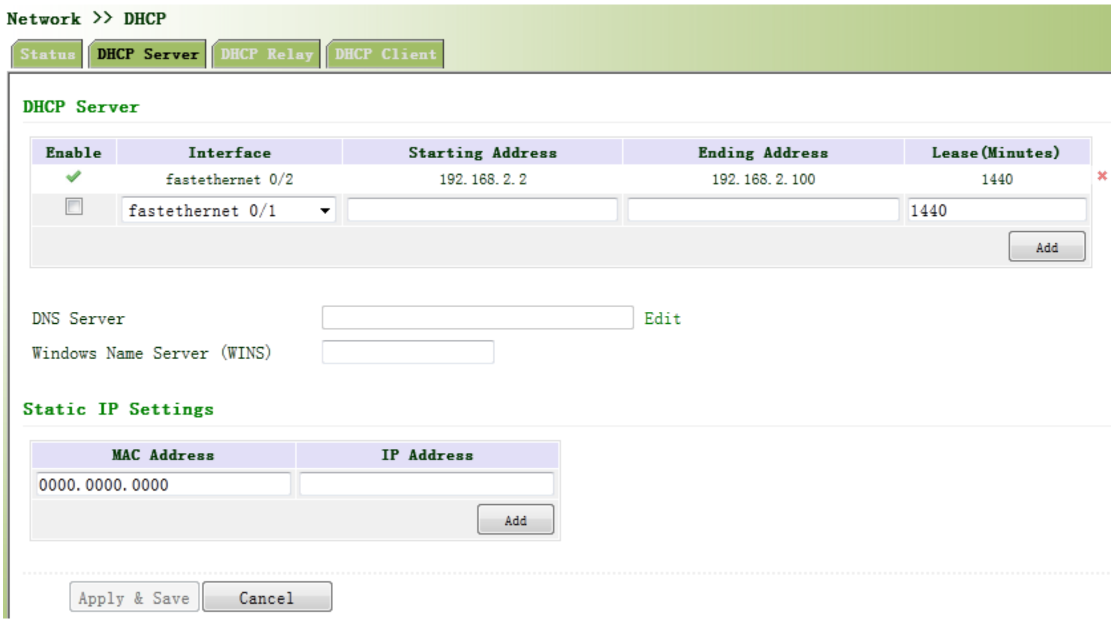
Interface	MAC Address	IP Address ⬆	Host	Lease
Fastethernet0/2	04:7D:7B:08:6D:BB	192.168.2.32		

Figure 3-39 DHCP Status

3.3.5.2 DHCP Server

The duty of DHCP Server is to distribute IP address when Workstation logs on and ensure each workstation is supplied with different IP address. DHCP Server has simplified some network management tasks requiring manual operations before to the largest extent.

From navigation panel, select Network >>DHCP, then enter “DHCP Server” page, as shown in Figure 3-40.



DHCP Server

Enable	Interface	Starting Address	Ending Address	Lease(Minutes)
✓	fastethernet 0/2	192.168.2.2	192.168.2.100	1440
□	fastethernet 0/1			1440

DNS Server

Windows Name Server (WINS)

Static IP Settings

MAC Address	IP Address
0000.0000.0000	

Figure 3-40 DHCP Server

Page description is shown in Table 3-17.

Table 3-17 DHCP Server Description

Parameters	Description	Default
Enable	On/Off	Off
Interface	dot11radio 1	dot11radio 1
Starting Address	Dynamical distribution of starting IP address	N/A
Ending Address	Dynamical distribution of ending IP address	N/A
Lease	Dynamical distribution of IP validity	1440
DNS Server	One or two, or None	N/A
WINS	Setup of WINS, generally left blank	N/A
Static IP Setup		
MAC Address	Set up a static specified DHCP’s MAC address (different from other MACs to avoid confliction)	0000.0000.0000
IP Address	Set up a static specified IP address (within the scope from start IP to end IP)	N/A

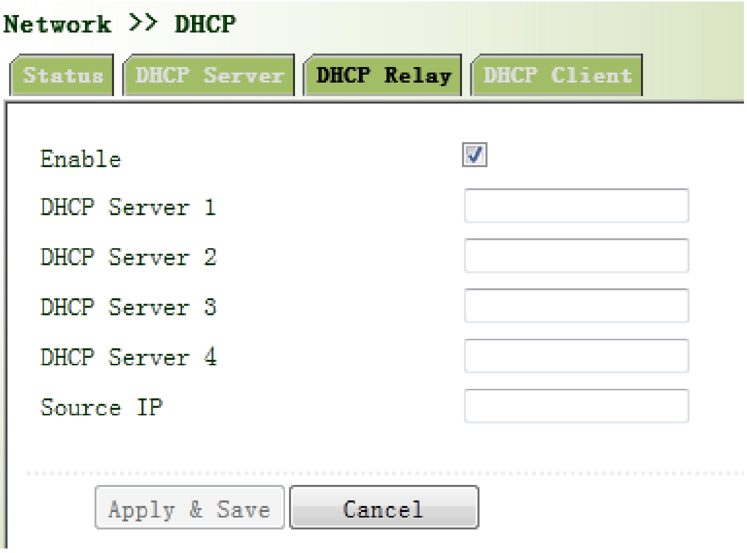
Attention

If the host connected with router chooses to obtain IP address automatically, then such service must be activated. Static IP setup could help a certain host to obtain specified IP address.

3.3.5.3 DHCP Relay

Generally, DHCP data packet is unable to be transmitted through router. That is to say, DHCP Server is unable to provide DHCP services for two or more devices connected with a router remotely. Through DHCP relay, DHCP requests and response data packet could go through many routers (Broadband Router).

From navigation panel, select Network/DHCP, then enter "DHCP Relay" page, as shown in Figure 3-41.



Network >> DHCP

Enable ☑

DHCP Server 1

DHCP Server 2

DHCP Server 3

DHCP Server 4

Source IP

Figure 3-41DHCP Relay

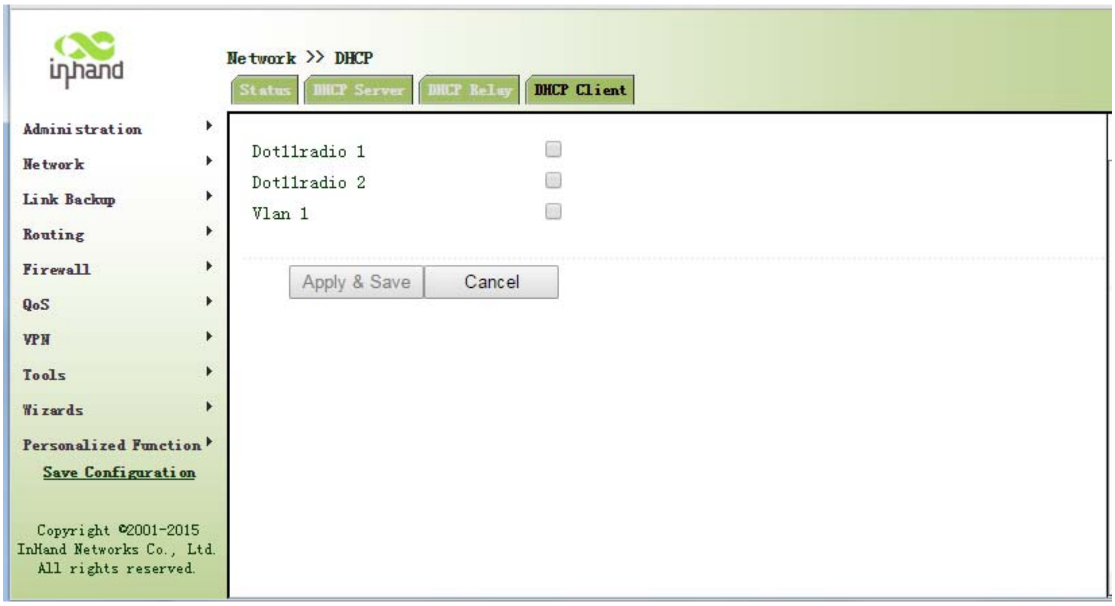
Page description is shown in Table 3-18.

Table 3-18 DHCP Realy Description

Parameters	Description	Default
Enable	On/Off	Off
DHCP Sever	Set DHCP server; up to 4 servers can be configured	N/A
Source IP	Address of the interface connected to the DHCP server	N/A

3.3.5.4 DHCP Client

From navigation panel, select Network/DHCP, then enter “DHCP Client” page, by clicking to enable, choose SSID interface, as shown in Figure 3-42.



Dot11radio 1 □
Dot11radio 2 □
Vlan 1 □

Figure 3-42DHCP Client

3.3.6 DNS Services

DNS (Domain Name System) is a DDB used in TCP/IP application programs, providing switch between domain name and IP address. Through DNS, user could directly use some meaningful domain name which could be memorized easily and DNS Server in network could resolve the domain name into correct IP address.

The device supports to achieve following two functions through domain name service configuration:

DNS Server: for dynamic domain name resolution.

DNS relay: the device, as a DNS Agent, relays DNS request and response message between DNS Client and DNS Server to carry out domain name resolution in lieu of DNS Client.

3.3.6.1 DNS Server

Domain Name Server: DNS stands for Domain Name System. It is a core service of the Internet. As a distributed database that can let the domain names and IP addresses mapping to each other, it allows people to more conveniently access to the Internet without the need to memorize the IP string that can be directly read by the computer.

From navigation panel, select Network/DNS, then enter “DNS Server” page. In manual setup of DNS Server, if it is blank, then dial to obtain DNS. Generally this item is required to be set when WAN port uses static IP, as shown in Figure 3-43.

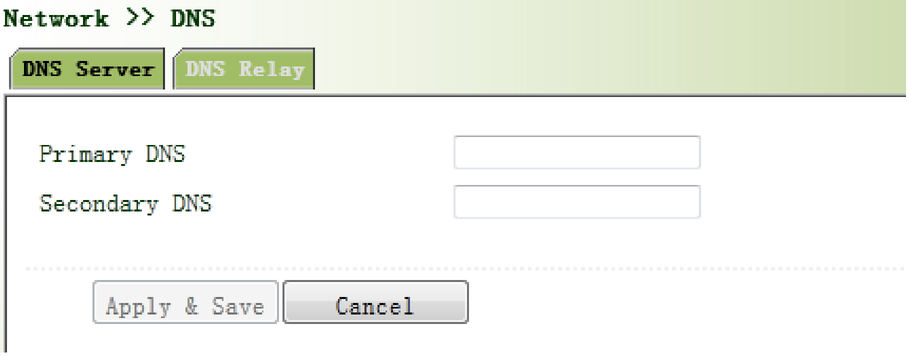


Figure 3-43 DNS Server

Page description is shown in Table 3-19.

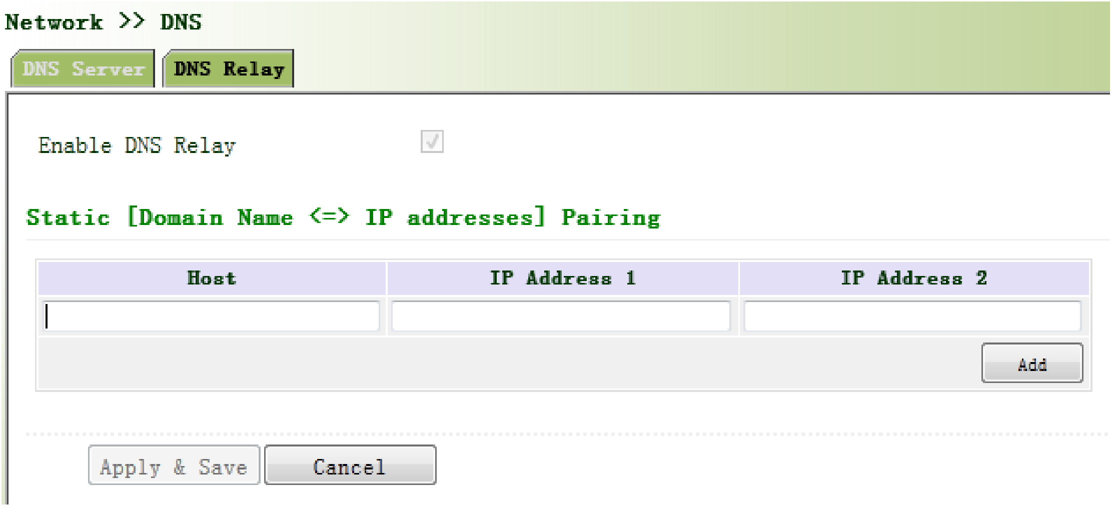
Table 3-19 DNS Server Description

Parameters	Description	Default
Primary DNS	User define Primary DNS address	N/A
Secondary DNS	User define Secondary DNS address	N/A

3.3.6.2 DNS Relay

DNS forwarding: DNS forwarding is open by default. You can set the specified [Domain Name <=> IP Address] to let IP address match with the domain name, thus allowing access to the appropriate IP through accessing to the domain name.

From navigation panel, select Network/DNS, then enter “DNS Relay” page, as shown in 3-44.



Enable DNS Relay ☑

Static [Domain Name <=> IP addresses] Pairing

Host	IP Address 1	IP Address 2

Figure 3-44 DNS Relay

Page description is shown in Table 3-20.

Table 3-20 DNS Delay Description

Parameters	Description	Default
Enable DNS Relay	On/Off	On
Host	Domain Name	N/A
IP Address 1	Set IP Address 1	N/A
IP Address 2	Set IP Address 2	N/A

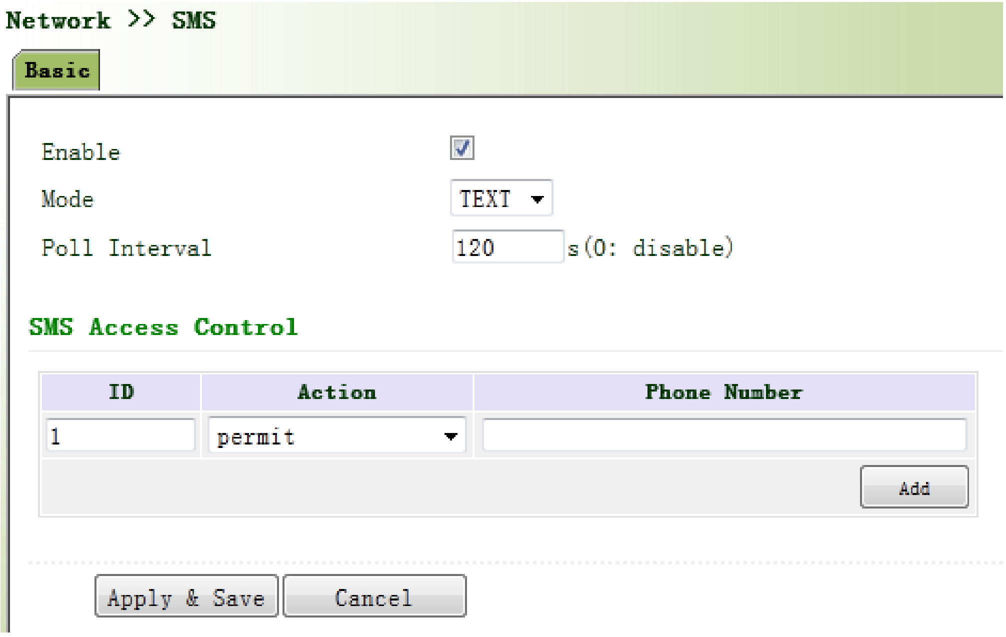
⚠ **Attention**

Once DHCP is turned on, DNS relay will be turned on as default and can't be turned off; to turn off DNS rely, DHCP Server has to be closed firstly.

3.3.7 SMS

SMS permits message-based reboot and manual dialing.

From navigation panel, select Network/SMS, then enter "Basic" page. Configure Permit action to Phone Number and click <Apply & Save>. After that you can send "reboot" command to restart the device or "cellular 1 ppp up/down" to redial or disconnect the device, as shown in Figure 3-45.



Enable ☑

Mode TEXT

Poll Interval 120 s(0: disable)

SMS Access Control

ID	Action	Phone Number
1	permit	

Figure 3-45 SMS

Page description is shown in Table 3-21.

Table 3-21 SMS Description

Parameters	Description	Default
Enable	On/Off	Off
Mode	TEXT and PDU	TEXT
Poll Interval	User define Poll Interval	120
SMS Access Control		
ID	User define ID	1
Action	Permit and refuseare available	Permit
Phone Number	Trusting phone number	N/A

3.3.8 VLAN Interface

VLAN (Virtual Local Area Network) divides LAN device logically into one and another network segment, enable emerging data exchange technology of virtual workgroups.

3.3.8.1 VLAN Configuration

From navigation panel "Network/VLAN" menu, enter "Configure VLAN Parameters" page, click <Add> button to add the VLAN, as shown in Figure 3-46.

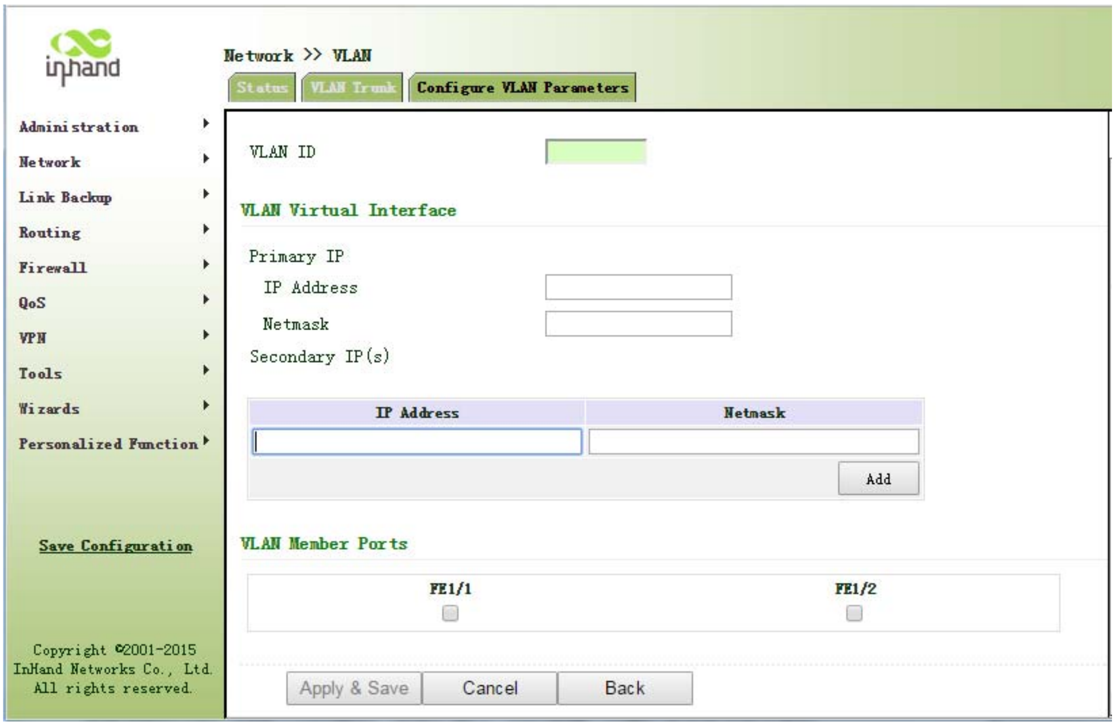


Figure 3-46 Configure VLAN Parameters

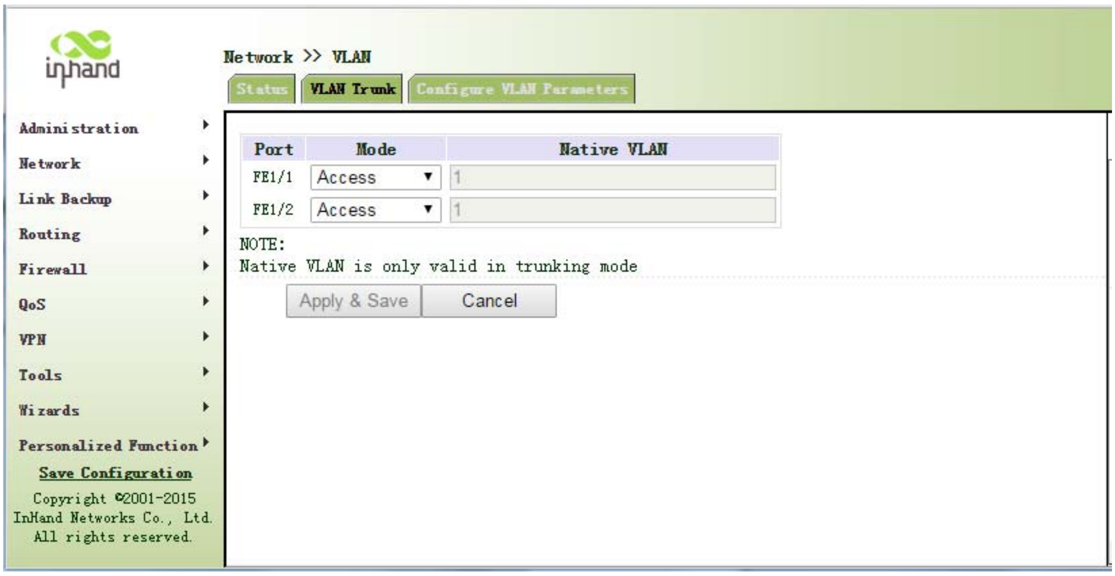
Page description is shown in Table 3-22.

Table 3-22 Configure VLAN Parameters Description

Parameters		Description	Default
VLAN ID		VLAN ID, User-defined	None
VLAN Interface			
Primary IP Address	IP address	Users can configure or change the primary IP address needed	None
	Subnet Mask	Users can configure or change the subnet mask if necessary	
Secondary IP Address	IP address	In addition to primary IP, user can also configure 10 Secondary IP addresses	None
	Subnet Mask	Users can configure or change the subnet mask if necessary	

3.3.8.2 VLAN Aggregation

From navigation panel "Network/VLAN” menu, enter "VLAN Trunk" page, set VLAN port mode for InPortal, the mode can be set to Access or Trunk, as shown in Figure 3-47.



Port	Mode	Native VLAN
FE1/1	Access	1
FE1/2	Access	1

NOTE:
Native VLAN is only valid in trunking mode

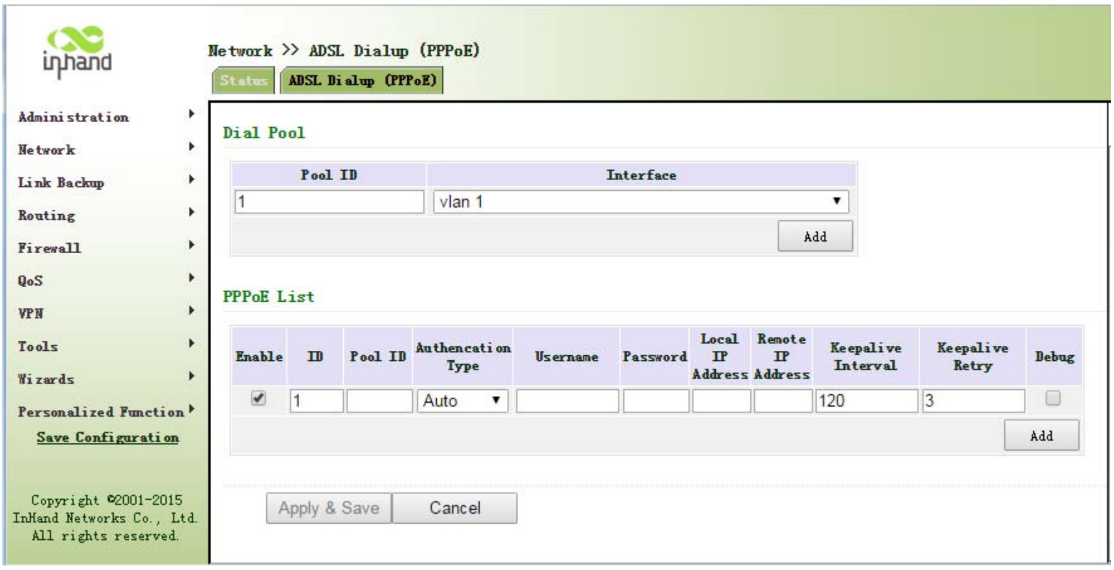
Figure 3-47 VLAN Trunk

3.3.9 ADSL Dialup（PPPoE）

PPPoE is Point to Point Protocol over Ethernet. Users need while maintaining the original access, install a PPPoE client. Through PPPoE, a remote access device can realize control and accounting of each access user.

Ethernet interface connection mode you configure here is PPPoE, namely the interface as PPPoE client.

From navigation panel "Network/ADSL Dialup (PPPoE)" menu, enter "ADSL Dialup (PPPoE)" page, as shown in Figure 3-48.



Dial Pool

Pool ID	Interface
1	vlan 1

PPPoE List

Enable	ID	Pool ID	Authencation Type	Username	Password	Local IP Address	Remote IP Address	Keepalive Interval	Keepalive Retry	Debug
☑	1		Auto					120	3	☐

Figure 3-48 PPPoE

Page description is shown in Table 3-23.

Table 3-23 PPPoE Description

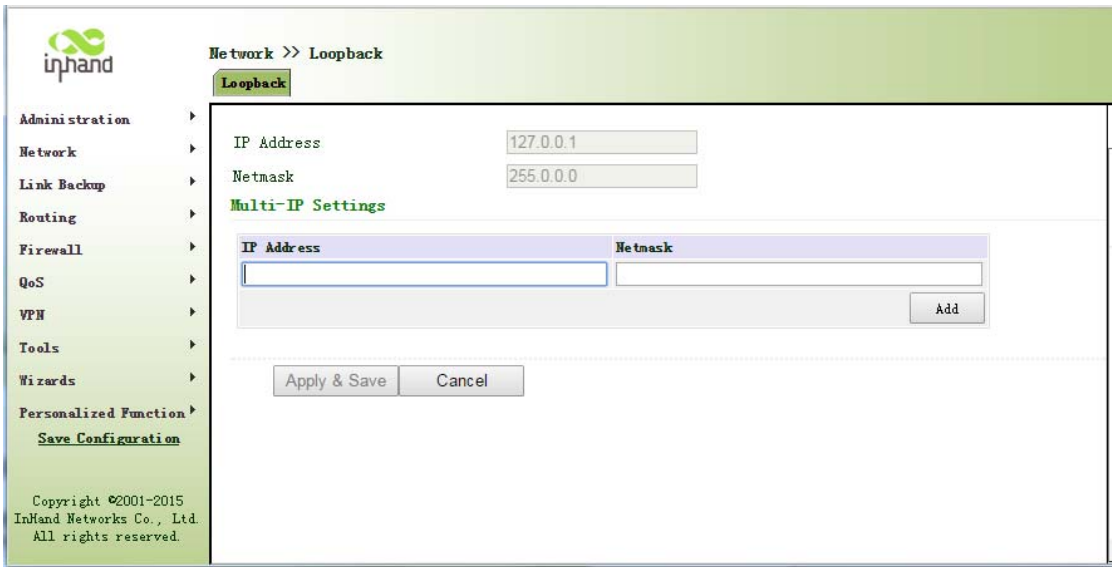
Parameters	Description	Default
Dial Pool	User-defined, easy to remember and manage	None
Interface	Select Fastethernet0/1 or Fastethernet0/2	Fastethernet0/1
PPPoE List		
ID	User-defined, easy to remember and manage	1
Pool ID	Dial pool Index	None
Authentication Type	Three options: Auto,PAP,CHAP	Auto
User Name	Relevant parameters provided by peer operator	None
Password	Relevant parameters provided by peer operator	None
Local IP Address	Assigned IP address to Ethernet interface	None
Remote IP Address	Remote IP address	None

3.3.10 Loopback Interface

Loopback is used to represent router ID, because if you use active interface, when activity interface DOWN, router ID is subject to re-selection, that would cause OSPF convergence time slow, thus loopback interface is generally used as a router ID.

Loopback interface is logical and virtual interface on routers. No default router loopback interface. You can create any number of loopback interfaces as needed. These interfaces on router treated like physical interface: You can assign them addressing information, including their choice to update the network number in routers, or even terminate IP connection on them.

From navigation panel "Network/Loopback Interface" menu, enter "loopback" page, shown in Figure 3-49.



IP Address 127.0.0.1

Netmask 255.0.0.0

Multi-IP Settings

IP Address	Netmask

Figure 3-49 Loopback

Page description is shown in Table 3-24.

Table 3-24 Loopback Interface Description

Parameters	Description	Default
IP Address	User can not change.	127.0.0.1
Subnet Mask	User can not change.	255.0.0.0
Multi-IP settings	In addition to the above IP, user also can be equipped with other IP addresses	None

Attention

Since loopback interface is exclusive of one IP address, subnet mask is generally recommended to 255.255.255.255, to save resources.

3.3.11 Dynamic Domain Name

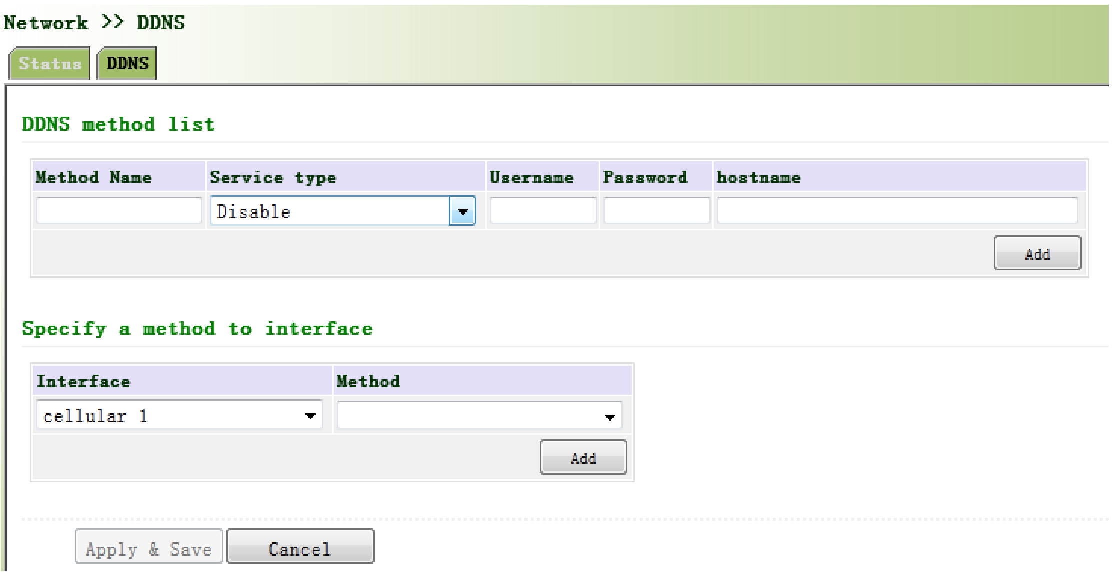
DDNS Dynamic Domain Name Service is mapping user dynamic IP address to a fixed domain name resolution services, when user connect to the network, client program will pass dynamic IP address of the host through information transfer to server program on the host of service providers, the server program is responsible for providing DNS service and realizing dynamic domain name resolution. That is, DDNS to capture changeable IP address, then corresponding with domain name, so that other Internet users can communicate through the domain name.

And all final customers to remember, is to remember the dynamic domain name given by suppliers, without having to pipe how they are implemented.

DDNS function as DDNS client tools, we need to work with DDNS server. Before using this feature, you need first to find corresponding sites such as (www.3322.org) and apply for registration of a domain name.

DDNS service type include: DynAccess, QDNS (3322)-Dynamic, QDNS (3322)-Static, DynDNS-Dynamic, DynDNS-Static and NoIP.

From navigation panel "Network/DDNS" menu, enter "DDNS" page. Set dynamic binding domain. As shown in Figure 3-50.



DDNS method list

Method Name	Service type	Username	Password	hostname
	Disable			

Specify a method to interface

Interface	Method
cellular 1	

Figure 3-50 Dynamic Domain Name

Page description is shown in Table 3-25.

Table 3-25 Dynamic Domain Name Description

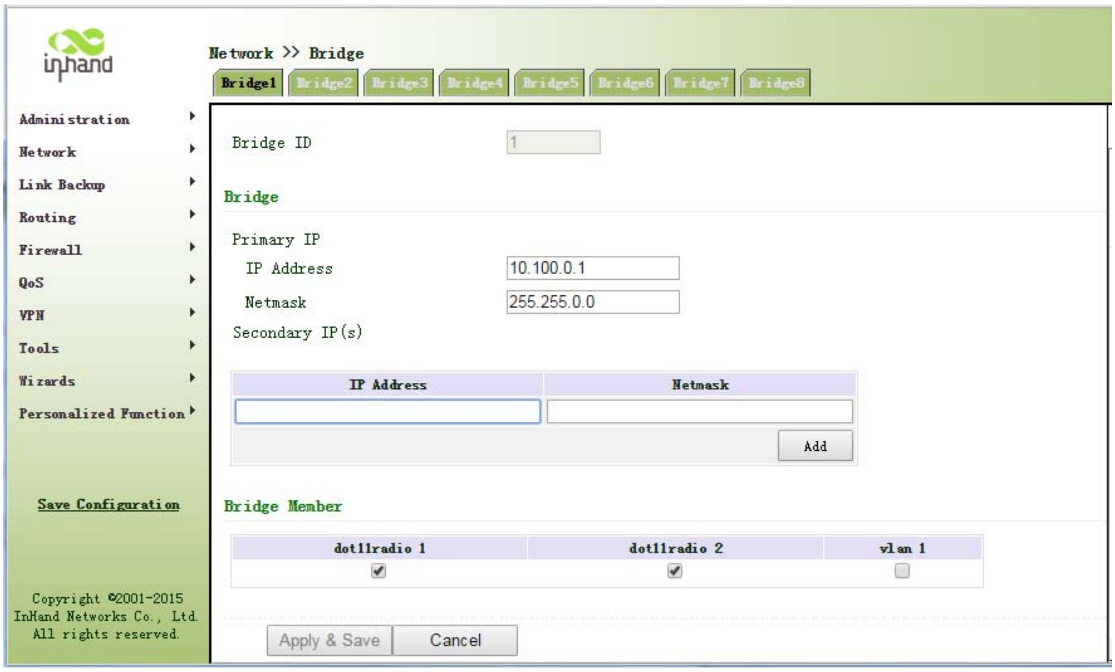
Parameters	Description	Default
Method	User-defined	None
Service Type	Select dynamic domain name service providers	Disable
User Name	Apply registration DDNS username	None
Password	Apply registration DDNS username	None
Host	Apply registration DDNS host	None
Specified Interface Update Method	Defined dynamic domain update method	None

Attention

If IP router dial obtain a private address, dynamic DNS function is not available.

3.3.12 Bridge Interface

From navigation panel "Network/Bridge " menu, enter "Bridge 1" page, set related parameters, as shown in Figure 3-51.



Bridge ID: 1

Bridge

Primary IP
IP Address: 10.100.0.1
Netmask: 255.255.0.0
Secondary IP(s)

IP Address	Netmask

Bridge Member

dot11radio 1	dot11radio 2	vlan 1
☑	☑	□

Figure 3-51 Bridge 1

Page description is shown in Table 3-26.

Table 3-26 Ethernet Interface Parameter Description

Parameters	Description	Default
Bridge ID	Bridge number can only be assigned to 1	None
Bridge Interface		
IP address and subnet mask of primary address	Configure or change the primary IP address and subnet mask as needed.	None
IP address and subnet mask of secondary address	In addition to primary IP from outside, clients also can be equipped with secondary IP address and subnet mask	None
Bridge Member		
Click enable bridge interface		None

3.4 Link Backup

3.4.1 SLA

Basic Concepts and Principles

Under normal circumstances, the edge router can detect if the link linked to the ISP is in fault. If the network linking to one ISP is in fault, another ISP will be used to transmit all the data streams. However, if the link of an ISP is normal and the infrastructure fails, the edge router will continue to use this route. Then, the data is no longer reachable.

One feasible solution is to using static routing or policy-based routing to first test the reachability of important destination. If it is unreachable, the static routing will be deleted.

The reachability test can be performed with InHand SLA to continuously check the reachability of ISP and be associated with static routing.

Basic principles of InHand SLA: 1.Object track: Track the reachability of the specified object. 2. SLA probe: The object track function can use InHand SLA to send different types of detections to the object. 3. Policy-based routing using route mapping table: It associates the track results with the routing process. 4. Using static routing and track options.

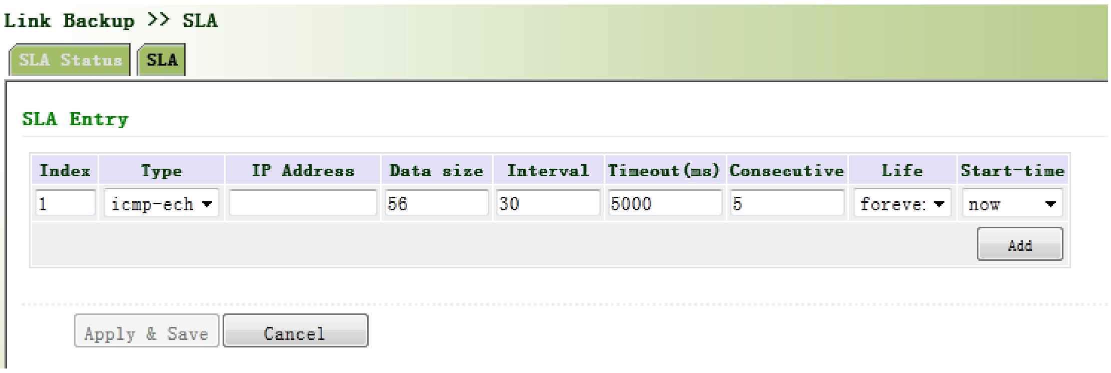
SLA Configuration Steps

Step 1: Define one or more SLA operations (detection).

Step 2: Define one or more track objects to track the status of SLA operation.

Step 3: Define measures associated with track objects.

From navigation panel, select Link Backup>>SLA, then enter “SLA” page, as shown in Figure 3-52.



Index	Type	IP Address	Data size	Interval	Timeout(ms)	Consecutive	Life	Start-time
1	icmp-ech		56	30	5000	5	foreve:	now

Figure 3-52 SLA

Page description is shown in Table3-27.

Table 3-27 SLA Description

Parameters	Description	Default
Index	SLAindex orID	1
Type	Detection type, default is icmp-echo, the user cannot change	icmp-echo
IP Address	Detected IP address	None
Data Size	User define data size	56
Interval	User define detection interval	30
Timeout (ms)	User define,Timeout for detection to fail	5000
Connecutive	Detection retries	5
Life	Default is "forever", user cannot change	forever
Start-time	Detection Start-time, select "now" or None	now

3.4.2 Track Module

Track is designed to achieve linkage consisting of application module, Track module and monitoring module. Linkage refers to achieve the linkage amongst different modules through the establishment of linkage items, namely, the monitoring module could trigger application module to take a certain action through Track module. Monitoring module is responsible for detection of link status, network performance and notification to application module of detection results via Track module. Once the application module finds out any changes in network status, corresponding measures will be taken on a timely basis so as to avoid interruption of communication or reduction of service quality.

Track module is located between application module and monitoring module with main functions of shielding the differences of different monitoring modules and providing uniform interfaces for application module.

Track Module and Monitoring Module Linkage

Through configuration, the linkage relationship between Track module and monitoring module is established. Monitoring module is responsible for detection of link status, network performance and notification to application module of detection results via Track module so as to carry out timely change of the status of Track item:

- Successful detection, corresponding track item is Positive
- Failed detection, corresponding track item is Negative

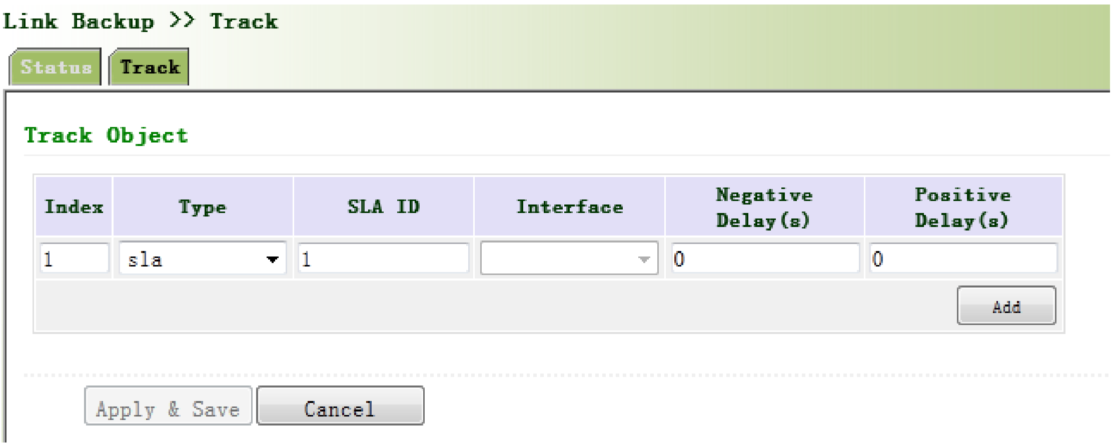
Track Module and Application Module Linkage

Through configuration, the linkage relationship between Track module and application module is established. In case of any changes in track item, a notification requiring correspondent treatment will be sent to application module.

Currently, application modules which could achieve linkage with track module include: VRRP, static routing, strategy-based routing and interface backup.

Under certain circumstances, once any changes in Track item are founded, if a timely notification is sent to application module, then communication may be interrupted due to routing's failure in timely restoration and other reasons. For example, Master router in VRRP backup group could monitor the status of upstream interface through Track. In case of any fault in upstream interface, Master router will be notified to reduce priority so that Backup router may ascend to the new Master to be responsible for relay of message. Once upstream interface is recovered, so long as Track immediately sends a message to original Master router to recover priority, then the router will take over the task of message relay. At that time, message relay failure may occur since the router has not restored to the upstream router. Under such circumstances, user to configure that once any changes take place in Track item, delays a period of time to notify the application module.

From navigation panel, select Link Backup/Track, then enter "Track" page, as shown Figure 3-53.



Track Object

Index	Type	SLA ID	Interface	Negative Delay(s)	Positive Delay(s)
1	sla	1		0	0

Figure 3-53Track M

Page description is shown in Table 3-28.

Table 3-28 Track Description

Parameters	Description	Default
Index	Track index orID	1
Type	Default “sla”,User cannot change	sla
SLA ID	Defined SLA Index or ID	None
Interface	Detect interface’s up/down state	cellular 1
Negative Delay (m)	In case of negative status, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching.	0
Positive Delay (m)	In case of failure recovery, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching.	0

3.4.3 VRRP

Default route provides convenience for user’s configuration operations but also imposes high requirements on stability of the default gateway device. All hosts in the same network segment are set up with an identical default route with gateway being the next hop in general. When fault occurs on gateway, all hosts with the gateway being default route in the network segment can’t communicate with external network.

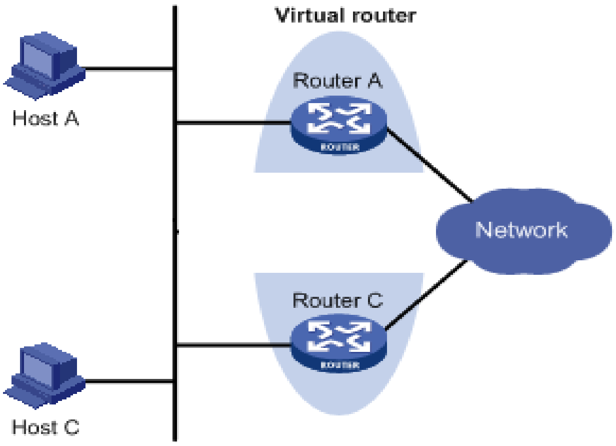
Increasing exit gateway is a common method for improving system reliability. Then, the problem to be solved is how to select route among multiple exits. VRRP (Virtual Router Redundancy Protocol) adds a set of routers that can undertake gateway function into a backup group to form a virtual router. The election mechanism of VRRP will decide which router to undertake the forwarding task and the host in LAN is only required to configure the default gateway for the virtual router.

VRRP will bring together a set of routers in LAN. It consists of multiple routers and is similar to a virtual router in respect of function. According to the vlan interface ip of different network segments, it can be virtualized into multiple virtual routers. Each virtual router has an ID number and up to 255 can be virtualized.

VRRP has the following characteristics:

- Virtual router has an IP address, known as the Virtual IP address. For the host in LAN, it is only required to know the IP address of virtual router, and set it as the address of the next hop of the default route.
- Host in the network communicates with the external network through this virtual router.
- 1 router will be selected from the set of routers based on priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in case of fault of gateway router, thus to guarantee uninterrupted communication between the host and external network

VRRP Networking Scheme：

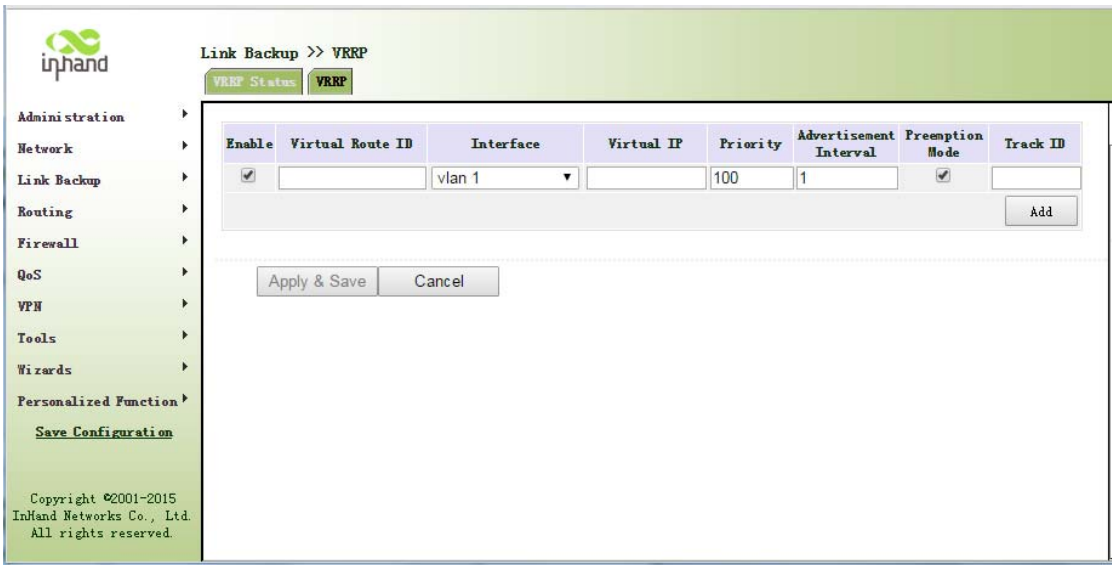


As shown in Figure above, Router A and Router C compose a virtual router. This virtual router has its own IP address. The host in LAN will set the virtual router as the default gateway. Router A or Router C, the one with the highest priority, will be used as the gateway router to undertake the function of gateway. Another router will be used as a Backup router.

Monitor interface function of VRRP better expands backup function: the backup function can be offered when interface of a certain router has fault or other interfaces of the router are unavailable.

When interface connected with the uplink is at the state of Down or Removed, the router actively reduces its priority so that the priority of other routers in the backup group is higher and thus the router with highest priority becomes the gateway for the transmission task.

From navigation panel, select Link Backup/VRRP, then enter “VRRP” page, as shown in Figure 3-54.



Enable	Virtual Route ID	Interface	Virtual IP	Priority	Advertisement Interval	Preemption Mode	Track ID
☑		vlan 1 ▾		100	1	☑	

Figure 3-54 VRRP

Page description is shown in Table 3-29.

Table 3-29 VRRP Description

Parameters	Description	Default
Enable	Enable/Disable	Enable
Virtual Route ID	User define Virtual Route ID	None
Interface	Configure the interface of Virtual Route	vlan1
Virtual IP Address	Configure the IP address of Virtual Route	None
Priority	The VRRP priority range is 0-255 (a larger number indicates a higher priority). The router with higher priority will be more likely to become the gateway router.	100
Advertisement Interval	Heartbeat package transmission time interval between routers in the virtual ip group	1
Preemption Mode	If the router works in the preemptive mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually	Enable

	replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	
Track ID	Trace Detection, select the defined Track index or ID	None

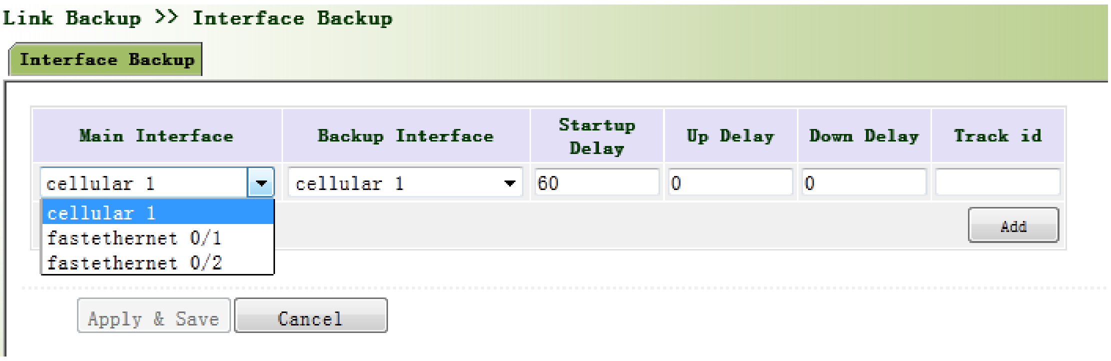
3.4.4 Interface Backup

Interface backup refers to backup relationship formed between appointed interfaces in the same equipment. When service transmission can’t be carried out normally due to fault of a certain interface or lack of bandwidth, rate of flow can be switched to backup interface quickly and the backup interface will carry out service transmission and share network flow so as to raise reliability of communication of data equipment.

When link state of main interface is switched from up to down, system will wait for preset delay first instead of switching to link of backup interface immediately. Only if the state of main interface still keeps down after the delay, system will switch to link of backup interface. Otherwise, system will not switch.

After link state of main interface is switched from down to up, system will wait for preset delay first instead of switching back to main interface immediately. Only if state of main interface still keeps up after the delay, system will switch back to main interface. Otherwise, system will not switch.

From navigation panel, select Link Backup/Interface Backup, then enter “Interface Backup” page, as shown in Figure 3-55.


Link Backup >> Interface Backup

Interface Backup

Main Interface	Backup Interface	Startup Delay	Up Delay	Down Delay	Track id
cellular 1	cellular 1	60	0	0	

Figure 3-55 Interface Backup

Page description is shown in Table 3-30.

Table 3-30 Interface Backup Description

Parameters	Description	Default
Primary Interface	The interface being used	cellular 1
Backup Interface	Interface to be switched	cellular 1
Start-up Delay	Set how long to wait for the start-up tracking detection policy to take effect	60
Up Delay	When the primary interface switches from failed detection to successful detection, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching.	0
Down Delay	When the primary interface switches from successful detection to failed detection, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching.	0
Track ID	Trace Detection, select the definedTrack index or ID	None

3.5 Routing

3.5.1 Static Route

Static routing is a special routing that requires your manual setting. After setting static routing, the package for the specified destination will be forwarded according to the path designated by you. In the network with relatively simple networking structure, it is required to set static routing to achieve network interworking. Proper setting and use static routing can improve the performance of network and can guarantee bandwidth for important network applications.

Disadvantages of static routing: It cannot automatically adapt to the changes in the network topology. The network failure or changes in topology may cause the route unreachable and network interrupted. Then, you are required to manually modify the setting of static routing.

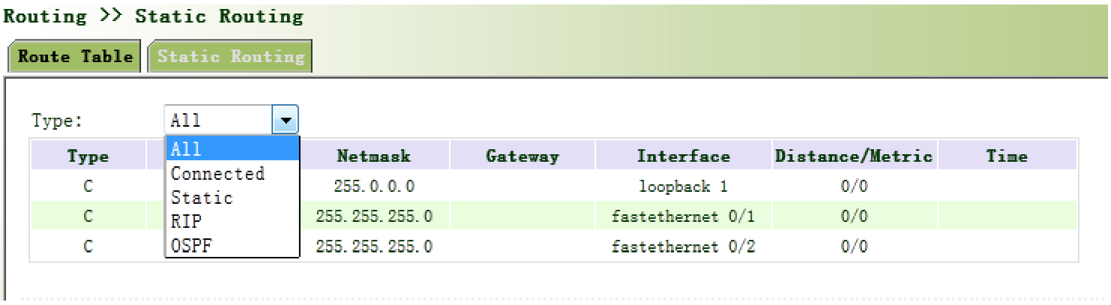
Static Routing performs different purposes in different network environments.

- When the network structure is comparatively simple, the network can work normally only with Static Routing.

- While in complex network environment, Static Routing can improve the performance of network and ensure bandwidth for important application.
- Static Routing can be used in VPN examples, mainly for the management of VPN route.

3.5.1.1 Routing Status

From navigation panel, select Routing/Static Routing, then enter “Route Table” page, as shown in Figure 3-56.



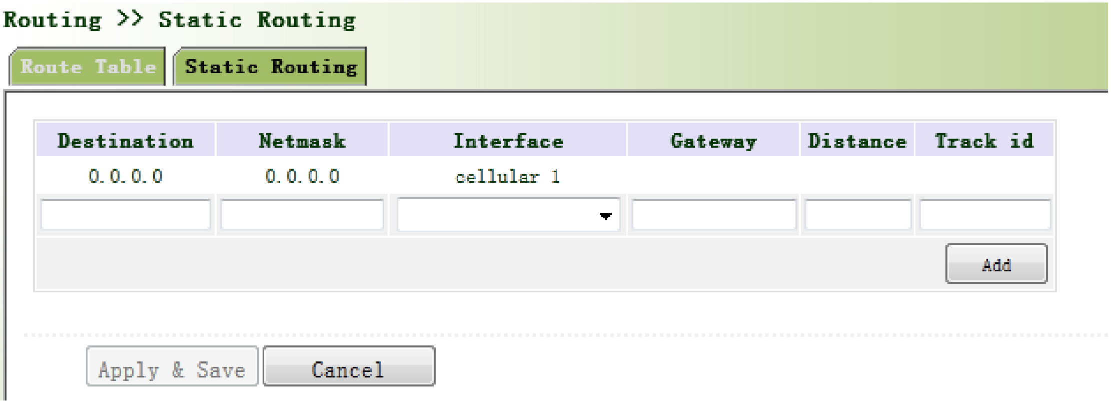
Type: All

Type		Netmask	Gateway	Interface	Distance/Metric	Time
C		255.0.0.0		loopback 1	0/0	
C		255.255.255.0		fastethernet 0/1	0/0	
C		255.255.255.0		fastethernet 0/2	0/0	

Figure 3-56 Routing Status

3.5.1.2 Static Routing

From navigation panel, select Routing/Static Routing, then enter “Static Routing,” page. Add/delete additional Router static routing. Normally users don not need to configure this item, as shown in 3-57.



Destination	Netmask	Interface	Gateway	Distance	Track id
0.0.0.0	0.0.0.0	cellular 1			

Figure 3-57 Static Routing

Page description is shown in Table 3-31.

Table 3-31Static Routing Description

Parameters	Description	Default

Destination address	Enter the destination IP address need to be reached	None
Subnet Mask	Enter the subnet mask of destination address need to be reached	None
Interface	The interface through which the data reaches the destination address	None
Gateway	IP address of the next router to be passed by before the input data reaches the destination address	None
Distance	Priority, smaller value contributes to higher priority	None
Track ID	Select the definedTrack index or ID	None

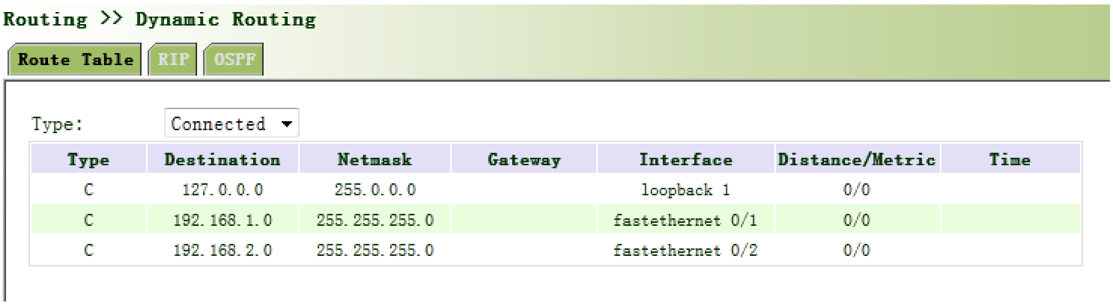
3.5.2 Dynamic Routing

The routing table entry on dynamic router is obtained in accordance with certain algorithm optimization through the information exchange between the connected routers, while the routing information is continuously updating in certain time slot so as to adapt to the continuously changing network and obtain the optimized pathfinding effects at any time.

In order to achieve efficient pathfinding of IP packet, IETF has developed a variety of pathfinding protocols, including Open Shortest Path First (OSPF) and Routing Information Protocol (RIP) for Autonomous System (AS) interior gateway protocol. The so-called autonomous system refers to the collection of hosts, routers and other network devices under the management of the same entity (e.g. schools, businesses, or ISP)

3.5.2.1 Routing Status

From navigation panel, select Routing/Dynamic Routing, then enter “Route Table” page,as shown in Figure 3-58.



Type: Connected

Type	Destination	Netmask	Gateway	Interface	Distance/Metric	Time
C	127.0.0.0	255.0.0.0		loopback 1	0/0	
C	192.168.1.0	255.255.255.0		fastethernet 0/1	0/0	
C	192.168.2.0	255.255.255.0		fastethernet 0/2	0/0	

Figure 3-58Routing Status

3.5.2.2 RIP

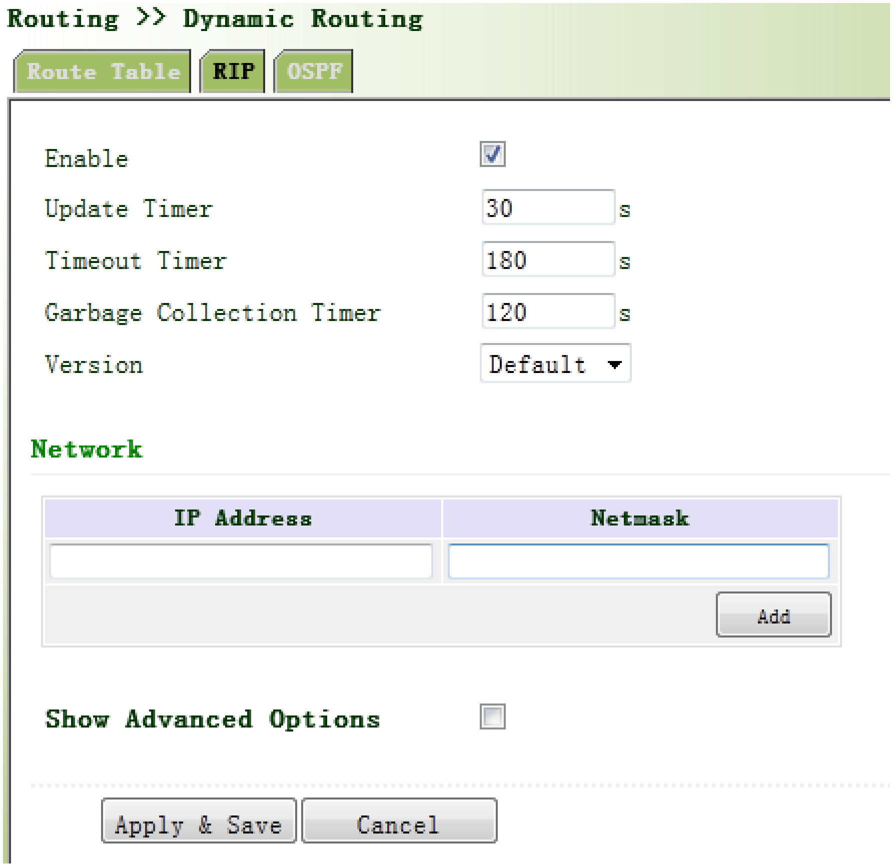
RIP (Routing Information Protocol) is a relatively simple interior gateway protocol (IGP), mainly used for smaller networks. The complex environments and large networks general do not use RIP. RIP uses Hop Count to measure the distance to the destination address and it is called RoutingCost. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to limit the convergence time, the specified RoutingCost of RIP is an integer in the range of 0~15 and hop count larger than or equal to 16 is defined as infinity, which means that the destination network or host is unreachable. Because of this limitation, the RIP is not suitable for large-scale networks. To improve performance and prevent routing loops, RIP supports split horizon function. RIP also introduces routing obtained by other routing protocols.

It is specified in RFC1058 RIP that RIP is controlled by three timers, i.e. Period update, Timeout and Garbage-Collection:

Each router that runs RIP manages a routing database, which contains routing entries to reach all reachable destinations. The routing entries contain the following information:

- Destination address: IP address of host or network.
- Address of next hop: IP address of interface of the router’s adjacent router to be passed by on the way to reach the destination.
- Output interface: The output interface for the router to forward package.
- RoutingCost: Cost for the router to reach the destination.
- Routing time: The time from the last update of router entry to the present. Each time the router entry is updated, the routing time will be reset to 0.

From navigation panel, select Routing>>Dynamic Routing, then enter “RIP” page, as shown Figure 3-59-1.



Enable ☑

Update Timer 30 s

Timeout Timer 180 s

Garbage Collection Timer 120 s

Version Default

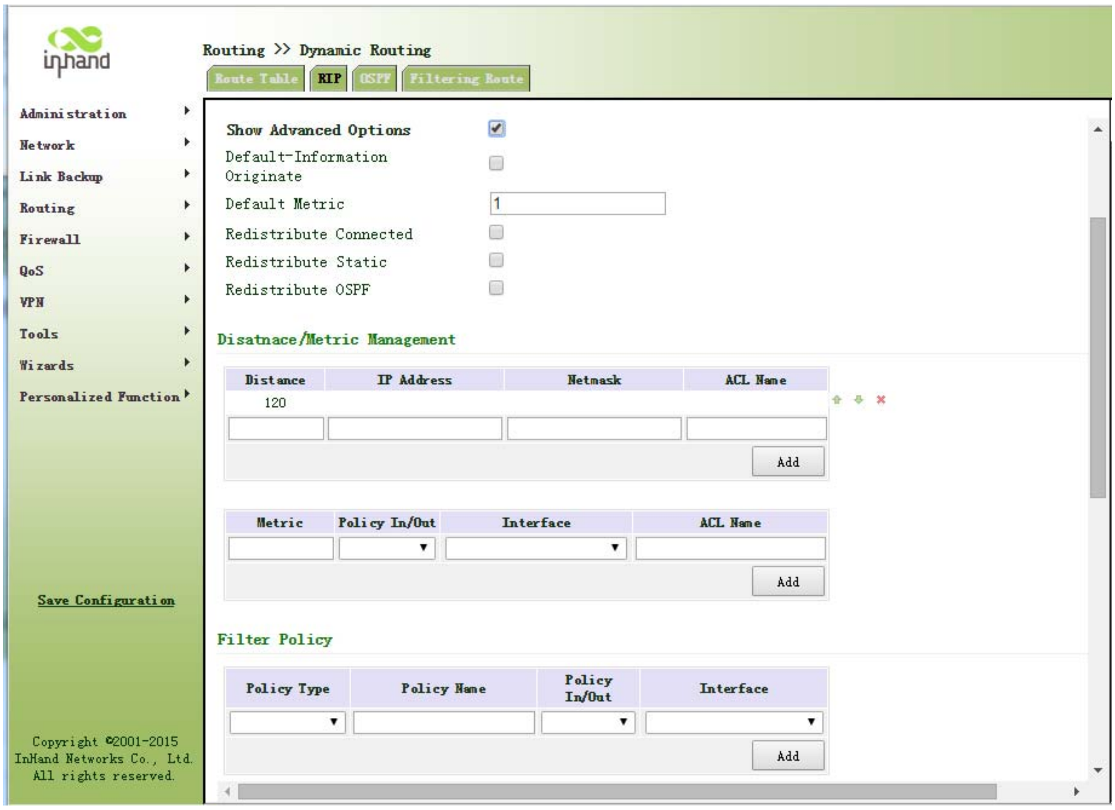
Network

IP Address	Netmask

Show Advanced Options □

Figure 3-59-1 RIP

Advanced Options are shown in Figure 3-59-2.



Show Advanced Options ☑

Default-Information Originate □

Default Metric 1

Redistribute Connected □

Redistribute Static □

Redistribute OSPF □

Disatnace/Metric Management

Distance	IP Address	Netmask	ACL Name
120			

Metric	Policy In/Out	Interface	ACL Name

Filter Policy

Policy Type	Policy Name	Policy In/Out	Interface

Copyright ©2001-2015 InHand Networks Co., Ltd. All rights reserved.

Figure 3-59-2 RIP

Page description is shown in Table 3-32.

Table 3-32 RIP Description

Parameters	Description	Default
Enable	Enable/ Disable	Disable
Update timer	It defines the interval to send routing updates	30
Timeout timer	It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16.	180
Clear Timer	It defines the time from the time when the RoutingCost of a routing becomes 16 to the time when it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the RoutingCost for sending updates of the routing. In case of timeout of Garbage-Collection and the routing still has not been updated, the routing will be completely removed from the routing table.	120
Network	The first IP addressand subnet mask of the segment	None
Advanced Options		
Default Post	Click Enable, the default information will enable publishing	Disable
Default Metric	Default cost of router to destination	1
Redirect direct route	Direct, Static, and OSP route agreement introduced to RIP route agreement	Disable
Redirect Static RoutE		Disable
Redirect OSP RoutE		Disable
Advanced Options - Distance/Metric Management		
Distance	Set RIP routing administrative distance, priority, the smaller value, the priority	120
IP address	Network number is the first IP address in network segment	None
Subnet Mask	Subnet mask, network number is subnet mask of the first IP address in network segment	None

Access List	Application of the ACL ID	None
Redirect routing metric	Rewrite default cost from route to the destination	None
Ingress/egress filtering policy	Set redirection route filtering policy (in/out)	in
Interface	Set Interface rewriting to route	None
Access List	Application of the ACL ID	None
Advanced Options - Route Filtering Policy		
Policy Type	Select the type of policy to implement	Access-list
Policy name	Custom policy name	None
Ingress/egress filtering policy	Select policy applied in the outbound or inbound	in
Interface	Select route filtering policy enforcement Interface	None
Send filtration	After enabling, only RIP packet send to the default routing interface.	Disable
Advanced Options - Interface		
Passive Interface	After enabling,only receive RIP packet, no send	Disable
RIP send version	Select Send RIP packet version	Default
RIP Receive version	Choose receive RIP packet version	Default
Horizontal split/ toxicity Flip	Select enable split horizon or poison reverse function	None
Authentication	Select the interface authentication mode	None
Key	Fill in the corresponding key	None
Advanced Options - Neighbor		
IP address	Neighbor IP address	None

3.5.2.3 OSPF

Open Shortest Path First (OSPF) is a link status based interior gateway protocol developed by IETF.

Router ID

If a router wants to run the OSPF protocol, there should be a Router ID. Router ID can be manually configured. If no Router ID is configured, the system will automatically select one IP address of interface as the Router ID.

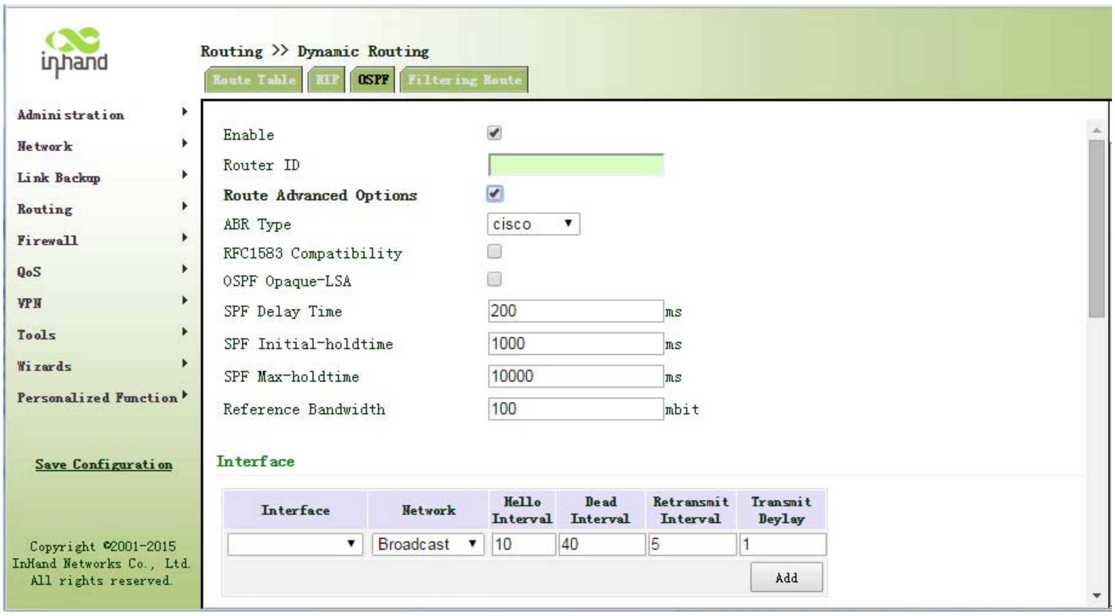
The selection order is as follows:

- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no LoopBack interface address is configured, choose the interface with the biggest IP adress from other interfaces as the Router ID.

Neighbor and Neighboring

After the start-up of OSPF router, it will send out Hello packets through the OSPF interface. Upon receipt of Hello packet, OSPF router will check the parameters defined in the packet. If both are consistent, a neighbor relationship will be formed. Not all both sides in neighbor relationship can form the adjacency relationship. It is determined based on the network type. Only when both sides successfully exchange DD packets and LSDB synchronization is achieved, the adjacency in the true sense can be formed. LSA describe the network topology around a router, LSDB describe entire network topology.

From navigation panel, select Routing/Dynamic Routing, then enter “OSPF” page,as shown in Figure 3-60.



Enable ☑

Router ID

Route Advanced Options ☑

ABR Type cisco

RFC1583 Compatibility □

OSPF Opaque-LSA □

SPF Delay Time 200 ms

SPF Initial-holdtime 1000 ms

SPF Max-holdtime 10000 ms

Reference Bandwidth 100 mbit

Interface

Interface	Network	Hello Interval	Dead Interval	Retransmit Interval	Transmit Deylay
	Broadcast	10	40	5	1

Figure 3-60 OSPF

Page description is shown in Table 3-33.

Table 3-33 OSPFDescription

Parameters	Description	Default
Enable	Enable/Disable	Disable
Router ID	RouterID of the originating the LSA	None
Interface		
Interface	The interface	None
Hello Interval	Send interval of Hello packet. If the the Hello	10

	time between two adjacent routers is different, you can not establish a neighbor relationship.	
Dead Interval	Dead Time. If no Hello packet is received from the neighbors, the neighbor is considered failed. If dead times of two adjacent routers are different, the neighbor relationship can not be established.	40
Retransmit Interval	When the router notifies an LSA to its neighbor, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbor.	5
LSA transmission delay timer	OSPF packet also need to spend time when traveling on links, so LSA aging time (age) before transferring to add a delay time, in the low-speed links require consideration of configuration.	1
Interface - Interface Advanced Options		
Interface Name	Configure OSPF interface parameters	None
Passive Interface	After enabling,only receive RIP packet, no send	Disable
Interface Cost	By default, an interface computes its cost according to the bandwidth	10
Protocol Priority	Configure OSPF router interface priority	10
Network		
IP Address	IP Address of local network	None
Subnet Mask	Subnet Mask of IP Address of local network	None
Area ID	Area ID of router which originating LSA	None

3.5.2.4 Filtering Route

Click navigation panel “Routing/Dynamic Routing” menu, enter “Filtering Route” interface, as shown in Figure 3-61.

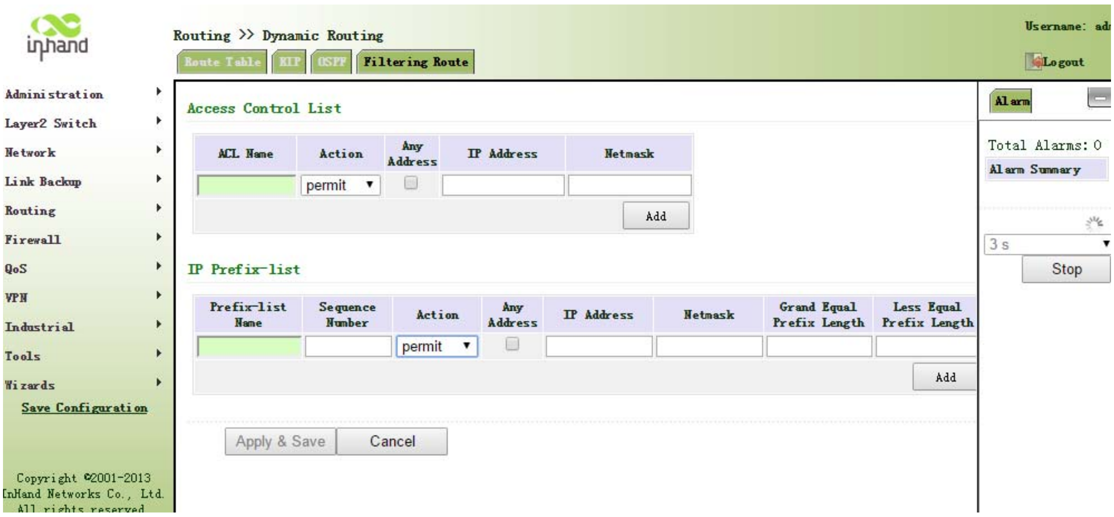


Figure 3-61Filtering Route

Page description is shown in Table 3-34.

Table 3-34 Filtering Route Description

Parameter	Description	Default
Access Control List		
Access list	User defined	None
Action	Permit and deny	Permit
Any Address	Any address after clicking, no matching IP address and subnet mask again	Disable

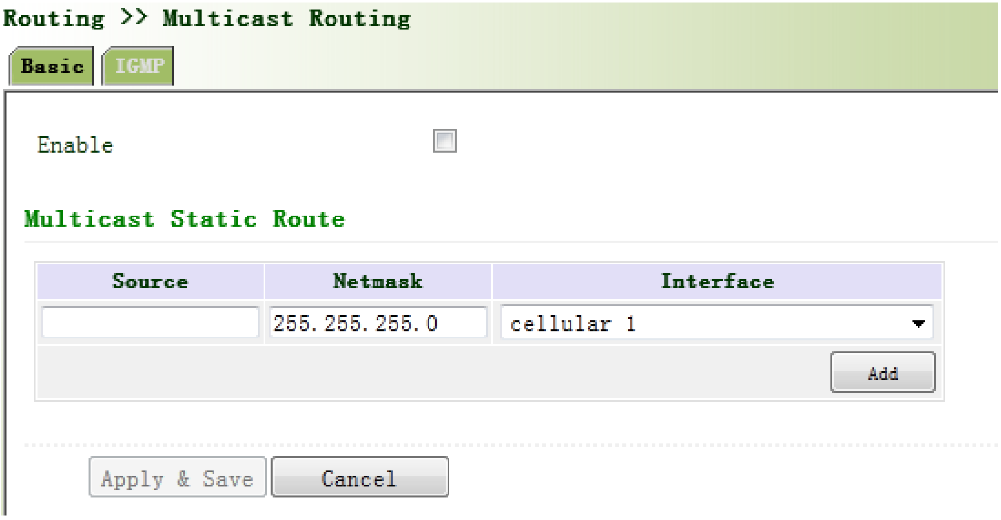
3.5.3 Multicast Routing

Multicast routing sets up an acyclic data transmission route from data source end to multiple receiving ends, which refers to the establishment of a multicast distribution tree. The multicast routing protocol is used for establishing and maintaining the multicast routing and forrelaying multicast data packet correctly and efficiently.

3.5.3.1 Basic Settings

The basic is mainly to define the source of multicast routing.

From navigation panel, select Routing/Multicast Routing, then enter “Basic” page,as shown in Figure 3-62.



Routing >> Multicast Routing

Enable □

Multicast Static Route

Source	Netmask	Interface
	255.255.255.0	cellular 1

Figure 3-62 Basic Settings

Page description is shown in Table 3-35.

Table 3-35 Basic Settings Description

Parameters	Description	Default
Enable	Open/Close	Close
Source	IP Address of Source	None
Netmask	Netmask of Source	255.255.255.0

3.5.3.2 IGMP

IGMP, being a multicast protocol in Internet protocol family, which is used for IP host to report its constitution to any directly adjacent router, defines the way for multicast communication of hosts amongst different network segments with precondition that the router itself supports multicast and is used for setting and maintaining the relationship between multicast members between IP host and the directly adjacent multicast routing. IGMP defines the way for maintenance of member information between host and multicast routing in a network segment.

In the multicast communication model, sender, without paying attention to the position information of receiver, only needs to send data to the appointed destination address, while the information about receiver will be collected and maintained by network facility. IGMP is such a signaling mechanism for a host used in the network segment of receiver to the router. IGMP informs the router the information about members and the router will acquire whether the multicast member exists on the subnet connected with the router via IGMP.

Function of multicast routing protocol:

- Discovering upstream interface and interface closest to the source for the reason that multicast routing protocol only cares the shortest route to the source.
- Deciding the real downstream interface via (S, G). A multicast tree will be finished after all routers acquire their upstream and downstream interfaces with root being router directly connected with the source host and branches being routers directly connected via subnet with member discovered by IGMP.
- Managing multicast tree. The message can be transferred once the address of next hop can be acquired by unicast routing, while multicast refers to relay message generated by source to a group.

From navigation panel, select Routing/Multicast Routing, then enter “IGMP” page,as shown in Figure 3-63.

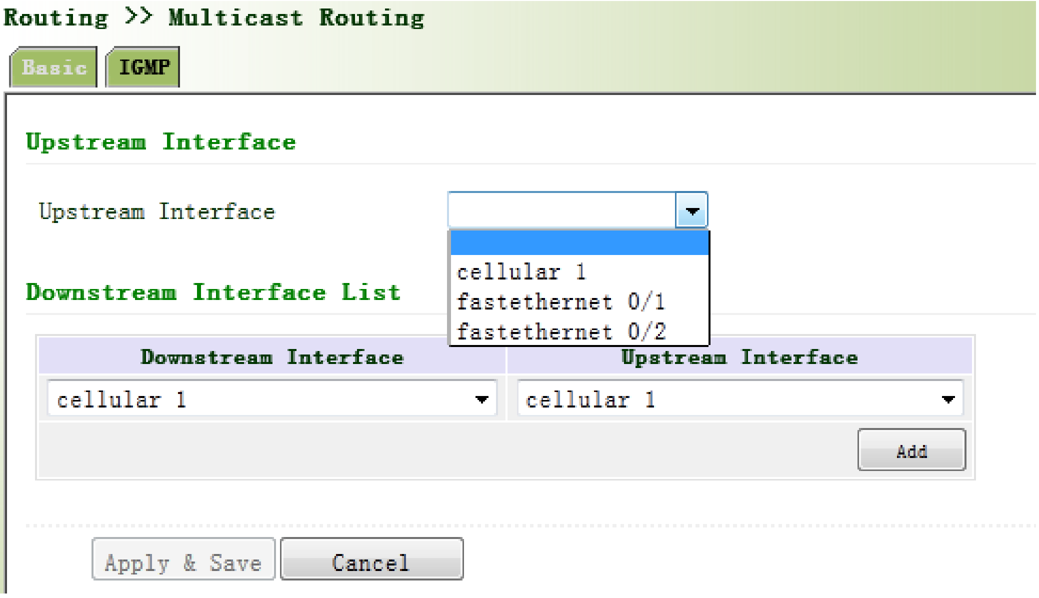


Figure 3-63 IGMP

Page description is shown in Table 3-36.

Table 3-36 IGMP Description

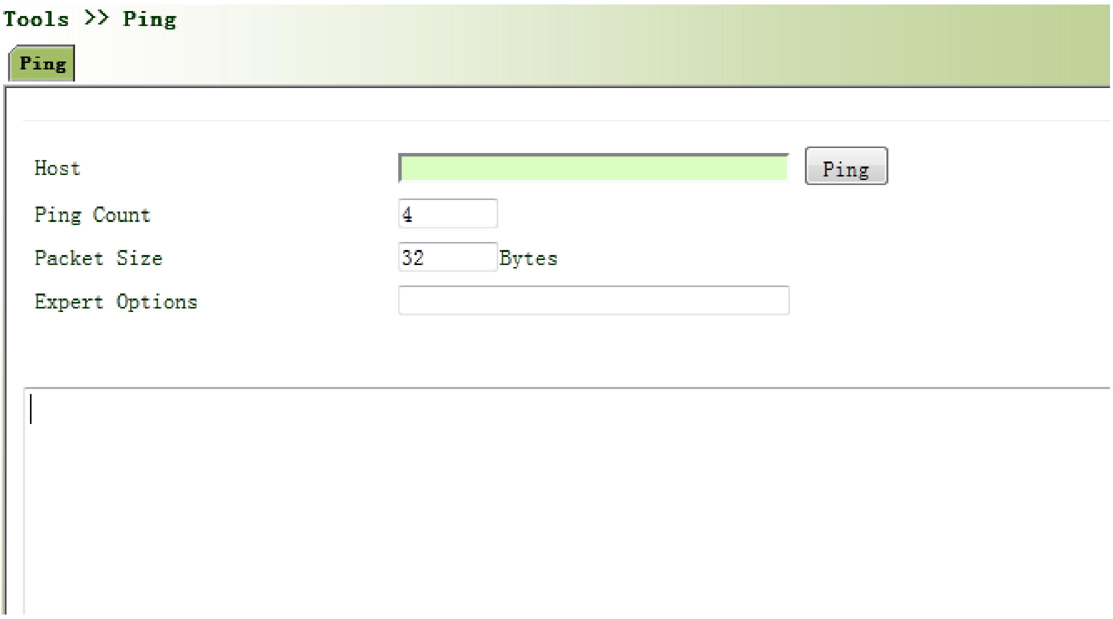
Parameters	Description	Default
Uplink Interface		
Uplink Interface	link to upper network device interface	None
Downlink Interface		
Downlink Interface	link to terminal equipment interface	cellular 1
Uplink Interface	link to upper network device interface	cellular 1

3.6 Tools

3.6.1 PING

Help to PING internet through route.

From navigation panel, select Tools/Ping, then enter "Ping" page, as shown in Figure 3-64.



Tools >> Ping

Ping

Host

Ping Count 4

Packet Size 32 Bytes

Expert Options

Figure 3-64 PING

Page description is shown in Table 3-37.

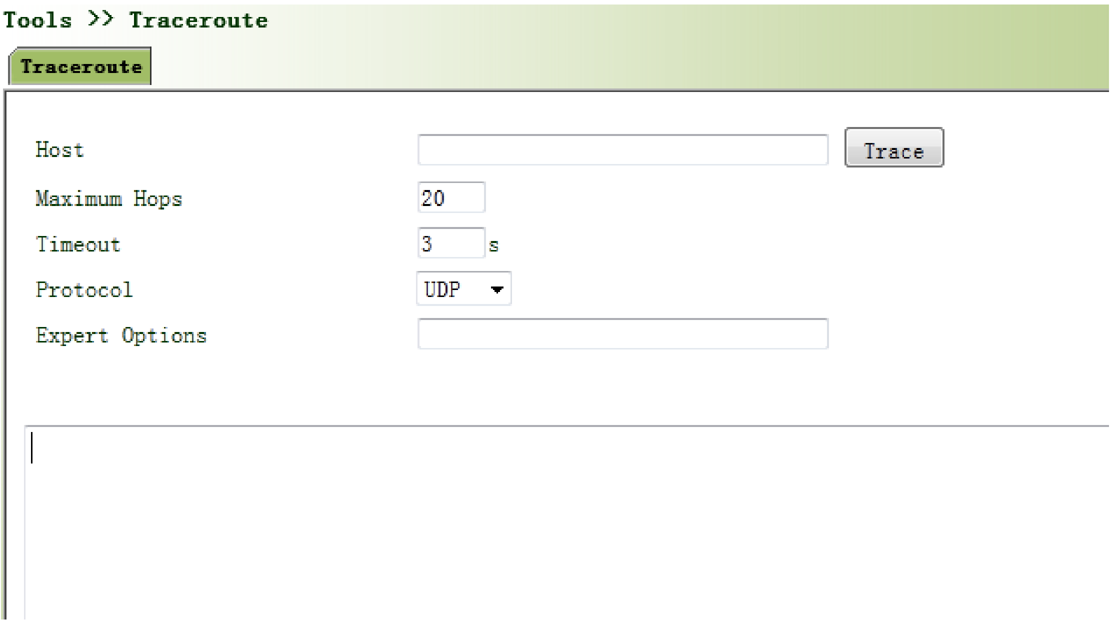
Table 3-37 PING Description

Parameters	Description	Default
Host	It requires the destination host address of PING detection	192.168.2.1
Ping Count	Set Ping detection count	4
Packet Size	Set packet size of ping detection	32 bytes
Expert Options	Advanced parameters of ping can be used	None

3.6.2 Routing Detection

It is used to detect network routing failure.

From navigation panel, select Tools/Traceroute, then enter "Traceroute" page, as shown in Figure 3-65.



Tools >> Traceroute

Traceroute

Host

Maximum Hops 20

Timeout 3 s

Protocol UDP

Expert Options

Figure 3-65 Traceroute

Page description is shown in Table 3-38.

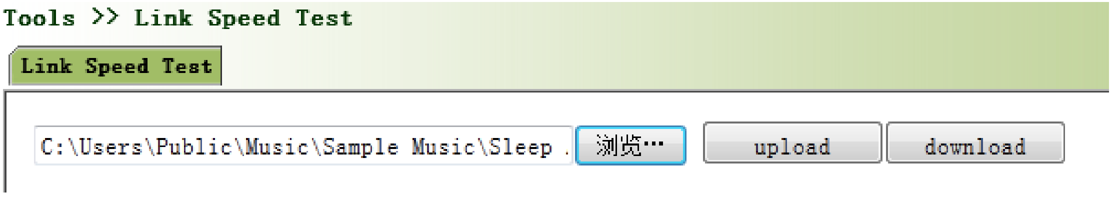
Table 3-38 Traceroute Description

Parameters	Description	Default
Host	Host address needs to detect	192.168.2.1
Maxium Hops	Set the maxium hops of routing detection	20
Timeout	Set timeout of routing detection	3 secs
Protocol	Select ICMP/UDP	UDP
Expert Options	Advanced parameters of ping can be used	None

3.6.3 Link Speed Test

Through upload and download files, link speed can be tested.

From navigation panel, select Tools/Link Speed Test, then enter “Link Speed Test” page,as shown in Figure 3-66.



Tools >> Link Speed Test

Link Speed Test

C:\Users\Public\Music\Sample Music\Sleep .

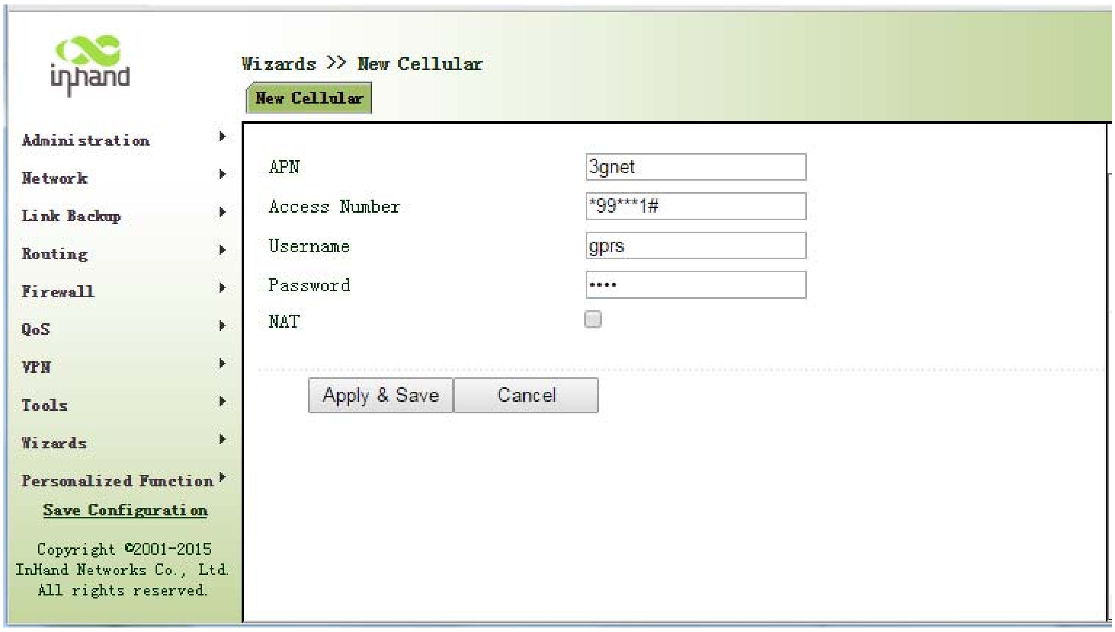
Figure 3-66 Link Speed Test

3.7 Installation Guide

Simplify general configuration, where the router with fast, simple, basic configuration, configuration result can not be displayed here, but view it when finished in a specific corresponding configuration setting.

3.7.1 New Dial

From navigation panel "Wizards/New Cellular" menu, enter " New Cellular " page, as shown in Figure 3-67.



APN 3gnet
Access Number *99***1#
Username gprs
Password ••••
NAT □

Figure 3-67 New Cellular

Page description is shown in Table 3-39.

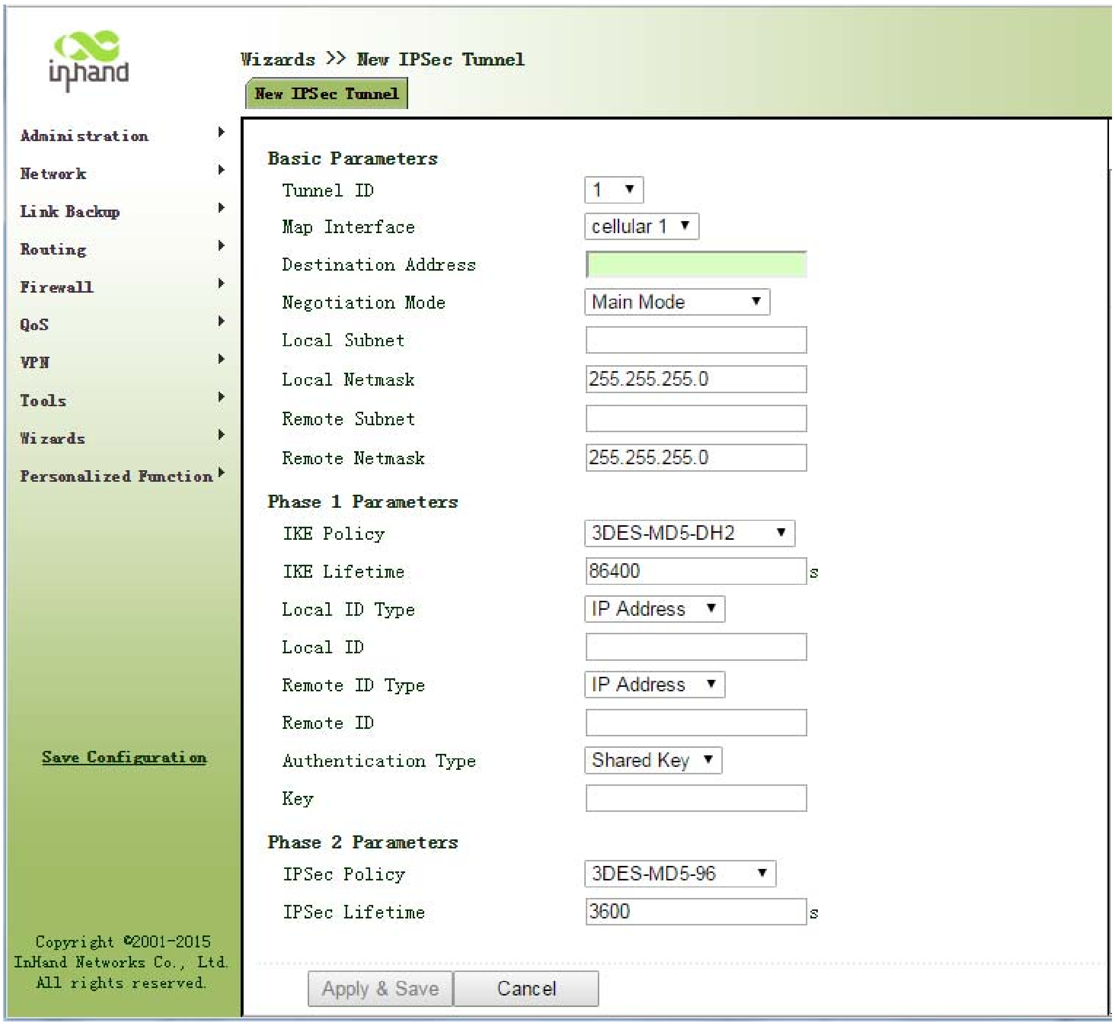
Table 3-39 New Cellular Description

Parameters	Description	Default
APN	Select New WAN Interface	3gnet
Access number	Mobile operator provide dial-up parameters (please choose according to the local operator)	*99***1#
User name	Mobile operator provide dial-up parameters (please choose according to the local operator)	gprs
password	Mobile operator provide dial-up parameters (please choose according to the local operator)	●●●●
Network Address	Click Enable, put private IP address converted into a public IP address	Disable

Translation		

3.7.2 New IPSec Tunnel

From navigation panel" Wizards /New IPSec Tunnel" menu, enter "New IPSec Tunnel" page, as shown in Figure 3-68.



Basic Parameters

Tunnel ID: 1

Map Interface: cellular 1

Destination Address:

Negotiation Mode: Main Mode

Local Subnet:

Local Netmask: 255.255.255.0

Remote Subnet:

Remote Netmask: 255.255.255.0

Phase 1 Parameters

IKE Policy: 3DES-MD5-DH2

IKE Lifetime: 86400 s

Local ID Type: IP Address

Local ID:

Remote ID Type: IP Address

Remote ID:

Authentication Type: Shared Key

Key:

Phase 2 Parameters

IPSec Policy: 3DES-MD5-96

IPSec Lifetime: 3600 s

Table 3-68 New IPSec Tunnel

Page description is shown in Table3-40.

Table 3-40 New IPSec Tunnel Description

Parameters	Description	Default
Basic		
Tunnel No.	Set Tunnel No.	1
Interface Name	Select Interface Name	cellular 1
Peer Address	Set VPN peer IP	None
Negotiation Mode	Optional main mode, aggressive mode. (Usually	Main mode

	select main mode)	
Local subnet address	Set IPSec local protection subnet	None
Local Subnet Mask	Set IPSec local protection subnet mask	255.255.255.0
Peer subnet address	Set IPSec peer protection subnet	None
Peer subnet mask	Set IPSec peer protection subnet mask	255.255.255.0
Phase 1		
IKE Policy	Optional 3DES-MD5-DH1 or 3DES-MD5-DH2, etc.	3DES-MD5-DH2
IKE Life Cycle	Set IKE Life Cycle	86400sec
Local Identity Type	Optional FQDN, USER FQDN, IP address	IP address
Local Index	Only in FQDN and USER FQDN. Fill in the appropriate identification according to the selected identity type (USER FQDN should be a standard mailbox format)	None
Peer Identity Type	Optional FQDN, USER FQDN, IP address	IP address
Peer Index	Only in FQDN and USER FQDN. Fill in the appropriate identification according to the selected identity type (USER FQDN should be a standard mailbox format)	None
Authentication	Choose to share keys and digital certificates	share keys
Key	Authentication mode select shared keys show the feature. Set IPSec VPN agreement key	None
Phase 2		
IPSec Policy	Optional 3DES-MD5-96 or 3DES -SHA1-96 etc.	3DES-MD5-96
IPSec Life Cycle	Set IPSec Life Cycle	3600sec

⚠ **Attention**

Create inbound and outbound rules to each tunnel collection. If only to create a one-way connection filter, the rule is not applied.

3.8 Personalization Features

According to the specific needs of individual customers, private custom functions can be equipped to InPortal.

3.8.1 Nginx Server

Set hard disk server function. After opening captive portal loginb, user share hard disk data.

From navigation panel "Personalized Function/Nginx" menu, enter "Nginx" page, as shown in Figure 3-69.

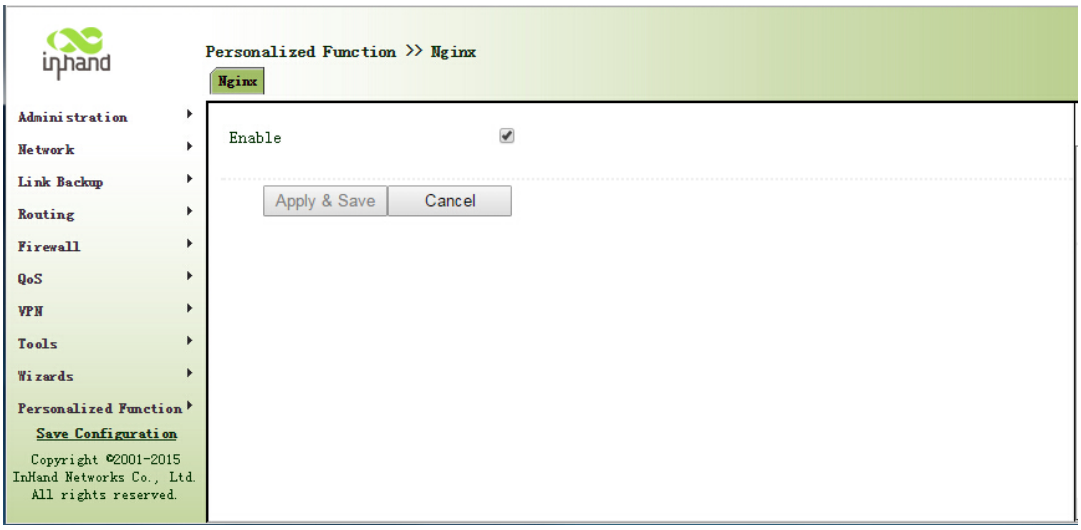


Figure 3-69 Nginx

3.8.2 File Synchronization

From navigation panel "Personalized Function/File Synchronization" menu, enter "File Synchronization" page, as shown in Figure 3-70.

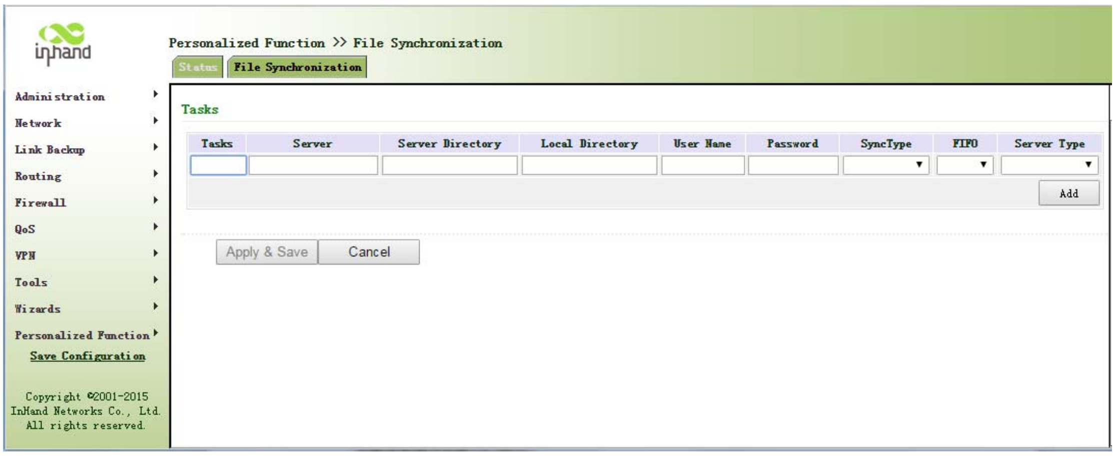


Figure 3-70 File Synchronization

Page description is shown in Table 3-41.

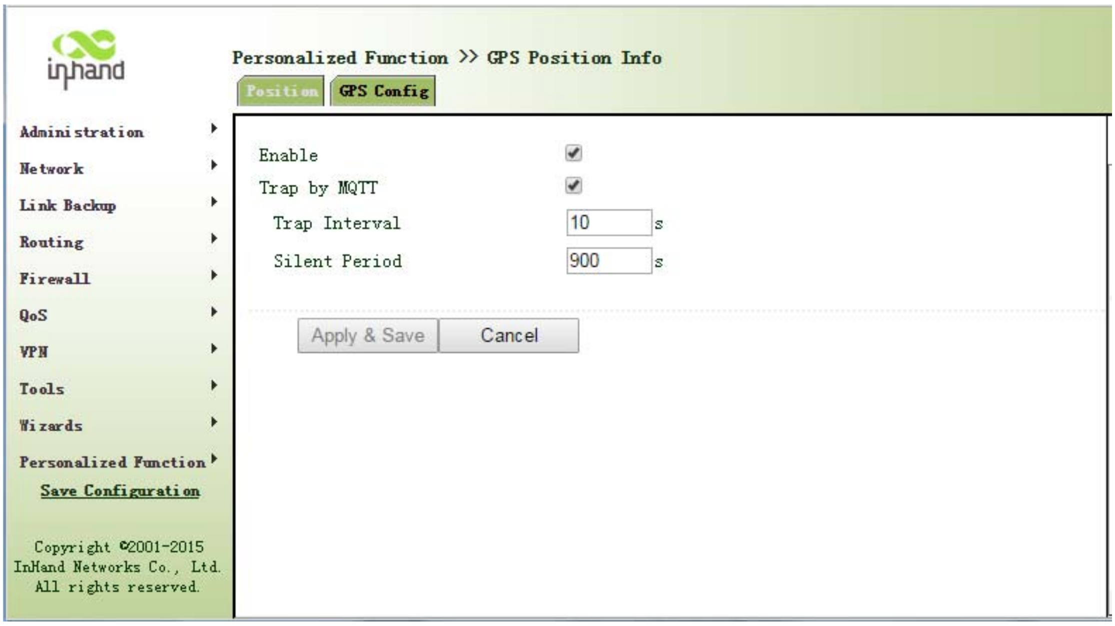
Table 3-41 File Synchronization Description

Parameters	Description	Default
Task	User-defined task name	None
Server	Rsync Server Address	None

Server Directory	Synchronize files to Rsync server address	None
Local Directory	Synchronize files to local directory	None
User name	Rsync server name	None
Password	Rsync server password	None

3.8.3 GPS Location Information

From navigation panel "Personalized Function /GPS Config"menu, enter " GPS Config " page, shown in Figure 3-71.



Enable ☑
Trap by MQTT ☑
Trap Interval 10 s
Silent Period 900 s

Figure 3-71GPS Settings

Page description is shown in Table 3-42.

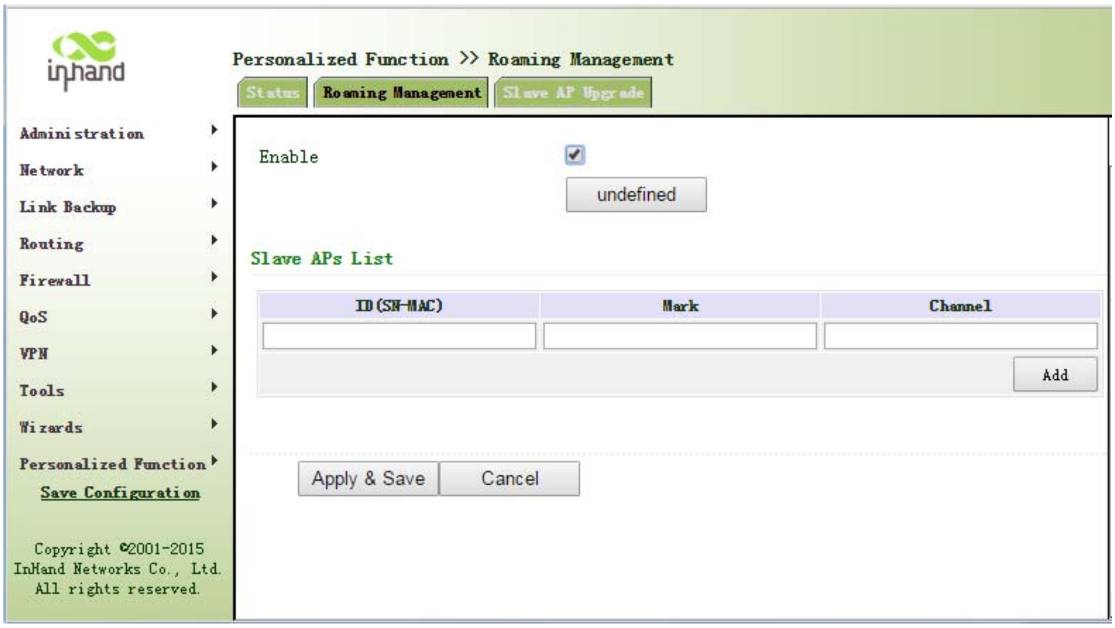
Table 3-42 GPS Config Description

Parameters	Description	Default
Server	upload location information server IP address	None
Port	Upload location information server port	80
Positioning time interval	Set positioning time interval	60
Upload Location information gap	Set upload Location information gap	60

3.8.4 Roaming Management

3.8.4.1 Roaming Management

From navigation panel “Personalized Function /Roaming Management" menu, enter "Roaming Management" page, shown in Figure 3-72.



Enable ☑

Slave APs List

ID(SN-MAC)	Mark	Channel

Figure 3-72 Roaming Management

3.8.4.2 Upgrade from AP

From navigation panel "Personalized Function /Roaming Management" menu, enter "Slave AP Upgrade" page, as shown in Figure 3-73.

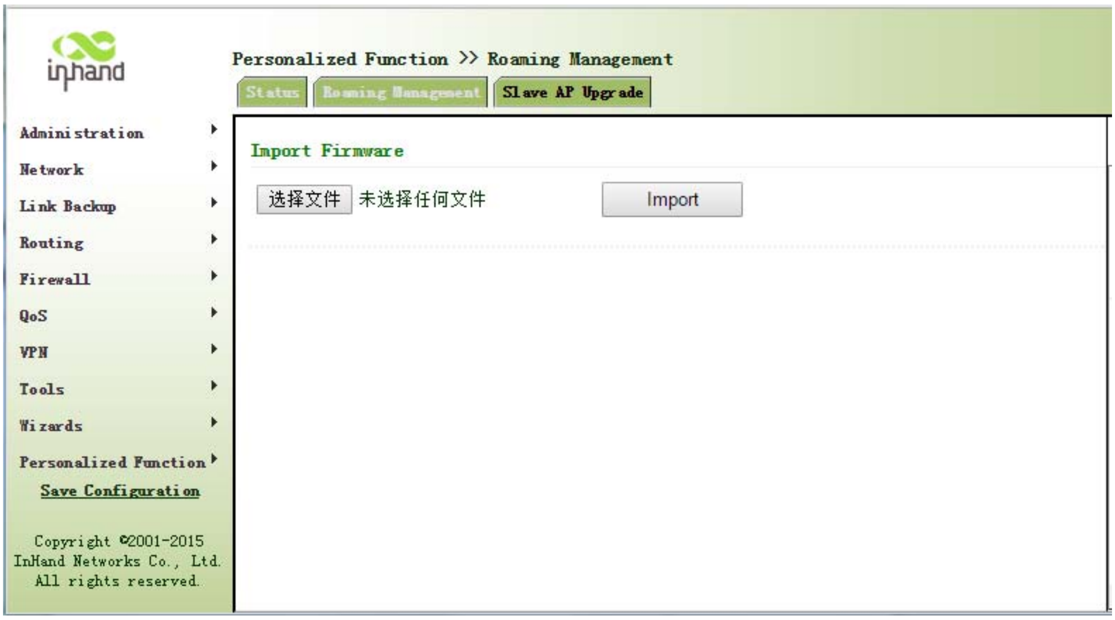


Figure 3-73 Slave AP Upgrade

3.9 Firewall

With the expansion of network and increase in flow, the control over network safety and the allocation of bandwidth become the important contents of network management. The firewall function of the router implements corresponding control to data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of message (such as: protocol style, source/destination IP address, etc.) and ensures safe operation of router and host in local area network.

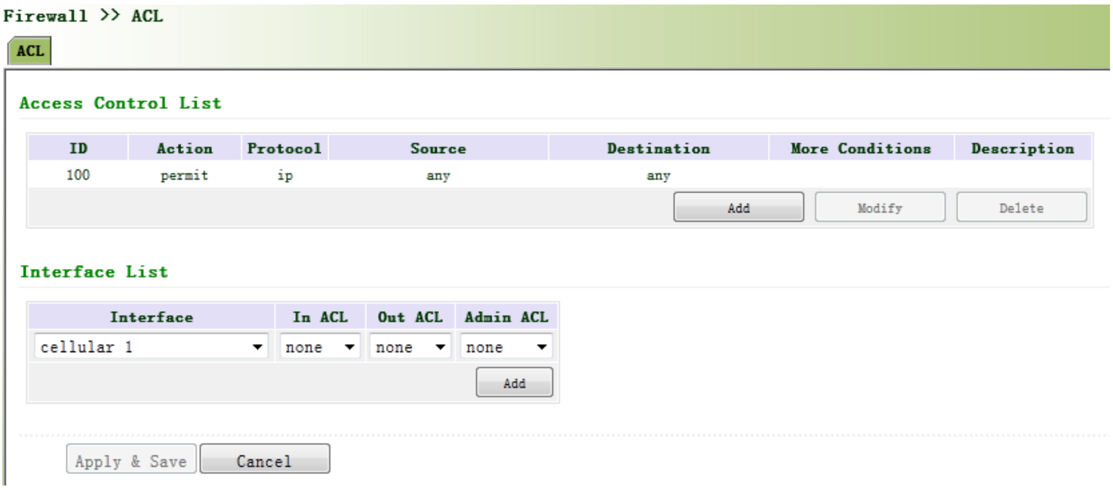
3.9.1 Access Control（ACL）

ACL, namely access control list, implements permission or prohibition of access for appointed data flow (such as prescribed source IP address and account number, etc.) via configuration of a series of matching rules so as to filter the network interface data. After message is received by port of router, the field is analyzed according to ACL rule applied on the current port. And after the special message is identified, the permission or prohibition of corresponding packet is implemented according to preset strategy.

ACL classifies data packages through a series of matching conditions. These conditions can be data packages' source MAC address, destination MAC address, source IP address, destination IP address, port number, etc.

The data package matching rules as defined by ACL can also be used by other functions requiring flow distinguish.

From navigation panel, select Firewall/ACL, then enter "ACL" page, as shown in Figure 3-74-1.



Access Control List

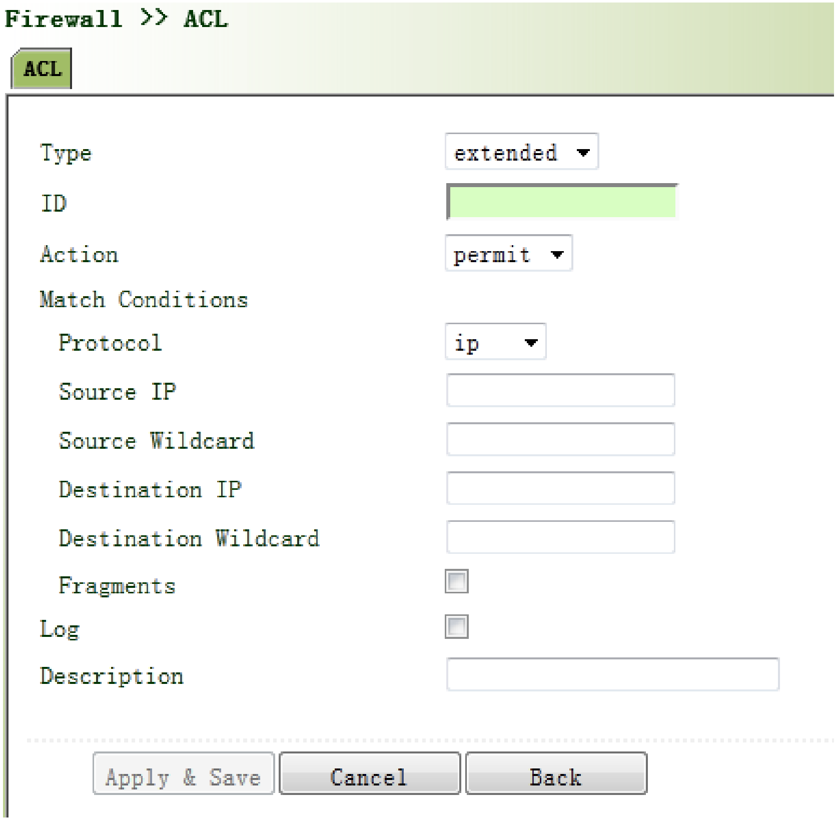
ID	Action	Protocol	Source	Destination	More Conditions	Description
100	permit	ip	any	any		

Interface List

Interface	In ACL	Out ACL	Admin ACL
cellular 1	none	none	none

Figure 3-74-1 Access Control（ACL）

Click <Add> to add new access control list, as shown in Figure 3-74-2.



Type	extended
ID	
Action	permit
Match Conditions	
Protocol	ip
Source IP	
Source Wildcard	
Destination IP	
Destination Wildcard	
Fragments	□
Log	□
Description	

Figure 3-74-2 Access Control（ACL）

Page description is shown in Table 3-43.

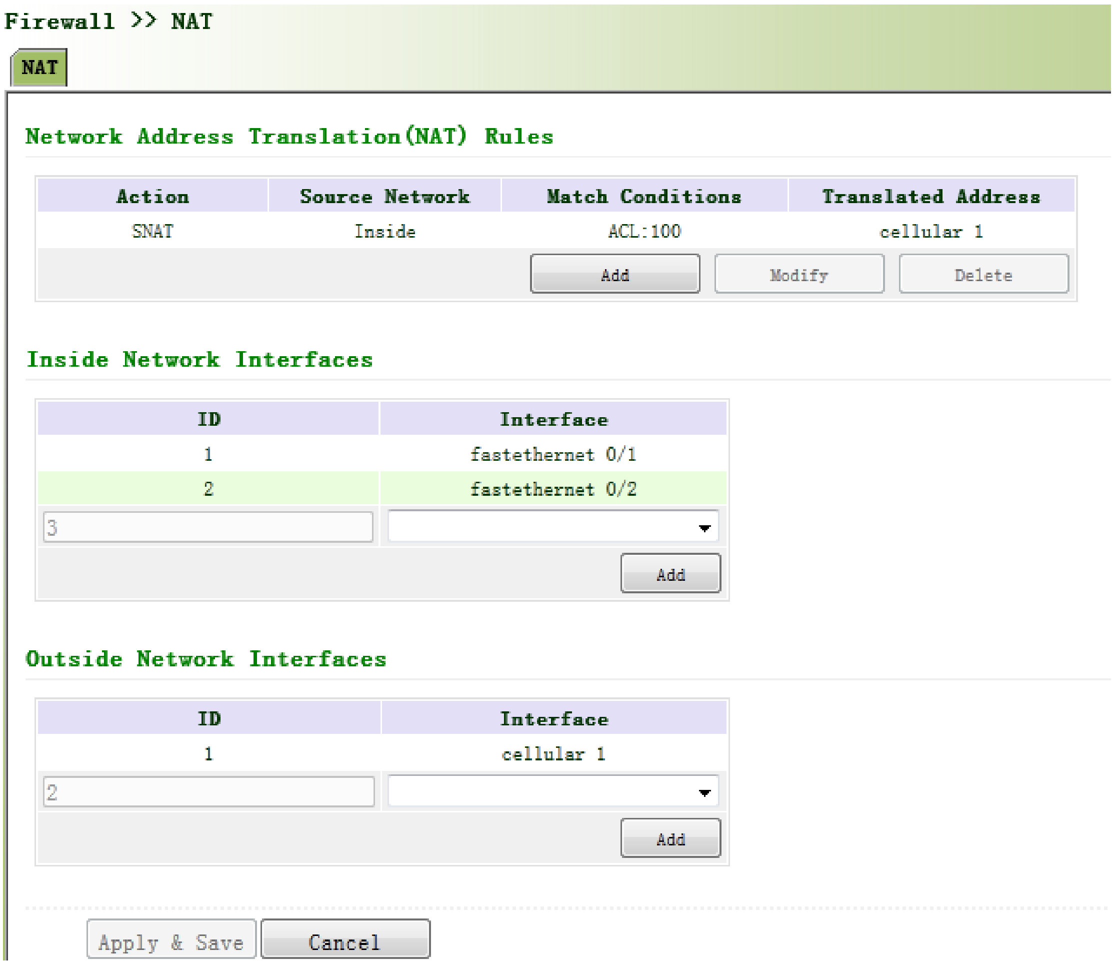
Table 3-43 Access Control Description

Parameters	Description	Default
Type	**Standard ACL** can block all communication flows from a network, or allow all communication flows from a particular network, or deny all communication flows of a protocol stack (e.g. IP) of. **The extended ACL** provides a wider range of control than that provided by the standard ACL. For example, if the network administrator wants to "allow external Web communication flows to pass through and reject external communication flows, e.g. FTP and Telnet", the extended ACL can be used to achieve the objective. The standard ACL can not be controlled so precisely.	Extended
ID	User define	None
Action	Permit/Deny	Permit
Protocol	Access Control Protocol	ip
Source IP Address	IP Address of Source	None
Destination IP	IP Address of Destination	None
Destination IP address	Destination network address	None
Destination Invert Mask	Destination address mask inverted	None
Logging	Click Enable, the system will record access control on a log	Disable
Description	Easy to record control access parameters on a log	None
Network Interface list		
Interface Name	Select Interface Name	cellular1
Rules	Select inbound, outbound and management rules	none

3.9.2 NAT

NAT can achieve Internet access by multiple hosts within the LAN through one or more public network IP addresses. It means that few public network IP addresses represent more private network IP addresses, thus saving public network IP addresses.

From navigation panel, select Firewall/NAT, then enter “NAT” page, as shown in Figure 3-75-1.



Network Address Translation(NAT) Rules

Action	Source Network	Match Conditions	Translated Address
SNAT	Inside	ACL:100	cellular 1

Inside Network Interfaces

ID	Interface
1	fastethernet 0/1
2	fastethernet 0/2
3	

Outside Network Interfaces

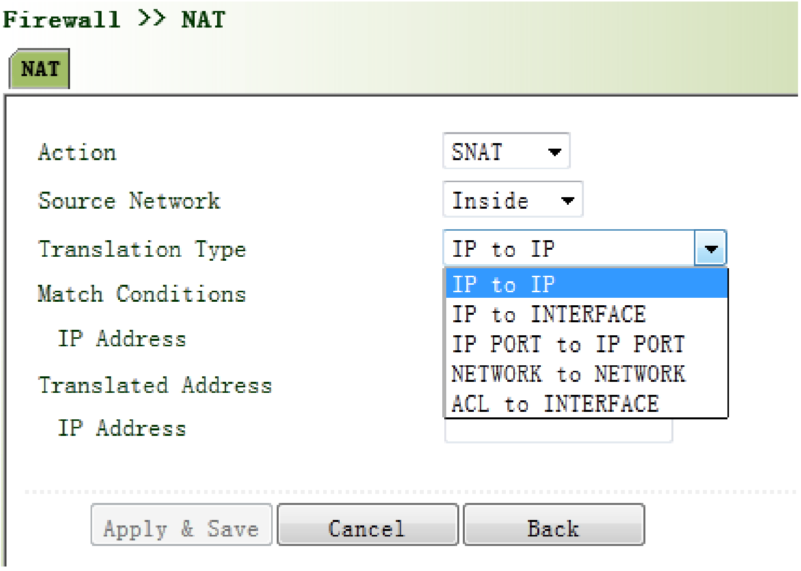
ID	Interface
1	cellular 1
2	

Figure 3-75-1 NAT

Attention

NAT rule is to apply ACL to address pool, only matching the ACL address before conversion.

Click <Add>to add new NAT rules, as shown in Figure 3-75-2.



Firewall >> NAT

NAT

Action: SNAT

Source Network: Inside

Translation Type: IP to IP

Match Conditions

IP Address

Translated Address

IP Address

Figure 3-75-2 NAT

Page description is shown in Table 3-44.

Table 3-44 NAT Description

Parameters	Description	Default
Action	**SNAT**：Source NAT： Translate IP packet's source address into another address **DNAT**： Destination NAT: Map a set of local internal addresses to a set of legal global addresses. **1:1NAT**： Transfer IP address one to one.	SNAT
Source Network	Inside： Inside address Outside： Outside address	Inside
Translation Type	Select the Translation Type	IP to IP

Instruction

Private network IP address refers to the IP address of internal network or host, while public network IP address is a globally unique IP address on the Internet.

RFC 1918 three IP address blocks for the private network as follows:

Class A: 10.0.0.0 ~ 10.255.255.255

Class B: 172.16.0.0~ 172.31.255.255

Class A: 192.168.0.0~ 192.168.255.255

The addresses within the above three ranges will not be allocated on the Internet. Therefore, they can be freely used in companies or enterprises without the need to make application to the operator or registration center

3.10 QoS

In the traditional IP network, all packets are treated equally without distinction. Each network device uses first in first out strategy for packet processing. The best-effort network sends packets to the destination, but it cannot guarantee transmission reliability and delay.

QoS can control network traffic, avoid and manage network congestion, and reduce packet dropping rate. Some applications bring convenience to users, but they also take up a lot of network bandwidth. To ensure all LAN users can normally get access to network resources, IP traffic control function can limit the flow of specified host on local network.

QoS provides users with dedicated bandwidth and different service quality for different applications, greatly improving the network service capabilities. Users can meet various requirements of different applications like guaranteeing low latency of time-sensitive business and bandwidth of multimedia services.

QoS can guarantee high priority data frames receiving, accelerate high-priority data frame transmission, and ensure that critical services are unaffected by network congestion. IR900 supports four service levels, which can be identified by receiving port of data frame, Tag priority and IP priority.

From navigation panel, select Qos/Traffic Control, then enter “Traffic Control” page, as shown in Figure 3-76.

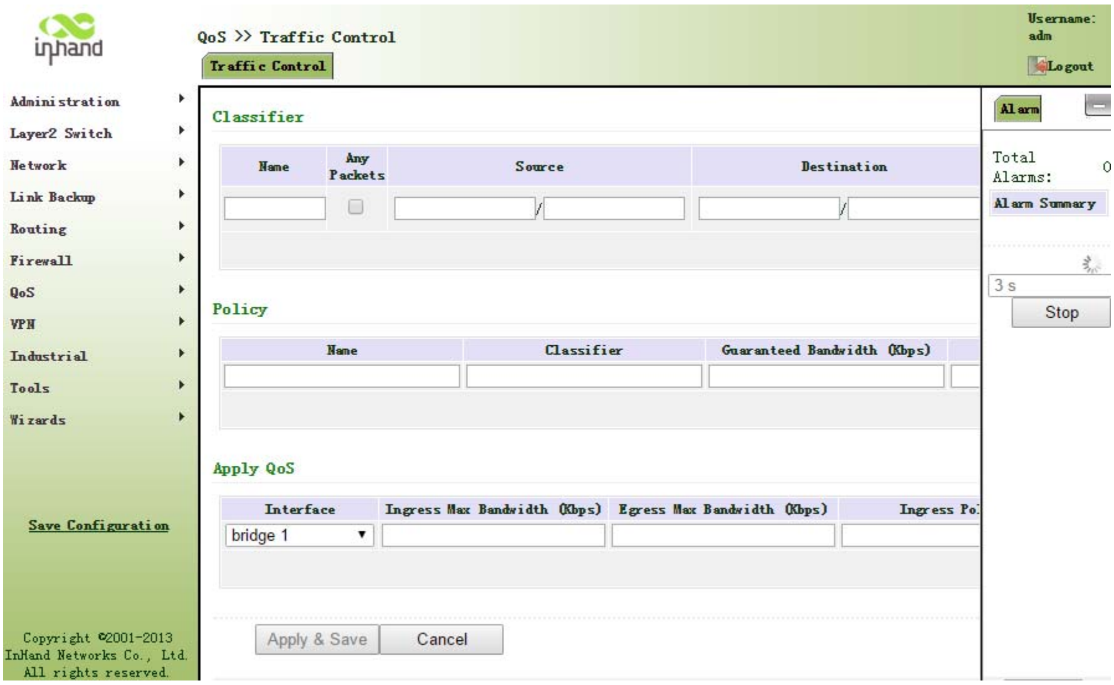


Figure 3-76 QoS

Page description is shown in Table 3-45.

Table 3-45 QoS Description

Parameters	Description	Default
Type		
Name	Name	Name
Any Packets	Click Startup for flow control to any packets	Disable
Source	Source address of flow control	N/A
Destination	Destination address of flow control	N/A
Protocol	Click to select protocol style	N/A
Policy		
Name	Name of user defined flow control strategy	N/A
Classifier	Name of style defined above	N/A
Guaranteed Bandwidth Kbps	User defined guaranteed bandwidth	N/A
Maximum Bandwidth Kbps	User defined maximum bandwidth	N/A
Local Priority	Local priority of selection strategy	N/A
Apply Qos		
Interface	Selection of flow control interface	cellular1

Ingress Max bandwidth Kbps	User define, bigger than maximum bandwidth of input strategy	N/A
Egress Max bandwidth Kbps	User define, bigger than maximum bandwidth of output strategy	N/A
Ingress Policy	Name of policy defined above	N/A
Egress Policy	Name of policy defined above	N/A

3.11 VPN

VPN is a new technology that rapidly developed in recent years with the extensive application of Internet. It is for building a private dedicated network on a public network. 'Virtuality" mainly refers to that the network is a logical network.

Two Basic Features of VPN:

- Private: the resources of VPN are unavailable to unauthorized VPN users on the internet; VPN can ensure and protect its internal information from external intrusion.
- Virtual: the communication among VPN users is realized via public network which, meanwhile can be used by unauthorized VPN users so that what VPN users obtained is only a logistic private network. This public network is regarded as VPN Backbone.

Fundamental Principle of VPN

The fundamental principle of VPN indicates to enclose VPN message into tunnel with tunneling technology and to establish a private data transmission channel utilizing VPN Backbone so as to realize the transparent message transmission.

Tunneling technology encloses the other protocol message with one protocol. Also, encapsulation protocol itself can be enclosed or carried by other encapsulation protocols. To the users, tunnel is logical extension of PSTN/link of ISDN, which is similar to the operation of actual physical link.

The common tunnel protocols include L2TP, PPTP, GRE, IPSec, MPLS, etc.

3.11.1 IPSec

A majority of data contents are Plaintext Transmission on the Internet, which has many potential dangers such as password and bank account information stolen and tampered, user identity imitated, suffering from malicious network attack, etc. After disposal of IPSec on the network, it can protect data transmission and reduce risk of information disclosure.

IPSec is a group of open network security protocol made by IETF, which can ensure the security of data transmission between two parties on the Internet, reduce the risk of disclosure and eavesdropping, guarantee data integrity and confidentiality as well as maintain security of service transmission of users via data origin authentication, data encryption, data integrity and anti-replay function on the IP level.

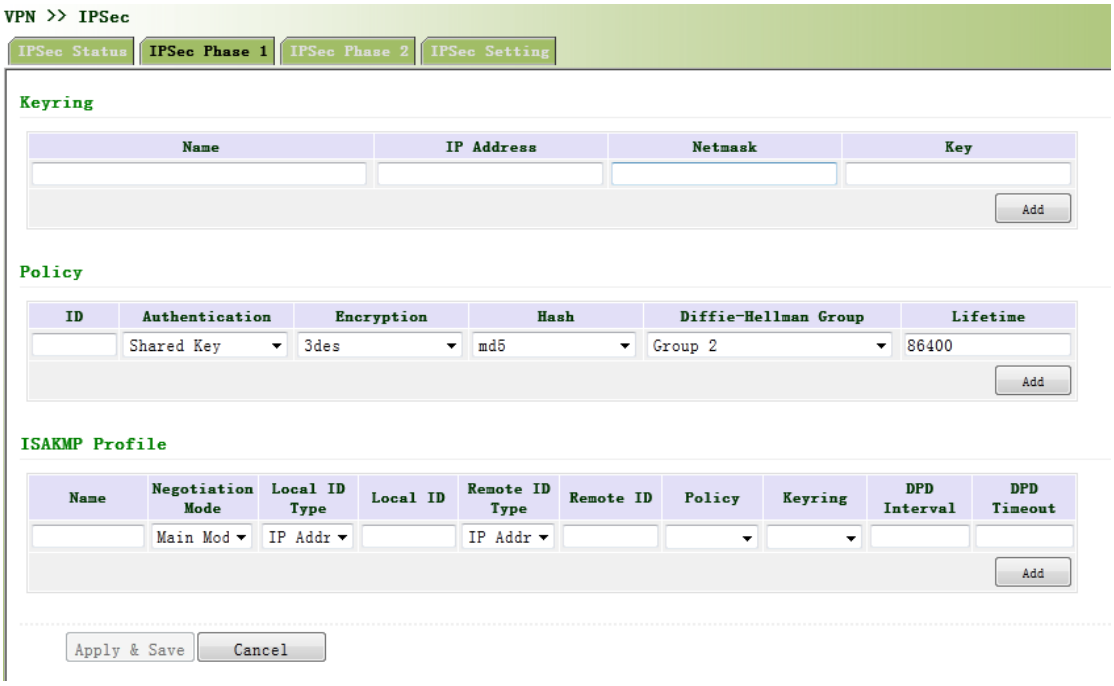
IPSec, including AH, ESP and IKE, can protect one and more date flows between hosts, between host and gateway, and between gateways. The security protocols of AH and ESP can ensure security and IKE is used for cipher code exchange.

IPSec can establish bidirectional Security Alliance on the IPSec peer pairs to form a secure and interworking IPSec tunnel and to realize the secure transmission of data on the Internet.

3.11.1.1 IPSec Phase 1

IKE can provide automatic negotiation cipher code exchange and establishment of SA for IPSec to simplify the operation and management of IPSec. The self-protection mechanisms of IKE can complete identity authentication and key distribution in an insecure network.

From navigation panel, select VPN/IPSec, then enter “IPSec Phase 1” page,as shown in Figure 3-77.



Keyring

Name	IP Address	Netmask	Key

Policy

ID	Authentication	Encryption	Hash	Diffie-Hellman Group	Lifetime
	Shared Key	3des	md5	Group 2	86400

ISAKMP Profile

Name	Negotiation Mode	Local ID Type	Local ID	Remote ID Type	Remote ID	Policy	Keyring	DPD Interval	DPD Timeout
	Main Mod	IP Addr		IP Addr					

Figure 3-77 IPSec Phase 1

Page description is shown in Table 3-46.

Table 3-46 IPSecPhase 1 Description

Parameters	Description	Default
Keyring		
Name	User define key	N/A
IP Address	End-to-end IP address	N/A
Subnet Mask	End-to-end subnet mask	N/A
Key	User define key content	N/A
IKE Policy		
Identification	Policy identification of user defined IKE	N/A
Authentication	Alternative authentication: shared key and digital certificate	Shared key
Encryption	3des: encrypt plaintext with three DES cipher codes of 64bit des: encrypt a 64bit plaintext block with 64bit cipher code Aes: encrypt plaintext block with AES Algorithm with cipher code length of 128bit, 192bit or 256bit	3des
Hash	md5: input information of arbitrary length to obtain 128bit	md5

	message digest. sha-1: input information with shorter length of bit to obtain 160bit message digest. Comparing both, md5 is faster while sha-1 is safer.	
Diffie-Hellman Key Exchange	Three options: Group 1, Group 2 and Group 5	Group 2
Lifetime	Active time of policy	86400
ISAKMP Profile		
Name	Name of user defined ISAKMP Profile	N/A
Negotiation Mode	**Main mode**: as an exchange method of IKE, main mode shall be established in the situation where stricter identity protection is required. **Aggressivemode**: as an exchange method of IKE, aggressive mode exchanging fewer message, can accelerate negotiation in the situation where ordinary identity protection is required.	Main mode
Local ID Type	Select type of local identification	IP Address
Local ID	The local ID corresponding to the selected local ID	N/A
Remote ID Type	Select type of Remote ID	IP Address
Remote ID	The Remote ID corresponding to the selected peer identification	N/A
Policy	The defined strategy identification in the IKE Strategy list	N/A
Key Ring	The defined key set in the key set list	N/A
DPD Interval	Used for detection interval of IPSec neighbor state. After initiating DPD, If receiving end can not receive IPSec cryptographic message sent by peer end within interval of	N/A

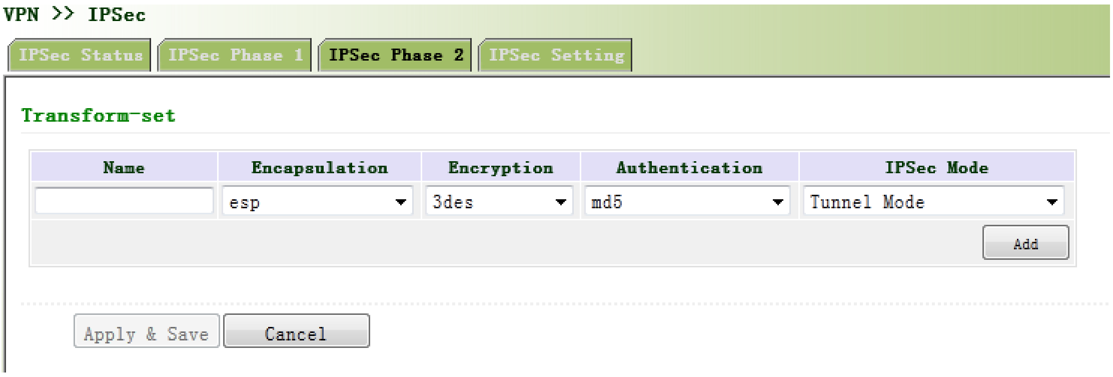
	triggering DPD, receiving end can make DPD check, send request message to opposite end automatically, detect whether IKE peer pair exists.	
DPD Timeout	Receiving end will make DPD check and send request message automatically to opposite end for check. If it does not receive IPSec cryptographic message from peer end beyond timeout, ISAKMP Profile will be deleted.	N/A

Instruction

The security level of three encryption algorithms ranks successively: AES, 3DES, DES. The implementation mechanism of encryption algorithm with stricter security is complex and slow arithmetic speed. DES algorithm can satisfy the ordinary safety requirements.

3.11.1.2 IPSec Phase 2

From navigation panel, select VPN>>IPSec, then enter “IPSec Phase 2” page, as shown in Figure 3-78.



Name	Encapsulation	Encryption	Authentication	IPSec Mode
	esp	3des	md5	Tunnel Mode

Figure 3-78 IPSec Phase 2

Page description is shown in Table 3-47.

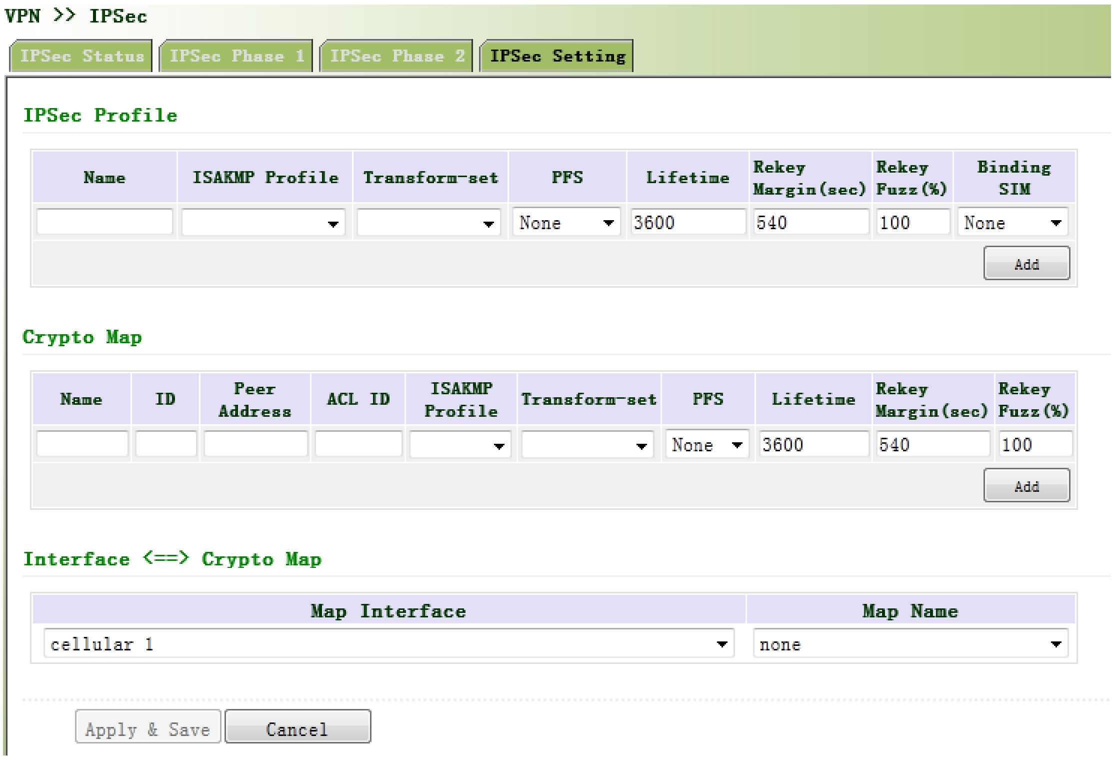
Table 3-47 IPSecIPSec Phase 2 Description

Parameters	Description	Default
Name	User define Transform Set name	N/A
Encapsulation	Choose encapsulation forms of data packet AH: protect integrity and authenticity of data packet from	esp

	hacker intercepting data packet or inserting false data packet on the internet. ESP: encrypt the user data needing protection, and then enclose into IP packet for the purpose of confidentiality of data.	
Encryption	Three options: AES, 3DES, DES	3des
Authentication	Alternative authentication: md5 and sha-1	md5
IPSec Mode	Tunnel Mode: besides source host and destination host, special gateway will be operated with password to ensure the safety from gateway to gateway. **TransmissionMode**: source host and destination host must directly be operated with all passwords for the purpose of higher work efficiency, but comparing with tunnel mode the security will be inferior.	Tunnel Mode

3.11.1.3 IPSec Configuration

From navigation panel, select VPN/IPSec, then enter “IPSec Setting” page, as shown in Figure3-79.



VPN >> IPSec

IPSec Profile

Name	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)	Binding SIM
			None	3600	540	100	None

Crypto Map

Name	ID	Peer Address	ACL ID	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)
						None	3600	540	100

Interface <==> Crypto Map

Map Interface	Map Name
cellular 1	none

Figure 3-79 IPSec Configuration

Page description is shown in Table 3-48.

Table 3-48 IPSec Configuration Description

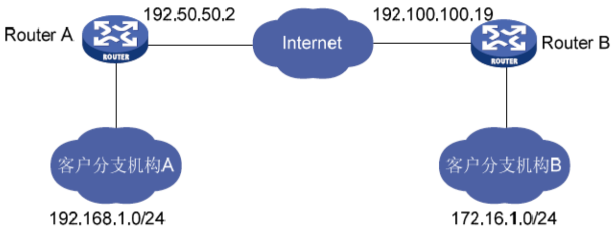
Parameters	Description	Default
IPSec Profile		
Name	User define IPSecProfile name	N/A
ISAKMP Profile	ISAKMP Profile names defined in the first stage of parameters of IPSec	N/A
Transform Set	Transform Set defined in the first stage of parameters of IPSec	N/A
Perfect Forward Security (PFS)	Means the reveal of one cipher code will not endanger information protected by other cipher codes.	Disable
Lifetime	Lifetime of IPSecProfile	3600
Rekey Margin (S)	Reconnection time for the second stage	540
Rekey Fuzz (%)	Deviation percentage of the reconnection time for the second stage	100
SIM Card Binding	With this function activated, successful dialing of the	Disable

	card with which IPSec is bonded is a precondition for the use of IPSec.	
Crypto Map		
Name	User define name of crypto map	N/A
ID	User define ID of crypto map	N/A
Peer Address	Peer IP Address	N/A
ACL ID	ID of ACL defined in ACL of firewall	N/A
ISAKMP Profile	ISAKMP Profile names defined in the first stage of parameters of IPSec	N/A
Transform Set	Transform Set defined in the first stage of parameters of IPSec	N/A
Perfect Forward Security (PFS)	Means the reveal of one cipher code will not endanger information protected by other cipher codes.	Disable
Lifetime	Validity of Crypto Map	3600
Rekey Margin (S)	Reconnection time for the second stage	540
Rekey Fuzz (％)	Deviation percentage of the reconnection time for the second stage	100
Parameters	**Description**	**Default**
Interface <==> Crypto Map		
MAP Interface	Select Interface Name	cellular1
Map Name	Select from defined names of Crypto Map. One name is matched with several marks.	none

3.11.1.4 IPSec VPN Configuration Example

Building a secure channel between Router A and Router B to ensure the secure data flow between Customer Branch A's subnet (192.168.1.0/24) and Customer Branch B's subnet (172.16.1.0/24). Security protocol is ESP, the encryption algorithm is 3DES, and authentication algorithm is SHA.

The topology is as follows:

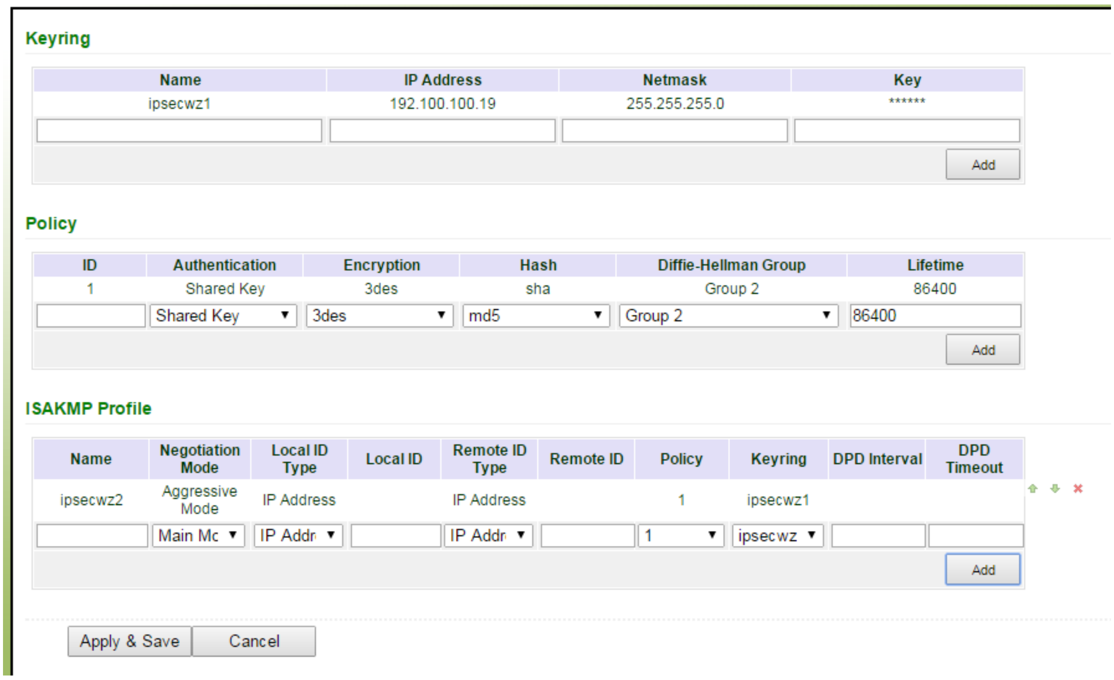


Configuration Steps:

(1) Router A Settings

Step 1: IPSec Setting Phase 1

From navigation panel, select **VPN/IPSec,** then enter “**IPSec Setting Phase 1**” page,as shown below.



Keyring

Name	IP Address	Netmask	Key
ipsecwz1	192.100.100.19	255.255.255.0	******

Policy

ID	Authentication	Encryption	Hash	Diffie-Hellman Group	Lifetime
1	Shared Key	3des	sha	Group 2	86400
	Shared Key ▼	3des ▼	md5 ▼	Group 2 ▼	86400

ISAKMP Profile

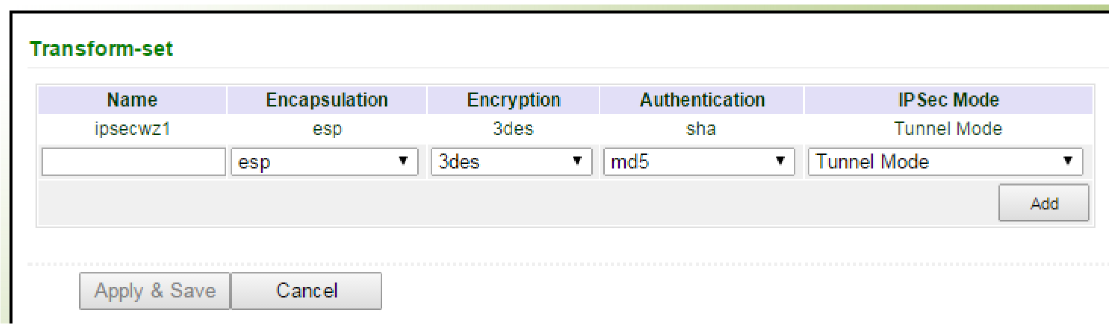
Name	Negotiation Mode	Local ID Type	Local ID	Remote ID Type	Remote ID	Policy	Keyring	DPD Interval	DPD Timeout
ipsecwz2	Aggressive Mode	IP Address		IP Address		1	ipsecwz1		
	Main Mc ▼	IP Addr ▼		IP Addr ▼		1 ▼	ipsecwz ▼		

Attention

No need to fill in Local ID Type and Remote ID Type.

Step 2: IPSec Setting Phase 2

From navigation panel, select VPN/IPSec, then enter “IPSec Setting Phase 2” page, as shown below.

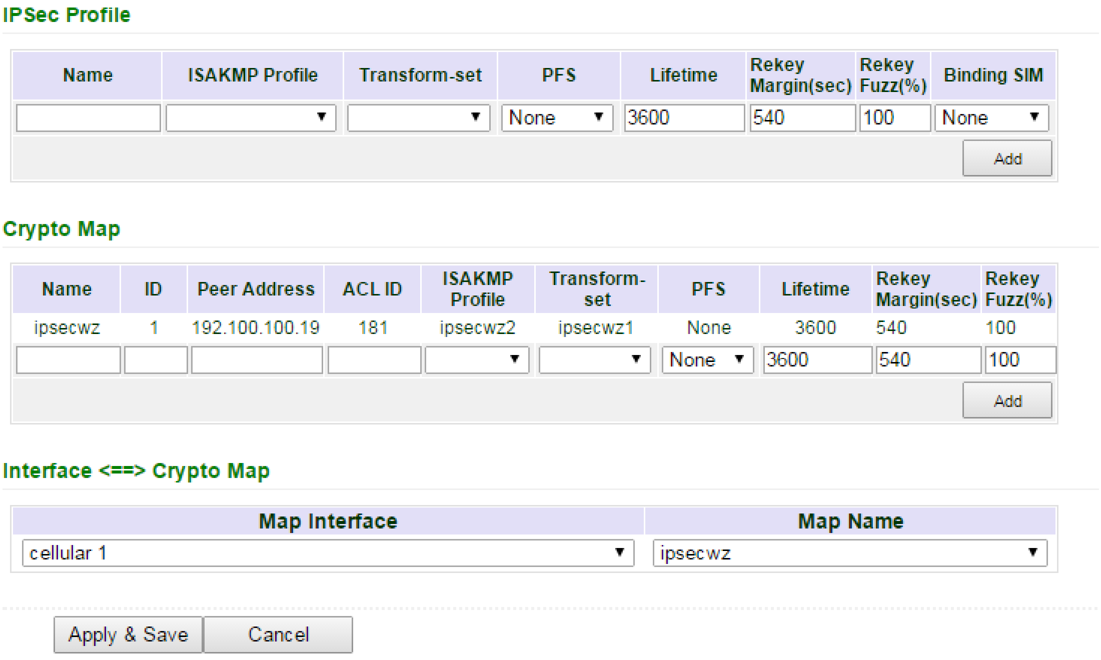


Transform-set

Name	Encapsulation	Encryption	Authentication	IPSec Mode
ipsecwz1	esp	3des	sha	Tunnel Mode
	esp ▼	3des ▼	md5 ▼	Tunnel Mode ▼

Step 3: IPSec Setting

From navigation panel, select VPN/IPSec, then enter “IPSec Setting” page,as shown below.



IPSec Profile

Name	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)	Binding SIM
	▼	▼	None ▼	3600	540	100	None ▼

Crypto Map

Name	ID	Peer Address	ACL ID	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)
ipsecwz	1	192.100.100.19	181	ipsecwz2	ipsecwz1	None	3600	540	100
				▼	▼	None ▼	3600	540	100

Interface <==> Crypto Map

Map Interface	Map Name
cellular 1 ▼	ipsecwz ▼

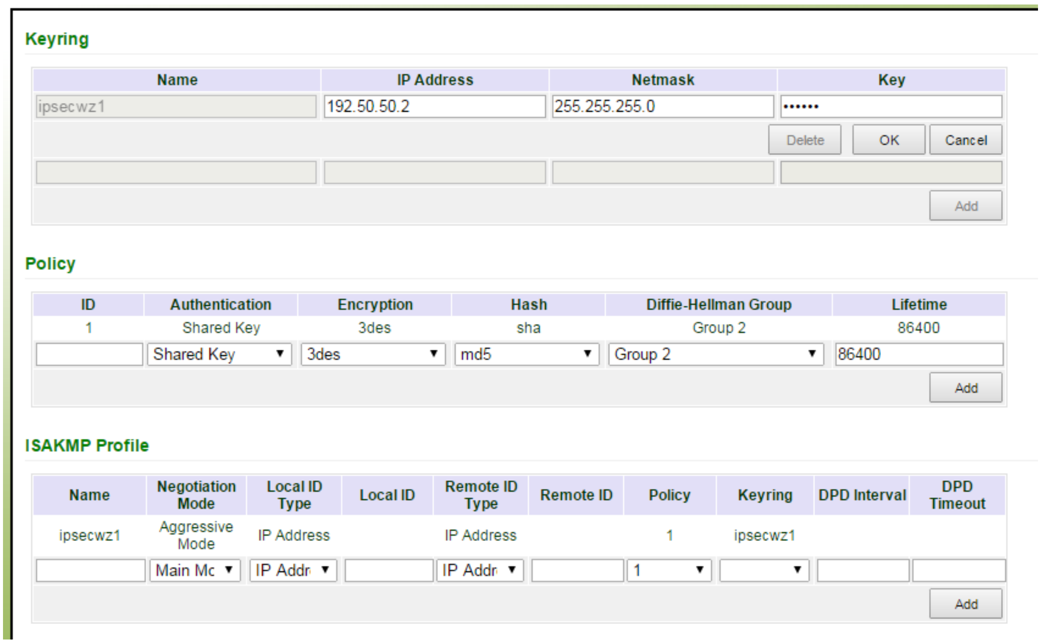
Attention

IPSec Profile setting is needed only when it’s DMVPN.

(2) Router B Settings

Step 1: IPSec Setting Phase 1

From navigation panel, select VPN/IPSec, then enter “IPSec Setting Phase 1” page, as shown below.



Keyring

Name	IP Address	Netmask	Key
ipsecwz1	192.50.50.2	255.255.255.0	••••••

Policy

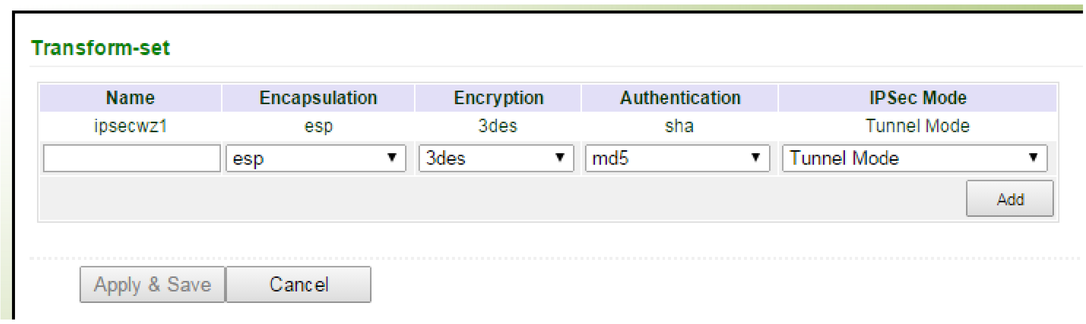
ID	Authentication	Encryption	Hash	Diffie-Hellman Group	Lifetime
1	Shared Key	3des	sha	Group 2	86400
	Shared Key ▾	3des ▾	md5 ▾	Group 2 ▾	86400

ISAKMP Profile

Name	Negotiation Mode	Local ID Type	Local ID	Remote ID Type	Remote ID	Policy	Keyring	DPD Interval	DPD Timeout
ipsecwz1	Aggressive Mode	IP Address		IP Address		1	ipsecwz1		
	Main Mc ▾	IP Addr ▾		IP Addr ▾		1 ▾	▾		

Step 2: IPSec Setting Phase 2

From navigation panel, select VPN/IPSec, then enter “IPSec Setting Phase 2” page, as shown below.

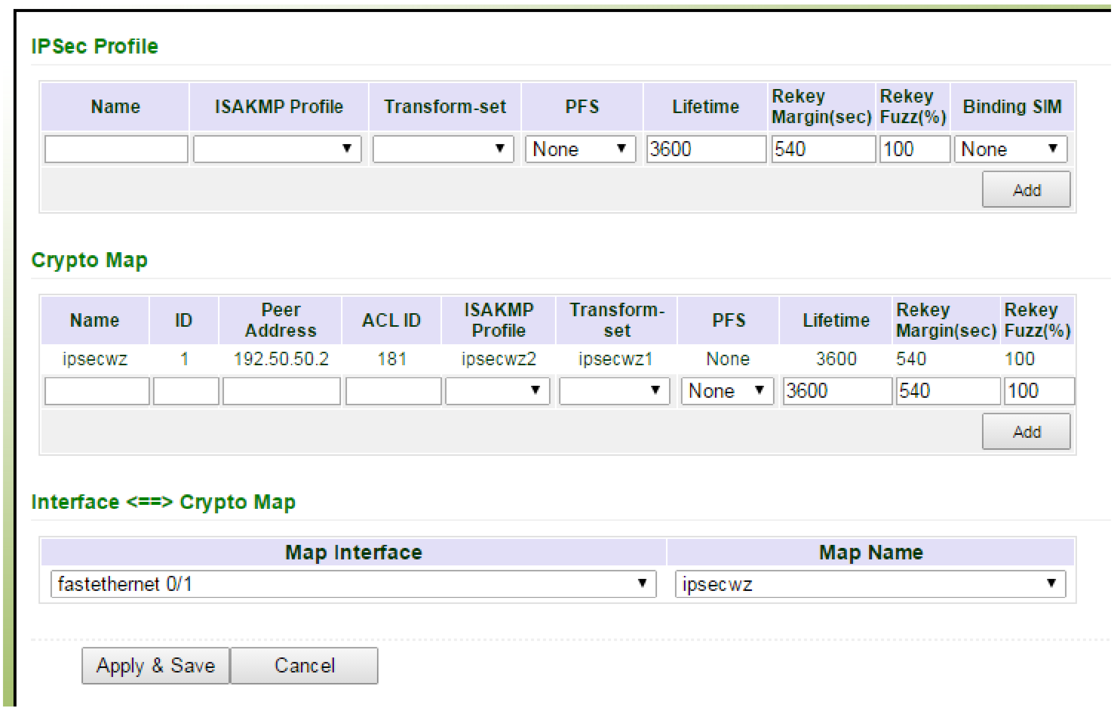


Transform-set

Name	Encapsulation	Encryption	Authentication	IPSec Mode
ipsecwz1	esp	3des	sha	Tunnel Mode
	esp ▾	3des ▾	md5 ▾	Tunnel Mode ▾

Step 3: IPSec Setting

From navigation panel, select VPN/IPSec, then enter “IPSec Setting” page,as shown below.



IPSec Profile

Name	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)	Binding SIM
	▼	▼	None ▼	3600	540	100	None ▼

Crypto Map

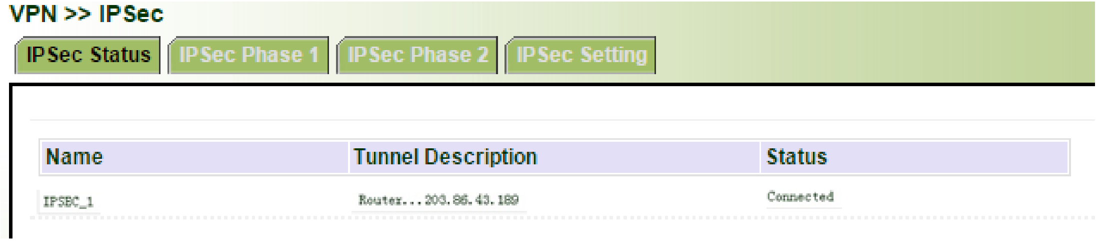
Name	ID	Peer Address	ACL ID	ISAKMP Profile	Transform-set	PFS	Lifetime	Rekey Margin(sec)	Rekey Fuzz(%)
ipsecwz	1	192.50.50.2	181	ipsecwz2	ipsecwz1	None	3600	540	100
				▼	▼	None ▼	3600	540	100

Interface <==> Crypto Map

Map Interface	Map Name
fastethernet 0/1 ▼	ipsecwz ▼

(3) VPN Status Checking

From navigation panel, select VPN/IPSec, then enter “IPSec Status” page, as shown below.

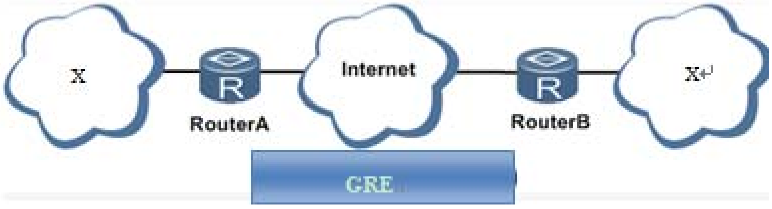


VPN >> IPSec

Name	Tunnel Description	Status
IPSEC_1	Router...203.86.43.189	Connected

3.11.2 GRE

Generic Route Encapsulation (GRE) defines the encapsulation of any other network layer protocol on a network layer protocol. GRE could be used as the L3TP of VPN to provide a transparent transmission channel for VPN data. In simple terms, GRE is a tunneling technology which provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends. GRE tunnel application networking shown as the following figure:



Along with the extensive application of IPv4, to have messages from some network layer protocol transmitted on IPv4 network, those messages could by encapsulated by GRE to solve the transmission problems between different networks.

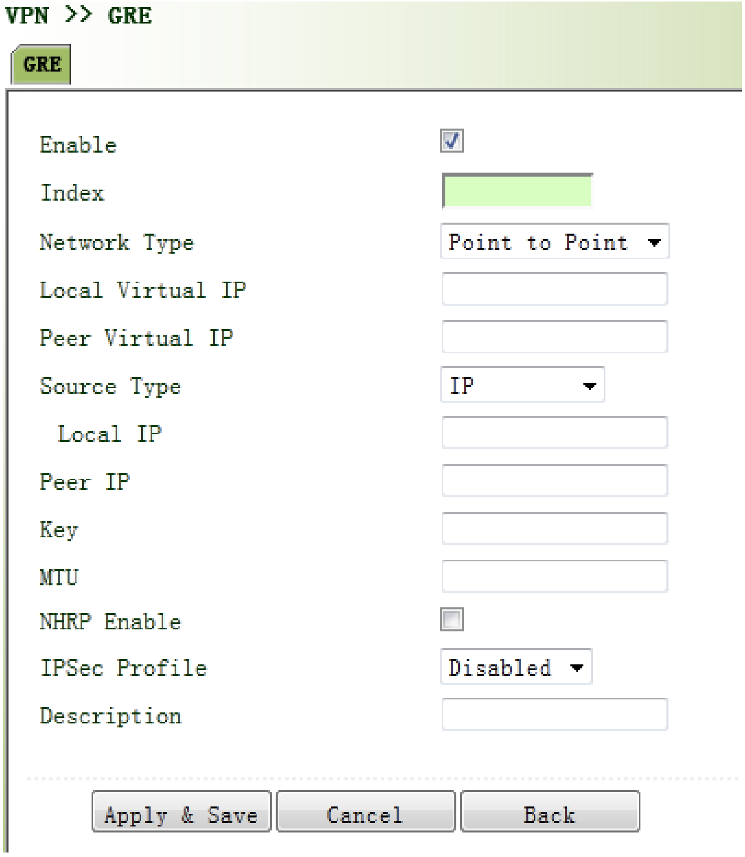
In following circumstances GRE tunnel transmission:

- GRE tunnel could transmit multicast data packets as if it were a true network interface. Single use of IPSec can not achieve the encryption of multicast.
- A certain protocol adopted can not be routed.
- A network of different IP address shall be required to connect other two similar networks.

GRE application example: combined with IPSec to protect multicast data

GRE can encapsulate and transmit multicast data in GRE tunnel, but IPSec, currently, could only carry out encryption protection against unicast data. In case of multicast data requiring to be transmitted in IPSec tunnel, a GRE tunnel could be established first for GRE encapsulation of multicast data and then IPSec encryption of encapsulated message so as to achieve the encryption transmission of multicast data in IPSec tunnel.

From navigation panel, select VPN/GRE, then enter “GRE” page, as shown in Figure 3-80.


VPN >> GRE

GRE

Enable	☑
Index	
Network Type	Point to Point
Local Virtual IP	
Peer Virtual IP	
Source Type	IP
Local IP	
Peer IP	
Key	
MTU	
NHRP Enable	□
IPSec Profile	Disabled
Description	

Figure 3-80 GRE Settings

Page description is shown in Table 3-49.

Table 3-49 GRE Description

Parameters	Description	Default
Enable	Click to open	Open
Index	Set GRE tunnel name	None
Network Type	Select GRE network type	peer to peer
Local Virtual IP	Set Local Virtual IP Address	None
Peer Virtual IP	Set Peer Virtual IP Address	None
Source Type	Select source type and set the according IP address or interface	IP
Local IP	Set Local IP Address	None
Peer IP	Set Peer IP Address	None
Key	Set the key of tunnel	None
MTU	Set the maximum transmission, unit in bytes	None
Enable NHRP	Next Hop Resolution Protocol, used to connect to non-broadcast multiple access (NBMA) formula subnetwork source station (host or router) decided to reach "NBMA next hop" internetworking layer address and NBMA subnetwork between the destination station address.	Enable
Description	Add description	None

3.11.3 L2TP

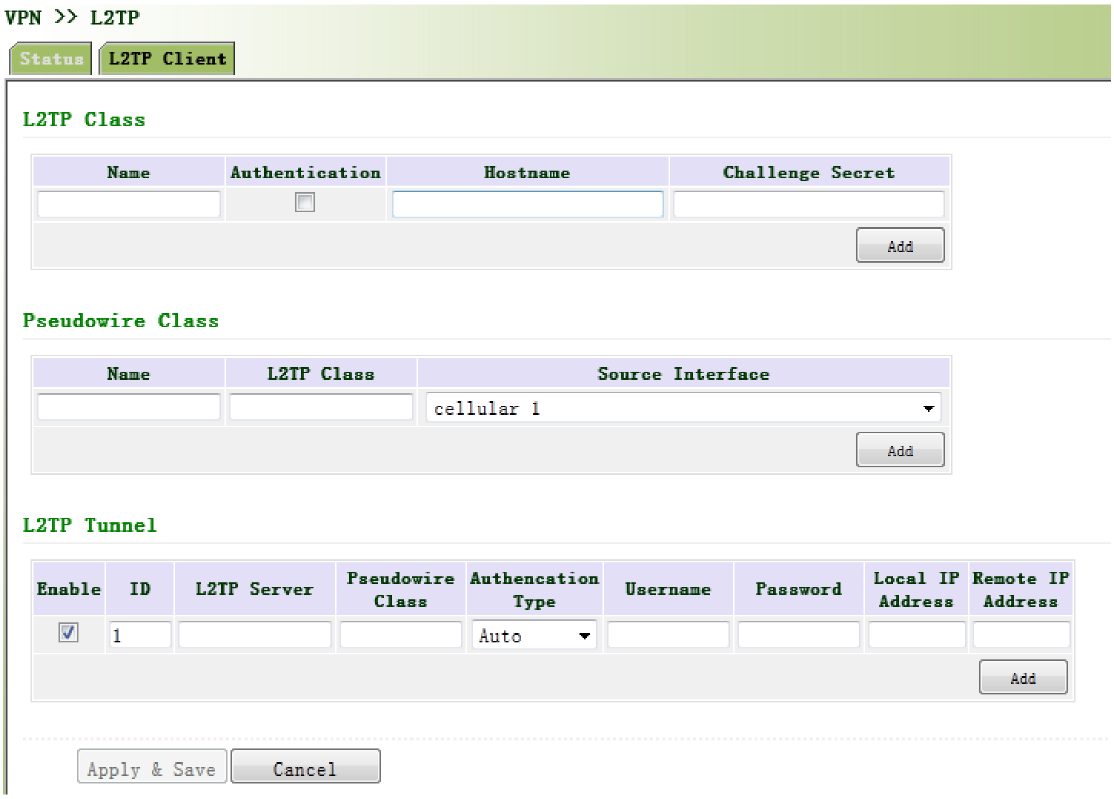
L2TP, one of VPDN TPs, has expanded the applications of PPP, known as a very important VPN technology for remote dial-in user to access the network of enterprise headquarters.

L2TP, through dial-up network (PSTN/ISDN), based on negotiation of PPP, could establish a tunnel between enterprise branches and enterprise headquarters so that remote user has access to the network of enterprise headquarters. PPPoE is applicable in L2TP. Through the connection of Ethernet and Internet, a L2TP tunnel between remote mobile officers and enterprise headquarters could be established.

L2TP-Layer 2 Tunnel Protocol, encapsulates private data from user network at the head of L2 PPP. No encryption mechanism is available, thus IPSes is required to ensure safety.

Main Purpose: branches in other places and employees on a business trip could access to the network of enterprise headquarter through a virtual tunnel by public network remotely.

From navigation panel, select VPN/L2TP, then enter “L2TP Client” page, as shown in Figure 3-81.



L2TP Class

Name	Authentication	Hostname	Challenge Secret
	□		

Pseudowire Class

Name	L2TP Class	Source Interface
		cellular 1

L2TP Tunnel

Enable	ID	L2TP Server	Pseudowire Class	Authencation Type	Username	Password	Local IP Address	Remote IP Address
☑	1			Auto				

Figure 3-81 L2TP Client

Page description is shown in Table 3-50.

Table 3-50 L2TP Client Description

Parameters	Description	Default
L2TP Class		
Name	User difine L2TP Class Name	None
Authentication	Click Enable, peer authentication is required to network connection when enable.	Disable
Host Name	Network connection to local host name, not to configure.	None
Tunnel Authentication key	When the tunnel must be configured to enable the authentication, click authentication key, or you will not need to configure.	None
Pseudowire Class		
Name	User difine Pseudowire Class Name	None
L2TP Class	L2TP Class name	None
Source Interface	Seclect source interface name	cellular 1
L2TP Tunnel		
Enable	Click to enable	Enable
Index	Automatic generated	1
L2TP Server	Set L2TP Server address	None

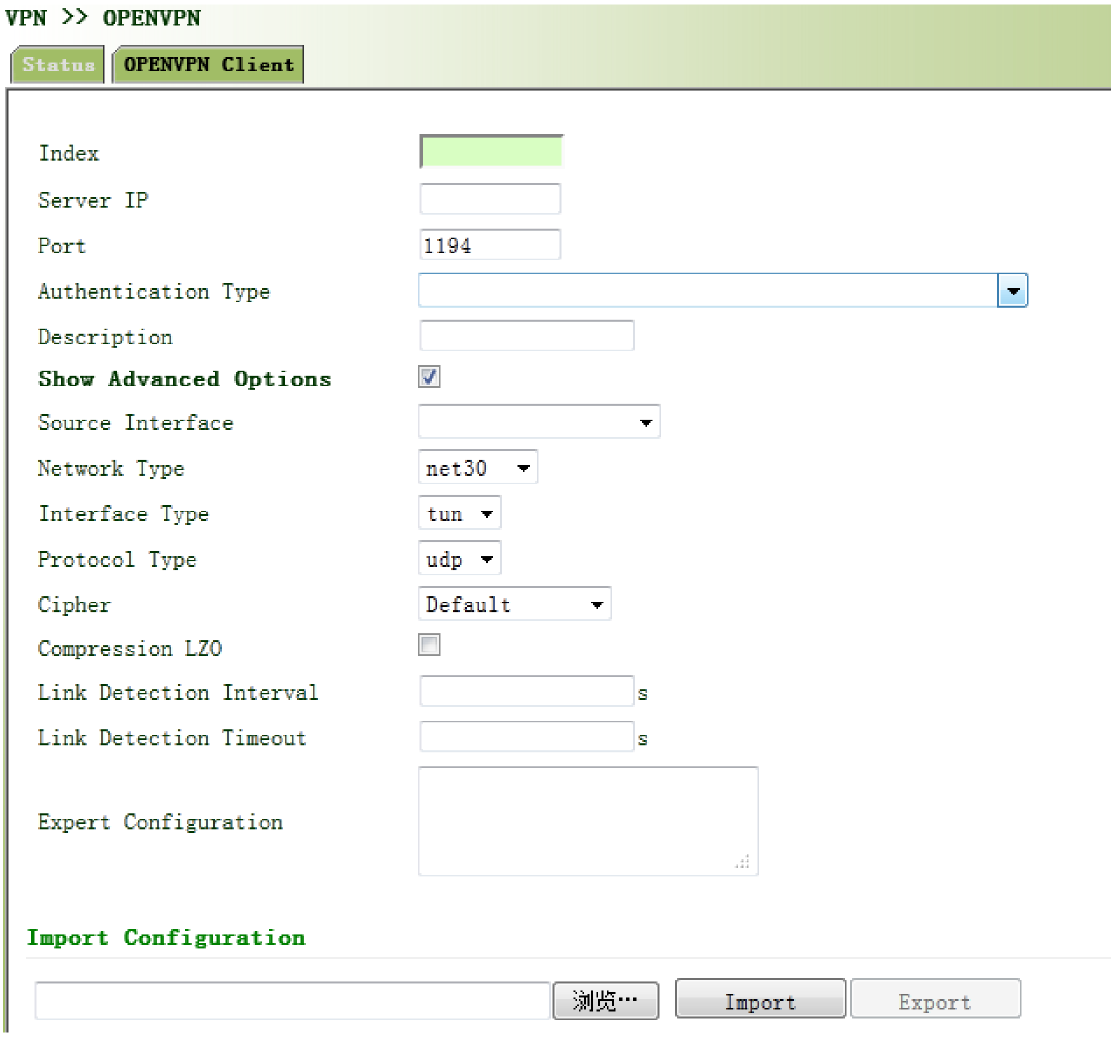
Pseudowire Class	Pseudowire Class name	None
Authentication Type	Select Authentication Type	Auto
Username	Peer Server username	None
Password	Peer Server password	None
Local IP Address	Set local IP address, or automatically allocated by peer server.	None
Remote IP Address	Set remote IP addres, or not	None

3.11.4 OPENVPN

Single point participating in the establishment of VPN is allowed to carry out ID verification by preset private key, third-party certificate or username/password. OpenSSL encryption library and SSLv3/TLSv1 protocol are massively used.

In OpenVpn, if a user needs to access to a remote virtual address (address family matching virtual network card), then OS will send the data packet (TUN mode) or data frame (TAP mode) to the visual network card through routing mechanism. Upon the reception, service program will receive and process those data and send them out through outer net by SOCKET, owing to which, the remote service program will receive those data and carry out processing, then send them to the virtual network card, then application software receive and accomplish a complete unidirectional transmission, vice versa.

From navigation panel, select VPN/OPENVPN, then enter “OPENVPN Client” page,as shown in Figure 3-82.



VPN >> OPENVPN

Index	
Server IP	
Port	1194
Authentication Type	
Description	
Show Advanced Options	☑
Source Interface	
Network Type	net30
Interface Type	tun
Protocol Type	udp
Cipher	Default
Compression LZO	□
Link Detection Interval	s
Link Detection Timeout	s
Expert Configuration	

Import Configuration

Figure 3-82OPENVPN Client

Page description is shown in Table 3-51.

Table 3-51OPENVPNOPENVPN Client Description

Parameter	Description	Default
Enable	Click Enable	Enable
ID	Set channel ID	None
Server IP Address	Set peer server IP addresss	None
Port Number	Set peer server port number	1194
Authentication Type	Select and configure authentication type parameters of type certification	User name/Password
User name	Keep consistency with server	None
Password	Keep consistency with server	None
Channel description	user define channel description	None
Advanced Options		
Source Port	Select source port name	None

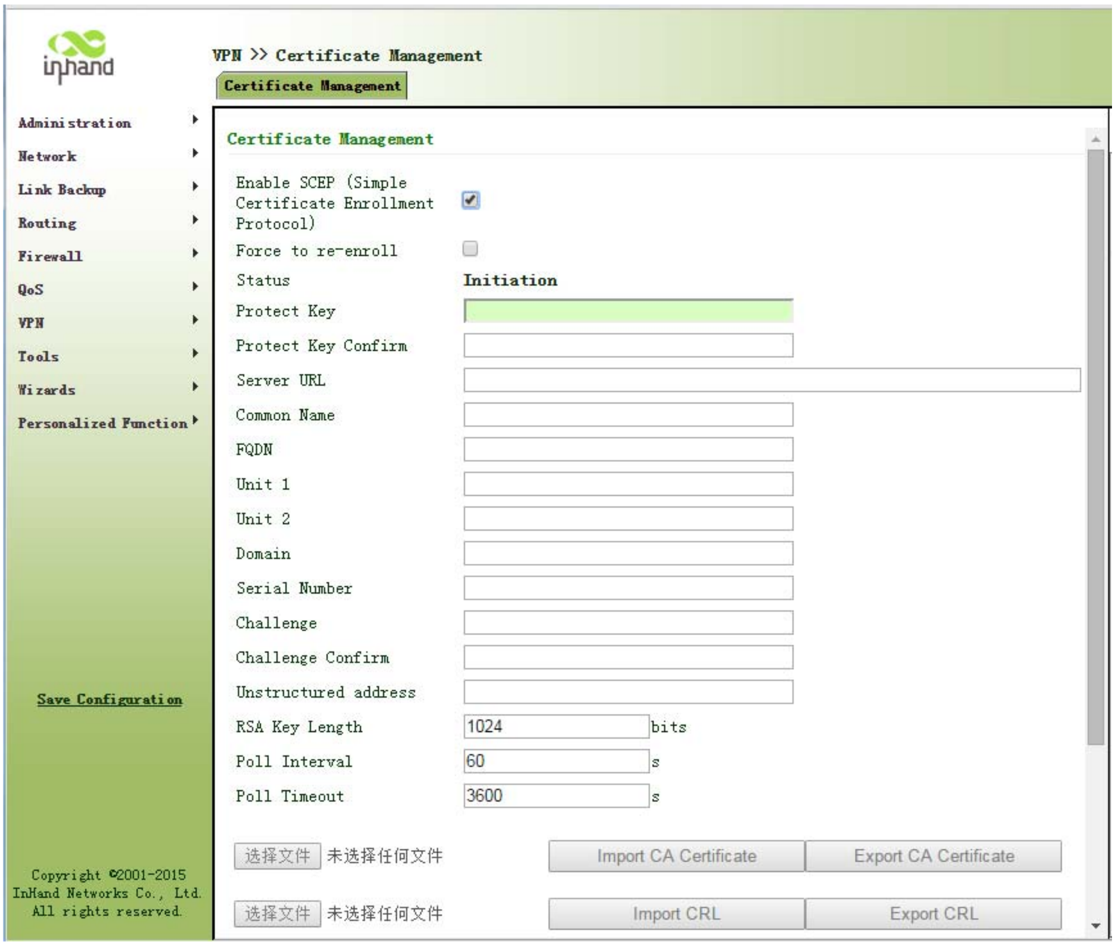
Network Type	Select network type	net30
Port Type	Select data form issued from the interface. tun- packet, tap- data frame	tun
Protocol Type	Keep consistency with server protocol	udp
Advanced Options		
Encryption Algorithm	keep consistency with server	Default
LZO Compression	Click Enable	Off
Connection Testing Interval	Set connecting testing time interval	None
Connection Testing Overtime	Set connecting testing overtime	None
Expert Configuration	Set expert option: blank advisable	None

Instruction

Import configurations can be directly imported into the configured documents generated from backend server and manual configuration of OPENVPN customer end parameter is in no need after import.

3.11.5 Certificate Management

From navigation panel, select VPN/Certificate Management, then enter "Certificate Management" page, as shown in Figure 3-83.



Certificate Management

Enable SCEP (Simple Certificate Enrollment Protocol) ☑

Force to re-enroll □

Status Initiation

Protect Key

Protect Key Confirm

Server URL

Common Name

FQDN

Unit 1

Unit 2

Domain

Serial Number

Challenge

Challenge Confirm

Unstructured address

RSA Key Length 1024 bits

Poll Interval 60 s

Poll Timeout 3600 s

Figure 3-83 Certificate Management

Page description is shown in Table 3-52.

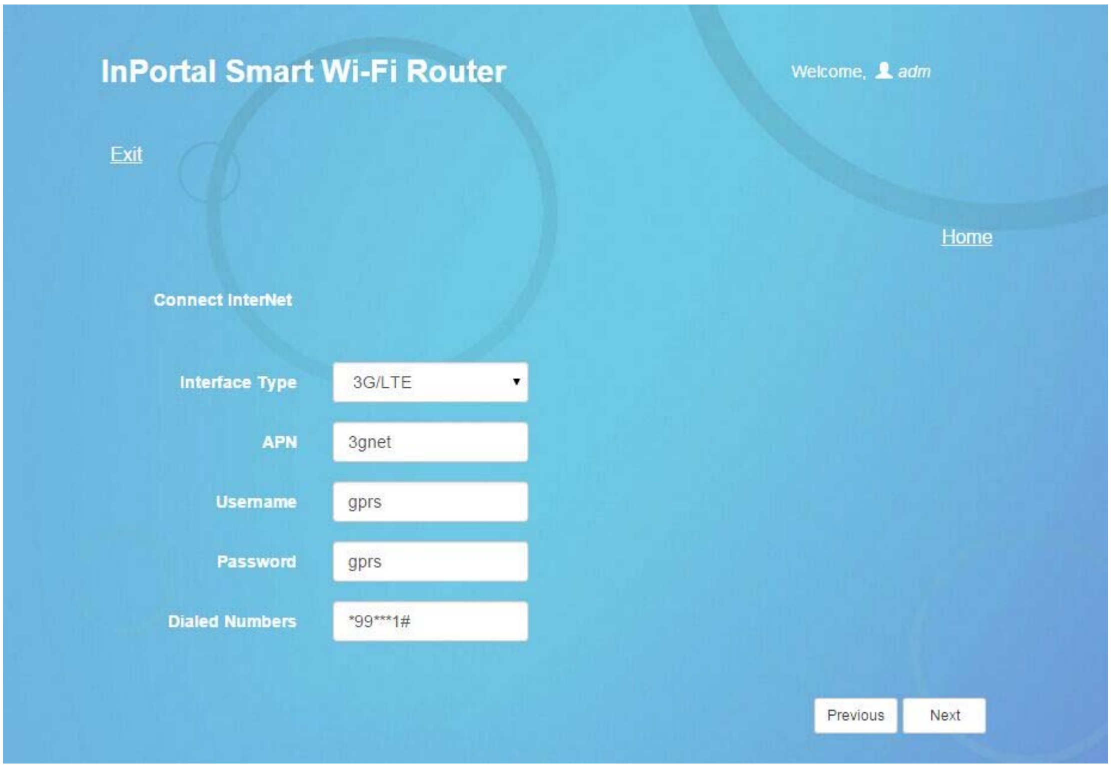
Table 3-52Certificate Management Description

Parameter	Description	Default
Forced to re-apply	If the certificate has not expired, but need to reapply, click forced to re-apply, re-configure the certificate request parameter.	Disable
Request Status	successful application, "Request Status" shows: Completion	Initiation
Certificate Protection Key	Set certificate protection key	None
Certificate Protection Key Confirmation	Confirm certificate protection key	None
Server URL	Set certificate server IP	None
Certificate name	Set certificate name	None

FQDN	Set full domain name	None
Unit Name 1	Set unit name 1	None
Unit Name 2	Set unit name 2	None
Domain Name	Set domain name	None
Serial Number	Set application certificate serial number	None
Authentication Password	Set authentication password	None
Authentication Password Confirmation	Confirm authentication password	None
Host IP	Set router address in the use of certificate application	None
RSA Key length	Set RSA key length	1024
Query Interval	Set query interval	60 sec
Query Timeout	Set query timeout	3600 sec

3.12 Configuration Wizard

After login the configuration page via Web, click “Connect Internet” to enter configuration page below:



Connect InterNet

Interface Type: 3G/LTE

APN: 3gnet

Username: gprs

Password: gprs

Dialed Numbers: *99***1#

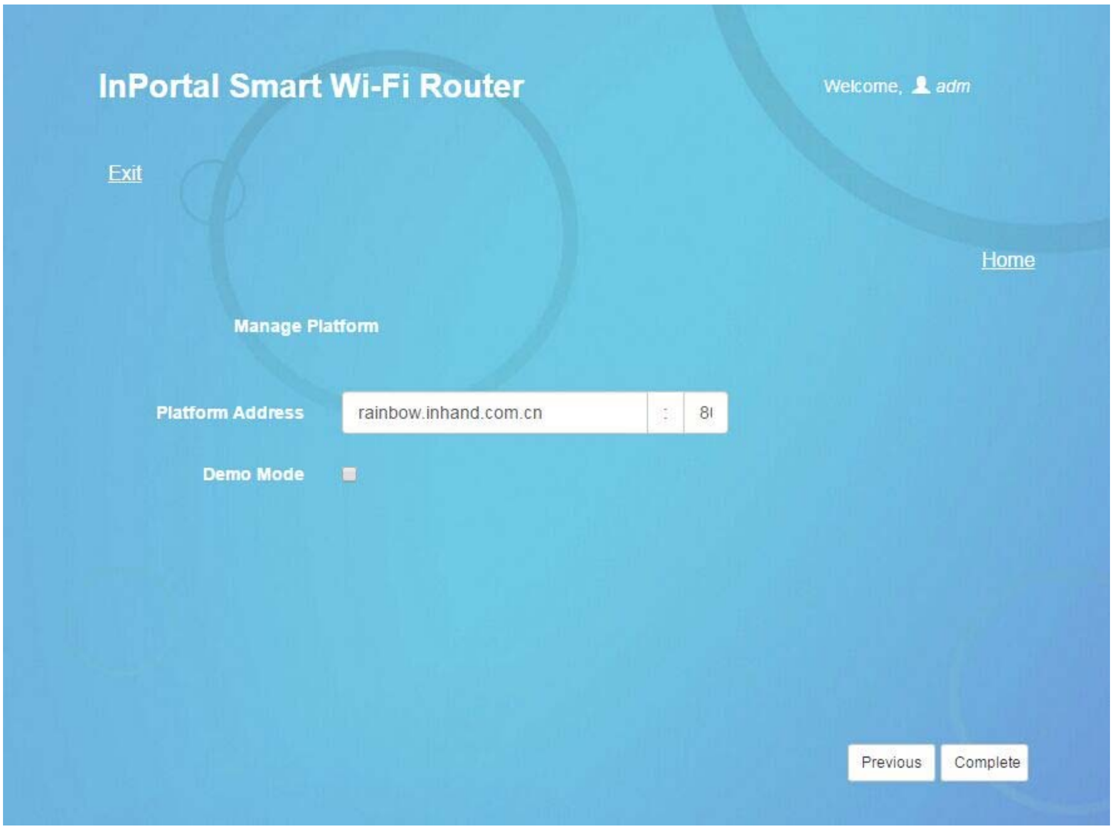
Figure 3-12-1Connect Internet

Page description:

Table 3-12-1Connect Internet Configuration Description

Parameters	Description	Default
Interface Type: 3G/LTE, ADSL, DHCP and Static IP Address		
3G/LTE		
APN	Provided by local operator	3gnet
Username	Provided by local operator	gprs
Password	Provided by local operator	gprs
Dialed Numbers	Provided by local operator	*99***1#
ADSL		
Username	Provided by local operator	N/A
Password	Provided by local operator	N/A
No configuration for DHCP		
Static IP Address		
IP Address	User define	N/A
Subnet mask	User define	255.255.255.0
Gateway	User define	N/A
Primary DNS	User define	N/A
Secondary DNS	User define	N/A

Save the configuration and click <Next Step> to enter “Cloud Platform” configuration page as shown below:



Platform Address rainbow.inhand.com.cn : 8(

Demo Mode □

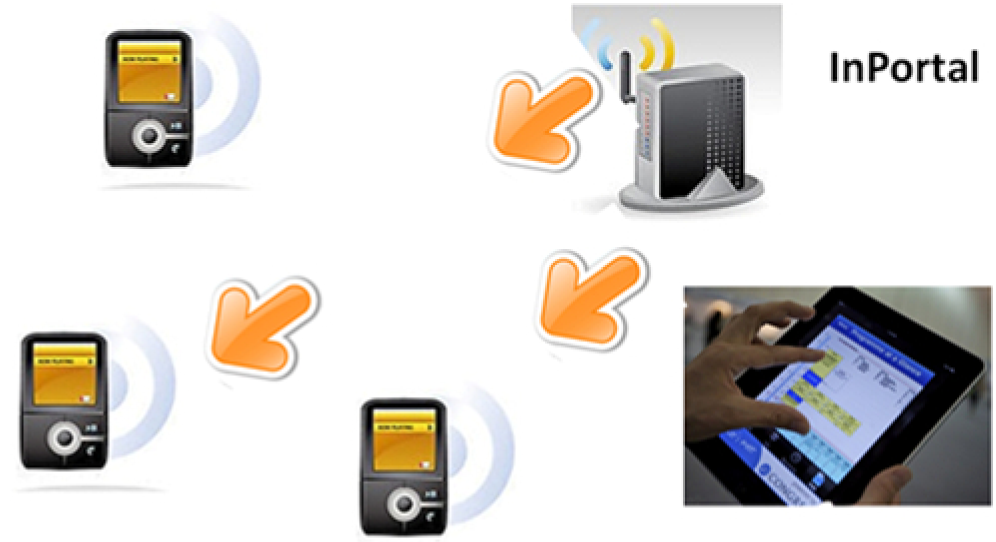
Figure 3-12-2 Cloud Management Platform

Table 3-12-2 Cloud Management Platform Configuration Description

Parameters	Description	Default
Platform Address	The address and port number of cloud platform	rainbow.inhand.com.cn：80
Demo Mode	Click to enable	Disable

4. Application Scenarios

Place on a bus one Inhand IPortal3000 server, using WIFI wireless coverage inside the car, built 3G/4G module to access the Internet. Passengers’ smart phones, tablet and notebooks and other intelligent terminal access to the WIFI hotspot, InPortal 3000 with Portal authentication method push specified page to the mobile terminal, to provide information, downloads, entertainment and other information services and Internet services. Information services available at the local store InPortal 3000 enhance user access experience, synchronous update Center and local content via 3G/4G.


InPortal

Appendix 1 Troubleshooting

This manual describes only a simple router troubleshooting method, if still can not rule out, you can get the service through Table 1-1.

1) Cannot log on locally router through Web setting page?

- ✧ use MS-DOS Ping command to check the network connection

  a. Ping 127.0.0.1 used to check the computer management TCP/IP protocol is installed.

  b. Ping collection to FE interface IP address which directly connected to router, used to check whether collection of management computer to router.

- ✧ Number of users allowed to manage the router has reached the maximum (for up to four users to simultaneously log), please try again later.
- ✧ Please check the Web browser is set up a proxy server or dial-up connection, if any, unset.
- ✧ See above PC firewall settings are used to configure the router, whether shielding function.
- ✧ Please check whether IE is equipped with third-party plug-ins (eg: 3721, IE partner, etc.) it is recommended to configure after uninstalling.

2) InPortal is powered on, but can not access Internet?

Please check：

- ✧ Whether the InPortal is inserted with a SIM card.
- ✧ Whether the SIM card is enabled with data service, whether the service of the SIM card is suspended because of an overdue charge.
- ✧ Whether the dialup parameters, e.g. APN, dialup number, account, and password are correctly configured.
- ✧ Whether the IP Address of your computer is the same subnet with InPortal and the gateway address is InPortal LAN address.

3) LAN users dropped cable, can not access the Internet?

- ✧ Check switch cable collected to router, and WAN port network cable, if there is loosening.
- ✧ Log into the router's Web setup page, check access control list, to check whether the IP address of a segment is not allowed to access the Internet.

4) InPortal is powered on, have a ping to detect InPortal from your PC and find packet loss?

- ✧ Please check if the network crossover cable is in good condition.

5) Forget the setting after revising IP address and cannot configure InPortal?

Method 1: connect InPortal with serial cable, configure it through console port.

Method 2: InPortal is powered on, press and hold RESET Reset button (until ERROR lights), release the RESET button (ERROR lamp is off), press and hold the RESET button again (until the ERROR indicator blinks), and you can restore the factory default settings.

After applying the above two methods, configure the InPortal**.**

6) After InPortal is powered on, it frequently auto restarts. Why does this happen?

Please check:

✧ Whether the module works normally.

✧ Whether the InPortalr is inserted with a SIM card.

✧ Whether the SIM card is enabled with data service, whether the service of the SIM card is suspended because of an overdue charge.

✧ Whether the dialup parameters, e.g. APN, dialup number, account, and password are correctly configured.

✧ Whether the signal is normal.

✧ Whether the power supply voltage is normal.

7) InPortal is powered on, but the Power LED is not on?

Please check:

✧ Check the fuse is burned out.

✧ Check supply voltage, and the polarity is connected correctly.

8) InPortal is powered on, connected to the PC, Why Ethernet port light is not on?

Please check:

✧ Check the network cable is normal.

✧ NIC characteristic on the PC is set to 10/100M, full duplex.

9) InPortal is powered on, when connected with PC, the Network LED is normal but cannot have a ping detection to the InPortal?

Check if the IP Address of the PC and InPortal are in the same network segment and InPortal IP as gateway address.

10) InPortal dialup always fails, I cannot find out why?

Please restore InPortal to factory default settings and configure the parameters again.

Table 1-1 Sales Service

Trouble	Description	Obtain service
Hardware failure	For example: InPortal does not appear normal power, did not plug the network cable while Ethernet port light was lit and other issues.	Please contact Inhand Technicial Support Hotline for help: 010-64391099
Software Prolem	For example: InPortal feature is unavailable, abnormal or configuration advice.	Please contact Inhand Technicial Support Hotline for help: 010-64391099

Appendix 2 Instruction of Command Line

Operating status LED:

POWER	STATUS	WARN	ERROR	Description
The power LED (red)	Status LED (green)	Alarm LED (yellow)	Error LED(red)	
on	on	on	off	Power status
on	blink	on	off	Power Success
on	blink	blink	off	Dialing
on	blink	off	off	Dialing Success
on	blink	blink	blink	Being upgraded
on	blink	on	blink	Reset Success

Signal Status LED and Description:

Signal Status Green LED 1	Signal Status Green LED 2	Signal Status Green LED 3	Description
off	off	off	No signal was detected
on	off	off	1-9 signal condition (in this case signal conditions describe problems, please check the antenna is installed intact, the signal situation in the region is good)
on	on	off	10-19 signal condition (in this case illustrate signal status is normal, InPortal can be used normally)
on	on	on	20-31 signal condition (in this case illustrate the signal in good condition)

Ethernet Port Status LED and Description:

Green LED	Description
on	The network port is 100M, in a normal state, no data transmission
blink	The network port is 100M, in a normal state, in data transmission
off	No connection

MODEM LED and Description

MODEM Green LED	Description
on	Already dialed
blink	Not dailed

POWER LED and Description

POWER Red LED	Description
on	Nomal power connection
off	No power connection

WLAN LED and Description

WLAN Green LED	Description
on	WLAN on function
off	WLAN off function

FCC STATEMENT

1. 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.

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

2. Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

InHand Networks

InHand Networks provides reliable, secured and intelligent M2M solution for electric power, industrial automation, commercial and medical devices. We are recognized by world class customers and partners and proven by a large install base.

InHand Networks has become leader in industrial grade network technology by providing industrial cellular routers, industrial Ethernet switches, wireless sensor network devices and cloud based M2M platforms.

Connecting devices, enabling service.

Rockwell Automation
Encompass™
Product Partner

Collaborative Automation
by
Schneider Electric

Deloitte.

RED HERRING
WINNER
100
ASIA

inhand

InHand Networks

7926 Jones Branch Dr. Suite 110

McLean, Virginia 22102

USA

T: +1-703-348-2988

F:+1-703-348-2988

info@inhandnetworks.com

www.inhandnetworks.com