InRouter900 Series
User Manual

InHand Networks

www.inhandnetworks.com

Version: v3.4

July 2017

Preface

Thanks for choosing InRouter900 series industrial routers! This user manual will guide you in detail on how to configure InRouter900.

Readers

This manual is mainly intended for the following engineers:

- Network planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

Conventions in the Manual

1. Format Conventions on Command Line

Format	Significance
Bold	Keywords of command line (the part that should be remained unchanged in command and be entered as it is) are expressed with **bold** font.
Italic	The parameters of command line (the part that must be replaced with the actual value in command) are expressed in *italic*.
[ ]	Indicating that the part in "[]" is optional in command configuration.
{ x | y | ... }	Indicating to select one from multiple options.
[x | y | ...]	Indicating to select one or not to select from multiple options.
{ x | y | ... } *	Indicating to select at least one from multiple options.
[x | y | ...] *	Indicating to select one or more or not to select from multiple options.
&<1-n>	Indicating that the parameter in front of the symbol & can be repeatedly entered for 1~n times.
#	The lines starting from no. "#" are comment lines.

2. Format Conventions on Graphic Interface

Format	Significance
<>	The content in angle brackets "<>" indicates button name, e.g. "click <OK> button."
[ ]	The content in square brackets "[]" indicates window name, menu name or data sheet, e.g. "pop-up the [New User] window".
/	Multi-level menu is separated by "/". For example, the multi-level menu [File / New / Folder] indicates the menu item [Folder] under the submenu [New] under the menu [File].

3. Various Signs

The manual also uses a variety of eye-catching signs to indicate the places to which special attention should be paid in operation. The significances of these signs are as follows:

 **Attention**	It indicates matters to be noted. Improper operation may cause data loss or damage to the device.
 **Instruction**	The necessary complement or description on the contents of operation.

Technical Support

E-mail: support@inhandneworks.com

www.inhandnetworks.com

Information Feedback

If you have any question on product information in use, you can feed back through the following ways:

E-mail : info@inhandnetworks.com

Thanks for your feedback to let us do better!

Contents

Main Text

I. InRouter900 Introduction

1.1 Overview

IR900 is a new generation of 4G LTE VPN industrial router developed by InHand Networks.

Integrating 4G LTE and various broadband WANs, IR900 provides uninterrupted access to internet. With the features of complete security and wireless service, IR900 can connect up to ten thousand devices, which can provide a high-speed data access for a real sense of equipment informatization. IR900 has also been built for rapid deployment and easy management with advanced software functions and full-industrialized hardware design platform, which enables enterprises to quickly set up large scale industrial network within a minimized investment scope. It also can provide multi-services such as data, voice and video.

There are currently three IR900 series: IR9x2, IR9x5, IR9x8, which can provide up to 8 intelligent ports at most and they support LAN/WAN protocol. IR900 products not only offer more options on WAN port access, but also effectively save additional purchasing cost on switch equipment.

With the development of industry, more businesses can be concentrated in data centre via wireless network. By serving IR900 router as an access device at industrial site, a virtual tunnel with high encryption performance can be set up via the VPN gateway of far-end industrial site and data centre, which can save expensive special line lease input. The data is transmitted via IR900 secure tunnel, which can effectively ensure the safe, rapid and reliable transmission of businesses. Network diagram is shown in Fig. 4-1.

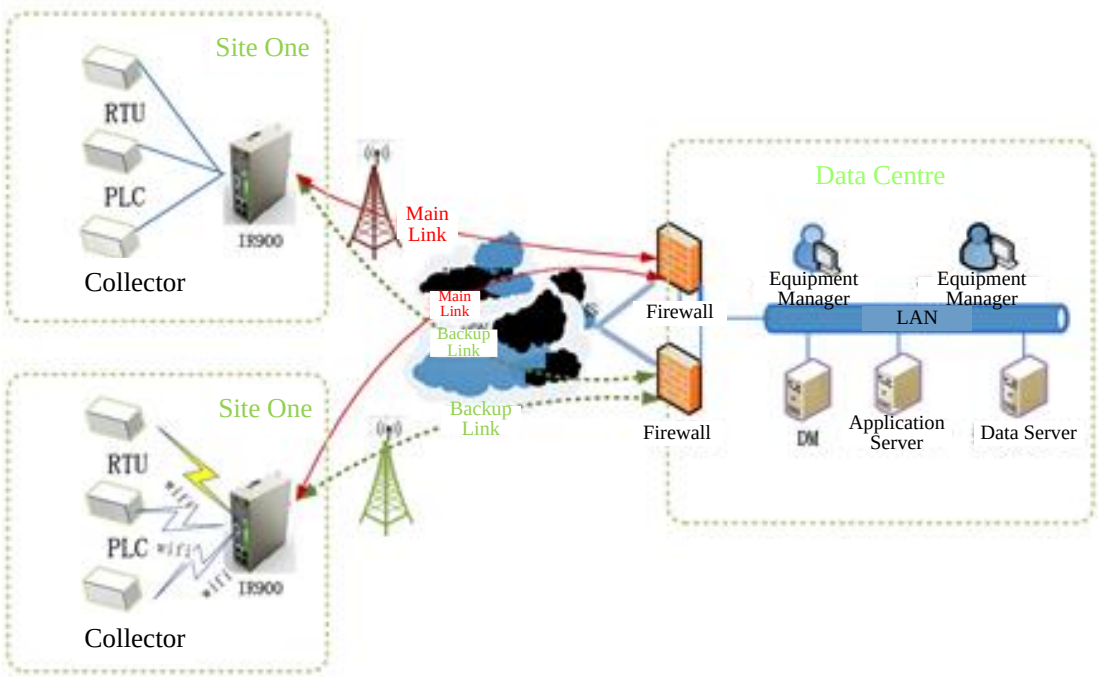


Fig. 4-1

1.2 Packing List

Standard Accessories

Accessories	Quantity	Description
IR900	1	IR900 series industrial 4G router

DIN-Rail	1	Router fixation
Power Terminal	1	2-pin green power terminal
Cable	1	1.5m cable
Antenna	1	3G/4G antenna

Optional Accessories

Accessories	Quantity	Description
AC power cord	1	AC power cord
Power Adapter	1	12VDC power adapter
Antenna	1	Wi-Fi antenna
Serial port cable	1	Serial port cable

1.3. Panel Introduction

Attention

IR900 series has a variety of panel appearances, but all of the installation methods are the same. The specific panel condition should be subject to the real object.

1.4 Introductions to Status LED

Status Description:

POWER (Red)	STATUS (Green)	WARN (Yellow)	ERROR (Red)	Description
On	On	On	Off	Powered On
On	Blinking	On	Off	Powered on succeed
On	Blinking	Blinking	Off	Dialing
On	Blinking	Off	Off	Dialing succeed
On	Blinking	Blinking	Blinking	Upgrading
On	Blinking	On	Blinking	Reset Succeed

Instruction

For the LED of two SIM card, the LED of SIM card 1 will be on during "Powered On" and "Powered on succeed" status. The following 4 conditions indicate the light turned on of SIM card 1 in use and the figure is described based on SIM card 1.

Signal status LED and description:

Green LED 1	Green LED 2	Green LED 3	Description
Off	Off	Off	No signal
On	Off	Off	Signal strength 1-9 (Signal strength is weak, please check antenna and the signal strength of current location)
On	On	Off	Signal strength 10-19 (signal strength is basically normal, and equipment can be used under normal conditions)
On	On	On	Signal strength 20-31 (signal strong)

Ethernet status LED and description:

Green LED	Description
On	ETH 100M, normal, no data transmission
Blinking	ETH 100M, normal, there is data transmission
Off	No connection

MODEM LED and description:

MODEM Green LED	Description
On	Dialing succeed
Blinking	Dialing failed

WLAN LED and description:

WLAN Green LED	Description
On	Enable WLAN
Off	Disable WLAN

II. Installation

Precautions:

- Power supply requirement: 24VDC (12~48VDC), please pay attention to the voltage grade of the power supply. Rated current: 0.15~0.6A.

- Environment requirement: working temperature -25℃~70℃, storage temperature -40℃~85℃, relative humidity 5%~95% (noncondensing). High temperature can be applied on equipment surface. During installation, surroundings should be taken into consideration and installation should be carried out within restricted area.
- Avoid direct sunlight, and keep away from heat sources or areas with strong electromagnetic interference.
- Routers need to be installed on an industrial DIN-Rail.
- Check if there are cables and splices needed by installation.

2.1 DIN Rail Mounting and Disassembly

2.1.1 DIN Rail Mounting

The specific steps are shown in below:

Step 1: select the installation location of equipment to ensure an enough space.

Step 2: fix the top of DIN rail seat on DIN rail. By slightly rotating the equipment upward from the bottom of equipment in the direction of arrow 2 shown below, the DIN rail seat can be fixed in DIN rail. It should be ensured that the equipment is reliably installed on DIN rail as shown in fig. 2-1-1.

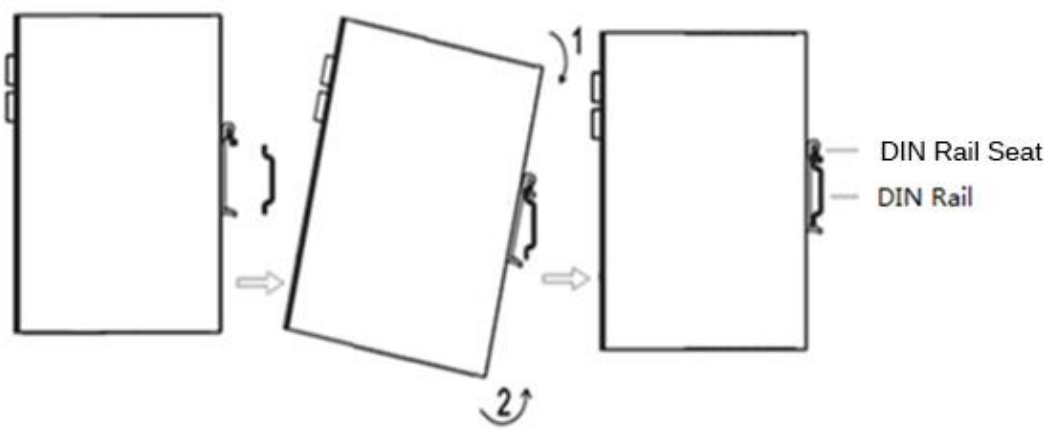


Fig. 2-1-1

2.1.2 DIN Rail Disassembly

The specific steps are shown in below:

Step 1: Press down the equipment to make the bottom of the equipment off the DIN rail as shown by arrow 1 in Fig. 2-1-2.

Step II: Turn the equipment as per the direction shown in arrow 2 and move the equipment bottom outwards simultaneously. Lift the equipment after the bottom is off the DIN rail. i.e., the equipment can be taken off from the DIN rail.

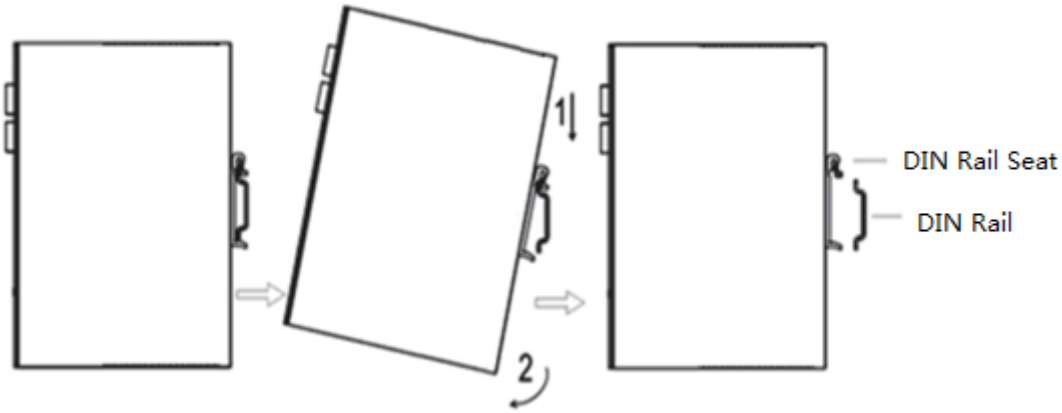


Fig. 2-1-2

2.2 Wall Mounting and Disassembly

2.2.1 Wall Mounting

The specific steps are shown in below:

Step 1: Select the installation location of the device, making sure there is enough space.

Step 2: Use a screwdriver to attach the wall mounting plate to the back of the device as shown in Figure 2-2-1.

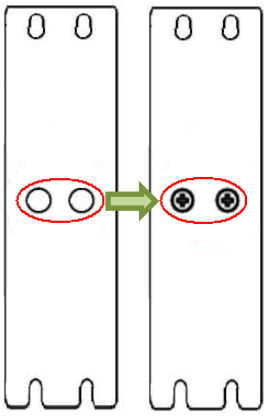


Fig. 2-2-1

Step 3: Take out screw (packaged in a complete set with wall mounting plate) and fix the screw on installation location. And then, pull down the device to ensure it is stable. As shown in Fig. 2-2-2.

Fig. 2-2-2

2.2.2 Wall Mounting Disassembly

The specific steps are shown in below:

Hold the device with a hand and disassemble the fixing screw on the top of device with another hand, so as to disassemble the device from installation location.

2.3 Installation of SIM Card and Antenna

The IR900 supports dual SIM cards. Press the button and SIM card holder will pop up, and then, install the SIM card.

Slightly rotate the movable part of metal SMA-J interface until it can not be rotated (at this time, external thread of antenna cable can not be seen). Do not forcibly screw the antenna by holding

black rubber lining.

Instruction

- IR900 support dual antennas: ANT antenna and AUX antenna. ANT antenna is for data receiving and transmission; AUX antenna is for increasing signal strength, which cannot be used separately without ANT antenna.
- Normally, ANT antenna is used; AUX antenna is required when the signal is weak.

2.4 Installation of Power Supply and Protective Grounding

Specific steps for power supply installation are shown below:

Step 1: take out the terminal from the router and screw down the lock screw on terminal;

Step 2: screw up the bolt after inserting power cable in terminal.

Specific steps for protective grounding installation are shown below:

Step 1: Remove the grounding nut.

Step 2: Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.

Attention

To improve the immunity from interference of whole router, the router must be grounded when using. According to operating environment, the ground wire should be connected with grounding stud of router.

2.5 Terminal Connection (only applicable to the device with industrial interface)

Serial port and IO port are of terminal access, thus relevant wires should be connected with terminals before use.

Serial port of device provides two interface modes: RS232 and RS485. Input end of IO port: IN indicates to digital quantity input end; COM indicates to grounding terminal. Input end of IO port: RELAY indicates the output end of relay.

Take down the terminal from the device and loosen the locking screw on the terminal. Then, insert the power supply cable into the terminal before tightening the screw. Cables are ordered as shown in Fig. 2-7-1.

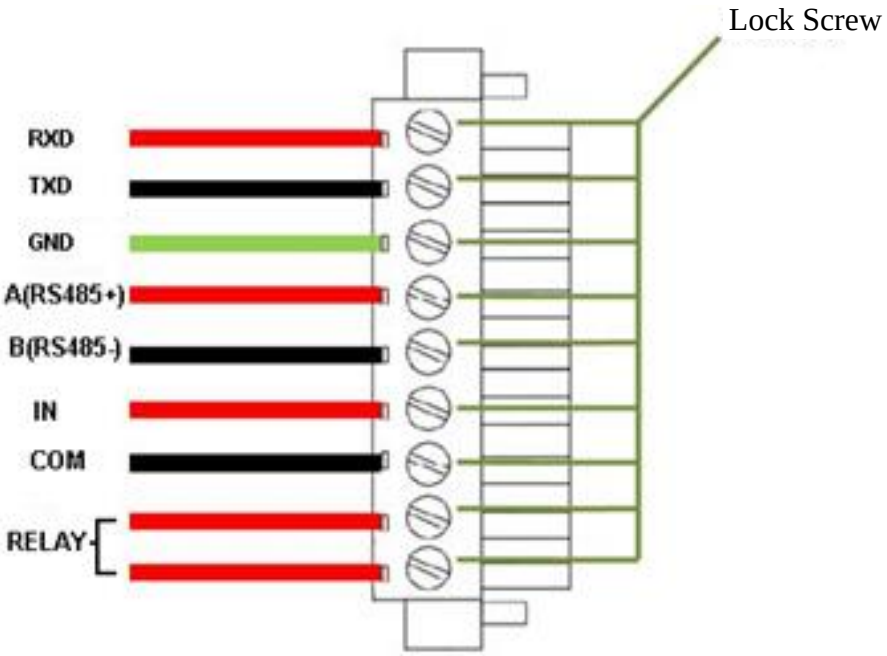


Fig. 2-7-1

2.6 Login Router

Firstly, IP address of PC should be changed to ensure it is within a same network segment as the device in the following two methods: automatic acquisition of IP address and static IP address. Proxy server (if any) should be cancelled for PC management settings. After setting the IP address of supervisory PC and ensuring there is no proxy server, the device can be logged in via web page.

I. 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 device automatically assign IP address for supervisory computer.

II. Set a static IP address

Set the IP address of supervisory PC (such as 192.168.2.2) and FE interface of device in same network segment (initial IP address of FE interface of device: 192.168.2.1, subnet mask: 255.255.255.0).

III. Cancel the Proxy Server

If the current supervisory PC uses a proxy server to access the Internet, it is required to cancel the proxy service. In the browser window, select "tools>>Internet options" and "connection" page and click the button of LAN Settings to enter "LAN Settings" window interface. Please confirm if the option "Use a Proxy Server for LAN" is checked; if it is checked, please cancel and click the button <OK>.

IV. Log in/exit Web settings page

Operate Web browser and enter http://192.168.2.1 in address bar (user name /password default: adm/123456). Click "exit" at the top right corner of Web interface and exit setting page after confirmation.

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.

III. Web Configuration

3.1 Management

The management includes 12 function modules: system, system time, management access, AAA, configuration management, SNMP, alarm, system log, system upgrade, reboot, network management platform and GPS locating information.

3.1.1 System

Here, system and network state and system time of synchronizing device and PC can be checked and router WEB configuration interface language can be set as well as the name of mainframe of router can be customized. Configuration interface can be directly entered via "Settings" after clicking Cellular1, Fastethernet 0/1 and Fastethernet 0/2 under network state.

3.1.2 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. System time is allowed to be set as any expected value after Year 2000 manually. Users can also use SNTP to achieve time synchronization of all devices equipped with a clock on network so as to provide multiple applications based on synced time.

Table 3-1-1 SNTP Client Parameter Description

Parameters	Description	Default
Enable	Enable/Disable SNTP client	Disable
Update Interval	Synchronization time intervals with SNTP server	3600
Source Interface	Cellular1, Fastethernet 0/1 and Fastethernet 0/2	None
Source IP	The corresponding IP of source interface	None
SNTP Servers List		
Server Address	SNTP server address (domain name /IP), maximum to set 10 SNTP servers	None
Port	The service port of SNTP server	123

Attention

- Before setting a SNTP server, users should ensure SNTP server reachable. Especially when the IP address of SNTP server is domain, users should ensure DNS server has been configured correctly.
- Users should configure either Source Interface or source IP. Source Interface and source IP cannot be configured at the same time.
- When setting multiple SNTP servers, system will poll all SNTP servers until an available SNTP server found.

3.1.3 Admin Access

Admin Access allows create users, modify users and management services.

Users include Super User and Common User:

- Super user: only one super user automatically created by the system, username adm. It has all access rights to the router.
- Common user: created by super user. Common users can view router configurations but don not have access to change configurations.

Instruction

Super User can neither modify nor delete its username (adm); but the password can be changed.

User right includes three levels:

- User right 1-11: only access to parameters check rather than configuration;
- User right 12-14: access to configure LAN IP, system time setting, basic configuration of firewall, virtual IP mapping table, system log, certificate application, access control, static routing, system upgrade and tool-ping detection. Others shown as grey, which can be checked but the configuration can not be modified;
- User right 15: access to the check and configuration for all parameters.

Management services include HTTP, HTTPS, TELNET and SSH.

- **HTTP:** users can log in the device via HTTP and access and control it through Web after clicking the button of "enable".
- **HTTPS:** HTTPS (security version of hypertext transfer protocol) is HTTP which supports SSL.
- **TELNET:** after clicking the button of "enable", users can provide remote login via network. 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**: Based on the RSA certification or the measures of encrypting username password and data transmission via encryption algorithm DES, 3DES and AES128, secure remote login can be provided via insecure network. IR900 only supports SSH server and it can receive many connections from SSH client.

Table 3-1-2 Management Service Parameter Description

Parameters	Description	Default
HTTP	Hypertext Transfer Protocol, Plaintext Transmission, Port: 80.	On
HTTPS	Secure SSL Encryption Transmission Protocol. Port: 443	Off
TELNET	Standard protocol and main way for Internet telnet service. Port: 23	On
SSH	Port: 22 **Timeout**: timeout of SSH session. No operation within this period on SSH Client, SSH Server disconnect. Default: 120s **Cipher Mode**: set up public key encryption method (currently only RSA supported)**. Cipher Code Length**: set up cipher code length, 512 or 1024. default: 1024	Off

3.1.4 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 services available.
- Charging: records of the utilization of network resources.

1) Radius

UDP protocol, generally applied in various network environments with higher requirements on

security and that permit remote user access.

2) Tacacs+

TCP protocol, mainly used for authentication, authorization and charging of access users and terminal users adopting PPP and VPDN.

3) LDAP

LDAP, simple as a table, only requires username, command, and something else, which makes it very simple.

Table 3-1-3 LDAP Parameter Description

Parameters	Description	Default
Name	Customized server name	None
Server Address	Server address (domain name / IP)	None
Port	Consistent with the server port	None
Base DN	The top of LDAP directory tree	None
Username	Username accessing the server	None
Password	Password accessing the server	None
Security	Encryption mod: None, SSL, StartTLS	None
Verify opposite end	Click to enable	Unopened

4) AAA

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

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, Tacacs+, local at the same time, priority order follow: 1 >2 >3.

3.1.5 Configuration Management

Here you can back up the configuration parameters, import the desired parameters configuration backup and reset the router.

Table 3-1-4 Configuration Management Parameter Description

Parameters	Description	Default
Browse	Choose the configuration file	None
Import	Import configuration file to router startup-config	None
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

Validity and order of imported configurations should be ensured. When importing the configuration, the system will filter incorrect configuration commands, and save the correct configuration as startup-config, when system restarts, it will orderly execute theses configurations. If the configuration files didn't be arranged according to effective order, the system won't enter the desired state.

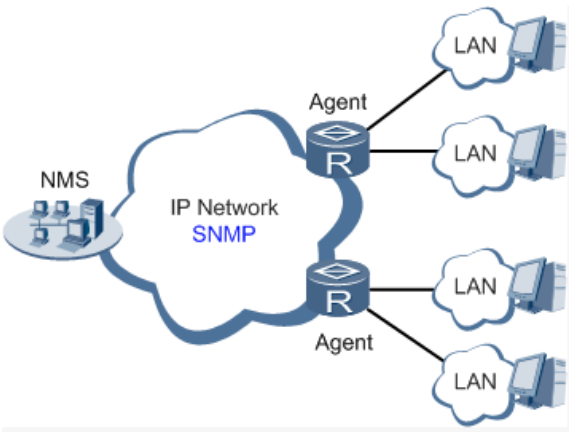
Instruction

In order not to affect current system running, when performing the import configuration and restoring the default configuration, and the new configuration will take effect after rebooting the router.

3.1.6 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 by different manufacturers and each manufacturer 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.

Figure showing how to manage devices through SNMP is shown below:



To configure SNMP in networking, NMS, a management program of SNMP, should be configured at the Manager. Meanwhile, Agent should 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 report current status information of device to NMS. In case of any problem, NMS will be notified immediately.

Currently, SNMP Agent of device supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication; SNMPv3 employs the authentication encryption way of username and password.

Table 3-1-5 SNMPv1 and SNMPv2c Parameter Description

Parameters	Description	Default
Enable SNMP	Enable/disable SNMP	Disable
SNMP version	Select SNMP version of management router, support SNMP v1/v2c/v3	v2c
Contact information	Fill contact information	Beijing_Inhand_Networks_Technology_Co.,Ltd.
Location information	Fill location information	Beijing_China
Community Management		
Community Name	User define Community Name	Public and private
Access Limit	Select access limit	ro (Read-only)
MIB View	Select MIB View	defaultView

Table 3-1-6 SNMPv3 Parameter Description

Parameters	Description	Default
User Group Management		
Groupname	User define, length: 1-32 characters	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		
Username	User define, length: 1-32 characters	None
Authentication mode	Select authentication mode, including two authentication modes: MD5 and SHA. Select "NoAuth" to disable it	SHA
Authentication Password	Enter authentication password only when authentication mode is not "NoAuth".	None
Encryption mode	Select whether employ DES encryption mode	DES
Encrypted password	Enter encrypted password only when encryption mode is not "NoPriv". Length: 8-32 characters	None
Groupname	Select corresponding user group, which should be identified firstly in management table of groupname	None

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.

Table 3-1-7 SnmpTrap Configuration Parameter Description

Parameters	Description	Default
Host Address	Fill in the NMS IP address	None
Security 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

3.1.7 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 users can troubleshoot problems.

According to the type of alarm, it can be divided into system alarm and port alarm.

- System Alarm: It produces because of system or environment happened to some exception, divided into hot start, cold start and insufficient memory.
- Port Alarm: It produces because of the network interface is up or down, divided into LINK-UP, LINK-DOWN.

Alarm status:

- Raise: Alarm is not confirmed
- Confirm: Alarm is temporarily unable to be resolved by users
- All: All alarms occurred

Alarm level:

- 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.

The following operations are feasible via alarm configuration dialog:

- On the “Alarm Status” page, you can view all the alarms since system was power on.
- On the “Alarm Input” page, you can define alarm types which you concern.
- On the “Alarm Output” page, you can set the way of alarm notice. Log record is in a default output way. When configuring the function and if there is an alarm, the system will send the alarm from email address sending alarm to objective email address, which is not recommended.
- On the “Alarm Map” page, you can map the alarm type which you concern to one or more alarm notice way. Alarm Map includes two type: CLI (console port) and Email. If Email map is required to be enabled, it should be enabled at Alarm Output part and configure email address.

3.1.8 System Log

System Log includes massive information about network and devices, including operating status, configuration changes and so on. Remote log server is feasible, and router will upload all system log to remote log server, which requires the cooperation of remote log software (such as) of

mainframe. 2323

Attention

When downloading system diagnosis records, configuration information of the router will be also downloaded.

3.1.9 System Upgrading

The upgrading process can be divided into two steps. In the first step, upgrading files will be written in backup firmware zone, e.g., the process in the section of System Upgrading; in second step: files in backup firmware zone will be copied to main firmware zone, which should be carried out during system restart. During software upgrading, any operation on web page is not allowed, otherwise software upgrading may be interrupted.

3.1.10 Reboot

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

3.1.11 Device Management

Device Management is a software platform to manage equipment. The equipment can be managed and operated via software platform when Device Management is started so that the internet can be in efficient operation. For instance, the operating status of equipment can be checked, equipment software can be upgraded, equipment can be restarted, configuration parameters can be sent down to equipment, and transmitting control or message query can be realized on equipment via Device Management.

Table 3-1-8 Device Management Parameter Description

Parameters	Description	Default
Schema	Message +IP	Forbidden
Supplier	Set name of equipment supplier	default
Equipment ID	Unaltered equipment ID	
server	Set IP address of device management	c.inhandnetworks.com
Port	Set port No. of device management	9002
Login retry times	Set retry times	3
Heartbeat interval time	Set heartbeat interval	120 秒
Serial port type	RS232/RS485	RS232

3.1.12 GPS Locating Information

Here the GPS function can be enabled or disabled and GPS IP transfer and GPS serial port transfer can be configured. GPS IP transfer has two types: client and server.

Table 3-1-9 GPS-IP Transfer Parameter Description

Parameters	Description	Default
GPS IP Transfer-Client		
Protocol	TCP or UDP	TCP
Connection Type	Long connection or short connection Keep consistency with server	Long connection
Heartbeat interval time	User define	100s
Heartbeat retry times	User define	10
Min. Reconnect	User define	15s

Interval		
Max. Reconnect Interval	User define	180s
Source Interface	Interface used to connect equipment with server	None
Information reporting interval	User define	30s
Including RMC	Send PMC data of GPS data	Enabled
Including GSA	Send GSA data of GPS data	Enabled
Including GGA	Send GGA data of GPS data	Enabled
Including GSV	Send GSV data of GPS data	Enabled
Message prefix	User define	None
Message suffix	User define	None
GPS IP Transfer-Client-Objective IP Address		
Server Address	Server address reported by GPS data	None
Server Port	Report the port number of server	None
GPS IP Transfer-Server		
Connection Type	Long connection or short connection Keep consistency with client	Long connection
Heartbeat interval time	User define	60s
Heartbeat retry times	User define	5
Information reporting interval	User define	30s
Including RMC	Send PMC data of GPS data	Enabled
Including GSA	Send GSA data of GPS data	Enabled
Including GGA	Send GGA data of GPS data	Enabled
Including GSV	Send GSV data of GPS data	Enabled
Message prefix	User define	None
Message suffix	User define	none

Table 3-1-10 GPS Serial Port Transfer Parameter Description

Parameters	Description	Default
Serial Port Type	Keep consistency with opposite end	RS232
Baud Rate	Keep consistency with opposite end	9600
Data Bit	Keep consistency with opposite end	8 bits
Parity	Keep consistency with opposite end	No check
Stop Bit	Keep consistency with opposite end	1 bits
Software Flow Control	Click to enable	Disabled
Including RMC	Send PMC data of GPS data	Enabled
Including GSA	Send GSA data of GPS data	Enabled
Including GGA	Send GGA data of GPS data	Enabled
Including GSV	Send GSV data of GPS data	Enabled

3.2 Network

The network module includes 10 function modules in total: Ethernet port, dialup port, ADSL dialing (PPPoE), loopback interface, DHCP service, DNS service, dynamic DNS, SMS, VLAN port and WLAN port.

3.2.1 Ethernet Port

Ethernet Port supports three connection modes:

- Automatic: configuration interface as DHCP Client and IP address obtained by DHCP.
- Manual: manually configure IP address and subnet mask for interface.
- PPPoE: configuration interface as PPPoE Client.

The connection of Ethernet port here is manual mode, namely, manually configuring an IP address and subnet mask.

Table 3-2-1 Ethernet Port Parameter Description

Parameters	Description	Default
Primary IP	IP address could be configured or changed according to demand	192.168.1.1
Subnet Mask	Auto generation	255.255.255.0
MTU	Maximal transmission unit, byte as the unit	1500
Speed/Duplex	Five options: Auto Negotiation, 100M Full Duplex, 100M Half -Duplex, 10M Full Duplex and 10M Half-Duplex	Auto Negotiation
Track L2 State	On: Port status after disconnection: Down Off: Port status after disconnection: UP	Off
Description	User defines the description	N/A
Multi-IP Settings	In addition to the primary IP, user could set Secondary IP addresses, 10 maximal.	N/A

Attention

In factory default state, DNS of PC connected at the lower end of F0/1 can not be applied with the original port IP of F0/1, otherwise, public domain can not be visited. But, visiting public domain can be realized by starting DHCP server or setting other DNS servers.

Table 3-2-2 Bridge Interface Parameter Description

Parameters	Description	Default
Bridge ID	Bridge ID can only be matched with 1	No
Bridge Interface		
IP Address of Main Address and Subnet Mask	Main IP address and subnet mask can be matched or modified according to the demand	No
IP Address of Slave Address and Subnet Mask	Users can be matched with IP address and subnet mask except for main IP	No
Bridge Member		
Click through the name of interface starting bridge interface		No

3.2.2 Dialup Port

SIM card dial out through dial access to achieve the wireless network connection function of router.

IR900 supports dial SIM card for backup. When primary SIM card breaks down or balance insufficiency, which results in network disconnection, rapid switching to backup SIM card is available, which will assume the task of network connection so as to improve the reliability of network connection.

Dial access supports three ways of connection: Always Online, Dial on Demand and Manual Dial.

Table 3-2-3 Dialup Port Parameter Description

Parameters	Description	Default
Dialup parameter set	Dial-up strategy	1
Roaming	Enable/Disable roaming	Enable
PIN Code	SIM card PIN code	None
Network Type	Five options: Auto, 2G, 3G, 4G and 3G2G	Auto
Static IP	Enable Static IP if your SIM card can get static IP address	Disable
Connection Mode	Optional Always Online, dial on demand (data activation, phone activation, SMS activation are allowed), manual dialing	Always Online
Redial Interval	The time interval between first dial fails can redial	10s
ICMP Detection Server	Far-end IP address to be detected	None
ICMP Detection Interval	Set ICMP Detection Interval	30s
ICMP Detection Timeout	Set ICMP Detection Timeout	5s
ICMP Detection Max Retries	Set the max number of retries if ICMP failed (redial if reaching max. times)	5
ICMP Detection Strict	Click to enable	Disable
Dialup Parameter Set		
Network Type	Choose mobile network type	GSM
APN (inapplicable to CDMA2000 series)	Mobile operator provides relevant parameters (according to ISP)	3gnet
Access Number	Mobile operator provides relevant parameters (according to ISP)	*99***1#
Username	Mobile operator provides relevant parameters (according to ISP)	gprs
Password	Mobile operator provides relevant parameters (according to ISP)	******
Advanced Options (following items are relevant parameters after enabling advanced options)		
Initial Commands	Used for advanced parameters, no need to be filled in generally	None
RSSI Poll interval	Set the signal query interval	120s
Dial Timeout	Dial timeout, the system will redial	120s
MTU	Set max transmit unit, In bytes	1500
MRU	Set max receive unit, In bytes	1500
Use default asyncmap	Enable default asyncmap	Forbidden
Use Peer DNS	Receiving mobile operators assigned DNS	Enable
Link detection interval	Set link detection interval	55s
Link detection Max Retries	Set the max retries if link detection failed (redial if reaching max. times)	5
Debug	System can print a more detailed log	Enable
Expert Option	Provide extra PPP parameters, normally user needn't set this.	None
Dual SIM Enable	Enable dual SIM card mode (**following items are**	Disable

	relevant parameter configuration after enabling)	
Main SIM	Choose to be a SIM car of main card	SIM1
Max Number of Dial	Set Max. dialing times (Reach the max number, SIM card will be switched)	5
Min Connected Time	Set min. connection time	0s
Signal threshold	Set signal threshold (signal detection will be performed again when lower than signal threshold)	0
Signal detect interval	Set signal detect interval	0
Signal detect retries	Set signal detect retries (redial if reaching max. times)	0
Backup SIM Timeout	From beginning to switch to the backup card counting, exceeds the timeout, router will switch to the primary card	0

3.2.3 ADSL Dialing (PPPoE)

PPPoE is a point-to-point protocol over Ethernet. User has to install a PPPoE Client on the basis of original connection way. Through PPPoE, remote access devices could achieve the control and charging of each accessed user.

Connection mode at Ethernet port must be PPPoE, namely, configuration interface must be the PPPoE Client.

Table 3-2-4 Dialing Port Parameter Description

Parameters	Description	Default
Pool ID	User define, easy to memorize and manage	None
Interface	Fastethernet0/1 and Fastethernet0/2 are choosable	Fastethernet0/1
PPPoE List		
ID	User define, easy to memorize and manage	1
Pool ID	Same as the dialup pool	None
Authentication Type	Auto, PAP, CHAP	Auto
User Name	Operators provide the relevant parameters	None
Password	Operators provide the relevant parameters	None
Local IP Address	Set the IP address assigned for Ethernet interface	None
Remote IP Address	Set the IP of remote device	None

3.2.4 Loopback Interface

Loopback interface is used to take place of router's ID since as long as an active interface is used, when it turns to DOWN, ID of router has to be selected again, resulting to long convergence time of OSPF. Therefore, generally loopback interface is recommended as the ID of router.

Loopback interface is a logic and virtual interface on router. Under default conditions, a router has no loopback interface which can be created for a number as required. Those interfaces are the same as physical interfaces on router: addressing information allocated, including their network number in router upgrade and even IP connection could be terminated on them.

Table 3-2-5 Loopback Interface Parameter Description

Parameters	Description	Default
IP Address	Users can not change	127.0.0.1
Netmask	Users can not change	255.0.0.0
Multi-IP Settings	Apart from above IP, user can configure other IP address	N/A

Attention

Since the loopback interface monopolizes one IP address, subnet mask is generally suggested to be 255.255.255.255 for the purpose of saving resources.

3.2.5 DHCP Service

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.

- 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.

- As DHCP Client, the device receives the IP address distributed by DHCP server after logging in the DHCP server, so the Ethernet interface of the device needs to be configured into an automatic mode.

Table 3-2-6 DHCP Server Parameters

Parameters	Description	Default
Enable	On/Off	Off
Interface	Fastethernet 0/1 and Fastethernet 0/2 available	Fastethernet 0/1
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.
- InRouter900 F0/2 enable DHCP server by default; obtaining IP address automatically is suggested.

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).

Table 3-2-7 DHCP Transfer Parameters

Parameters	Description	Default

Enable	On/Off	Off
DHCPSever	Set DHCP server; up to 4 servers can be configured	N/A
Source address	Address of the interface connected to the DHCP server	N/A

3.2.6 DNS Services

DNA (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.

Manually set the DNS, use DNS via dialing if it is empty. Generally, it needs to set this only when using the static IP at the WAN port.

Table 3-2-8 DNS Parameters

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

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.

Table 3-2-9 DNS Transfer Parameters

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.

3.2.7 Dynamic Domain Name

DDNS maps user's dynamic IP address to a fixed DNS service. When the user connects to the network, the client program will pass the host's dynamic IP address to the server program on the service provider's host through information passing. The server program is responsible for providing DNS service and realizing dynamic DNS. It means that DDNS captures user's each change of IP address and matches it with the domain name, so that other Internet users can communicate through the domain name. What end customers have to remember is the domain name assigned by the dynamic domain name registrar, regardless of how it is achieved.

DDNS serves as a client tool of DDNS and is required to coordinate with DDNS Server. Before the application of this function, a domain name shall be applied for and registered on a proper

website such as www.3322.org. After the settings of dynamic domain name on WBR204n, a corresponding relationship between the domain name and IP address of WAN port of the device is established.

IR900 DDNS service types include DynAccess, QDNS (3322)-Dynamic, QDNS (3322)-Static, DynDNS-Dynamic, DynDNS-Static and NoIP.

Table 3-2-10 DDNS Parameters

Parameters	Description	Default
Method Name	User define	None
Service Type	Select the domain name service providers	None
User Name	User name assigned in the application for dynamic domain name	None
Password	Password assigned in the application for dynamic domain name	None
Host Name	Host name assigned in the application for dynamic domain name	None
Method	The update method of specified interface	None

Attention

If the IP address obtained via router dialing is a private address, the dynamic DNS function is not available.

3.2.8 SMS

SMS permits message-based reboot and manual dialing. 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.

Table 3-2-11 SMS Parameters

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 refuse are available	Permit
Phone Number	Trusting phone number	N/A

3.2.9 VLAN Interface

VLAN is a kind of new data exchange technology that realizes virtual workgroups by logically dividing the LAN device into network segments.

Table 3-2-12 VLAN Parameters

Parameters		Description	Default
VLAN ID		i.e. VLAN ID, user defined	N/A
SMS Access Control			
Primary IP address	IP address	User can configure or change the primary IP address as required	N/A
	Subnet mask	User can configure or change the subnet mask as required	

Secondary IP address	IP address	Besides the primary IP, user can also configure 10 secondary IP addresses	N/A
	Subnet mask	Configure or change the subnet mask as required	

3.2.10 WLAN Interface

WLAN refers to Wireless Local Area Network. WLAN has two types of interfaces, the Access point and the Client.

Table 3-2-13 WLAN Parameters

Parameters	Description	Default
Access point		
SSID broadcast	After turning on, use can search the WLAN via SSID name	Turn on
RF type	Six type for options: 802.11g/n, 802.11g, 802.11n, 802.11b, 802.11b/g , 802.11b/g/n	802.11g/n
Channel	Select the channel	11
SSID	SSID name defined by user	InRouter900
Authentication method	Four authentication methods for option: open type, shared type, WPA-PSK and WPA2-PSK	Open type
Encryption	Support NONE, WEP40 and WEP104 as per different authentication methods	NONE
Wireless bandwidth	Both 20MHz and 40MHz for selection	20MHz
Maximum number of clients	User defined (at most 128)	N/A
Client		
SSID	Fill in the name of the SSID to be connected	N/A
Authentication method	Stay the same with the authentication method of the SSID to be connected	Open type
Encryption	Stay the same with the encryption method of the SSID to be connected	NONE

The device usually needs three steps of setting when used as Client:

Step I: Click the “Network>>Dial interface” menu in the navigation tree to enter the “ail interface”, close the dial interface. This step will be unnecessary when the device is without a module. Instead, directly operate the second step.

Step II: Click the “Network>>WLAN interface” menu in the navigation tree to enter the “WLAN interface”. Select “Client” for the interface type and configure relevant parameters.

Step III: Click the “Setup Wizard>>New WLAN” menu in the navigation tree to enter the “New WLAN” interface. Select fastethernet 0/1 as the interface; the type can be either the dynamic address (DHCP) or static IP. If the static IP is selected, it needs to configure relevant parameters in the “IP setting” interface and the Client IP address must be the same with that of the AP network segment.

The scanning function of the SSID can be started only when selecting the Client at the WLAN interface type. In the “SSID scanning” interface, all available SSID names as well as the connection status of the device as Client will be displayed.

3.3 Link Backup

3.3.1 SLA

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.

Table 3-3-1 SLA Parameters

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
Connective	Detection retries	5
Life	Default is “forever”, user cannot change	forever
Start-time	Detection Start-time, select “now” or None	now

3.3.2 Track Module

Track is designed to achieve linkage consisting of application module, Track module and monitoring module. 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. 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.

Table 3-3-2 Track Module Parameters

Parameters	Description	Default
Index	Track index or ID	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	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	In case of failure recovery, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching.	0

3.3.3 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

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.

Table 3-3-3 VRRP Parameters

Parameters	Description	Default
Enable	Enable/Disable	Enable

Virtual Route ID	User define Virtual Route ID	None
Interface	Configure the interface of Virtual Route	None
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 replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Enable
Track ID	Trace Detection, select the defined Track index or ID	None

3.3.4 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.

Table 3-3-4 Interface Backup Parameters

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

3.4 Routing

3.4.1 Static Route

Generally, user does not need to set this. 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.

Table 3-4-1 Static Route Parameters

Parameters	Description	Default
Destination address	Enter the destination IP address need to be reached	0.0.0.0
Subnet Mask	Enter the subnet mask of destination address need to be reached	0.0.0.0
Interface	The interface through which the data reaches the destination address	Cellular1
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

3.4.2 Dynamic Routing

The gateway protocol used in the autonomous system (AS) consists of the OSPF protocol and the RIP protocol.

1) RIP

RIP is mainly used for smaller networks. 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.
- Routing Cost: 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.

Table 3-4-2 RIP Parameters

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	180

	routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16.	
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
Version	Version number of RIP	V2
Network	The first IP address and subnet mask of the segment	None
Advanced Options		
Filter In	Only send RIP packets do not receive RIP packets	Disable
Filter Out	RIP packets sent to the default routing interface	Disable
Default-Information Originate	Default information will be released	Disable
Default Metric	The default overhead of the router reach to destination	1
Distance	Set the RIP routing administrative distance	120
Redistribute router	Introduce the directly connected, static, OSPF protocols into the RIP protocol	Disable
Passive Default	Interface only receives RIP packets, do not send RIP packets	None
Neighbour	For neighbouring routers, after configuring neighbours, rip package will only be sent to neighbouring routers	None

2) 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 address from other interfaces as the Router ID.

OSPF has five types of packets:

- Hello Packet
- DD Packet (Database Description Packet)
- LSR packet (Link State Request Packet)
- LSU Packet (Link State Update Packet)
- LSAck packet (Link State Acknowledgment Packet)

Neighbour and Neighbouring

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 neighbour relationship will be formed. Not all both sides in neighbour 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.

Table 3-4-3 OSPF Parameters

Parameters	Description	Default
Enable	Enable/Disable	Disable
Router ID	RouterID of the originating the LSA	None
Advanced Options		
Default Metric	The default overhead of the router reach to destination	None
Redistribute Router	Introduce the directly connected, static, RIP protocols into the OSPF protocol	Disable
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
Interface		
Interface	The interface	None
Hello Interval	Send interval of Hello packet. If the Hello time between two adjacent routers is different, you can not establish a neighbour relationship.	None
Dead Interval	Dead Time. If no Hello packet is received from the neighbours, the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship can not be established.	None
Network	Select OSPF network type	None
Priority	Set the OSPF priority of interface	None
Retransmit Interval	When the router notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour.	None
Interface	The interface	None
Hello Interval	Send interval of Hello packet. If the Hello time between two adjacent routers is different, you can not establish a neighbour relationship.	None

3) Routing Policy

Table 3-4-4 Routing Policy Parameters

Parameters	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	Forbidden
IP Address	User defined	None
Subnet Mask	User defined	None
Prefix List		
Prefix Name List	User defined	None
Serial Number	A prefix name list can be matched with multiple rules, one rule is matched with one serial number	None
Action	Permit and deny	Permit
Any Address	Any address after clicking, no matching IP address and subnet mask again	None
IP Address	User defined	None

Subnet Mask	User defined	None
Grand Equal Prefix Length	Filling in network marking length of subnet mask and restricting the minimum IP address in IP section	None
Less Equal Prefix Length	Filling in network marking length of subnet mask and restricting the maximum IP address in IP section	None

3.4.3 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 for relaying multicast data packet correctly and efficiently.

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

Table 3-4-5 Basic Setup Parameters

Parameters	Description	Default
Enable	Open/Close	Close
Source	IP Address of Source	None
Netmask	Netmask of Source	255.255.255.0
Interface	Interface of Source	cellular1

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 signalling 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.

Table 3-4-6 IGMP Parameters

Parameters	Description	Default
Upper port	The port connecting the upper-level network device	N/A
Lower port list		
Lower port	The port connecting the lower terminal device	cellular 1
Upper port	The port connecting the upper-level network device	cellular 1

3.5 Firewall

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.

3.5.1 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 present 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.

Table 3-5-1 AC Parameters

Parameters	Description	Default
Type	**Standard ACL** can prevent all the communication flow of some network or permit all the communication flow of some network or refuse all the communication flow of some protocol stack (like IP). **Expanded ACL** can provide more extensive control scope than standard ACL does. For instance, network manager can make use of expanded ACL instead of standard ACL to permit Web communication flow, refuse FTP and Telnet because the control of ACL is not as desired.	Expanded
ID	User self-defined number	No
Action	Permit/refuse	Permit
Agreement	ACP	Ip
Source IP address	Source network address (blank in case of any configuration)	No
Source address wildcard mask	Radix-minus-one complement of mask in source network address	No
Destination IP address	Destination network address (blank in case of any configuration)	No
Destination address wildcard mask	Radix-minus-one complement of mask in destination address	No
Writing log	Click starting and the log about access control will be recorded in the system after starting	Forbidden
Description	Convenient for recording parameters of access control	No
Network Interface List		
Port name	Select the name of network interface	cellular1
Rule	Select the rules for in and out and management	none

3.5.2 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.

Table 3-5-2 Network Address Translation (NAT) Parameters

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

Attention

NAT rule is to apply ACL into address pool, and only address matched with ACL can be translated.

Instruction

Private network IP address refers to the IP address of home network or mainframe, and IP address of public network refers to the only global IP address on the internet. RFC 1918 reserves 3 IP addresses for private network, as shown followed:
A: 10.0.0.0~10.255.255.255
B: 172.16.0.0~172.31.255.255
C: 192.168.0.0~192.168.255.255
The addresses in the three types above will not be distributed on the internet, so they can be used in companies or enterprises instead of being applied to operator or registration center.

3.5.3 MAC-IP Binding

If the default process in the basic setting of firewall is disabled, only hosts specified in MAC-IP can have an access to outer net.

Table 3-5-3 MAC-IP Binding Parameters

Parameters	Description	Default
MAC address	Set the binding MAC address	00:00:00: 00:00:00
IP address	Set the binding MAC address	Empty
description	convenient for recording the meaning of the binding rule of each piece of MAC-IP	Empty

3.6 QoS

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.

Table 3-6-1 Flow Control Parameters

Parameters	Description	Default
Type		
Name	Name of user self-defined flow control	No
Any Message	Click starting, control the flow of any message after starting	Forbidden
Source Address	Source address of flow control (blank in case of any configuration)	No
Destination Address	Destination address of flow control (blank in case of any configuration)	No
Protocol	Click protocol type	No
Strategy		
Name	Name of user self-defined flow control strategy	No
Type	Name of defined types above	No
Assured Bandwidth Kbps	Assured bandwidth in user self-definition	No
Maximum Bandwidth Kbps	Maximum bandwidth in user self-definition	No
Local Preference	Local preference in selecting strategy	No
Application Qos		
Port	Control port of selecting flow	cellular1
Maximum Input Bandwidth Kbps	Maximum bandwidth more than input strategy in user self-definition	No
Maximum Output Bandwidth Kbps	Maximum bandwidth more than output strategy in user self-definition	No
Input Strategy	Strategy name defined above	No
Output Strategy	Strategy name defined above	No

3.7 VPN

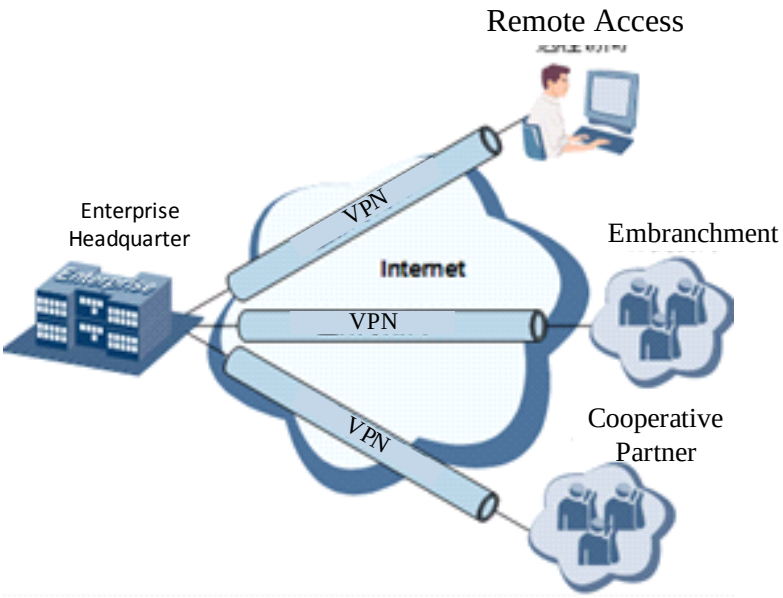
VPN is for building a private dedicated network on a public network via the Internet. 'Virtuality" mainly refers to that the network is a logical network.

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.

Build a credible and secure link by connecting remote users, company branches, partners to the network of the headquarters via VPN so as to realize secure transmission of data. It is shown in the figure below:



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.

3.7.1 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.

Table 3-7-1 IPSec Configuration Parameters

Parameters	Description	Default
IKEv1 Policy		
Identification	Policy identification of user defined IKE	N/A
Authentication	Alternative authentication: shared key and digital certificate	AES128
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	SHA1
Hash	MD5: input information of arbitrary length to obtain 128bit 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.	Group2
Diffie-Hellman Key Exchange	Three options: Group 1, Group 2 and Group 5	86400
IKEv2 policy		
Identification	User defined IKE policy identification	N/A
Encryption algorithm	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	AES128
Integrity	MD5: input information of arbitrary length to obtain 128bit message digest. SHA-1: input information with shorter length of bit to obtain 160bit message digest.	SHA1
Diffie-Hellman key exchange	Multiple options	Group2
Lifetime	Valid time of policy	86400
IPSec Policy		
Name	User define Transform Set name	N/A
Encapsulation	Choose encapsulation forms of data packet AH: protect integrity and authenticity of data packet from 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.	ESP
Encryption	Multiple options	AES128
Authentication	Multiple options	SHA1
IPSec Mode	**Tunnel Mode**: besides source host and destination host, special gateway will be operated with	Tunnel Mode

	password to ensure the safety from gateway to gateway. **Transmission Mode**: 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.	
IPSec tunnel configuration-basic parameters		
Opposite end address	Opposite end IP address	
Interface name	Select the interface name	Cellular 1
IKE version	Select the IKE version	IKEv1
IKEv1 policy	Policy identification defined in the IKEv1 policy list	
Ipsec policy	Policy identification defined in the IPsec policy list	
Negotiation Mode	**Main mode**: as an exchange method of IKE, main mode shall be established in the situation where stricter identity protection is required. **Aggressive mode**: 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
Authentication	Alternative authentication: shared key and digital certificate	Shared key
Local subnet address	The source network in the reverse crypto map ACL defined by IPESC	N/A
Subnet address of subnet addresses	The source network in the destination network defined by IPESC	N/A
IPSec tunnel configuration-IKE advanced option (stage 1)		
Local identification	The local identification corresponds to the selected local identification	N/A
Opposite end identification	The opposite end identification corresponds to the selected opposite end identification	N/A
IKE connection detection (DPD)	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. Used for detection interval of IPSec neighbour state. After initiating DPD, If receiving end can not receive IPSec cryptographic message sent by peer end within interval of triggering DPD, receiving end can make DPD check, send request message to opposite end automatically, detect whether IKE peer pair exists.	0, 0 Proposed parameter 60, 180
XAUTH	XAUTH user name, XAUTH code	N/A
IPSec tunnel configuration- IPSec advanced option (stage 2)		
Perfect Forward Security (PFS)	Means the reveal of one cipher code will not endanger information protected by other cipher codes.	Ban
IPsec SA Lifetime	Lifetime of IPSec Profile	3600
IPSec tunnel configuration-Tunnel advanced option		
Respond Only	If it is used, the local can only passively receive the Ipsec request and will not connect actively. It is commonly used in the server mode.	Ban
Rules for local/remote sending of certificates	When using the certificate to build Ipsec, both ends shall know the certificate of each other and pass the verification before a successful connection can be	Always send certificate

	built. The local certificate is generally kept but the certificate of the opposite end may be kept or may be not (common situation); generally, both ends will send the request for "certificate request" when IPSEC is being connected. The ipsec server will send its certificate to the opposite end after having received this request. **Always send certificate:** Some ipsec server does not send a "certificate request" request and it has not place to keep the certificate send from the opposite end, so the opposite end can build Ipsec only by being configured as "always send certificate". **Send certificate under request:** The local certificate is sent only when the opposite end sends a request. **Not send certificate:** The certificate will be send to the opposite end no matter the opposite end sends a request or not.	
ICMP detection	Detection server, detecting local address, detection interval, detection time-out, maximum number of retries	N/A, N/A, 60, 5, 10

Table 3-7-2 IPSec Extension Parameters

Parameters	Description	Default
Basic parameters		
Name	User defined	admin
IKE version	Select the IKE version	IKEv1
IKEv1 policy	Policy identification defined in the IKEv1 policy list	N/A
Ipsec policy	Policy identification defined in the IPsec policy list	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. **Aggressive mode**: 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
Authentication	Alternative authentication: shared key and digital certificate	Shared key
IKE advanced option (stage 1)		
Local identification	The local identification corresponds to the selected local identification	N/A
Opposite end identification	The opposite end identification corresponds to the selected opposite end identification	N/A

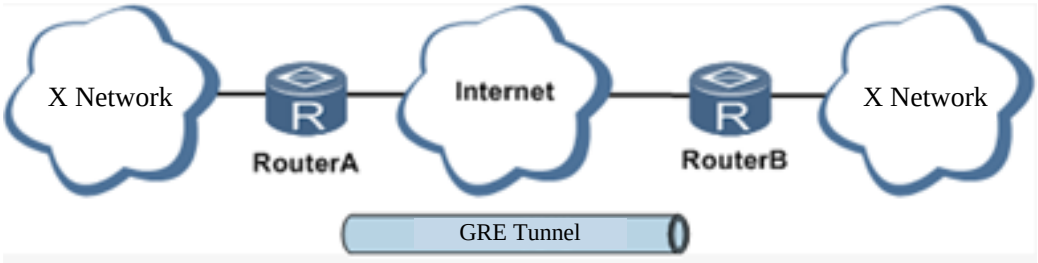
IKE connection detection (DPD)	Receiving end will make DPD check and send request message automatically to opposite end for check. If it does not receive IPSec cryptographic message from peer end beyond timeout, ISAKMP Profile will be deleted. Used for detection interval of IPSec neighbour state. After initiating DPD, If receiving end can not receive IPSec cryptographic message sent by peer end within interval of triggering DPD, receiving end can make DPD check, send request message to opposite end automatically, detect whether IKE peer pair exists.	0, 0
IPSec advanced option (stage 2)		
Perfect Forward Security (PFS)	Means the reveal of one cipher code will not endanger information protected by other cipher codes.	Ban
IPsec SA Lifetime	Lifetime of IPSec Profile	3600

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.

3.7.2 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 is applied:

- GRE tunnel could transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot 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. As shown below:

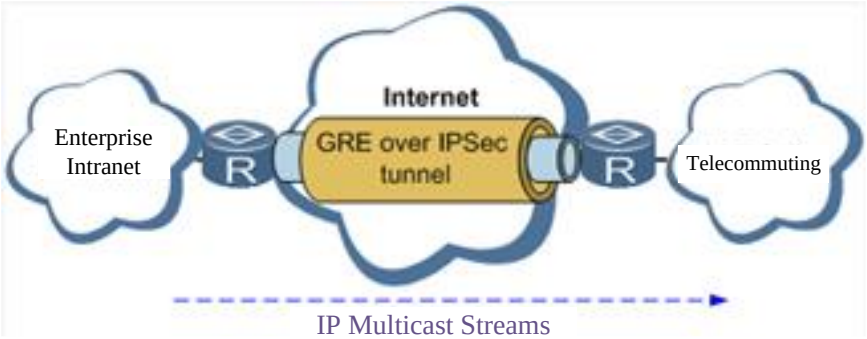


Table 3-7-3 GRE Key Parameters Description

Parameters	Description	Default
Enable	Click to enable	Enabled
Interface Identifier	Configure the name of GRE tunnel	NO
Network type	Select GRE network type	Point-to-point
Local visual IP	Configure local visual IP address	NO
Peer visual IP	Configure peer visual IP address	NO
Source address type	Select source address type, and configure corresponding types of IP addresses or interface names	IP
Local IP address	Configure local IP address	NO
Peer address	Configure peer address	NO
Password	Configure tunnel password	NO
MTU	Configure maximum transmission unit, in bytes	NO
Enable NHRP	Next Hop Resolution Protocol applied in access connected source stations with to non-broadcast multiple access (NBMA) sub-network (mainframe or router). It also determines the network layer address and NBMA sub-network address of “NBMA next hop” before reaching targeted stations.	Enabled
Description	Add description	NO

3.7.3 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, and 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.

Typical L2TP network diagram is shown below:

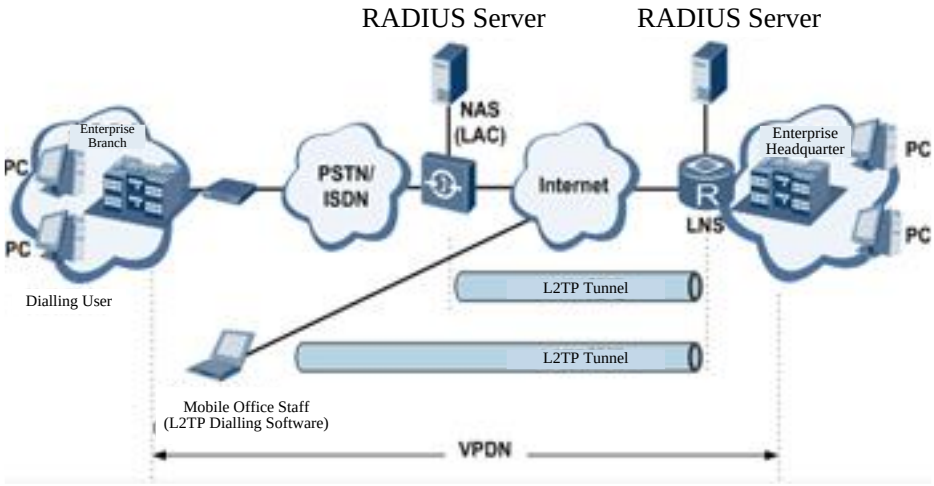


Table 3-7-4 Key Parameters Description for Flow Control

Parameters	Description	Default
L2TP Class		
Name	User-defined L2TP Class name	No
Authentication	Click to enable, authentication of backend is needed in network connection	Disable
Host Name	Host name for home terminal network connection, unmatched is acceptable	No
Tunnel Authentication Password	When authentication is enabled, tunnel authentication password must be configured, or no configuration will be required	No
Pseudowire Class		
Name	User defined pseudowire class name	No
L2TP Class	L2TP class name defined above	No
Source port	Select Source port name	cellular 1
L2TP Tunnel		
Enable	Click to enable	Enabled
Identifier	Generated Automatically	1
L2TP Server	Set L2TP Server address	No
Pseudowire Class	Pseudowire class name defined above	No
Authentication Type	Select authentication type	Auto
Username	Peer server username	No
Password	Peer server password	No
Local IP Address	Set local IP address, or let peer server allocate automatically	No
Remote IP Address	Set remote IP address, unmatched is acceptable	No

3.7.4 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.

Table 3-7-5 Parameters Description for OPENVPN Client

Parameters	Description	Default
Enable	Click to enable	Enabled
ID	Set channel ID	No
Server IP Address	Fill in IP address of backend server	No
Port Number	Fill in port number of backend server	1194
Certification Type	Select certification type and configure corresponding parameters of certification type	Username/Password
Username	Keep consistency with server	No
Password	Keep consistency with server	No
Channel Description	Content described in user's self-defined channel	No
Advanced Options		
Source Port	Select name of source port	No
Network Type	Select type of network	net30
Port Type	Select the data form sending out from the port. tun-data package, tap-data frame	Tun
Protocol Type	Protocol in server communication and keep consistency with server protocol	Udp
Encryption Algorithm	Keep consistency with server	Default
LZO Compression	Click to enable	Off
Connection Testing Interval	Set connecting testing time interval	No
Connection Testing Overtime	Set connecting testing overtime	No
Expert Configuration	Set expert option: blank advisable	No

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.

3.7.5 Authentication Management

Table 3-7-6 GRE Key Parameters Description for Authentication Management

Parameters	Description	Default
Authentication Protected Password	Configure authentication protected password	No
Confirmation of Authentication Protected Password	Confirm authentication protected password	No

3.8 Industrial (this Chapter Only Applies for IR900 Devices with Industrial Interface

Routers can connect with terminals through industrial interfaces, and can wirelessly upload data to upper devices. This realizes the wireless communication between terminals and upper devices.

Router's industrial interface has two types: serial port and IO interface. Serial port has RS232 and RS485 modes and IO interface has digital input and relay output modes.

RS232 adopts full-duplex communication with one transmission line, one receiving line and one ground line. RS232 is generally used for communication within 20m.

RS485 adopts half-duplex communication to achieve long-distance transmission of serial communication data. To ensure the accuracy of long distance transmission for industrial sites, RS485 is normally used on industrial sites. RS485 is used for communication from tens of meters to kilometers.

Digital input of IO interface can convert electrical signals into binary digital control signals. The digital is a logical variable or switch variable with only two values 0 and 1. Low voltage corresponds to the "0" and high voltage to "1"

IO's relay output functions as an "auto switch" to automatically adjust protect and switch circuit.

3.8.1 DTU

3.8.1.1 Serial Port Settings

Setting the parameters of router's serial port according to the serial port of the terminal device connected with router to achieve the normal communication between router and terminal device.

Table 3-8-1 Serial Port Setting Parameter Description

Parameters	Description	Default
Serial Port Type	Serial Port 1 is RS232, Serial Port 2 is RS485; cannot be changed	RS232/RS485
Baud Rate	Same with the baud rate of connected terminal device	9600
Data Bit	Same with the data bit of connected terminal device	8 bits
Parity	Same with the parity of connected terminal device	None
Stop Bit	Same with the stop bit of connected terminal device	1 bits
Software Flow Control	Click to enable	Off
Description	User define	No

Attention

The parameters of router's serial port must be the same with that of terminal device connected.

3.8.1.2 DTU 1

Table 3-8-2 DTU 1 Parameter Description

Parameters	Description	Default
Enable	Click to enable	Off
DTU Protocol	Transparent and TCP: router used as client when Transparent is chosen, router used as server when TCP is chosen. RFC2217: no need to configure serial port IEC101-104: for power industry, similar with TCP in function	Transparent
Protocol	TCP or UDP	TCP Protocol
Connection Type	Long connection or Short connection	Long connection
Heartbeat interval	User define	60

time		
Heartbeat Retry	User define, TOP connection is off when reaching retry limit	5
Serial Buffer Frames	User define	4
Serial Frame Length	User define	1024
Serial Frame Interval	User define	100
Min Reconnect Interval	User define. If connection fails in device star-up, reconnection will be done based on this min interval, until the max reconnection interval reaches user defined value.	15
Max Reconnect Interval	User define. When connection interval reaches maximum, reconnection will be done according to this interval (user defined value).	180
Multi-Server Policy	**Parallel:** connect the center of destination IP address list at the same time **Polling:** connect to the first address in the list, if connect fail, continue to connect next address until connect one successfully, then stop.	Parallel
Source port	4 options; No need to choose	IP
Local IP Address	The device's IP in Source port "IP" selection. No need to configure	No
DTU Identification	User defined. DTU identification will be sent automatically to server after successful connection. Can remain empty without configuration.	No
Debug Log	Click to enable	Off
Destination IP Address		
Server Address	User define	No
Server Port	User define	No

Instruction

- Destination IP Addresses maximum 10.
- DTU 2 configuration is same with DTU 1.

3.8.2 IO Interface

Relay output is off by default and it can be turned on/off manually. The disconnect time can be set manually and after reaching the set parameters relay output is automatically turned off.

Table 3-8-3 IO Interface Status Parameters Description

Parameters	Description	Default
Digital Input		
Digital Input 1	Voltage under 10V correspond to "low" (0) Voltage equals and above 10V correspond to "high" (1)	Low (0)
Relay Output		
Relay Output 1	Off by default. Can be turned on manually, otherwise it is remains off.	On
Action	**Off:** Click to turn off **On:** Click to turn on **Off->On:** user define off time, after off time, it turns on automatically	Off time: 1000ms

3.9 Tools

3.9.1 PING Detection

Provide the function of router ping outer network.

Table 3-9-1 PING Detection Parameter Description

Parameters	Description	Default
Host	Address of the destination host of PING detection is required.	192.168.2.1
PING Count	Set the PING count	4 times
Packet Size	Set the packet size	32 bytes
Expert Options	Advanced parameter of PING is available.	No

3.9.2 Traceroute

Applied for network routing failures detection.

Table 3-9-2 Traceroute Parameter Description

Parameters	Description	Default
Host	Address of the destination host which to be detected is required.	192.168.2.1
Maximum Hops	Set the maximum hops for traceroute	20
Timeout	Set the timeout of traceroute	3 seconds
Protocol	Optional: ICMP/UDP	UDP
Expert Options	Advanced parameter for traceroute is available.	No

3.9.3 Link Speed Test

Determine link speed using uploading and downloading files.

3.10 Configuration Wizard

Simplified normal configuration allows the rapid, simple and basic configuration of router, but cannot display the results of configuration which can be checked in corresponding configuration details previously upon the accomplishment.

3.10.1 New LAN

Table 3-10-1 New LAN Parameters Description

Parameters	Description	Default
Port	Select new LAN port	fastethernet 0/2
Host IP	Host IP address can be configured all altered according to user definition	No
Subnet Mask	User define subnet mask (generates automatically)	255.255.255.0
DHCP Service	Enable/Disable	Disabled
Start Address	Set a starting IP address of dynamic allocation	No
End Address	Set an ending IP address of dynamic allocation	No
Validity Period	Set IP time limits of dynamic allocation	1440

3.10.2 New WAN

Table 3-10-2 New WAN Parameters Description

Parameters	Description	Default
Port	Select new WAN port	fastethernet 0/1
Type	Configuration type of WAN port IP Address	Static IP
Host IP	Host IP address can be configured all altered according to user definition	No
Subnet Mask	User define subnet mask (generates automatically)	255.255.255.0
Gateway	Configure gateway IP address	No
Network Address Switch	Click to enable, can switch IP address of private network into public ones	Disabled

3.10.3 New Dial

Table 3-10-3 New Dial Parameters Description

Parameters	Description	Default
APN	Select new WAN port	3gnet
Dialing Number	Relevant dialing parameters provided be mobile operators (select according to local operator)	*99***1#
Username	Relevant dialing parameters provided be mobile operators (select according to local operator)	gprs
Password	Relevant dialing parameters provided be mobile operators (select according to local operator)	••••
Network Address Switch	Click to enable, can switch IP address of private network into public ones	Disabled

3.10.4New IPSec Tunnel

Table 3-10-4 New IPSec Parameters Description

Parameters	Description	Default
Basic Parameters		
Tunnel Serial Number	Set a serial number for new tunnel	1
Port Name	Select port name	cellular 1
Peer Address	Set VPN peer IP	No
Negotiation Mode	Main mode or aggressive mode selectable.(Main mode is chosen normally)	Main Mode
Local Subnet Address	Set IPSec local protection subnet	No
Local Subnet Mask	Set IPSec local protection subnet mask	255.255.255.0
Peer Subnet Address	Set IPSec peer protection subnet	No
Peer Subnet Mask	Set IPSec peer protection subnet mask	255.255.255.0
Phase I Parameters		
IKE Strategy	3DES-MD5-DH1 or 3DES-MD5-DH2	3DES-MD5-DH2
IKE Life Cycle	Set IKE life cycle	86400 seconds
Local Identifier Type	FQDN, USERFQDN, IP address	IP address
Local Identifier	FQDN and USER FQDN only. Fill in the identifier according to the identifier type (USER FQDN is standard email format)	No
Peer Identifier Type	FQDN, USER FQDN, IP address	IP address
Peer Identifier	FQDN and USER FQDN only. Fill in the identifier according to the identifier type (USER FQDN is standard email format)	No
Authentication Type	Shared key, digital certificate	Shared key
Password	This item is displayed if the authentication type is shared password. Set the IPSec VPN negotiation password	No
Phase II Parameters		
IPSec Strategy	3DES-MD5-96 or 3DES –SHA1-96	3DES-MD5-96
IPSec Life Cycle	Set IPSec life cycle	3600 seconds

Attention

Inbound and out bound protocols shall be set for each tunnel connection. In the case of setting filter for one-way connections, the protocols will not be applied.

3.10.5 New Port Mapping

Table 3-10-5 New Port Mapping Parameters Description

Parameters	Description	Default
Protocol	TCP or UDP	TCP
Outside Port	Outer net connection port selected by user	Cellular
Service Port	TCP or UDP data transmission port	No
Internal Address	The device address of mapping subject	No
Internal Port	TCP or UDP port of mapping subject	No
Description	User define	No

4 Typical Application Configuration

4.1 DDNS Application Example

Example: an IR900 is connected with IP of public network via dial mode, set DDNS to address map the dynamic IP of users on a fixed domain name service.

Configuration procedures of router are as follows:

First: Configure the parameters of dynamic domain name of equipment. Refer to Fig. 4-1-1 for configuration in case of tailored domain name parameters and refer to Fig. 4-1-2 for configuration in case of general domain name parameters.

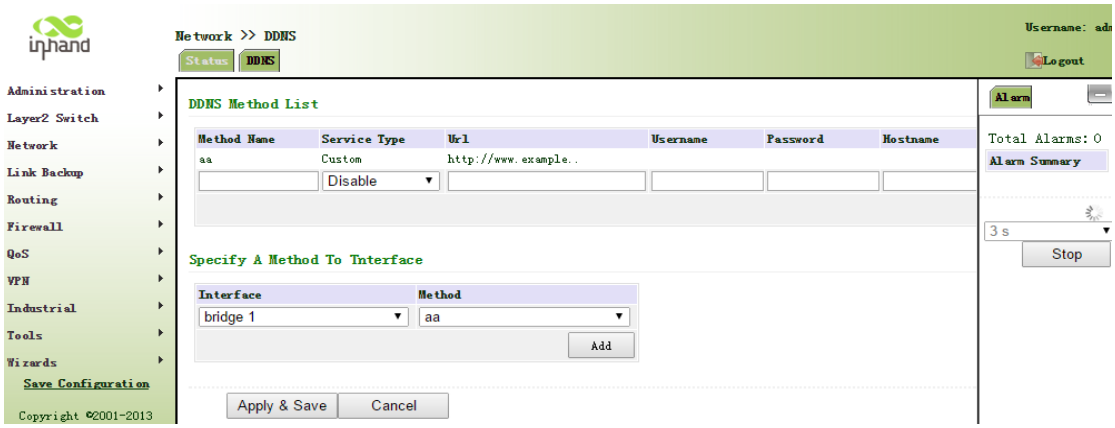


Fig. 4-1-1

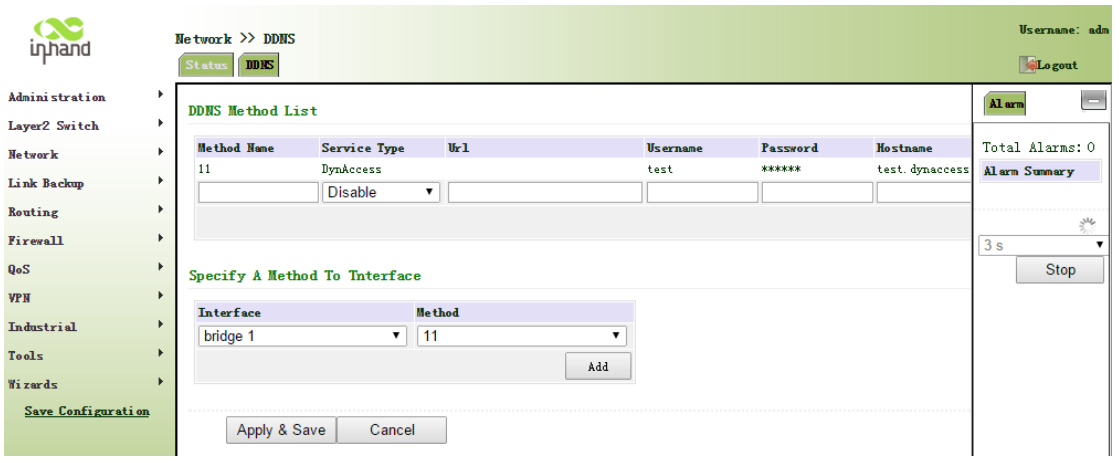


Fig. 4-1-2

Second: Wait for minutes when dynamic domain names are configured and application is in storage, then ping the domain name to confirm the successful configuration of dynamic domain name, as shown in Fig. 4-1-3:


命令提示符
正在 Ping walker1204.ddns.net [211.136.69.179] 具有 32 字节的数据:
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
来自 211.136.69.179 的回复: 字节=32 时间<1ms TTL=64
211.136.69.179 的 Ping 统计信息:
数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
最短 = 0ms, 最长 = 0ms, 平均 = 0ms

Fig. 4-1-3

4.2 Device Management Application Example

Applications: add equipment to Device Management

Configuration procedures of router are as follows:

Step 1: Configure parameters of Device Management, in particular, server: c2.inhandnetworks.com, port: 20003, as shown in Fig. 4-2-1.

Fig. 4-2-1

Step 2: Log in device management (http://c2.inhandnetworks.com) and add the equipment.

4.3 Restore Factory Default Settings

4.3.1 Via Web Interface

Log in WEB page, click “Administration>>Configuration Management” in the navigation panel and enter “Configuration Management”. Click <Restore Factory Default Settings>, reboot system after reset is confirm and complete the process.

4.3.2 Via RESET Button

Restore to factory default via front panel RESET button:

Step 1. Locate the RESET button on the device;

Step 2. Turn on the device’s power; within 10 seconds, press and hold RESET button;

Step 3. When ERR LED is on, release the RESET button;

Step 4. Within a few seconds, ERR LED should go off; then press and hold the RESET button again;

Step 5. When the ERR LED blinks, release the RESET button; If the ERR LED goes off, that means InRouter900 is now restoring to factory default settings;

4.4 Import/Export Configuration

Log in WEB page, click “Administration>>Configuration Management” in the navigation panel and enter “Configuration Management”.

- Click <Browse>to select configuration files, then click <import> button. Reboot the system after configuration files are imported to gain effect.

- Click <backup running-config > to export and save currently applied configuration parameter files. The format of exported files is .cnf, default file name is running-config.cnf.

- Click <backup running-config > to export and save configuration parameter files in equipment staring process. The format of exported files is .cnf, default file name is startup-config.cnf.

4.5 Logs and Diagnostics

Log in WEB page, click “Administration>>Configuration Management” in the navigation panel and enter “System Logs”. Click respective buttons to complete downloads of logs and diagnostics.

4.6Network Mode

4.6.1 Cellular

First step: click the “Network>> Cellular” in the navigation panel and enter the “Cellular” page, as shown below.

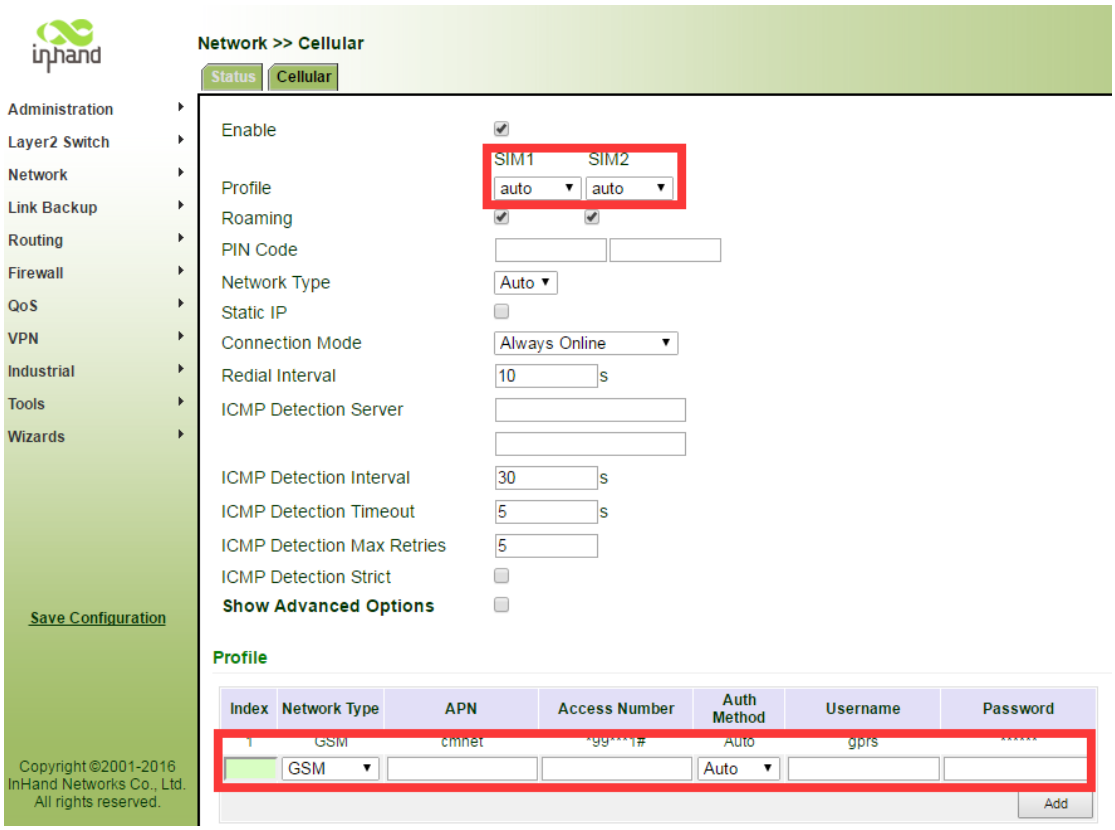


Fig. 4-6-1

4.6.2 ADSL Dialup

Step 1: disable cellular. Click “Network>>Cellular” menu in navigation, uncheck Enable, as is shown in Fig. 4-6-2.

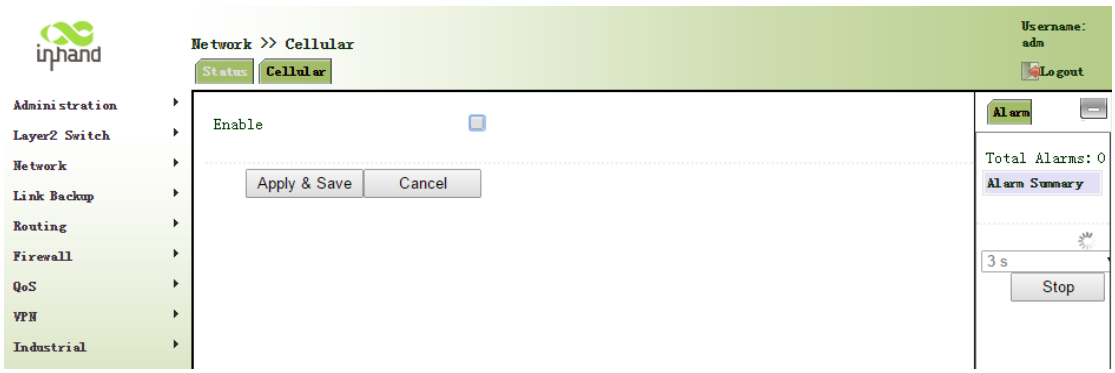


Fig. 4-6-2

Step 2: Establish new WAN, which is divided into three types. Click “Wizards >> New WAN” menu in navigation panel. Fig.4-6-3, Fig. 4-6-4 and Fig. 4-6-5 are examples of static IP type, ADSL dialup (PPPoE) type and DHCP type.

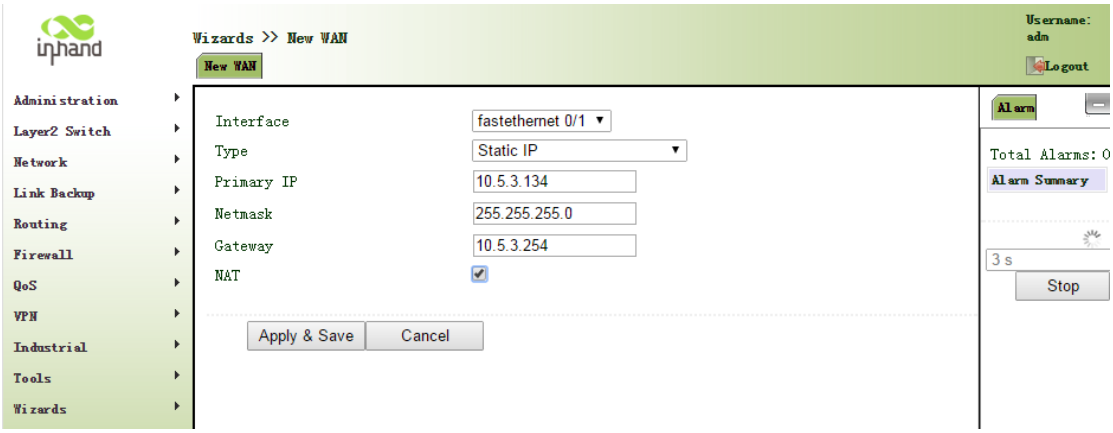


Fig. 4-6-3

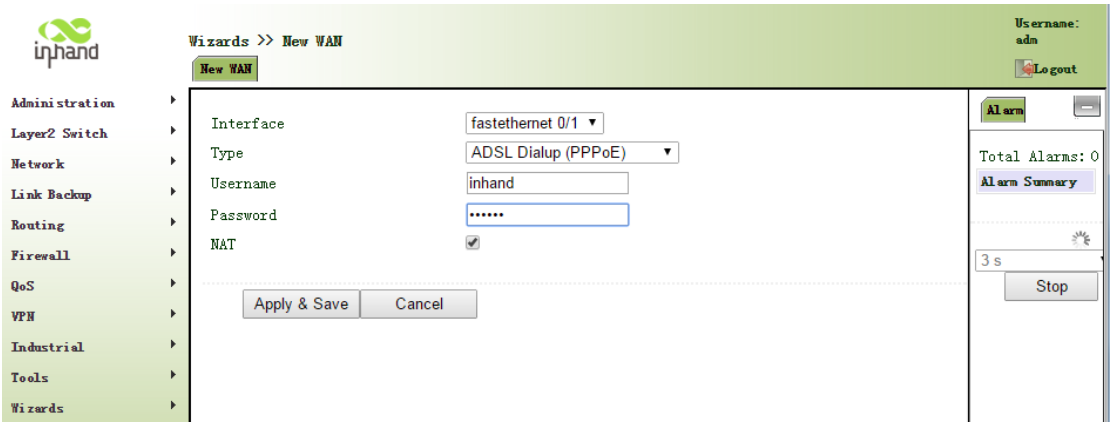


Fig. 4-6-4

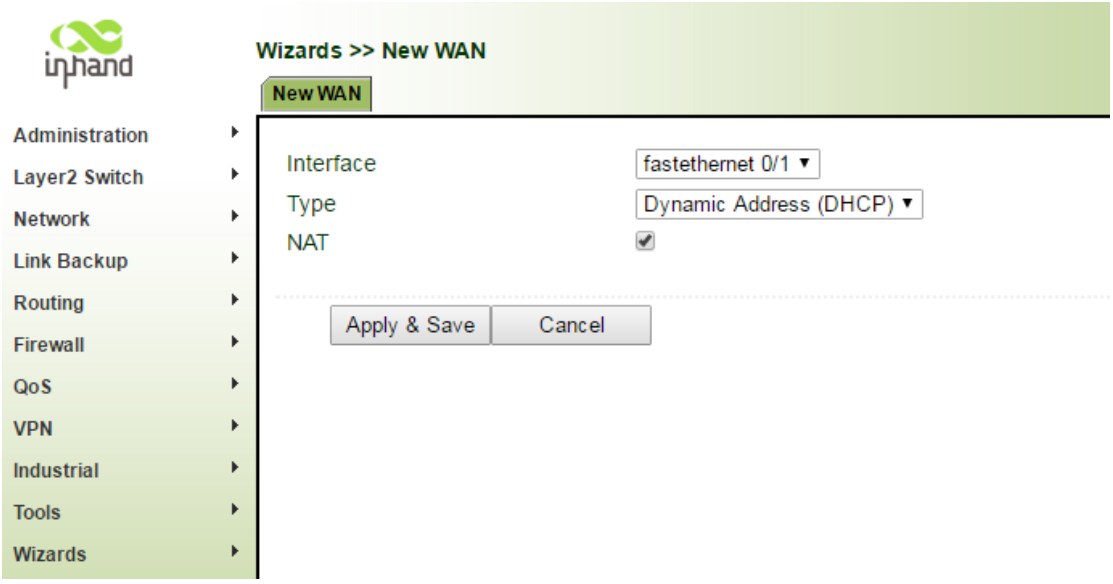


Fig. 4-6-5

4.7 New LAN

From navigation panel, select Wizards>>New LAN, as shown in Fig. 4-7-1.

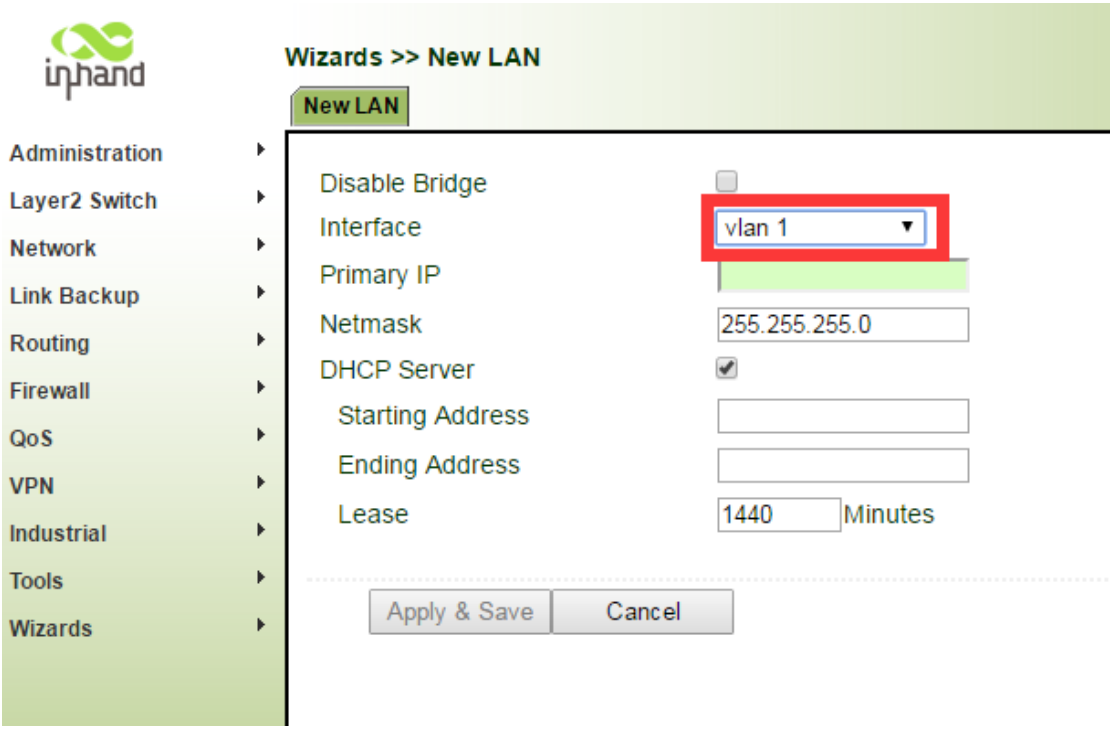


Fig. 4-7-1

4.8 VRRP Typical Configuration Example

1. Networking Demand

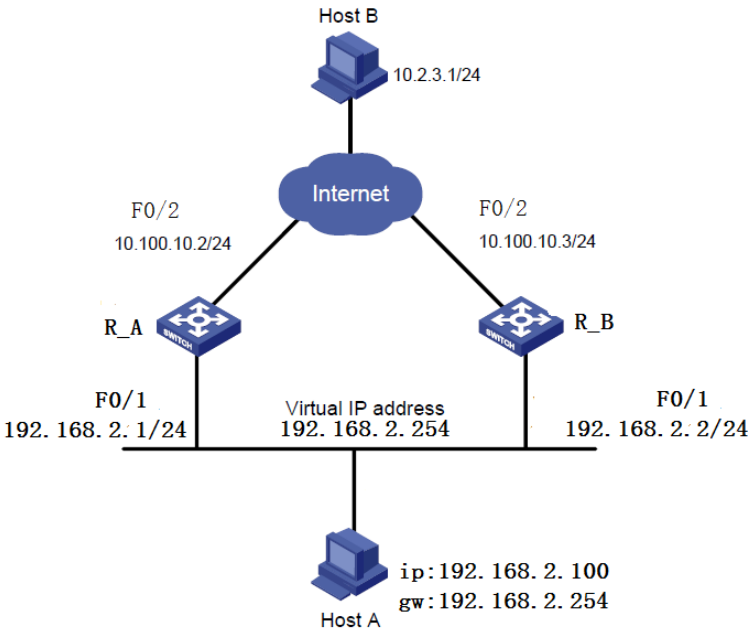
Mainframe A makes VRRP backup combined with router A and router B as its default gateway to visit the mainframe B on internet.

VRRP backup is composed of:

- Backup group ID 1
- IP address of backup group virtual router 192.168.2.254/24
- Interchanger A: Master
- Interchanger B: backup, interchanger preemptive allowable

Router	Ethernet interface connected with host A	IP address of interface connected with host A	Priority	Working mode
R_A	F0/1	192.168.2.1	110	preemptive
R_B	F0/1	192.168.2.2	100	preemptive

2. Networking Diagram



3. Configuration Procedures

(1) Configure router A

First: Configure F0/1

Click navigation panel “Link Backup>>VRRP”, enter “VRRP” interface, configure VRRP, as shown in Fig. 4-8-1.

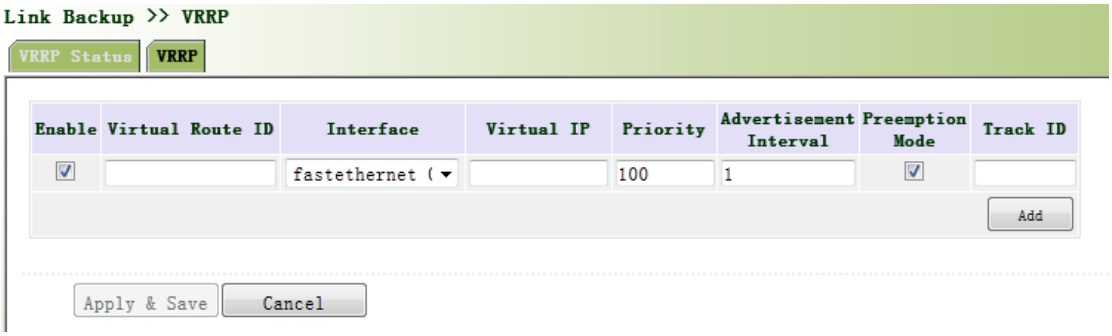


Fig. 4-8-1

Click navigation panel “Link Backup>>VRRP”, enter “VRRP” interface, examine VRRP, as shown in Fig. 4-8-2.

Fig. 4-8-2

First: Configure F0/2

Click navigation panel “Internet>>Ethernet Interface”, enter “Ethernet Interface 0/2”, configure Ethernet interface 0/2, as shown in Fig. 4-8-3.

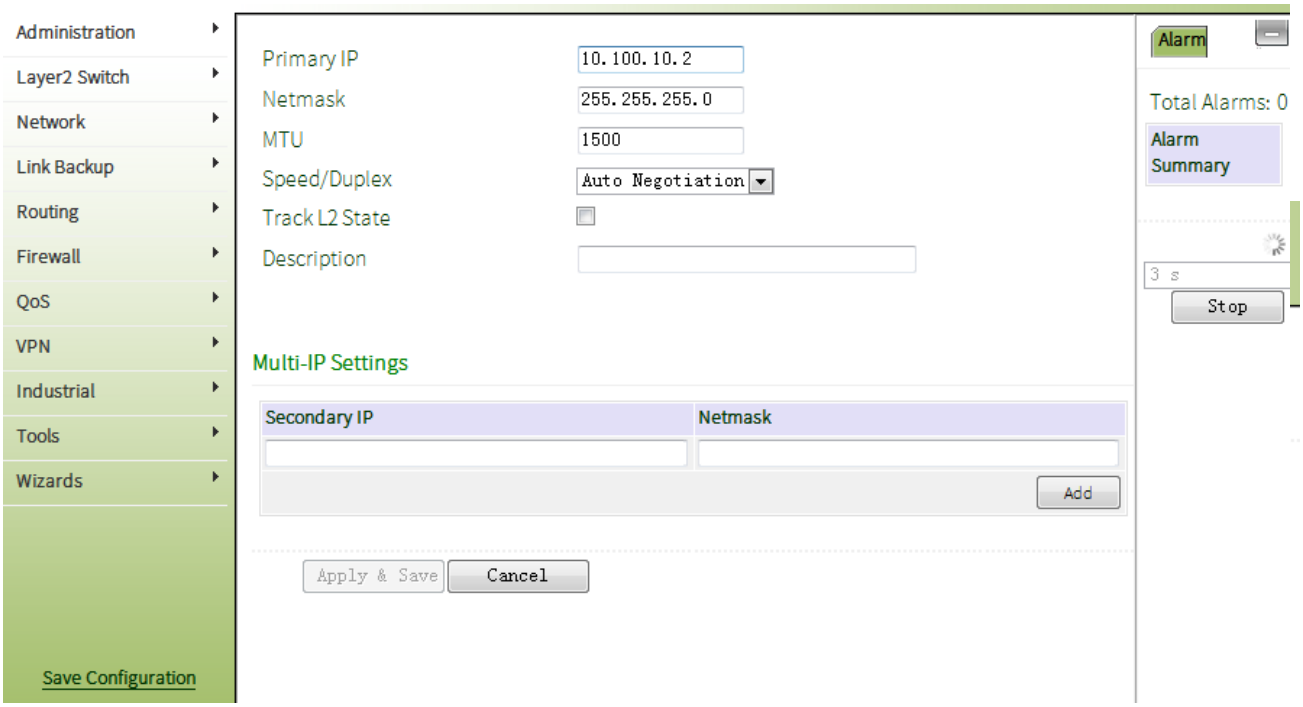


Fig. 4-8-3

(2) Configure router B

First: Configure F0/1

Click navigation panel “Link Backup>>VRRP”, enter “VRRP” interface, configure VRRP, as shown in Fig. 4-8-4.

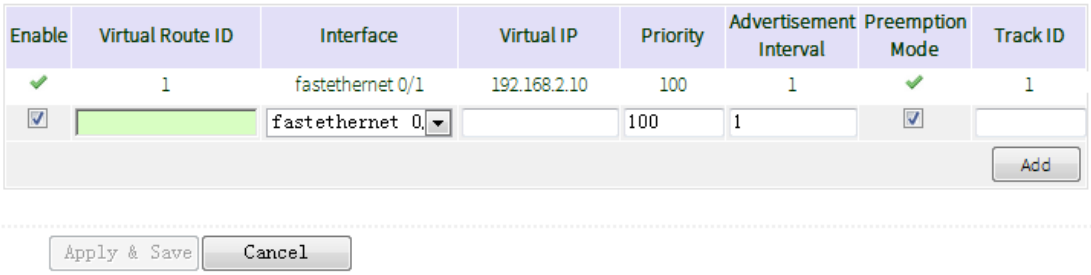


Fig. 4-8-4

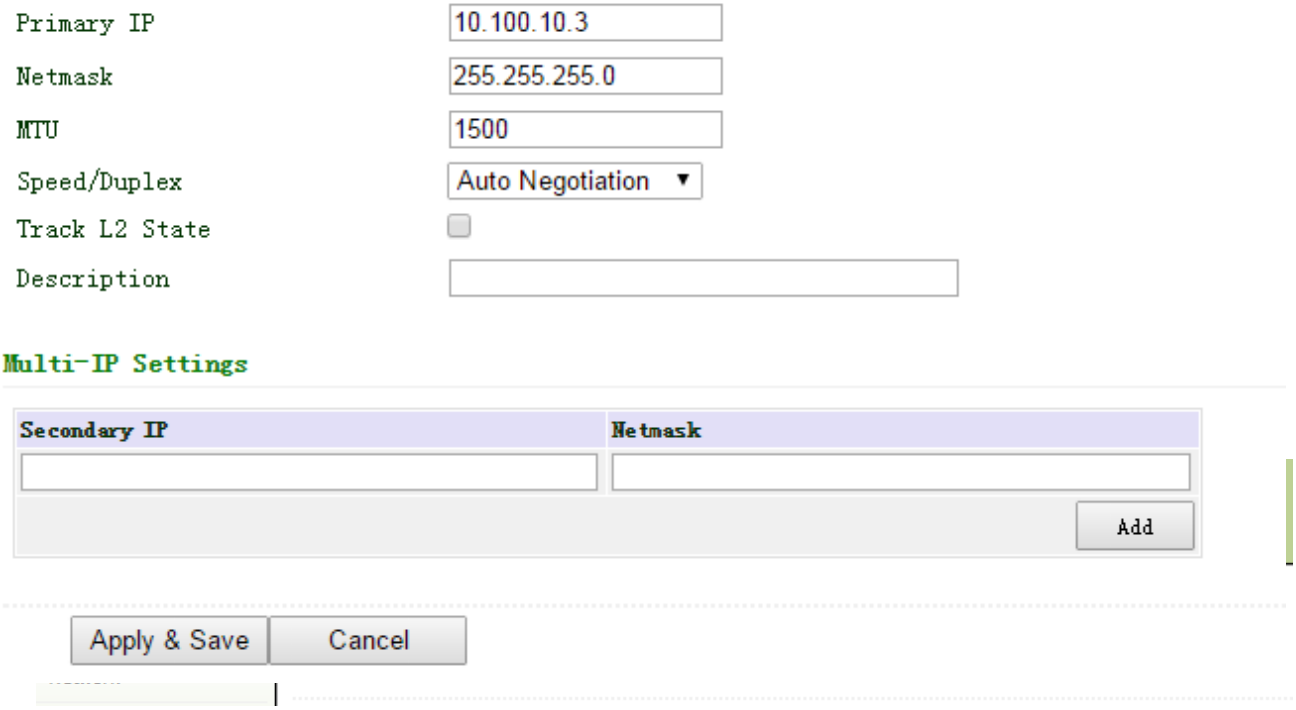
Click navigation panel “Link Backup>>VRRP”, enter “VRRP” interface, examine VRRP, as shown in Fig. 4-8-4:

Fig. 4-8-5

First: Configure F0/2

Click navigation panel “Internet>>Ethernet Interface”, enter “Ethernet Interface 0/2”, configure Ethernet interface 0/2, as shown in Fig. 4-8-6.

Fig. 4-8-6

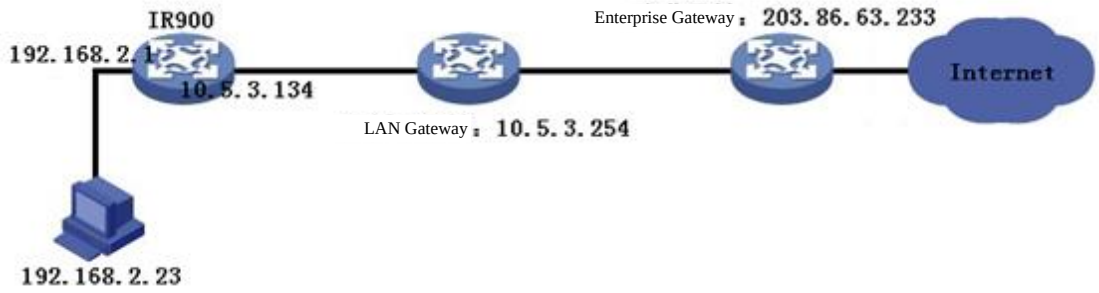


Default gateway of mainframe A is 192.168.2.254. Router A functions as the gateway under normal working conditions and router B will take over the function when router A closes down or breaks down. Setting preemption is to keep the function of router A as gateway under Master when router A returns to work.

4.9 Interface Backup Application Example

Example: a router IR900 is connected with PC at its fastethernet 0/2, fastethernet 0/1 of IR900 is connected with the internet via wired network, topological graph is shown in the following figure.

Establish interface backup in configuring router so that it can surf the internet through dial-up in malfunction of wired network.



Configuration procedures of router are as follows:

Step 1: Open "**Wizards>>New WAN**", configure parameters of wired network, as shown in Fig. 4-9-1.

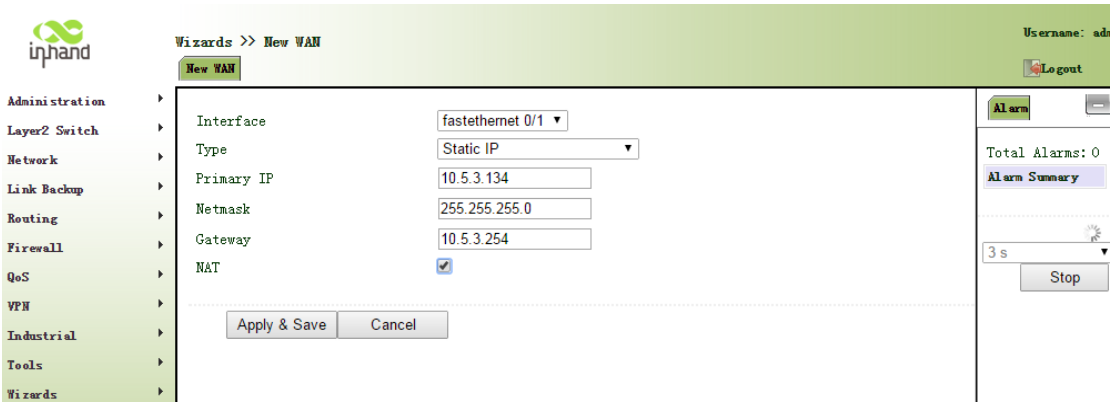


Fig. 4-9-1

Step 2: Open "DNS" in "Network>>DNS", configure corresponding parameters, as shown in Fig. 4-9-2. Examine PC to ensure its normal access to the internet after configuration.

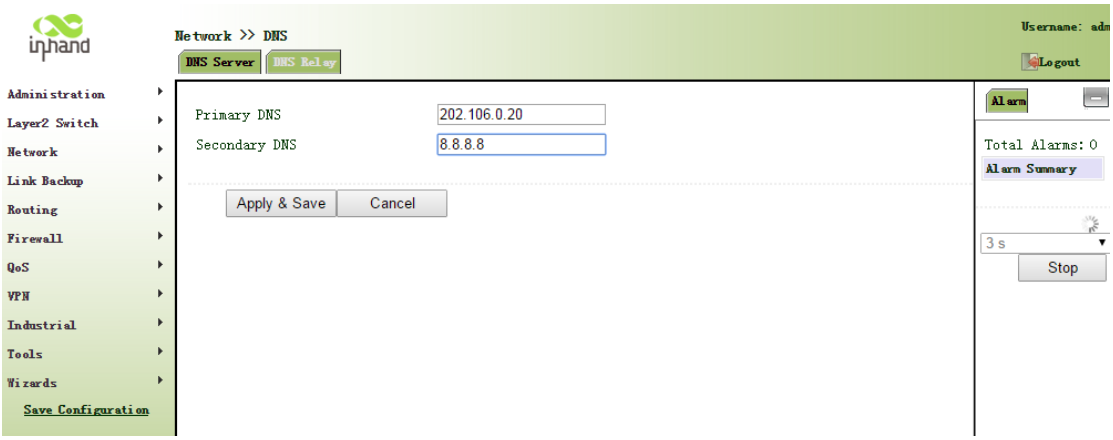


Fig. 4-9-2

Step 3: Open "Link Backup>>SLA", configure corresponding parameters, the IP address shall be the host address explored by ICMP in public network or private network, for instance, 203.86.63.233 is the gateway address of enterprise where PC is affiliated, as shown in Fig 4-9-3.

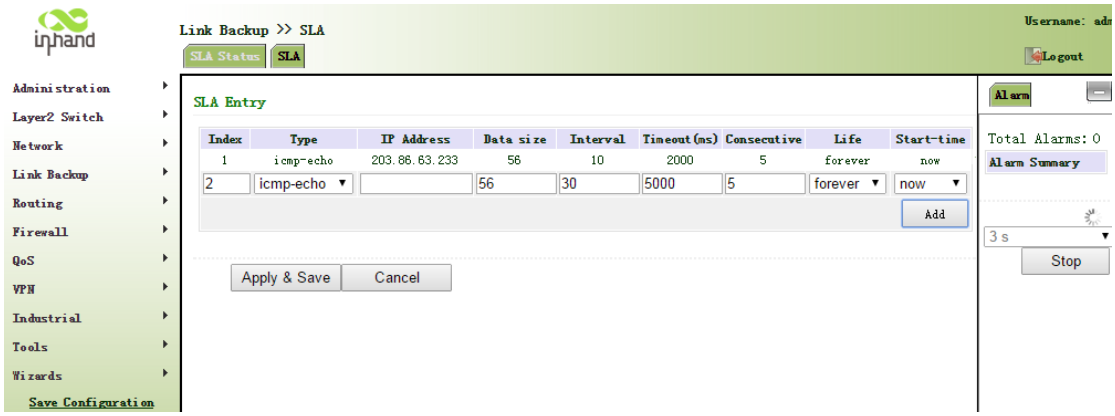


Fig. 4-9-3

Step 4: Open "**Link Backup>>Track**", configure corresponding parameters, as shown in Fig. 4-9-4.

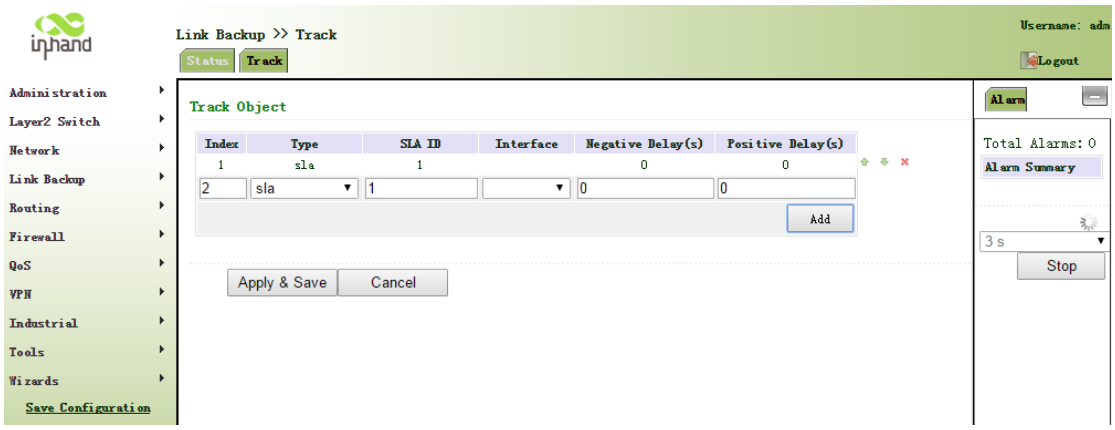


Fig. 4-9-4

Step 5: Open "Link Backup>>Interface Backup", configure corresponding parameters, as shown in Fig. 4-9-5.

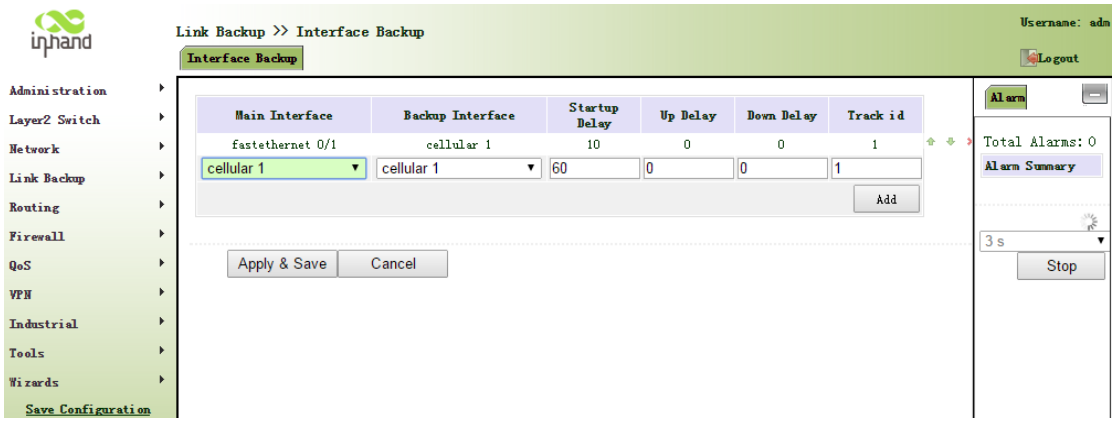


Fig. 4-9-5

Step 6: Open "Routing>>Static Routing", configure corresponding parameters and add 3 routes, 10.5.3.234 is the gateway of LAN where PC is affiliated, as shown in Fig.4-9-6. The distance parameter indicates the priority, the smaller the numerical the more the priorities.

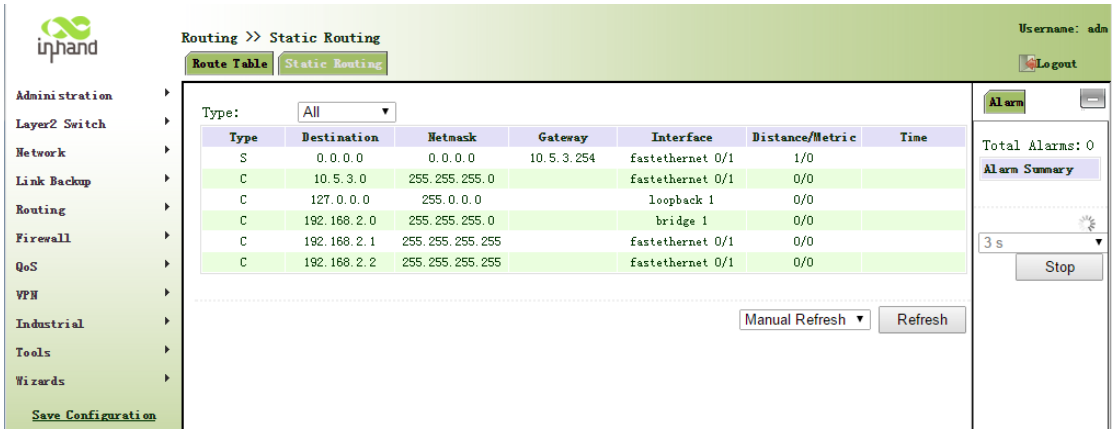
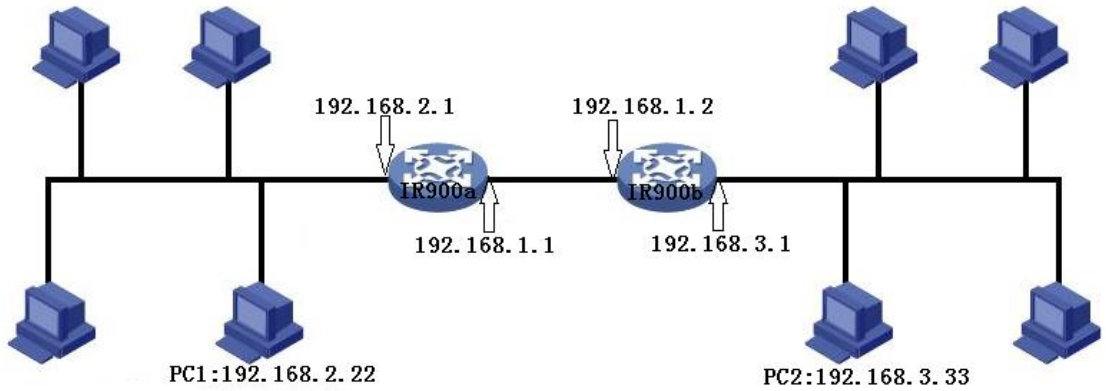


Fig. 4-9-6

Step 7: Pull up cable to make malfunction of wired internet, then router can have access to internet via dial-up through cellular; cable internet can be applied once again when cable is set again.

4.10 Static Routing Application Example

Example: Establish static routing between two LAN for their intercommunication; refer to the following figure for topological graph.



Configuration procedures of router are as follows:

Step 1: Configure IR900a, the parameter configuration is shown in Fig.4-10-1.

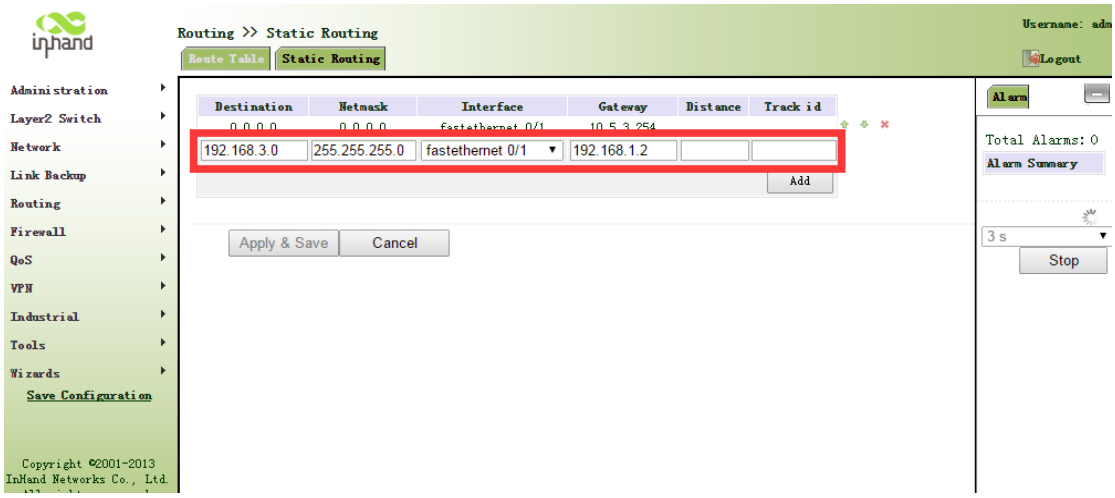


Fig. 4-10-1

Step 1: Configure IR900b, the parameter configuration is shown in Fig.4-10-2.

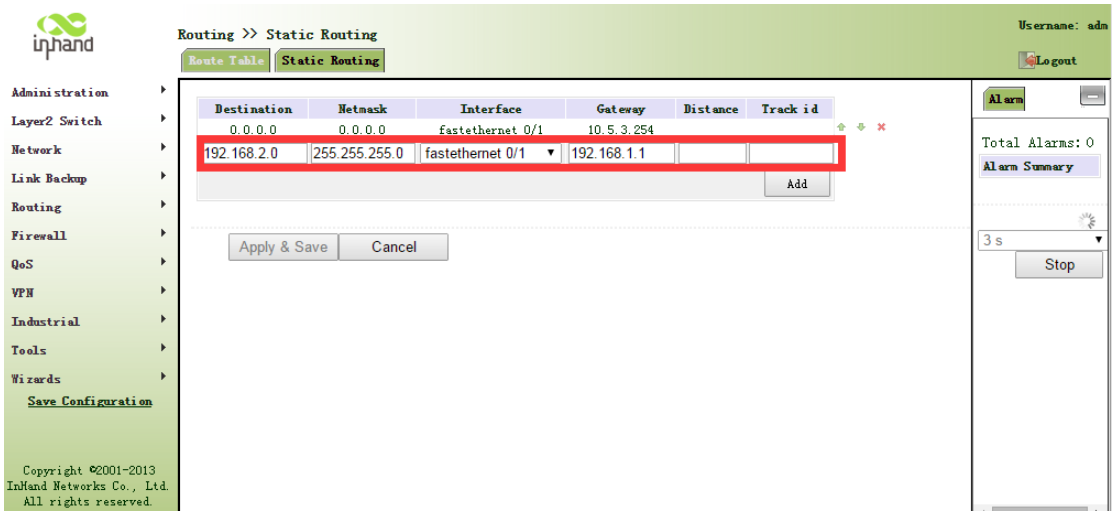
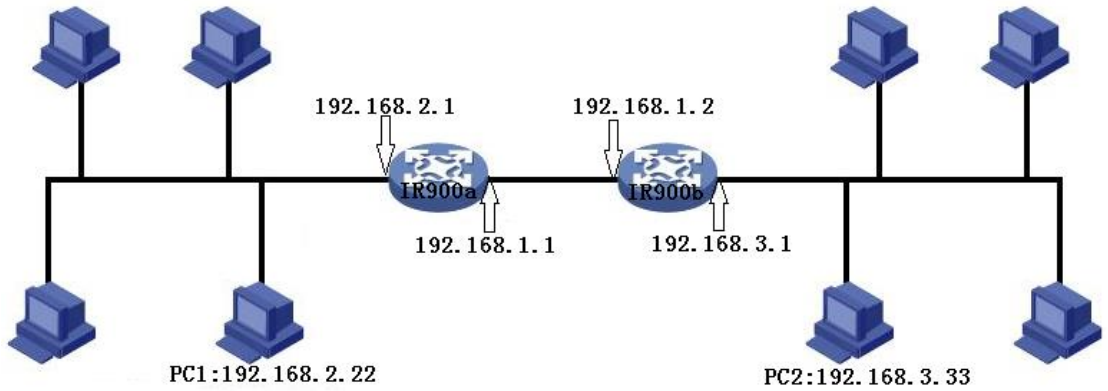


Fig. 4-10-2

Step 3: PC1 and PC2 can be intercommunicated, adding static routing is successful.

4.11 Dynamic Routing Application Example

Example: Establish dynamic routing between two LANs for intercommunication; refer to the following figure for the topological graph.



I) RIP

Configuration procedures of router are as follows:

Step 1: Configure IR900a, the parameter configuration is shown in Fig.4-11-1.

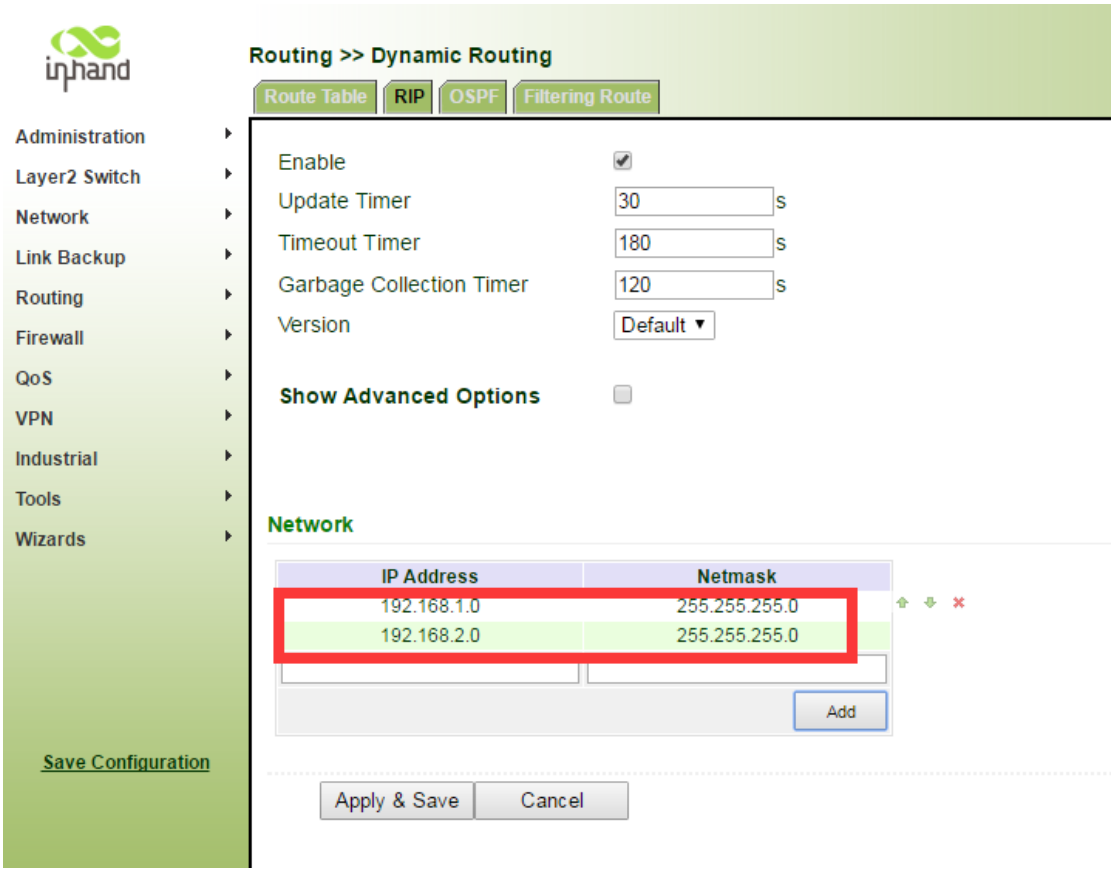


Fig. 4-11-1

Step 1: Configure IR900b, the parameter configuration is shown in Fig.4-11-2.

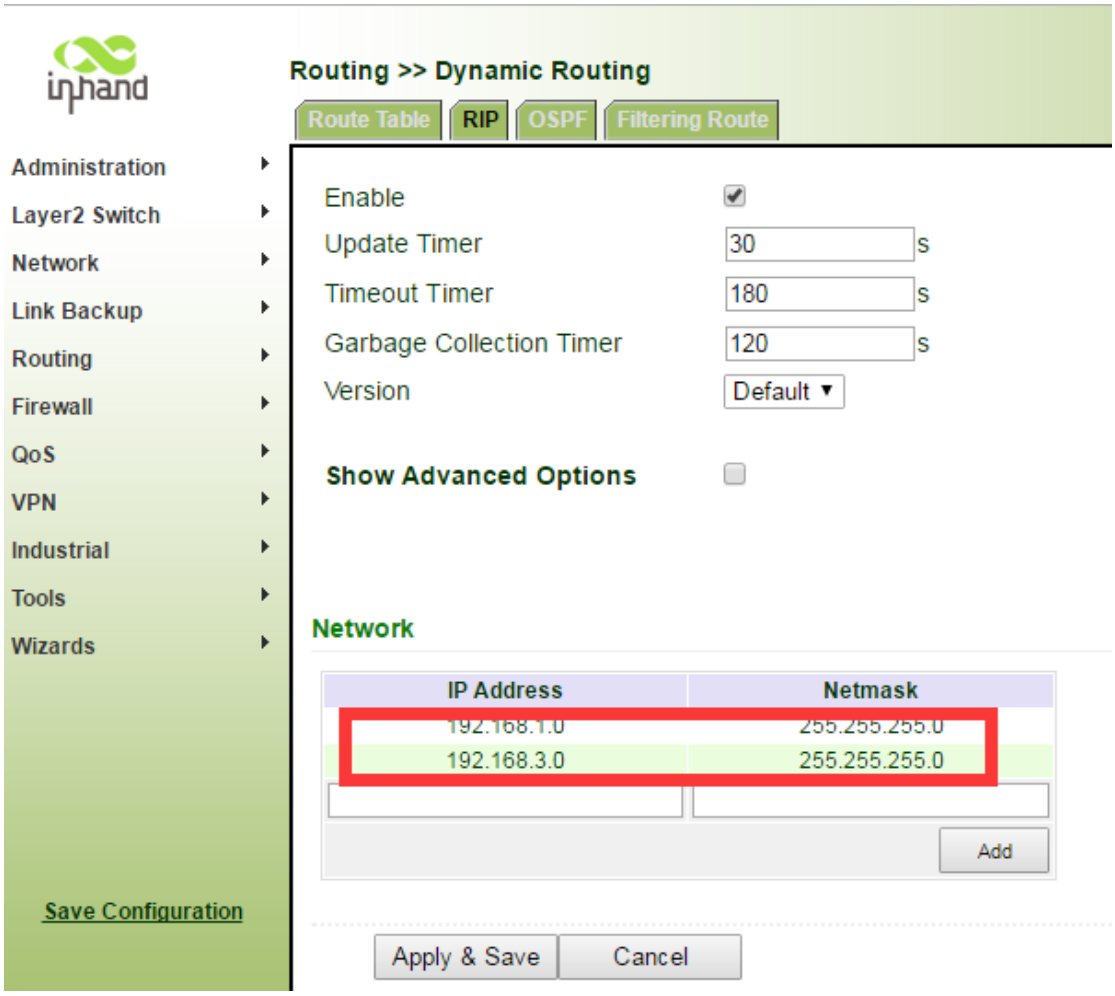


Fig. 4-11-2

Step 3: PC1 and PC2 can be intercommunicated, adding static routing is successful.

II) OSPF

Configuration procedures of router are as follows:

Step 1: Configure IR900a, the parameter configuration is shown in Fig.4-11-3.

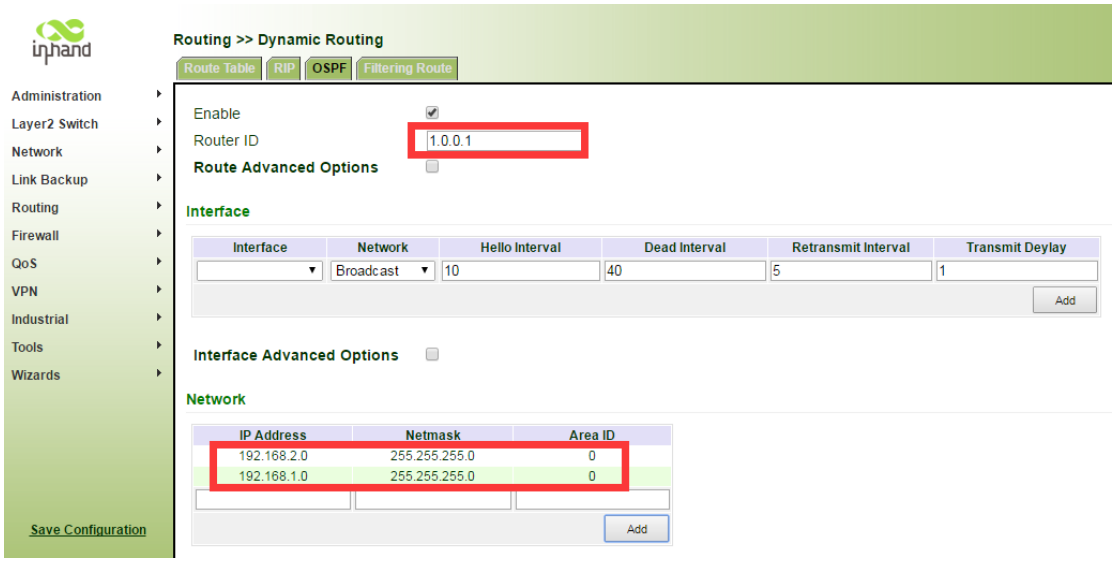


Fig. 4-11-3

Step 1: Configure IR900b, the parameter configuration is shown in Fig.4-11-4.

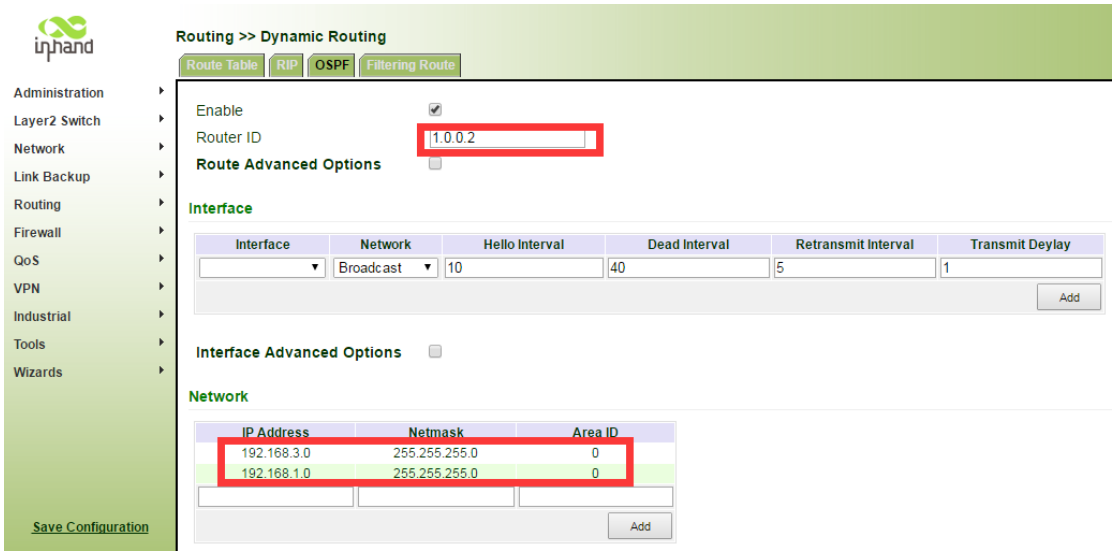
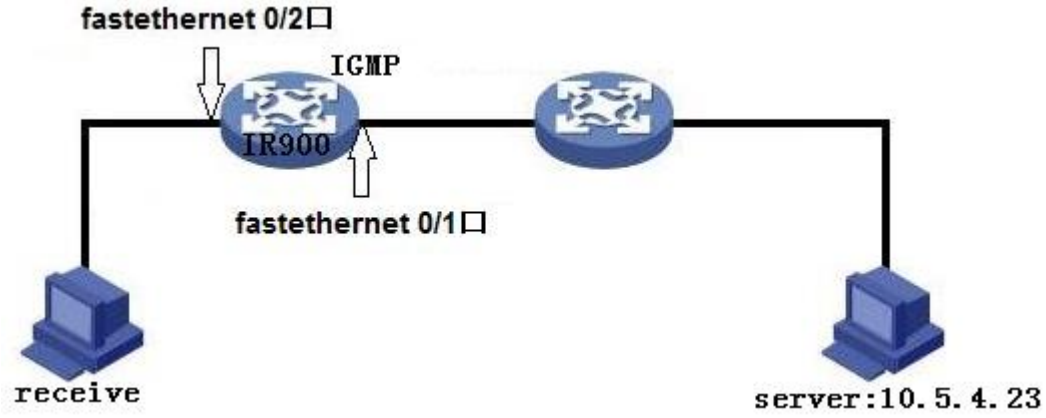


Fig. 4-11-4

Step 3: PC1 and PC2 can be intercommunicated, adding static routing is successful.

4.12 Multicast Routing Application Example

Example: Set router to receive the multicast data from network and refer to the following figure for topological graph.



Configuration procedures of router are as follows:

Step 1: Start multicast routing and configure parameters for multicast routing, as shown in Fig. 4-12-1.

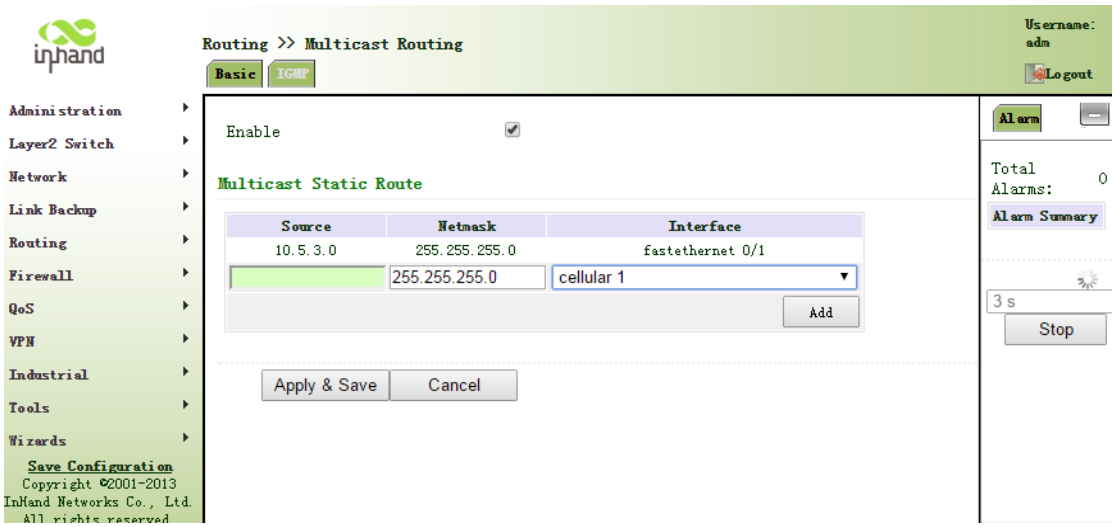


Fig. 4-12-1

Step 2: Configure IGMP parameter, as shown in Fig. 4-12-2.

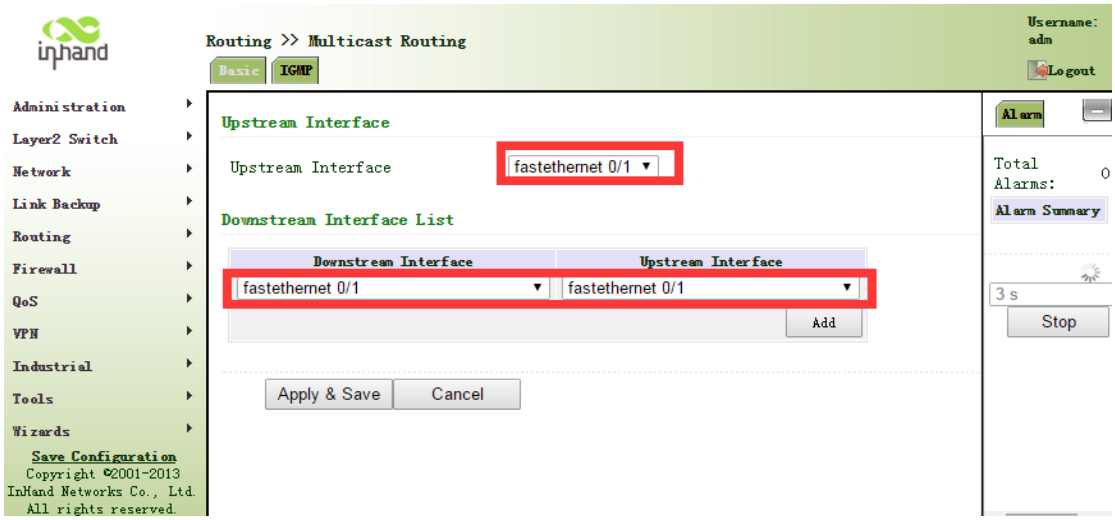

Routing >> Multicast Routing
Basic
IGMP
Username: adm
Logout
Administration
Layer2 Switch
Network
Link Backup
Routing
Firewall
QoS
VPN
Industrial
Tools
Wizards
Save Configuration
Copyright ©2001-2013 InHand Networks Co., Ltd. All rights reserved.
Upstream Interface
Upstream Interface
fastethernet 0/1
Downstream Interface List
Downstream Interface
Upstream Interface
fastethernet 0/1
fastethernet 0/1
Add
Apply & Save
Cancel
Alarm
Total Alarms:
0
Alarm Summary
3 s
Stop

Fig. 4-12-2

4.13 Access Control Application Example

Example: a router IR900 is connected with intranet at its FE 0/1, the net section of intranet is 192.168.1.2/254; FE 0/2 is connected with intranet with the net section of intranet 192.168.1.2/254. Configure router for no access to the internet with FE 0/2 and access into Internet can be realized when FE 0/1 is connected with intranet.

Configuration procedures of router are as follows:

Step 1: Open “ACL”, click <add> for access control list and configure parameters as shown in Fig. 4-13-1.

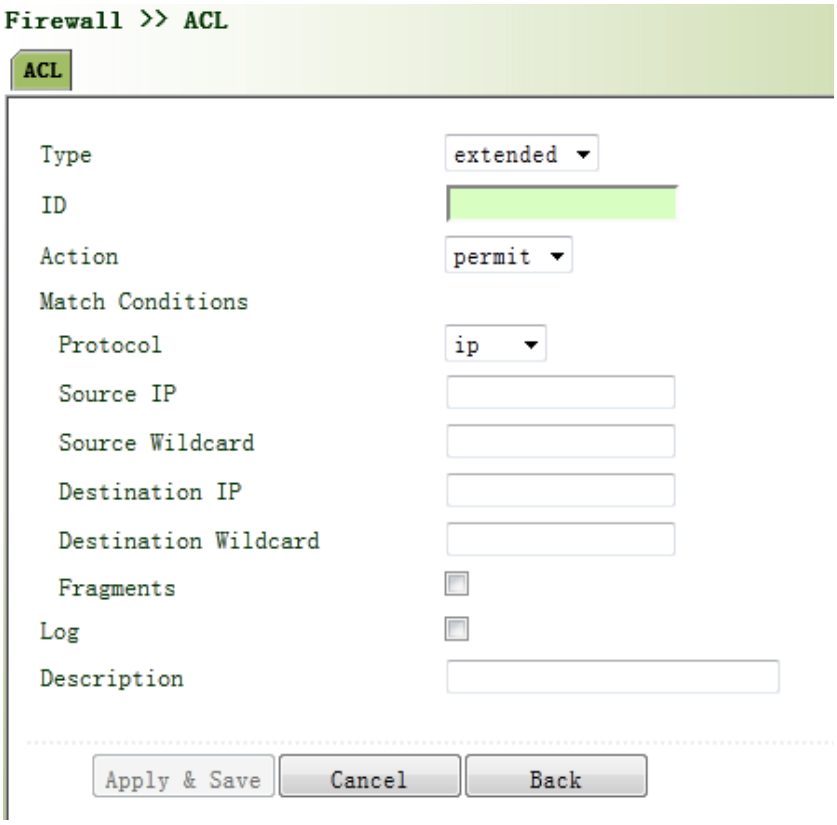


Fig. 4-13-1

Step 2: Click <**Apply and Store**> when parameter configuration is done, then ID “**101**” can be seen on the newly established access control list, as is shown in Fig. 4-13-2.

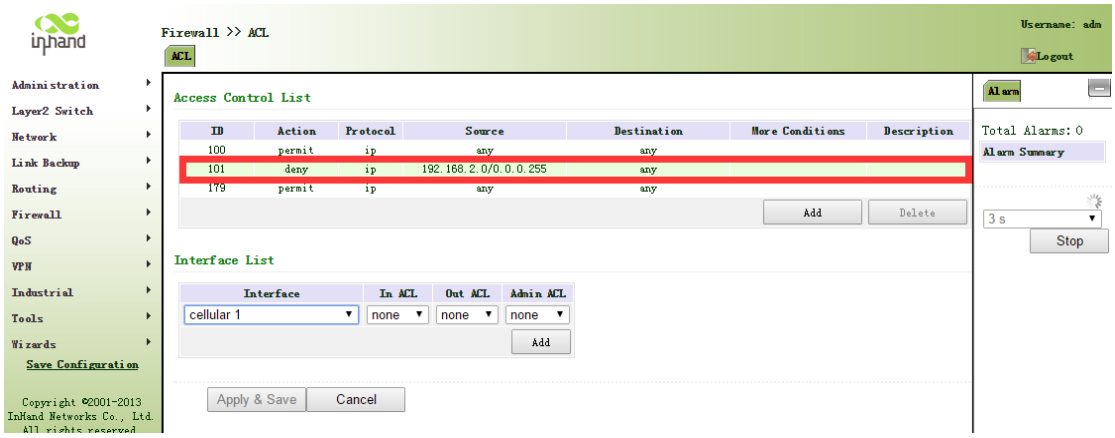


Fig. 4-13-2

Step 3: Select “cellular1” in “Port Name” of “Network Port List”, select “101” in “Out Rules”, click <add> and store, as shown in Fig. 4-13-3.

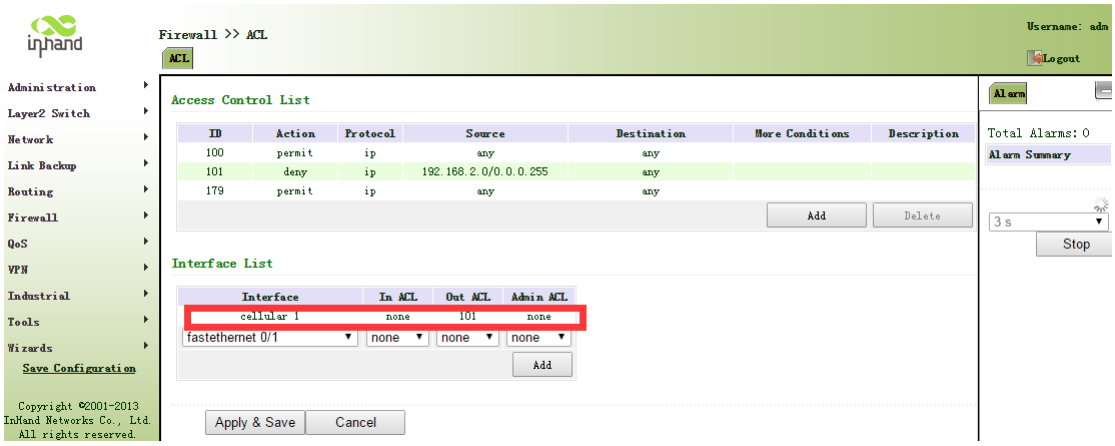


Fig. 4-13-3

4.14 NAT Application Example

Example: a router IR900 has access to internet via dial-up; FE 0/2 is connected with a server whose IP address is 192.168.2.23. Configure router to make public network have access to the server.

(Port mapping way) configuration of router is shown in Fig. 4-14-1:

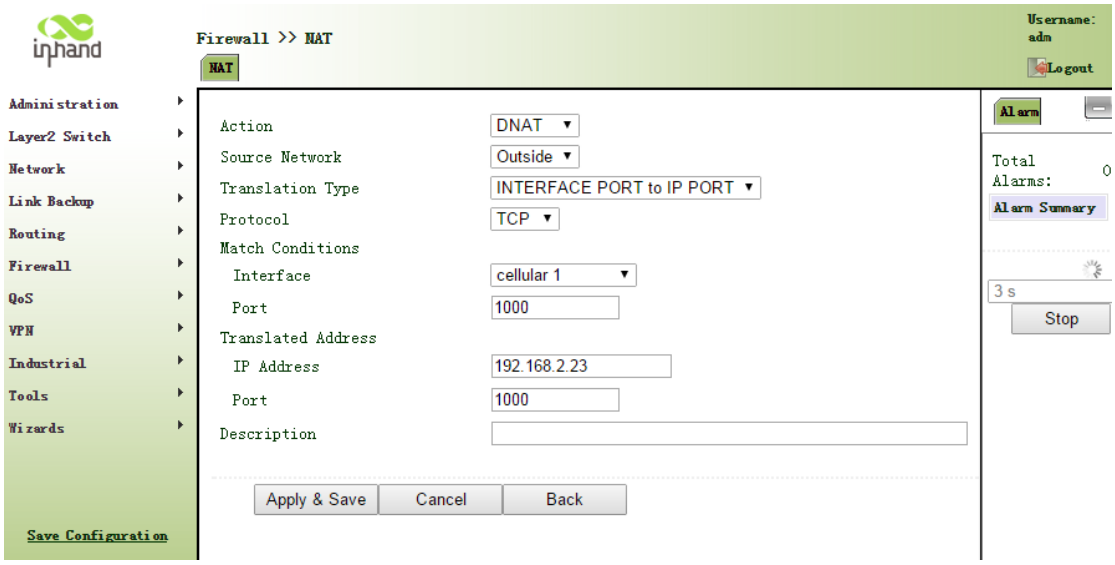


Fig. 4-14-1

(DMZ way) configuration of router is shown in Fig. 4-14-2:

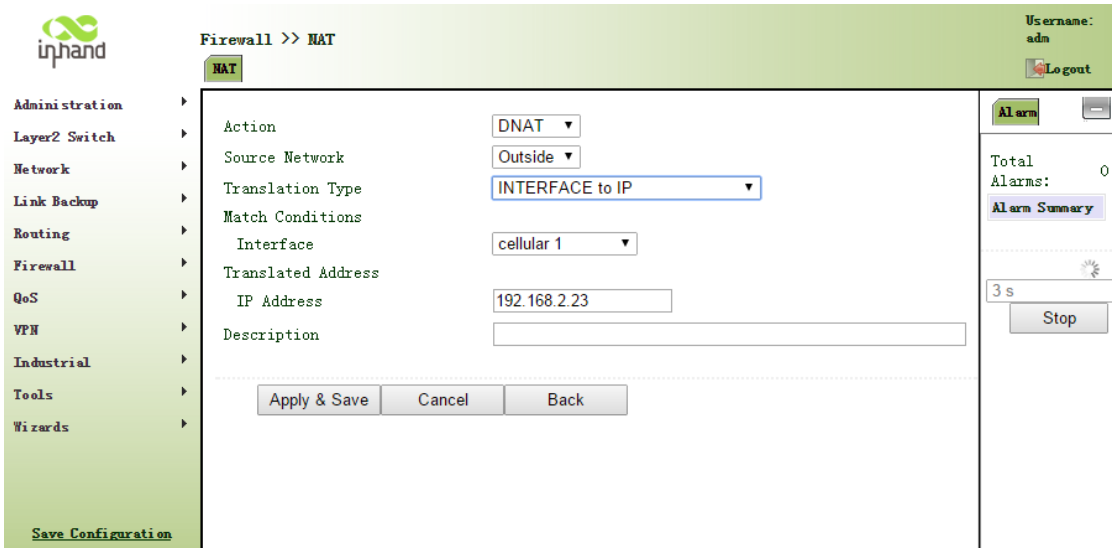


Fig. 4-14-2

4.15 QoS Application Example

Example: Set router to distribute local preference to different downloading channels.

Configuration procedures of router are as follows:

Step 1: Add “type” to describe downloading flow, for example, the IP address of local mainframe appointed shall be the destination.

Step 2: Add “strategy” to guarantee the bandwidth and local preference of each “type”.

Step 3: Select the out-port in strategy application and distribute an out maximum bandwidth for port. As shown in Fig. 4-15-1.

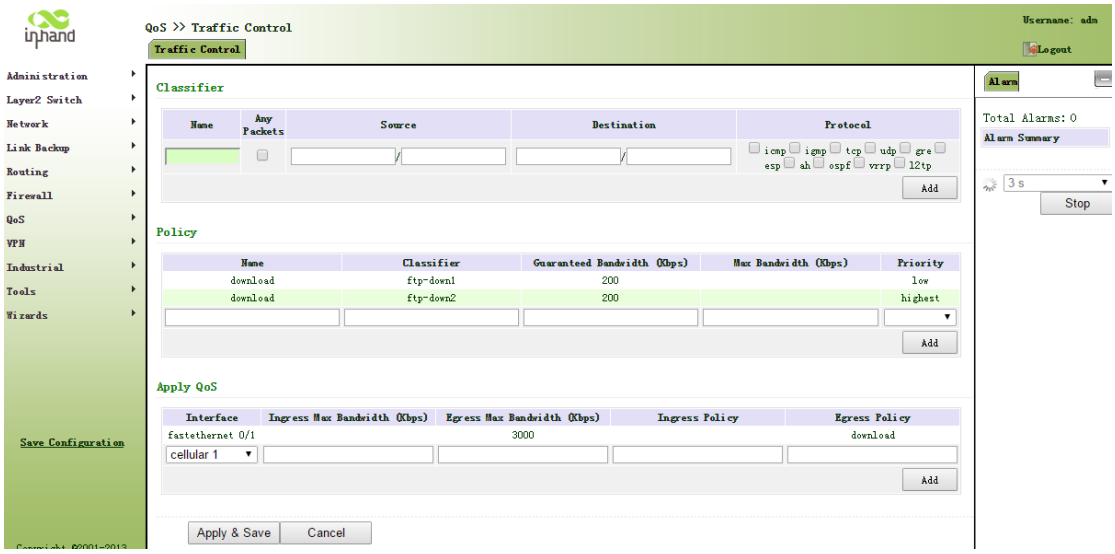
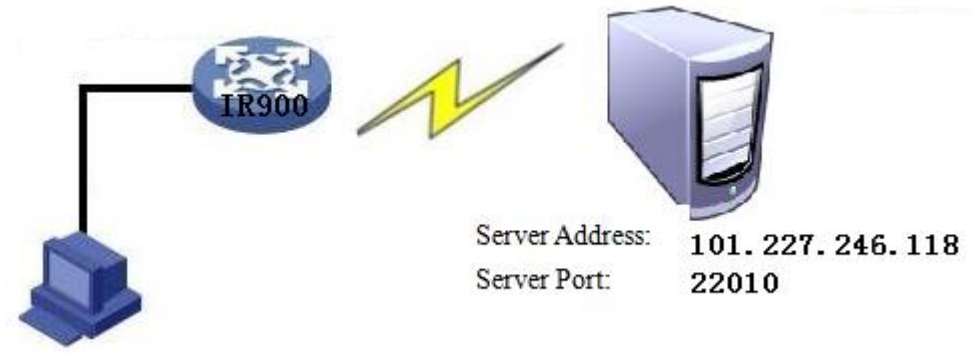


Fig. 4-15-1

4.16 DTU Application Example

Example: An IR900 shall be functioned with DTU for the intercommunication between it and server, and refer to the following figure for topological graph.



Configuration procedures of router are as follows:

Step 1: Configure DTU serial port parameter. The serial port parameter shall be kept in consistency with the serial port parameter of end equipment, as shown in Fig. 4-16-1.

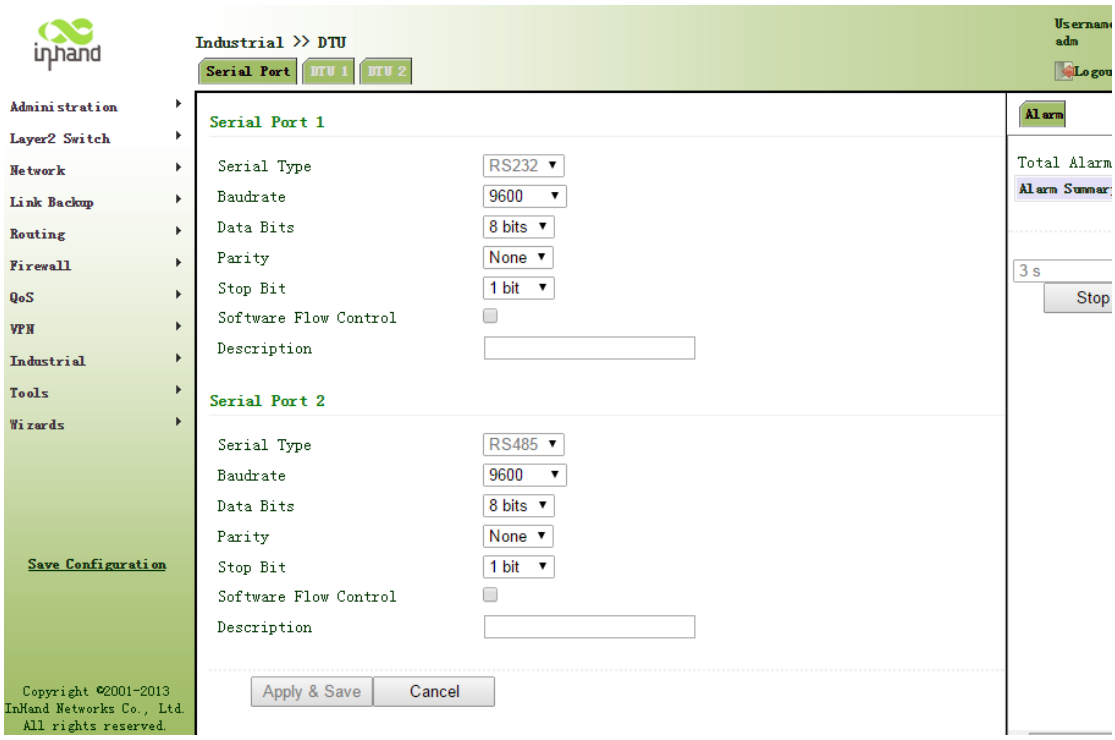


Fig. 4-16-1

Step 2: Configure DTU function parameters, as shown in Fig. 4-16-2.

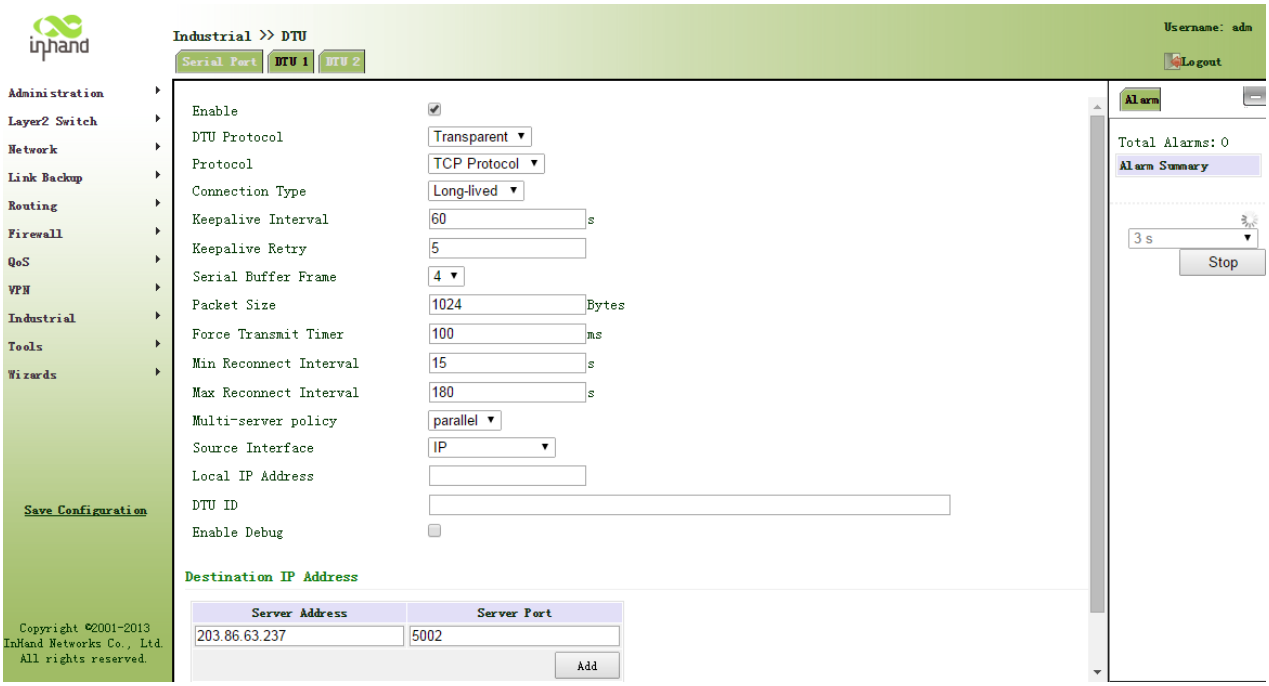


Fig. 4-16-2

Step 3: Establish and start server, IR900 is connected with server via DTU function and will automatically send DTU marks (no sending in case of the blank parameter of DTU mark) to server, as shown in Fig. 4-16-3.

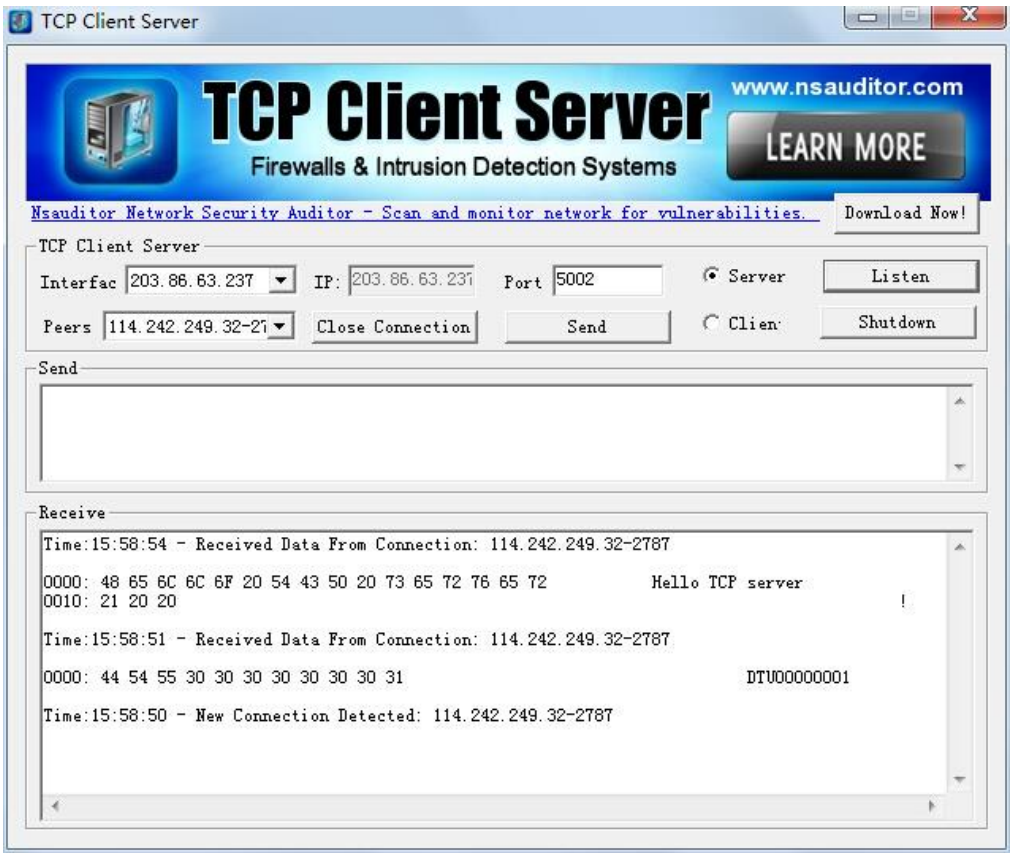


Fig. 4-16-3

Step 4: Via DTU function, the PC connected with IR900 and the server can send data to each other, as shown in Fig. 4-16-5.

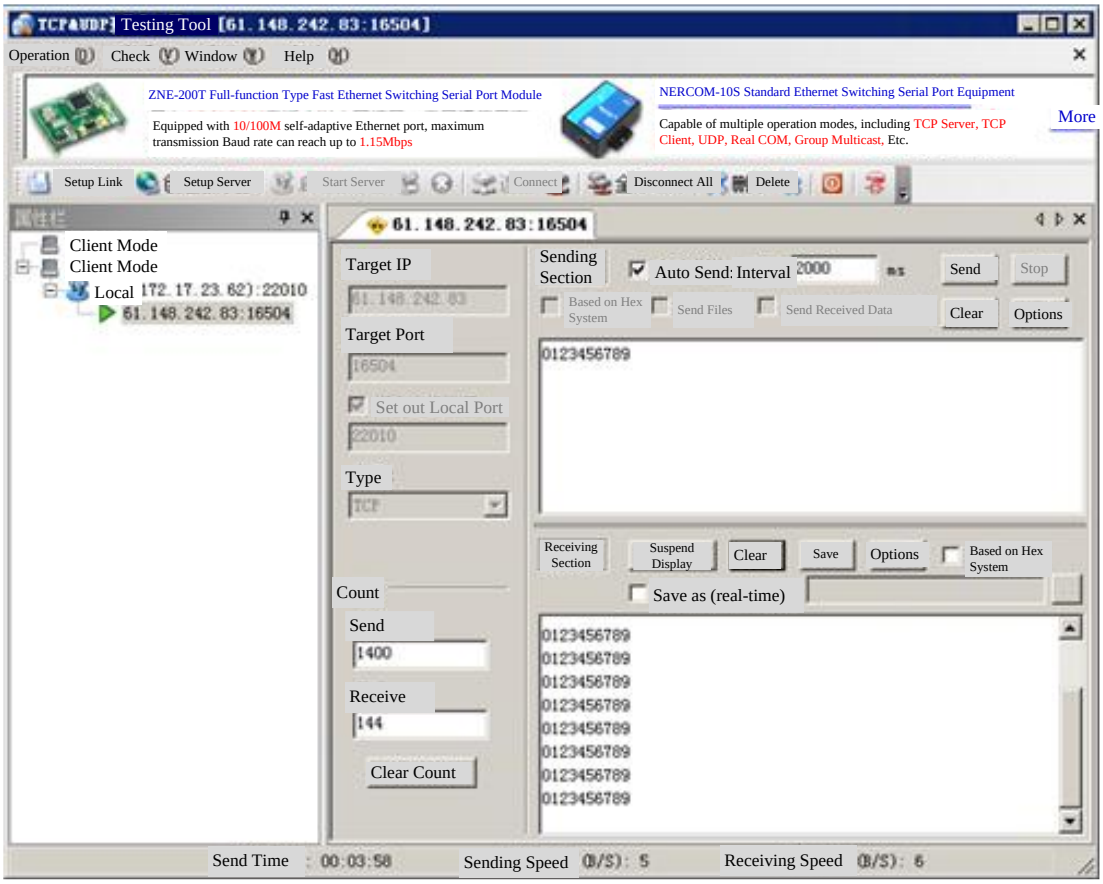


Fig. 4-16-4

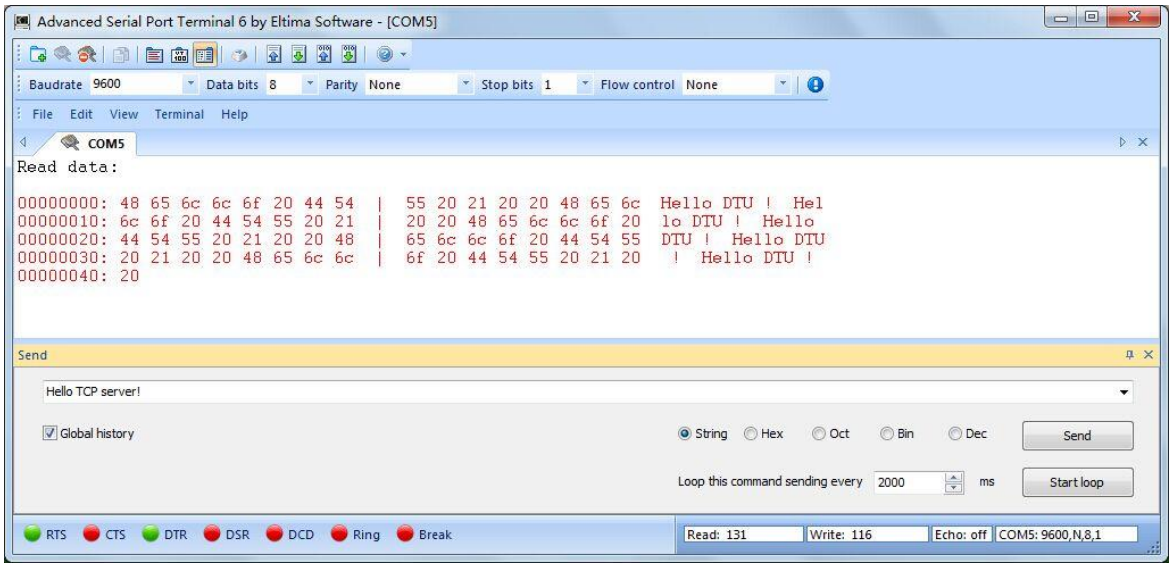


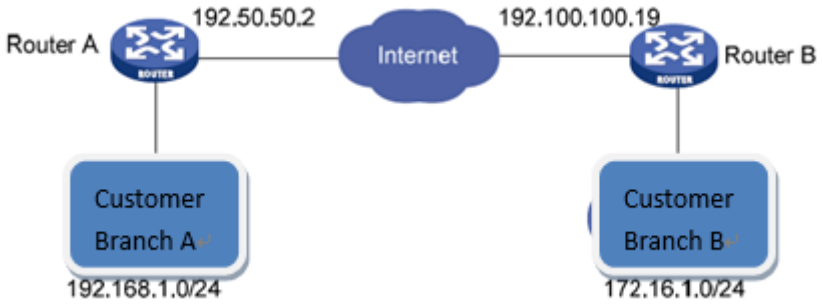
Fig. 4-16-5

4.17 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: From navigation panel, select VPN>>IPSec, then enter “IPSec Setting” page, as is shown in Fig. 4-17-1.

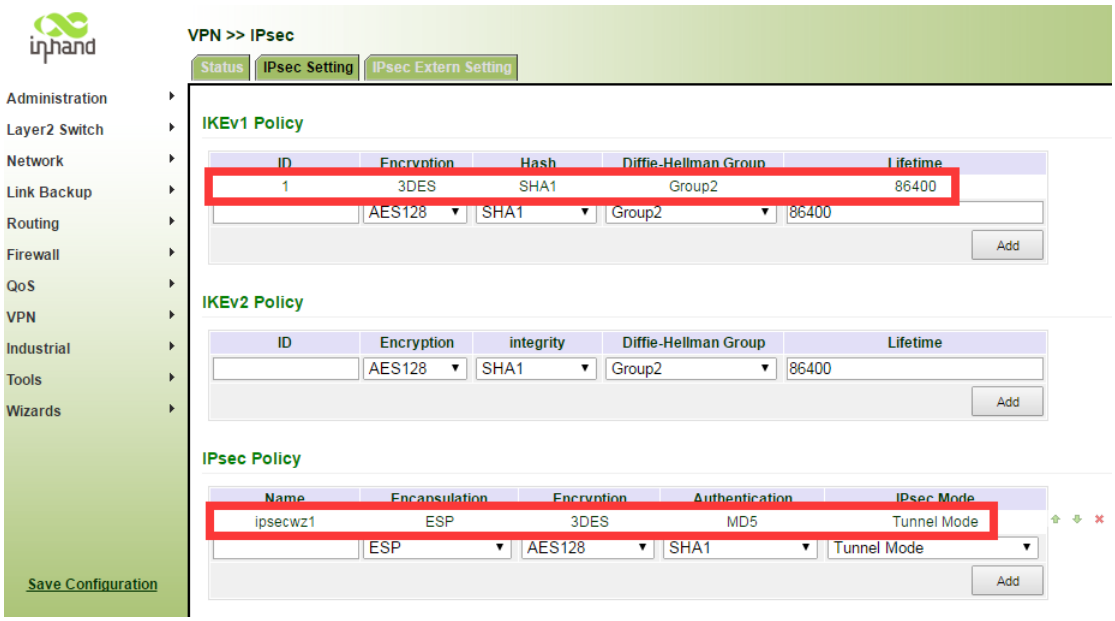


Fig. 4-17-1

Step 2: From navigation panel, select VPN>>IPSec, then enter “IPSec Setting” page, select “Add” in “IPSec Tunnel Configuration” and configure parameters in newly opened page, as is shown in Fig. 4-17-2.

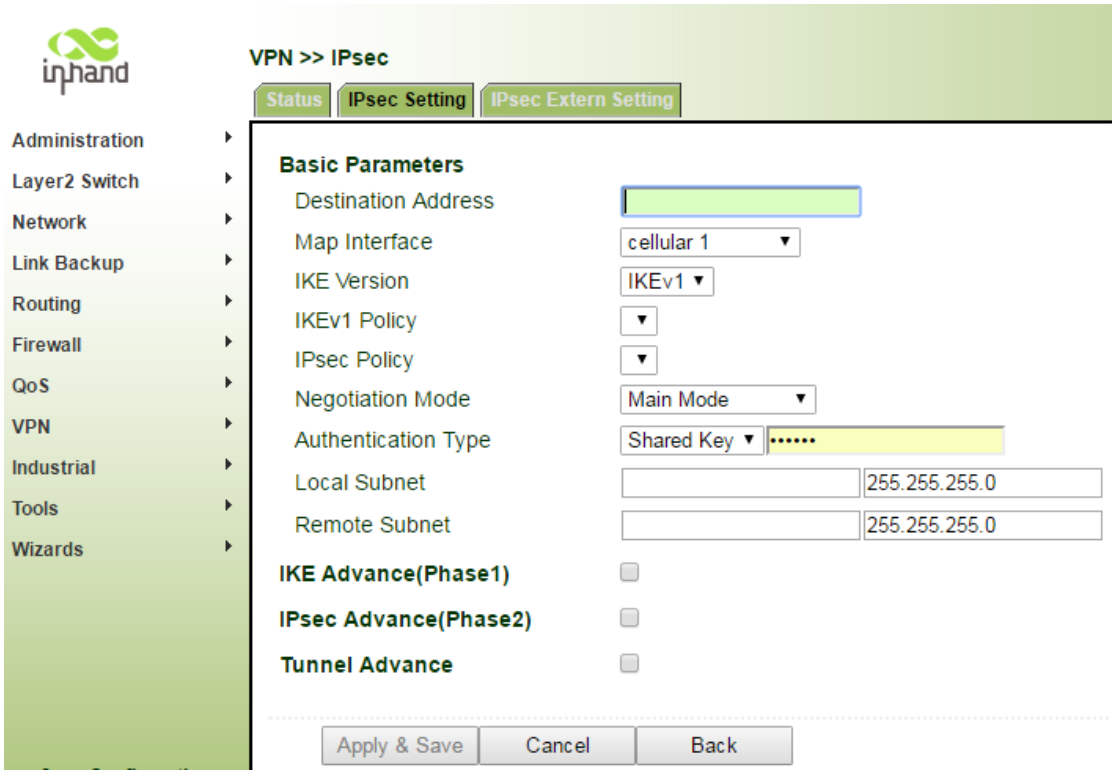


Fig. 4-17-2

Attention

No need to fill in local identifier or peer identifier.
No need to configure IPSec Profile when establishing IPSec VPN. IPSec Profile is only used for DMVPN.

2) Router B Settings

Step 1: From navigation panel, select VPN>>IPSec, then enter “IPSec Setting” page, as is shown in Fig. 4-17-3.

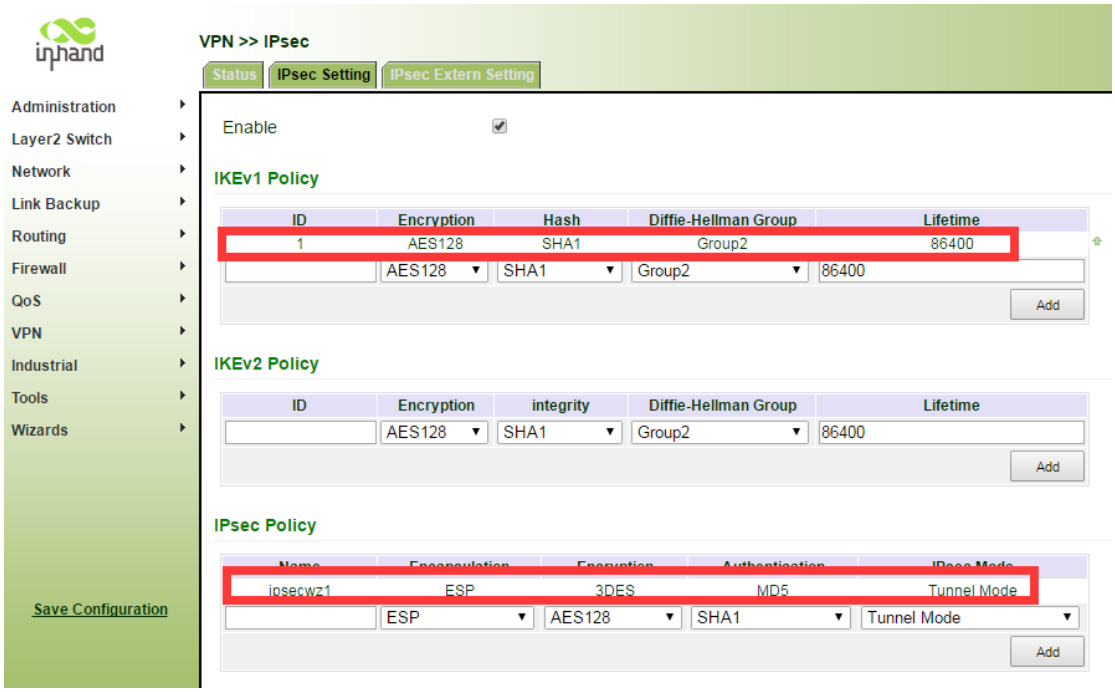


Fig. 4-17-3

Step 2: From navigation panel, select VPN>>IPSec, then enter “IPSec Setting” page, select “Add” in “IPSec Tunnel Configuration” and configure parameters in newly opened page, as is shown in Fig. 4-17-4.

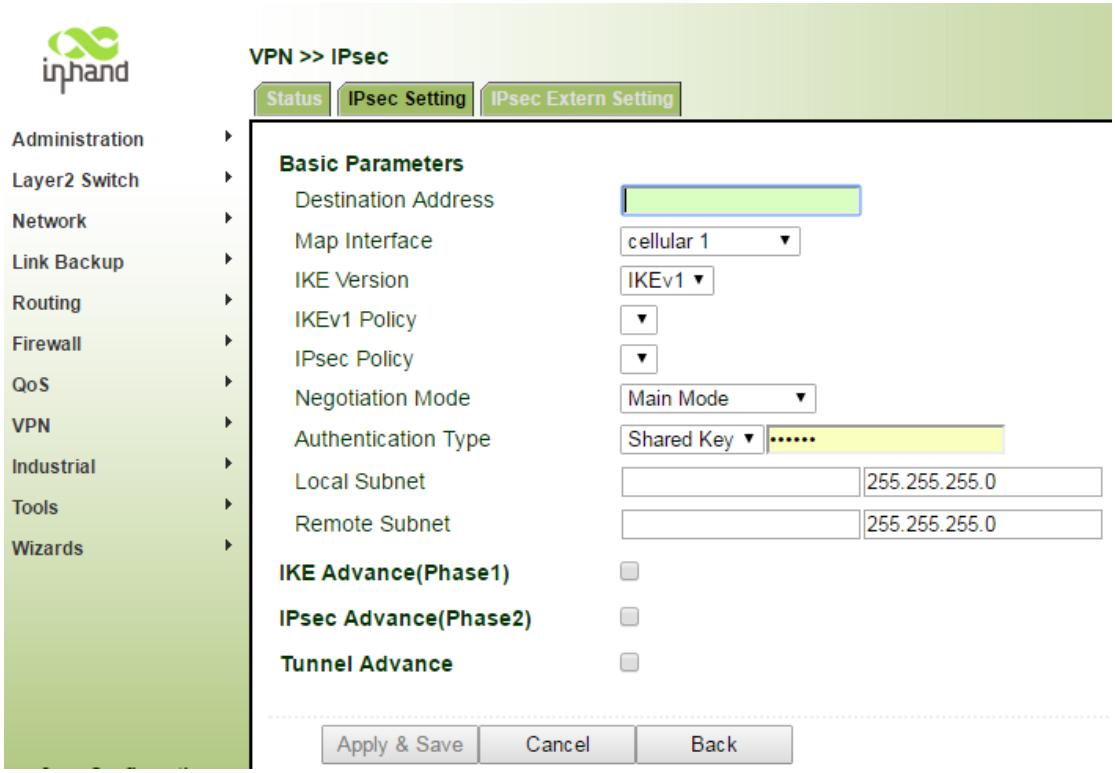


Fig. 4-17-4

3) VPN Status Checking

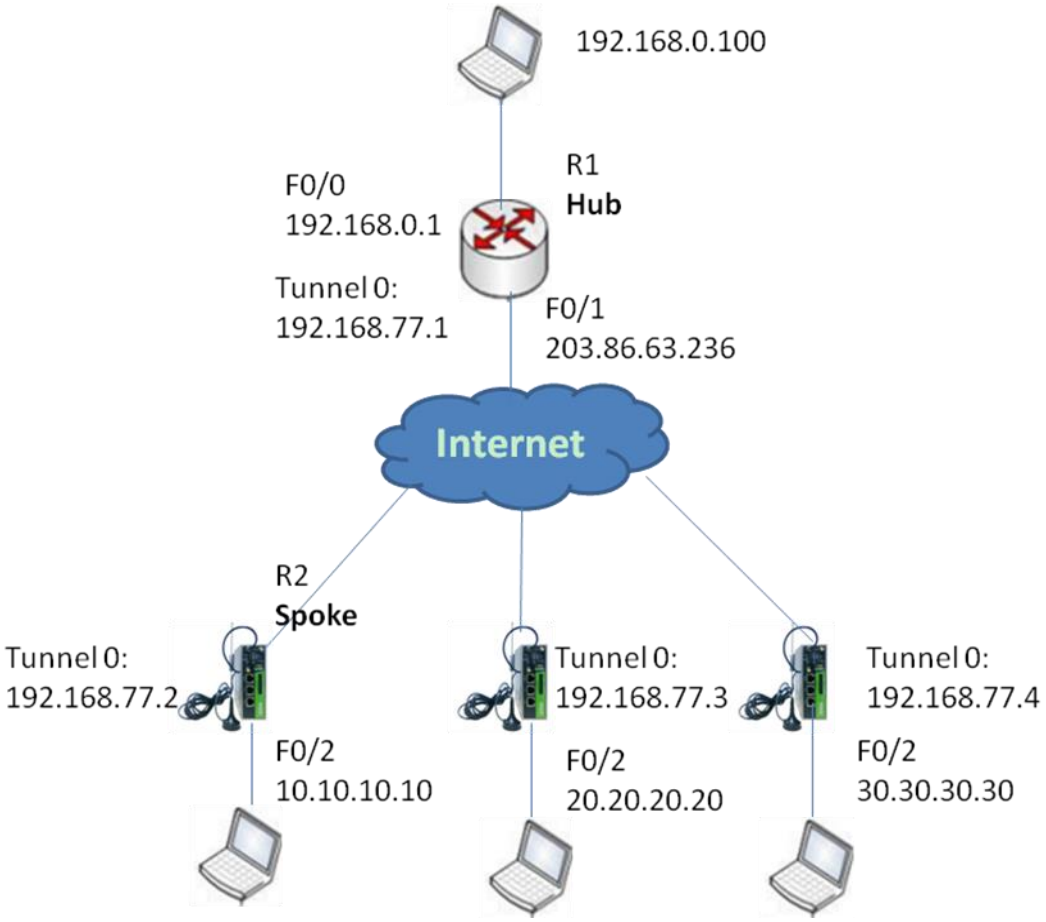
Step 1: From navigation panel, select VPN>>IPSec, then enter “IPSec Status” page, as is shown in Fig. 4-17-5.


Name
Tunnel Description
Status
IPSEC_1
Router...203.86.43.189
Connected
3 Seconds
Stop

Fig. 4-17-5

4.18 DMVPN Networking Configuration Example

Network Topology



Networking Environment

- R1: Must have a fixed and public IP address (as HUB);
- R2/R3/R4: Dial-up, dynamically get public IP address (as SPOKE);
- Establish DMVPN between R2/R3/R4 and HUB, make all the LANs can access each other;
- Related points: GRE tunnel/NHRP/Dynamical routing/IPsec VPN.

Networking Configuration:

1) Settings of R2/R3/R4

Step I: Configure IPsec

Navigate to "**VPN>>IPsec**", enter the page "**IPsec Configuration**", configuration is shown in Fig. 4-18-1.

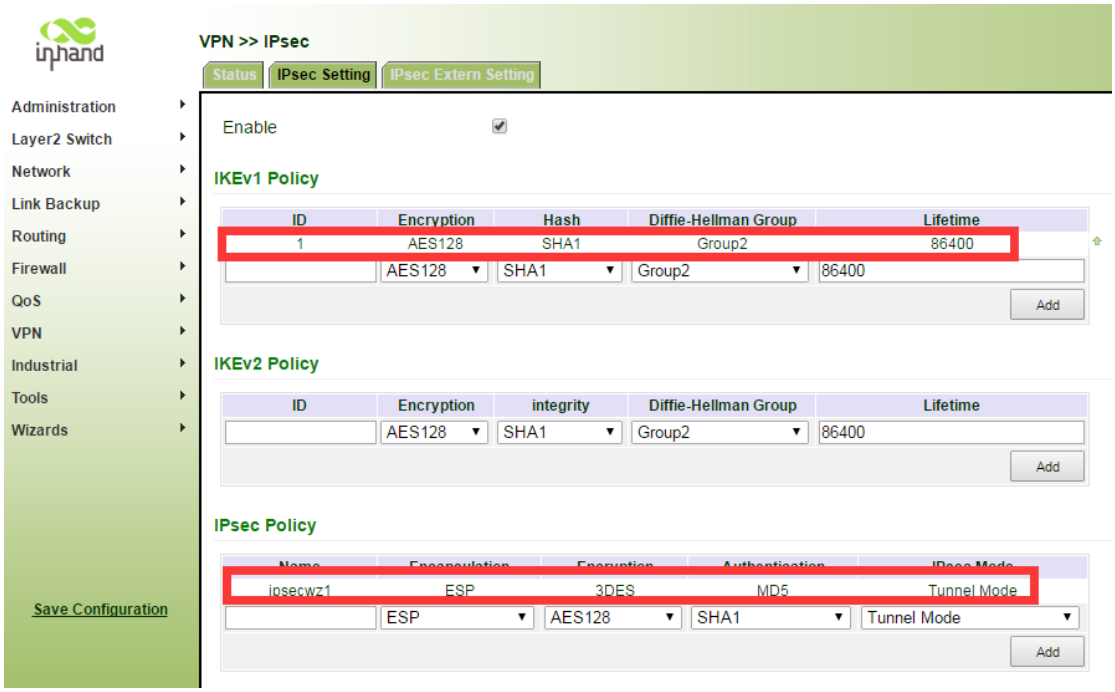


Fig. 4-18-1

Navigate to "**VPN>>IPsec**", enter the page "**IPsec Extension**", configuration is shown in Fig. 4-18-2.

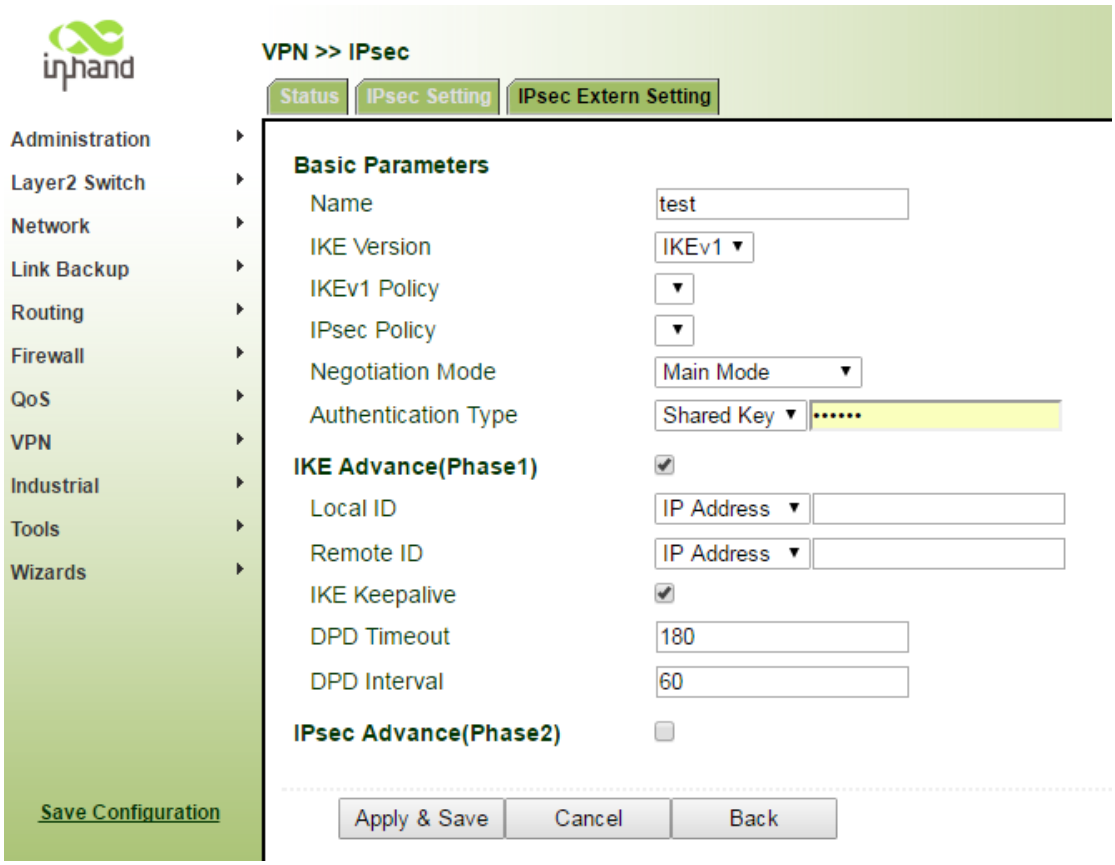


Fig. 4-18-2

Step II: Configure GRE

Navigate to "VPN >> GRE" menu, enter "GRE" page, select <new> to enter GRE configuration,

as is shown in Fig. 4-18-3.

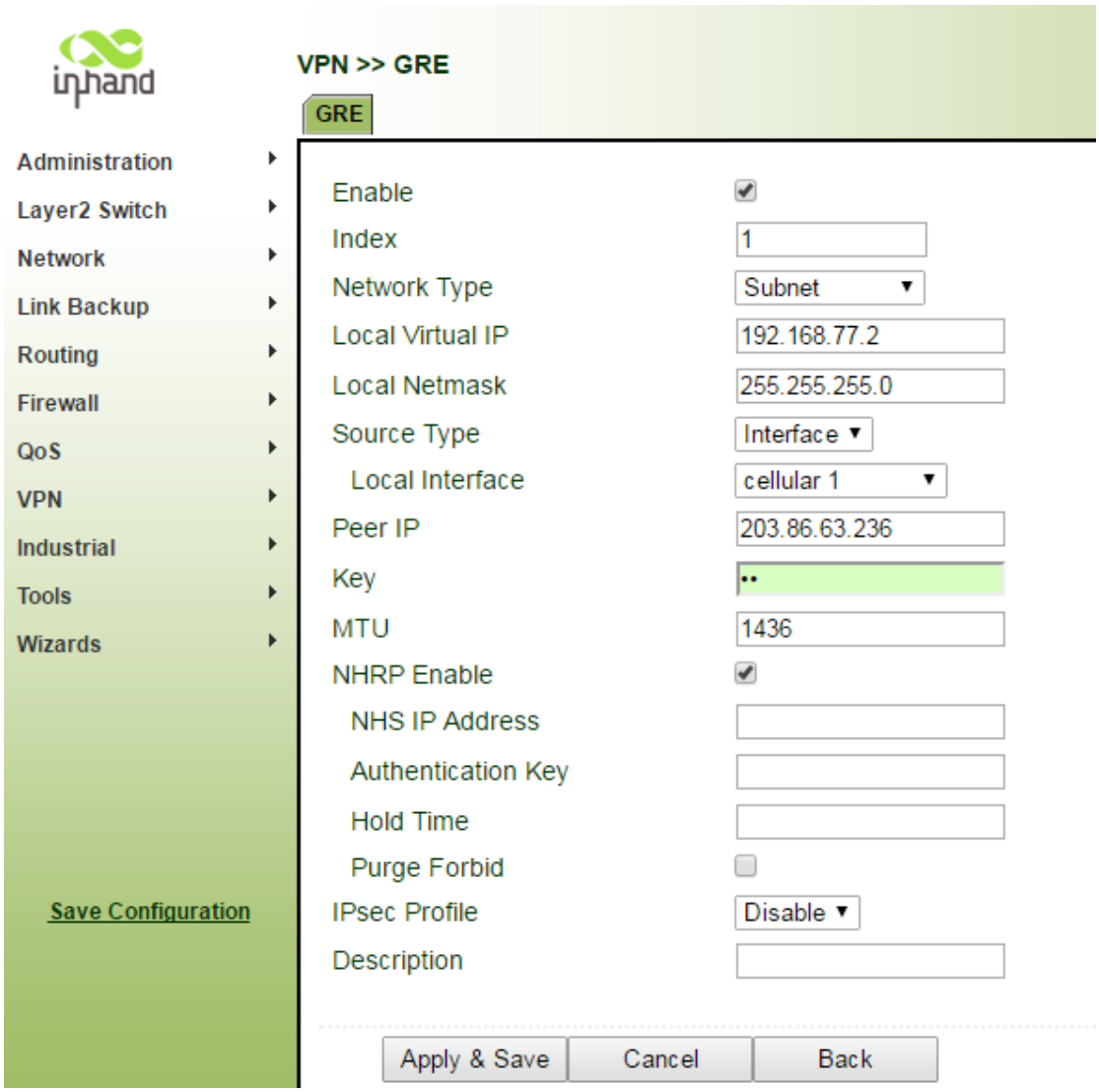


Fig. 4-18-3

Step III: Configure Dynamic Routing RIP

Click the “Status>>Route status” menu in the navigation tree to enter “RIP” interface as shown in Figure 4-18-4.

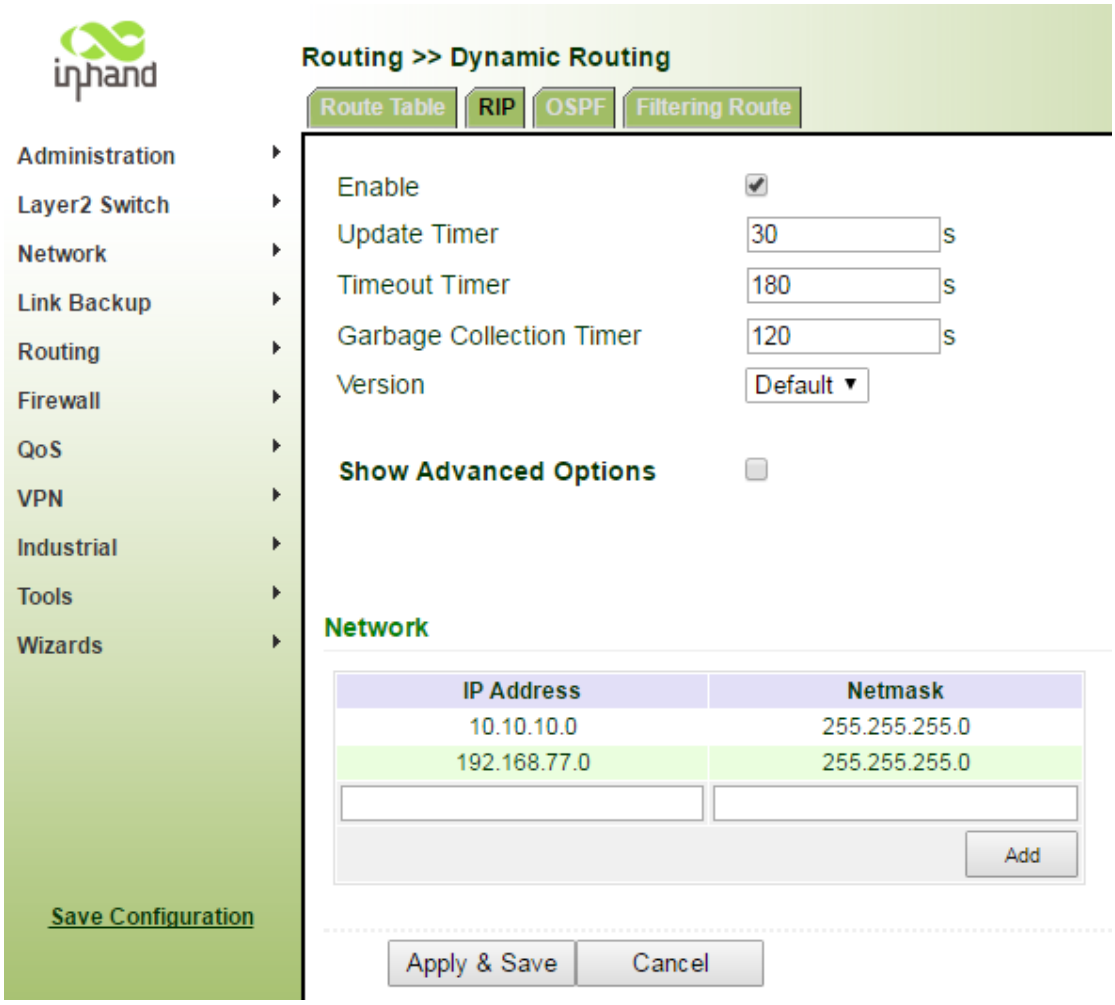


Fig. 4-18-4

Step IV: Check IPSec Status

Step 1: From navigation panel, select “VPN>>IPSec”, then enter “IPSec Status” page, as is shown in Fig. 4-18-5.

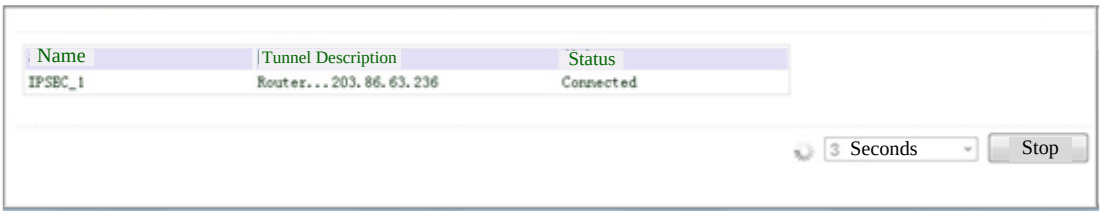


Fig. 4-18-5

2) HUB Configuration (Command Configuration is Applied)

Step 1: Configure IPsec VPN

#ipsec config

crypto ipsec-daemon stop

crypto ikev1 policy 1

encryption 3des

hash sha1

```
        group 2
        lifetime 86400
crypto ikev1 keyring test_keyring
        pre-shared-key address 0.0.0.0 0.0.0.0 key 1234567890
crypto ikev1 profile test
        authentication pre-share
        identity local address
        match identity remote address
        keyring test_keyring
        policy 1
        dpd 180 60
crypto ipsec transform-set ipsecwz1 esp-3des esp-md5-hmac
        mode tunnel
crypto ipsec profile test
        set ikev1-profile test
        set transform-set ipsecwz1
        set security-association lifetime seconds 3600
18:34:23 Router#
```

Step 2: Configure GRE and NHRP

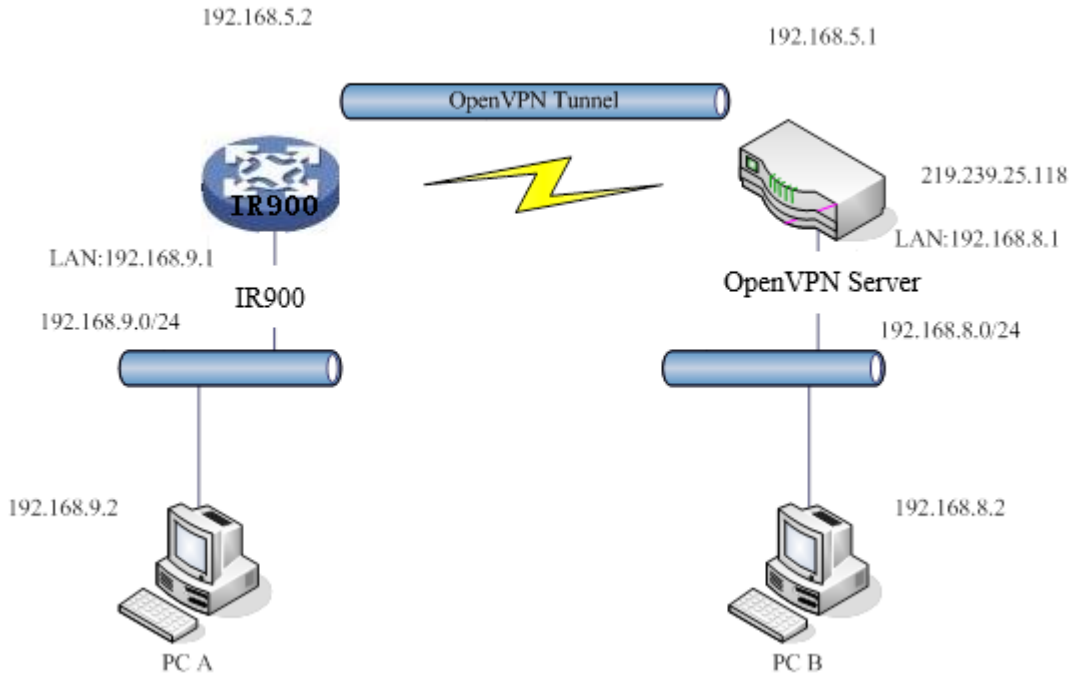
```
interface Tunnel1
 ip address 192.168.77.1 255.255.255.0
ip mtu 1436
 ip nhrp map multicast dynamic
 ip nhrp network-id 10
 ip nhrp holdtime 180
 no ip split-horizon
 tunnel source FastEthernet0/1
 tunnel mode gre multipoint
 tunnel key 123456
 tunnel protection ipsec profile abc
```

Step III: Configure Dynamic Routing Protocol

```
HUB(config)#router rip
HUB(config-router)#network192.168.0.1 255.255.255.0
HUB(config-router)#network192.168.77.1255.255.255.0
```

4.19 OPENVPN Application Example

Example: OpenVPN is based on TCP/UDP and can be applied to any port. Refer to the following figure for topological graph.



In the figure, an OpenVPN channel is established on equipment A and OpenVPN server. The virtual IPs at both sides of the channel are 192.168.5.2 and 192.168.5.1.

a. If OpenVPN of equipment A is in routing mode, the routing to 192.168.8.0/24 will be to OpenVPN channel and OpenVPN server. Accordingly, a static routing will be added to OpenVPN server so that the packet routing to 192.168.9.0/24 will be to OpenVPN channel. In this way, PC A and PC B are intercommunicated via OpenVPN and two-way visit can be realized.

b. if OpenVPN is in NAT mode via equipment A, OpenVPN server is in no need to increase the static routing about 192.168.9.0/24. Now, PC A can have access into PC B, but PC B cannot directly have access into PC A. It is applied to initial uploading. Now, PC A can have access into PC B, but PC B cannot directly have access into PC A. It is applied to initial uploading.

Configuration procedures of router are as follows:

Step 1: Configure relevant parameters of OpenVPN, as shown in Fig.4-19-1.

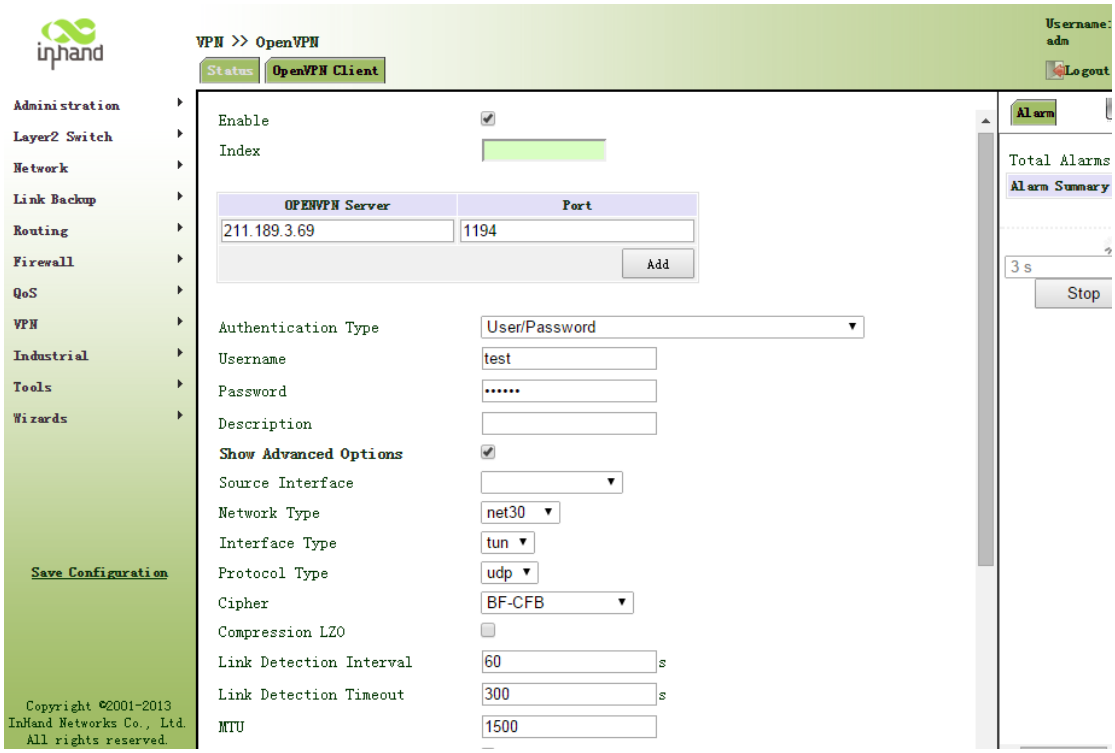


Fig. 4-19-1

Step 2: Configure different certificates in accordance with different certification demand when the channel is successfully established. The type of certification and certificate are as follows:

None ------ in no need of certificate

Pre-shared Key ----- in no need of certificate

User/Password ----- only CA certificate like ca.crt

X.509 Cert (multi-client), X.509 Cert ----- in need of CA certificate, equipment public key certificate, equipment private key certificate like ca.crt, my.crt, my.key.

Attention

1. The suffix of CA and public key certificate is .crt and the suffix of private key certificate is .key.
2. The time of equipment must be accurate when using certificate.

Step 3: Configure OpenVPN server after router is configured. Add a static routing to 192.168.2.0/24, route add -net 192.168.2.0 netmask 255.255.255.0 dev tun0 (suppose the net port of OpenVPN server is tun0).

Appendix Instruction of Command Line

1 Help Command

Help command can be obtained after entering help or "?" into console, "?" can be entered at any time during the process of command input to obtain the current command or help from command parameters, and command or parameters can be automatically complemented in case of only command or command parameter.

1.1 Help

[Command] help [<cmd>]

[Command] help [<cmd>].

[View] all views

[**Parameters**] <cmd> command name

[Example]

- enter: help

Get the list of all current available command.

- enter: help show

Display all the parameters of show command and using instructions thereof.

2 View Switchover Command

2.1 Enable

[Command] enable [15 [<*password*>]]

[Function] Switchover to privileged user level.

[View] Ordinary user view.

[Parameter]15 User right limit level, only supports right limit 15 (super users) at current.

<*password*> Password corresponded to privileged user limit level, hint of password inputting will be given in case of no entering.

[Example] Enter enable adm in ordinary user view

Switchover to super users and the password 123456

2.2 Disable

[Command] disable

[Function] Exit the privileged user level.

[View] Super user view, configure view

[Parameter] No

[Example] Enter disable in super user view

Return to ordinary user view.

2.3 End and !

[Command]end or !

[Function] Exit the current view and return to the last view.

[View] Configure view.

[Parameter] No

[Example] Enter end in configured view

Return to super user view.

2.4 Exit

[Command]exit

[Function] Exit the current view and return to the last view (exit console in case that it is ordinary user)

[View] all views

[Parameter] No

[Example]

- enter exit in configured view

Return to super user view.

- enter exit in ordinary user view

Exit console.

3 Check system state command

3.1 Show version

[Command] show version

[Function] Display the type and version of software of router

[View] all views

[Parameter] No

[Example] enter: show version

Display the following information:

Type : display the current factory type of equipment

Serial number : display the current factory serial number of equipment

Description : www.inhandnetworks.com

Current version : display the current version of equipment

Current version of Bootloader: display the current version of equipment

3.2 Show system

[Command] show system

[Function] display the information of router system

[View] all views

[Parameter] No

[Example] enter: show system

Display the following information

Example: 00:00:38 up 0 min, load average: 0.00, 0.00, 0.00

3.3 Show clock

[Command] show clock

[Function] display the system time of router

[View] all views

[Parameter] No

[Example] enter: show clock

Display the following information:

For example Sat Jan 1 00:01:28 UTC 2000

3.4 Show modem

[Command] show modem

[Function] Display the MODEM state of router

[View] all views

[Parameter] No

[Example] Enter: show modem

Display the following information:

Modem type

state

manufacturer

product name

signal level

register state

IMSI number

Internet state

3.5 Show log

[Command] show log [lines <n>]

[Function] display the log of router system and display the latest 100 logs in default.

[View] all views

[Parameter]lines <*n*> limits the log numbers displayed, wherein, n indicates the latest n logs in case that it is positive integer and indicates the earliest n logs in case that it is negative integer and indicates all the logs in case that it is 0.

[Example] enter: show log

Display the latest 100 log records.

3.6 Show users

[Command] show users

[Function] display the user list of router.

[View] all views

[Parameter] No

[Example] input: show users

Displayed user list of system is as follows:

User:

---

* adm

Wherein, user marked with * is super user.

3.7 Show startup-config

[Command]show startup-config

[Function] Display the starting device of router.

[View] super user view and configuration view

[Parameter] No

[Example] enter: show startup-config

Display the starting configuration of system.

3.8 Show running-config

[Command] show running-config

[Function] display the operational configuration of router

[View] super user view, configuration view

[Parameter] No

[Example] Enter: show running-config

Display the operational configuration of system.

4 Check the Command of Internet State

4.1 Show interface

[Command] show interface

[Function] Display the information of port state of router

[View] all views

[Parameter] No

[Example]enter: show interface

Display the state of all ports.

4.2 Show route

[Command] Show ip route

[Function] Display the routing list of router

[View] all views

[Parameter] No

[Example] enter: Show ip route

Display the routing list of system

4.3 Show arp

[Command] show arp

[Function] Display the ARP list of router

[View] all views

[Parameter] No

[Example] enter: show arp

Display the ARP list of system

5 Internet Testing Command

Router has provided ping , telnet and traceroute for internet testing.

5.1 Ping

[Command]ping <*hostname*> [count <*n*>] [size <*n*>] [source <*ip*>]

[Function] apply ICMP testing for appointed mainframe.

[View] all views

[Parameter]<*hostname*> tests the address or domain name of mainframe.

count <*n*> testing times

size <*n*> tests the size of data package (byte)

source <*ip*> IP address of appointed testing

[Example] Input: ping www.g.cn

Test www.g.cn and display the testing results

5.2 Telnet

[Command] telnet <*hostname*> [<*port*>] [source <*ip*>]

[Function] telnet logs in the appointed mainframe

[View] all views

[Parameter]<*hostname*> in need of the address or domain name of mainframe logged in.

<*port*>telnet port

source <*ip*> appoints the IP address of telnet logged in.

[Example] enter: telnet 192.168.2.2

telnet logs in 192.168.2.2

5.3 Traceroute

[Command] traceroute <*hostname*> [maxhops <*n*>] [timeout <*n*>]

[Function] test the acting routing of appointed mainframe.

[View] all views

[Parameter]<*hostname*> tests the address or domain name of mainframe

maxhops <*n*> tests the maximum routing jumps

timeout <*n*> timeout of each jumping testing (sec)

[Example] enter: traceroute www.g.cn

Apply the routing of www.g.cn and display the testing results.

6 Configuration Command

In super user view, router can use configure command to switch it over configure view for management. Some setting command can support no and default, wherein, no indicates the setting of cancelling some parameter and default indicates the recovery of default setting of some parameter.

6.1 Configure

[Command] configure terminal

[Function] switchover to configuration view and input the equipment at the terminal end.

[View] super user view

[Parameter] No

[Example] enter configure terminal in super user view

Switchover to configuration view.

6.2 Hostname

[Command] hostname [<*hostname*>]

default hostname

[Function] Display or set the mainframe name of router.

[View] Configuration view

[Parameter]<*hostname*> new mainframe name

[Example]

- enter hostname in configuration view

Display the mainframe name of router.

- enter hostname MyRouter in configuration view

Set the mainframe name of router MyRouter.

- enter default hostname in configuration view

Recover the mainframe name of router to the factory setting.

6.1 Configure

[Command] configure terminal

[Function] switchover to configuration view and input the equipment at the terminal end.

[View] super user view

[Parameter] No

[Example] enter configure terminal in super user view

Switchover to configuration view.

6.2 Hostname

[Command] hostname [<*hostname*>]

default hostname

[Function] Display or set the mainframe name of router.

[View] Configuration view

[Parameter]<*hostname*> new mainframe name

[Example]

- enter hostname in configuration view

Display the mainframe name of router.

- enter hostname MyRouter in configuration view

Set the mainframe name of router MyRouter.

- enter default hostname in configuration view

Recover the mainframe name of router to the factory setting.

6.4 clock set

[Command]clock set <*YEAR/MONTH/DAY*> [<*HH:MM:SS*>]

[Function] set the date and time of router.

[View] Configuration view

[Parameter]<*YEAR/MONTH/DAY*> date, format: Y-M-D

<*HH:MM:SS* > time, format: H-M-S

[Example] enter clock set 2009-10-5 10:01:02 in configuration view

The time of router set is 10:01:02 of Oct. 5th, 2009 morning.

6.5 Ntp server

[Command]ntp server <*hostname*>

no ntp server

default ntp server

[Function] set the customer end of internet time server

[View] configuration view

[Parameter]<*hostname*> address or domain name of mainframe of time server

[Example] enter sntp-client server pool.ntp.org in configuration view

Set the address of internet time server pool.ntp.org.

7 System Management Command

7.1 Reboot

[Command] reboot

[Function] System restarts.

[View] super user view, configuration view

[Parameter] No

[Example] enter reboot in super user view

System restarts.

7.2 Enable password

[Command] enable password [<*password*>]

[Function] modify the password of super user.

[View] configuration view

[Parameter]<*password*> new super user password

[Example] enter enable password in configuration view

Enter password according to the hint.

7.3 Username

[Command] username <*name*> [password [<*password*>]]

no username <*name*>

default username

[Function] set user name, password

[View] configuration view

[Parameter] No

[Example]

- enter username abc password 123 in configuration view

Add an ordinary user, the name is abc and the password is 123.

- enter no username abc in configuration view

Delete the ordinary user with the name of abc.

- enter default username in configuration view.

Delete all the ordinary users.