



# **IR900 Series Industrial Router User's Manual**

Version: V1.0

**Copyright © 2012-2013** All rights are reserved by Beijing InHand Network Technology Co., Ltd. and its licensors. Without the written permission of the Company, no unit or individual is allowed to excerpt, reproduce or transmit in any form part or all of the contents in the manual.



, INHAND and InHand are trademarks of Beijing InHand Network Technology Co., Ltd. The trademarks of other companies, product logos and trade names in the manual are possessed by their respective owners.

The contents of this manual may be changed due to product version upgrade or other reasons. InHand reserves the right to modify the contents of this manual without any notice or prompt. This manual is only used as the guidance. InHand makes every effort to provide accurate information in this manual, but InHand does not guarantee that there is no error in the manual. All statements, information and recommendations in this manual do not constitute any express or implied warranty.

## Preface

Welcome to use our InRouter900 series industrial routers! This user's manual will guide you in detail how to configure our InRouter900.

The preface includes the following contents:

- [Readers](#)
- [Conventions in the Manual](#)
- [Obtaining Documentation](#)
- [Technical Support](#)
- [Information Feedback](#)

## 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   |
|-------------------|--|
| <b>Bold</b>       | Keywords of command line (the part that should be remained unchanged in command and be entered as it is) are expressed with <b>bold font</b> . |
| <i>Italic</i>     | The parameters of command line (the part that must be replaced with the actual value in command) are expressed in <i>italic</i> .              |
| [ ]               | 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:

|  |   |
|--|---|
|  <b>Attention</b>   | It indicates matters to be noted. Improper operation may cause data loss or damage to the device. |
|  <b>Instruction</b> | The necessary complement or description on the contents of operation.                             |

## Obtaining Documentation

The latest product information is available on the website of InHand ([www.inhandnetworks.com](http://www.inhandnetworks.com)):

The main columns related to product information on the website of InHand are described as follows:

- [Service Support / Document Center]: Product information in terms of hardware installation, software upgrade, configuration, etc., is available.
- [Product Technology]: Documents on product introduction and technology introduction including relevant introduction on product, technical introduction, technical white papers, etc., are available.
- [Service Support / Software Download]: The supporting information on software version is available.

## Contents

|  |           |
|--|-----------|
| <b>IR900 INTRODUCTION .....</b>  | <b>7</b>  |
| <b>1.1 Overview .....</b>  | <b>7</b>  |
| <b>1.2 Product Features.....</b>   | <b>7</b>  |
| <b>LOGIN ROUTER .....</b>  | <b>11</b> |
| <b>2.1 Establish Network Connection .....</b>  | <b>11</b> |
| 2.1.1 Automatic acquisition of IP address (recommended) .....                                | 11        |
| 2.1.2 Set a static IP address .....  | 14        |
| <b>2.2 Confirm that the network between the supervisory PC and router is connected .....</b> | <b>15</b> |
| <b>2.3 Cancel the Proxy Server .....</b>   | <b>16</b> |
| <b>WEB CONFIGURATION .....</b>   | <b>19</b> |
| <b>3.1 Login the Web Setting Page of Router.....</b>   | <b>19</b> |
| <b>3.2 Management .....</b>  | <b>20</b> |
| 3.2.1 System .....   | 20        |
| 3.2.2 System Time.....   | 21        |
| 3.2.3 Admin Access.....  | 24        |
| 3.2.4 AAA .....  | 28        |
| 3.2.5 Configuration Management.....  | 33        |
| 3.2.6 SNMP .....   | 34        |
| 3.2.7 Alarm .....  | 38        |
| 3.2.8 System Log.....  | 42        |
| 3.2.9 System Upgrading .....   | 43        |
| 3.2.10 Reboot .....  | 44        |
| <b>3.3 Network.....</b>  | <b>44</b> |
| 3.3.1 Ethernet Port .....  | 44        |
| 3.3.2 Dialup Port.....   | 46        |
| 3.3.3 PPPoE.....   | 50        |
| 3.3.4 Loopback.....  | 51        |
| 3.3.5 DHCP service.....  | 51        |
| 3.3.6 DNS Services .....   | 55        |
| 3.3.7 Dynamic Domain Name .....  | 56        |
| 3.3.8 SMS .....  | 57        |
| <b>3.4 Link Backup.....</b>  | <b>58</b> |
| 3.4.1 SLA .....  | 58        |

|   |           |
|---|-----------|
| 3.4.2 Track Module .....                            | 59        |
| 3.4.3 VRRP .....                                    | 61        |
| 3.4.4 Interface Backup .....                        | 62        |
| <b>3.5 Routing .....</b>                            | <b>63</b> |
| 3.5.1 Static Route.....                             | 63        |
| 3.5.2 Dynamic Routing.....                          | 65        |
| 3.5.3 Multicast Routing.....                        | 70        |
| <b>3.6 Firewall .....</b>                           | <b>71</b> |
| 3.6.1 Access Control .....                          | 72        |
| 3.6.2 NAT .....                                     | 73        |
| <b>3.7 Qos .....</b>                                | <b>75</b> |
| <b>3.8 VPN.....</b>                                 | <b>77</b> |
| 3.8.1 IPSec .....                                   | 77        |
| 3.8.2 GRE .....                                     | 82        |
| 3.8.3 DMVPN .....                                   | 83        |
| 3.8.4 L2TP .....                                    | 86        |
| 3.8.5 OPENVPN .....                                 | 87        |
| 3.8.6 Certificate Management .....                  | 88        |
| <b>3.9 Tools .....</b>                              | <b>89</b> |
| 3.9.1 PING .....                                    | 89        |
| 3.9.2 Routing detection .....                       | 90        |
| 3.9.3 Link Speed Test .....                         | 90        |
| <b>3.10 Configuration Wizard .....</b>              | <b>91</b> |
| 3.10.1 New LAN .....                                | 91        |
| 3.10.2 New WAN .....                                | 91        |
| 3.10.3 New Cellular .....                           | 92        |
| 3.10.4 New IPSec Tunnel .....                       | 92        |
| <b>APPENDIX 1 TROUBLESHOOTING .....</b>             | <b>94</b> |
| <b>APPENDIX 2 GLOSSARY OF TERMS.....</b>            | <b>96</b> |
| <b>APPENDIX 3 FCC STATEMENT .....</b>               | <b>98</b> |
| <b>APPENDIX 4 IMPORTANT SAFETY INFORMATION.....</b> | <b>99</b> |

## IR900 Introduction

This chapter includes the following parts:

- Overview
- Product Features

### 1.1 Overview

Thanks for choosing IR900 series industrial router. InRouter 900 is the new generation of industrial router developed by InHand Networks for M2M in 4G era.

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. InRouter 900 has also been built for rapid deployment and easy management, which enables enterprises to quickly set up large scale industrial network with minimized cost and time.

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

### 1.2 Product Features

#### ➤ Uninterrupted Access to Internet

Redundant WAN connection, 2 Ethernet ports, 3G/4G embedded, various DSL, InRouter 900 is built to support various WAN and ensure network availability. Whether the device is located in commercial region or wild field, it can always keep on line with broadband service or widespread 3G/4G connection. Furthermore, InRouter 900 can automatically switch over between broadband and 3G/4G when one link is failed, so as to ensure uninterrupted WAN connection. With InRouter 900, your business is always online.

#### ➤ Support Large Scale Deployment

In your M2M application, there are thousands of remote machines, or tens of thousands of VPN connection, which turns out to be a big challenge for network management. InRouter 900 make large-scale deployment much easier with following features:

- Multiple configuration tools including Web and CLI, enable administrator to rapidly configure

thousands of InRouter

- Remote Network Management: InRouter 900 works with network management platforms installed in application center or headquarter. To remotely batch configure, download and upload configuration file, upgrade firmware, monitor status of connection and VPN tunnel... all these become essential for operating a M2M system especially when a large number of devices scatter widely with limited field staff or even totally unattended.
- InRouter 900 supports industrial standard SNMP and 3rd SNMP software platform, so as to integrate into enterprise level IT management system.
- InRouter 900 also collaborates with InHand Device Manager to handle cellular specialty of network management. InHand Device Manager can be cloud based or installed within enterprise's intranet. InHand Device Manager improves for cellular circumstance to monitor cellular data flow, signal strength on site, location of the device. Even better, there's no need to apply costly private network from telecomm operator, and you can build your worldwide M2M system across multiple operators.
- Multiple diagnostic tools, supporting 3G/4G modem status, IMEI, IMSI and registration status of cellular networks, help engineer out of complex network circumstance.
- Support dynamic routing of RIP, OSPF, automatically update routing of whole network, and largely increase efficiency of large scale deployment.
- Support Dynamic Multipoint VPN (DM VPN), greatly reduce workload to configure thousands of remote InRouter 900. Establishing a large & secured remote network never made so easy!
- Robust Security
  - Secured VPN Connections  
Support GRE, L2TP, IPSec VPN, DMVPN, OpenVPN; CA, ensure data security
  - Security of Network  
Support firewall functions to protect from network attacks, such as: Stateful Packet Inspection (SPI), Access Control List (ACL), resist DoS attack, intrusion protection, attack protection, IP/MAC Binding and etc.
  - Security of Devices



Support AAA, TACACS, Radius, LDAP, local authentication, and multi levels user authority, so as to establish a secured mechanism on centralized authentication and authorization of device access.

➤ High Reliability

- Redundancy

WAN Redundancy: support link backup, VRRP to support automatic switch over between WANs.

Dual SIM cards: backup between different mobile operators to ensure networks availability and bargaining power on data plan.

- Automatic Link Detection & Recovery

PPP Layer Detection: keep the connection with mobile network, prevent forced hibernation, able to detect dial link stability.

Network connection Detection: automatic redial when link broken, keep Long Connection.

VPN Tunnel Detection: sustain VPN tunnel, to ensure availability of business.

- InRouter Auto-recovery

InRouter embeds hardware watchdog, able to automatically recover from various failure, ensure highest level of availability.

➤ Entirely Ruggedized

InRouter 900 inherits InHand Networks' legacy on best-in-class ruggedized design. From component selection to circuit layout, InRouter 900 satisfies electric power and industrial applications on EMC, IP protection, temperature range and etc. InRouter 900 is designed to last in harshest circumstances.

➤ High Performance, High Bandwidth

- Equipped with powerful Cortex-A8 processor and 256MB memory, support more application needs

- Support 4G/LTE (100Mbps downlink and 50Mbps uplink) and HSPA+ (21Mbps downlink and 5.76Mbps uplink)

➤ InHand Network Operation System: INOS 2.0

InHand Network Operation System (INOS) has been built as the highly reliable & real-time basis for all network functions, as well as easy-to-use configuration interface via Web, CLI or

SNMP. INOS is in modular design, expandable, and adaptable to various M2M applications.

- Embed WIFI AP and Client, Easy to Establish Versatile Wireless Network
- Support 802.11 b/g/n standard, fulfill the need to connect WLAN devices, up to 150Mbps throughput
- Easily establish wireless LAN, support WEP/WPA/WPA2 for network security
- WIFI can be the backup WAN link for 3G/4G

## Login Router

This chapter mainly contains the following contents:

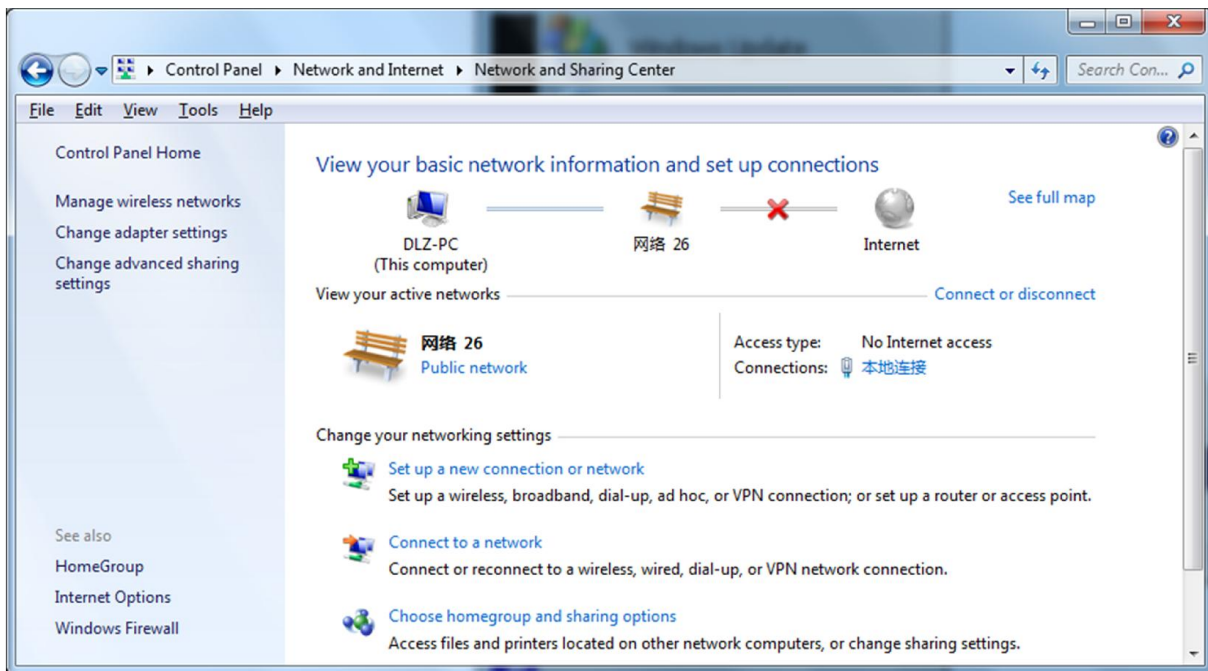
- [Establish Network Connection](#)
- [Confirm that the connection between supervisory PC and router](#)
- [Cancel the Proxy Server](#)

### 2.1 Establish Network Connection

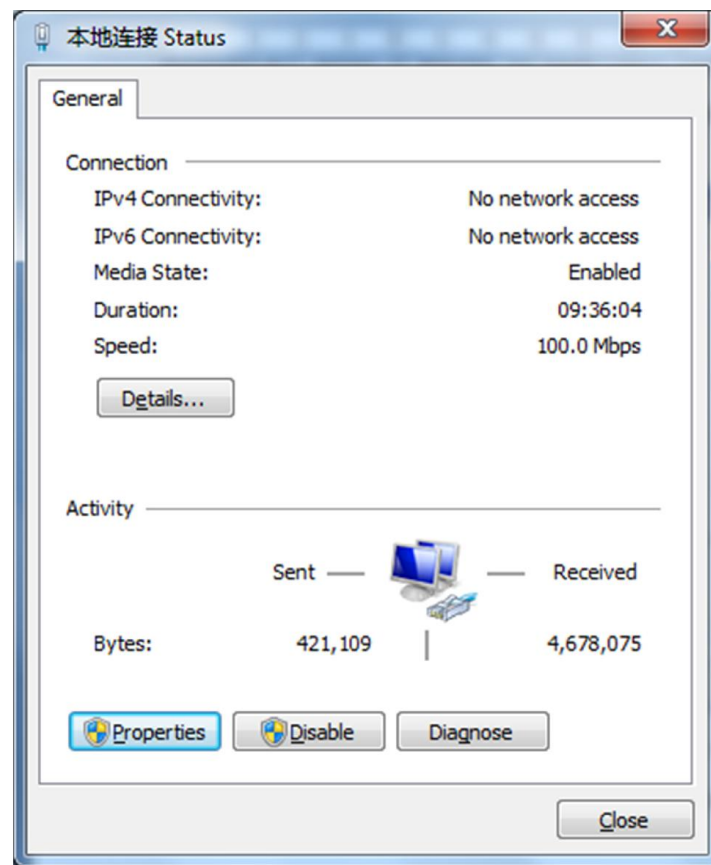
#### 2.1.1 Automatic acquisition of IP address (recommended)

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

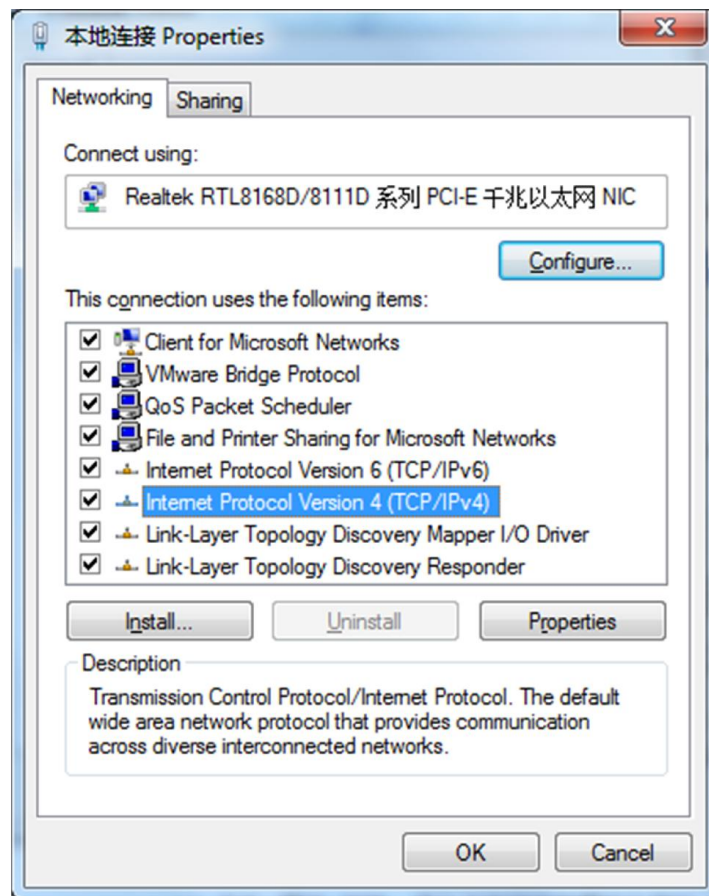
- 1) Open "Control Panel", double click "Network and Internet" icon, enter "Network and Sharing Centers"



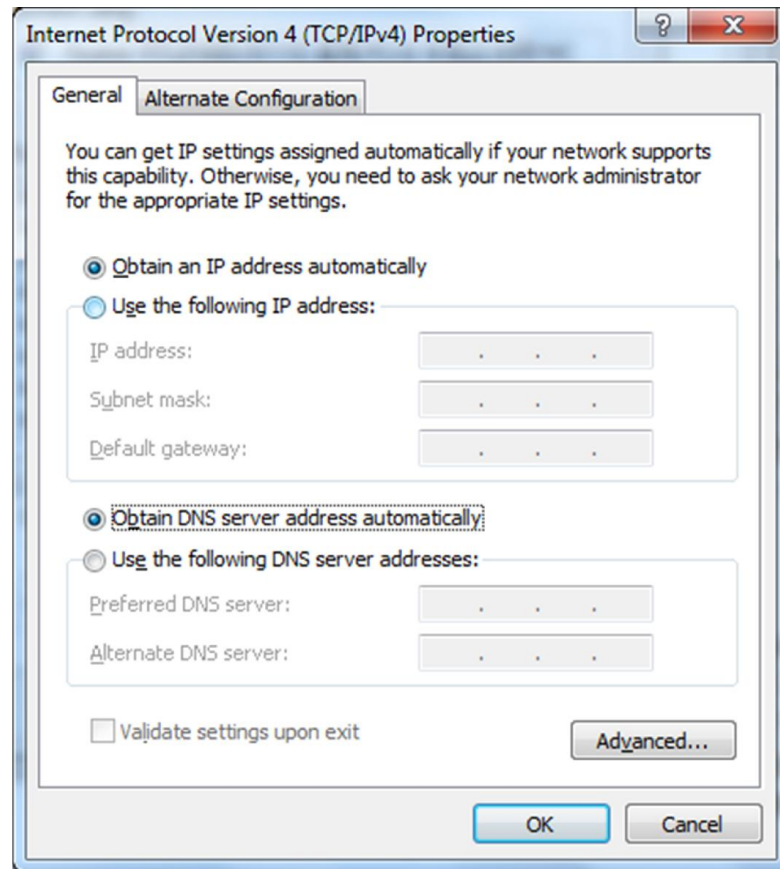
- 2) Click the button <Local Connection> to enter the window of "Local Connection Status"



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

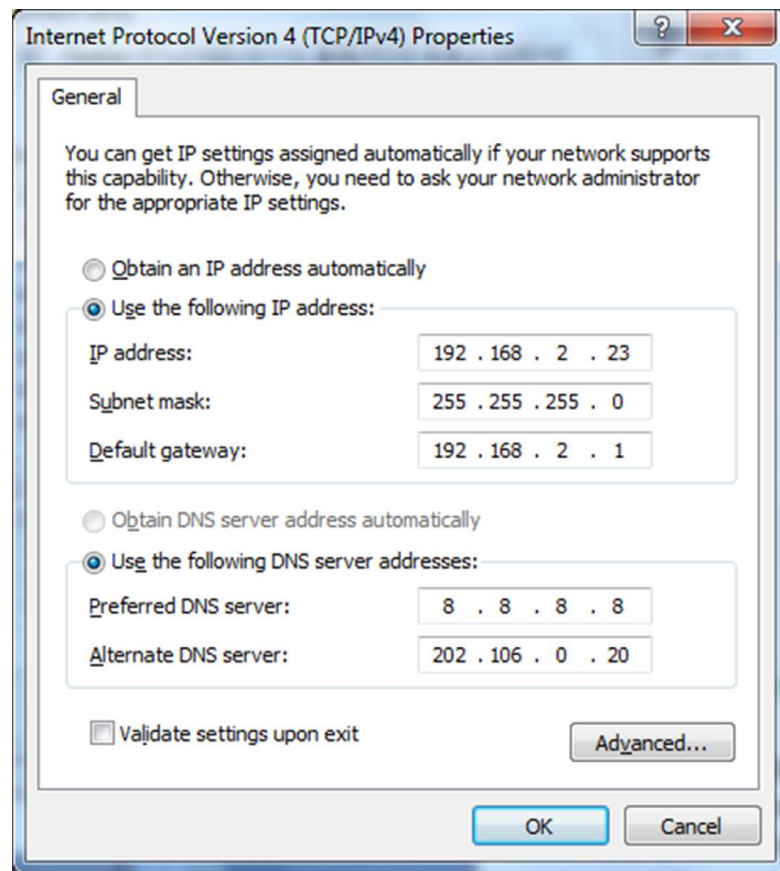


- 4) Select “Internet Portocol Version 4(TCP/IPv4)”, click <Properties> to enter “Internet Portocol Version 4 (TCP/IPv4) Properties” page. Select “Obtain an IP address automatically” and “Obtain DNS Server address automatically”, then click <OK> to finish setting, as shown below.



### 2.1.2 Set a static IP address

Enter “**Internet Portocol Version 4 (TCP/IPv4) Properties**” page, select “**Use the following IP address**”, type IP address (arbitrary value between 192.168.2.2~192.168.2.254), Subnet Mask (255.255.255.0), and Defafult Gateway (192.168.2.1), then click <OK> to finish setting, as shown below.



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

- 1) Click the button <Start> at the lower left corner to research “cmd.exe”, and run cmd.exe

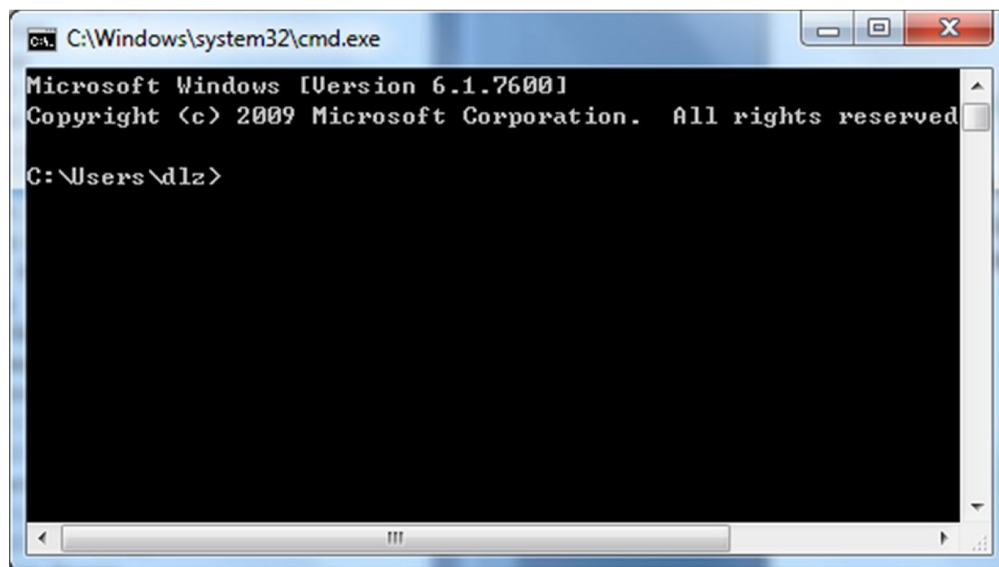
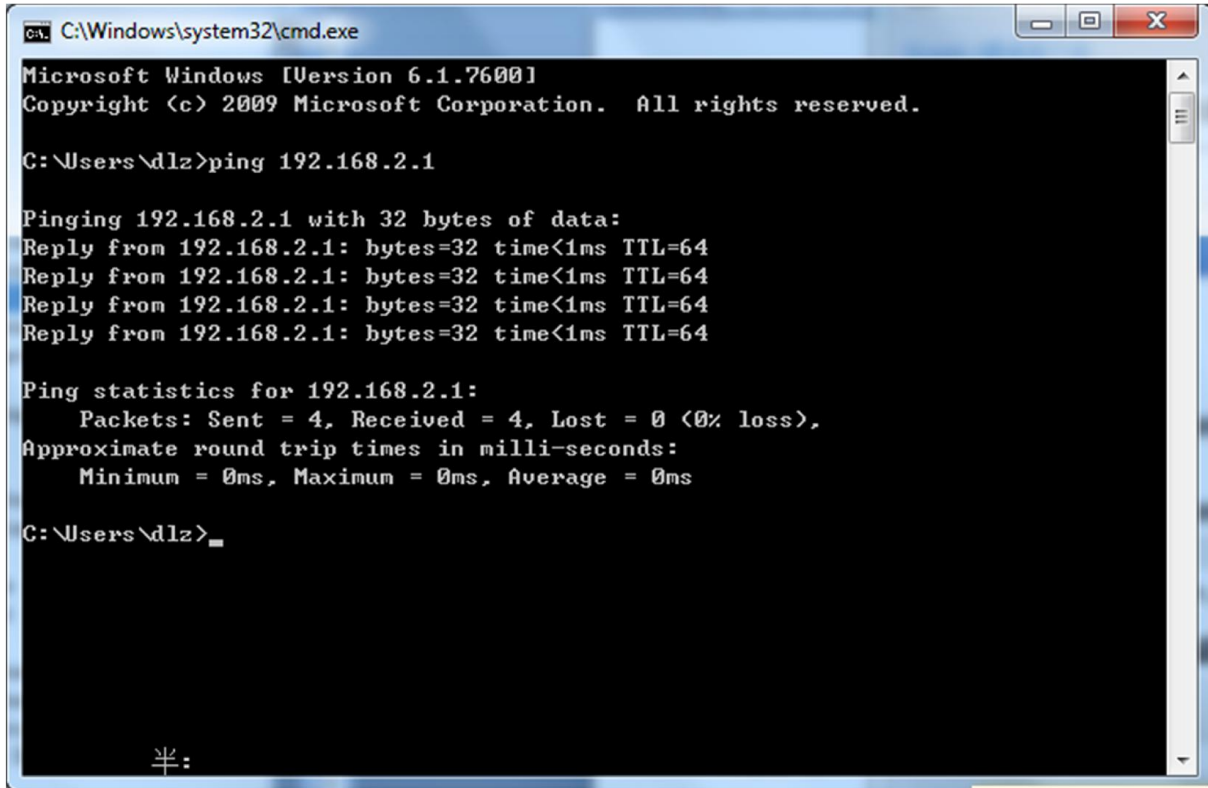


图 2-6 运行

- 2) Enter "ping 192.168.2.1 (IP address of router; it is the default IP address), and click the button <OK>. If the pop-up dialog box shows the response returned from the router side, it

indicates that the network is connected; otherwise, check the network connection.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\dlz>ping 192.168.2.1

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

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

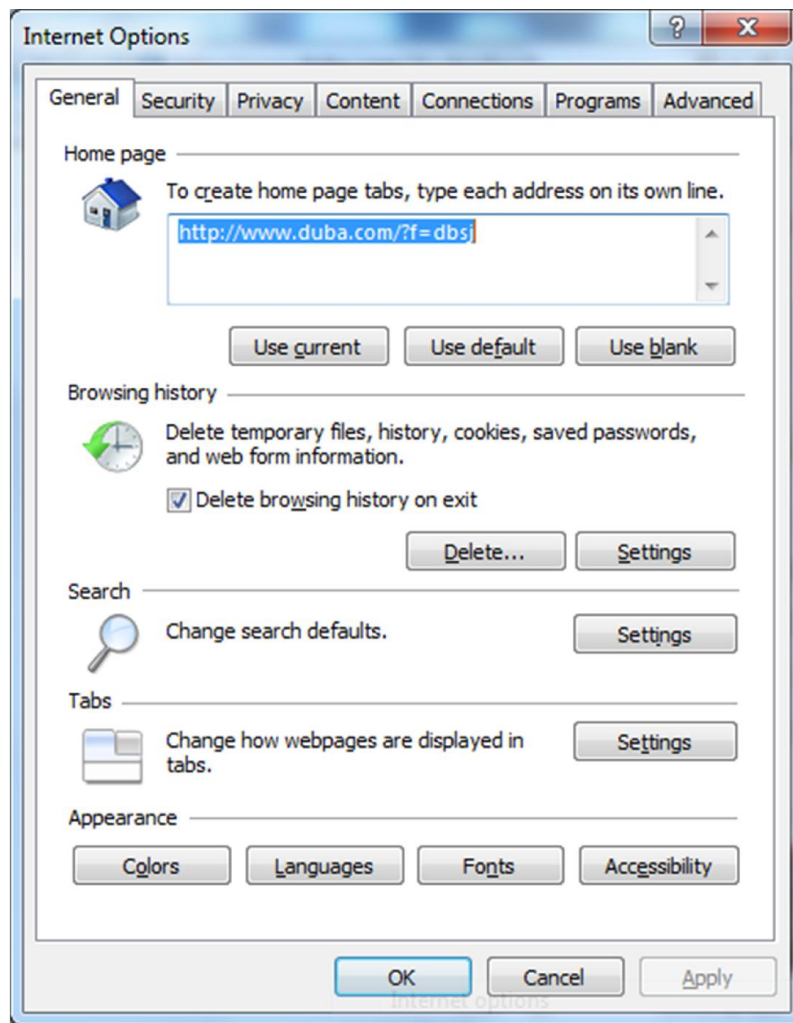
C:\Users\dlz>
```

## 2.3 Cancel the Proxy Server

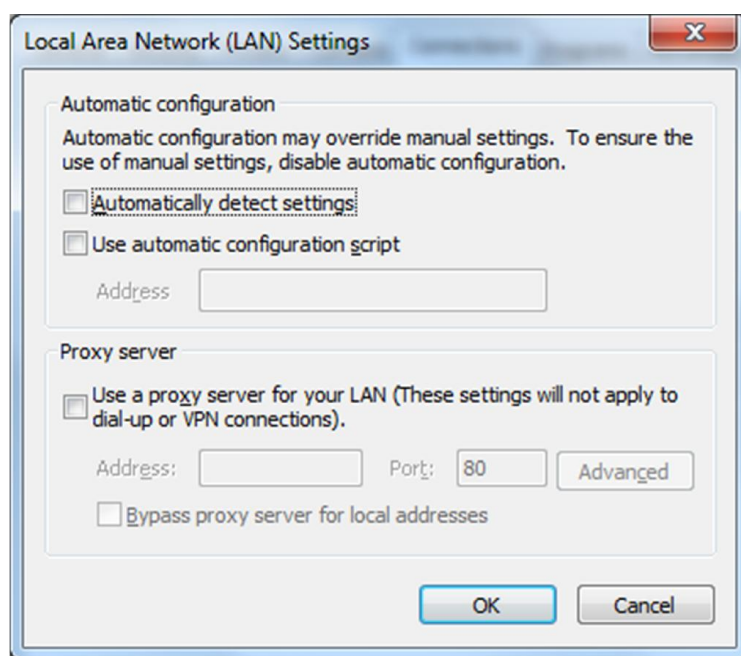
If the current supervisory computer uses a proxy server to access the Internet, it is required to cancel the proxy service and the operating steps are as follows:

- (1) Select [Tools/Internet Options] in the browser to enter the window of [Internet Options]





- (2) Select the tab "Connections" and click the button "LAN Setting(L)" to enter the page of "LAN Setting". Please confirm if the option "Use a Proxy Server for LAN" is checked; if it is checked, please cancel and click the button "OK".



## Web Configuration

This chapter includes the following parts:

- [Login/out Web Configuration Page](#)
- [Management](#)
- [Network](#)
- [Link Backup](#)
- [Routing](#)
- [Firewall](#)
- [QOS](#)
- [VPN](#)
- [Tools](#)
- [Installation Guide](#)

### 3.1 Login the Web Setting Page of Router

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



#### Instruction

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

## 3.2 Management

### 3.2.1 System

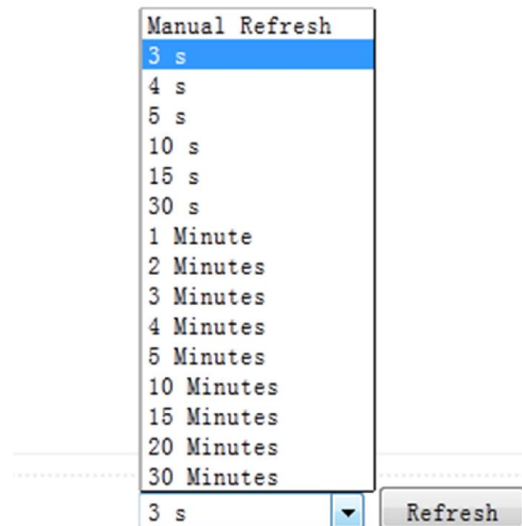
#### 3.2.2.1 System Status

From the left navigation panel, select **Administration << System**, then enter “**System Status**” page. On this page you can check system status and network status, as shown below. In system status, by clicking <**Sync Time**> you can make the time of router synchronized with the system time of the host. Click the “**Set**” behind Cellular1, Fastethernet 0/1 and Fastethernet 0/2 respectively on network status to enter into the configuration screen directly. For configuration methods, refer to Section [3.3.1](#) and [3.3.2](#).

The screenshot displays the InHand network management web interface. The top navigation bar shows 'Administration >> System' and the user 'adm'. The left sidebar lists various system functions: Administration, Network, Link Backup, Routing, Firewall, QoS, VPN, Tools, and Wizards. The main content area is titled 'System Status' and contains a table of system information. The table lists fields such as Name, Model, Serial Number, MAC Address, Current Version, Current Bootloader Version, Router Time, PC Time, Up time, CPU Load, and Memory consumption. A 'Sync Time' button is visible next to the PC Time field. The bottom right corner of the interface features a refresh interval dropdown menu set to '3 s' and a 'Stop' button. The footer of the interface includes the copyright notice 'Copyright ©2001-2013 InHand Networks Co., Ltd. All rights reserved.'

| System Status              |  |
|----------------------------|--|
| Name                       | Router   |
| Model                      | 902P   |
| Serial Number              | 00000000   |
| MAC Address                | 0018.0510.0003   |
|                            | 0018.0510.0004   |
| Current Version            | 1.0.0.r3194  |
| Current Bootloader Version | 2011.09.r3049  |
| Router Time                | 2013-07-10 10:17:50  |
| PC Time                    | 2013-07-10 10:17:53 <input type="button" value="Sync Time"/> |
| Up time                    | 0 day, 00:20:46  |
| CPU Load (1 / 5 / 15 mins) | 0.00 / 0.00 / 0.00   |
| Memory consumption         | 247.39MB / 216.68MB (87.59%)                                 |
| Total/Free                 |  |

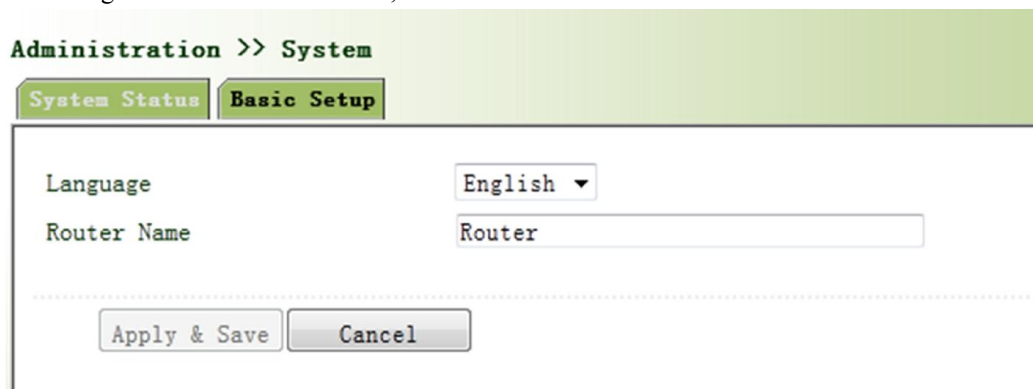
User can define the refresh interval of the screen through the drop down list at the lower right corner of the screen.



A dropdown menu titled "Manual Refresh" is shown. The menu contains the following options: 3 s, 4 s, 5 s, 10 s, 15 s, 30 s, 1 Minute, 2 Minutes, 3 Minutes, 4 Minutes, 5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, and 30 Minutes. The "3 s" option is currently selected and highlighted in blue. Below the dropdown is a small button labeled "Refresh".

### 3.2.1.2 Basic Settings

Select **Administration << System**, then enter “**Basic Setup**” page. You can set the language of Web Configuration Page and define Router Name, as shown below.



The "Basic Setup" page is displayed under the "Administration >> System" menu. It features two tabs: "System Status" and "Basic Setup". The "Basic Setup" tab is active. The page contains two configuration fields: "Language" with a dropdown menu set to "English", and "Router Name" with a text input field containing the text "Router". At the bottom of the page, there are two buttons: "Apply & Save" and "Cancel".

Page description is shown below:

| Parameter Name | Description                      | Default |
|----------------|----------------------------------|---------|
| Language       | Select system language of Router | English |
| Router Name    | Define Router Name               | Router  |

### 3.2.2 System Time

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

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

#### 3.2.2.1 System Time

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

From the left navigation panel, select **Administration >> System Time**, then enter “**System Time**” page, as shown below.

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

**Administration >> System Time**

**System Time** | **SNTP Client**

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

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

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

Page description is shown below:

| Parameters      | Description                      | Default                 |
|-----------------|----------------------------------|-------------------------|
| Router Time     | System time of Router            | 1970.01.01              |
| PC Time         | Time of connected PC             | None                    |
| Year/Month/Date | Set the expected Year/Month/Date | Current Year/Month/Date |
| Hour:Min:Sec    | Set the expected Hour:Min:Sec    | Current Hour:Min:Sec    |
| Timezone        | Set timezone                     | UTC+08:00               |

### 3.3.2.2 SNTP Client

SNTP, namely Simple Network Time Protocol, is a system for synchronizing the clocks of networked computers as a computer network protocol and provides comprehensive mechanisms to access national time and frequency dissemination services, organize the time-synchronization subnet and adjust the local clock in each participating subnet peer. In most places of the Internet today, SNTP provides accuracies of 1-50ms depending on the characteristics of the synchronization source and network paths.

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

From the left navigation panel, select **Administration << System Time**, then enter “**SNTP Client**” page, as

shown below.

## Administration >> System Time

System Time

SNTP Client

Enable ☐  
 Update Interval  s (60-2592000)  
 Source Interface   
 Source IP

### SNTP Servers List

| Server Address                     | Port                             |
|------------------------------------|----------------------------------|
| <input type="text"/>               | <input type="text" value="123"/> |
| <input type="button" value="Add"/> |                                  |



Page description is shown below:

| Parameters        | Description  | Default |
|-------------------|--|---------|
| Enable            | Enable/Disable SNTP client   | Disable |
| Update Interval   | Synchronization time intervals with SNTP server                      | 3600    |
| Source Interface  | Cellular1, Fastethernet 0/1, 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 server | None    |
| Port              | The service port of SNTP server                                      | 123     |

The meanings of key items in the page are shown in the table below



### Attention

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



### Instruction

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

### 3.2.3 Admin Access

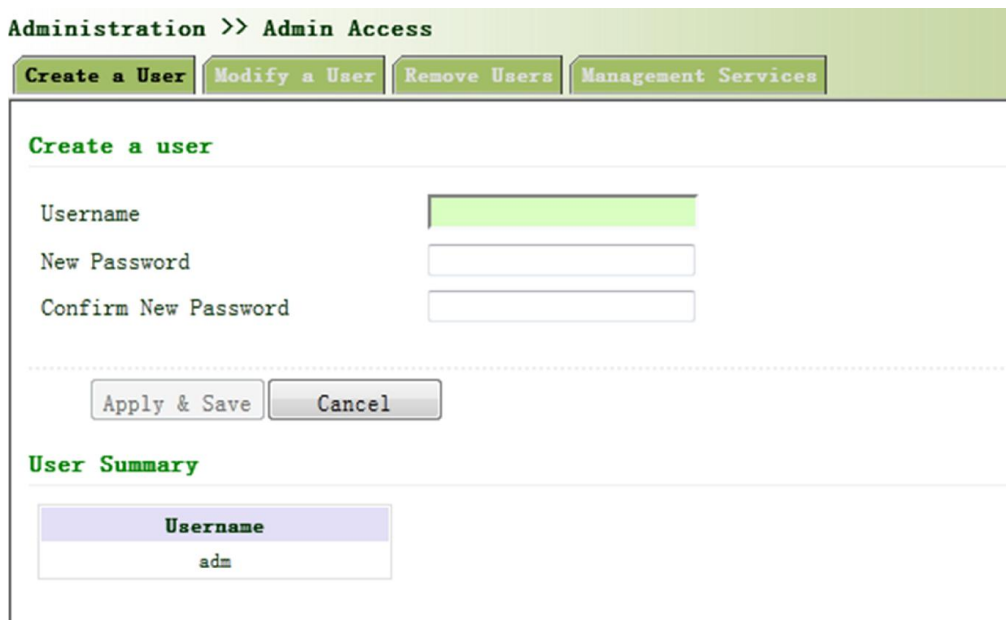
Admin Access allows the management of users which are categorized into superuser and common user.

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

#### 3.2.3.1 Create a User

Select **Administration >>Admin Access**, then enter “**Create a User**” page, as shown below.

Create a user



Page description is shown below:

| Parameters           | Description                          | Default |
|----------------------|--------------------------------------|---------|
| Username             | New username                         | None    |
| New Password         | New password                         | None    |
| Confirm New Password | Confirm the new password             | None    |
| User Summary         | List all the users of current system | None    |

#### 3.2.3.2 Modify a User

From the left navigation panel, select **Administration << Admin Access**, then enter “**Modify a User**” page, as shown below.

Press the user that needs to modify in “User Summary”, after the background turns blue, enter new information in “**Modify a User**”.



## Modify user information

Administration >> Admin Access

Create a User

Modify a User

Remove Users

Management Services

User Summary

Username

adm

Modify a user

Username

adm

New Password

Confirm New Password

Apply & Save

Cancel

Page description is shown below:

| Parameters           | Description                          | Default |
|----------------------|--------------------------------------|---------|
| User Summary         | List all the users of current system | adm     |
| Username             | The username needs to modify         | None    |
| New Password         | New password                         | None    |
| Confirm New Password | Confirm the new password             | None    |

### 3.2.3.3 Remove Users

From the left navigation panel, select **Administration << Admin Access**, then enter “**Remove Users**” page, as shown below.

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



#### Instruction

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

Administration >> Admin Access

Create a User

Modify a User

Remove Users

Management Services

User Summary

Username

adm

Delete

Cancel

### 3.2.3.4 Management Service

#### HTTP

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

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

#### HTTPS

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

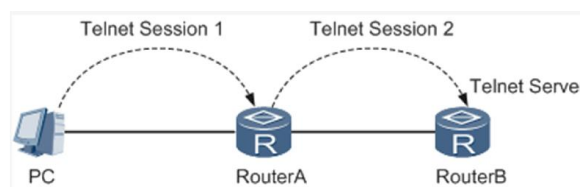
HTTPS, depending on SSL, is able to improve the device's security through following aspects:

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

#### TELNET

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

Connection of Telnet is shown in following figure:



Router A now functions as the Telnet Server, but also provides Telnet Client service. Router B and Router A provides Telnet Client function.

## SSH

Telnet adopts TCP to execute Plaintext Transmit, lacking of secure authentication mode and being vulnerable to DoS (Denial of Service), Host IP spoofing and routing spoofing and other malicious attacks, generating great potential security hazards.

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

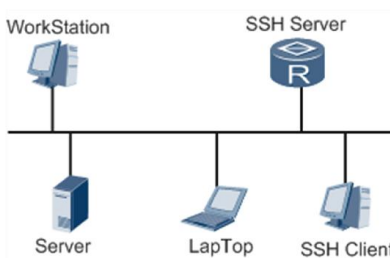
Through following measures SSH will realize the secure telnet on insecure network:

- Support RAS authentication.
- Support encryption algorithms such as DES, 3DES and AES128 to encrypt username password and data transmission.

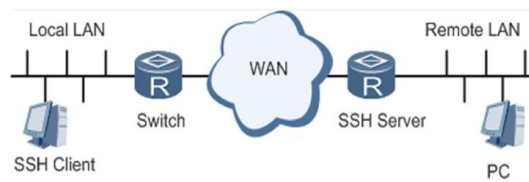
IR900 only supports SSH Server and could connect with multiple SSH Clients.

SSH supports local connection and WAN connection.

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



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



From the left navigation panel, select **Administration << Admin Access**, then enter “**Management Service**” page, as shown below.

## Administration &gt;&gt; Admin Access

Create a User

Modify a User

Remove Users

Management Services

## HTTP

Enable



Port

80

## HTTPS

Enable



Port

443

## TELNET

Enable



Port

23

## SSH

Enable



Port

22

Timeout

120

s (0-120)

Key Mode

RSA

Key Length

1024

Apply &amp; Save

Cancel

Page description is shown below:

| 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<br><b>Timeout:</b> timeout of SSH session. No operation within this period on SSH Client, SSH Server disconnect. Default: 120s<br><b>Cipher Mode:</b> set up public key encryption method (currently only RSA supported). <b>Cipher Code Length:</b> set up cipher code length, 512 or 1024. default: 1024 | Off     |

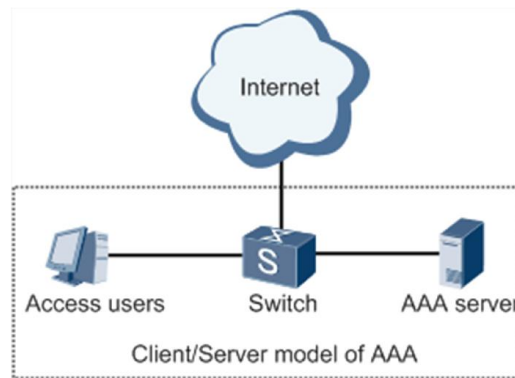
## 3.2.4 AAA

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

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

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

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

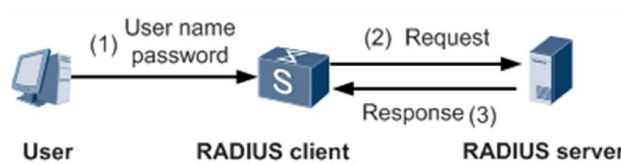


#### 3.2.4.1 Radius

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

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

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



- User name and passport will be sent to the NAS when the user logs on it;
- Radius Client on NAS receives username and password and then sends an authentication request to Radius Server;

- Upon the reception of legal request, Radius Server executes authentication and feeds back required user authorization information to Client; For illegal request, Radius Server will feed back Authentication Failed to Client.

From the left navigation panel, select **Administration << AAA**, then enter “**Radius**” page, as shown below.

**Administration >> AAA**

**Radius** **Tacacs+** **LDAP** **AAA Settings**

**Server List**

| Server Address       | Port | Key                  |
|----------------------|------|----------------------|
| <input type="text"/> | 1812 | <input type="text"/> |

Page description is shown below:

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

### 3.2.4.2 Tacacs+

Tacacs+, or Terminal Access Controller Access Control System, similar to Radius, adopts Client/Server mode to achieve the communication between NAS and Tacacs+ Server. But, Tacacs+ adopts TCP while Radius adopts UDP.

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

From the left navigation panel, select **Administration << AAA**, then enter “**Tacacs+**” page, as shown below.

## Administration &gt;&gt; AAA

Radius Tacacs+ LDAP AAA Settings

## Server List

| Server Address       | Port | Key                  |
|----------------------|------|----------------------|
| <input type="text"/> | 49   | <input type="text"/> |
| Add                  |      |                      |

Apply & Save Cancel

Page description is shown below:

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

## 3.2.4.3 LDAP

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

From the left navigation panel, select **Administration << AAA**, then enter "LDAP" page, as shown below.

## Administration &gt;&gt; AAA

Radius Tacacs+ LDAP AAA Settings

## Server List

| Name                 | Server Address       | Port                 | Base DN              | Username             | Password             | Security | Verify Peer              |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------|--------------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | None     | <input type="checkbox"/> |
| Add                  |                      |                      |                      |                      |                      |          |                          |

Apply & Save Cancel

Page description is shown below:

| Parameters     | Description                       | Default |
|----------------|-----------------------------------|---------|
| Name           | Define server name                | None    |
| Server Address | Server address (domain name / IP) | None    |
| Port           | Consistent with the server port   | None    |
| Base DN        | The top of LDAP directory tree    | None    |
| Username       | Username accessing the server     | None    |

|             |                                   |          |
|-------------|-----------------------------------|----------|
| Password    | Password accessing the server     | None     |
| Security    | Encryption mod: None,SSL,StartTLS | None     |
| Verify Peer | Verify Peer                       | Unopened |

### 3.2.4.4 AAA Settings

#### AAA supports following authentication ways:

- None: with great confidence to users, legal check omitted, generally not recommended.
- Local: Have user's information stored on NAS. Advantages: rapidness, cost reduction. Disadvantages: storage capacity limited by hardware.
- Remote: Have user's information stored on authentication server. Radius, Tacacs+ and LDAP supported for remote authentication. ◦

#### AAA supports following authorization ways:

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

From the left navigation panel, select **Administration << AAA**, then enter “**AAA Setting**” page, as shown below.

Administration >> AAA

Radius Tacacs+ LDAP AAA Settings

| Service | Authentication |        |        | Authorization |        |        |
|---------|----------------|--------|--------|---------------|--------|--------|
|         | 1              | 2      | 3      | 1             | 2      | 3      |
| console | none ▾         | none ▾ | none ▾ | none ▾        | none ▾ | none ▾ |
| telnet  | none ▾         | none ▾ | none ▾ | none ▾        | none ▾ | none ▾ |
| ssh     | none ▾         | none ▾ | none ▾ | none ▾        | none ▾ | none ▾ |
| web     | none ▾         | none ▾ | none ▾ | none ▾        | none ▾ | none ▾ |

Apply & Save
Cancel

Page description is shown below:

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



**Attention**

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

**Instruction**

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

### 3.2.5 Configuration Management

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

From the left navigation panel, select **Administration << Config Management**, then enter “**Config Management**” page, as shown below.

Page description is shown below:

| 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**

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



## Instruction

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

### 3.2.6 SNMP

#### Definition

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

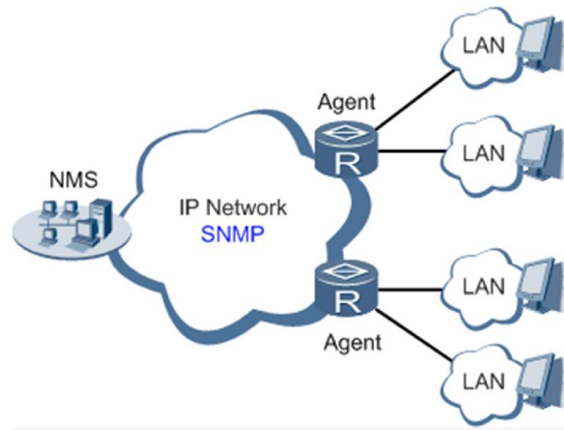
- **Simplicity:** SNMP adopts polling mechanism, provides the most basic sets of features and could be used in small-scale, rapid, low cost environments. SNMP, with UDP message as the carrier, is supported by a great majority of devices.
- **Powerfulness:** objective of SNMP is to ensure the transmission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

#### Benefits

- Network administrators could make use of SNMP to accomplish the information query, modification, troubleshooting and other jobs on any node on network to achieve higher efficiency.
- Shielding of physical differences between devices. SNMP only provides the most basic sets of features for mutual independence between administration and the physical properties, network types of devices under administration; therefore, it could realize the uniform management of different devices at a lower cost.
- Simple design, lower cost. Simplicity is stressed on addition of software/hardware, types and formats of message on devices so as to minimize the influence and cost on devices caused by running SNMP.

#### Application: management of device is achieved through SNMP

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



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

Through SNMP:

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

SNMP(Simple Network Management Protocol) is an application-layer communication protocol, through SNMP, network administrators can manage network performance, find and solve network problems, and plan network growth.

SNMP includes NMS and Agent:

- NMS(Network Management Station) is a station which runs client procedure.
- Agent is service software which is running in device.

The purpose of NMS and Agent is as followed:

- NMS can send getRequest, getNextRequest, setRequest packets to Agent, when the Agent receive these packets, it will execute read or write operations according to the type of packet and create Response packet back to NMS.
- When device happens to status change (for example port plug), Agent will send Trap packet and report all the events to NMS.

#### 3.2.6.1 SNMP Basic Setting

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

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

From the left navigation panel, select **Administration << SNMP**, then enter “SNMP” page, as shown below.

Administration >> SNMP

**SNMP** **SnmpTrap**

Enable ☒

SNMP Version

Contact Information

Location Information

**Community Management**

| Community Name       | Access Limit                           | MIB View                                 |
|----------------------|--|--|
| public               | Read-Only                              | defaultView                              |
| private              | Read-Write                             | defaultView                              |
| <input type="text"/> | <input type="text" value="Read-Only"/> | <input type="text" value="defaultView"/> |

Page description is shown below:

| Parameters           | Description                | Default                                     |
|----------------------|----------------------------|---|
| Enable               | Enable/Disable SNMP        | Disable                                     |
| SNMP Version         | 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 | Publi and private                           |
| Access Limit         | Select access limit        | Read-only                                   |
| MIB View             | Select MIB View            | defaultView                                 |

When choosing SNMPv3 version, the corresponding Use and User Group should be configured. The configuraion page is shown below.

## Administration &gt;&gt; SNMP

SNMP

SnmTrap

Enable ☒  
 SNMP Version   
 Contact Information   
 Location Information

## User Group Management (v3)

| Groupname   | Security Level | Read-only View | Read-write View | Inform View |
|---|----------------|----------------|-----------------|-------------|
| <input type="text"/>  | NoAuth/NoPriv  | defaultView    | defaultView     | defaultView |
| <input type="button" value="Add"/> <span>+</span> <span>-</span> <span>x</span> |                |                |                 |             |

## Usm Management (v3)

| Username                           | Groupname            | authentication | authentication password | encryption | encryption password  |
|------------------------------------|----------------------|----------------|-------------------------|------------|----------------------|
| <input type="text"/>               | <input type="text"/> | None           | <input type="text"/>    | None       | <input type="text"/> |
| <input type="button" value="Add"/> |                      |                |                         |            |                      |

Page description is shown below:

| Parameters      | Description                                    | Default       |
|-----------------|--|---------------|
| Groupname       | User define, length:1-32 charaters             | None          |
| Security Level  | Includes NoAuth/NoPriv, Auth/NoPriv, Auth/priv | NoAuth/NoPriv |
| Read-only View  | Only support defaultView at present            | defaultView   |
| Read-write View | Only support defaultView at present            | defaultView   |
| Inform View     | Only support defaultView at present            | defaultView   |

## 3.2.6.2 SnmpTrap Setting

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

From the left navigation panel, select **Administration << SNMP**, then enter “**SnmTrap**” page, as shown below.

## Administration &gt;&gt; SNMP

SNMP

SnmpTrap

## Configure SnmpTrap

| Host address         | Security Name        | UDP Port                           |
|----------------------|----------------------|------------------------------------|
| <input type="text"/> | <input type="text"/> | 162                                |
|                      |                      | <input type="button" value="Add"/> |

Apply &amp; Save

Cancel

Page description is shown below:

| 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     |

### 3.2.7 Alarm

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

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

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

Alarm status divided into raise, confirm, clear, When alarm occurs , it is in the state of "raise", if the user thinks this alarm is not great importance or the exception has been solved , he can directly set it to "clear" state; if the user is temporarily unable to resolve this anomaly, he can set it to "confirm" state, when the exceptions had been eliminated , it was set to "clear".

Alarm level can be divided:

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

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, including relay and Email, log record is a default output way.

On the “Alarm Map” page, you can map the alarm type which you concern to one or more alarm notice way.

### 3.2.7.1 Alarm Status

From the left navigation panel, select **Administration>> Alarm**, then enter “**Alarm State**” page, as shown below. Through this page, you can check all the alrms since the router is powered.

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



Page description is shown below:

| Parameters  | Description                                       | Default |
|-------------|---|---------|
| ID          | Alarm index                                       | None    |
| Status      | Current alarm status                              | ALL     |
| Level       | Current alarm level                               | None    |
| Date        | Date of alarm occurs                              | None    |
| System Time | The time from system startup to alarm produce (s) | None    |
| Content     | Alarm description                                 | None    |

### 3.2.7.2 Alarm Input

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

From the left navigation panel, select **Administration >>Alarm**, then enter “**Alarm Input**” page, as shown below.

Administration >> Alarm

Alarm Status

Alarm Input

Alarm Output

Alarm Map

Warm Start

Cold Start

Memory Low

FE0/1 Link Down

FE0/1 Link Up

FE0/2 Link Down

FE0/2 Link Up

Cellular Up/Down

ADSL Dialup (PPPoE) Up/Down

Ethernet Up/Down

Apply & Save

Cancel

Page description is shown below:

| Parameters             | Description                   | Default |
|------------------------|-------------------------------|---------|
| Warm Start             | On/Off Warm Start alarm       | Off     |
| Cold Start             | On/Off Cold Start alarm       | Off     |
| Memory Low             | On/Off Memory Low alarm       | Off     |
| Fastethernet LINK-UP   | On/Off LINK-UP alarm          | Off     |
| Fastethernet LINK-DOWN | On/Off LINK-Down alarm        | Off     |
| Cellular Up/Down       | On/Off Cellular Up/Down alarm | Off     |
| PPPoE Up/Down          | On/Off PPPoE Up/Down alarm    | Off     |
| Ethernet Up/Down       | On/Off Ethernet Up/Down alarm | Off     |

### 3.2.7.3 Alarm Output

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

From the left navigation panel, select **Administration >>Alarm**, then enter “**Alarm Output**” page, as shown below.



**Administration >> Alarm**

**Alarm Status** **Alarm Input** **Alarm Output** **Alarm Map**

**Email Alarm**

Enable Email Alarm: ☒

Mail Server IP/Name:

Mail Server Port:

Account Name:

Account Password:

Crypt:

**Email Addresses (At least one address is needed.)**

Page description is shown below:

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



### Attention

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

### 3.2.7.4 Alarm Map

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

From the left navigation panel, select **Administration >> Alarm**, then enter “**Alarm Map**” page, as shown below.

### Administration >> Alarm

| Alarm Status                | Alarm Input | Alarm Output | Alarm Map |
|-----------------------------|-------------|--------------|-----------|
|                             | CLI         | Email        |           |
| Warm Start                  |             |              |           |
| Cold Start                  |             |              |           |
| Memory Low                  |             |              |           |
| FE0/1 Link Down             |             |              |           |
| FE0/1 Link Up               |             |              |           |
| FE0/2 Link Down             |             |              |           |
| FE0/2 Link Up               |             |              |           |
| Cellular Up/Down            |             |              |           |
| ADSL Dialup (PPPoE) Up/Down |             |              |           |
| Ethernet Up/Down            |             |              |           |

## 3.2.8 System Log

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

### 3.2.8.1 Log

From the left navigation panel, select **Administration >>Log**, then enter “**System Log**” page, as shown below.

### Administration >> Log

View recent  Lines

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

### 3.2.8.2 System Log Settings

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

From navigation panel, select **Administration >>Log**, then enter “**System Log**” page, as

shown below.

Administration >> Log

Log System Log

Log to Remote System ☒

IP Address / Port(UDP) : 514

Log to Console ☒

Apply & Save Cancel

Page description is shown below:

| Parameters            | Description                         | Default |
|-----------------------|-------------------------------------|---------|
| Log to Remote System  | Open/close remote log function      | Close   |
| IP Address/ Port(UDP) | Set remote server's IP address/Port | 514     |
| Log to Console        | Open/close console log function     | Open    |

### 3.2.8.3 Kiwi Syslog Daemon

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

### 3.2.9 System Upgrading

From navigation panel, select **Administration >>Upgrade**, then enter “**Upgrade**” page, as shown below.

Administration >> Upgrade

Select the file to use:

浏览... Upgrade

Current Version : 1.0.0.r3194

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



#### Attention

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

**Instruction**

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

### 3.2.10 Reboot

From navigation panel, select **Administration >>Reboot**, then enter “**Reboot**” page, as shown below. Click <Yes> to reboot the system.

**Attention**

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

## 3.3 Network

### 3.3.1 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. PPPoE, the short form of Point-to-Point Protocol over Ethernet, achieves networking of a large number of hosts through Ethernet, connects with internet through a remote access device and carries out control and charging of each connected host. High performance and favorable price are the key factors for PPPoE's extensive applications in community networking construction and so on.

#### 3.3.1.1 Status

From navigation panel, select **Network >>Ethernet**, then enter “**Status**” page, as shown below.

| Network >> Ethernet     |                                   |
|-------------------------|-----------------------------------|
| <b>Status</b>           | Fastethernet 0/1 Fastethernet 0/2 |
| <b>Fastethernet 0/1</b> |                                   |
| Connection Type         | Static IP                         |
| IP Address              | 192.168.1.1                       |
| Netmask                 | 255.255.255.0                     |
| Gateway                 | 0.0.0.0                           |
| DNS                     | 0.0.0.0                           |
| MTU                     | 1500                              |
| Status                  | Up                                |
| Connection time         | 0 day, 00:31:05                   |
| Remaining Lease         |                                   |
| <b>Fastethernet 0/2</b> |                                   |
| Connection Type         | Static IP                         |
| IP Address              | 192.168.2.1                       |
| Netmask                 | 255.255.255.0                     |
| Gateway                 | 0.0.0.0                           |
| DNS                     | 0.0.0.0                           |
| MTU                     | 1500                              |
| Status                  | Up                                |
| Connection time         | 0 day, 00:31:05                   |
| Remaining Lease         |                                   |

### 3.3.1.2 Ethernet Port

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

The configuration of the two Ethernet ports is the same. Take Ethernet 0/1 as an example.

From navigation panel, select **Network >>Ethernet**, then enter “**Fastethernet 0/1**” page, as shown below.

## Network >> Ethernet

Status
Fastethernet 0/1
Fastethernet 0/2

Primary IP
192.168.1.1

Netmask
255.255.255.0

MTU
1500

Speed/Duplex
Auto Negotiation

Track L2 State
☐

Description

Multi-IP Settings

Secondary IP
Netmask

Add

Apply & Save
Cancel

Page description is shown below:

| Parameters        | Description  | Default          |
|-------------------|--|------------------|
| Primary IP        | IP address could be configured or changed according to demand  | 192.168.1.1      |
| Subnet Mask       | Autogeneration   | 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<br>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              |

### 3.3.2 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.

#### 3.3.2.1 Status

From navigation panel, select **Network >>Cellular**, then enter “**Status**” page, as shown below.

| Network >> Cellular |                       |
|---------------------|-----------------------|
| Status              | Cellular              |
| <b>Modem</b>        |                       |
| Active SIM          | SIM 1                 |
| IMEI Code           | 357784044005575       |
| IMSI Code           |                       |
| Phone Number        |                       |
| Signal Level        | ●●●● (0 asu -113 dBm) |
| Register Status     | registering           |
| Operator            |                       |
| Network Type        |                       |
| LAC                 |                       |
| Cell ID             |                       |
| <b>Network</b>      |                       |
| Status              | Disconnected          |
| IP Address          | 0.0.0.0               |
| Netmask             | 0.0.0.0               |
| Gateway             | 0.0.0.0               |
| DNS                 | 0.0.0.0               |
| MTU                 | 1500                  |
| Connection time     | 0 day, 00:00:00       |

### 3.3.2.2 Dialup Port

In “Cellular”page, wireless dialup can be configured.

From navigation panel, select **Network >>Cellular**, then enter “**Cellular**” page, as shown below.

## Network &gt;&gt; Cellular

Status Cellular

|                            | SIM1                                | SIM2                                |
|----------------------------|-------------------------------------|-------------------------------------|
| Profile                    | 1                                   |                                     |
| Roaming                    | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| PIN Code                   | 1234                                |                                     |
| Network Type               | Auto                                |                                     |
| Static IP                  | <input type="checkbox"/>            |                                     |
| Connection Mode            | Always Online                       |                                     |
| Redial Interval            | 10 s                                |                                     |
| ICMP Detection Server      |                                     |                                     |
| ICMP Detection Interval    | 30 s                                |                                     |
| ICMP Detection Timeout     | 5 s                                 |                                     |
| ICMP Detection Max Retries | 5                                   |                                     |
| ICMP Detection Strict      | <input type="checkbox"/>            |                                     |
| Show Advanced Options      | <input type="checkbox"/>            |                                     |

## Profile

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

Advanced Options are shown below:

## Network &gt;&gt; Cellular

Status Cellular

|                       |                                     |
|-----------------------|-------------------------------------|
| Show Advanced Options | <input checked="" type="checkbox"/> |
| Initial Commands      |                                     |
| RSSI Poll Interval    | 120 s                               |
| Dial Timeout          | 120 s                               |
| MTU                   | 1500                                |
| MRU                   | 1500                                |
| Use default asyncmap  | <input type="checkbox"/>            |
| Use Peer DNS          | <input checked="" type="checkbox"/> |
| LCP Interval          | 55 s(0: disable)                    |
| LCP Max Retries       | 5                                   |
| Dual SIM Enable       | <input type="checkbox"/>            |
| Debug                 | <input checked="" type="checkbox"/> |
| Expert Options        |                                     |

## Profile

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

Add



Page description is shown below:

| Parameters                 | Description  | Default       |
|----------------------------|--|---------------|
| Profile                    | Dial-up strategy   | 1             |
| Roaming                    | Enable/Disable roaming   | Enable        |
| PIN Code                   | SIM card PIN code  | None          |
| Network Type               | Three options: Auto, 2G, and 3G  | Auto          |
| Static IP                  | Enable Static IP if your SIM card can get static IP address  | Disable       |
| Connection Mode            | Optional Always Online,connect on demand   | Always Online |
| Redial Interval            | the time interval between first dail fials can redial  | 10s           |
| ICMP Detection Server      | Set ICMP Detection Server  | 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   | 5             |
| ICMP Detection Strict      | No matter whether InRouter have some data receive or transmit, InRouter always send the ICMP probe packet                                | Disable       |
| <b>Profile</b>             |  |               |
| Network Type               | Choose mobile network type   | GSM           |
| APN                        | APN parameters provided by Local ISP, you can set TWO different group of dialup parameters (APN/Username/Password) and set one as backup | 3gnet         |
| Access Number              | APN parameters provided by Local ISP   | *99***1#      |
| Username                   | APN parameters provided by Local ISP   | gprs          |
| Password                   | APN parameters provided by Local ISP   | *****         |
| <b>Advanced Options</b>    |  |               |
| Initial Commands           | Used for advanced parameters   | 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, PPP advanced option   | Disable       |
| Use Peer DNS               | Receiving mobile operators assigned DNS  | Enable        |
| LLCP Interval              | LCP Detection Interval   | 55s           |
| LCP Max Retries            | et the max retries if link detection failed  | 5             |
| Debug                      | System can print a more detailed log   | Enable        |
| Expert Option              | Provide extra PPP parameters, normally user needn't set this.  | None          |
| <b>Dual SIM Cards</b>      |  |               |
| Dual SIM Enable            | Enable dual SIM card mode  | Disable       |
| Main SIM                   | The dual SIM card work mode  | SIM1          |
| Max Number of Dial         | Reach the max number, SIM card will be switched  | 5             |

|                     |   |    |
|---------------------|---|----|
| Min Connected Time  | Set min conected time   | 0s |
| CSQ Threshold       | Set signal strength threshold, the signal strength under this threshold, router will redetect the signal strength | 0  |
| CSQ Detect Interval | Set signal strength detect interval   | 0  |
| CSQ Detect Retries  | Set signal strength detect retries  | 0  |
| Backup SIM Timeout  | From beginning to switch to the backup card counting, exceeds the tiemout, router will switch to the primary card | 0  |

### 3.3.3 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 is PPPoE, namely, configuration interface as PPPoE Client.

From navigation panel, select **Network >>ADSL Dialup**, then enter “**PPPoE**” page, as shown below.

**Network >> ADSL Dialup (PPPoE)**

Status **ADSL Dialup (PPPoE)**

**Dial Pool**

| Pool ID | Interface        |
|---------|------------------|
| 1       | fastethernet 0/1 |

Add

**PPPoE List**

| Enable                              | ID | Pool ID | Authentication Type | Username | Password | Local IP Address | Remote IP Address | Debug                    |
|-------------------------------------|----|---------|---------------------|----------|----------|------------------|-------------------|--------------------------|
| <input checked="" type="checkbox"/> | 1  |         | Auto                |          |          |                  |                   | <input type="checkbox"/> |

Add

Apply & Save Cancel

Page description is shown below:

| Parameters          | Description                               | Default         |
|---------------------|---|-----------------|
| Pool ID             | User define, easy to memorize and manage  | None            |
| Interface           | Fastethernet0/1, Fastethernet0/2          | Fastethernet0/1 |
| <b>PPPoE List</b>   |   |                 |
| ID                  | User define, easy to memorize and manage  | 1               |
| Pool ID             | Same with the dialup pool                 | None            |
| Authentication Type | Auto, PAP, CHAP                           | Auto            |
| User Name           | Operators provide the relevant parameters | None            |

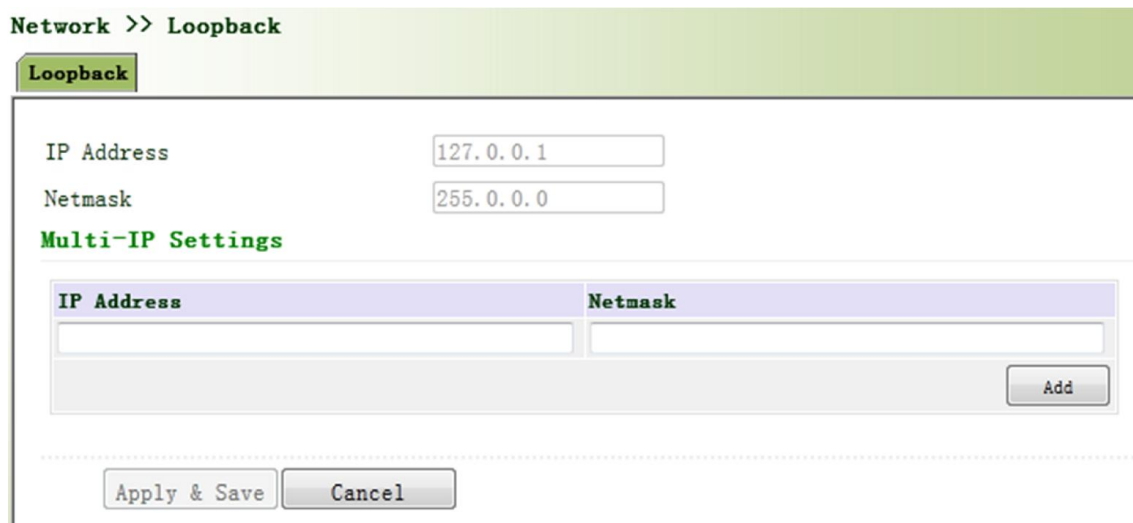
|                   |  |      |
|-------------------|--|------|
| Password          | Operators provide the relevant parameters          | None |
| Local IP Address  | Set the IP address assigned for Ethernet interface | None |
| Remote IP Address | Set the IP of remote device                        | None |

### 3.3.4 Loopback

Loopback Interface is 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. As default, a router has no Loopback Interface which can be created for a number. 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.

From navigation panel, select **Network >> Loopback**, then enter "**Loopback**" page, as shown below.



Page description is shown below:

| 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

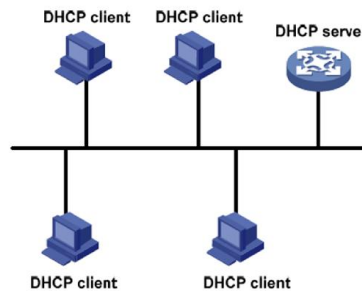
Since loopback interface takes up one IP address, subnet mask is suggested to be 255.255.255.255 for the purpose of saving resources.

### 3.3.5 DHCP service

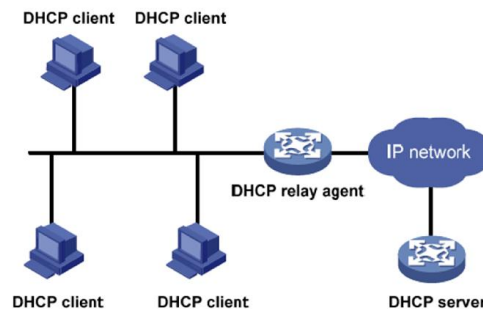
Along with the continuous expansion of network size and complication of network, number of computers often exceeds distributable IP addresses. Meanwhile, in pace with the extensive application of portable devices and wireless network, position of computer changes frequently, resulting to the frequent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

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

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



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



### 3.3.5.1 Status

From navigation panel, select **Network >>DHCP**, then enter “**Status**” page, as shown below.

Network >> DHCP

Status DHCP Server DHCP Relay DHCP Client

| Interface       | MAC Address       | IP Address   | Host | Lease |
|-----------------|-------------------|--------------|------|-------|
| FastEthernet0/2 | 04:7D:7B:08:6D:BB | 192.168.2.32 |      |       |

Manual Refresh Refresh

### 3.3.5.2 DHCP Server

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

From navigation panel, select **Network >>DHCP**, then enter “**DHCP Server**” page, as shown below.

Network >> DHCP

Status DHCP Server DHCP Relay DHCP Client

**DHCP Server**

| Enable                              | Interface        | Starting Address | Ending Address | Lease (Minutes) |
|-------------------------------------|------------------|------------------|----------------|-----------------|
| <input checked="" type="checkbox"/> | fastethernet 0/2 | 192.168.2.2      | 192.168.2.100  | 1440            |
| <input type="checkbox"/>            | fastethernet 0/1 |                  |                | 1440            |

Add

DNS Server  Edit

Windows Name Server (WINS)

**Static IP Settings**

| MAC Address    | IP Address |
|----------------|------------|
| 0000.0000.0000 |            |

Add

Apply & Save Cancel

Page description is shown below:

| Parameters             | Description   | Default         |
|------------------------|---|-----------------|
| Enable                 | On/Off  | Off             |
| Interface              | Fastethernet0/1and Fastethernet0/2 available  | Fastethernet0/1 |
| 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             |
| <b>Static IP Setup</b> |   |                 |
| MAC Address            | Set up a static specified DHCP's MAC address (different from other MACs to avoid confliction) | 0000.0000.0000  |
| IP Address             | Set up a static specified IP address (within the scope from start IP to end IP)               | N/A             |



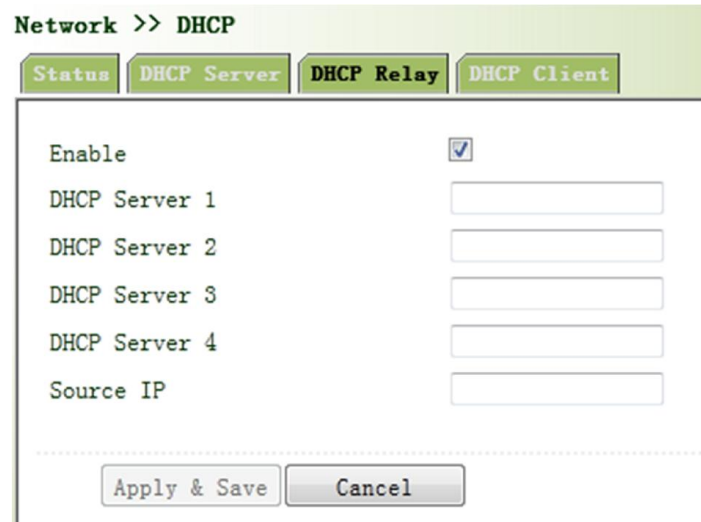
**Attention**

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

### 3.3.5.3 DHCP Relay

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

From navigation panel, select **Network >>DHCP**, then enter “**DHCP Relay**” page, as shown below.



Page description is shown below:

| 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     |

### 3.3.5.4 DHCP Client

DHCP Client obtains an IP address assigned by DHCP server after logging onto it. The IP address is obtained through DHCP.

From navigation panel, select **Network >>DHCP**, then enter “**DHCP Client**” page, as shown below.

**Network >> DHCP**

Fastethernet 0/1 ☐

Fastethernet 0/2 ☐

.....

### 3.3.6 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.

#### 3.3.6.1 DNS Server

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

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

**Network >> DNS**

Primary DNS

Secondary DNS

.....

Page description is shown below:

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

### 3.3.6.2 DNS Relay

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

From navigation panel, select **Network >>DNS**, then enter “**DNS Relay**” page, as shown below.

Page description is shown below:

| 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 relay, DHCP Server has to be closed firstly.

### 3.3.7 Dynamic Domain Name

DDNS is the abbreviation of Dynamic Domain Name Server.

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](http://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.

From navigation panel, select **Network >>DDNS**, then enter “**DDNS**” page, as shown below.

**Network >> DDNS**

**Status** **DDNS**

**DDNS method list**

| Method Name | Service type | Username | Password | hostname |
|-------------|--------------|----------|----------|----------|
|             | Disable      |          |          |          |

Add

**Specify a method to interface**

| Interface  | Method |
|------------|--------|
| cellular 1 |        |

Add

Apply & Save Cancel

Page description is shown below:

| 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    |

### 3.3.8 SMS

SMS permits message-based reboot and manual dialing.

From navigation panel, select **Network >>SMS**, then enter “**Basic**” page, as shown below. 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.

## Network &gt;&gt; SMS

## Basic

Enable ☒

Mode

Poll Interval  s(0: disable)

## SMS Access Control

| ID | Action | Phone Number |
|----|--------|--------------|
| 1  | permit |              |

Add

Apply &amp; Save

Cancel

Page description is shown below:

| 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     |

## 3.4 Link Backup

### 3.4.1 SLA

#### 1. Basic Concepts and Principles

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

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

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

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

routing process. 4. Using static routing and track options.

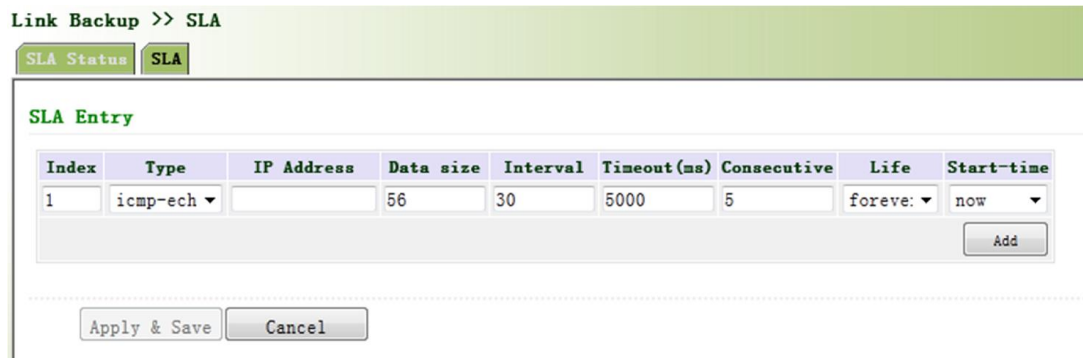
### SLA Configuration Steps

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

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

Step 3: Define measures associated with track objects.

From navigation panel, select **Link Backup>>SLA**, then enter “SLA” page, as shown below.



Page description is shown below:

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

### 3.4.2 Track Module

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

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

### Track Module and Monitoring Module Linkage

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

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

### Track Module and Application Module Linkage

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

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

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

From navigation panel, select **Link Backup>>Track**, then enter “Track” page, as shown below.

Link Backup >> Track

Status
Track

Track Object

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

Add

Apply & Save
Cancel

Page description is shown below:

| 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 (m) | In case of negative status, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching. | 0          |

|                    |  |   |
|--------------------|--|---|
| Positive Delay (m) | In case of failure recovery, switching can be delayed based on the set time (0 represents immediate switching), rather than immediate switching. | 0 |
|--------------------|--|---|

### 3.4.3 VRRP

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

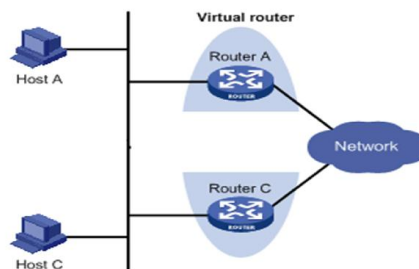
Increasing exit gateway is a common method for improving system reliability. Then, the problem to be solved is how to select route among multiple exits. VRRP (Virtual Router Redundancy Protocol) adds a set of routers that can undertake gateway function into a backup group to form a virtual router. The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

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

VRRP has the following characteristics:

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

VRRP Networking Scheme:



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

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

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

From navigation panel, select **Link Backup>>VRRP**, then enter “VRRP” page, as shown below.

**Link Backup >> VRRP**

VRRP Status VRRP

| Enable                              | Virtual Route ID | Interface        | Virtual IP | Priority | Advertisement Interval | Preemption Mode                     | Track ID |
|-------------------------------------|------------------|------------------|------------|----------|------------------------|-------------------------------------|----------|
| <input checked="" type="checkbox"/> |                  | fastethernet (▼) |            | 100      | 1                      | <input checked="" type="checkbox"/> |          |

Add

Apply & Save Cancel

Page description is shown below:

| 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    |
| Parameters             | Description   | Default |
| 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    |

### 3.4.4 Interface Backup

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

When link state of main interface is switched from up to down, system will wait for preset delay first instead

of switching to link of backup interface immediately. Only if the state of main interface still keeps down after the delay, system will switch to link of backup interface. Otherwise, system will not switch.

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

From navigation panel, select **Link Backup>>Interface Backup**, then enter “**Interface Backup**” page, as shown below.

**Link Backup >> Interface Backup**

**Interface Backup**

| Main Interface   | Backup Interface | Startup Delay | Up Delay | Down Delay | Track id |
|------------------|------------------|---------------|----------|------------|----------|
| cellular 1       | cellular 1       | 60            | 0        | 0          |          |
| cellular 1       |                  |               |          |            |          |
| fastethernet 0/1 |                  |               |          |            |          |
| fastethernet 0/2 |                  |               |          |            |          |

Apply & Save Cancel

Page description is shown below:

| 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 defined Track index or ID  | None       |

## 3.5 Routing

### 3.5.1 Static Route

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



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

Static Routing performs different purposes in different network environments.

- When the network structure is comparatively simple, the network can work normally only with Static Routing.
- While in complex network environment, Static Routing can improve the performance of network and ensure bandwidth for important application.
- Static Routing can be used in VPN examples, mainly for the management of VPN route.

### 3.5.1.1 Static Routing Status

From navigation panel, select **Routing>>Static Routing**, then enter “**Route Table**” page, as shown below.

**Routing >> Static Routing**

**Route Table** **Static Routing**

Type:

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

### 3.5.1.2 Static Routing

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

**Routing >> Static Routing**

**Route Table** **Static Routing**

| Destination          | Netmask              | Interface            | Gateway              | Distance             | Track id             |
|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| 0.0.0.0              | 0.0.0.0              | cellular 1           |                      |                      |                      |
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Page description is shown below:



| 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 defined Track index or ID  | None      |

### 3.5.2 Dynamic Routing

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

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

#### 3.5.2.1 Dynamic Routing status

From navigation panel, select **Routing>>Dynamic Routing**, then enter “**Route Table**” page, as shown below.

| Routing >> Dynamic Routing        |             |               |         |                  |                 |      |
|-----------------------------------|-------------|---------------|---------|------------------|-----------------|------|
| <div> Route Table RIP OSPF </div> |             |               |         |                  |                 |      |
| Type:                             | Connected ▾ |               |         |                  |                 |      |
| Type                              | Destination | Netmask       | Gateway | Interface        | Distance/Metric | Time |
| C                                 | 127.0.0.0   | 255.0.0.0     |         | loopback 1       | 0/0             |      |
| C                                 | 192.168.1.0 | 255.255.255.0 |         | fastethernet 0/1 | 0/0             |      |
| C                                 | 192.168.2.0 | 255.255.255.0 |         | fastethernet 0/2 | 0/0             |      |

#### 3.5.2.2 RIP

RIP (Routing Information Protocol) is a relatively simple interior gateway protocol (IGP), mainly used for smaller networks. The complex environments and large networks general do not use RIP.

RIP uses Hop Count to measure the distance to the destination address and it is called RoutingCost. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to limit the convergence time, the

specified RoutingCost of RIP is an integer in the range of 0~15 and hop count larger than or equal to 16 is defined as infinity, which means that the destination network or host is unreachable. Because of this limitation, the RIP is not suitable for large-scale networks. To improve performance and prevent routing loops, RIP supports split horizon function. RIP also introduces routing obtained by other routing protocols.

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

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

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

From navigation panel, select **Routing>>Dynamic Routing**, then enter “**RIP**” page, as shown below.

The screenshot shows the 'Routing >> Dynamic Routing' configuration window. At the top, there are three tabs: 'Route Table', 'RIP' (which is selected), and 'OSPF'. Below the tabs, there are several configuration options:

- Enable:** A checkbox that is checked.
- Update Timer:** A text box containing '30' followed by a unit 's'.
- Timeout Timer:** A text box containing '180' followed by a unit 's'.
- Garbage Collection Timer:** A text box containing '120' followed by a unit 's'.
- Version:** A dropdown menu set to 'Default'.

Below these options is a section titled 'Network'. It contains a table with two columns: 'IP Address' and 'Netmask'. There are empty text boxes for entering values into these columns. To the right of the table is an 'Add' button.

At the bottom of the window, there is a checkbox labeled 'Show Advanced Options' which is currently unchecked. Below this, there are two buttons: 'Apply & Save' and 'Cancel'.

Advanced Options are shown as below.

Routing >> Dynamic Routing

Route Table
RIP
OSPF

Filter In(Deny Any) ☐  
Filter Out(Permit Default-route Interface) ☐  
Default-Information Originate ☐  
Default Metric   
Distance   
Redistribute Connected ☐  
Redistribute Static ☐  
Redistribute OSPF ☐

Passive default

Passive default ☐

Interface
  
Add

Neighbor

IP Address
  
Add

Page description is shown below:

| Parameters    | Description   | Default |
|---------------|---|---------|
| Enable        | Enable/ Disable   | Disable |
| Update timer  | It defines the interval to send routing updates   | 30      |
| Timeout timer | It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16.  | 180     |
| Clear Timer   | It defines the time from the time when the RoutingCost of a routing becomes 16 to the time when it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the RoutingCost for sending updates of the routing. In case of timeout of Garbage-Collection and the routing still has not been updated, the routing will be completely removed from the routing table. | 120     |

|                               |  |         |
|-------------------------------|--|---------|
| Version                       | Version number of RIP  | V2      |
| Network                       | The first IP address and subnet mask of the segment  | None    |
| <b>Advanced Options</b>       |  |         |
| 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    |
| Neighbor                      | For neighboring routers, after configuring neighbors, rip package will only be sent to neighboring routers | None    |

### 3.5.2.3 OSPF

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

#### Router ID

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

The selection order is as follows:

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

#### Neighbor and Neighboring

After the start-up of OSPF router, it will send out Hello packets through the OSPF interface. Upon receipt of Hello packet, OSPF router will check the parameters defined in the packet. If both are consistent, a neighbor relationship will be formed. Not all both sides in neighbor relationship can

form the adjacency relationship. It is determined based on the network type. Only when both sides successfully exchange DD packets and LSDB synchronization is achieved, the adjacency in the true sense can be formed. LSA describe the network topology around a router, LSDB describe entire network topology.

From navigation panel, select **Routing>>Dynamic Routing**, then enter “OSPF” page, as shown below.

**Routing >> Dynamic Routing**

Route Table **RIP** **OSPF**

Enable ☒

Router ID

Show Advanced Options ☐

**Network**

| IP Address                         | Netmask              | Area ID              |
|------------------------------------|----------------------|----------------------|
| <input type="text"/>               | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                      |                      |

**Interface**

| Interface                          | Cost                            | Hello Interval                  | Dead Interval                   | Network                                | Priority                       | Retransmit Interval            | Transmit Delay                 |
|------------------------------------|---------------------------------|---------------------------------|---------------------------------|--|--------------------------------|--------------------------------|--------------------------------|
| <input type="text"/>               | <input type="text" value="10"/> | <input type="text" value="10"/> | <input type="text" value="40"/> | <input type="text" value="Broadcast"/> | <input type="text" value="1"/> | <input type="text" value="5"/> | <input type="text" value="1"/> |
| <input type="button" value="Add"/> |                                 |                                 |                                 |  |                                |                                |                                |

Page description is shown below:

| Parameters              | Description  | Default |
|-------------------------|--|---------|
| Enable                  | Enable/Disable   | Disable |
| Router ID               | Router ID of the originating the LSA   | None    |
| <b>Advanced Options</b> |  |         |
| 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 |
| <b>Network</b>          |  |         |
| 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    |
| <b>Interface</b>        |  |         |
| Interface               | The interfae   | None    |
| Hello Interval          | Send interval of Hello packet. If the the Hello time between two adjacent routers is different, you can not establish a neighbor relationship. | None    |
| Dead Interval           | Dead Time. If no Hello packet is received from the neighbors, the neighbor is considered failed. If  | None    |

|                     |   |      |
|---------------------|---|------|
|                     | dead times of two adjacent routers are different, the neighbor relationship can not be established.   |      |
| Network             | Select OSPF network type  | None |
| Priority            | Set the OSPF priority of interface  | None |
| Retransmit Interval | When the router notifies an LSA to its neighbor, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbor. | None |

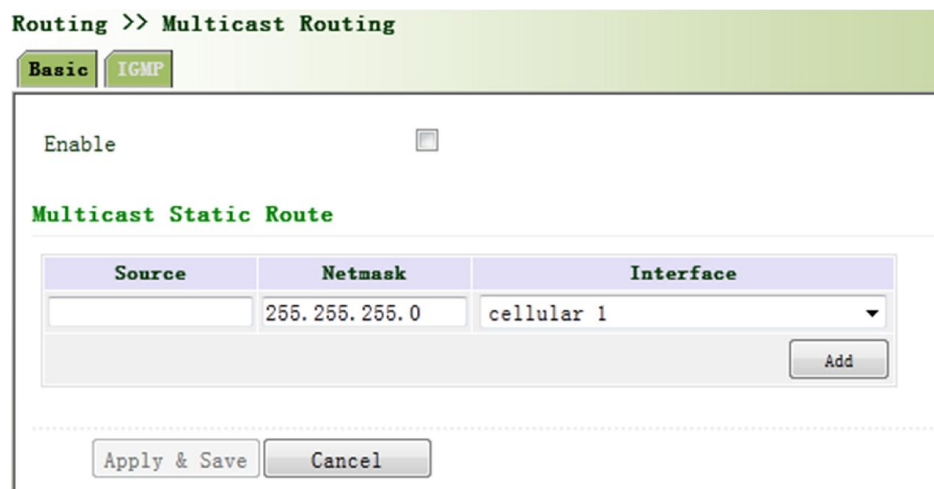
### 3.5.3 Multicast Routing

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

#### 3.5.3.1 Basic

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

From navigation panel, select **Routing>>Multicast Routing**, then enter “**Basic**” page, as shown below.



Page description is shown below:

| 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     |

#### 3.5.3.2 IGMP

IGMP, being a multicast protocol in Internet protocol family, which is used for IP host to report its

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

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

Function of multicast routing protocol:

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

From navigation panel, select **Routing>>Multicast Routing**, then enter “IGMP” page, as shown below.

The screenshot shows the 'Routing >> Multicast Routing' configuration page. It has two tabs: 'Basic' and 'IGMP', with 'IGMP' being the active tab. The page is divided into two main sections: 'Upstream Interface' and 'Downstream Interface List'. In the 'Upstream Interface' section, there is a dropdown menu currently showing 'cellular 1'. The 'Downstream Interface List' section contains a table with two columns: 'Downstream Interface' and 'Upstream Interface'. Both columns have 'cellular 1' selected in their respective dropdowns. Below the table is an 'Add' button. At the bottom of the page are two buttons: 'Apply & Save' and 'Cancel'.

| Downstream Interface | Upstream Interface |
|----------------------|--------------------|
| cellular 1           | cellular 1         |

### 3.6 Firewall

With the expansion of network and increase in flow, the control over network safety and the allocation of bandwidth become the important contents of network management. The firewall function of the router implements corresponding control to data flow at entry direction (from Internet to local area



network) and exit direction (from local area network to Internet) according to the content features of message (such as: protocol style, source/destination IP address, etc.) and ensures safe operation of router and host in local area network.

### 3.6.1 Access Control

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

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

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

From navigation panel, select **Firewall>>ACL**, then enter “ACL” page, as shown below.

Firewall >> ACL

ACL

Access Control List

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

Add Modify Delete

Interface List

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

Add

Apply & Save Cancel

Click <Add> to add new access control list, as shown below.



Firewall >> ACL

ACL

Type

extended ▼

ID

Action

permit ▼

Match Conditions

Protocol

ip ▼

Source IP

Source Wildcard

Destination IP

Destination Wildcard

Fragments

☐

Log

☐

Description

Apply & Save

Cancel

Back

Page description is shown below:

| Parameters        | Description   | Default  |
|-------------------|---|----------|
| Type              | <p><b>Standard ACL</b> can block all communication flows from a network, or allow all communication flows from a particular network, or deny all communication flows of a protocol stack (e.g. IP) of.</p> <p><b>The extended ACL</b> provides a wider range of control than that provided by the standard ACL. For example, if the network administrator wants to "allow external Web communication flows to pass through and reject external communication flows, e.g. FTP and Telnet", the extended ACL can be used to achieve the objective. The standard ACL can not be controlled so precisely.</p> | Extended |
| ID                | User define   | Permit   |
| Action            | Permit/Deny   | Permit   |
| Protocol          | Access Control Protocol   | ip       |
| Source IP Address | IP Address of Source  | None     |
| Destination IP    | IP Address of Destination   | None     |

### 3.6.2 NAT

NAT can achieve Internet access by multiple hosts within the LAN through one or more public

network IP addresses. It means that few public network IP addresses represent more private network IP addresses, thus saving public network IP addresses.

From navigation panel, select **Firewall>>NAT**, then enter “NAT” page, as shown below.

**Firewall >> NAT**

**NAT**

**Network Address Translation(NAT) Rules**

| Action                         | Source Network | Match Conditions | Translated Address |
|--------------------------------|----------------|------------------|--------------------|
| SNAT                           | Inside         | ACL:100          | cellular 1         |
| <div> Add Modify Delete </div> |                |                  |                    |

**Inside Network Interfaces**

| ID               | Interface        |
|------------------|------------------|
| 1                | fastethernet 0/1 |
| 2                | fastethernet 0/2 |
| 3                |                  |
| <div> Add </div> |                  |

**Outside Network Interfaces**

| ID               | Interface  |
|------------------|------------|
| 1                | cellular 1 |
| 2                |            |
| <div> Add </div> |            |

Apply & Save
Cancel

Click **<Add>** to add new NAT rules, as shown below.

**Firewall >> NAT**

**NAT**

Action

SNAT

Source Network

Inside

Translation Type

IP to IP

Match Conditions

IP to IP
IP to INTERFACE
IP PORT to IP PORT
NETWORK to NETWORK
ACL to INTERFACE

Translated Address

IP Address

Apply & Save
Cancel
Back

Page description is shown below:

| Parameters | Description | Default |
|------------|-------------|---------|
|------------|-------------|---------|

|                  |   |          |
|------------------|---|----------|
| Action           | <b>SNAT:</b> Source NAT: Translate IP packet's source address into another address<br><b>DNAT:</b> Destination NAT: Map a set of local internal addresses to a set of legal global addresses.<br><b>1:1NAT:</b> Transfer IP address one to one. | SNAT     |
| Source Network   | Inside: Inside address<br>Outside: Outside address  | Inside   |
| Translation Type | Select the Translation Type   | IP to IP |



### Instruction

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

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

Class A: 10.0.0.0 ~ 10.255.255.255

Class B: 172.16.0.0~ 172.31.255.255

Class A: 192.168.0.0~ 192.168.255.255

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

## 3.7 Qos

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

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

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

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

From navigation panel, select **Qos>>Traffic Control**, then enter “**Traffic Control**” page, as shown below.

## QoS >> Traffic Control

### Traffic Control

#### Classifier

| Name                               | Any Packets              | Source                                      | Destination                                 | Protocol  |
|------------------------------------|--------------------------|---|---|---|
| <input type="text"/>               | <input type="checkbox"/> | <input type="text"/> / <input type="text"/> | <input type="text"/> / <input type="text"/> | <input type="checkbox"/> icmp <input type="checkbox"/> igmp <input type="checkbox"/> tcp <input type="checkbox"/> udp <input type="checkbox"/> gre <input type="checkbox"/><br><input type="checkbox"/> esp <input type="checkbox"/> ah <input type="checkbox"/> ospf <input type="checkbox"/> vrrp <input type="checkbox"/> l2tp |
| <input type="button" value="Add"/> |                          |   |   |   |

#### Policy

| Name                               | Classifier           | Guaranteed Bandwidth (Kbps) | Max Bandwidth (Kbps) | Priority             |
|------------------------------------|----------------------|-----------------------------|----------------------|----------------------|
| <input type="text"/>               | <input type="text"/> | <input type="text"/>        | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                      |                             |                      |                      |

#### Apply QoS

| Interface                          | Ingress Max Bandwidth (Kbps) | Egress Max Bandwidth (Kbps) | Ingress Policy       | Egress Policy        |
|------------------------------------|------------------------------|-----------------------------|----------------------|----------------------|
| cellular 1                         | <input type="text"/>         | <input type="text"/>        | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                              |                             |                      |                      |



Page description is shown below:

| Parameters                 | Description   | Default   |
|----------------------------|---|-----------|
| Name                       | Name  | Name      |
| Any Packets                | Click Startup for flow control to any packets                 | Forbidden |
| Source                     | Source address of flow control                                | N/A       |
| Destination                | Destination address of flow control                           | N/A       |
| Protocol                   | Click to select protocol style                                | N/A       |
| Policy                     |   |           |
| Name                       | Name of user defined flow control strategy                    | N/A       |
| Classifier                 | Name of style defined above                                   | N/A       |
| Guaranteed Bandwidth Kbps  | User defined guaranteed bandwidth                             | N/A       |
| Maximum Bandwidth Kbps     | User defined maximum bandwidth                                | N/A       |
| Local Priority             | Local priority of selection strategy                          | N/A       |
| Apply Qos                  |   |           |
| Interface                  | Selection of flow control interface                           | cellular1 |
| Ingress Max bandwidth Kbps | User define, bigger than maximum bandwidth of input strategy  | N/A       |
| Egress Max bandwidth Kbps  | User define, bigger than maximum bandwidth of output strategy | N/A       |
| Ingress Policy             | Name of policy defined above                                  | N/A       |
| Egress Policy              | Name of policy defined above                                  | N/A       |

## 3.8 VPN

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

### Two Basic Features of VPN:

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

### Fundamental Principle of VPN

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

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

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

### 3.8.1 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 data flows between hosts, between host and gateway, and between gateways. The security protocols of AH and ESP can ensure security and IKE is used for cipher code exchange.

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

#### 3.8.1.1 IPsec Phase 1

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

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

VPN >> IPSec

IPSec Status IPSec Phase 1 IPSec Phase 2 IPSec Setting

**Keyring**

| Name                               | IP Address           | Netmask              | Key                  |
|------------------------------------|----------------------|----------------------|----------------------|
| <input type="text"/>               | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                      |                      |                      |

**Policy**

| ID                                 | Authentication | Encryption | Hash | Diffie-Hellman Group | Lifetime |
|------------------------------------|----------------|------------|------|----------------------|----------|
| <input type="text"/>               | Shared Key     | 3des       | md5  | Group 2              | 86400    |
| <input type="button" value="Add"/> |                |            |      |                      |          |

**ISAKMP Profile**

| Name                               | Negotiation Mode | Local ID Type | Local ID             | Remote ID Type | Remote ID            | Policy               | Keyring              | DPD Interval         | DPD Timeout          |
|------------------------------------|------------------|---------------|----------------------|----------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/>               | Main Mod         | IP Addr       | <input type="text"/> | IP Addr        | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                  |               |                      |                |                      |                      |                      |                      |                      |

Page description is shown below:

| Parameters                  | Description  | Default    |
|-----------------------------|--|------------|
| <b>Keyring</b>              |  |            |
| Name                        | User define key  | N/A        |
| IP Address                  | End-to-end IP address  | N/A        |
| Subnet Mask                 | End-to-end subnet mask   | N/A        |
| Key                         | User define key content  | N/A        |
| <b>Policy</b>               |  |            |
| Identification              | Policy identification of user defined IKE  | N/A        |
| Authentication              | Alternative authentication: shared key and digital certificate   | Shared key |
| Encryption                  | 3des: encrypt plaintext with three DES cipher codes of 64bit<br>des: encrypt a 64bit plaintext block with 64bit cipher code<br>Aes: encrypt plaintext block with AES Algorithm with cipher code length of 128bit, 192bit or 256bit | 3des       |
| Hash                        | md5: input information of arbitrary length to obtain 128bit message digest.<br>sha-1: input information with shorter length of bit to obtain 160bit message digest.<br>Comparing both, md5 is faster while sha-1 is safer.         | md5        |
| Diffie-Hellman Key Exchange | Three options: Group 1, Group 2 and Group 5  | Group 2    |
| Lifetime                    | Active time of policy  | 86400      |

| ISAKMP Profile   |  |            |
|------------------|--|------------|
| Name             | Name of user defined ISAKMP Profile  | N/A        |
| Negotiation Mode | <b>Main mode:</b> as an exchange method of IKE, main mode shall be established in the situation where stricter identity protection is required.<br><b>Aggressive mode:</b> as an exchange method of IKE, aggressive mode exchanging fewer message, can accelerate negotiation in the situation where ordinary identity protection is required. | Main mode  |
| Local ID Type    | Select type of local identification  | IP Address |
| Local ID         | The local ID corresponding to the selected local ID  | N/A        |
| Remote ID Type   | Select type of Remote ID   | IP Address |
| Remote ID        | The Remote ID corresponding to the selected peer identification  | N/A        |
| Policy           | The defined strategy identification in the IKE Strategy list   | N/A        |
| Keyring          | The defined key set in the key set list  | N/A        |
| DPD interval     | Used for detection interval of IPSec neighbor state.<br>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.                      | N/A        |
| DPD Timeout      | Receiving end will make DPD check and send request message automatically to opposite end for check. If it does not receive IPSec cryptographic message from peer end beyond timeout, ISAKMP Profile will be deleted.   | N/A        |



### Instruction

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

### 3.8.1.2 IPsec Phase 2

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

VPN &gt;&gt; IPSec

IPSec Status IPSec Phase 1 IPSec Phase 2 IPSec Setting

Transform-set

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

Add

Apply &amp; Save

Cancel

Page description is shown below:

| Parameters     | Description   | Default     |
|----------------|---|-------------|
| Name           | User define Transform Set name  | N/A         |
| Encapsulation  | Choose encapsulation forms of data packet<br>AH: protect integrity and authenticity of data packet from hacker intercepting data packet or inserting false data packet on the internet.<br>ESP: encrypt the user data needing protection, and then enclose into IP packet for the purpose of confidentiality of data.   | esp         |
| Encryption     | Three options: AES, 3DES, DES   | 3des        |
| Authentication | Alternative authentication: md5 and sha-1   | md5         |
| IPSec Mode     | Tunnel Mode: besides source host and destination host, special gateway will be operated with password to ensure the safety from gateway to gateway.<br><b>Transmission Mode:</b> source host and destination host must directly be operated with all passwords for the purpose of higher work efficiency, but comparing with tunnel mode the security will be inferior. | Tunnel Mode |

### 3.8.1.3 IPsec configuration

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



## VPN &gt;&gt; IPSec

IPSec Status IPSec Phase 1 IPSec Phase 2 IPSec Setting

## IPSec Profile

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

## Crypto Map

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

## Interface &lt;=&gt; Crypto Map

| Map Interface | Map Name |
|---------------|----------|
| cellular 1    | none     |

Apply &amp; Save

Cancel

Page description is shown below:

| Parameters                     | Description   | Default   |
|--------------------------------|---|-----------|
| IPSec Profile                  |   |           |
| Name                           | User define IPSecProfile name   | N/A       |
| ISAKMP Profile                 | ISAKMP Profile names defined in the first stage of parameters of IPSec  | N/A       |
| Transform Set                  | Transform Set defined in the first stage of parameters of IPSec   | N/A       |
| Perfect Forward Security (PFS) | Means the reveal of one cipher code will not endanger information protected by other cipher codes.                              | Forbidden |
| Lifetime                       | Lifetime of IPSecProfile  | N/A       |
| Rekey Margin (S)               | Reconnection time for the second stage  | N/A       |
| Rekey Fuzz (%)                 | Deviation percentage of the reconnection time for the second stage  | N/A       |
| SIM Card Binding               | With this function activated, successful dialing of the card with which IPSec is bonded is a precondition for the use of IPSec. | Forbidden |
| Crypto Map                     |   |           |
| Name                           | User define name of crypto map  | N/A       |
| ID                             | User define ID of crypto map  | N/A       |
| Peer Address                   | Peer IP Address   | N/A       |
| ACL ID                         | ID of ACL defined in ACL of firewall  | N/A       |
| ISAKMP Profile                 | ISAKMP Profile names defined in the first stage of parameters of IPSec  | N/A       |
| Transform Set                  | Transform Set defined in the first stage of parameters of IPSec   | N/A       |
| Perfect Forward Security (PFS) | Means the reveal of one cipher code will not endanger information protected by other cipher codes.                              | Forbidden |
| Lifetime                       | Validity of Crypto Map  | N/A       |

| Rekey Margin (S)         | Reconnection time for the second stage   | N/A       |
|--------------------------|--|-----------|
| Rekey Fuzz ( % )         | Deviation percentage of the reconnection time for the second stage               | N/A       |
| Parameters               | Description  | Default   |
| Interface <=> Crypto Map |  |           |
| MAP Interface            | Select Interface Name  | cellular1 |
| Map Name                 | Select from defined names of Crypto Map. One name is matched with several marks. | none      |

### 3.8.2 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 be encapsulated by GRE to solve the transmission problems between different networks.

**In following circumstances GRE tunnel transmission:**

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

**GRE application example: combined with IPSec to protect multicast data**

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

From navigation panel, select **VPN>>GRE**, then enter “**GRE**” page, as shown below.

VPN >> GRE

GRE

|                  |                                     |
|------------------|-------------------------------------|
| Enable           | <input checked="" type="checkbox"/> |
| Index            | <input type="text"/>                |
| Network Type     | Point to Point ▾                    |
| Local Virtual IP | <input type="text"/>                |
| Peer Virtual IP  | <input type="text"/>                |
| Source Type      | IP ▾                                |
| Local IP         | <input type="text"/>                |
| Peer IP          | <input type="text"/>                |
| Key              | <input type="text"/>                |
| MTU              | <input type="text"/>                |
| NHRP Enable      | <input type="checkbox"/>            |
| IPSec Profile    | Disabled ▾                          |
| Description      | <input type="text"/>                |

Page description is shown below:

| Parameters       | Description  | Default |
|------------------|--|---------|
| Enable           | Click to open  | Open    |
| Index            | Set GRE tunnel name  | None    |
| Network Type     | Select GRE network type  | 点对点     |
| Local Virtual IP | Set Local Virtual IP Address                                     | None    |
| Peer Virtual IP  | Set Peer Virtual IP Address                                      | None    |
| Source Type      | Select source type and set the according IP address or interface | IP      |
| Local IP         | Set Local IP Address   | None    |
| Peer IP          | Set Peer IP Address  | None    |
| Key              | Set the key of tunnel  | None    |
| Description      | Add description  | None    |

### 3.8.3 DMVPN

#### 3.8.3.1DMVPN Introduction

VPN is a combination of MGRE, NHRP and IPSec, shortened as DMVPN. It could provide a low cost safe interconnection plan based on Internet for enterprises and companies with a large number of branches in many cities. Its backbone network adopts Hub and Spoke. Dynamic tunneling is allowed to be established between different branches for data transmission. When two branches are in the same city but the center is in another, data could be directly transmitted between the two branches to reduce delay and consumption of central router, being

much more economical; adding of branches will not change the configuration of the center and other branches while maintenance work is reduced exponentially; branch node could use dynamic IP address for saving IP address resource in public network; dynamic tunnel is featured by a large network scale. Those advantages make it extremely suitable for the safe interconnection of enterprises and companies with a large number of branches in many cities.

### 3.8.3.2 DMVPN Solution

DMVPN is achieved through the combination of multi-point GRE (mGRE) and Next Hop Resolution Protocol (NHRP).

In DMVPN solution, IPsec is used to achieve encryption, GRE or multi-point GRE (mGRE) is used to create a tunnel, and NHRP is used to resolve the problem of dynamic address. DMVPN only requires that the center nodes must apply for a static public IP address.

Next Hop Resolution Protocol (NHRP) is defined in RFC 2332 by the IETF. It is used to obtain the interconnected network layer address and NBMA subnetwork address for reaching the “next hop” of destination nodes for the source node (host or router) on the non-broadcast multiple access (NBMA) network.

- **Automatic Starting of IPsec Encryption**

be encrypted. It means that when there is a data package matching the defined ACL, the IPsec encryption tunnel will be created. When GRE Over IPsec is used, GRE tunnel configuration has included the address of GRE tunnel’s opposite end. This address is also on the address of the opposite terminal of IPsec tunnel. Therefore, it is unnecessary to separately define matching ACL for IPsec. Through binding GRE tunneling with IPsec, once the GRE tunnel is established, IPsec encryption will be immediately triggered.

- **Dynamic Tunnel Establishment of Spoke-to-Hub**

In DMVPN network, there is no branch GRE or IPsec configuration information on the center router, while it is required to configure GRE tunnel according to the external network’s public IP address and NHRP protocol of the center router. When the branch router is energized and started up, the IP address can be obtained through DHCP at ISP, and an IPsec encrypted GRE tunnel can be automatically established and the IP address of external port can be registered at the center router through NHRP. There are reasons in three aspects:

- 1) Since the IP address of branch router’s external network port is automatically obtained, the IP address may be different every time. Therefore, the center router can not be configured based on the address information.
- 2) The center router is not required to configure GRE or IPsec information for all branches, which will greatly simplify the configuration of the center router. All relevant information can be automatically obtained through NHRP.

- 3) In case of DMVPN network expansion, it is not required to change the configuration of the center router and other branch routers. The new branch routers will be automatically registered in the center router. Through the dynamic routing protocol, all other branch routers can learn this new routing and the new branch routers can also learn the routing information to reach all other routers.

- **Dynamic Tunnel Establishment of Spoke-to-Spoke**

In DMVPN network, the Spoke-to-Hub tunnel, once established, will persist, while it is not required to directly configure a continuous tunnel between branches. When a branch wants to transmit data package to another branch, it will use NHRP to dynamically acquire the IP address of destination branch. In this process, the center router acts as the NHRP server to respond to the request of NHRP and provide the public network address of destination branch to the source branch. Hence, an IPSec tunnel can be dynamically established between two branches through the mGRE port for data transmission. The tunnel will be automatically removed after a predefined cycle.

- **Support for Dynamic Routing Protocols**

DMVPN is based on GRE tunnel, while GRE tunnel supports the transmission of multicast or broadcast IP packet in tunnel. Therefore, DMVPN network supports running dynamic routing protocols on IPSec and mGRE tunnels. It should be pointed out that NHRP must be configured as dynamic multicast mapping, so that when the branch router registers unicast mapped address on the NHRP server (center router), NHRP will also establish a multicast / broadcast mapping for the branch router.

We have mentioned above that IPSec tunnel does not support multicast / broadcast packet encapsulation, while GRE tunnel encapsulates multicast / broadcast packet in GRE packet, and GRE packet is a unicast packet and can be encrypted by IPSec. In encryption of GRE packet with IPSec, IPSec can be configured to the transmission mode, because GRE has encapsulated the original packet as the unicast IP packet and it is unnecessary to let IPSec re-encapsulate a header.

The transmission mode IPSec requires that the source and destination addresses of encrypted data packet must match with the addresses of the IPSec tunnel's both terminals. It means that the addresses of the GRE tunnel's both terminals must be the same with those of the IPSec tunnel's both terminals. Since the routers on both terminals of GRE tunnel are the same routers on both terminals of IPSec tunnel, so this can be guaranteed.

Through the combination of GRE tunnel and IPSec encryption, we can utilize the dynamic routing protocol to update the routing tables on the routers at both ends of the encrypted tunnel. The subnet learned from the tunnel peer will contain the IP address of tunnel's opposite terminal as the next hop address of the opposite terminal's subnet. So that, in case of change in the network at any terminal of tunnel, the other end will dynamically learn this change and maintain the connectivity of network without changing the configuration of router.

### 3.8.3.3 Realization of Dynamic Routing Protocol in DMVPN Network

We have mentioned above that in the DMVPN network, the Spoke-to-Hub tunnel, once established, will persist, while there is no persistent tunnel between branches. So that, after the

initialization of router, the center router will announce the reachable routings of other branch subnets to branch routers through the persistent tunnel. Therefore, the "next hop" address reaching other branch subnet in the branch router's routing table will be the address of center router's tunnel port instead of the address of other branch router's tunnel port. Thus, the data transmission between branches will still pass through the center router.

To solve this problem, it is required to set on the center router. When a branch subnet's reachable routing is announced on the port of mGRE tunnel, the "next hop" address is the address of this branch router's tunnel port instead of the address of the center router.

In RIP or EIGRP equidistant vector routing protocol, the function of split horizon is usually achieved, to prevent sending the routing information back to its source port and avoid routing loop on the adjacent routers. If RIP or EIGRP protocol runs on the DMVPN network, it is required to turn off the split horizon function. Otherwise, the branch routers will not be able to learn the routing to the other branch subnets. For RIP, this is enough, because when RIP sends the routing to the routing information source port, its "next hop" address will not be changed and remains to be the original address. When EIGRP sends the routing to the routing information source port, its "next hop" address will change to the address of the port. Therefore, it is necessary to turn off this feature (EIGRP is private protocol of CISCO. The IOS command to turn off this feature is `no ip next-hop-self eigrp`).

OSPF is a link status type routing protocol and itself does not have the problem of split horizon. However, in configuring OSPF network type, it is required to be configured as a broadcast rather than the point-to-multipoint type. Otherwise, the above problems will be caused. In addition, it should also be noted that it is required to configure the center router (Hub) of DMVPN as the designated router (DR) of OSPF, which can be achieved by specifying a higher OSPF priority for the center router (Hub).

### 3.8.4 L2TP

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

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

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

VPN → L2TP → L2TP Client

From navigation panel, select **VPN>>L2TP**, then enter “**L2TP Client**” page, as shown below.



VPN &gt;&gt; L2TP

Status L2TP Client

### L2TP Class

| Name                               | Authentication           | Hostname             | Challenge Secret     |
|------------------------------------|--------------------------|----------------------|----------------------|
| <input type="text"/>               | <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/> |                          |                      |                      |

### Pseudowire Class

| Name                               | L2TP Class           | Source Interface |
|------------------------------------|----------------------|------------------|
| <input type="text"/>               | <input type="text"/> | cellular 1       |
| <input type="button" value="Add"/> |                      |                  |

### L2TP Tunnel

| Enable                              | ID | L2TP Server          | Pseudowire Class     | Authentication Type | Username             | Password             | Local IP Address     | Remote IP Address    |
|-------------------------------------|----|----------------------|----------------------|---------------------|----------------------|----------------------|----------------------|----------------------|
| <input checked="" type="checkbox"/> | 1  | <input type="text"/> | <input type="text"/> | Auto                | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |
| <input type="button" value="Add"/>  |    |                      |                      |                     |                      |                      |                      |                      |



Page description is shown below:

| Parameters              | Description                       | Default    |
|-------------------------|-----------------------------------|------------|
| <b>L2TP Class</b>       |                                   |            |
| Name                    | L2TP class name                   | None       |
| Host Name               | Local host name                   | None       |
| Challenge Secret        | Set challenge secret              | None       |
| <b>Pseudowire Class</b> |                                   |            |
| Name                    | User define Pseudowire Class name | None       |
| Source Interface        | Select source interface name      | cellular 1 |
| <b>L2TP Tunnel</b>      |                                   |            |
| Enable                  | Click to enable                   | Enable     |
| L2TP Server             | Set L2TP Server address           | None       |
| Pseudowire Class        | Pseudowire Class name             | None       |
| Authentication Type     | Select Authentication Type        | Auto       |
| Username                | Peer Server username              | None       |
| Password                | Peer Server password              | None       |
| Local IP Address        | Set local IP address              | None       |
| Remote IP Address       | Set remote IP address             | None       |

### 3.8.5 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 virtual network card through routing mechanism. Upon the reception, service program will receive and process those data and send them out through outer net by SOCKET, owing to which, the remote service program will receive those data and carry out processing, then send them to the virtual network card, then application software receive and accomplish a complete unidirectional transmission, vice versa.

From navigation panel, select **VPN>>OPENVPN**, then enter “**OPENVPN Client**” page, as shown below.

**VPN >> OPENVPN**

**Status** **OPENVPN Client**

|                         |                                      |
|-------------------------|--------------------------------------|
| Index                   | <input type="text"/>                 |
| Server IP               | <input type="text"/>                 |
| Port                    | <input type="text" value="1194"/>    |
| Authentication Type     | <input type="text"/>                 |
| Description             | <input type="text"/>                 |
| Show Advanced Options   | <input checked="" type="checkbox"/>  |
| Source Interface        | <input type="text"/>                 |
| Network Type            | <input type="text" value="net30"/>   |
| Interface Type          | <input type="text" value="tun"/>     |
| Protocol Type           | <input type="text" value="udp"/>     |
| Cipher                  | <input type="text" value="Default"/> |
| Compression LZ0         | <input type="checkbox"/>             |
| Link Detection Interval | <input type="text"/> s               |
| Link Detection Timeout  | <input type="text"/> s               |
| Expert Configuration    | <input type="text"/>                 |

**Import Configuration**

### 3.8.6 Certificate Management

From navigation panel, select **VPN>>Certificate Management**, then enter “**Certificate Management**” page, as shown below.



VPN >> Certificate Management

**Certificate Management**

Certificate Management

Protect Key

Protect Key Confirm

浏览... Import CA Certificate Export CA Certificate

浏览... Import CRL Export CRL

浏览... Import Public Key Certificate Export Public Key Certificate

浏览... Import Private Key Certificate Export Private Key Certificate

浏览... Import PKCS12 Certificate Export PKCS12 Certificate

Apply & Save Cancel

## 3.9 Tools

### 3.9.1 PING

From navigation panel, select **Tools>>Ping**, then enter “**Ping**” page, as shown below.

**Tools >> Ping**

**Ping**

Host  Ping

Ping Count

Packet Size  Bytes

Expert Options

Page description is shown below:

| Parameters  | Description  | Default     |
|-------------|--|-------------|
| Host        | It requires the destination host address of PING detection | 192.168.2.1 |
| Ping Count  | Set Ping detection count                                   | 4           |
| Packet Size | Set packet size of ping detection                          | 32 bytes    |

|                |   |  |
|----------------|---|--|
| Expert Options | Advanced parameters of ping can be used |  |
|----------------|---|--|

### 3.9.2 Routing detection

It is used to detect network routing failure.

From navigation panel, select **Tools>>Traceroute**, then enter “**Traceroute**” page, as shown below.

**Tools >> Traceroute**

**Traceroute**

Host

Maximum Hops

Timeout  s

Protocol

Expert Options

Page description is shown below:

| Parameters     | Description                              | Default     |
|----------------|--|-------------|
| Host           | Host address needs to detect             | 192.168.2.1 |
| Maxium Hops    | Set the maxium hops of routing detection | 20          |
| Timeout        | Set timeout of routing detection         | 3 secs      |
| Protocol       | Select ICMP/UDP                          | UDP         |
| Expert Options | Advanced parameters of ping can be used  |             |

### 3.9.3 Link Speed Test

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

From navigation panel, select **Tools>>Link Speed Test**, then enter “**Link Speed Test**” page, as shown below.

**Tools >> Link Speed Test**

**Link Speed Test**

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

## 3.10 Configuration Wizard

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

### 3.10.1 New LAN

From navigation panel, select **Wizards>>New LAN**, then enter “New LAN” page, as shown below.

Wizards >> New LAN

New LAN

|                  |                                     |
|------------------|-------------------------------------|
| Interface        | fastethernet 0/2 ▼                  |
| Primary IP       | <input type="text"/>                |
| Netmask          | 255.255.255.0                       |
| DHCP Server      | <input checked="" type="checkbox"/> |
| Starting Address | <input type="text"/>                |
| Ending Address   | <input type="text"/>                |
| Lease            | 1440 Minutes                        |

Apply & Save Cancel

### 3.10.2 New WAN

From navigation panel, select **Wizards>>New WAN**, then enter “New WAN” page, as shown below.

Wizards >> New WAN

New WAN

|            |                          |
|------------|--------------------------|
| Interface  | fastethernet 0/1 ▼       |
| Type       | Static IP ▼              |
| Primary IP | <input type="text"/>     |
| Netmask    | 255.255.255.0            |
| Gateway    | <input type="text"/>     |
| NAT        | <input type="checkbox"/> |

Apply & Save Cancel

### 3.10.3 New Cellular

From navigation panel, select **Wizards>>New Cellular**, then enter “**New Cellular**” page, as shown below.

Wizards >> New Cellular

New Cellular

|               |                          |
|---------------|--------------------------|
| APN           | 3gnet                    |
| Access Number | *99***1#                 |
| Username      | gprs                     |
| Password      | ••••                     |
| NAT           | <input type="checkbox"/> |

Apply & Save Cancel

### 3.10.4 New IPSec Tunnel

From navigation panel, select **Wizards>>New IPSec Tunnel**, then enter “**New IPSec Tunnel**” page, as shown below.

## Wizards &gt;&gt; New IPSec Tunnel

## New IPSec Tunnel

|                           |                      |
|---------------------------|----------------------|
| Tunnel ID                 | 1 ▼                  |
| Map Interface             | cellular 1 ▼         |
| Destination Address       | <input type="text"/> |
| Negotiation Mode          | Main Mode ▼          |
| Local Subnet              | <input type="text"/> |
| Local Netmask             | 255.255.255.0        |
| Remote Subnet             | <input type="text"/> |
| Remote Netmask            | 255.255.255.0        |
| <b>Phase 1 Parameters</b> |                      |
| IKE Policy                | 3DES-MD5-DH2 ▼       |
| IKE Lifetime              | 86400 s              |
| Local ID Type             | IP Address ▼         |
| Local ID                  | <input type="text"/> |
| Remote ID Type            | IP Address ▼         |
| Remote ID                 | <input type="text"/> |
| Authentication Type       | Shared Key ▼         |
| Key                       | <input type="text"/> |
| <b>Phase 2 Parameters</b> |                      |
| IPSec Policy              | 3DES-MD5-96 ▼        |
| IPSec Lifetime            | 3600 s               |

## Appendix 1 Troubleshooting

### 1. InRouter is powered on, but can not access Internet through it?

Please check:

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

### 2. InRouter is powered on, have a ping to detect InRouter from your PC and find packet loss?

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

### 3. Forget the setting after revising IP address and can't configure InRouter?

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

Method 2: within 5 seconds after InRouter is powered on, press and hold the Restore button until the ERROR LED flashes, then release the button and the ERROR LED should go off, press and hold the button again until the ERROR LED blinks 6 times, the InRouter is now restored to factory default settings. You may configure it now.

### 4. After InRouter is powered on, it frequently auto restarts. Why does this happen?

Please check:

- ✧ Whether the module works normally.
- ✧ Whether the InRouter is inserted with a SIM card.
- ✧ Whether the SIM card is enabled with data service, whether the service of the SIM card is suspended because of an overdue charge.
- ✧ Whether the dialup parameters, e.g. APN, dialup number, account, and password are correctly configured.
- ✧ Whether the signal is normal.
- ✧ Whether the power supply voltage is normal.

### 5. Why does upgrading the firmware of my InRouter always fail?

Please check:

- ✧ When upgrading locally, check if the local PC and InRouter are in the same network segment.
- ✧ When upgrading remotely, please first make sure the InRouter can access Internet.

### 6. After InRouter establishes VPN with the VPN server, your PC under InRouter can connect to the server, but the center can't connect to your PC under InRouter?

Please make sure the firewall of your computer is disabled.

### 7. After InRouter establishes VPN with the VPN server, Your PC can't connect to the server?

Please make sure "Shared Connection" on "Network=>WAN" or "Network=>Dialup" is enabled in the configuration of InRouter.

### 8. InRouter is powered on, but the Power LED is not on?

- ✧ Check if the protective tube is burn out.
- ✧ Check the power supply voltage range and if the positive and negative electrodes are correctly connected.

**9. InRouter is powered on, but the Network LED is not on when connected to PC?**

- ✧ When the PC and InRouter are connected with a network cable, please check whether a network crossover cable is used.
- ✧ Check if the network cable is in good condition.
- ✧ Please set the network card of the PC to 10/100M and full duplex.

**10. InRouter is powered on, when connected with PC, the Network LED is normal but can't have a ping detection to the InRouter?**

- ✧ Check if the IP Address of the PC and InRouter are in the same subnet and the gateway address is InRouter LAN address.

**11. InRouter is powered on, but can't configure through the web interface?**

- ✧ Whether the IP Address of your computer is the same subnet with InRouter and the gateway address is InRouter LAN address.
- ✧ Check the firewall settings of the PC used to configure InRouter, whether this function is shielded by the firewall.

**12. The InRouter dialup always fails, I can't find out why?**

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

**13. How to restore InRouter to factory default settings?**

- IR900 routers:

1. Press and hold the Restore button, power on InRouter;
2. Release the button until after the STATUS LED flashes and the ERROR LED is on;
3. After the button is released, the ERROR LED will go off, within 30s press and hold the Restore button again until the ERROR LED flashes;
4. Release the button, the system is now successfully restored to factory default settings.

## Appendix 2 Glossary of Terms

| Abbreviation | Full English Name                          | Meaning  |
|--------------|--|--|
| 100Base-TX   | 100Base-TX                                 | 100Mbit / s baseband Ethernet specification uses two pairs of category 5 twisted-pair connection, which can provide the maximum transmission rate of 100Mbit / s   |
| 10Base-T     | 10Base-T                                   | 10Mbit / s baseband Ethernet specification uses two pairs of twisted-pair (category 3/4/5 twisted pair) connection, one of which will be used for sending data and the other for receiving data, which can provide the maximum transmission rate of 10Mbit / s   |
| DDNS         | Dynamic Domain Name Service                | Dynamic Domain Name Service can achieve the resolution between the fixed domain name and the dynamic IP address  |
| DHCP         | Dynamic Host Configuration Protocol        | Dynamic Host Configuration Protocol dynamically assigns IP address, subnet mask, gateway and other information of the host in the network  |
| DHCP Server  | Dynamic Host Configuration Protocol Server | Dynamic Host Configuration Protocol Server is a device running DHCP Dynamic Host Configuration Protocol and is mainly used to assign IP address to the clients of DHCP   |
| DNS          | Domain Name Service                        | Domain Name Service resolves domain name into IP address. DNS information is distributed hierarchically between DNS servers throughout the Internet. When we visit a website, DNS server views the domain name sending the request and searches for the corresponding IP address. If the DNS server can not find the IP address, it will submit the request to the superior DNS server and continue to search for the IP address. For example, the IP address corresponding to the domain name <a href="http://www.yahoo.com">www.yahoo.com</a> is 216.115.108.243 |
| Firewall     | Firewall                                   | Firewall technology protects your computer or local area network from malicious attacks or access from the external network  |
| Abbreviation | Full English Name                          | Meaning  |
| MAC address  | Media Access Control address               | Media Access Control address is the permanent physical address assigned by the manufacturer to the device. It is composed of 6 pairs of hexadecimal digits. For example: 00-0F-E2-80-65-25. Each network device has a global unique MAC address  |
| NAT          | Network Address Translation                | Network Address Translation can convert multiple computers within the LAN through NAT to share one or more public network IP addresses and access to the Internet. This way can not only shield LAN users, but also has the  |



|              |   |  |
|--------------|---|--|
|              |   | effect of network security. Usually, broadband routers sharing the Internet use this technology.   |
| Ping         | Packet Internet Grope                           | Ping command is a diagnostic tool used to test whether the machine can communicate with other computers on the network. Ping command sends message to the specified computer. If the computer receives the message, it will return a response message                                |
| QoS          | Quality of Service                              | Quality of Service is a technology used to solve the problems of network delay and obstruction. In case of network overload or congestion, QoS can ensure that important business volume will not be delayed or discarded, while ensuring efficient operation of network.            |
| RJ-45        | RJ-45   | Standard plug for connecting Ethernet switches, hubs, routers, and other devices. Straight-through cable and crossover cable usually use this connector  |
| Route        | Route   | Select the outgoing interface or gateway that is able to reach the destination network or address through the effective routing based on the destination address of data and the current network conditions for data forwarding. The device with routing functions is called router. |
| SNMP         | Simple Network Management Protocol              | SNMP is a communication rule between the management device and managed device in the network. It defines a series of messages, methods and syntax used to achieve access to and management of managed devices by the management device   |
| Abbreviation | Full English Name                               | Meaning  |
| TCP          | Transfer Control Protocol                       | Transfer Control Protocol is a connection-oriented and reliable transport layer protocol.  |
| TCP/IP       | Transmission Control Protocol/Internet Protocol | Transmission Control Protocol/Internet Protocol is the cluster of basic communication protocols for network communication. TCP / IP defines a set of protocols, including not only TCP and IP  |
| Telnet       | Telnet  | A character-based interactive program used to access a remote host. Telnet allows the user to remotely login and manage the device.  |
| UDP          | User Datagram Protocol                          | User Datagram Protocol is a non-connected based transport layer protocol.  |
| WAN          | Wide Area Network                               | Wide Area Network is a data communication network covering a relatively wide geographical scope, e.g. Internet   |
| LAN          | Local Area Network                              | Local Area Network generally refers to the internal network, e.g. home network, internal network of small and medium-sized enterprises, etc.   |

## Appendix 3 FCC STATEMENT

1. This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

- (1) This device may not cause harmful interference.
- (2) This device must accept any interference received, including interference that may cause undesired operation.

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

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.

This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

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

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

### FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body

## Appendix 4 Important Safety Information

**This product is installed in the restricted environment.**

**Product is not intended for use in the following circumstances**

- Area(s) where radio transmission equipment (such as cell phone) are not permitted.
- Hospitals, health care facilities and area(s) where cell phones are restricted by law.
- Gas stations, fuel storage and places where chemical are stored.
- Chemical plants or places with potential explosion hazard.
- Any metal surface that may weaken the radio signal level.

### **RF safety distance**

- For GPRS router, the compliance boundary distance is  $r=0.26\text{m}$  for GSM 900MHz and  $r=0.13\text{m}$  for DCS 1800 MHz.
- For HSPA router, the compliance boundary distance is  $r=0.26\text{m}$  for GSM 900MHz and
- $r=0.13\text{m}$  for DCS 1800 MHz,  $r=0.094$  for WCDMA 900MHz,  $r=0.063$  for WCDMA 2100MHz.

### **Warning**

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

### **WEEE Notice**

The Directive on Waste Electrical and Electronic Equipment (WEEE), which entered into force as European law on 13th February 2003, resulted in a major change in the treatment of electrical equipment at end-of-life.

The purpose of this Directive is, as a first priority, the prevention of WEEE, and in addition, to promote the reuse, recycling and other forms of recovery of such wastes so as to reduce disposal.

The WEEE logo (shown at the left) on the product or on its box indicates that this product must not be disposed of or dumped with your other household waste. You are liable to dispose of all your electronic or electrical waste equipment by relocating over to the specified collection point for recycling of such hazardous waste. Isolated collection and proper recovery of your electronic and electrical waste equipment at the time of disposal will allow us to help conserving natural resources. Moreover, proper recycling of the electronic and electrical waste equipment will ensure safety of human health and environment.



For more information about electronic and electrical waste equipment disposal, recovery, and collection points, please contact your local city centre, household waste disposal service, shop from where you purchased the equipment, or manufacturer of the equipment.