InRouter315 Industrial Router

User Manual

Issue: V1.0— April, 2024

Declaration

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

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

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

© 2023 InHand Networks. All rights reserved.

Conventions

Symbol	Indication
< >	Content in angle brackets "<>" indicates a button name. For example, the <OK> button.
" "	'' '' indicates a window name or menu name. For example, the pop-up window "New User."
>	A multi-level menu is separated by the double brackets ">". For example, the multi-level menu File > New > Folder indicates the menu item [Folder] under the sub-menu [New], which is under the menu [File].
Cautions	Means reader be careful. Improper action may result in loss of data or device damage.
Note	Notes contain detailed descriptions and helpful suggestions.

Contact Us

Add: 43671 Trade Center Place, Suite 100, Dulles, VA 20166 USA

E-mail: support@inhandneworks.com

T: +1 (703) 348-2988

URL: www.inhandnetworks.com

Contents

I. INTRODUCTION

1.1 Overview

The InRouter315 (IR315) is an IoT cellular router that integrates 4G LTE (cellular1 and cellular2 support Tx/Rx), Wi-Fi, and VPN technologies to provide an easy, reliable, and secure Internet connectivity. With technologies such as 4G wireless wide area network and Wi-Fi wireless local area network, it provides uninterrupted multiple network access capabilities, and with its comprehensive security and wireless services, it realizes up to 10 thousands equipment networking and provides high-speed data access for equipment networking.

This product is suitable for the networking of unattended devices and sites. It is embedded with watchdog and multi-layer link detection mechanisms to ensure reliable and stable communications.

The router can be deployed easily to build large scale networks scaling up to tens of thousands of devices. Using our InHand Device Manager cloud platform, users can manage their network efficiently.

The IR315 can be used in a wide range of industrial and commercial IoT applications, providing an option of good balance between cost and performance.

1.2 Panel Introduction

1.3 LED Indicator & Signal

IR315 LED	Status
PWR	Red off --- Power off Steady in red --- Power on
SYS	Green off --- System error Blink in Green --- System upgrading
Wi-Fi	Green off --- Wi-Fi disable Blink in Green --- Wi-Fi connecting
NET	Green off --- Network disconnected Blink in Green --- Network connecting
Signal	Three green lights steady on --- Dial-up successful, signal strength ≥ 20. Two green lights steady on --- Dial-up successful, 19 ≥ signal

1.4 Reset to default settings

1) When the device is powered on, press the reset button immediately and keep it for

10 seconds until the SYS LED is steady on.

2) Loosen the Reset button and the SYS will off.

3) Immediately press and hold the Reset button, SYS will flash, then loosen the Reset

button. Then device will reset to default settings.

II. INSTALLATION

2.1 PREPARATIPNS

Precautions:

Please be sure there is 3G/4G network coverage and there is no shield on site. 100-240V

AC or 9~36V DC shall be provided on site. First installation shall be done under

direction of the engineer recognized by InHand Networks.

- 1 PC

- 1 or 2 SIM card:

  Ensure the card is enabled with data service and its service is not

  suspended because of an overdue charge.

- Power supply:

  100-240V AC: can be used with DC power adaptor of the device

  9~36V DC: Ripple voltage < 100 mV

- Fixation:

  Please place InRouter on flat level and have it installed in an environment

  with small vibrational frequency.

⚠ Caution

The device shall be installed and operated in powered-off status!

2.2 INSTALLATION

2.2.1 SIM/UIM Card

InRouter315 uses pop-up card holder. Stab the hollow at the left of the card holder and the card holder will pop up. Then, install the SIM/UIM card and press the card holder back to the card slot.

2.2.2 Antenna

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

2.2.3 Power Supply

Upon installation of the antenna, connect the device to 9~36V DC power and see if the Power LED on the panel of the device is on. If not, please contact technical support of InHand Networks immediately.

2.3 LOGIN ROUTER

Upon installation of hardware, be sure the Ethernet card has been mounted in the supervisory PC prior to logging in the page of Web settings of the router.

I. Automatic Acquisition of IP Address (Recommended)

Please set the supervisory computer to "automatic acquisition of IP address" and "automatic acquisition of DNS server address" (default configuration of computer

system) to let the device automatically assign IP address for supervisory computer.

II. Set a Static IP Address

Set the IP address of supervisory PC (such as 192. 168. 2. 2) and LAN interface of device in same network segment (initial IP address of LAN interface of device: 192. 168. 2. 1, subnet mask: 255. 255. 255. 0).

III. Cancel the Proxy Server

If the current supervisory PC uses a proxy server to access the Internet, it is required to cancel the proxy service. The operating steps are shown below:

1) In the browser window, select "tools>>Internet options";

2) select "connection" page and click the button of LAN Settings to enter "LAN Settings" window interface. Please confirm if the option "Use a Proxy Server for LAN" is checked. if it is checked, please cancel and click the button <OK>.

IV. Log in/Exit Web Settings Page

Open IE or other browser and enter IP address of InRouter315, such as http://192.168.2.1 in address bar (default setting of InRouter315). Upon connection, log in from the login interface as Admin, i.e. enter username and password at the login interface (user name /password default: adm/123456).

Note

For security, you are suggested to modify the default login password after the first

login and safe keep the password information.

III. WEB CONFIGURATION

The device need to be effectively configured before using. This chapter will introduce how to configure your router via Web.

3. 1 SYSTEM

Here, system and network state and system time of synchronizing device and PC can be checked and router WEB configuration interface language can be set as well as the name of mainframe of router can be customized.

3.1.1 Basic Setup

Here, WEB configuration interface language can be set; name of mainframe of router can be customized.

From the navigation tree, select System >> Basic Setup, then enter the "Basic Setup" page.

Table 3-1-1 Basic Setup Parameters

Basic settings		
Function description: Select display language of the router configuration interface and set personalized name.		
Parameters	**Description**	**Default**
Language	Configure language of WEB configuration interface	Chinese

Host Name	Set a name for the host or device connected to the router for viewing.	Router

3.1.2 System Time

To ensure the coordination between this device and other devices, user is required to set the system time in an accurate way since this function is used to configure and check system time as well as system time zone. System time is used to configure and view system time and system time zone. It aims to achieve time synchronization of all devices equipped with a clock on network so as to provide multiple applications based on synced time.

From the navigation tree, select System >> Time, then enter the "Time" webpage, as shown below. Click <Sync Time> to synchronize the time of the gateway with the system time of the host.

Table 3-1-2 Parameters of System Time

System Time		
Function description: Set local time zone and automatic updating time of NTP.		
Parameters	**Description**	**Default**
Router Time	Display present time of router	8:00:00 AM, 12/12/2015
PC Time	Display present time of PC	Present time
Timezone	Set time zone of router	Custom
Custom TZ String	Set TZ string of router	CST-8

Auto update Time	Select whether to automatically update time, you may select when on startup or every 1/2/...hours.	On startup
NTP Time Servers	Set NTP server to sync time via network	114.80.81.1

3.1.3 Admin Access

Admin services include HTTP, HTTPS, TELNET, SSHD, HTTP API and Console.

HTTP

HTTP (Hypertext Transfer Protocol) is used for transferring web pages on Internet. After enabling HTTP service on device, users can log on via HTTP and access and control the device using a web browser.

HTTPS

HTTPS (Secure Hypertext Transfer Protocol) is the secure version of hypertext transfer protocol. As a HTTP protocol which supports SSL protocol, it is more secure.

TELNET

Telnet protocol provides telnet and virtual terminal functions through a network. Depending on Server/Client, Telnet Client could send request to Telnet server which provides Telnet services. The device supports Telnet Client and Telnet Server.

SSHD

SSH protocol provides security for remote login sessions and other network services. The SSHD service uses the SSH protocol, which has higher security than Telnet.

HTTP_API

User can check router's status and configure router without login the router remotely by sending HTTP request with HTTP API. Please ask to technical support for more information about HTTP API.

Console (only in IR315-S)

User can access to IR315 CLI via RS232 and enable Console.

From the navigation tree, select System >> Admin Access, then enter "Admin Access" page.

Table3-1-3 Parameters of Admin Access

Admin Access		
Function description: 1. Modify username and password of router. 2. The router may be set by the following 5 ways, i.e. http, https, telnet, SSHD and console. 3. Set login timeout.		
Parameters	**Description**	**Default**
Username/Password		
Username	Set name of user who logs in WEB configuration	adm
Old Password	Previous password access to WEB configuration	123456
New	New password access to WEB configuration	N/A

Password		
Confirm New Password	Reconfirm the new password	N/A
Amin functions		
Service Port	Service port of HTTP/HTTPS/TELNET/SSHD/HTTP_API	80/443/23/22/44 44
Local Access	Enable - Allow local LAN to administrate the router with corresponding service (e.g. HTTP) Disable - Local LAN cannot administrate the router with corresponding service (e.g. HTTP)	Enable
Remote Access	Enable - Allow remote host to administrate the router with corresponding service (e.g. HTTP) Disable - Remote host cannot administrate the router with corresponding service (e.g. HTTP)	Enable
Allowed Access from WAN (Optional)	Set allowed access from WAN	The host controlling service at this moment can be set, e.g. 192.168.2.1/30 or

		192.168.2.1-192. 168.2.10
Descriptio n	For recording significance of various parameters of admin functions (without influencing router configuration)	N/A
Console Login User (Click <new>　button after setting a group of username and password)		
Username	Configure console login user, custom	N/A
Password	Configure the password, custom	N/A
Other Parameters		
Log Timeout	Set login timeout (router will automatically disconnect the configuration interface after login timeout)	500 seconds

Note

● In "Username/Password" section, users can modify username and password rather than create new username, i.e. only this username can be used in logins.

● In "Console Login User" section, we can create multiple usernames, i.e. multiple usernames can be used by serial port or TELNET console logins.

3.1.4 System Log

A remote log server can be set through "System Log Settings," and all system logs will be uploaded to the remote log server through the gateway. This makes remote log software, such as Kiwi Syslog Daemon, a necessity on the host.

Kiwi Syslog Daemon is free log server software for Windows. It can receive, record and display logs from host (such as gateway, exchange board and Unix host). After downloading and installing Kiwi Syslog Daemon, it must be configured through the menus "File >> Setup >> Input >> UDP.

From the navigation tree, select System >> System Log, then enter "System Log" page.

Table 3-1-4   Parameters of System Log

System Log		
Function description: Configure IP address and port number of remote log server which will record router log.		
Parameters	Description	Default
Log to Remote System	Enable log server	Disable
Log server address and port (UDP)	Set address and port of remote log server	N/A: 514
Log to Console	Output device log by serial port	Disable

3.1.5 Config Management

Here you can back up the configuration parameters, import the desired parameters

backup and reset the router.

From the navigation tree, select "System >> Config Management", then enter the

"Config Management" page.

Table 3-1-5   Parameters of Config Management

Config Management		
Function description: Set parameters of configuration management.		
Parameters	**Description**	**Default**
Browse	Choose the configuration file	N/A
Import	Import configuration file to router	N/A
Backup	Backup configuration file to host	N/A
Restore default configuration	Select to restore default configuration (effective after rebooting)	N/A
Disable the hardware reset button	Select to disable hardware reset button of the router	Disable
Modem drive program	For configuring drive program of module	N/A
Network Provider (ISP)	For configuring APN, username, password and other parameters of the network providers across the	N/A

	world	

⚠️ **Caution**

Validity and order of imported configurations should be ensured. The good configs will later be serially executed in order after system reboot. If the configuration files didn't be arranged according to effective order, the system won't enter the desired state.

📝 **Note**

In order not to affect the operation of the current system, when performing an import configuration and restore default configuration, users need to restart the device to make the new configuration to take effect.

3.1.6 Schedule

After this function is enabled, the device will reboot as the scheduled time. Scheduler function will take effect after router sync time.

From the navigation tree, select "System >> Schedule", then enter "Schedule" page.

Table 3-1-6   Parameters of Scheduler

Scheduler		
Function description: set scheduler for system reboot		
Parameters	**Description**	**Default**

Enable	Enable/disable this function	Disable
Time	Select the reboot time	0:00
Days	Reboot the router everyday	Everyday
Show advanced options	Enable more detailed schedule rules, allow to set multiple rules to reboot the router in specific time or interval. Enable this feature will disable everyday reboot feature above.	Disable
Reboot after dialed	Router will reboot after dial up successfully, will not take effort if this parameter is blank.	N/A

3.1.7 Upgrade

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

From the navigation tree, select "System >> Upgrade", then enter the "Upgrade" page.

To upgrade the system, firstly, click <Browse> choose the upgrade file, secondly, click <Upgrade> and then click <OK> to begin upgrade; thirdly, upgrade firmware succeed, and click <Reboot> to restart the device.

3.1.8 Reboot

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

To reboot the system, please click the "System>>Reboot", then click <OK>.

3.1.9 Logout

To logout, click "System >> Logout", and then click <OK>.

3.2 NETWORK

3.2.1 CELLULAR

Insert SIM card and dial to achieve the wireless network connection function of router. Click the "Network>>Dial Interface" menu in the navigation tree to enter the "Dial Interface".

Table3-2-1-1 Parameters of Dialup/Cellular

Dialup/Cellular Connection		
Function description: Configure parameters of PPP dialup. Generally, users only need to set basic configuration instead of advanced options.		
Parameters	Description	Default

Enable	Enable cellular dialup.	Enable
Time Schedule	Set time schedule	ALL
Force Reboot	Router will reboot if cannot dialup for a long time and reach the max retry time	Enable
Shared connection (NAT)	Enable — Local device connected to Router can access to the Internet via Router. Disable — Local device connected to Router cannot access to the Internet via Router.	Enable
Default Route	Enable default route	Enable
SIM1 Network Provider	Select network provider profile for SIM1	Profile 1
Network Type	Select network type, router will try 4G, 3G, 2G in proper order if select in Auto	Auto
Connection Mode	Optional Always Online, Connect On Demand, Manual. It will support to configure Triggered by SMS if select Connect On Demand mode,	Always Online
Redial Interval	Set the redialing time when login fails.	30 s
Show Advanced Options		
Dual SIM Enable	Enable Dual SIM card	Disable

SIM2 Network Provider	Select network provider for SIM2 card	Profile 1
SIM2 Blinding ICCID	Set ICCID of SIM2	N/A
SIM2 PIN Code	For setting SIM2 PIN code	N/A
SIM2 SIM Card Operator	Set the ISP that SIM2 card connects to	Auto
Main SIM	Set the SIM card that uses to dialup at first	SIM1
Max Number of Dial	Set max number of dial, if cannot dial up successfully after this number, router will switch SIM card	5
CSQ Threshold	Set threshold of signal, if current signal level is lower than this, router will switch SIM card	0(Disable)
Min Connect Time	Set the min connect time for each try of dial up	0(Disable)
Initial Commands	Set customize initial AT commands which will be operated at the beginning of dialing up	AT
Blinding ICCID	Set ICCID of SIM	N/A
PIN Code	For setting PIN code of SIM	N/A
MTU	Set max transmission unit after enable	1500

Use Peer DNS	Click to receive peer DNS assigned by the ISP	Enable
Link detection interval	Set link detection interval	55 s
Debug	Enable debug mode, print debug log in system log	Disable
Debug Modem*	Send modem debug data to console	Disable
ICMP Detection Mode	Set ICMP detection mode, router will check the link connection status via ICMP packet. Ignore Traffic: Router will send ICMP packet no matter whether there is traffic in cellular interface. Monitor Traffic: Router will not send ICMP packet if there is traffic in cellular interface.	Ignore Traffic
ICMP Detection Server	Set the ICMP Detection Server. N/A represents not to enable ICMP detection.	N/A
ICMP Detection Interval	Set ICMP Detection Interval	30 s
ICMP Detection Timeout	Set ICMP Detection Timeout (the link will be regarded as down if ICMP times out)	20 s

ICMP Detection Retries	Set the max. number of retries if ICMP fails (router will redial if reaching max. times)	5

*Not all models support this

Table 3-2-1-2 Parameters of Dialup/Cellular - Schedule

Administration of dialup/Cellular - Schedule		
Function description: Online or offline based on the specified time.		
Parameters	**Description**	**Default**
Name of Schedule	schedule 1	schedule1
Sunday ~ Saturday	Click to enable	
Time Range 1	Set time range 1	9:00-12:00
Time Range 2	Set time range 2	14::00-18:00
Time Range 3	Set time range 3	0:00-0:00
Description	Set description content	N/A

3.2.2 WAN

Click the "Network>>WAN" to set WAN port.

WAN supports three types of wired access including static IP, dynamic address (DHCP) and ADSL (PPPoE) dialing.

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.

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.

WAN of the device is disabled by default.

Click the "Network>>WAN" menu in the navigation tree to enter the "WAN"

Interface.

Table 3-2-2-1 Static IP Parameters of WAN

WAN - Static IP		
Function description: Access to Internet via wired lines with fixed IP.		
Parameters	**Description**	**Default**
Shared connection (NAT)	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable

Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address
IP Address	Set IP address of WAN	192.168.1.29
Subnet mask	Set subnet mask of WAN	255. 255. 255. 0
Gateway	Set gateway of WAN	192. 168. 1. 1
MTU	Max. transmission unit, default/manual settings	default (1500)
Multiple IP support (at most 8 additional IP addresses can be set)		
IP Address	Set additional IP address of LAN	N/A
Subnet mask	Set subnet mask	N/A
Description	For recording significance of additional IP address	N/A

Table 3-2-2-2 Dynamic Address (DHCP) Parameters of WAN

WAN - Dynamic Address (DHCP)		
Function description: Support DHCP and can automatically get the address allocated by other routers.		
Parameters	**Description**	**Default**
Shared connection (NAT)	Enable—Local device connected to Router can access to the Internet via Router.	Enable

	Disable—Local device connected to Router cannot access to the Internet via Router.	
Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address
MTU	Max. transmission unit, default/manual settings	default (1500)

Table 3-2-2-3 ADSL Dialing (PPPoE) Parameters of WAN

WAN - ADSL Dialing (PPPoE)		
Function description: Set ADSL dialing parameters.		
Parameters	**Description**	**Default**
Shared connection	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable
Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address

MTU	Max. transmission unit, default/manual settings	default (1492)
WAN - ADSL Dialing (PPPoE)		
Username	Set name of dialing user	N/A
Password	Set dialing password	N/A
Static IP	Click to enable static IP	Disable
Connection Mode	Set dialing connection method (always online, dial on demand, manual dialing)	Always online
Parameters of Advanced Options		
Service Name	Set service name	N/A
Set length of transmit queue.	Set length of transmit queue.	3
Enable IP header compression	Click to enable IP header compression	Disable
Use Peer DNS	Click to enable use peer DNS	Enable
Link detection interval	Set link detection interval	55 s
Link detection Max. Retries	Set link detection max. retries	10
Enable Debug	Click to enable debug	Disable
Expert Option	Set expert options	N/A
ICMP Detection Server	Set ICMP detection server	N/A

ICMP Detection Interval	Set ICMP Detection Interval	30 s
ICMP Detection Timeout	Set ICMP detection timeout	20 s
ICMP Detection Retries	Set ICMP detection max. retries	3

3.2.3 VLAN

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

After set VLAN, click "modify" to configure LAN settings of each VLAN.

Click "Network >> VLAN" to configure VLAN in router.

Table 3-2-3 VLAN Parameters

VLAN		
Function description: Set VLAN parameters for LAN port.		
Parameters	**Description**	**Default**
VLAN ID	Set VLAN ID	1
LAN1~LAN4	Set which LAN port to be a part of VLAN	LAN1~LAN4 enabled
Primary IP/Netmask	Set VLAN's IP and netmask	192.168.2.1/255.255.255.0
Port mode		
MAC	Device's MAC address	Hardware MAC address

Enable	Able to configure Trunk mode after enable	Enable
Speed Duplex	Set speed and duplex of LAN port	Auto Negotiation
Mode	Set LAN mode, Access or Trunk	Access
Native LAN	Traffic will not have VLAN tag if it is transferred by native VLAN	1
GARP		
Enable	Router will send ARP broadcast to LAN devices automatically	Disable
Broadcast Count	Set ARP broadcast times	5
Broadcast Timeout	Set ARP broadcast timeout time	10

Table 3-2-4 LAN Parameters

LAN – Static IP		
Function description: Devices in LAN use static IP to connect to network.		
Parameters	**Description**	**Default**
IP Address	IP Address of router's LAN gateway	192.168.2.1
Netmask	Subnet mask of LAN gateway	255.255.255.0
MTU	Max. transmission unit, default/manual settings	default (1500)
Secondary IP(s) (at most 8 additional IP addresses can be set)		

IP Address	Set additional IP address of LAN	N/A
Subnet mask	Set subnet mask	N/A

3.2.4 Switch WLAN Mode

IR315 supports two types of WLAN mode: AP and STA.

Click the "Network>>Switch WLAN Mode" menu in the navigation tree to set WLAN

mode of the router. After change and save the configuration, please reboot the device

to make the configuration take effort.

3.2.5 WLAN Client (AP Mode)

When working in AP mode, the device WLAN will provide network access point for

other wireless network devices so that they will have normal network communication.

Click the "Network>>WLAN" menu in the navigation tree to enter the "WLAN"

interface.

Table 3-2-5 Parameters of WLAN Access Port

WLAN		
Function description: Support Wi-Fi function and provide wireless LAN access on site and identity authentication of wireless user.		
Parameters	**Description**	**Default**
SSID	After turning on, use can search the WLAN via SSID	Enable

broadcast	name	
Mode	Six type for options: 802. 11g/n, 802. 11g, 802. 11n, 802. 11b, 802. 11b/g , 802. 11b/g/n	802.11b/g/n
Channel	Select the channel	11
SSID	SSID name defined by user	inhand
Authenticatio n method	Support open type, shared type, auto selection of WEP, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA/WPA2, WPAPSK/WPA2PSK	Open type
Encryption	Select encryption method of AP	NONE
Wireless bandwidth	Support 20MHz and 40MHz	20MHz
Enable WDS	Click to enable WDS, router will connect other AP to extend wireless coverage	Disable
Default Route	Click to enable Route	Disable
Bridged SSID	Set bridged SSID of other AP, support to click "Scan" button to connect to available AP in network	None
Bridged BSSID	Set bridged BSSID	None
Scan	Click "Scan" to scan the available AP nearby	
Auth Mode	Open type, shared type, WPA-PSK, WPA2-PSK	Open type
Encryption Method	Support NONE, WEP	None

3.2.6 WLAN Client (STA Mode)

When working in STA mode, the router can access the Internet by connecting to access point. The Router need to reboot after this operation.

Click the "Network>>WLAN Client" menu in the navigation tree to enter the "WLAN" interface. Select "Client" for the interface type and configure relevant parameters. (At this moment, the dialing interface in the "Network>>Dialing Interface" should be closed.)

The SSID scan function is enabled only when Client is selected as WLAN interface. Click "Scan" button to get all available AP and status, select AP and configure corresponding parameter to connect. After configure WLAN Client, please configure access type in "Network>>WAN(STA)".

Table 3-2-6 Parameters of WLAN Client

WLAN Client		
Function description: Support Wi-Fi function and access to wireless LAN as client.		
Parameters	**Description**	**Default**
Mode	Support many modes including 802.11b/g/n	802.11b/g/n
SSID	Name of the SSID to be connected	inhand
Authentication	Keep consistent with the access point	Open type

method	to be connected	
Encryption	Keep consistent with the access point to be connected	NONE

3.2.7 Link Backup

Click the "Network>>Link Backup" in the navigation tree to configuration interface.

Table 3-2-7-1 Parameters of Link Backup

Link Backup		
Function description: When the system runs, main link will first be enabled for communication. However, when the main link is disconnected, the system will automatically switch to the backup link to ensure communication.		
Parameters	**Description**	**Default**
Enable	Click to enable link backup	Disable
Backup mode	Optional hot failover, cold failover or load balance	Hot failover
Main Link	Optional WAN or dialing interface	WAN
ICMP Detection Server	Set ICMP detection server	N/A
Backup Link	Optional cellular or WAN	Cellular 1
ICMP Detection Interval	Set ICMP Detection Interval	10 s
ICMP Detection Timeout	Set ICMP detection timeout	3 s

ICMP Detection Retries	Set ICMP detection max. retries	3
Restart Interface When ICMP Failed	Restart main link when ICMP failed	Disable

Table 3-2-7-2 Parameters of Link Backup - Backup Mode

Link Backup - Backup Mode	
Function description: Select the way of link backup.	
Parameters	**Description**
Hot failover	Main link and backup Link keep online at the same time, switch if current link is off
Cold failover	Backup line will only be online when the main link is disconnected.
Load balance	Transfer data via corresponding route after ICMP detect succeed

3.2.8 VRRP

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 local communicates with the external network through this virtual router.

- A router will be selected from the set of routers based on priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in case of fault of gateway router, thus to guarantee uninterrupted communication between the host and external network.

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

When uplink interface is 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 tree, select "Network >>VRRP" menu, then enter "VRRP" page.

Table 3-2-8 VRRP Parameters

VRRP		
Function description: Configure parameters of VRRP.		
Parameters	**Description**	**Default**
Enable VRRP-I	Click to enable VRRP function	Disable
Group ID	Select ID of router group (range: 1-255)	1
Priority	Select a priority (range: 1-254)	20 (the larger numerical value indicates higher priority)
Advertisement Interval	Set an advertisement interval.	60 s
Virtual IP	Set a virtual IP	N/A
Authentication method	Select "None" or Password type	None (a password is needed when password type is selected)
Monitor	Set monitor	N/A
VRRP-II	Set as above	Disable

3.2.9 IP Passthrough

IP penetration function distributes the address obtained by WAN port to the device at the lower end of LAN port. When external access to the router downstream devices the router transmits data to the downstream device. Click "Network >>IP Passthrough" menu, then enter "IP Passthrough" page.

Table 3-2-9 IP Passthrough Parameters

IP Passthrough		
Function description: LAN port device to obtain WAN port address, used for external access to router downstream devices.		
Parameters	Description	Default
IP Passthrough	Enable IP Passthrough	Disable
IP Passthrough Mode	Select work mode（DHCP Dynamic/DHCP fix MAC)	DHCP Dynamic
Fix MAC Address	Set fix MAC address if in DHCP fix MAC mode	00:00:00:00: 00:00
DHCP lease	Set DHCP lease time and reacquired after expiration	120S

3.2.10 Static Route

Static route needs to be set manually, after which packets will be transferred to appointed routes.

To set static route, click the "Network >> Static Route" menu in the navigation tree, then

enter "Static Route" interface.

Table 3-2-10 Static Route Parameters

Static Route		
Function description: Add/delete additional static rote of router. Generally, it's unnecessary for users to set it.		
Parameters	**Description**	**Default**
Destination Address	Set IP address of the destination	0.0.0.0
Netmask	Set subnet mask of the destination	255.255.255. 0
Gateway	Set the gateway of the destination	N/A
Interface	Select LAN/CELLULAR/WAN/WAN(STA) interface of the destination	N/A
Description	For recording significance of static route address (not support Chinese characters)	N/A

3.2.11 OSPF

The Open Shortest Path First (OSPF) protocol is a link-status-based internal gateway

protocol mainly used on large-scale networks.

Example: Build OSPF route between two routers, and allow their LAN can be accessed

by each other.
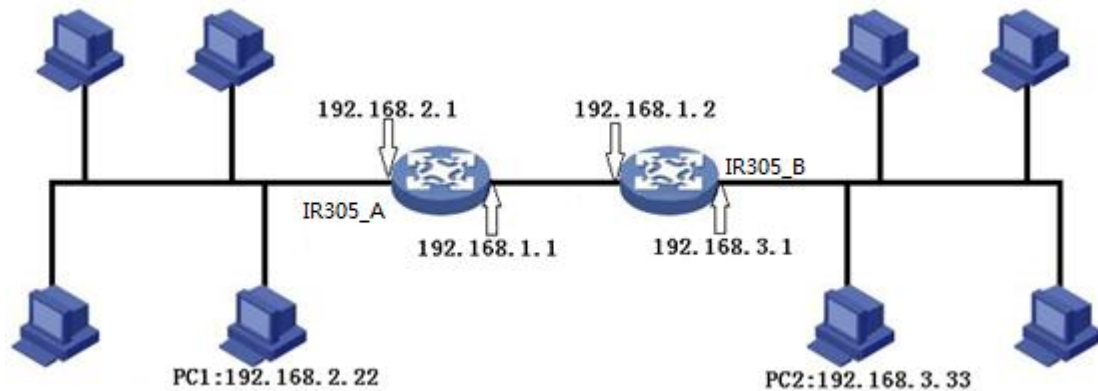
1) Configure IR315_A. Click "Network >> OSPF" to access to OSPF configure page.

"Router ID" should be in the same segment to IR315_B. Configure IR315_A in

"Network" bar to announce the routing entry of the device.

2) Configure IR315_B

3) OSPF has been built successfully if PC1 and PC2 can access to each other.

3.3 SERVICE

3.3.1 DHCP service

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

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

- As DHCP Client, the device receives the IP address distributed by DHCP server after logging in the DHCP server, so the Ethernet interface of the device needs to be

configured into an automatic mode.

To enable the DHCP server, find the navigation tree, select Services >> DHCP Service,
then enter "DHCP Service" page.

Table 3-3-1 Parameters of DHCP Service

DHCP Service		
Function description: If the host connected with router chooses to obtain IP address automatically, then such service must be activated. Static designation of DHCH allocation could help certain host to obtain specified IP address.		
Parameters	**Description**	**Default**
Enable DHCP	Enable DHCP service and dynamically allocate IP address	Enable
IP Pool Starting Address	Set starting IP address of dynamic allocation	192.168. 2.2
IP Pool Ending Address	Set ending IP address of dynamic allocation	192.168.2.10 0
Lease	Set lease of IP allocated dynamically	60 minutes
DNS	Set DNS Server	192.168.2.1
Windows Name Server	Set windows name server.	N/A
Static designation of DHCH allocation (at most 20 DHCPs designated statically can be set)		
MAC Address	Set a statically specified DHCP's MAC	N/A

	address (different from other MACs to avoid confliction)	
IP Address	Set a statically specified IP address	192.168.2.2
Host	Set the hostname.	N/A

3.3.2 DNS

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 makes analysis on dynamic domain name via DNS.

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

Click the "Service>>Domain Name Service" menu in the navigation tree to enter the "Domain Name Service" interface.

Table 3-3-2 DNS Parameters

DNS (DNS Settings)		
Function description: Configure parameters of DNS.		
Parameters	**Description**	**Default**
Primary DNS	Set Primary DNS	0. 0. 0. 0

Secondary DNS	Set Secondary DNS	0. 0. 0. 0
Disable local DNS server	Not to transfer local DNS server address	Disable

3.3.3 DNS Relay

IR315 works as a DNS Agent and relays DNS request and response message between DNS Client and DNS Server to carry out domain name resolution in lieu of DNS Client.

From navigation tree, select "Service>>DNS Relay" menu, then enter "DNS Relay" page.

Table 3-3-3 DNS Transfer Parameters

DNS Relay service		
Function description: If the host connected with router chooses to obtain DNS address automatically, then such service must be activated.		
Parameters	**Description**	**Default**
Enable DNS Relay service	Click to enable DNS service	Enable (DNS will be available when DHCP service is enabled.)
Designate [IP address <=> domain name] pair (20 IP address <=> domain name pairs can be designated)		
IP Address	Set IP address of designated IP address	N/A

	<=> domain name	
Host	Domain Name	N/A
Description	For recording significance of IP address <=> domain name	N/A

⚠ **Caution**

When enabling DHCP, the DHCP relay is also enabled automatically. Relay cannot be

disabled without disabling DHCP.

3.3.4 DDNS

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.

InRouter315 DDNS service types include QDNS (3322)-Dynamic, QDNS(3322)-Static, DynDNS-Dynamic, DynDNS-Static, DynDNS-Custom and No-IP.com.

To set DDNS, click the "Service >> Dynamic Domain Name" menu in the navigation tree, then enter "Dynamic Domain Name" interface.

Table 3-3-4-1 Parameters of Dynamic Domain Name

Dynamic Domain Name		
Function description: Set dynamic domain name binding.		
Parameters	**Description**	**Default**
Current Address	Display present IP of router	N/A
Service Type	Select the domain name service providers	Disable

Table 3-2-4-2 Main Parameters of Dynamic Domain Name

Enable function of dynamic domain name		
Function description: Set dynamic domain name binding. (Explain with the configuration of QDNS service type)		
Parameters	**Description**	**Default**
Service Type	QDNS (3322)-Dynamic	Disable
URL	http://www.3322.org/	http://www.3322.org/

Username	User name assigned in the application for dynamic domain name	N/A
Password	Password assigned in the application for dynamic domain name	N/A
Host Name	Host name assigned in the application for dynamic domain name	N/A
Wildcard	Enable wildcard character	Disable
MX	Set MX	N/A
Backup MX	Enable backup MX	Disable
Force Update	Enable force update	Disable

3.3.5 Device Manager

Inhand provides a software platform to manage devices. The device can be managed and operated via software platform. For instance, the operating status of device can be checked, device software can be upgraded, device can be restarted, configuration parameters can be sent down to device, and transmitting control or message query can be realized on device via Device Manager.

Click the "Service>>Device Manager" menu in the navigation tree to enter the "Device

Manager" interface. North American users should select Servicer address: iot.inhandnetworks.com.

Table 3-3-5 Device remote management platform

Device Manager - Only SMS		
Function description: Configuration of device manager functions can connect the router to the platform		
Parameters	Description	Default
Enable	Enable platform	Disable
Service Type	Platform work mode:	Device Manager
	Device Manager	
	InConnect Service	
	Custom	
Server	Input address of server	Ics.inhand.com.cn
Secure Channel	Enable Secure Channel	Enable
Registered Account	Account registered in Device Manager	N/A
LBS info Upload Interval	Cellular information upload interval	1 Hour
Series Info Upload Interval	Traffic information upload interval	1 Hour
Channel Keepalive	Keep alive packet interval	30 Seconds

3.3.6 SNMP

Network devices are usually sparsely-located on a network. It is time-consuming for the administrator to configure and manage these network devices on site. In addition, if these devices are from different vendors, each of which provides a suite of independent management interfaces (for example, different command line interfaces), the workload of configuring the devices in batches is huge. In this situation, traditional manual configuration method has the deficiencies of high cost and low efficiency. The network administrator can use the Simple Network Management Protocol (SNMP) to remotely configure and manage the devices and perform real-time monitoring on them.
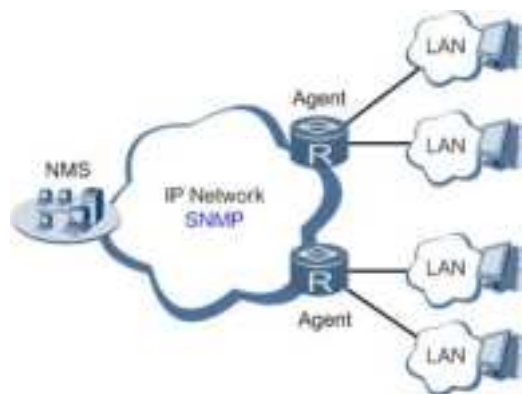
Figure 3- 3-6 SNMP Topology

To run the SNMP protocol on a network, configure the NMS program on the management side and SNMP agent on the managed devices.

By using SNMP:

- The NMS can collect status information of the managed devices anytime and anywhere through agents and remotely control these devices.

- The agents can promptly report the current status and faults of managed devices to the NMS.

Currently, the SNMP agents support SNMPv1, SNMPv2c and SNMPv3. SNMPv1 and SNMPv2c use community names for authentication; SNMPv3 uses user names and passwords for authentication. Click "Service>>SNMP" menu to configure.

Table 3- 3-6-1 SNMPv1 and SNMPv2c Parameters

Parameters	Description	Default
Enable	Enable/disable the SNMP function.	Disabled
Version	Set the version of the SNMP protocol used to manage the router. The versions of SNMPv1, v2c, and v3 are available. SNMPv1 is applicable to small-sized networks with simple networking and low security requirements, or the secure and stable small networks, such as campus networks and small enterprise networks. SNMPv2c is applicable to the medium- and large-sized networks with low security requirements, or with good security (for example, VPNs) but running many services, which may lead to traffic congestion. SNMPv3 is applicable to networks of various sizes, especially the networks that have strict	v1

	security requirements and can be managed only by authorized network administrators. For example, SNMPv3 can be used if data between the NMS and managed device is transmitted over a public network.	
Contact Information	Fill in the contact information.	Empty
Location Information	Fill in the location.	Empty
Community Management		
Community Name	User-defined community name. The community names of SNMPv1 and SNMPv2c are the passwords used by the NMS to read and write data on agents. This parameter must be set the same on both agents and NMS.	public and private
Access Limit	Access limit includes the MIB objects that can be read only or read/written by the NMS.	Read-Only
MIB View	Select the MIB objects that can be monitored and managed by the NMS. Only the default view is supported currently.	defaultView

Table 3- 3-6-2 SNMPv3 Parameters

Parameters	Description	Default
User Group Management		
Groupname	User-defined user group name. The length is 1 to 32 characters.	None
Security Level	Select a security level for the group. The values include NoAuth/NoPriv, Auth/NoPriv, and Auth/Priv.	NoAuth/NoPriv
Read-only View	Select the SNMP read-only view. Only the default view is supported currently.	defaultView
Read-write View	Select the SNMP read-write view. Only the default view is supported currently.	defaultView
Inform View	Select the SNMP inform view. Only the default view is supported currently.	defaultView
Usm Management		
Username	User-defined user name. The length is 1 to 32 characters.	None
Groupname	The group to which a user is added must have been configured in the user group management table.	None
Authentication	Select an authentication mode. Three authentication modes are available: MD5, SHA, and None. If you select None, authentication is disabled.	None
Authenticati	This parameter is available only when the	None

on	authentication mode is not None.	
Password	The length is 8 to 32 characters.	
Encryption	Select the encryption mode. The values are None, AES, and DES.	None
Encryption Password	This parameter is available only when the authentication mode is not None. The length is 8 to 32 characters.	None

3.3.7 SNMP Trap

SNMP trap is a type of entrance. When this entrance is reached, the SNMP managed devices actively notify the NMS, instead of waiting for the polling of NMS. On an SNMP-enabled network, the agents on managed devices can report errors to the NMS anytime, without the need of waiting for the polling of NMS. The errors are reported to the NMS through traps. Click "Service>>SNMP Trap" menu to configure.

Table 3-3-7 SNMP Trap Configuration Parameters

Parameters	Description	Default
Trap Signal Level	Set the trap signal threshold. When this threshold is reached, the agent outputs logs to the NMS.	10
Destination Address	Fill in the IP address of the NMS.	None
Security	Fill in the community name for SNMPv1 or SNMPv2c, and	None

Name	fill in the user name for SNMPv3. The length is 1 to 32 characters.	
UDP Port	Fill in the UDP port number, ranging from 1 to 65535.	162

3.3.8 I/O

Click "Service >> I/O" in the navigation menu to check and configure I/O and relay of the device.

Voltage range:

DI: 0~30V, 0~3V means low, 10~30V means high, and the max input voltage is 30V.

DO: Wet contact, low means 0V, high means 13V (pull up, cannot be used as power supply for other device directly).

Only IR315-<WMNN>-<WLAN/NA> supports this feature.

Table 3-3-8 I/O Parameters

I/O		
Function description: Configuration I/O mode and relay of the device.		
Parameters	**Description**	**Default**
I/O mode	Set I/O mode, input or output	Output
I/O default output level	Set I/O output level when I/O mode is output, low or high	low
Dry/Wet contract	Set I/O input type when I/O mode is input, Dry or Wet contact	Dry
Input triggered	Report when input triggers in some situation	Disable

report		
Trigger edge	Set trigger edge of the relay	Falling edge

3.3.9 DTU RS232/RS485

Configure DTU function, device can transmit serial data to customer's server.

Only IR315-<WMNN>-<WLAN/NA>-S supports this feature.

Table 3-3-9 DTU RS232/RS485 Parameters

DTU RS232/RS485		
Function Description: Transmit RS232 data to server.		
Parameters	**Description**	**Default**
Enable	Enable serial port	Disable
Serial Basic Config		
Serial type	Serial port type, cannot change	RS232 or RS485
Baudrate	Set serial port's baudrate	115200
Data Bits	Set serial port's data bits	8
Parity	Set parity of serial port	None
Stop Bit	Set stop bit of serial port	1
Software Flow	Enable software flow control can avoid data flow	Disable

Control	lost	
DTU Configuration		
Function Description: Configure the protocol of data transmission, take transparent transmission as example		
DTU Protocol	Set the transmit protocol of DTU	Transparent
Protocol	Configure type of protocol, TCP/UDP	TCP
Mode	Set the connection mode between router and server	Client
Frame Interval	Set frame interval of serial	100 ms
Serial Buffer Frames	Set the number of serial buffer frames	4
Keep alive Interval	Set the interval to test the connectivity between router and server	60
Keep alive Retry Time	The number of times to retry when connection lose	5
Multi-Server Policy	The policy for multi server	Parallel
Min Reconnect Interval	Set the min interval to reconnect	15
Max Reconnect Interval	Set the max interval to reconnect	180

DTU ID	The ID of router when connect to server	
Source IP	The source IP router uses when connect to server, will use WAN IP if this parameter is blank	
Source port	The source port router uses when connect to server, will use random port if this parameter is blank	
DTU ID Report Interval	Set the interval to upload DTU ID	0
DTU Serial Port Traffic Statistics	Upload serial port statistics data to "Status/DTU"	Disable
Multi Server		
Function Description: Router can transmit data to multi servers, take transparent transmission as example		
Server Address	Set the server address to receive data	N/A
Server Port	Set the server port to receive data	N/A

3.3.10 SMS

SMS permits message-based reboot and manual dialing. Configure Permit to Phone Number and click <Apply and Save>. After that you can send "reboot" command to restart the device or send custom connection or disconnection command to redial or

disconnect the device.

From navigation tree, select "Service>>SMS" menu, then enter "SMS" page.

Table 3-3-10 SMS Parameters

Short message		
Function description: Configuration SMS function to manage the router in the form of SMS.		
Parameters	**Description**	**Default**
Enable	Click to enable backup DTU function	Disable
Status Query	Users define the English query instruction to inquire current working status of the router.	N/A
Reboot	Users define the English query instruction to reboot the router.	N/A
SMS Access Control		
Default Policy	Select the manner of access processing.	Accept
Phone Number	Fill in accessible mobile number	N/A
Action	Accept or block	Accept
Description	Describe SMS control.	

3.3.11 Traffic Manager

This function is mainly used to count data traffic in cellular interface. If the threshold is 0, router will only count and the rules will not take effort. This function requires enabling

NTP function.

Choose Services >> Traffic Manager to go to the "Traffic Manager" page.

Table 3-3-11 Traffic Manager - Basic Configuration Parameters

Traffic Manager		
Function: Monitor and manage the traffic use of the router.		
Parameters	**Description**	**Default**
Enable	Click to enable the traffic manager function.	Disable
Start Day	The day to start counting data traffic every month	1
Monthly Threshold	Data traffic threshold every month	0MB
When Over Monthly Threshold	Operation when data traffic used within a month reaches the threshold: • Only Reporting • Block Except Management(will not influence DM and management requirement) • Shutdown Interface	Only Reporting
Last 24-Hours Threshold	Data traffic threshold in last 24 Hours	0KB
When Over 24-Hours Threshold	Operation when data traffic used within 24 hours reaches the threshold	Only Reporting
Advance	Custom statistics and operations last several hours	Disable

3.3.12 Alarm Settings

When an abnormality occurs, router will report alarm according to the settings. Currently router supports sending alarm in following situations: System Service Fault, Memory Low, WAN/LAN1 Link-Up/Down, LAN2 Link-Up/Down, Cellular Up/Down, Traffic Alarm, Traffic Disconnect Alarm, SIM/UIM Card Switch, Active Link Switch, SIM/UIM Card Fault, Signal Quality Fault.

In the Alarm Manager interface, you can perform the following operations:

• Select alarm types in the "Alarm Input" area.

• Set the alarm notification method of the console in the "Alarm Output" area.

Choose Services >> Alarm Manager to go to the "Alarm Manager" page.

3.3.13 User Experience Plan

InHand Networks' User Experience Program is designed to improve the product user experience and customer service quality.

User can disable or enable User Experience Plan in "Services >> User Experience Plan".

3.4 FIREWALL

The firewall function of the router implements corresponding control to data flow at entry direction (from Internet to LAN) and exit direction (from LAN 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.

3.4.1 Basic

From the navigation tree, select Firewall >> Basic Setup, then enter the "Basic Setup"

page.

Table 3-4-1 Firewall - Basic Setup Parameters

Basic Setup of Firewall		
Function description: Set basic firewall rules.		
Parameters	**Description**	**Default**
Default Filter Policy	Select accept/block	Accept
Filter PING detection from Internet	Select to filter PING detection	Disable
Filter Multicast	Select to filter multicast function	Enable
Defend DoS Attack	Select to defend DoS attack	Enable
SIP ALG	Select to enable SIP ALG	Disable

3.4.2 Filtering

Filter the network data by customize rules to allow or prohibit the specified data flow

forwarded by router.

To enable Access Control from the navigation tree, select Firewall >> Filtering, then

enter "Filtering" page.

Table 3-4-2 Filtering Parameters

Access Control of Firewall		
Function description: Control the protocol, source/destination address and source/destination port passing through network packet of the router to provide a safe intranet.		
Parameters	**Description**	**Default**
Enable	Check to enable filtering.	Enable
Protocol	Select all/TCP/UDP/ICMP	ALL
Source address	Set source address of access control	0.0.0.0/0
Source Port	Set source port of access control	Not available
Destination Address	Set destination address	N/A
Destination Port	Set destination port of access control	Not available
Action	Select accept/block	Accept
Log	Click to enable log and the log about access control will be recorded in the system	Disable
Description	Convenient for recording parameters of access control	N/A

3.4.3 Device Access Filtering

Set customize rules to allow or prohibit data and access to the router.

From the navigation tree, select Firewall >> Device Access Filtering, then enter "Device Access Filtering" page.

Table 3-4-3 Device Access Filtering Parameters

Device Access Filtering		
Function description: Control the protocol, source/destination address and source/destination port to the router.		
Parameters	**Description**	**Default**
Enable	Check to enable device access filtering.	Enable
Protocol	Select ALL/TCP/UDP/ICMP	ALL
Source	Set source address of network access	0.0.0.0/0
Source Port	Set source port of network access	Not available
Destination	Set destination address	N/A
Destination Port	Set destination port of network access	Not available
Interface	Set interface of network access	All WANs
Action	Select Accept/Block	Accept
Log	Click to enable log and the log about access control will be recorded in the system.	Disable

Description	Convenient for recording parameters of access control	N/A

3.4.4 Content Filtering

Set rules to disable access to specific URLs.

From navigation tree, select "Firewall>>Content Filtering" menu, then enter "Content

Filtering" page.

Table 3-4-4 Content - Filtering Parameters

Filtering		
Function description: Set settings of firewall related to filtering and generally set forbidden URL.		
Parameters	**Description**	**Default**
Enable	Click to enable filtering	Enable
URL	Set URL that needs to be filtered	N/A
Action	Select accept/block	Accept
Log	Click to write log and the log about filtering will be recorded in the system.	Disable
Description	Record the meanings of various parameters of filtering	N/A

3.4.5 Port Mapping

Port mapping is also called virtual server. Setting of port mapping can enable the host

of extranet to access to specific port of host corresponding to IP address of intranet.

To configure port mapping, go into the navigation tree, select "Firewall >> Port Mapping", then enter "Port Mapping" page.

Table 3-4-5 Firewall - Port Mapping Parameters

Port Mapping (at most 100 port mappings can be set)		
Function description: Configure parameters of port mapping.		
Parameters	**Description**	**Default**
Enable	Check to enable port mapping.	Enable
Proto	Select TCP/UDP/TCP&UDP	TCP
Source	Set source address of port mapping	0.0.0.0/0
Service Port	Set service port number of port mapping	8080
Internal Address	Set internal address of port mapping	N/A
Internal Port	Set internal port of port mapping	8080
Log	Click to enable log and the log about port mapping will be recorded in the system.	Disable
External Interface (optional)	Set external interface of port mapping	N/A
External Address (optional)	Set external address/tunnel name of port mapping	N/A
Description	For recording significance of each port mapping rule	N/A

3.4.6 Virtual IP Mapping

Both router and the IP address of the host of intranet can correspond with one virtual IP.

Without changing IP allocation of intranet, the extranet can access to the host of

intranet via virtual IP.   This function is always used with VPN.

To configure virtual IP mapping, go into the navigation tree, select "Firewall >> Virtual

IP Mapping".

Table 3-4-6 Firewall - Virtual IP Mapping Parameters

Virtual IP Address		
Function description: Configure parameters of virtual IP address.		
Parameters	**Description**	**Default**
Virtual IP address of router	Set virtual IP address of router	N/A
Range of source address	Set range of the external source IP addresses.	N/A
Enable	Click to enable virtual IP address	Enable
Virtual IP	Set virtual IP address of virtual IP mapping	N/A
Real IP	Set real IP address of virtual IP mapping	N/A
Log	Click to enable log and the log about virtual IP address will be recorded in the system.	Disable
Description	For recording significance of each virtual IP	N/A

	address rule	

3.4.7 DMZ

After mapping all ports, extranet PC can access to all ports of internal device by DMZ

settings.

From the navigation tree, select Firewall >> DMZ, then enter the "DMZ" page.

Table 3-4-7 Firewall - DMZ Parameters

DMZ		
Function description: Configure DMZ settings.		
Parameters	**Description**	**Default**
Enable DMZ	Check to enable the DMZ.	Disable
DMZ Host	Set address of DMZ Host	N/A
Source Address Range	Enter range of external source address	N/A
Interface	Select external interface of DMZ	N/A

3.4.8 MAC-IP Binding

If the default filter policy in the basic setting of firewall is disabled, only hosts specified

in MAC-IP Binding can have an access to outer net.

From the navigation tree, select Firewall >> MAC-IP Binding, then enter the "MAC-IP

Binding" page.

Table 3-4-8 Firewall - MAC-IP Binding Parameters

MAC-IP Binding (at most 20 MAC-IP Bindings can be set)		
Function description: Configure MAC-IP parameters.		
Parameters	**Description**	**Default**
MAC Address	Set the binding MAC address	00:00:00:00:00:00
IP Address	Set the binding MAC address	192. 168. 2. 2
Description	For recording the significance of each MAC-IP binding configuration	N/A

3.4.9 NAT

NAT is the network address translation function, including source address translation (SNAT) and destination address translation (DNAT).

SNAT refers to the communication between the internal network and the external network when the destination address remains unchanged. DNAT refers to the translation of the destination address of the internal network into the external network without changing the source address when accessing the internal network.

Table 3-4-9 NAT Parameters

NAT		
Function description: Configure parameters of NAT		
Parameters	**Description**	**Default**
Enable	Enable NAT	Enable
Type	Set convert type	SNAT

Proto	Select protocol	TCP
Source IP	Set source IP of the NAT rule	0.0.0.0/0
Source Port	Set source port of the NAT rule	N/A
Destination	Set destination IP of the NAT rule	0.0.0.0/0
Destination Port	Set destination port of the NAT rule	0.0.0.0/0
Interface	Set interface of the NAT rule	N/A
Translated Address	Translate the IP address if match the rule	0.0.0.0
Translated Port	Translate the port if match the rule	N/A

3.5 QoS

To ensure all LAN users can normally get access to network resources, IP traffic control function can limit the flow of specified host in LAN. QoS provides dedicated bandwidth and different service quality for different applications, greatly improving the network service capabilities.

3.5.1 IP BW Limit

Bandwidth control sets a limit on the upload and download speeds when accessing external networks.

From the navigation tree, select QoS >> Bandwidth Control, then enter the "IP BW Limit" page.

Table 3-5-1　Parameters of IP BW Limit

IP Bandwidth Limit		
Function description: Configure parameters of IP bandwidth limit.		
Parameters	**Description**	**Default**
Enable	Click to enable IP bandwidth limit	Disable
Download bandwidth	Set download total bandwidth	1000kbit/s
Upload bandwidth	Set upload total bandwidth	1000kbit/s
Control port of flow	Select CELLULAR/WAN	CELLULAR
Host Download Bandwidth		
Enable	Click to enable	Enable
IP Address	Set IP address	N/A
Guaranteed Rate (kbit/s)	Set rate	1000kbit/s
Priority	Select priority	Medium
Description	Describe IP bandwidth limit	N/A

3.6 VPN

VPN is for building a private dedicated network on a public network via the Internet. "Virtuality" is a logical network.

Two Basic Features of VPN:

- Private: the resources of VPN are unavailable to unauthorized VPN users on the internet; VPN can ensure and protect its internal information from external intrusion.

● Virtual: the communication among VPN users is realized via public network which, meanwhile can be used by unauthorized VPN users so that what VPN users obtained is only a logistic private network.　This public network is regarded as VPN Backbone.

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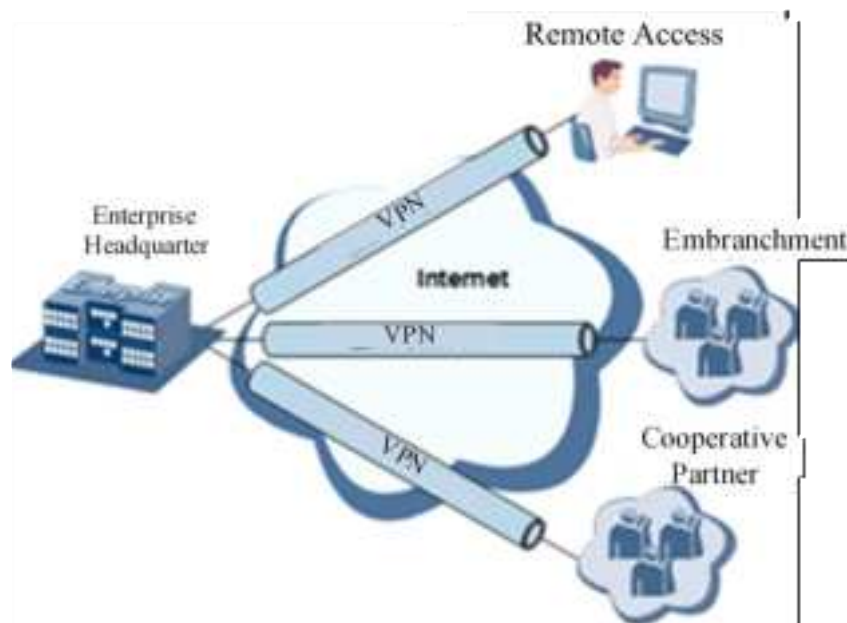
Fundamental Principle of VPN

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

Tunneling technology encloses the other protocol message with one protocol. Also,

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

3.6.1 IPSec Settings

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 via data origin authentication, data encryption, data integrity and anti-replay function on the IP level. It is able to reduce the risk of disclosure and guarantee data integrity and confidentiality and well as maintain security of service transmission of users.

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

IPSec can establish bidirectional Security Alliance on the IPSec peer pairs to form a

secure and interworking IPSec tunnel and to realize the secure transmission of data on

the Internet.

From navigation tree, select VPN>>IPSec Settings, then enter "IPSec Settings" page.

Table 3-6-1 Parameters of IPSec Settings

IPSec settings		
Function description: Select the log level of IPSec.		
Parameters	**Description**	**Default**
Log level	Click to select log level. Normal: Only key log will be printed into system log. Debug: More log in debug level will be printed. Data: All log of IPSec will be printed.	Normal

3.6.2 IPSec Tunnels

From navigation tree, select VPN>>IPSec Tunnels, enter "IPSec Tunnels" and click

<add>.

Table 3-6-2 Parameters of IPSec Tunnels

IPSec Tunnels		
Function description: Configure IPSec tunnels		
Parameters	**Description**	**Default**

Show Advanced Options	Click to enable advanced options	Disable(open advanced options after enabling)
Basic parameters		
Tunnel Name	User defines tunnel name	IPSec_tunnel_1
Destination Address	Set destination IP address or domain name	0. 0. 0. 0
IKE Version	Set IKE version: IKEv1/IKEv2	IKEv1
Startup Modes	Select Auto Activated/Triggered by Data/Passive/Manually Activated	Auto Activated
Restart WAN when failed	Router will restart WAN interface cannot establish IPsec tunnel	Enable
Negotiation Mode (IKEv1)	Select main mode or aggressive mode	Main Mode
IPSec Protocol (Advanced Option)	Select ESP/AH	ESP
IPSec Mode (Advanced Option)	Select tunnel mode/transmission mode	Tunnel Mode
VPN over IPSec (Advanced Option)	Select L2TP over IPSec/GRE over IPSec/None	None
Tunnel Type	Select	Subnet-Subnet

	Host-Host/Host-Subnet/Subnet-Host/Subnet-Subnet	
Local subnet address	Set local subnet IP address	192. 168. 2. 1
Local Subnet Mask	Set local subnet mask	255. 255. 255. 0
Peer Subnet Address	Set peer subnet IP address	0. 0. 0. 0
Peer Subnet Mask	Set remote netmask	255. 255. 255. 0
Phase I Parameters		
IKE Policy	Multiple strategies available	3DES-MD5-DH2
IKE Lifetime	Set IKE lifetime	86400 s
Local ID Type	Select IP address/User FQDN/FQDN Fill in the ID according to the ID type (User FQDN is standard email format)	IP Address
Remote ID Type	Select IP address/User FQDN/FQDN	IP Address
Authentication type	Select shared key/digital certificate	Shared key
Key	Set IPSec VPN key	N/A
XAUTH Parameters (Advanced Option)		
XAUTH Mode	Click to enable XAUTH mode	Disable
XATUTH username	User defines XATUTH username	N/A
XATUTH password	User defines XATUTH password	N/A

MODECFG	Click to enable MODECFG	Disable
Phase II Parameters		
IPSec Policy	Multiple strategies available	3DES-MD5-96
IPSec Lifetime	Set IPSec lifetime	3600 s
Perfect Forward Secrecy (PFS) (Advanced Option)	Select disable/Group 1/Group 2/Group 5	Disable (this needs to match the server)
Link Detection Parameters (Advanced Option)		
DPD Interval	Set time interval.	60 s
DPD Timeout	Set the timeout for dropped packets.	180 s
ICMP Detection Server	Set ICMP detection server	N/A
ICMP Detection Local IP	Set ICMP detection local IP	N/A
ICMP Detection Interval	Set ICMP Detection Interval	60 s
ICMP Detection Timeout	Set ICMP detection timeout	5 s
ICMP Detection Retries	Set ICMP detection max. retries	10

 Note

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.

3.6.3 GRE Tunnels

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

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

In following circumstances GRE tunnel transmission is applied:

- GRE tunnel could transmit multicast data packets as if it were a true network interface.   Single use of IPSec cannot achieve the encryption of multicast.

- A certain protocol adopted cannot be routed.

- A network of different IP address shall be required to connect other two similar networks.

GRE application example: combined with IPSec to protect multicast data

GRE can encapsulate and transmit multicast data in GRE tunnel, but IPSec, currently, could only carry out encryption protection against unicast data. In case of multicast data requiring to be transmitted in IPSec tunnel, a GRE tunnel could be established first for GRE encapsulation of multicast data and then IPSec encryption of encapsulated message so as to achieve the encryption transmission of multicast data in IPSec tunnel. As shown below:
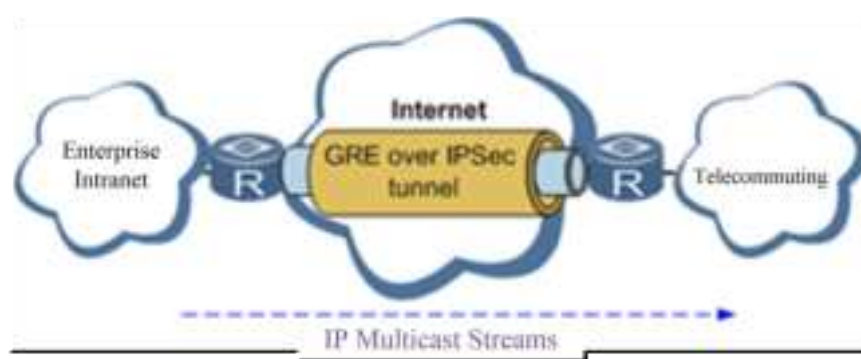
From navigation tree, select VPN>>GRE Tunnels and enter "GRE Tunnels".

Table 3-6-3 Parameters of GRE Tunnels

GRE Tunnels		
Function description: Configure GRE tunnels		
Parameters	**Description**	**Default**
Enable	Click to enable GRE	Enable
Name	User defines name of GRE tunnel	tun0
Local visual IP	Set local virtual IP	0. 0. 0. 0
Destination	Set remote IP address	0. 0. 0. 0

Address		
Peer visual IP	Set peer virtual IP	0. 0. 0. 0
Peer Subnet Address	Set peer subnet IP address	0. 0. 0. 0
Peer Subnet Mask	Set remote netmask	255. 255. 255. 0
Key	Configure the key of GRE tunnel	N/A
NAT	Click to enable NAT	Disable
Description	For recording the significance of each GRE tunnel configuration	N/A

3.6.4 L2TP Client

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

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

L2TP-Layer 2 Tunnel Protocol encapsulates private data from user network at the head

of L2 PPP. No encryption mechanism is available, thus IPSes is required to ensure safety.

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

Typical L2TP network diagram is shown below:
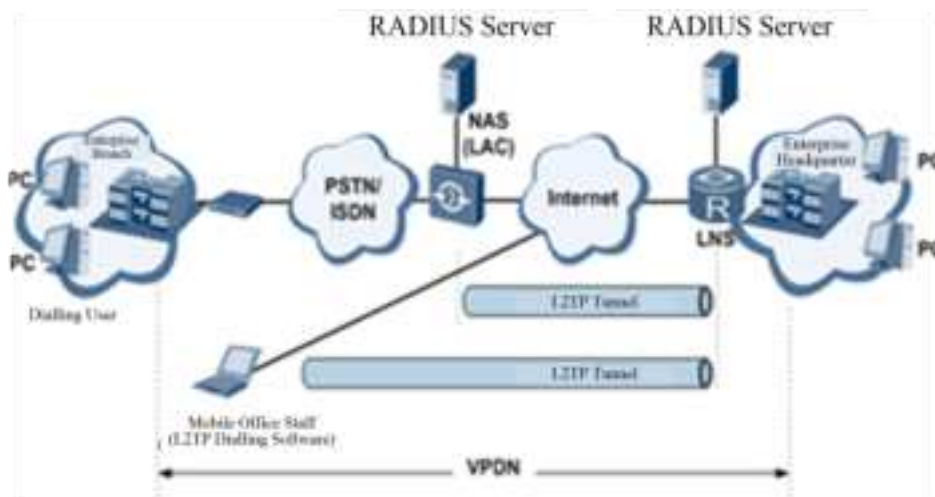
From navigation tree, select VPN>>L2TP Client, enter "L2TP Client" and click <add>.

Table 3-6-4 Parameters of L2TP Client

L2TP Client		
Function description: Configure parameters of L2TP client.		
Parameters	**Description**	**Default**
Enable	Click to enable L2TP client	Disable
Tunnel Name	User defines tunnel name of L2TP client	L2TP_tunnel_1
L2TP Server	Set L2TP Server address	N/A

Username	Set server's username	N/A
Password	Set server's password	N/A
Server Name	Set server name	l2tpserver
Startup Modes	Select Auto Activated/Triggered by Data/Passive/Manually Activated/L2TPOverIPSec	Auto Activated
Authentication Method	Select CHAP/PAP	CHAP
Enable Challenge secrets	Click to enable challenge secrets	Disable
Challenge secret (after enabling)	Set challenge secret	N/A
Local IP Address	Set local IP address	N/A
Remote IP Address	Set remote IP address	N/A
Remote Subnet	Set remote subnet address	N/A
Remote Netmask	Set remote subnet mask	255. 255. 255. 0
Link Detection Interval	Set link detection interval	60 s
Max. Retries for Link Detection	Set the max. number of retries	5
Enable NAT	Click to enable NAT	Disable
MTU	Set max. transmission unit	1500
MRU	Set max. receiving unit	1500
Enable Debug	Enable debug mode.	Disable

Expert Option (not recommended)	Set expert option, not recommended	N/A

3.6.5 PPTP Client

From navigation tree, select VPN>>PPTP Client, enter "PPTP Client" and click <add>.

Table 3-6-5 Parameters of PPTP Client

PPTP Client		
Function description: Configure parameters of PPTP client.		
Parameters	**Description**	**Default**
Enable	Click to enable PPTP client	Disable
Tunnel Name	User defines tunnel name	PPTP_tunnel_1
PPTP Server	Set PPTP Server address	N/A
Username	Set username of PPTP server	N/A
Password	Set password of PPTP server	N/A
Startup Modes	Select Auto Activated/Triggered by Data/Passive/Manually Activated	Auto Activated
Authentication method	Select Auto/CHAP/PAP/MS-CHAPv1/MS-CHAPv2	Auto
Local IP Address	Set local IP address	N/A
Remote IP Address	Set remote IP address	N/A
Remote Subnet	Set remote subnet address	N/A

		255. 255.
Remote Netmask	Set remote subnet mask	255. 0
Link Detection Interval	Set link detection interval	60 s
Max. Retries for Link Detection	Set the max. number of retries	5
Enable NAT	Click to enable NAT	Disable
Enable MPPE	Click to enable MPPE	Disable
Enable MPPC	Click to enable MPPC	Disable
MTU	Set max. transmission unit	1500
MRU	Set max. receiving unit	1500
Enable Debug	Enable debug mode.	Disable
Set expert option (not recommended)	Set expert option, not recommended	N/A

3.6.6 OpenVPN

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

In OpenVPN, if a user needs to access to a remote virtual address (address family matching virtual network card), then OS will send the data packet (TUN mode) or data

frame (TAP mode) to the visual network card through routing mechanism. Upon the

reception, service program will receive and process those data and send them out

through outer net by SOCKET, owing to which, the remote service program will receive

those data and carry out processing, then send them to the virtual network card, then

application software receive and accomplish a complete unidirectional transmission,

vice versa.

From navigation tree, select "VPN>>OpenVPN", then enter "OpenVPN" page, and

click <Add>.

Table 3-6-6 IPSec Configuration Parameters

OpenVPN		
Function description: Configure OpenVPN parameters.		
Parameters	**Description**	**Default**
Tunnel Name	OpenVPN tunnel name, cannot be changed by the system	OpenVPN_T_1
Enable	Click to enable	Enable
Mode	Client/server	Client
Protocol	UDP/ICMP	UDP
Port	Set port	1194
OPENVPN Server	Set OPENVPN Server address	N/A
Authentication method	N/A pre-shared key	N/A

| | username/password

digital certificate (multiple client)

digital certificate

username and digital certificate | |
|---|---|---|
| Local IP Address | Set local IP address | N/A |
| Remote IP Address | Set remote IP address | N/A |
| Remote Subnet | Set remote subnet address | N/A |
| Remote Netmask | Set remote subnet mask | 255.   255.   255.   0 |
| Link Detection Interval | Set link detection interval | 60 s |
| Link   Detection Timeout | Set link detection timeout | 315 s |
| Enable NAT | Click to enable NAT | Enable |
| Enable LZO | Click to enable LZO compression | Enable |
| Encryption Algorithms | Blowfish(128)/DES(128)/3DES(192)/AES(128)/AES(192)/AES(256) | Blowfish(128) |
| MTU | Set max. transmission unit | 1500 |
| Max. Fragment Size | Set max. fragment size | N/A |
| Debug Level | Error/warning/information/debug | Warning |
| Interface Type | TUN/TAP | TUN |
| Expert   Option   (not recommended) | Set expert option, not recommended | N/A |

3.6.7 OpenVPN Advanced

From navigation tree, select "VPN>>OpenVPN Advanced" and enter "OpenVPN Advanced" interface.

Table 3-6-7 Configuration Parameters of OpenVPN Advanced

OpenVPN Advanced		
Function description: Configure parameters of OpenVPN Advanced.		
Parameters	**Description**	**Default**
Enable Client-to-Client (Server Mode Only)	Click to enable	Disable
Client Management		
Enable	Click to enable client management	Enable
Tunnel Name	Set tunnel name	OpenVPN_T_1
Username/CommonName	Set username/commonname	N/A
Password	Set client password	N/A
Client IP (4th byte must be 4n+1)	Set client IP address	N/A
Local Static Route	Set local static route	N/A
Remote Static Route	Set remote static route	N/A

3.6.8 WireGuard Tunnels

WireGuard is a new generation VPN which aims at providing more efficient and more

security VPN service with advanced encryption algorithm.

Click Add button to configure and create WireGuard tunnel, and check the VPN status

in this page.

From navigation tree, select VPN >> WireGuard Tunnels, then enter WireGuard VPN

configure page.

Table 3-6-8 WireGuard Configure Parameters

WireGuard Tunnels		
Function description: Configure WireGurad VPN.		
Parameters	**Description**	**Default**
Tunnel Name	Set the name of WireGuard tunnel	WireGuard_tun_1
Enable	Enable/Disable tunnel	Enable
Address	Local virtual IP address and mask in CIDR format, for example 192.168.2.1/24	N/A
Shared Connection(NAT)	Enable — Local device connected to Router can access to the Internet via this tunnel.	Enable

	Disable — Local device connected to Router cannot access to the Internet via this tunnel.	
Listening Port	VPN port, system will listen to default port (51820) if this parameter is blank. Different tunnel needs to use different listening port.	51820
Private Key	Private key generated by WireGuard	N/A
MTU	MTU of VPN packet	1500
Peer Parameters		
Name	Name of VPN peer side	N/A
End Point	IP address and port of remote side, for example 1.2.3.4:51820	N/A
Allowed IPs	Limit the local address that can access via this tunnel	0.0.0.0/0(all)
Public Key	Generated by WireGuard, is corresponding to the local private key	N/A
Pre-shared Key(Optional)	Generated by WireGuard, can increase the security of the tunnel	N/A
Persistent Keepalive	Keep alive interval when enable NAT, 0 means disable	25
WireGuard Key Generator		

Click Generate button to create private key, public key or pre-shared key by

WireGuard. It is also supports to create public key after entering private key.

Private key is used in local tunnel parameters, public key is used in peer public key.

3.6.9 ZeroTier VPN

ZeroTier VPN supports user to build a network that allow all client devices to access to

each other. There are two network types in ZeroTier VPN, planet and moon. In planet

network, user needs to login and create VPN network in https://www.zerotier.com/ at

first. Moon network is private VPN network created by user.

From navigation tree, select VPN >> ZeroTier VPN, then enter "ZeroTier VPN"

configure page.

Table 3-6-9 ZeroTier VPN Parameters

ZeroTier VPN		
Function description: Configure parameters of ZeroTier VPN.		
Parameters	**Description**	**Default**
Enable	Click to enable/disable ZeroTier VPN	Disable
Tunnel Name	Set local VPN tunnel name to identify tunnel	N/A
Network Type	Select network type: planet or moon	planet
Network ID	Set network ID (16 letters) to connect to VPN server	N/A

3.6.10 Certificate Management

From navigation tree, select VPN >> Certificate Management, then enter "Certificate

Management" page.

Table 3-6-10 Parameters of Certificate Management

Certificate Management		
Function description: Configure parameters of certificate management.		
Parameters	**Description**	**Default**
Enable SCEP (Simple Certificate Enrollment Protocol)	Click to enable	Disable
Protect Key	Set protect key	N/A
Protect Key Confirm	Confirm protect key	N/A
Enable SCEP (Simple Certificate Enrollment Protocol)		
Force to Re-enroll	Click to enable force to re-enroll	Disable
Request Status	The system is "ready to refile an enrollment", cannot be changed	Ready to refile an enrollment
Server URL	Set server URL	N/A
Common Name	Set common name	N/A
FQDN	Set FQDN	N/A
Unit 1	Set unit 1	N/A

Unit 2	Set unit 2	N/A
Domain	Set domain	N/A
Serial Number	Set serial number	N/A
Challenge	Set challenge	N/A
Challenge Confirm	Challenge confirm	N/A
Protect Key	Set protect key	N/A
Protect Key Confirm	Confirm protect key	N/A
Unstructured address	Set unstructured address	N/A
RSA Key Length	Set RSA key length	1024
Poll Interval	Set poll interval	60 s
Poll Timeout	Set poll timeout	3600 s
Import/Export Certificate		
Import CA Certificate	Manually import local CA to the router	N/A
Export CA Certificate	Manually export CA to local computer	N/A
Import CRL	Manually import CRL to the router	N/A
Export CRL	Manually export CRL to local computer	N/A
Import Public Key Certificate	Manually import Public Key Certificate to the router	N/A
Export Public Key Certificate	Manually export Public Key Certificate to local computer	N/A
Import Private Key Certificate	Manually import Private Key Certificate to the router	N/A

Export Private Key Certificate	Manually export Private Key Certificate to local computer	N/A
Import PKCS12	Manually import PKCS12 to the router	N/A
Export PKCS12	Manually export PKCS12 to local computer	N/A

Note: When using certificate, please make sure the time of the router is sync with real time.

3.7 TOOLS

3.7.1 PING

To do a ping, enter the navigation tree, select Tools>>Ping Detection, then enter the "Ping Detection" page.

Table 3-7-1 PING Detection Parameters

PING Detection		
Function description: PING outside network.		
Parameters	**Description**	**Default**
Host	Address of the destination host of PING detection is required.	N/A
PING Count	Set the PING count	4
Packet Size	Set the size of PING detection	32 bytes
Expert Option	Advanced parameter of PING is	N/A

	available.	

3.7.2 Traceroute

To perform traceroute, select "Tools>>Traceroute" menu in the navigation tree, then enter the "Traceroute" page.

Table 3-7-2 Traceroute Parameters

Traceroute		
Function description: Applied for network routing failures detection.		
Parameters	**Description**	**Default**
Host	Address of the destination host which to be detected is required.	N/A
Maximum Hops	Set the max. hops for traceroute	20
Timeout	Set the timeout of traceroute	3 s
Protocol	ICMP/UDP	UDP
Expert Option	Advanced parameter for traceroute is available.	N/A

3.7.3 Link Speed Test

Enter the navigation tree, select "Tools>>Link Speed Test", then enter the "Link Speed Test" page.

Select a file locally and click upload/download, then check the network speed in log.

3.7.4 TCPDUMP

Enter the navigation tree, select "Tools>>TCPDUMP", then enter the TCP dump page.

Table 3-7-4　TCPDUMP Parameters

TCPDUMP		
Function description: Capture the packet transferring through specific interface		
Parameters	**Description**	**Default**
Interface	Select the interface to capture the packet	ANY
Capture number	Stop TCP dump after capture this number of packets	10
Expert Option	Advanced parameter for TCPDUMP	N/A

3.8 APPLICATION

3.8.1 Smart ATM

Select Application >> Smart ATM, then enter the "Smart ATM" page. You can set the configuration about ATM platform.

Table 3-8-1　Smart Parameters

Smart ATM		
Function description: configure parameters for docking intelligent ATM cloud platform		
Parameters	**Description**	**Default**

Smart ATM	Enable Smart ATM	disable
Server	Configure parameters of server,Click Edit to show more information	iot.inhand.com.cn
Enable SSL proxy	Enable proxy of SSL	diable
Multi Server	Click add to set multi server	N/A
Protocol	Configure listener protocol type standard 1/3,Visa Standard 3	Standard 1/3
TLS Encryption	Enable TLS encryption	Enable
Get TID	Matching TID	Disable
Incoming TCP Port	Set TCP Port of inbound direction	N/A
Outgoing IP/Host	Set IP/Host name of outbound direction	N/A
Outgoing TCP Port	Set TCP Port of outbound direction	N/A
Outgoing Backup TCP Port	Set Backup TCP Port of outbound direction	N/A
Outgoing TCP Source Port	Set TCP Source port of outbound direction	0 (All)

3.8.2 Status Report

Select Application >> Status Report, then enter the "Status Report" page. You can set the configuration about Status Report.

Table 3-8-2 Smart Report Parameters

Status Report		
Function description: Monitor device status and Report to cloud platform		
Parameters	**Description**	**Default**
Status Report	Enable status upload service	Disable
Server	Set server name	N/A
Server Port	Set server port	N/A
Username	Set user name	test
User Password	Set user password	test
Status info Upload Interval	Time of upload interval	60 second
Protocol	Monitor protocol type	TCP
Log Enable	Enable log	Close
HTTP API	Enable HTTP API	OPEN
Show router report args settiong	Setting status upload message	Disable
Router hostname	show router name	Disable
Router serial number	Show router serial number	Enable
Cellular ip address	Show cellular ip address	Enable
Signal strength	Show signal strength	Enable
Terminal ID	Show terminal ID	Disable
MNC、MCC、Cell ID、LAC	Show MNC、MCC、Cell ID、LAC	Disable

Uptime	Uptime	
Current firmware version	Show current firmware version	Disable
Timestamp	Show timestamp	Disable
Advice config	Set advance config	N/A

3.8.3 Smart-EMS

Select Application >> Smart-EMS, then enter the "Smart-EMS" page. You can set the

configuration about Smart-EMS.

Table 3-8-3 Smart-EMS Parameters

Smart-EMS		
Function description: configure parameters for docking intelligent Smart-EMS cloud platform		
Parameters	**Description**	**Default**
Server URL	Fill in server address	N/A
Username	Fill in user name	N/A
Password	Fill in user password	N/A
Contact interval	Set time of contacting interval	N/A
Send running config	Enable send run configuration	Disable
Write startup	Enable write startup	Disable

3.9 STATUS

3.9.1 System

From navigation tree, select Status >> System, then enter the "System" page. This page displays system statistics, including name, model, serial number, description, current version, current Bootloader version, router time, PC time, UP time, CPU load and memory consumption. Technicians may click the <Sync Time> button to synchronize the router with the system time of the host, as covered in the set-up chapter.

3.9.2 Modem

From navigation tree, select Status >> Modem, then enter the "Modem" page. This page displays the basic information of dialup, including status, signal level, register status, IMEI (ESN) code, IMSI code, LAC and cell ID.

Click Status >> Modem, then enter the "Modem" page to configure parameters.

3.9.3 Traffic Statistics

Choose Status >> Traffic Statistics to go to the "Traffic Statistics" page to query traffic statistics. This page displays the traffic statistics on the dialing interface, including the statistics on the traffic received in the latest month, traffic transmitted in the latest month, traffic received on the last day, traffic transmitted on the last day, traffic received in the last hour, and traffic transmitted in the last hour.

3.9.5 DTU

Only IR315 serial type supports this page.

Choose Status >> DTU to go to the "DTU" page to check serial connection status.

3.9.5 Alarm

Choose Status >> Alarm to go to the "Alarm" page to view all alarms generated in the

system since power-on. You can clear or confirm the alarms.

The alarms have the following states:

- Raise: indicates that the alarm has been generated but not been confirmed.

- Confirm: indicates that the alarm cannot be solved currently.

- All: indicates all generated alarms.

The alarms are classified into the following levels:

- EMERG: The device undergoes a serious error that causes a system reboot.

- CRIT: The device undergoes an unrecoverable error.

- WARN: The device undergoes an error that affects system functions.

- NOTICE: The device undergoes an error that affects system performance.

- INFO: A normal event occurs.

3.9.6 WLAN

Choose Status >> WLAN to go to the "WLAN" page to query the WLAN connection status. This page displays the WLAN connection information, including channel, SSID, BSSID, security, signal (%), mode, and status.

3.9.7 Network Connections

From navigation tree, select Status >> Network Connections, then enter "Network Connections" page to see the connections status. This page shows the basis information of dialup and LAN. WAN includes MAC address, connection type, IP address, netmask, gateway, DNS, MTU, Status and etc. Dialup includes connection type, IP address, netmask, gateway, DNS, MTU, status and connection time. LAN includes connection type, MAC address, IP address, netmask, gateway, MTU and DNS.

3.9.8 Device Manager

From navigation tree, select Status >> Device Manager, then enter "Device Manager" page to check the connections status between router and Device Manager.

3.9.9 Route Table

From navigation tree, select Status >> Route Table, then enter "Route Table" page to see router status. This page displays the active route table, including destination, netmask, gateway, metric and interface.

3.9.10 Device List

From navigation tree, select Status >> Device List, then enter "Device List" page to inquire the device list. This page displays the device list, including interface, MAC address, IP address, host and lease (click MAC address to link to IEEE to inquire validity of the address).

3.9.11 Log

From navigation tree, select Status >> Log, then enter "Log" page. This page displays the logs, including select to see the number of log lines (20/50/……/all), log level (information, debug and warning), time, module and content. Clear log, download log file, download system diagnosis record (refresh rate of this page is 5/10/…… 1min by default).

3.9.11 Third Party Software Notices

From navigation tree, select Status >> Third Party Software Notices, then enter "Third Party Software Notices" page to check the third party software used in router system.

Appendix A FAQ

1. InRouter is powered on, but can't access Internet through it?

Please first 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, username 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 goes 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?

First 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, username 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?

Examination:

✧ 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 under InRouter can't connect to the server ping?

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.

✧ Please check whether your IE has any third-party plugin (e.g. 3721 and IEMate). It is recommended to configure after unloading the plugin.

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?

The method to restore InRouter to factory default settings:

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 B Instruction of Command Line

1 Help Command

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

1.1 Help

[Command] Help [<cmd>]

[Function] Get help from command.

[View] All views

[Parameter]

      <cmd> command name

[Example]

  ✧ Enter:

help

    Get the list of all current available command.

  ✧ enter:

    help show

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

2 View Switchover Command

2.1 Enable

[Command] Enable [15 [<password>]]

[Function] Switchover to privileged user level.

[View] Ordinary user view.

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

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

[Example]

    Enter exit in ordinary user view:

    enable 123456

    Switchover to super users and the password 123456.

2.2 Disable

[Command] Disable

[Function] Exit the privileged user level.

[View] Super user view, configure view

[Parameter] No

[Example]

      Enter in super user view:

      disable

      Return to ordinary user view.

2. 3 End and !

[Command] End or !

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

[View] Configure view.

[Parameter] No

[Example]

      Enter in configured view:

      end

      Return to super user view.

2. 4 Exit

[Command] Exit

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

[View] All views

[Parameter] No

[Example]

  ✧ Enter in configured view:

      exit

      Return to super user view.

  ✧ enter exit in ordinary user view:

      exit

      Exit console.

3 Check system state command

3. 1 Show version

[Command] Show version

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

[View] All views

[Parameter] No

[Example]

Enter:

show version

Display the following information:

Type : display the current factory type of equipment

Serial number : display the current factory serial number of equipment

Description : www.inhand.com.cn

Current version : display the current version of equipment

Current version of Bootloader: display the current version of equipment

3. 2 Show system

[Command] Show system

[Function] Display the information of router system

[View] All views

[Parameter] No

[Example]

Enter:

show system

Display the following information:

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

3. 3 show clock

[Command] Show clock

[Function] Display the system time of router

[View] All views

[Parameter] No

[Example]

Enter:

show clock

Display the following information:

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

3. 4 Show modem

[Command] Show modem

[Function] Display the MODEM state of router

[View] All views

[Parameter] No

[Example]

Enter:

show modem

Display the following information:

Modem type

state

manufacturer

Product name

signal level

register state

IMSI number

Network Type

3. 5 Show log

[Command] Show log [lines <n>]

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

[View] All views

[Parameter]

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

[Example]

Enter:

show log

Display the latest 100 log records.

3. 6 Show users

[Command] Show users

[Function] Display the user list of router.

[View] All views

[Parameter] No

[Example]

Enter:

show users

Displayed user list of system is as follows:

User:

----

* adm

Wherein, user marked with * is super user.

3. 7 Show startup-config

[Command] Show startup-config

[Function] Display the starting device of router.

[View] Super user view and configuration view

[Parameter] No

[Example]

   Enter:

   show startup-config

   Display the starting configuration of system.

3. 8 Show running-config

[Command] Show running-config

[Function] Display the operational configuration of router

[View] Super user view and configuration view

[Parameter] No

[Example]

   Enter:

   show startup-config

   Display the operational configuration of system.

4 Check Network Status Command

4. 1 Show interface

[Command] Show interface

[Function] Display the information of port state of router

[View] All views

[Parameter] No

[Example]

   Enter:

   show interface

   Display the state of all ports.

4. 2 Show ip

[Command] Show ip

[Function] Display the information of port state of router

[View] All views

[Parameter] No

[Example]

   Enter:

   Show ip

   Display system ip status

4. 3 Show route

[Command] Show route

[Function] Display the routing list of router

[View] All views

[Parameter] No

[Example]

enter:

show route

Display the routing list of system

4. 4 Show arp

[Command] Show arp

[Function] Display the ARP list of router

[View] All views

[Parameter] No

[Example]

Enter:

show arp

Display the ARP list of system

5 Internet Testing Command

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

5. 1 Ping

[Command] Ping <hostname> [count <n>] [size <n>] [source <ip>]

[Function] Apply ICMP testing for appointed mainframe.

[View] All views

[Parameter]

<hostname> tests the address or domain name of mainframe.

count <n> testing times

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

source <ip> IP address of appointed testing

[Example]

Enter:

ping www.g.cn

Test www. g. cn and display the testing results

5. 2 Telnet

[Command] Telnet <hostname> [<port>] [source <ip>]

[Function] Telnet logs in the appointed mainframe

[View] All views

[Parameter]

<hostname> in need of the address or domain name of mainframe logged in.

                <port>telnet port

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

[Example]

        Enter:

        telnet 192.168.2.2

        telnet logs in 192. 168. 2. 2

5. 3 Traceroute

[Command] Traceroute <hostname> [maxhops <n>] [timeout <n>]

[Function] Test the acting routing of appointed mainframe.

[View] All views

[Parameter]

        <hostname> tests the address or domain name of mainframe.

        maxhops <n> tests the maximum routing jumps

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

[Example]

        Enter:

        traceroute www.g.cn

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

6 Configuration Command

    In super user view, router can use configure command to switch it over configure view for management.

    Some setting command can support no and default, wherein, no indicates the setting of canceling some parameter and default indicates the recovery of default setting of some parameter.

6. 1 Configure

[Command] Configure terminal

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

[View] Super user view

[Parameter] No

[Example]

        Enter in super user view:

        configure terminal

        Switchover to configuration view.

6. 2 Hostname

[Command] Hostname [<hostname>]

        default hostname

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

[View] Configure view.

[Parameter]

        <hostname> new mainframe name

[Example]

    ✧   Enter in configured view:

      hostname

      Display the mainframe name of router.

    ✧   Enter in configured view:

      hostname MyRouter

      Set the mainframe name of router MyRouter.

    ✧   Enter in configured view:

      defaulthostname

      Recover the mainframe name of router to the factory setting.

6. 3 Clock timezone

[Command] Clock timezone <timezone><n>

      default clock timezone

[Function] Set the time zone information of the router.

[View] Configure view.

[Parameter]

      <timezone> timezone name, 3 capitalized English letters

      <n> time zone deviation value, -12~+12

[Example]

    ✧   Enter in configured view:

      clock timezone CST -8

      The time zone of IG601is east eighth area and the name is CST (China's standard time).

    ✧   Enter in configured view:

      default clock timezone

      Recover the timezone of router to the factory setting.

6. 4 Ntp server

[Command]

      ntp server <*hostname*>

      no ntp server

      default ntp server

[Function] Set the customer end of Internet time server

[View] Configure view.

[Parameter]

      <hostname> address or domain name of mainframe of time server

[Example]

✧ Enter in configured view:

ntp server pool.ntp.org

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

✧ Enter in configured view:

no ntp server

Disable the router to get system time via network.

✧ Enter in configured view:

default ntp server

Recover the network time server of router to the factory setting.

6.5 Config export

[Command] Config export

[Function] Export config

[View] Configure view.

[Parameter] No

[Example]

Enter in configured view:

config export

The current config. is exported.

6.6 Config import

[Command] Config import

[Function] Import config

[View] Configure view.

[Parameter] No

[Example]

Enter in configured view:

config import

The config. is imported.

7 System Management Command

7. 1 Reboot

[Command] Reboot

[Function] System restarts.

[View] Super user view and configuration view

[Parameter] No

[Example]

Enter in super user view:

reboot

System restarts.

7. 2 Enable username

[Command] Enable password [<name>]

[Function] Modify the username of super user.

[View] Configure view.

[Parameter]

<name> new super user username

[Example]

Enter in configured view:

enable username admin

The username of super user is changed to admin.

7.3 Enable password

[Command] Enable password [<password>]

[Function] Modify the password of super user.

[View] Configure view.

[Parameter]

<password> new super user password

[Example]

✧ Enter in configured view:

enable password

Enter password according to the hint.

7.4 Username

[Command] Username <name> [password [<password>]]

no username <name>

default username

[Function] Set user name, password

[View] Configure view.

[Parameter] No

[Example]

✧ Enter in configured view:

username abc password 123

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

✧ Enter in configured view:

no username abc

Delete the ordinary user with the name of abc.

✧ Enter in configured view:

default username

Delete all the ordinary users.

FCC STATEMENT

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

(1) This device may not cause harmful interference, and

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

NOTE 1: 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, 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.

NOTE 2: Any changes or modifications to this unit not expressly approved by the

party responsible for compliance could void the user's authority to operate the equipment.

RF Exposure

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

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The availability of some specific channels and/or operational frequency bands is country dependent and firmware programmed at the factory to match the intended destination.

The firmware setting is not accessible by the end user.

IC STATEMENT

This device complies with Industry Canada license-exempt RSS standard(s): Operation is subject to the following Two conditions:

(1) this device may not cause interference, and

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

Le present appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes :

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

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

CAN ICES-3 (B)

Avis d'Industrie Canada Le présent appareil est conforme aux CNR d'industrie Canada applicables aux appareils radio exem pts de licence L'exploitation est autorisée aux deux conditions suivantes:

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

2) I'utillsateur de I'appareil doit accepterbrouillage radioélectrique subi meme si le brouillage est susceptible d'encompromettre le fonctionnement. mauvais fonctionnement de I'appareil. Cet appareil numériquie de la classe B est conforme à la norme NMB-003 du Canada.

CAN NMB-3 (B)

Radiation Exposure Statement:

This equipment complies with IC 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.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements IC établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20cm de distance entre la source de rayonnement et votre corps.