InHand Networks

Industrial Router IR315 Product User Manual

Table of contents

Declaration

Thank you for choosing our product. Before using the product, please read this manual carefully.
The contents of this manual cannot be copied or reproduced in any form without the written permission of InHand.
Due to continuous updates, InHand cannot guarantee that the contents are consistent with the actual product information and does not assume any disputes caused by inconsistencies in technical parameters. The information in this document is subject to change without notice. InHand reserves the right for final changes and interpretation.

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	This means the reader needs to be careful. Improper action may result in loss of data or device damage.
Note	Notes contain detailed descriptions and helpful suggestions.

1. Introduction

1.1 Overview

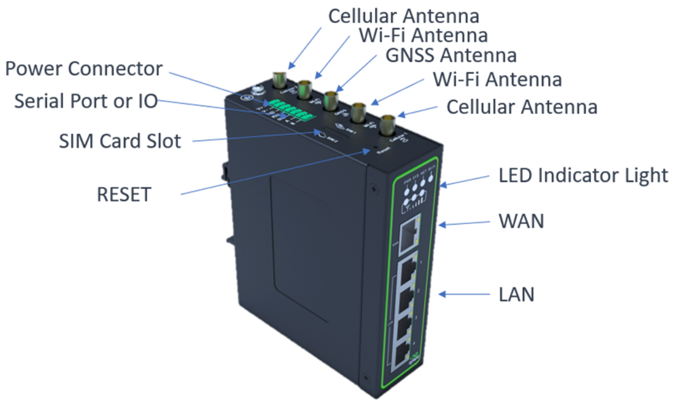
The InRouter315 (IR315) is an IoT cellular router that integrates 4G LTE, Wi-Fi, and VPN technologies to provide easy, reliable, and secure internet connectivity. With technologies such as 4G wireless wide-area network and Wi-Fi wireless local area network, it offers uninterrupted access to multiple networks. Its comprehensive security and wireless services allow networking for up to ten thousand devices, enabling high-speed data access.

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

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

The IR315 finds application in a wide range of industrial and commercial IoT scenarios, providing a good balance between cost and performance.

1.2 Panel Introduction



1.3 LED Indicators & Signal

Table 1-3 LED Indicators Status

IR315 LED	Status
PWR	Red off --- Power off Steady in red --- Power on
SYS	Green off --- System error

	Blink in Green --- System upgrading Steady in Green --- System working
Wi-Fi	Green off --- Wi-Fi disable Blink in Green --- Wi-Fi connecting Steady in Green --- Wi-Fi working
NET	Green off --- Network disconnected Blink in Green --- Network connecting Steady in Green --- Network connected
Signal	Three green lights steady on --- Dial-up successful, signal strength ≥ 20. Two green lights steady on --- Dial-up successful, 19 ≥ signal strength ≥ 10. One green light steady on --- Dial-up successful, signal strength ≤ 9.

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 be off.
3. Immediately press and hold the Reset button, SYS will flash, then loosen the Reset button. Then the device will reset to default settings.

2. Installation

2.1 Preparation

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. The first installation shall be done under the direction of the engineer recognized by InHand Networks.

- 1 PC
- 1 or 2 SIM cards: 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 the DC power adaptor of the device. 9~36V DC: Ripple voltage < 100 mV
- Fixation: Please place InRouter on a flat level and have it installed in an environment with a small vibrational frequency.

Caution:
The device shall be installed and operated in power-off status!

2.2 Installation

2.2.1 SIM/UIM Card

InRouter315 uses a pop-up card holder. Stab the hollow at the left of the cardholder and the cardholder 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 the metal SMA-J interface until it cannot be rotated (at this time, an external thread of the antenna cable cannot be seen). Do not forcibly screw the antenna by holding a 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 before logging in to the page 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 an IP address for the supervisory computer.

ii. **Set a Static IP Address:** Set the IP address of the supervisory PC (such as 192. 168. 2. 2) and LAN interface of the device in the 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:

  i. In the browser window, select "tools>>Internet options";

  ii. Select the "connection" page and click the button of LAN Settings to enter the "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 the Web Setting Page:** Open IE or another browser and enter the IP address of InRouter315, such as http://192.168.2.1 in the 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 safely keep the password information.

3. Web Configuration

The device needs to be effectively configured before use. This chapter will introduce how to configure your router via the Web.

3.1 System

Here, the 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 the mainframe of the router can be customized.

3.1.1 Basic Settings

Here, the Web configuration interface language can be set; the name of the mainframe of the 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 the display language of the router configuration interface and set a 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, a user is required to set the system time accurately since this function is used to configure and check system time as well as the 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 the network 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 System time Parameters

System Time		
Function description: Set local time zone and automatic updating time of NTP.		
Parameters	**Description**	**Default**
Router Time	Display the present time of the router	8:00:00 AM, 12/12/2015
PC Time	Display the present time of the PC	Present time
Timezone	Set the time zone of the 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 the NTP server to sync time via the 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 the Internet. After enabling HTTP service on the 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 an HTTP protocol which supports SSL protocol, it is more secure.
- **TELNET**: Telnet protocol provides telnet and virtual terminal functions through a network. Depending on the Server/Client, the Telnet Client could send a request to the 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**: Users can check the router’s status and configure the router without login the router remotely by sending an HTTP request with HTTP API. Please ask technical support for more information about HTTP API.
- **Console (only in IR315-S)**:Users can access IR315 CLI via RS232 and enable Console. From the navigation tree, select System >> Admin Access, then enter the “Admin Access” page.

Table 3-1-3 Parameters of Admin Access

Admin Access
Function description:

1. Modify the username and password of the router.

2. The router may be set in the following 5 ways, i.e. http, https, telnet, SSHD and console.

3. Set login timeout.

Parameters	**Description**	**Default**
Username/Password		
Username	Set the name of the user who logs in WEB configuration	adm
Old Password	Previous password access to WEB configuration	123456
New Password	New password access to WEB configuration	N/A
Confirm New Password	Reconfirm the new password	N/A
Amin functions		
Service Port	Service port of HTTP/HTTPS/TELNET/SSHD/HTTP_API	80/443/23/22/4444
Local Access	Enable - Allow local LAN to administrate the router with the corresponding service (e.g. HTTP) Disable - Local LAN cannot administrate the router with the corresponding service (e.g. HTTP)	Enable
Remote Access	Enable - Allow the remote host to administrate the router with the corresponding service (e.g. HTTP) Disable - The remote host cannot administrate the router with the 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
Description	For recording the 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 the “Username/Password” section, users can modify their username and password rather than create a new username, i.e. only this username can be used in logins.
- In the “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 a host (such as a 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 the “System Log” page.

Table 3-1-4 Parameters of System Log

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

3.1.5 Configuration 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 the hardware reset button of the router	Disable
Modem drive program	For configuring the drive program of the module	N/A
Network Provider (ISP)	For configuring APN, username, password and other parameters of the network providers across the world	N/A

Caution
Validity and order of imported configurations should be ensured. The good configs will later be serially executed in order after the system reboot. If the configuration files aren’t 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 restoring the default configuration, users need to restart the device to make the new configuration take effect.

3.1.6 Schedule

After this function is enabled, the device will reboot at the scheduled time. The scheduler function will take effect after router sync time.
From the navigation tree, select “System > Schedule”, then enter the “Schedule” page.

Table 3-1-6 Parameters of Schedule

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 every day	Everyday
Show advanced options	Enable more detailed schedule rules, and allow setting multiple rules to reboot the router at a specific time or interval. Enable this feature will disable the everyday reboot feature above.	Disable
Reboot after dialed	The router will reboot after dialling up successfully, and 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 the backup file zone, in the second step: firmware in the backup file zone will be copied to the main firmware zone, which should be carried out during system restart. During software upgrading, any operation on the 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> to choose the upgrade file, secondly, click <Upgrade> and then click <OK> to begin the 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 Log Out

To log out, click “System >> Logout”, and then click <OK>.

3.2 Network

3.2.1 Cellular

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

Table 3-2-1-a 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 schedule	ALL
Force Reboot	The router will reboot if cannot dialup for a long time and reach the max retry time	Enable
Shared connection (NAT)	Enable—Local devices connected to the Router can access the Internet via the Router. Disable—Local devices connected to the Router cannot access the Internet via the Router.	Enable
Default Route	Enable default route	Enable
SIM1 Network Provider	Select the network provider profile for SIM1	Profile 1
Network Type	Select network type, the router will try 4G, 3G, and 2G in proper order if selected 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 the 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 the SIM2 PIN code	N/A
SIM2 SIM Card Operator	Set the ISP that the SIM2 card connects to	Auto
Main SIM	Set the SIM card that is used to dialup at first	SIM1
Max Number of Dial	Set the max number of dials, if cannot dial up successfully after this number, the router will switch the SIM card	5
CSQ Threshold	Set threshold of signal, if the current signal level is lower than this, the 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 customised 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 the 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 the system log	Disable
Debug Modem*	Send modem debug data to the console	Disable
ICMP Detection Mode	Set ICMP detection mode, router will check the link connection status via the ICMP packet. Ignore Traffic: The Router will send an ICMP packet no matter whether there is traffic in the cellular interface. Monitor Traffic: Router will not send an ICMP packet if there is traffic in the 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-b 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 the WAN port.

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

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

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

The WAN of the device is disabled by default.

Click the “Network>>WAN” menu in the navigation tree to enter the “WAN" Interface.

Table 3-3-2-a Static IP Parameters for WAN

WAN - Static IP		
Function description: Access to the Internet via wired lines with fixed IP.		
Parameters	**Description**	**Default**
Shared connection (NAT)	Enable—Local devices connected to the Router can access the Internet via the Router. Disable—Local devices connected to the Router cannot access the Internet via the Router.	Enable
Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device’s MAC address

IP Address	Set the 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 the additional IP address of the LAN	N/A
Subnet mask	Set subnet mask	N/A
Description	For recording the significance of additional IP address	N/A

Table 3-3-2-b Dynamic Address(DHCP) Parameters for 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 devices connected to the Router can access the Internet via the Router. Disable—Local devices connected to the Router cannot access the Internet via the 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 (1500)

Table 3-3-2-c ADSL Dialing(PPPoE) Parameters for WAN

WAN - ADSL Dialing (PPPoE)		
Function description: Set ADSL dialling parameters.		
Parameters	**Description**	**Default**
Shared connection	Enable—Local devices connected to the Router can access the Internet via the Router.	Enable

	Disable—Local devices connected to the Router cannot access the Internet via the 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 (1492)
WAN - ADSL Dialing (PPPoE)		
Username	Set the name of the dialing user	N/A
Password	Set dialing password	N/A
Static IP	Click to enable static IP	Disable
Connection Mode	Set dialling connection method (always online, dial on demand, manual dialling)	Always online
Parameters of Advanced Options		
Service Name	Set service name	N/A
Set the length of the transmit queue.	Set the length of the transmit queue.	3
Enable IP header compression	Click to enable IP header compression	Disable
Use Peer DNS	Click to enable the use of 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 based 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 setting the VLAN, click “modify” to configure the LAN settings of each VLAN.

Click “Network >> VLAN” to configure VLAN in the router.

Table 3-2-3 VLAN Parameters

VLAN		
Function description: Set VLAN parameters for the LAN port.		
Parameters	**Description**	**Default**
VLAN ID	Set VLAN ID	1
LAN1~LAN4	Set which LAN port to be a part of the 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 a VLAN tag if it is transferred by a native VLAN	1
GARP		
Enable	The 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 the network.

Parameters	**Description**	**Default**
IP Address	IP Address of router’s LAN gateway	192.168.2.1
Netmask	The subnet mask of the 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 the additional IP address of the LAN	N/A
Subnet mask	Set subnet mask	N/A

3.2.4 Switch WLAN Mode

IR315 supports two types of WLAN modes: AP and STA.
Click the “Network>>Switch WLAN Mode” menu in the navigation tree to set the WLAN mode of the router. After changing and saving the configuration, please reboot the device to make the configuration take more effort.

3.2.5 WLAN Client(AP Mode)

When working in AP mode, the device WLAN will provide a 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 users.		
Parameters	**Description**	**Default**
SSID broadcast	After turning it on, users can search the WLAN via the SSID name	Enable
Mode	Six types of 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
SID	SSID name defined by the user	in hand
Authentication method	Support open type, shared type, auto-selection of WEP, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA/WPA2, WPA-PSK/WPA2PSK	Open type
Encryption	Select the encryption method of AP	NONE
Wireless bandwidth	Support 20MHz and 40MHz	20MHz

Enable WDS	Click to enable WDS, router will connect to other APs 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 the 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 dialling interface in the "Network>>Dialing Interface" should be closed.)
The SSID scan function is enabled only when the Client is selected as a WLAN interface. Click the “Scan” button to get all available APs and status, select AP and configure the corresponding parameter to connect. After configuring the WLAN Client, please configure the 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 the 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	in hand
Authentication method	Keep consistent with the access point to be connected	Open type
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 configure the interface.

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

Link Backup
Function description: When the system runs, the 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 dialling 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 the main link when ICMP failed	Disable

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

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

- The 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 the virtual router and set it as the address of the next hop of the default route.
- The host locally 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 a fault of the gateway router, thus guaranteeing uninterrupted communication between the host and external network.

The monitor interface function of VRRP better expands the backup function: the backup function can be offered when the interface of a certain router has a fault or other interfaces of the router are unavailable.
When the 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 the highest priority becomes the gateway for the transmission task.
From the navigation tree, select the "Network >>VRRP" menu, then enter the “VRRP” page.

Table 3-2-8 VRRP Parameters

VRRP		
Function description: Configure parameters of VRRP.		
Parameters	**Description**	**Default**
Enable VRRP-I	Click to enable the 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 Passthroug

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

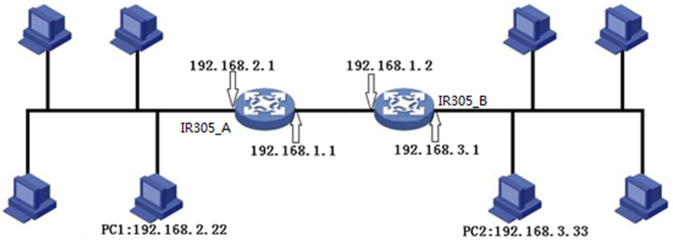
Static route needs to be set manually, after which packets will be transferred to appointed routes.
To set a static route, click the "Network >> Static Route" menu in the navigation tree, then enter the “Static Route” interface.

Table 3-2-10 Static Route Parameters

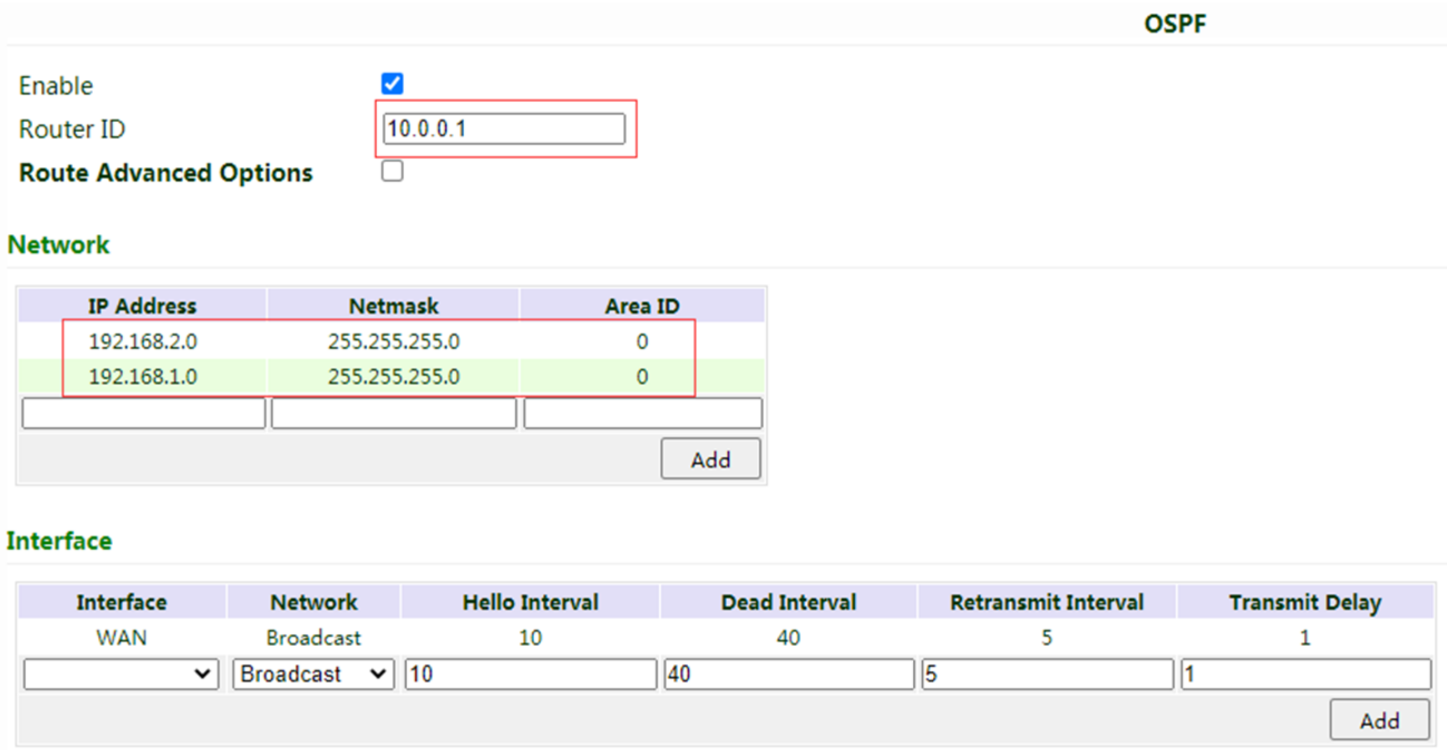
Static Route		
Function description: Add/delete additional static rote of router. Generally, users don't have to set it.		
Parameters	**Description**	**Default**
Destination Address	Set the IP address of the destination	0.0.0.0
Netmask	Set the subnet mask of the destination	255.255.255.0
Gateway	Set the gateway of the destination	N/A
Interface	Select LAN/CELLULAR/WAN/WAN(STA) interface of the destination	N/A
Description	For recording the 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 an 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 as IR315_B. Configure IR315_A in the “Network” bar to announce the routing entry of the device.



OSPF

Enable ☑

Router ID 10.0.0.1

Route Advanced Options □

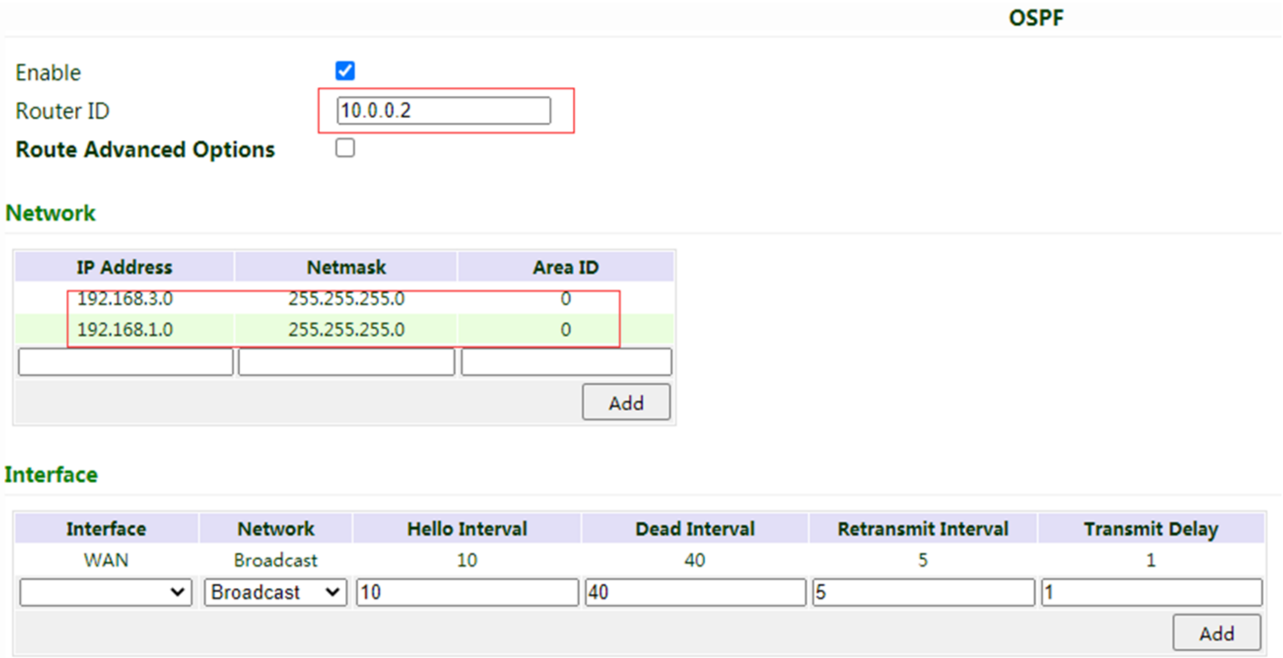
Network

IP Address	Netmask	Area ID
192.168.2.0	255.255.255.0	0
192.168.1.0	255.255.255.0	0

Interface

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

2. Configure IR315-B



OSPF

Enable ☑

Router ID 10.0.0.2

Route Advanced Options □

Network

IP Address	Netmask	Area ID
192.168.3.0	255.255.255.0	0
192.168.1.0	255.255.255.0	0

Interface

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

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

3.3 Service

3.3.1 DHCP Service

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

- DHCP Server has to distribute the IP address when the Workstation logs on and ensure each workstation is supplied with a different IP address. DHCP Server has simplified some network management tasks requiring manual operations before to the largest extent.
- As a DHCP Client, the device receives the IP address distributed by the DHCP server after logging in to 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 the "DHCP Service" page.

Table 3-3-1 Parameters of DHCP Service

DHCP Service

Function description: If the host connected with the router chooses to obtain an IP address automatically, then such service must be activated. Static designation of DHCH allocation could help the certain host to obtain a 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 the ending IP address of the dynamic allocation	192.168.2.100
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 address (different from other MACs to avoid conflict)	N/A
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 a switch between domain name and IP address. Through DNS, users could directly use some meaningful domain name which could be memorized easily and the DNS Server in a network could resolve the domain name into the correct IP address. The device analyzes dynamic domain names via DNS.

Manually set the DNS, use DNS via dialling if it is empty. Generally, it needs to be set only when a 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 the 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 messages between DNS Client and DNS Server to carry out domain name resolution instead of the DNS Client.
From the navigation tree, select the "Service>>DNS Relay" menu, then enter the “DNS Relay” page.

Table 3-3-3 DNS Transfer Parameters

DNS Relay service		
Function description: If the host connected with the router chooses to obtain the 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 the IP address of designated IP address <=> domain name	N/A
Host	Domain Name	N/A
Description	For recording the 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 a 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 the user's 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 the “Dynamic Domain Name” interface.

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

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

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

Enable the function of dynamic domain name		
Function description: Set dynamic domain name binding. (Explain the configuration of the 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 a software platform. For instance, the operating status of the device can be checked, the device software can be upgraded, the device can be restarted, configuration parameters can be sent down to the device, and transmitting control or message query can be realized on the device via the Device Manager.
Click the "Service>>Device Manager" menu in the navigation tree to enter the "Device Manager" interface. North American users should select the Servicer address: iot.inhandnetworks.com.

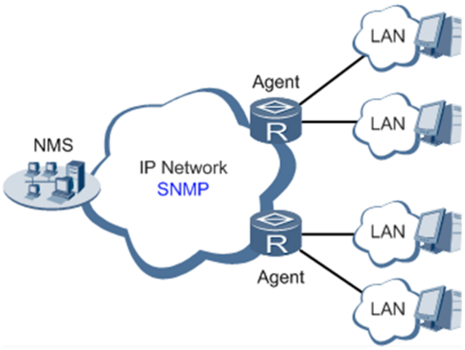
Table 3-3-5 Device Remote Management Platform

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 InConnect Service	Device Manager

	Custom	
Server	Input address of a 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, the 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 of them.



To run the SNMP protocol on a network, configure the NMS program on the management side and the 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 the "Service>SNMP" menu to configure.

Table 3-3-6-1 SNMPv1 and SNMPv2 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 applies to small-sized networks with simple networking and low-security requirements, or secure and stable small networks, such as campus networks and small enterprise networks. SNMPv2c applies to medium- and large-sized networks with low-security requirements, or with	v1

	good security (for example, VPNs) but running many services, which may lead to traffic congestion. SNMPv3 applies to networks of various sizes, especially networks that have strict 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 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.	default view

Table 3-3-6-2 SNMPv3 Parameters

Parameters	**Description**	**Default**
User Group Management		
Group name	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.	default view
Read-write View	Select the SNMP read-write view. Only the default view is supported currently.	default view
Inform View	Select the SNMP inform view. Only the default view is supported currently.	default view
Usm Management		
Username	User-defined user name. The length is 1 to 32 characters.	None
Group name	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
Authentication Password	This parameter is available only when the authentication mode is None. The length is 8 to 32 characters.	None
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 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 to wait for the polling of the NMS. The errors are reported to the NMS through traps. Click the "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 Name	Fill in the community name for SNMPv1 or SNMPv2c, and fill in the user name for SNMPv3. The length is 1 to 32 characters.	None
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 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 a power supply for another device directly).

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

Table 3-3-8 I/O Parameters

I/O		
Function description: Configuration of 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	Report when input triggers in some situation	Disable
Trigger edge	Set the trigger edge of the relay	Falling edge

3.3.9 DTU RS232/RS485

Configure the DTU function, the device can transmit serial data to the 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 a server.		
Parameters	**Description**	**Default**
Enable	Enable serial port	Disable
Serial Basic Config		
Serial type	Serial port type, cannot change	RS232 or RS485
Baudrate	Set the serial port’s baud rate	115200
Data Bits	Set serial port’s data bits	8
Parity	Set parity of the serial port	None
Stop Bit	Set stop bit of serial port	1
Software Flow Control	Enable software flow control can avoid data flow lost	Disable
DTU Configuration		
Function Description: Configure the protocol of data transmission, take transparent transmission as an example		
DTU Protocol	Set the transmit protocol of DTU	Transparent
Protocol	Configure type of protocol, TCP/UDP	TCP
Mode	Set the connection mode between the router and the 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 the router and the server	60
Keep alive Retry Time	The number of times to retry when a 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 the router when connected to the server	
Source IP	The source IP router uses when connected to the server, will use WAN IP if this parameter is blank	

Source port	The source port the router uses when connecting to the server, will use a random port if this parameter is blank	
DTU ID Report Interval	Set the interval to upload the DTU ID	0
DTU Serial Port Traffic Statistics	Upload serial port statistics data to “Status/DTU”	Disable
Multi Server		
Function Description: The Router can transmit data to multiple servers, taking transparent transmission as an 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 dialling. Configure Permit to Phone Number and click <Apply and Save>. After that, you can send a “reboot” command to restart the device or send a custom connection or disconnection command to redial or disconnect the device.

From the navigation tree, select the "Service>>SMS" menu, then enter the “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 the 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 the 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 the cellular interface. If the threshold is 0, the router will only count and the rules will not take effort. This function requires enabling the 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 the 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 the 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, the router will report an alarm according to the settings. Currently, the router supports sending alarms in the 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.
Users can disable or enable the User Experience Plan in "Services >> User Experience Plan".

3.4 Firwall

The firewall function of the router implements corresponding control to data flow at the entry direction (from Internet to LAN) and exit direction (from LAN to Internet) according to the content features of the 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 the 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 customising rules to allow or prohibit the specified data flow forwarded by the router.
To enable Access Control from the navigation tree, select Firewall >> Filtering, then enter the “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 the 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 the destination port of access control	Not available
Action	Select accept/block	Accept
Log	Click to enable the 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 customised rules to allow or prohibit data and access to the router.

From the navigation tree, select Firewall > Device Access Filtering, then enter the “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 the destination port of network access	Not available
Interface	The 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 the navigation tree, select the "Firewall > Content Filtering" menu, then enter the “Content Filtering” page.

Table 3-4-4 Content Filtering Parameters

Filtering		
Function description: Set settings of firewall related to filtering and generally set forbidden URLs.		
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 Maping

Port mapping is also called a virtual server. Setting port mapping can enable the host of the extranet to access to specific port of the host corresponding to the IP address of the intranet.

To configure port mapping, go into the navigation tree, select "Firewall >> Port Mapping", then enter the “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 the internal address of the port mapping	N/A
Internal Port	Set the 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 the external interface of port mapping	N/A
External Address (optional)	Set the external address/tunnel name of the port mapping	N/A
Description	For recording the significance of each port mapping rule	N/A

3.4.6 Virtual IP Maping

Both the router and the IP address of the host of an intranet can correspond with one virtual IP. Without changing the IP allocation of the intranet, the extranet can access the host of the intranet via virtual IP. This function is always used with VPN.

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

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

Virtual IP Address

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

3.4.7 DMZ

After mapping all ports, the extranet PC can access all ports of an 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 the range of external source address	N/A
Interface	Select the external interface of DMZ	N/A

3.4.8 MAC-IP Binding

If the default filter policy in the basic setting of the firewall is disabled, only hosts specified in MAC-IP Binding can have access to the 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

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

3.5 QOS

To ensure all LAN users can normally get access to network resources, the IP traffic control function can limit the flow of specified hosts 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

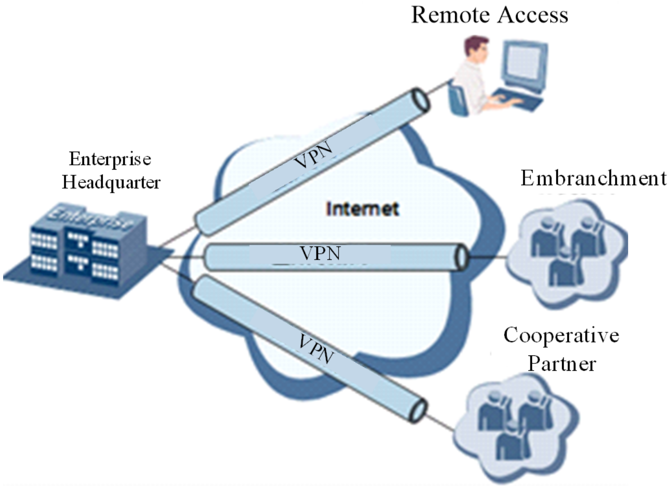
IP Bandwidth Limit		
Function description: Configure parameters of IP bandwidth limit.		
Parameters	**Description**	**Default**
Enable	Click to enable the IP bandwidth limit	Disable
Download bandwidth	Set download total bandwidth	1000kbit/s
Upload bandwidth	Set upload total bandwidth	1000kbit/s
Control 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 the 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 a VPN are unavailable to unauthorized VPN users on the internet; a VPN can ensure and protect its internal information from external intrusion.
- Virtual: the communication among VPN users is realized via the public network which, meanwhile can be used by unauthorized VPN users so that what VPN users obtain is only a logistic private network. This public network is regarded as a VPN Backbone.

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



Fundamental Principle of VPN

The fundamental principle of VPN indicates enclosing the VPN message into the tunnel with tunnelling technology and establishing a private data transmission channel utilizing VPN Backbone to realize transparent message transmission.

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

3.6.1 IPSec Setting

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

IPSec is a group of open network security protocols 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 can reduce the risk of disclosure and guarantee data integrity and confidentiality as well as maintain security of service transmission of users.

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

IPSec can establish a 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 the navigation tree, select VPN>>IPSec Settings, then enter the “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 the key log will be printed into the system log. Debug: More log-in debug levels will be printed. Data: All logs of IPSec will be printed.	Normal

3.6.2 IPSec Tunnels

From the 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

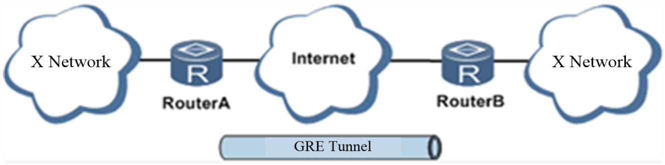
Parameters	Description	Default
Show Advanced Options	Click to enable advanced options	Disable(open advanced options after enabling)
Basic parameters		
Tunnel Name	The user defines the tunnel name	IPSec_tunnel_1
Destination Address	Set destination IP address or domain name	0. 0. 0. 0
IKE Version	Set IKE version: IKEv1/IKEv2	IKEv1
Startup Modes	Select Auto Activated/Triggered by Data/Passive/Manually Activated	Auto Activated
Restart WAN when failed	The router will restart the WAN interface but cannot establish an 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 Host-Host/Host-Subnet/Subnet-Host/Subnet-Subnet	Subnet-Subnet
Local subnet address	Set the local subnet IP address	192. 168. 2. 1
Local Subnet Mask	Set the 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 the IPSec VPN key	N/A
XAUTH Parameters (Advanced Option)		
XAUTH Mode	Click to enable XAUTH mode	Disable
XATUTH username	The user defines XATUTH username	N/A
XATUTH password	The 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, and DES. The implementation mechanism of an encryption algorithm with stricter security is complex and slow arithmetic speed. DES algorithm can satisfy ordinary safety requirements.

3.6.3 GRE Tunnels

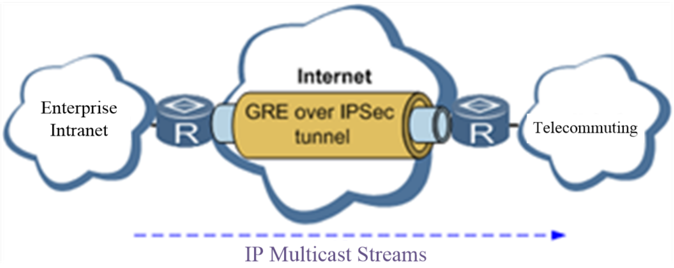
Generic Route Encapsulation (GRE) defines the encapsulation of any other network layer protocol on a network layer protocol. GRE could be used as the L3TP of a VPN to provide a transparent transmission channel for VPN data. In simple terms, GRE is a tunnelling technology which provides a channel through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



Along with the extensive application of IPv4, to have messages from some network layer protocol transmitted on the IPv4 network, those messages could be encapsulated by GRE to solve the transmission problems between different networks.
In the 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 addresses 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 the case of multicast data requiring to be transmitted in an IPSec tunnel, a GRE tunnel could be established first for GRE encapsulation of multicast data and then IPSec encryption of encapsulated message to achieve the encryption transmission of multicast data in an IPSec tunnel. As shown below:



From the 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 the GRE	Enable
Name	The user defines the name of the GRE tunnel	tun0
Local visual IP	Set local virtual IP	0. 0. 0. 0
Destination Address	Set the remote IP address	0. 0. 0. 0
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 the GRE tunnel	N/A
NAT	Click to enable the NAT	Disable

Description	For recording the significance of each GRE tunnel configuration	N/A

3.6.4 L2TP Client

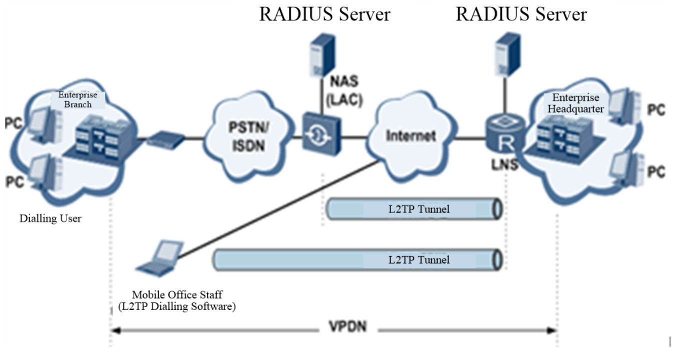
L2TP, one of VPDN TPs, has expanded the applications of PPP, known as a very important VPN technology for remote dial-in users to access the network of enterprise headquarters.

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

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

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

A typical L2TP network diagram is shown below:



From the 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 the L2TP client.		
Parameters	**Description**	**Default**
Enable	Click to enable the L2TP client	Disable
Tunnel Name	The user defines the tunnel name of the L2TP client	L2TP_tunnel_1
L2TP Server	Set the L2TP Server address	N/A
Username	Set the server's username	N/A
Password	Set the 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 the local IP address	N/A
Remote IP Address	Set the remote IP address	N/A
Remote Subnet	Set remote subnet address	N/A
Remote Netmask	Set the 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 the 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 the 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 the parameters of the PPTP client.		
Parameters	**Description**	**Default**
Enable	Click to enable the PPTP client	Disable
Tunnel Name	The user defines the tunnel name	PPTP_tunnel_1
PPTP Server	Set the PPTP Server address	N/A
Username	Set username of PPTP server	N/A
Password	Set the password of the 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 the local IP address	N/A
Remote IP Address	Set the remote IP address	N/A
Remote Subnet	Set remote subnet address	N/A
Remote Netmask	Set the 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 the 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

A single point participating in the establishment of a VPN is allowed to carry out ID verification by a 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 a remote virtual address (address family matching virtual network card), then the OS will send the data packet (TUN mode) or data frame (TAP mode) to the visual network card through the routing mechanism. Upon reception, the 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 the processing, then send them to the virtual network card, then application software receive and accomplish a complete unidirectional transmission, vice versa.

From the navigation tree, select "VPN>>OpenVPN", then enter the “OpenVPN” page, and click <Add>.

Table 3-6-6 Parameters of OpenVPN

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 the OpenVPN Server address	N/A
Authentication method	N/A pre-shared key username/password digital certificate (multiple client) digital certificate username and digital certificate	N/A
Local IP Address	Set the local IP address	N/A
Remote IP Address	Set the remote IP address	N/A
Remote Subnet	Set remote subnet address	N/A
Remote Netmask	Set the 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 the navigation tree, select "VPN>>OpenVPN Advanced" and enter the "OpenVPN Advanced" interface.

Table 3-6-7 Configuration of OpenVPN

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/common name	N/A
Password	Set client password	N/A
Client IP (4th byte must be 4n+1)	Set the client's IP address	N/A
Local Static Route	Set a local static route	N/A
Remote Static Route	Set a remote static route	N/A

3.6.8 WireGuard Tunnels

WireGuard is a new generation VPN which aims to provide a more efficient and more secure VPN service with advanced encryption algorithms.
Click the Add button to configure and create a WireGuard tunnel, and check the VPN status on this page.
From the navigation tree, select VPN >> WireGuard Tunnels, then enter the WireGuard VPN configure page.

Table 3-6-8 WireGuard Configuration

WireGuard Tunnels		
Function description: Configure WireGurad VPN.		
Parameters	**Description**	**Default**
Tunnel Name	Set the name of the 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 devices connected to the Router can access the Internet via this tunnel. Disable—Local devices connected to the Router cannot access the Internet via this tunnel.	Enable
Listening Port	VPN port, the system will listen to the default port (51820) if this parameter is blank. The different tunnel needs to use different listening ports.	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 be accessed via this tunnel	0.0.0.0/0(all)
Public Key	Generated by WireGuard, it corresponds 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 enabling NAT, 0 means disable	25
WireGuard Key Generator		
Click the Generate button to create a private key, public key or pre-shared key by WireGuard. It also supports to creation public key after entering the private key. The private key is used in local tunnel parameters, public key is used in the peer public key.		

3.6.9 ZeroTier VPN

ZeroTier VPN supports users to build a network that allows all client devices to access each other. There are two network types in ZeroTier VPN, planet and moon. In Planet network, the user needs to log in and create a VPN network https://www.zerotier.com/ at first. Moon network is a private VPN network created by the user.
From the navigation tree, select VPN >> ZeroTier VPN, then enter the “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 the tunnel	N/A
Network Type	Select network type: planet or moon	planet
Network ID	Set network ID (16 letters) to connect to the VPN server	N/A

3.6.10 Certificate Management

From the navigation tree, select VPN >> Certificate Management, then enter the “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", and 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 the 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 the 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 the local computer	N/A

Note：
When using the certificate, please make sure the time of the router is synced 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	The address of the destination host of	N/A

	PING detection is required.	
PING Count	Set the Ping count	4
Packet Size	Set the size of the Ping detection	32 bytes
Expert Option	Advanced parameters of Ping are available.	N/A

3.7.2 Traceroute

To perform a traceroute, select the "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 failure detection.		
Parameters	**Description**	**Default**
Host	The 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 the traceroute	3 s
Protocol	ICMP/UDP	UDP
Expert Option	Advanced parameters for traceroute are 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 the 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 a specific interface		
Parameters	**Description**	**Default**
Interface	Select the interface to capture the packet	ANY
Capture number	Stop TCP dump after capturing 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 of the ATM platform.

Smart ATM		
Function description: configure parameters for docking intelligent ATM cloud platform		
Parameters	**Description**	**Default**
Smart ATM	Enable Smart ATM	disable
Server	Configure the parameters of the server, Click Edit to show more information	iot.inhand.com.cn
Enable SSL proxy	Enable proxy of SSL	disable
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 the IP/Host name of the 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 of the 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 setting	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 Uptime	Show MNC、MCC、Cell ID、LAC Uptime	Disable
Current firmware version	Show the 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 for Smart-EMS.

Smart-EMS		
Function description: configure parameters for docking intelligent Smart-EMS cloud platform		
Parameters	**Description**	**Default**
Server URL	Fill in the server address	N/A
Username	Fill in the user name	N/A
Password	Fill in the 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 the 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 the 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 Statistic

Choose Status >> Traffic Statistics to go to the "Traffic Statistics" page to query traffic statistics. This page displays the traffic statistics on the dialling 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.

3.9.4 DTU

Only the IR315 serial type supports this page.
Choose Status >> DTU to go to the "DTU" page to check the 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 has 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 the navigation tree, select Status >> Network Connections, then enter the “Network Connections” page to see the status of the connections. This page shows the basic information of dialup and LAN. WAN includes MAC address, connection type, IP address, netmask, gateway, DNS, MTU, Status, 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 the navigation tree, select Status >> Device Manager, then enter the “Device Manager” page to check the status of the connections between the router and Device Manager.

3.9.9 Route Table

From the navigation tree, select Status >> Route Table, then enter the “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 the navigation tree, select Status >> Device List, then enter the “Device List” page to inquire about 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).

3.9.11Log

From the navigation tree, select Status >> Log, then enter the “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).

3.9.12Third-Party Software Notices

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

Appendix A: FAQ

1.InRouter is powered on, but can't access the 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 the 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 the IP address and can't configure InRouter.

- Method 1: connect InRouter with a serial cable, and configure it through the console port.
- Method 2: Within 5 seconds after InRouter is powered on, press and hold the Restore button until the ERROR LED flashes, then release the button and the ERROR LED should go off, press and hold the button again until the ERROR LED blinks 6 times, the InRouter is now restored to factory default settings.

You may configure it now.

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

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?**

First check:

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

6.After InRouter establishes a VPN with the VPN server, your PC under InRouter can connect to the server, but the centre 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 burned 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 the 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 the 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 the InRouter LAN address.
- Check the firewall settings of the PC used to configure InRouter, and whether this function is shielded by the firewall.
- Please check whether your IE has any third-party plugins (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 the 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

The help command can be obtained after entering help or “?” into the 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 the command.

[View] All views

[Parameter]

<cmd>   command name

[Example]

Enter:

help

Get the list of all currently available commands.

enter:

help show

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

2 View Switchover Command

2.1 Enable

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

[Function] Switchover to the 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] Superuser 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 it is an 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 the system state command

3. 1 Show version

[Command] Show version

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

Description: www.inhand.com.cn

Current version: display the current version of the equipment

Current version of Bootloader: display the current version of equipment

3. 2 Show system

[Command] Show system

[Function] Display the information on the 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 the 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 the 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 the router system and display the latest 100 logs by default.

[View] All views

[Parameter]

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

[View] All views

[Parameter] No

[Example]

Enter:

show users

The displayed user list of the system is as follows:

```
  User:
-------------------------------------------------
* adm
------
```

Wherein, the user marked with * is a super user.

3. 7 Show startup-config

[Command] Show startup-config

[Function] Display the starting device of the router.

[View] Superuser view and configuration view

[Parameter] No

[Example]

Enter:

show startup-config

Display the starting configuration of the system.

3. 8 Show running-config

[Command] Show running-config

[Function] Display the operational configuration of the router

[View] Superuser view and configuration view

[Parameter] No

[Example]

Enter:

show startup-config

Display the operational configuration of the system.

4 Check Network Status Command

4. 1 Show interface

[Command] Show interface

[Function] Display the information on the port state of the 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 on the port state of the 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 the router

[View] All views

[Parameter] No

[Example]

enter:

show route

Display the routing list of the 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 the system

5 Internet Testing Command

The 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 the appointed mainframe.

[View] All views

[Parameter]

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

count <n> testing times

size <n> tests the size of the 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 the mainframe logged in.

<port>telnet port

source <ip> appoints the IP address of the 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 the appointed mainframe.

[View] All views

[Parameter]

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

max hops <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 the super user view, the router can use the configure command to switch it over configure view for management.

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

6. 1 Configure

[Command] Configure terminal

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

[View] Superuser 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 the router.

[View] Configure view.

[Parameter]

<hostname> new mainframe name

[Example]

Enter in configured view:

hostname

Display the mainframe name of the router.

Enter in configured view:

hostname MyRouter

Set the mainframe name of the router MyRouter.

Enter in configured view:

default hostname

Recover the mainframe name of the 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 IG601 is east east-eighth area and the name is CST (China's standard time).

Enter in configured view:

```
default clock timezone
```

Recover the timezone of the 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 the 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 the Internet time server pool. ntp. org.

Enter in configured view:

```
no ntp server
```

Disable the router to get system time via the network.

Enter in configured view:

```
default ntp server
```

Recover the network time server of the 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] Superuser 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 the superuser.

[View] Configure view.

[Parameter]

<name> new super user username

[Example]

Enter in configured view:

enable username admin

The username of the superuser is changed to admin.

7.3 Enable password

[Command] Enable password [<password>]

[Function] Modify the password of the super user.

[View] Configure view.

[Parameter]

<password> New super user password

[Example]

Enter in configured view:

enable password

Enter the 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 abc.

Enter in configured view:

```
default username
```

Delete all the ordinary users.