InHand Networks CR202 Portable 4G Router

User Manual

Issue: V1.0— March, 2023

InHand Networks
Global Leader in Industrial IoT
www.inhandnetworks.com

Declaration

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

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

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

Conventions

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

Contact Us

43671 Trade Center Place, Suite 100, Dulles, VA 20166

E-mail: support@inhandneworks.com

T: +1 (703) 348-2988

URL: www.inhandnetworks.com

Contents

I. INTRODUCTION

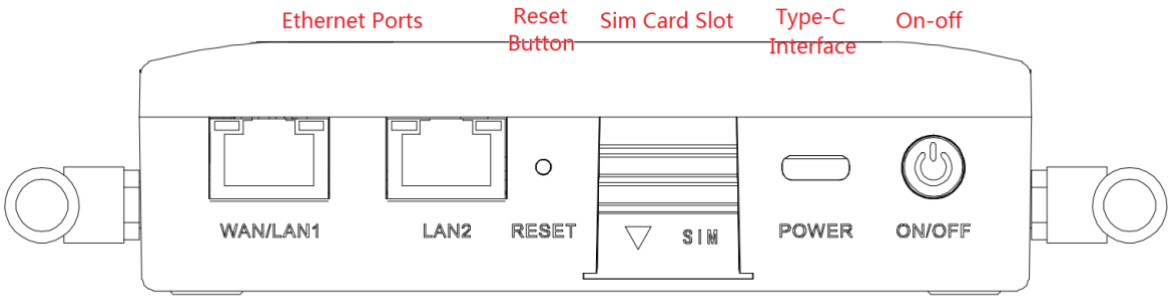
1.1 OVERVIEW

The mobile 4G cellular router CR202 greatly increases the access flexibility in remote office/study, mobile scenarios, and field scenarios with a reliable Internet connectivity. It can also guarantee a smooth business operation for small and medium-sized branches and self-service terminal scenarios and avoid any network failure may exist.

CR202 supports wired networks to wireless access, which increases the diversity of device access to the network and can effectively ensure that the network is not interrupted. The powerful built-in battery also allows you to work anytime and anywhere. With the lightweight design, it allows for unrestricted device mobility.

Combined with InHand Device Manager cloud management platform, CR202 guarantees efficient device management capabilities, provides customers with high-speed network access, simple and convenient network management services to empower the core network.

1.2 PANEL INTRODUCTION



1.3 LED INDICATION &SIGNAL

CR202 LED	Status
System	Off --- Power off Blink in green --- Device starting Steady in green --- Device working Blink in yellow --- Upgrading
Network	Off --- Cellular disable Blink in green --- Dialing up Blink in yellow --- Dialing abnormal Blink in red --- No SIM card, cannot read SIM card or modem abnormal Steady in green --- Dialed up, signal level≥20 Steady in yellow --- Dialed up, 19≥signal level≥10 Steady in red --- Dialed up, 9≥signal level
Wi-Fi	Off --- Wi-Fi disable Blink in green --- Wi-Fi connected, data transmitting Steady in green --- Wi-Fi enable
Battery	Blink --- Battery charging Steady --- Battery discharging Green --- 80%＜battery level ≤100% Yellow --- 20%＜battery level ≤80% Red --- 0＜battery level ≤20%

1.4 Reset to default settings

To restore to default settings via the reset button, please perform the following steps:

1. Press the RESET button immediately after power on the device.

2. When System LED is steady on, release RESET button, system LED will blink, and press the RESET button again.

4. When System LED blinks slowly, release the RESET button. The device has been restored to default settings and will start up normally later.

II. INSTALLATION

2.1 PREPARATIPNS

Precautions:

Please be sure there is 3G/4G network coverage. Avoid direct sunlight, away from heat source or strong electromagnetic interference. First installation shall be done under direction of the engineer recognized by InHand Networks.

- 1 PC

  OS: Windows 7, Windows 10, Windows 11

  Ethernet port: At least one (10M/100M)

- 1 SIM card:

  Ensure the card is enabled with data service and its service is not suspended because of an overdue charge.

- Power supply:

  5V/2A Type-C interface

  Internal battery

- Fixation:

  Please place CR202 on flat level and have it installed in an environment with small vibrational frequency.

Caution

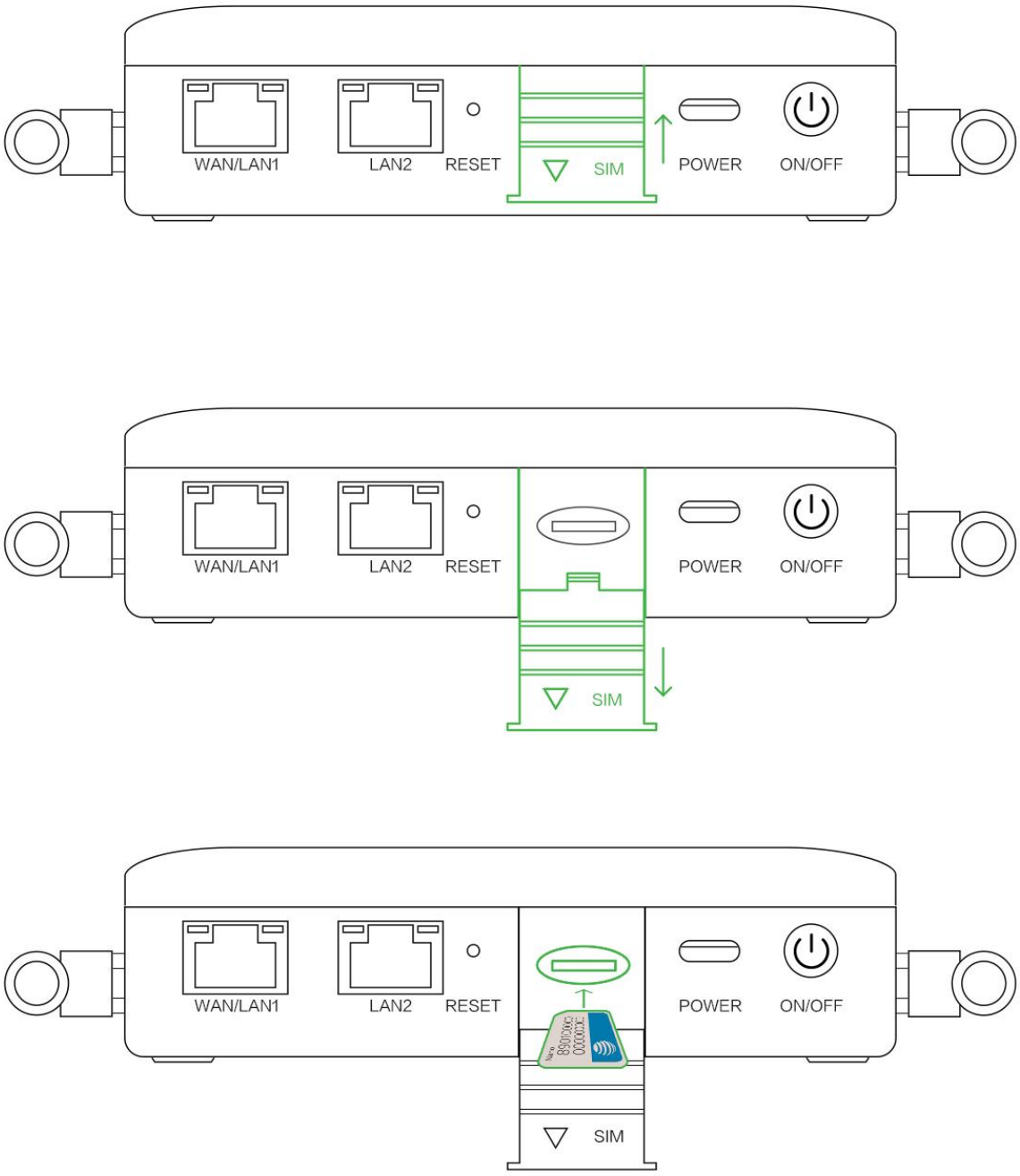
The device shall be installed and operated in powered-off status!

2.2 INSTALLATION

2.2.1 SIM/UIM Card

CR202 supports single nano SIM card or eSIM. Please install the SIM card like below if use nano

SIM card.



2.2.2 Antenna

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

black rubber lining.

2.2.3 Power Supply

CR202 supports internal battery or Type-C interface (5V/2A), please pay attention to the power voltage level.

2.3 LOGIN ROUTER

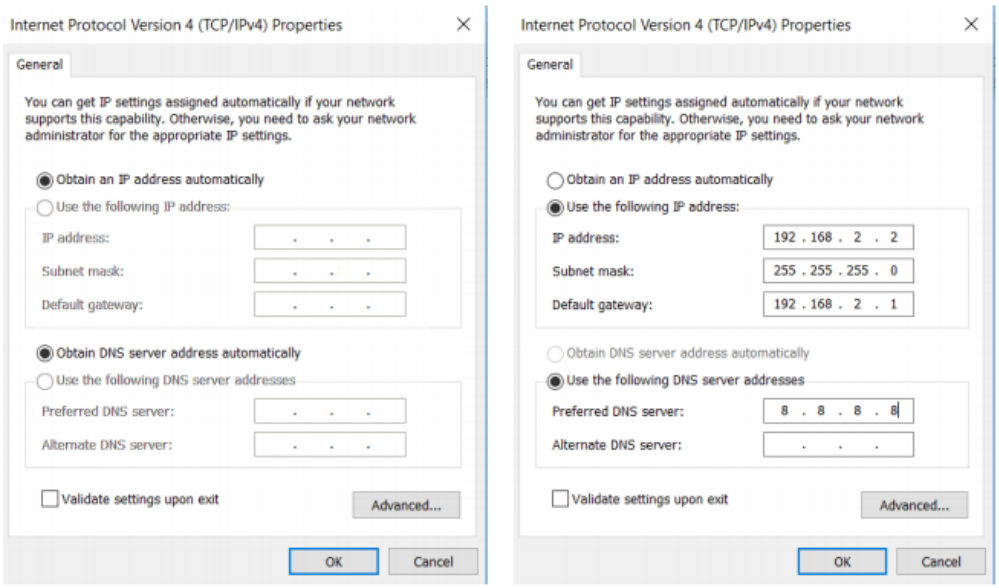
Upon installation of hardware, be sure the Ethernet card has been mounted in the supervisory PC prior to logging in the page of Web settings of the router.

I. Automatic Acquisition of IP Address (Recommended)

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

II. Set a Static IP Address

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



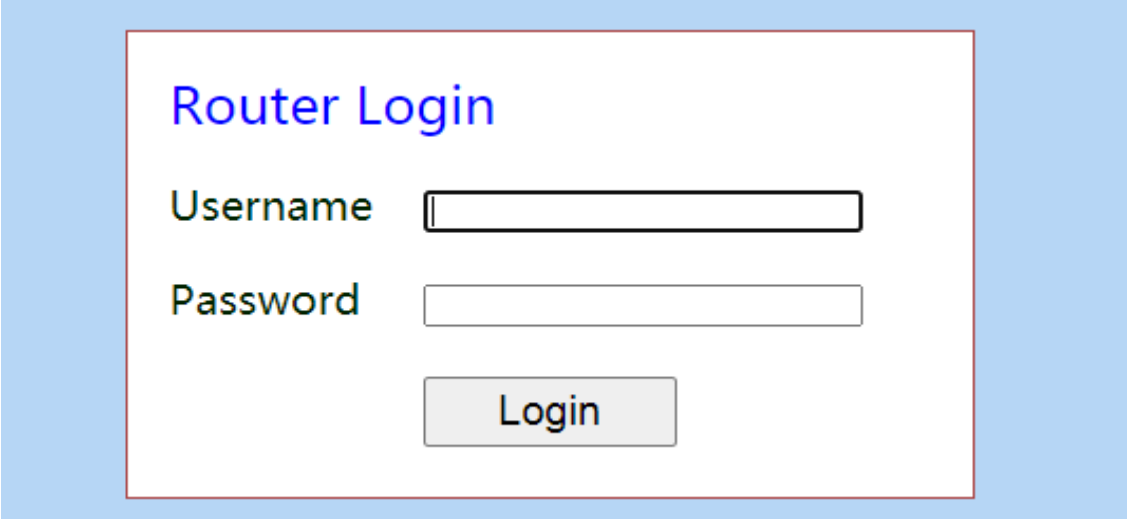
Automatic Acquisition of IP Address (left) and Static IP Address (right)

III. Cancel the Proxy Server

If the current supervisory PC uses a proxy server to access the Internet, it is required to cancel the proxy service. The operating steps are shown below: 1) In the browser window, select "tools>>Internet options"; 2) select "connection" page and click the button of LAN Settings to enter "LAN Settings" window interface. Please confirm if the option "Use a Proxy Server for LAN" is checked; if it is checked, please cancel and click the button <OK>.

IV. Log in/Exit Web Settings Page

Access to the default IP address 192.168.2.1 in a browser, enter username and password (adm/123456 by default) in pop-up window and then access to router's WEB management page. If the browser alarms the connection is not private, show advanced, and proceed to access to the address.



Note

For security, please modify the default login password after the first login and keep the password information.

III. WEB CONFIGURATION

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

3. 1 SYSTEM

This part is used to check and configure system time, router WEB configuration interface, language as well as the name of router.

3.1.1 Basic Setup

Check and set WEB configuration interface language and the name of router.

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

Table 3-1-1 Basic Setup Parameters

Basic settings		
Function description: Select display language of the router web page and set personalized name.		
Parameters	**Description**	**Default**
Language	Configure language of WEB configuration interface	English
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, it is required to set the system time in an accurate way since this function is used to configure and check system time as well as system time zone. System time page is used to configure and view system time and system time zone.

From the navigation tree, select System >> Time, then enter the “Time” webpage, as shown below.

Click <Sync Time> to synchronize the time of the router with the system time of the PC.

Table 3-1-2 Parameters of System Time

System Time

Function description: Set local time zone and automatic updating time of NTP.		
Parameters	**Description**	**Default**
Time of Router	Display present time of router	8:00:00 AM, 12/12/2015
PC Time	Display present time of PC	Present time
Timezone	Set time zone of router	Custom
Custom TZ String	Set TZ string of router	CST-8
Auto update Time	Select whether to automatically update time, you may select when startup or every 1/2/...hours.	On startup
NTP Time Servers	Select NTP server to synchronize time	1.pool.ntp.org

3.1.3 Admin Access

Admin services include HTTP, HTTPS, TELNET and SSHD.

HTTP

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

HTTPS

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

TELNET

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

SSHD

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

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

Table3-1-3 Parameters of Admin Access

Admin Access
Function description: 1. Modify username and password of router. 2. The router can be accessed by the following 4 methods, http, https, telnet and SSHD.

3. Set login timeout.		
Parameters	**Description**	**Default**
Username/Password		
Username	Set name of user who logs in WEB configuration page	adm
Old Password	Previous password access to WEB configuration page	
New Password	New password access to WEB configuration pagee	N/A
Confirm New Password	Reconfirm the new password	N/A
Amin functions		
Service Port	Service port of HTTP/HTTPS/TELNET/SSHD	80/443/23/22
Local Access	Enable - Allow local LAN to administrate the router with corresponding service (e.g. HTTP) Disable - Local LAN cannot administrate the router with corresponding service (e.g. HTTP)	Enable
Remote Access	Enable - Allow remote host to administrate the router with corresponding service (e.g. HTTP) Disable - Remote host cannot administrate the router with corresponding service (e.g. HTTP)	Enable
Allowed Access from WAN (Optional)	Set allowed access from WAN	Set the hosts which are allowed to access the router, e.g. 192.168.2.1/30 or 192.168.2.1-192.168.2.10
Description	For recording significance of various parameters of admin functions (without influencing router configuration)	N/A
Non-privileged users		
Username	Configure non-privileged login user name	N/A
Password	Configure the password of the non-privileged user	N/A
Other Parameters		
Log Timeout	Set login timeout (router will automatically disconnect the configuration interface after login timeout)	500 seconds

Note

- In “Username/Password” section, users can modify username and password rather than

create new username, i.e. only this username can be used in logins.

3.1.4 System Log

A remote log server can be set through “System Log”, and all system log will be uploaded to the remote log server through Internet. This requires remote log software, in such as Kiwi Syslog Daemon, on remote log server.

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

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

Table 3-1-4 Parameters of System Log

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

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 Configuration Management

Configuration Management		
Function description: Set parameters of configuration management.		
Parameters	**Description**	**Default**
Browse	Choose the configuration file	N/A
Import	Import configuration file to router	N/A
Backup	Backup configuration file to host	N/A
Restore default configuration	Select to restore default configuration (effective after rebooting)	N/A

Disable the hardware reset button	Select to disable hardware reset button of the router	Disable
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. Acceptable configuration will later be serially executed in order after system reboot. If the configuration files didn't be arranged according to effective order, the system won't enter the desired state.

Note

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

3.1.6 Scheduler

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

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

Table 3-1-6 Parameters of Scheduler

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

3.1.7 Upgrade

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

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

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

3.1.8 Reboot

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

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

3.1.9 Logout

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

3.2 NETWORK

3.2.1 CELLULAR

Insert SIM card and dial up to achieve the wireless network connection.

Click the “Network>>Cellular” in the navigation tree to enter Cellular configure page.

Table3-2-1-1 Parameters of Cellular

Cellular
Function description: Configure parameters of PPP dialup. Generally, users only need to set

basic configuration instead of advanced options.		
Parameters	**Description**	**Default**
Enable	Enable Cellular dialup.	Enable
Time Schedule	Set time schedule	ALL
Force Reboot	Router will reboot if cannot dialup for a long time and reach the max retry time	Enable
Shared connection (NAT)	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable
Default Route	Enable default route	Enable
SIM Network Provider	Select network provider for inserted SIM card	Profile 1
Network Select Type	Select network type, router will try 4G, 3G, 2G in proper order if select in Auto	Auto
Connection Mode	Optional Always Online, Connect On Demand, Manual. It will support to configure Triggered by SMS if select Connect On Demand mode,	Always Online
Redial Interval	Set the redialing time when dial up fails.	30 s
Show Advanced Options		
Dual SIM Enable	Some of CR202 types support eSIM, enable this option to enable eSIM dial up	Disable
eSIM Network Provider	Select network provider for eSIM card	Profile 1
eSIM Blinding ICCID	Set ICCID of eSIM	N/A
eSIM PIN Code	For setting eSIM PIN code	N/A
eSIM SIM Card Operator	Set the ISP that eSIM card connects to	Auto
Main SIM	Set the SIM card that uses to dialup at first	SIM
Max Number of Dial	Set max number of dial, if cannot dial up successfully after this number, router will switch SIM card	5
CSQ Threshold	Set threshold of signal, if current signal level is lower than this, router will switch SIM card	0(Disable)
Min Connect Time	Set the min connect time for each try of dial up	0(Disable)
Initial Commands	Set customize initial AT commands which will be operated at the beginning of dialing up	AT
Blinding ICCID	Set ICCID of SIM	N/A
PIN Code	For setting PIN code of SIM	N/A
Static MTU	Set max transmission unit after enable	Disable
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	Disable
ICMP Detection Mode	Set ICMP detection mode, router will check the link connection status via ICMP packet. Ignore Traffic: Router will send ICMP packet no matter whether there is traffic in cellular interface. Monitor Traffic: Router will not send ICMP packet if there is traffic in cellular interface.	Ignore Traffic
ICMP Detection Server	Set the ICMP Detection Server. N/A represents not to enable ICMP detection.	N/A
ICMP Detection Interval	Set ICMP Detection Interval	30 s
ICMP Detection Timeout	Set ICMP Detection Timeout (the link will be regarded as down if ICMP times out)	20 s
ICMP Detection Retries	Set the max. number of retries if ICMP fails (router will redial if reaching max. times)	5

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

Administration of Cellular - Schedule		
Function description: Online or offline based on the specified time.		
Parameters	**Description**	**Default**
Name	Name of Schedule	Schedule_1
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/LAN Switch

Click the “Network>>WAN/LAN Switch” to set WAN/LAN1 port.

When configure this port as WAN, CR202 supports three types of wired access including static IP, dynamic address (DHCP) and ADSL (PPPoE) dialing. When configure this port as LAN, it supports to jump to LAN configure page via Settings button on the right of the select box.

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

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

WAN/LAN1 is working as LAN by default.

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

WAN - Static IP		
Function description: Access to Internet via wired lines with fixed IP.		
Parameters	**Description**	**Default**
Shared connection (NAT)	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable
Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address
IP Address	Set IP address of WAN	192.168.1.29
Netmask	Set subnet mask of WAN	255. 255. 255. 0
Gateway	Set gateway of WAN	192. 168. 1. 1
MTU	Max. transmission unit, default/manual settings	default (1500)
Multiple IP support (at most 8 additional IP addresses can be set)		
IP Address	Set additional IP address of LAN	N/A
Subnet mask	Set subnet mask	N/A
Description	For recording significance of additional IP address	N/A

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

WAN - Dynamic Address (DHCP)		
Function description: Set WAN in DHCP mode to get the address allocated by other routers automatically.		
Parameters	**Description**	**Default**
Shared connection (NAT)	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable

Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address
MTU	Max. transmission unit, default/manual settings	default (1500)

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

WAN - ADSL Dialing (PPPoE)		
Function description: Set ADSL dialing parameters.		
Parameters	**Description**	**Default**
Shared connection	Enable—Local device connected to Router can access to the Internet via Router. Disable—Local device connected to Router cannot access to the Internet via Router.	Enable
Default route	Enable default route	Enable
MAC Address	MAC Address of the device	Device's MAC address
MTU	Max. transmission unit, default/manual settings	default (1492)
WAN - ADSL Dialing (PPPoE)		
Username	Set name of dialing user	N/A
Password	Set dialing password	N/A
Static IP	Click to enable and configure static IP	Disable
Connection Mode	Set dialing connection method (always online, dial on demand, manual dialing)	Always online
Parameters of Advanced Options		
Service Name	Set service name	N/A
TX Queue Length	Set length of transmit queue.	3
Enable IP header compression	Click to enable IP header compression	Disable
Use Peer DNS	Click to enable use peer DNS	Enable
Link detection interval	Set link detection interval	55 s
Link detection Max. Retries	Set link detection max. retries	10
Debug	Click to enable debug mode	Disable
Expert Option	Set expert options	N/A
ICMP Detection Server	Set ICMP detection server, blank means disable ICMP detection feature	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 LAN

Click “Network >> LAN” to configure LAN interface of router and other devices can access to Internet via Ethernet cable in LAN.

Table 3-2-3 LAN Parameters

LAN – Static IP		
Function description: Devices in LAN use static IP to connect to network.		
Parameters	**Description**	**Default**
MAC Address	MAC Address of router’s LAN gateway	Router’s LAN MAC address
IP Address	IP Address of router’s LAN gateway	192.168.2.1
Netmask	Subnet mask of LAN gateway	255.255.255.0
MTU	Max. transmission unit, default/manual settings	default (1500)
LAN Mode	Set transport mode in LAN interface	Auto Negotiation
Multi-IP Settings (at most 8 additional IP addresses can be set)		
IP Address	Set additional IP address of LAN	N/A
Subnet mask	Set subnet mask	N/A
Description	For recording significance of additional IP address	N/A
LAN Port Enable		
port1/port2	Enable corresponding LAN port	Enable
GARP		
Enable	Router will send ARP broadcast to LAN devices automatically	Disable
Broadcast Count	Set ARP broadcast times	5
Broadcast Timeout	Set ARP broadcast timeout time	10

3.2.4 Switch WLAN Mode

CR202 supports two types of WLAN mode: AP and STA

Click the “Network>>Switch WLAN Mode” menu in the navigation tree to set WLAN mode of the router. After change and save the configuration, please reboot the device to make the

configuration take effort.

3.2.5 WLAN Client (AP Mode)

When working in AP mode, CR202 WLAN will provide network access point for other wireless network devices. Please sure that CR202 has already connect to Internet via WAN or cellular.

Click the “Network>>WLAN” menu in the navigation tree to enter the “WLAN" interface.

Table 3-2-5 Parameters of WLAN Access Port

WLAN		
Function description: Support Wi-Fi function and provide wireless LAN access on site and identity authentication of wireless user.		
Parameters	**Description**	**Default**
SSID broadcast	After turning on, clients can search the WLAN via SSID name	Enable
Mode	Six type for options: 802. 11g/n, 802. 11g, 802. 11n, 802. 11b, 802. 11b/g , 802. 11b/g/n	802.11b/g/n
Channel	Select the channel	11
SSID	SSID name defined by user	inhand
Auth Mode	Support OPEN, SHARED, WEPAUTO, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA/WPA2, WPAPSK/WPA2PSK	OPEN
Encryption Method	Select encryption method of AP	NONE
Bandwidth	Support 20MHz and 40MHz	20MHz
Enable WDS	Click to enable WDS, router will connect other AP to extend wireless coverage	Disable
Default Route	Click to enable Route	Disable
Bridged SSID	Set bridged SSID of other AP, support to click “Scan” button to connect to available AP in network	None
Bridged BSSID	Set bridged BSSID of AP	None
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 other AP.

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

cellular interface in the "Network>>Cellular" should be closed.)

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

Table 3-2-6 Parameters of WLAN Client

WLAN Client		
Function description: Support Wi-Fi function and access to wireless LAN as client.		
Parameters	**Description**	**Default**
Mode	Support multiple modes including 802.11b/g/n	802.11b/g/n
SSID	Name of the SSID to be connected	inhand
Auth Mode	Keep consistent with the access point to be connected	Open type
Encryption Method	Keep consistent with the access point to be connected	NONE

3.2.7 IP Passthrough

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

Table 3-2-7 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	2 Minutes

3.2.8 Static Route

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

To set static route, click the "Network >> Static Route" menu in the navigation tree, then enter “Static Route” interface.

Table 3-2-8 Static Route Parameters

Static Route		
Function description: Add/delete additional static route of router. Generally, it's unnecessary for users to set it.		
Parameters	**Description**	**Default**
Destination Address	Set IP address of the destination	0.0.0.0
Netmask	Set subnet mask of the destination	255.255.255.0
Gateway	Set the gateway of the destination	N/A
Interface	Select WAN/CELLULAR 1/LAN/WAN(STA) of the destination	N/A
Description	For recording significance of static route address (not support Chinese characters)	N/A

3.3 SERVICES

3.3.1 DHCP Service

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

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

in the DHCP server, so the Ethernet interface of the device needs to be configured into an automatic mode.

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

Table 3-3-1 Parameters of DHCP Service

DHCP Service		
Function description: If the host connected with router chooses to obtain IP address automatically, then such service must be activated. Static designation of DHCH allocation could help certain host to obtain specified IP address.		
Parameters	**Description**	**Default**
Enable DHCP	Enable DHCP service and dynamically allocate IP address	Enable
IP Pool Starting Address	Set starting IP address of dynamic allocation	192.168. 2.2
IP Pool Ending Address	Set ending IP address of dynamic allocation	192.168.2.100
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 confliction)	N/A
IP Address	Set a statically specified IP address	192.168.2.2
Host	Set the hostname.	N/A

3.3.2 DNS

DNS (Domain Name System) is a DDB used in TCP/IP application programs, providing switch between domain name and IP address. Through DNS, user could directly use some meaningful domain name which could be memorized easily and DNS Server in network could resolve the domain name into correct IP address. Manually set the DNS, use DNS via dialing if it is empty. Generally, it needs to set only when static IP is used on the WAN port.

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

Table 3-3-2 DNS Parameters

DNS (DNS Settings)

Function description: Configure parameters of DNS.		
Parameters	**Description**	**Default**
Primary DNS	Set Primary DNS	0. 0. 0. 0
Secondary DNS	Set Secondary DNS	0. 0. 0. 0
Disable local DNS server	Not to transfer local DNS server address	Disable

3.3.3 DNS Relay

CR202 works as a DNS Agent and relays DNS request and response message between DNS Client and DNS Server to carry out domain name resolution in lieu of DNS Client.

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

Table 3-3-3 DNS Transfer Parameters

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

Caution

When enabling DHCP, the DHCP relay is also enabled automatically. Relay cannot be disabled without disabling DHCP.

3.3.4 DDNS

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

DDNS serves as a client tool of DDNS and is required to coordinate with DDNS Server. Before the application of this function, a domain name shall be applied for and registered on a proper website such as www. 3322. org.

InRouter305 DDNS service types include QDNS (3322)-Dynamic, QDNS(3322)-Static, DynDNS-Dynamic, DynDNS-Static, DynDNS-Custom and No-IP.com.

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

Table 3-3-4-1 Parameters of DDNS

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

Table 3-2-4-2 Main Parameters of DDNS

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

	dynamic domain name	
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

CR202 supports connect to InHand Device Manager for remote managing InHand products remote. Customers can manage and operate routers, check status, upgrade software in batch via this platform.

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

Table 3-3-5 Device Manager

Device Manager		
Function description: Connect the router to the platform for cloud management		
Parameters	**Description**	**Default**
Enable	Enable Device Manager	Disable
Service Type	Platform work mode: Device Manager or Custom	Device Manager
Server	Select cloud platform address, iot.inhand.com.cn: China, iot.inhandnetworks.com: global	iot.inhandnetworks.com
Secure Channel	Use encryption protocol for security data transmission between router and platform	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 SMS

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

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

Table 3-3-6 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 SMS function	Disable
Status Query	Define the English query instruction to inquire current working status of the router.	N/A
Reboot	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 mobile number	N/A
Action	Accept or block	Accept
Description	Describe SMS control.	

3.3.7 Traffic Manager

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

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

Table 3-3-7 Traffic Manager

Traffic Manager		
Function: Monitor and manage the traffic use of the router.		
Parameters	**Description**	**Default**
Enable	Click to enable the traffic manager function.	Disable
Start Day	The day to start counting data traffic every month	1
Monthly Threshold	Data traffic threshold every month	0MB
When Over Monthly Threshold	Operation when data traffic used within a month reaches the threshold: Only Reporting, Block Except Management(will not influence DM and	Only Reporting

	management requirement), Shutdown Interface	
Last 24-Hours Threshold	Data traffic threshold in last 24 Hours	0KB
When Over 24-Hours Threshold	Operation when data traffic used within 24 hours reaches the threshold	Only Reporting
Advance	Custom statistics and operations last several hours	Disable

3.3.8 Alarm Settings

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

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

- Select alarm types in the "Alarm Input" area.
- Set the alarm notification method of the console in the "Alarm Output" area.

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

3.3.9 User Experience Plan

InHand Networks' User Experience Program is designed to improve the product user experience and customer service quality.
User can disable or enable User Experience Plan in "Services >> User Experience Plan"

3.4 FIREWALL

The firewall function of the router implements corresponding control to data flow at entry direction (from Internet to LAN) and exit direction (from LAN to Internet) according to the content features of message (such as: protocol style, source/destination IP address, etc.) and ensures safe operation of router and host in local area network.

3.4.1 Basic

From the navigation tree, select Firewall >> Basic, then enter basic setup page.

Table 3-4-1 Firewall - Basic Parameters

Basic Setup of Firewall		
Function description: Set basic firewall rules.		
Parameters	**Description**	**Default**
Default Filter Policy	Select accept/block	Accept
Block Anonymous WAN Requests (ping)	Select to filter WAN detection packet like PING detection	Disable
Filter Multicast	Select to filter multicast function	Enable
Defend DoS Attack	Select to defend DoS attack	Enable
SIP ALG	Select to enable SIP ALG	Disable

3.4.2 Filtering

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

To enable Access Control from the navigation tree, select Firewall >> Filtering, then enter "Filtering" page.

Table 3-4-2 Filtering Parameters

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

3.4.3 Device Access Filtering

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

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

Table 3-4-3 Device Access Filtering Parameters

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

3.4.4 Content Filtering

Set rules to disable access to specific URLs.

From navigation tree, select "Firewall>>Content Filtering" menu, then enter “Content Filtering” page.

Table 3-4-4 Content Filtering Parameters

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

	in the system.	
Description	Record the meanings of various parameters of filtering	N/A

3.4.5 Port Mapping

Setting of port mapping can enable the host of extranet to access to specific port of host corresponding to IP address of intranet.

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

Table 3-4-5 Firewall - Port Mapping Parameters

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

3.4.6 Virtual IP Mapping

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

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

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

Virtual IP Address		
Function description: Configure parameters of virtual IP address.		
Parameters	**Description**	**Default**

Virtual IP for router	Set virtual IP address of router	N/A
Source IP Range	Set range of the external source IP addresses.	N/A
Enable	Click to enable virtual IP address	Enable
Virtual IP	Set virtual IP address of virtual IP mapping	N/A
Real IP	Set real IP address of virtual IP mapping	N/A
Log	Click to enable log and the log about virtual IP address will be recorded in the system.	Disable
Description	For recording significance of each virtual IP address rule	N/A

3.4.7 DMZ

Extranet PC can access to all ports of internal device by DMZ settings.

Router will not forward data in some of ports which is used by router service, like HTTP or HTTPS in Admin Access.

From the navigation tree, select Firewall >> DMZ.

Table 3-4-7 Firewall - DMZ Parameters

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

3.4.8 MAC-IP Binding

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

From the navigation tree, select Firewall >> MAC-IP Binding, then enter the “MAC-IP Binding” page.

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

MAC-IP Binding (at most 20 MAC-IP Bindings can be set)		
Function description: Configure MAC-IP parameters.		
Parameters	**Description**	**Default**
MAC Address	Set the binding MAC address	00:00:00:00:00:00
IP Address	Set the binding IP address	192. 168. 2. 2

Description	For recording the significance of each MAC-IP binding configuration	N/A

3.4.9 NAT

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

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

Table 3-4-9 NAT Parameters

NAT		
Function description: Configure parameters of NAT		
Parameters	**Description**	**Default**
Enable	Enable NAT	Enable
Type	Set convert type	SNAT
Proto	Select protocol	TCP
Source IP	Set source IP of the NAT rule	0.0.0.0/0
Source Port	Set source port of the NAT rule	N/A
Destination	Set destination IP of the NAT rule	0.0.0.0/0
Destination Port	Set destination port of the NAT rule	0.0.0.0/0
Interface	Set interface of the NAT rule	N/A
Translated Address	Translate the IP address if match the rule	0.0.0.0
Translated Port	Translate the port if match the rule	N/A

3.5 QoS

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

3.5.1 IP BW Limit

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

From the navigation tree, select QoS >> IP BW Limit.

Table 3-5-1 Parameters of IP BW Limit

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

3.6 TOOLS

3.6.1 PING

Enter the navigation tree, select Tools>>Ping.

Table 3-7-1 PING Detection Parameters

PING		
Function description: Use ICMP to detection the connection status between router and destination address.		
Parameters	**Description**	**Default**
Host	Address of the destination host	N/A
PING Count	Set the PING count	4
Packet Size	Set the size of PING detection	32 bytes
Expert Option	Advanced parameter of PING is available.	N/A

3.6.2 Traceroute

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

Table 3-6-2 Traceroute Parameters

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

3.6.3 Link Speed Test

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

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

3.6.4 TCPDUMP

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

Table 3-6-4 TCPDUMP Parameters

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

3.8 APPLICATION

Customize application for specific customer.

3.8.1 SMBC

Select Application >> SMBC, configure Samba client function.

Table 3-8-1 SMBC Parameters

SMBC		
Function description: configure parameters for SMBC		
Parameters	**Description**	**Default**
Enable SMBC	Enable SMBC function	disable
SMBC Configuration		
MAC address	Select or enter LAN device address manually	00:00:00:00:00:00
IP address	Corresponding IP address	N/A
Description	Description of the device	N/A

3.9 STATUS

3.9.1 System

From navigation tree, select Status >> System, then enter the “System” page.

This page displays system statistics, including name, model, serial number, description, current version, current Bootloader version, router time, PC time, UP time, CPU load and memory consumption. Allow to click the <Sync Time> button to synchronize the router with the system time of the host, as covered in the set-up chapter.

3.9.2 Modem

From navigation tree, select Status >> Modem, then enter the “Modem” page.

This page displays the basic information of dialup, including status, signal level, register status, IMEI (ESN) code, IMSI code, LAC and cell ID.

3.9.3 Traffic Statistics

Choose Status >> Traffic Statistics to go to the "Traffic Statistics" page to query traffic statistics.

This page displays the traffic statistics on the dialing interface, including the statistics on the traffic received in the latest month, traffic transmitted in the latest month, traffic received on the last day, traffic transmitted on the last day.

3.9.4 Alarm

Choose Status >> Alarm to go to the "Alarm" page to view all alarms generated in the system since power-on. You can clear or confirm the alarms.

The alarms have the following states:

- Raise: indicates that the alarm has been generated but not been confirmed.
- Confirm: indicates that the alarm cannot be solved currently.
- All: indicates all generated alarms.

The alarms are classified into the following levels:

- EMERG: The device undergoes a serious error that causes a system reboot.
- CRIT: The device undergoes an unrecoverable error.
- WARN: The device undergoes an error that affects system functions.
- NOTICE: The device undergoes an error that affects system performance.
- INFO: A normal event occurs.

3.9.5 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.

3.9.6 Network Connections

From navigation tree, select Status >> Network Connections, then enter “Network Connections” page to see the connections status.

This page shows the basis information of dialup and LAN.

WAN includes MAC address, connection type, IP address, netmask, gateway, DNS, MTU, Status and etc.

Dialup includes connection type, IP address, netmask, gateway, DNS, MTU, status and connection time.

LAN includes connection type, MAC address, IP address, netmask, gateway, MTU and DNS.

3.9.7 Device Manager

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

3.9.8 Route Table

From navigation tree, select Status >> Route Table, then enter “Route Table” page to see router status.

This page displays the active route table, including destination, netmask, gateway, metric and interface.

3.9.9 Device List

From navigation tree, select Status >> Device List, then enter “Device List” page to inquire the device list.

This page displays the device list, including interface, MAC address, IP address, host and lease (click MAC address to link to IEEE to inquire validity of the address).

3.9.10 Log

From navigation tree, select Status >> Log, then enter “Log” page.

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

3.9.11 Third Party Software Notices

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

Appendix A FAQ

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

Please first check:

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

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

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

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

Try following method to restore the device.

1. Press the RESET button immediately after power on the device.

2. When System LED is steady on, release RESET button, system LED will blink, and press the RESET button again.

3. When System LED blinks slowly, release the RESET button. The device has been restored to default settings and will start up normally later.

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

First check:

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

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

Examination:

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

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

Please make sure the firewall of your computer is disabled.

7. After InRouter establishes VPN with the VPN server, your PC under InRouter can't connect to

the server ping?

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

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

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

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

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

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

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

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

- ✧ Whether the IP Address of your computer is the same subnet with InRouter and the gateway address is InRouter LAN address.
- ✧ Check the firewall settings of the PC used to configure InRouter, whether this function is shielded by the firewall.
- ✧ Please check whether your IE has any third-party plugin (e.g. 3721 and IEMate). It is recommended to configure after unloading the plugin.

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

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

13. How to restore InRouter to factory default settings?

The method to restore InRouter to factory default settings:

1. Press the RESET button immediately after power on the device.

2. When System LED is steady on, release RESET button, system LED will blink, and press the RESET button again.

3. When System LED blinks slowly, release the RESET button. The device has been restored to default settings and will start up normally later.

Appendix B Instruction of Command Line

1 Help Command

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

1.1 Help

[Command] Help [<cmd>]

[Function] Get help from command.

[View] All views

[Parameter]

<cmd> command name

[Example]

✧ Enter:

help

Get the list of all current available command.

✧ enter:

help show

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

2 View Switchover Command

2.1 Enable

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

[Function] Switchover to privileged user level.

[View] Ordinary user view.

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

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

[Example]

Enter exit in ordinary user view:

enable 123456

Switchover to super users and the password 123456.

2.2 Disable

[Command] Disable

[Function] Exit the privileged user level.

[View] Super user view, configure view

[Parameter] No

[Example]

Enter in super user view:

disable

Return to ordinary user view.

2. 3 End and !

[Command] End or !

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

[View] Configure view.

[Parameter] No

[Example]

Enter in configured view:

end

Return to super user view.

2. 4 Exit

[Command] Exit

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

[View] All views

[Parameter] No

[Example]

- ✧ Enter in configured view:

  exit

  Return to super user view.

- ✧ enter exit in ordinary user view:

  exit

  Exit console.

3 Check system state command

3. 1 Show version

[Command] Show version

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

[View] All views

[Parameter] No

[Example]

Enter:

show version

Display the following information:

Type : display the current factory type of equipment

Serial number : display the current factory serial number of equipment

Description : www.inhand.com.cn

Current version : display the current version of equipment

Current version of Bootloader: display the current version of equipment

3. 2 Show system

[Command] Show system

[Function] Display the information of router system

[View] All views

[Parameter] No

[Example]

Enter:

show system

Display the following information:

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

3. 3 show clock

[Command] Show clock

[Function] Display the system time of router

[View] All views

[Parameter] No

[Example]

Enter:

show clock

Display the following information:

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

3. 4 Show modem

[Command] Show modem

[Function] Display the MODEM state of router

[View] All views

[Parameter] No

[Example]

Enter:

show modem

Display the following information:

Modem type

state

manufacturer

Product name

signal level

register state

IMSI number

Network Type

3. 5 Show log

[Command] Show log [lines <n>]

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

[View] All views

[Parameter]

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

[Example]

Enter:

show log

Display the latest 100 log records.

3. 6 Show users

[Command] Show users

[Function] Display the user list of router.

[View] All views

[Parameter] No

[Example]

Enter:

show users

Displayed user list of system is as follows:

User:

---

* adm

Wherein, user marked with * is super user.

3. 7 Show startup-config

[Command] Show startup-config

[Function] Display the starting device of router.

[View] Super user view and configuration view

[Parameter] No

[Example]

Enter:

show startup-config

Display the starting configuration of system.

3. 8 Show running-config

[Command] Show running-config

[Function] Display the operational configuration of router

[View] Super user view and configuration view

[Parameter] No

[Example]

Enter:

show startup-config

Display the operational configuration of system.

4 Check Network Status Command

4. 1 Show interface

[Command] Show interface

[Function] Display the information of port state of router

[View] All views

[Parameter] No

[Example]

Enter:

show interface

Display the state of all ports.

4. 2 Show ip

[Command] Show ip

[Function] Display the information of port state of router

[View] All views

[Parameter] No

[Example]

Enter:

Show ip

Display system ip status

4. 3 Show route

[Command] Show route

[Function] Display the routing list of router

[View] All views

[Parameter] No

[Example]

enter:

show route

Display the routing list of system

4. 4 Show arp

[Command] Show arp

[Function] Display the ARP list of router

[View] All views

[Parameter] No

[Example]

Enter:

show arp

Display the ARP list of system

5 Internet Testing Command

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

5. 1 Ping

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

[Function] Apply ICMP testing for appointed mainframe.

[View] All views

[Parameter]

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

count <n> testing times

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

source <ip> IP address of appointed testing

[Example]

Enter:

ping www.g.cn

Test www. g. cn and display the testing results

5. 2 Telnet

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

[Function] Telnet logs in the appointed mainframe

[View] All views

[Parameter]

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

<port>telnet port

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

[Example]

Enter:

telnet 192.168.2.2

telnet logs in 192. 168. 2. 2

5. 3 Traceroute

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

[Function] Test the acting routing of appointed mainframe.

[View] All views

[Parameter]

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

maxhops <n> tests the maximum routing jumps

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

[Example]

Enter:

traceroute www.g.cn

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

6 Configuration Command

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

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

6. 1 Configure

[Command] Configure terminal

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

[View] Super user view

[Parameter] No

[Example]

Enter in super user view:

configure terminal

Switchover to configuration view.

6. 2 Hostname

[Command] Hostname [<hostname>]

default hostname

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

[View] Configure view.

[Parameter]

<hostname> new mainframe name

[Example]

- Enter in configured view:

  hostname

  Display the mainframe name of router.

- Enter in configured view:

  hostname MyRouter

  Set the mainframe name of router MyRouter.

- Enter in configured view:

  defaulthostname

  Recover the mainframe name of router to the factory setting.

6. 3 Clock timezone

[Command] Clock timezone <timezone><n>

default clock timezone

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

[View] Configure view.

[Parameter]

<timezone> timezone name, 3 capitalized English letters

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

[Example]

- ✧ Enter in configured view:

  clock timezone CST -8

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

- ✧ Enter in configured view:

  default clock timezone

  Recover the timezone of router to the factory setting.

6. 4 Ntp server

[Command]

ntp server <*hostname*>

no ntp server

default ntp server

[Function] Set the customer end of Internet time server

[View] Configure view.

[Parameter]

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

[Example]

- ✧ Enter in configured view:

  ntp server pool.ntp.org

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

- ✧ Enter in configured view:

  no ntp server

  Disable the router to get system time via network.

- ✧ Enter in configured view:

  default ntp server

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

6.5 Config export

[Command] Config export

[Function] Export config

[View] Configure view.

[Parameter] No

[Example]

Enter in configured view:

config export

The current config. is exported.

6.6 Config import

[Command] Config import

[Function] Import config

[View] Configure view.

[Parameter] No

[Example]

Enter in configured view:

config import

The config. is imported.

7 System Management Command

7. 1 Reboot

[Command] Reboot

[Function] System restarts.

[View] Super user view and configuration view

[Parameter] No

[Example]

Enter in super user view:

reboot

System restarts.

7. 2 Enable username

[Command] Enable password [<name>]

[Function] Modify the username of super user.

[View] Configure view.

[Parameter]

<name> new super user username

[Example]

Enter in configured view:

enable username admin

The username of super user is changed to admin.

7.3 Enable password

[Command] Enable password [<password>]

[Function] Modify the password of super user.

[View] Configure view.

[Parameter]

<password> new super user password

[Example]

- Enter in configured view:

enable password

Enter password according to the hint.

7.4 Username

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

no username <name>

default username

[Function] Set user name, password

[View] Configure view.

[Parameter] No

[Example]

- ✧ Enter in configured view:

  username abc password 123

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

- ✧ Enter in configured view:

  no username abc

  Delete the ordinary user with the name of abc.

- ✧ Enter in configured view:

  default username

  Delete all the ordinary users.