InRouter6x1 Series User's Manual

InRouter 6x1 Series User's Manual

Technical Support Contact Information
InHand Networks, China
Tel: +86-010-64391099
Fax: +86-010-84170089
Email: support@inhandnetworks.com

Content

I

Introduction to InRouter 6x1

- Overview
- Package Checklist
- Product Features & Specifications
- Product Models

1.1 Overview

InRouter6x1 series products are Industrial Cellular Router that integrated 2/3G/4G network and virtual private network (VPN) technologies. The products meet fundamental needs of field communication in industry, support international commercial UMTS (HSPA+), LTE networks, and respectively backward compatible with EDGE and GPRS network.

The design of the InRouter6x1 series fully incorporated the requirements of industrial users, adopted multi-level software detection mechanism, and supporting InHand Device Manager Cloud, which facilitates remote management, ensuring stable operation of devices, achieving intelligent management. Multiple VPN protocol ensures security in data transmission, preventing malicious access and tampering of data. The humanized WEB configuration interface is easy for customer to use. It supports Wi-Fi (optional), providing wireless LAN access and wireless user identification authentication services on customer site.

The IR6x1 series wireless routers are the ideal choice for industrial usage, having low power consumption, wide working temperature range from -20° C to 70° C, small size and light weight that is easy for application in harsh, narrow industrial environment. The series includes multiple models like InRouter601, and InRouter691, and multiple types of wireless networks to meet various function needs of customers.

Important Safety Information

This product is not intended for use in the following circumstances

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

Warning

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.
The equipment intended for installation in a RESTRICTED ACCESS LOCATION

WEEE Notice

The Directive on Waste Electrical and Electronic Equipment (WEEE), which entered into force as European law on 13th February 2003, resulted in a major change in the treatment of electrical equipment at end-of-life.
The purpose of this Directive is, as a first priority, the prevention of WEEE, and in addition, to promote the reuse, recycling and other forms of recovery of such wastes so as to reduce disposal.

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

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

FCC Caution:

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

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

FCC Radiation Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

1.2 Package Checklist

We put each In Router 6x1 cellular router in a box with standard accessories. Additionally, there're optional accessories can be ordered. When you receive our package, please check carefully, and if there're items missing or appearing to be damaged, please contact with your InHand Networks sales representative.

Items in package include:

Standard Accessories:

Accessories	Description
InRouter6x1 Serials Wireless Router	1
Cable	1 Cross line,CAT-5,1.5M
Document and Software CD	1
Antenna	3 Wi-Fi(2); 2G/3G/4G(1) for IR611
Power Supply	DC9~26V

1.3 Product Features

1.3.1 Interface

Cellular Interface:

Band Options:

GSM/GPRS/EDGE:
850/900/1800/1900 MHz
UMTS /HSPA/HSPA+:
850/900/1900/2100 MHz
E-UTRA: B2/B4/B5/17

Wi-Fi (Optional)

Wireless: 150Mbps 802.11b/g/n Work mode: AP/Client

LAN

Number of Ports: 1
Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX
Magnetic Isolation Protection: 1.5 KV built-in

Serial

A. Serial Type: RS232/485
B. Serial form: COM, DB-9
C. Data bit: 5/6/7/8
D. Stop bit: 1/2
E. Check bit: N/O/D
F. Baud rate: 1,200bit/s~ 115,200bit/s

SIM Interface

SIM Control: 3 V

1.3.2 Functions

PPP

Support VPDN/APN, fast access to virtual private dial-up network (VPDN) provided by mobile operator, ensure high-security data transmission.
Support CHAP/PAP/MS-CHAP/MS-CHAP V2 authorization
Support Connection Detection, auto-recovery, auto-link, ensure reliable communication.
Support On-demand connection, SMS Activity

Wi-Fi (Optional)

Wireless: 150Mbps 802.11b/g/n Work mode: AP/Client

Authentication: open, WEP, WPA/WPA-2(Personal), PA/WPA-2(Enterprise)

Dynamic IP

Support DHCP, applied as Server/Client

Dynamic DNS

Support Dynamic DNS-IP Binding

Provide DDNS analyze to help access dynamic data center

Flux Management

Support rate limiting,

Firewall Function

Package filtering

Port Mapping

Virtual Address Mapping

DMZ zone

MAC addresses binding.

Route function

Support Static Routing Table

VPN (for IR691 only)

IPSec/SSL VPN

L2TP/PPTP VPN

GRE

Link Backup

VRRP

Support VRRP protocols, realizing immediate link backup

DNS Forwarding

Support DNS Forwarding, support DNS record

Network tools

Support Ping, Trace Route and Telnet

1.3.3 Environmental Limits

Operating Temperature: -20 to 70°C

Operating Humidity: 5 to 95% RH

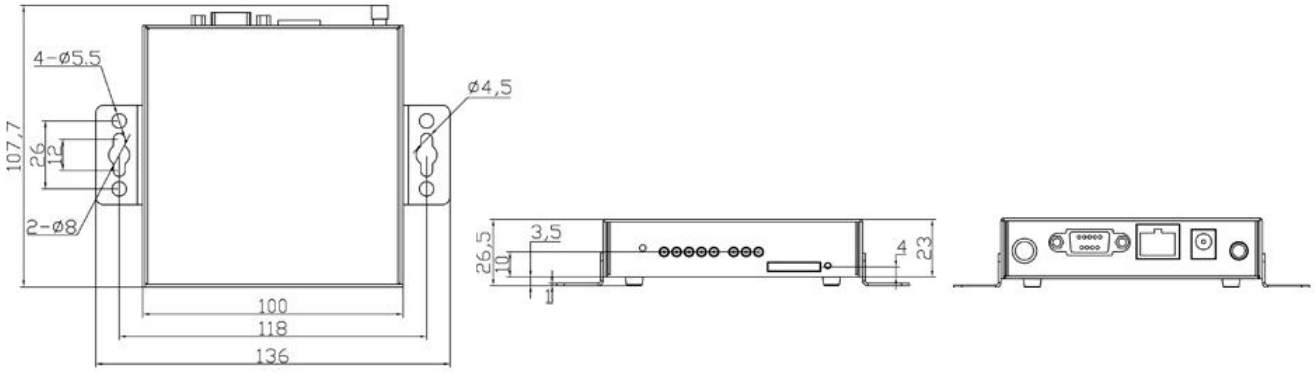
Storage Temperature: -40 to 85°C

1.3.4 Power Requirements

Power Inputs: 1 terminal block, including power jack and serial.
Input Voltage: 9 -26 VDC

1.3.5 Physical Characteristics

Housing: Steel, providing IP30 protection
Weight: 490g
Dimensions (mm)



1.3.6 Advanced Industrial Characteristics

Physical Characteristics:
Shell: Metal, IP30

1.3.7 Device Management Software

Device Manager:
Centralized management solution for InHand Networks Devices

1.3.8 Warranty

Warranty Period: 1 year (Optional service for 3 years)

1.4 Product Models

The models are classified according to main differences on cellular network support, VPN support (Once the InRouter supporting WIFI release, we will upgrade this list).

Model	IR6x1
Part Number	**IR6<X>1<N>-<W>-<S>**
X (Option VPN)	**0**：standard router **9**：VPN, support IPSec/OpenVPN/PPTP/L2TP/GRE
N (Network)	Quad band HSPA+/HSPA/UMTS: 850/900/1900/2100MHz Quad band GSM: 850/900/1800/1900MHz E-UTRA:B2/B4/B5/B17
W (WIFI)	**<NA>:** No Wi-Fi function **AP:**Wi-Fi AP model **STA:**Wi-Fi client model
S (Serial Port)	**<NA>**：RS232 **485** ：RS485
Example	**IR691PH09-AP**： UMTS, Support VPN(IPSec/PPTP/L2TP/GRE) ,Wi-Fi AP, RS232 serial port

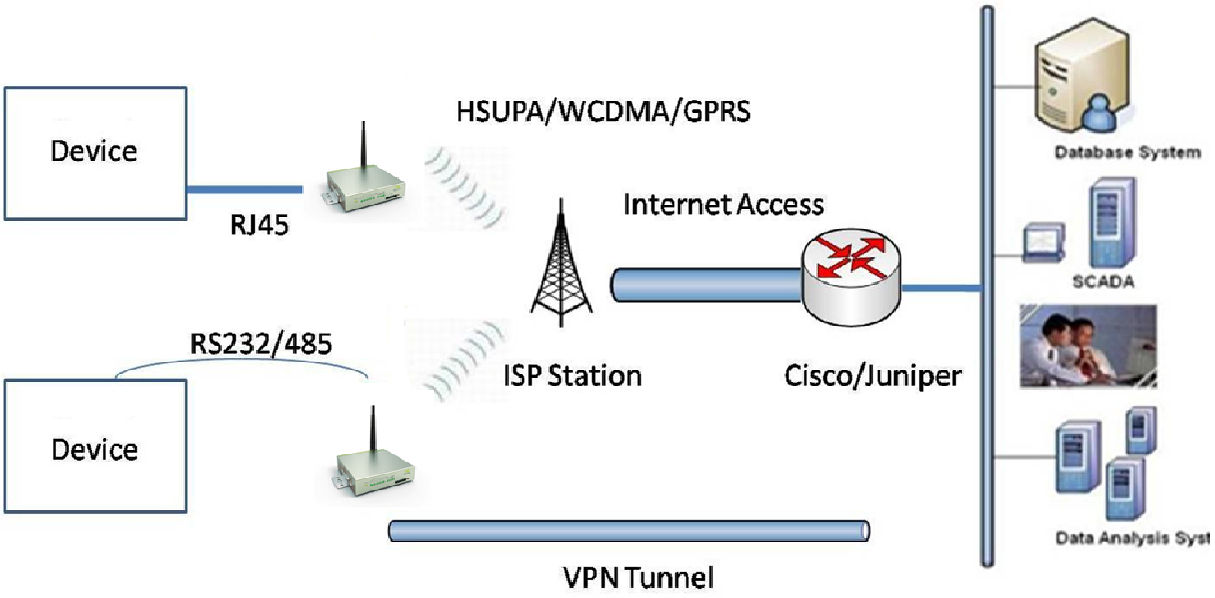
Notice: IR691PH09-AP/STA does not support Open VPN.

II

Quick Installation Guide

- Typical Application
- Panel Layout
- Quick Connect to Internet
- Quick IPSec VPN Configuration
- Reset to Factory Defaults

2.1 Typical Application

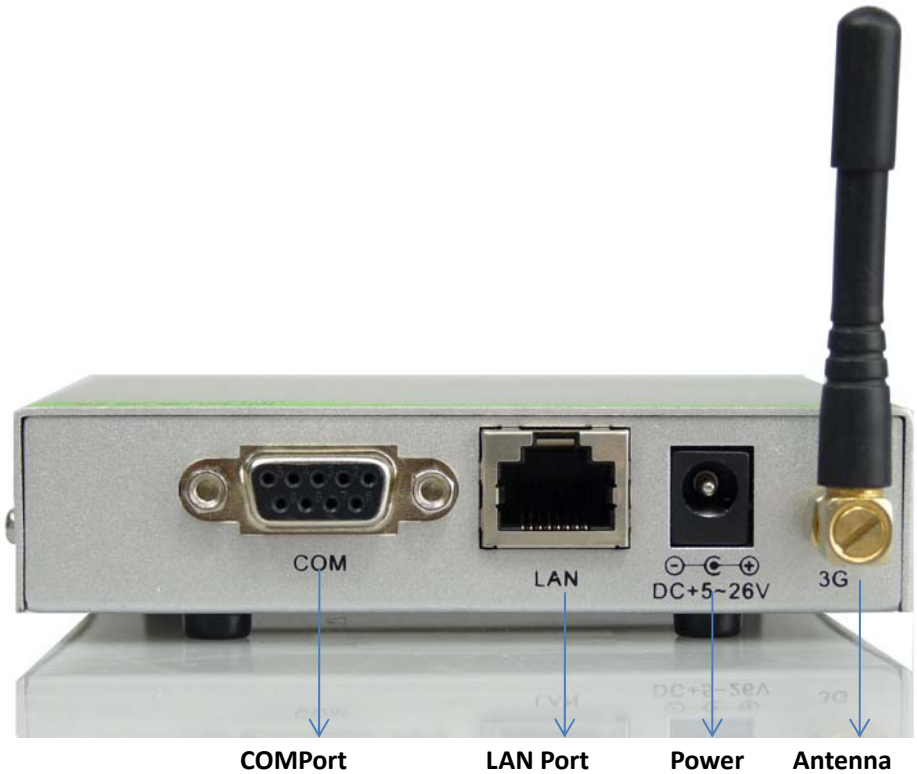


InRouter6x1 series can be used to connect your device (with RS232/485/Ethernet Interface) to internet via GPRS/HSUPA cellular network. Meanwhile, to ensure the security and access, InRouter6x1 series support VPN, enabling remote access and secure data transmission through Internet.

2.2 Panel Layout

Front view:

Back view:



Interface	Description
Power Interface	Access 9-26V DC Power Supply
Serial	Access to the serial line, realizing
Ethernet Ports	One 10/100Base-TX RJ45 Port (IR601,IR611)
ANTENNA	2.5G/3G antenna
SIM Card Connector	Hold SIM card

Description of LED

Legend: On-- **Off--** **Blink--**

Power on

Start to run firmware

Begin dial to Internet

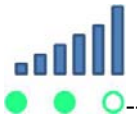
Connect to internet

Upgrading firmware

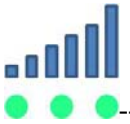
Restore factory default

Signal Status LED Description

----- Signal: 1-9 (poor signal level, router cannot work, please check the antenna and local signal level)



------ Signal: 10-19 (Router can work under this signal level)



------ Signal: 20-31 (Perfect signal level)

2.3 Quick Connection to Internet

2.3.1 Insert SIM Card

Push the yellow button next to the SIM card slot, then insert SIM card in the slot.

2.3.2 Antenna Installation

After installing IR6x1, connect the interface of enhanced antenna to the interface of skin antenna and screw tightly. Put the amplifier of enhanced antenna to where it can receive the signal well.

Attention: Position and angle of the antenna may influence the quality of signal.

2.3.3 Power Supply

Connect InRouter to power supply with the power supply cord in the package, observe whether the Power LED on the panel of InRouter goes on. If not, please contact InHand for technical support.
You can start to configure IR6X1 after the Power LED turns on.

2.3.4 Connect

Link IR6x1 with a PC:

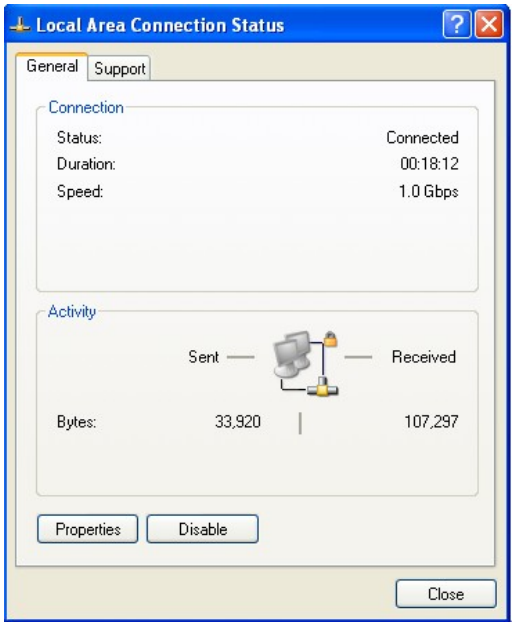
(1) Use a cable to link IR6x1 with a PC;

(2) After connected, you can see one LED of RJ45 Interface turns green and the other flashes.

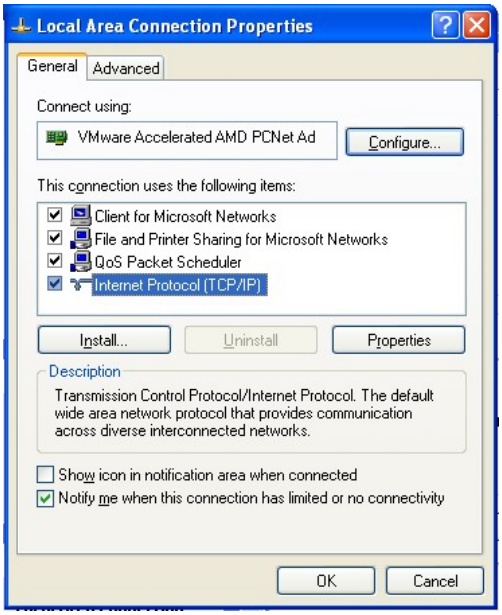
2.3.5 Build Connection between InRouter and PC

IR6x1 Router can auto-distribute IP address for PC. Please set the PC to automatically obtain IP address via DHCP. (Based on Windows Operation System):

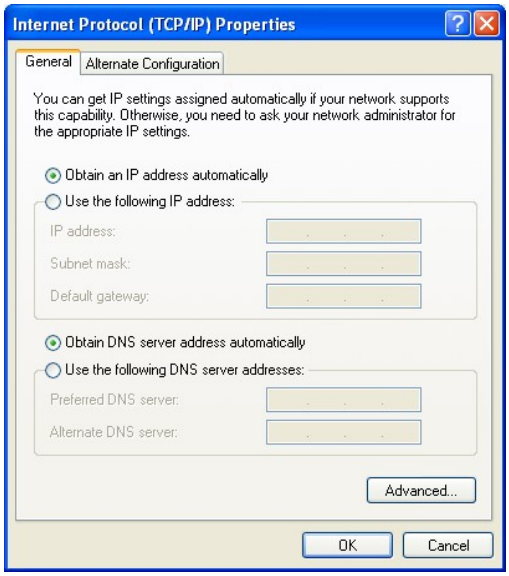
1) Open “Control Panel”, double click “Network Connections” icon, and enter “Network Connections” Screen.
2) Double click “Local Area Connection”, enter “Local Area Connection Status” screen:



3) Click “Properties”, enter “Local Area Connection Properties” screen



Choose “Internet Protocol (TCP/IP)” and click on “Properties”, ensure your PC can obtain IP and DNS address automatically. (Or you can set your PC in the subnet: 192.168.2.0/24, for example, set as IP: 192.168.2.10, Net Mask: 255.255.255.0, Default Gateway: 192.168.2.1)

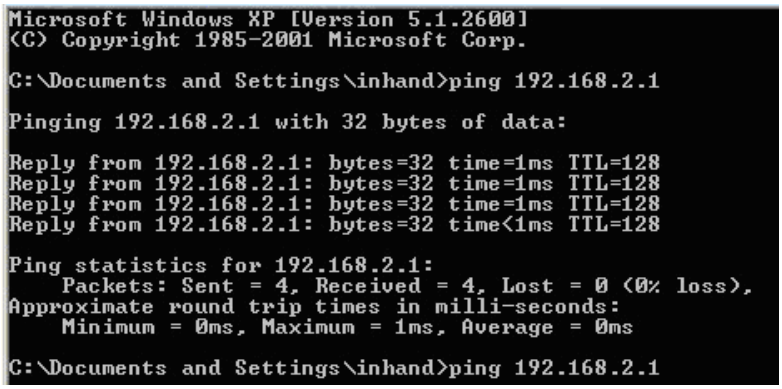


Click “OK”, InRouter will allocate an IP address: 192.168.2.x, and a gateway: 192.168.2.1(the default address of IR6x1).

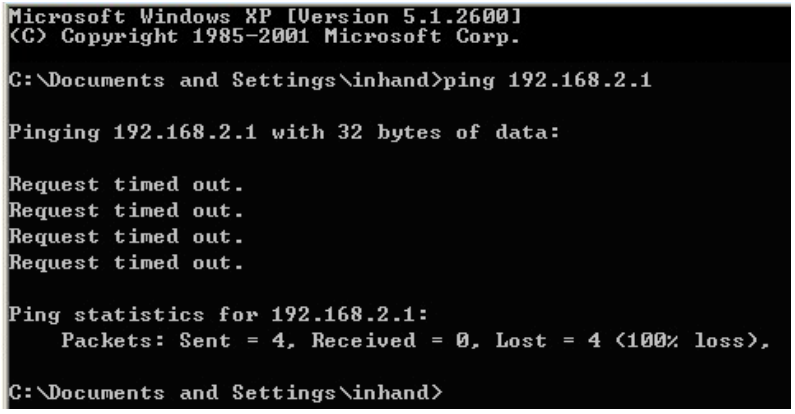
After configure TCP/IP protocols, you can use ping command to check whether the link between PC and Router is built correctly. Below is an example to execute Ping command under Windows XP:

Ping 192.168.2.1

If the screen shows:



Then the PC and InRouter are correctly connected. Else if it shows:

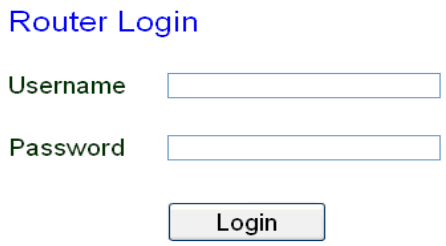


The connection is not built, you need to check step by step starting from Section 2.3.4.

2.3.6 Start to configure your InRouter6x1(Optional)

After you have finished the former steps, you can start to configure the InRouter:

1) Open IE browser, input the default IP address of the Router: http://192.168.2.1, you can see the login page as below:



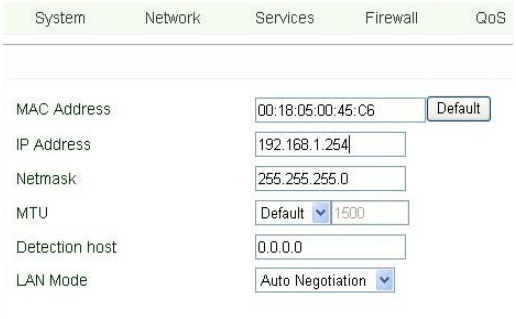
Input “username” (default: adm) and “password” (default: 123456), then click “login” to enter the operation screen.

2) Change IP address:

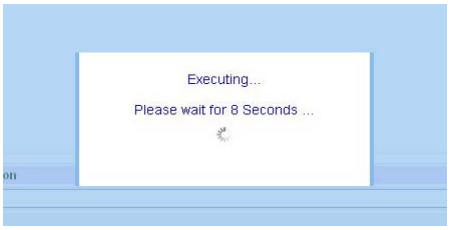
Attention: After updating the configuration, please click “apply” to activate your configuration.

If you want to set your own IP of InRouter 6x1, please follow the instructions below:

Click “Network”=>“LAN”, change the IP address to 192.168.1.254:



3) Click “Apply”, then you will see:

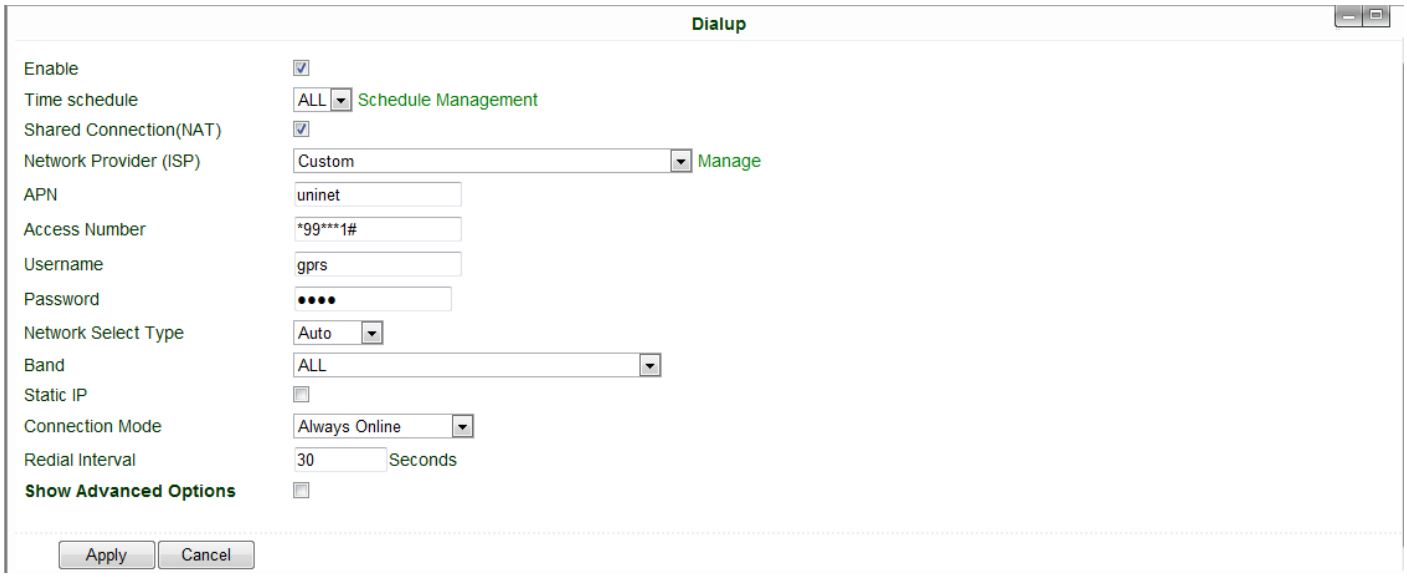


Now the IP address of IR6x1 has been reset, and in order to enter the configuration page, you need to set your PC in the same subnet as InRouter, for example: 192.168.1.10/24,then input the updated IP address (192.168.1.254) in your IE Browser.

2.3.7 Connect InRouter with Internet

Follow the configuration steps below to enable IR6X1 to connect to Internet.

Click “Network”=>“Dialup”, enter dialup configuration interface:



Please check the APN, Dialup Number, Username and Password.

Dialup Number, Username and Password are provided by local mobile operator. The following examples show parameters provided by China Mobile, Vodafone. Please contact with local operator for details.

1: China Mobile

APN: CMNET

Phone Number: *99#

User Name: web

Password: web

2: Vodafone

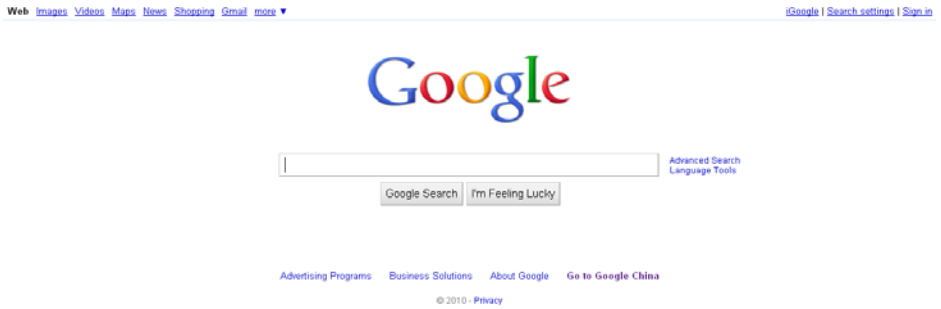
APN: internet

Phone Number: *99#

User Name: web

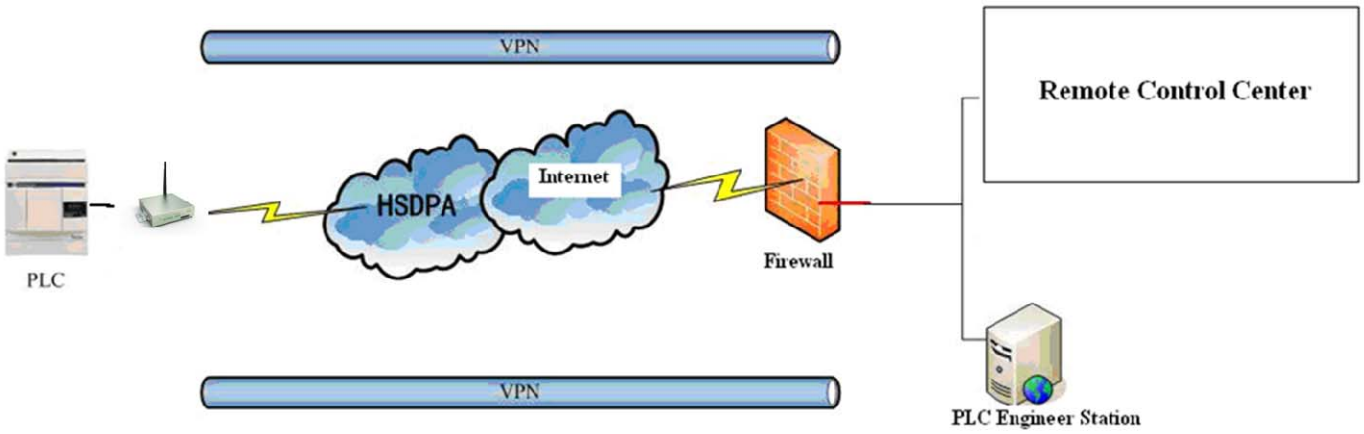
Password: web

After correctly configuring, InRouter6x1 can now access Internet. Open IE Browser, input www.google.com, you sould see the Google home page:

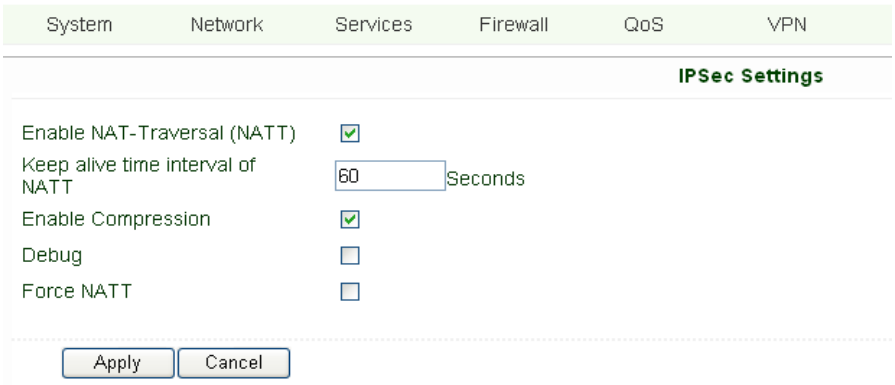


2.4 Quick IPSec VPN Configuration

If you need to build a VPN tunnel to access to your remote PLC through Internet or you need to ensure security of the data transmission, here's a quick configuration guide of IPSecfor InRouter6x1 Series



Connect PC with InRouter to enter router configuration interface, select “VPN” => “IPSec setting”:



Enable NAT-Traversal (NATT): select enable.

Keep alive time interval of NATT: set the “Keep alive time interval of NATT”, default is 60 seconds.

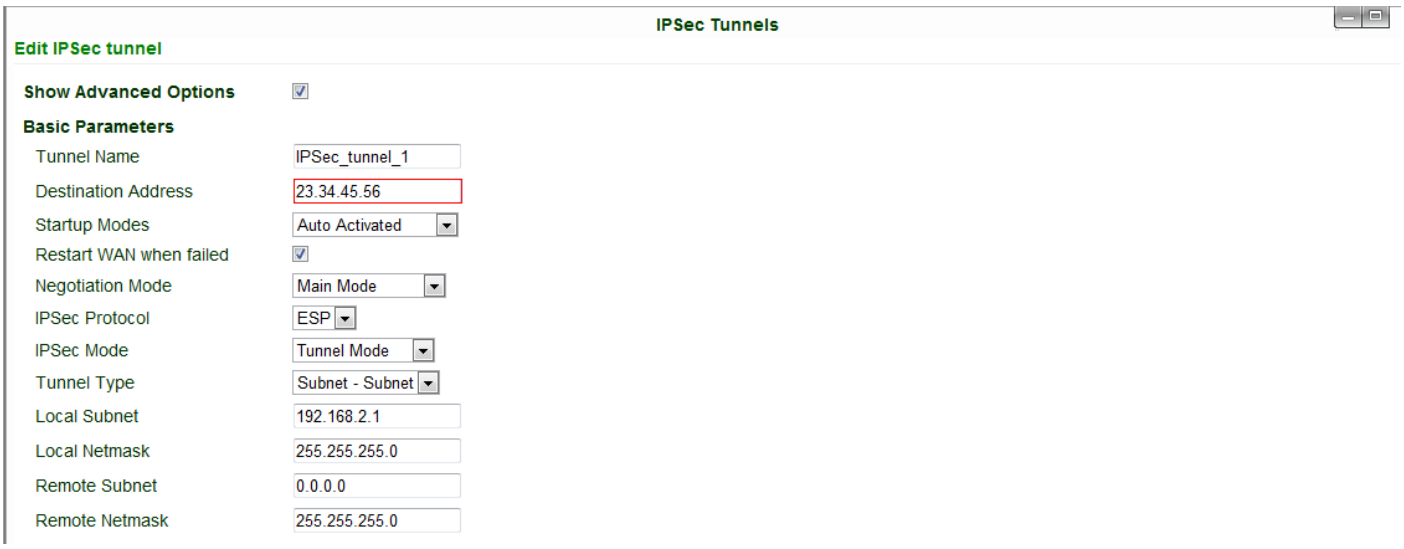
Enable Compression: select enable.

Please change the parameters according to actual situation.

Click “Apply” to complete the configuration.

1） Select “VPN”=> “IPSec Tunnels” to check or modify parameters of IPSec Tunnels.

Click “Add” to add a new IPSec Tunnel:



Basic Parameters: basic parameters of IPSec tunnel.

Tunnel Name: name IPSec tunnel, the default is IPSec_tunnel_1.

Destination Address: set to VPN server IP/domain, e.g.: the domain provided by GJJ is gjj-ovdp.3322.org.

Startup Modes: select Auto Activated.

Negotiation Mode: optional between Main Mode and Aggressive Mode. Generally, select Main Mode.

IPSec Protocols: optional among ESP, AH. Generally, select ESP.

IPSec Mode: optional between Tunnel Mode and Transport Mode. Generally, select Tunnel Mode.

Tunnel Type: optional among Host-Host, Host-Subnet, Subnet-Host and Subnet-Subnet.

Local Subnet: IPSec local subnet protected. E.g.: 172.16.16.0.

Local Net Mask: IPSec local Net Mask protected. E.g.: 255.255.255.252.

Remote Subnet: IPSec remote subnet protected. E.g.: 172.16.0.0.

Remote Net Mask: IPSec remote Net Mask protected. E.g.: 255.240.0.0.

Phase 1 Parameters: configuration parameters during Phase 1 of IPSec negotiation.

IKE Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IKE Lifetime: the default is 86400 seconds.

Local ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Remote ID Type: optional among FQDN, USERFQDN, IP address, suggest selecting IP address.

Authentication Type: optional between Shared Key and Certificate, generally choose Shared Key.

Key: set IPSec VPN negotiating key.

Phase 2 Parameters: configuration parameters during Phase 2 of IPSec negotiation.

IPSec Policy: optional between 3DES-MD5-96 and AES-MD5-96, suggest selecting 3DES-MD5-96.

IPSec Lifetime: the default is 3600 seconds.

Perfect Forward Encryption: Optional among None, GROUP1, GROUP2 and GROUP5. This parameter should match with the server, generally, select “None”.

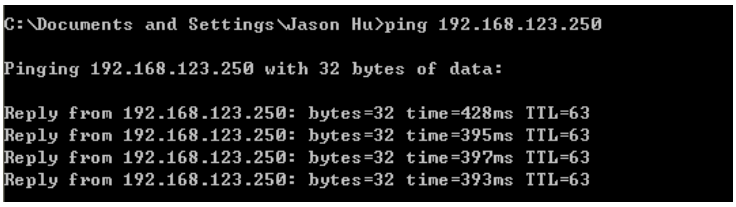
Click “Save” to finish adding IPSec Tunnel:

You can click “Show Detail Status” to observe the specific connection details, or click “Add” to add a new tunnel. Now you have successfully built a high-security IPSec tunnel.

Here’s an example. We set an IPSec Tunnel from subnet: 192.168.220.0/24 to subnet: 192.168.123.0/24, when it succeeds, the screen will show:

And the PC in IPSec client subnet can get access to the server’s subnet.

Open command in your PC, then ping a PC in the server’s subnet:

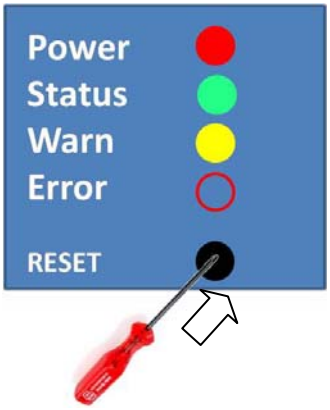


2.5 Reset to Factory Defaults

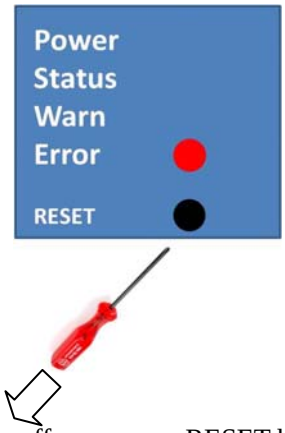
2.5.1 Hardware Approach

Legend: On-- **Off--** **Blink--**

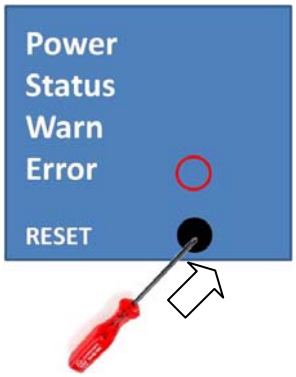
1) Press and hold RESET button while turning on IR6x1:



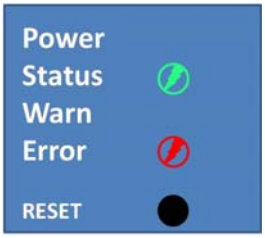
2) When you see ERROR LED turns on (about 10 seconds after power on), release the RESET button:



3) After a few seconds, the ERROR LED will turn off, now press RESET button again:



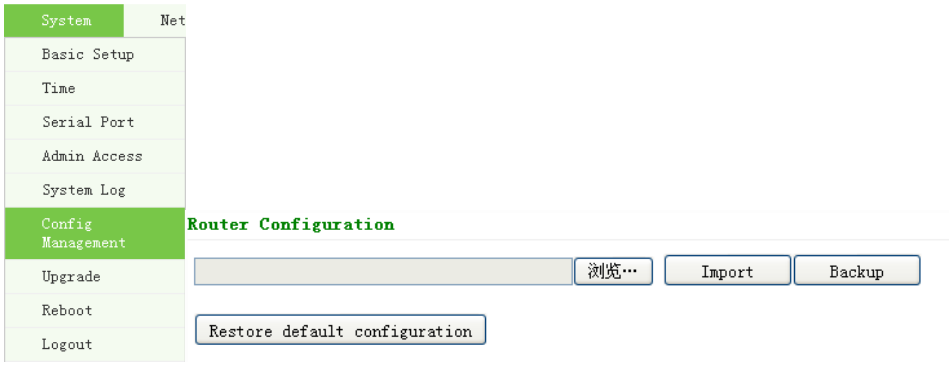
4) Then you will see ERROR and STATUS LED blink, which means reset to factory defaults succeed!



Factory default settings:
IP: 192.168.2.1
Net Mask: 255.255.255.0
Serial parameter: 19200-8-N-1

2.5.2 Web Approach

1) Login the web interface of IR6x1, select “System”→”Config Management”:



2) Click “Restore default configuration” to Reset IR6x1.

III

Advanced Configuration

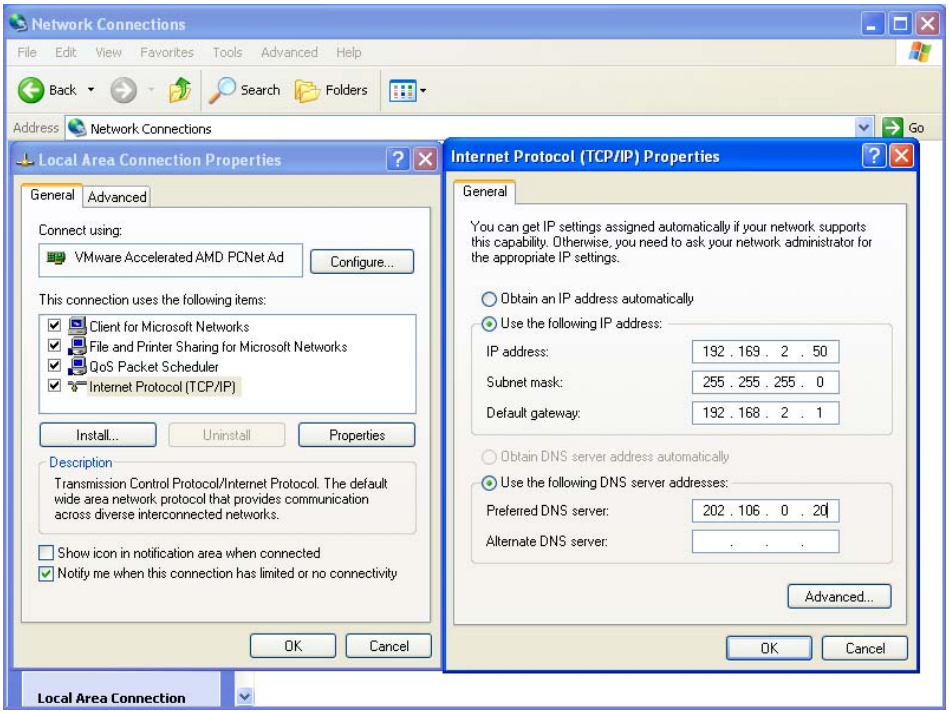
- Configuration on Web
- CLI Configuration

3.1 Configuration on Web

InRouter must be correctly configured before use. This chapter will show you how to configure InRouter via Web interface.

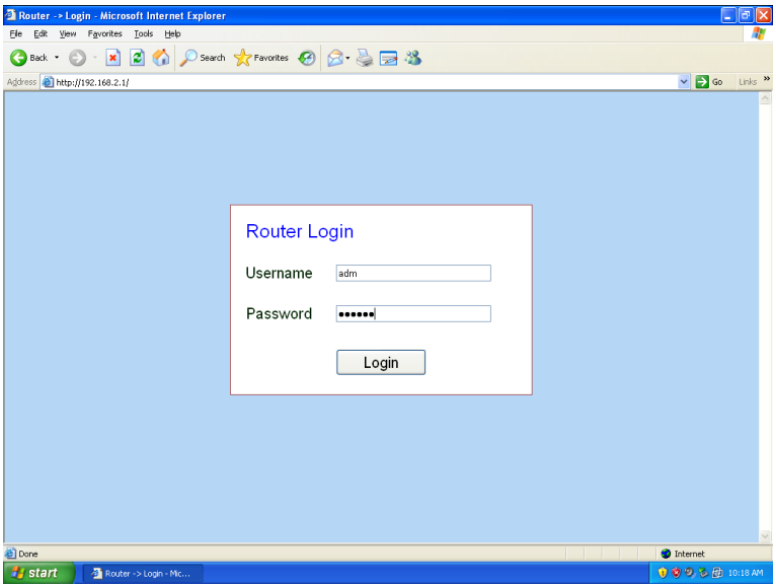
3.1.1 Preparation

First, connect your device to IR6x1 with a cable or a HUB (switch), then set the IP of PC and IR6x1 in the same subnet, for example: Set PC IP to 192.168.2.50, net mask: 255.255.255.0, gateway (default IP of IR6x1: 192.168.2.1):

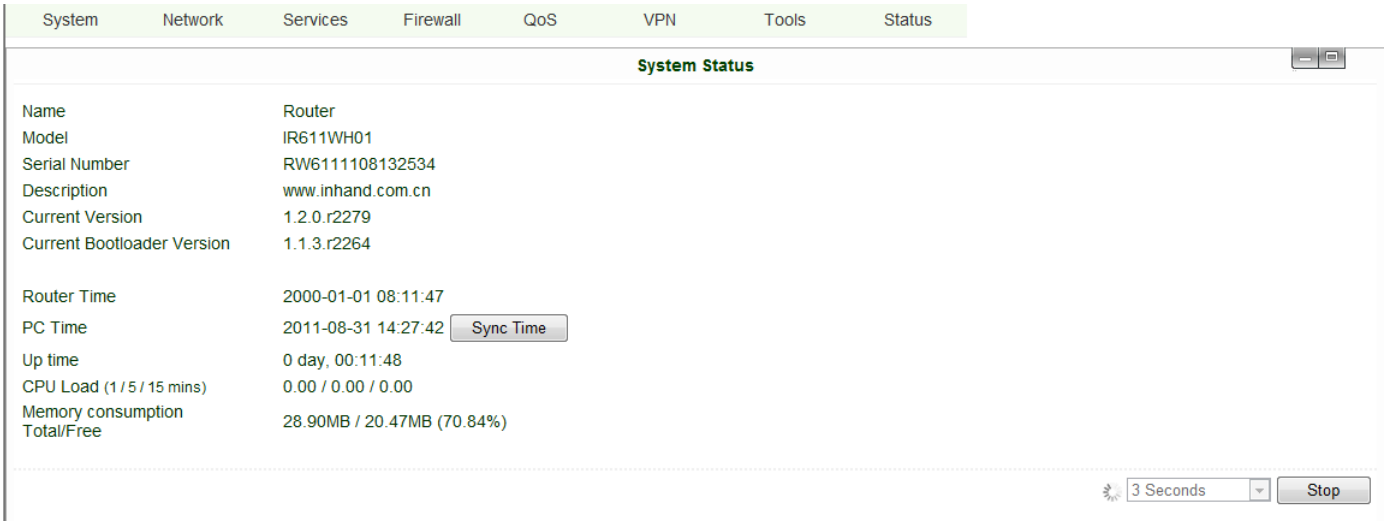


Open IE browser, input the IP address of IR6x1: http://192.168.2.1 (default IP of IR6x1).

Then you'll see the Login window pop up, you need to login as Administrator. Input the username and password (default: adm/123456).



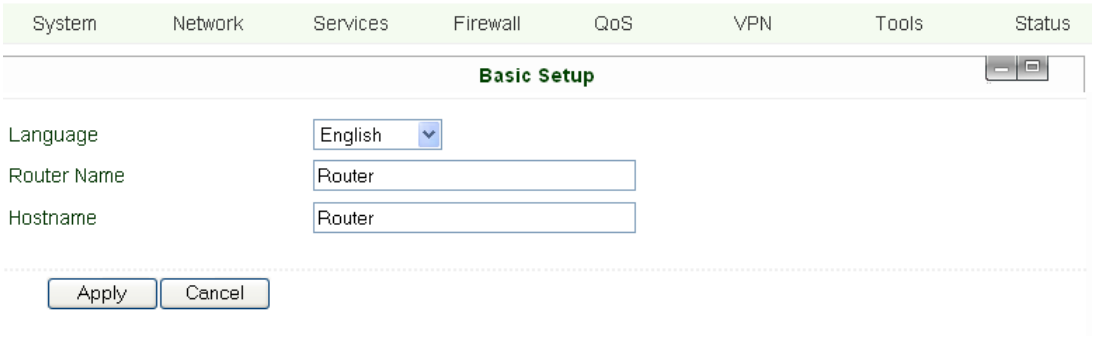
Click "Login" to enter the configuration interface:



3.1.2 System

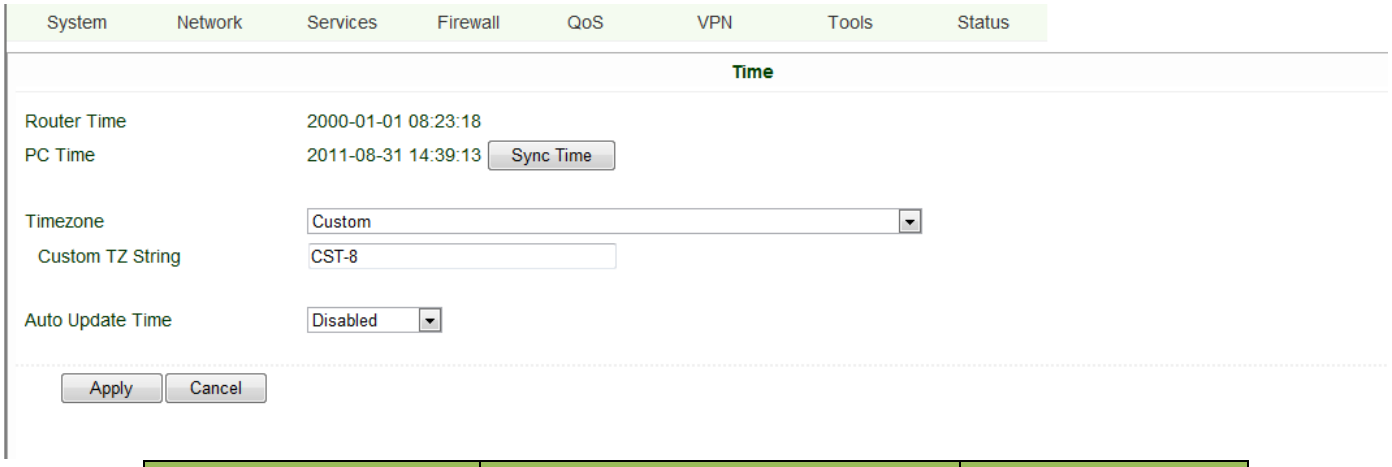
System settings include 9 parts: Basic Setup, Time, Serial Port, Admin Access, System Log, Config Management, Update, Reboot and Logout.

(1) Basic Setup



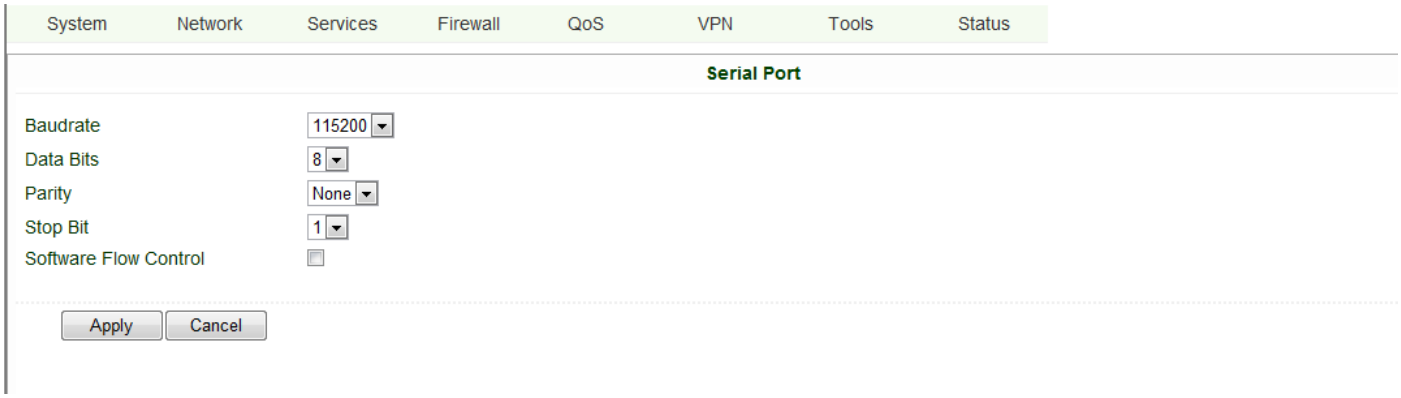
Parameters Name	Description	Default	Example
Language	Choose language of configuration web	Chinese	English
Router Name	Set name of InRouter	Router	My InRouter
Host Name	Name the device/PC linked with IR6X1	Router	My InRouter

(2) Time



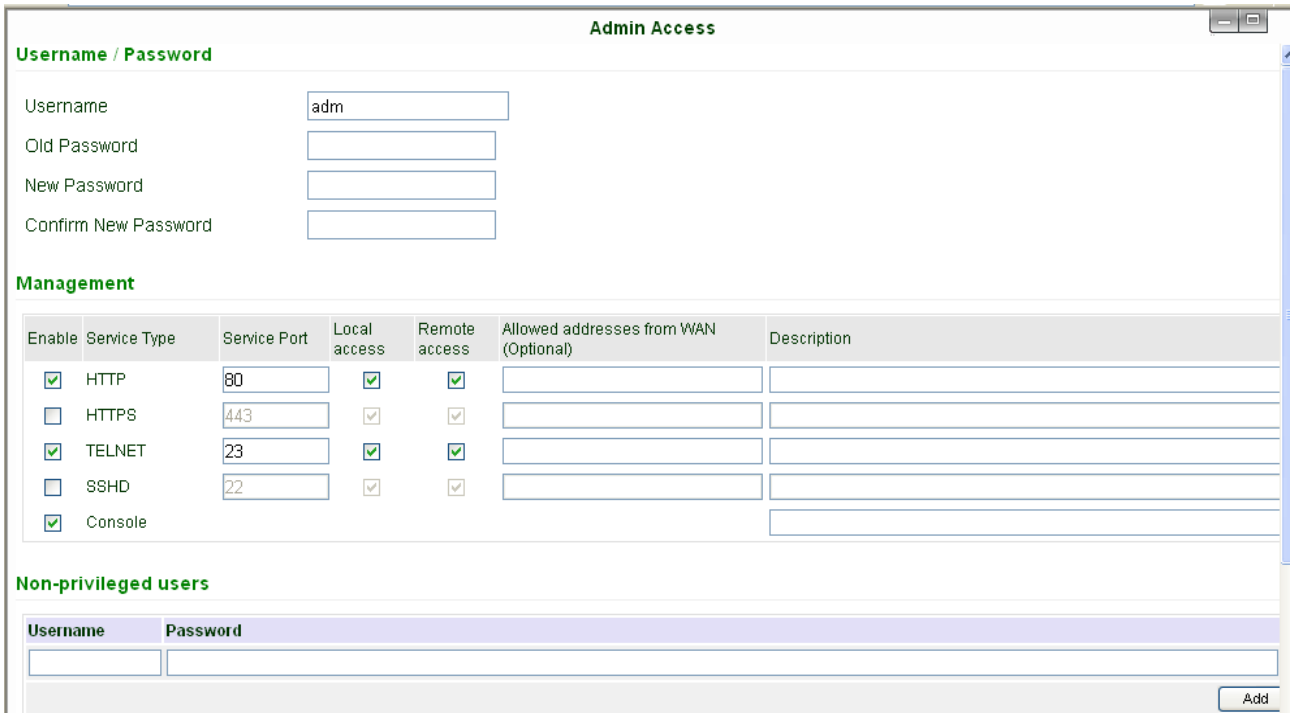
Name	Description	Default
Router Time	Display router time	2000-01-01 8:00:00
PC Time	Display PC time (or the time of device linked with router)	
Time Zone	Set time zone	Custom
Custom TZ string	Set the string of time zone of Router	CST-8
Auto Update Time	Time Update Interval	Disabled
NTP Time Servers (after enable the Auto Update Time)	Setting for NTP Time server. (Three at the most)	pool.ntp.org

(3) Serial Port



Name	Description	Default
Baud Rate	Serial baud rate	115200
Data Bit	Serial data bits	8
Parity	Set parity bit of serial data.	None
Stop Bit	Set stop bit of serial data.	1
Hardware Flow Control	Enable Hardware Flow Control	Disable
Software Flow Control	Enable Software Flow Control	Disable

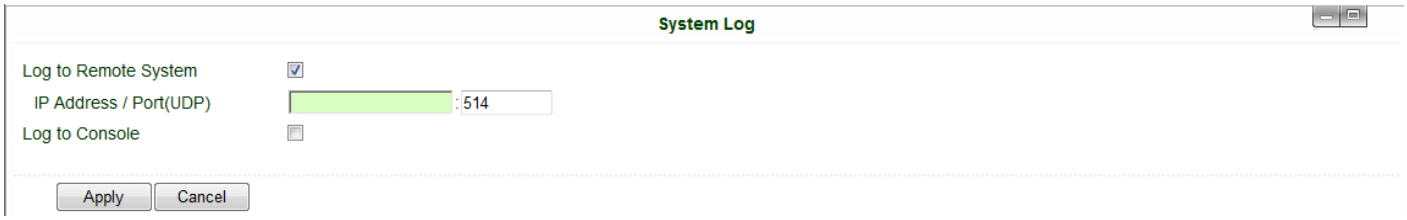
(4) Admin Access



Name	Description	Default
Username/Password		
Username	Username for configuration web login	adm
Old Password	To change the password, you need to input the old one	123456
New Password	Input new password	

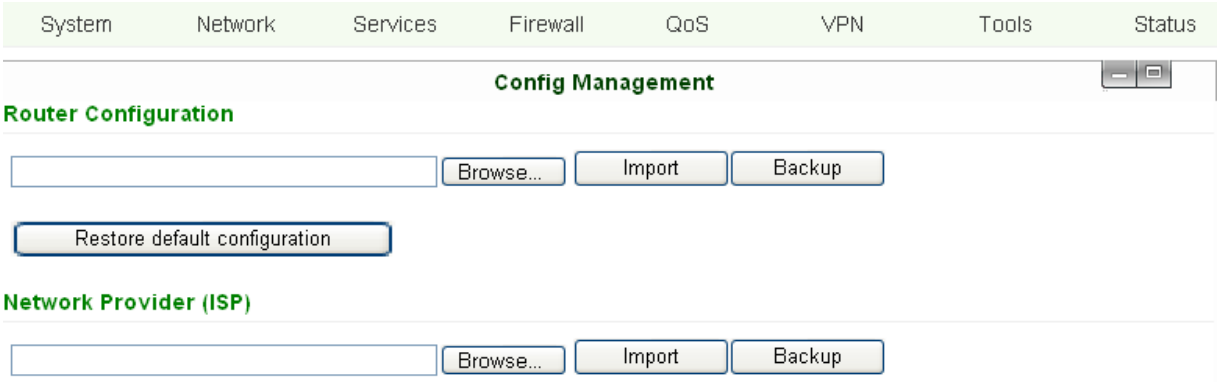
Confirm New Password	Input the new password again	
Management		
HTTP/HTTPS/TELNET/SSHD/Console		
Enable	Select to enable	Enable
Service Type	HTTP/HTTPS/TELNET/SSHD/Console	80/443/23/22/Blank
Local Access	Enable—allow manage Router by LAN(e.g.: HTTP) Disable—forbid manage Router by LAN.	Enable
Remote Access	Enable—allow to manage IR6x1 by WAN. (e.g.: HTTP) Disable—forbid to manage IR6x1 by WAN. (e.g.: HTTP)	Enable
Allowed Access from WAN (Optional)	Set the range of allowed IP address for WAN (HTTP/HTTPS/TELNET/SSHD)	Control services server can be set at this time, for example 192.168.2.1/30 or 192.168.2.1-192.168.2.10
Description	Describe the parameters of management (non-influence to IR6x1)	
Other Parameters		
Log Timeout	Set the Log Timeout, configuration web will be disconnected after timeout	500 seconds

(5) System Log



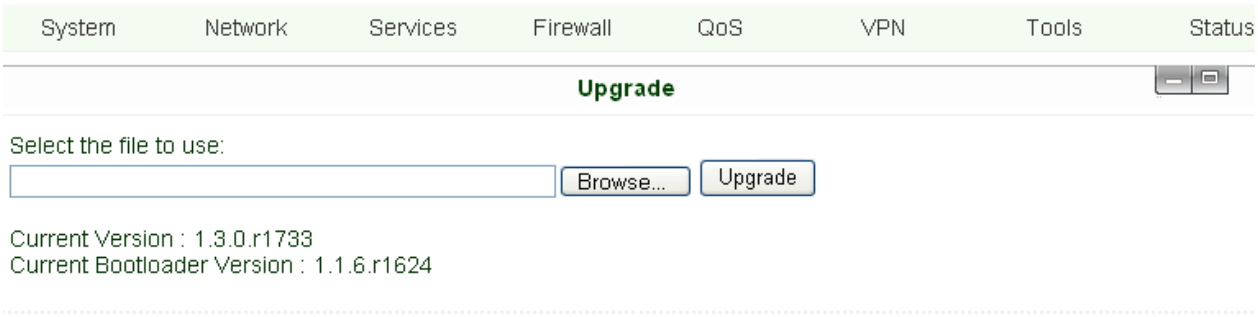
Name	Description	Default
Log to Remote System	Enable remote log server	Disable
IP address/Port (UDP)	Set the IP and Port of remote log server	Port: 514
Log to Console	Enable remote log server	Disable

(6) Config Management

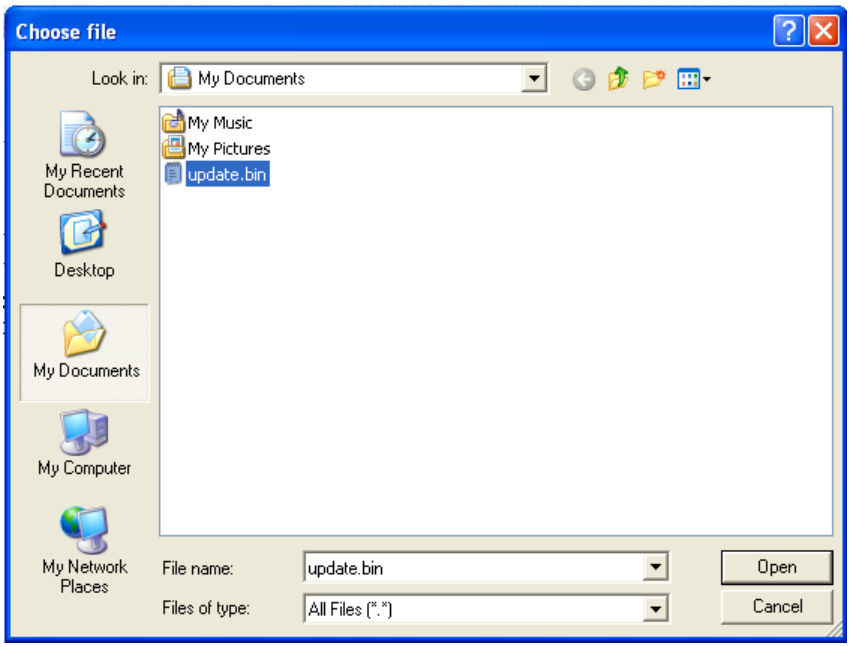


Name	Description
Router Configuration	Import/Backup configuration file
Restore default configuration	Click to reset IR6X1 (to enable RESET, you need to reboot IR6X1)
Network Provider (ISP)	Used to configure the APN, username, password and other parameters of major operators

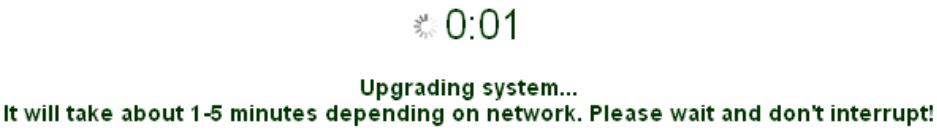
(7) System Upgrade



To upgrade the system, click “System”=>”System upgrade” to enter upgrade page, then follow the steps below:
Click “Browse”, choose the upgrade file;



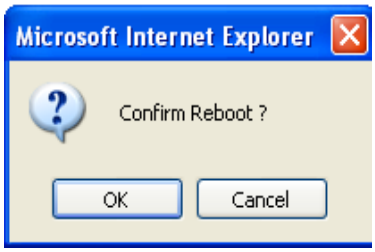
Click “update”, and then click “sure” to begin update, the window will show as below.



Upgrade firmware succeed, and click “reboot” to restart IR6X1.

(8) Reboot

If you need to reboot system, please click ”System”=>”Reboot”, Then click ”OK” to restart system.



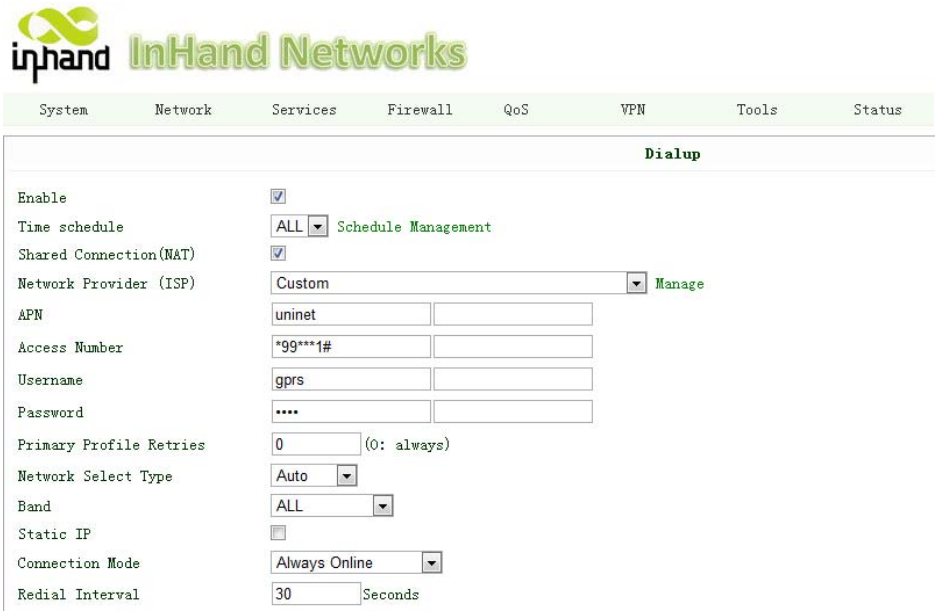
(9) Logout

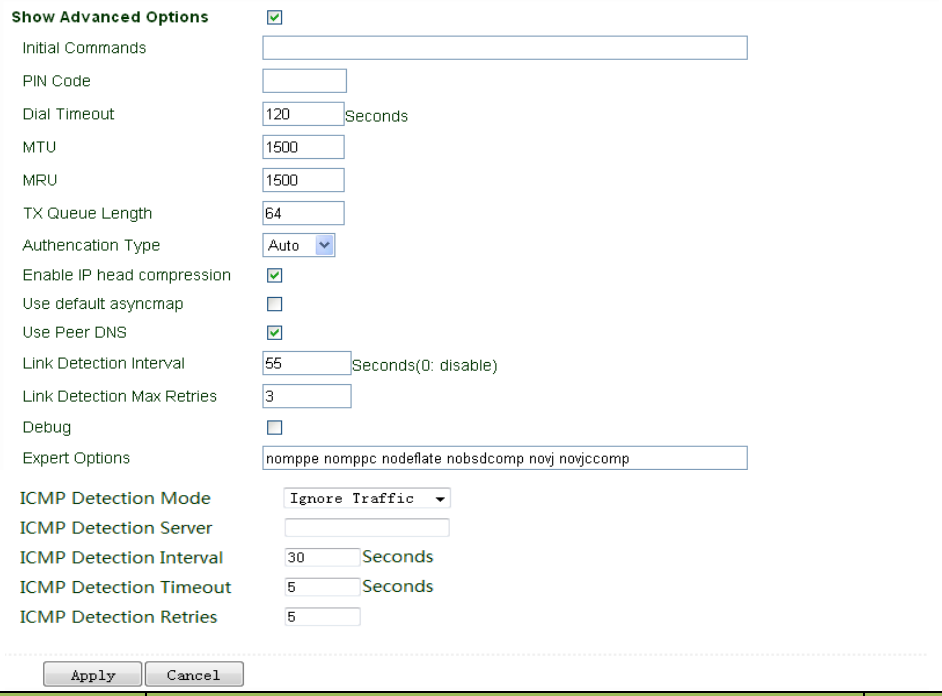
If you need to logout system, click “System”=>”Logout”, and then click “OK”.

3.1.3 Network

Network settings include Dialup, LAN, WLAN, DNS, DDNS, Static Route,etc.

(1) Dialup

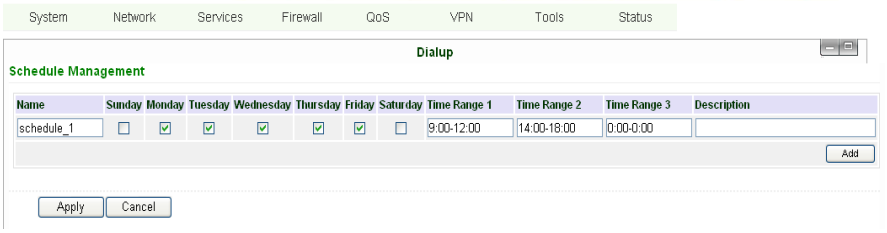




Name	Description	Default
Enable	Enable PPP dialup	Enable
Time Schedule	Set time for online and offline	ALL
SHARED	Enabled—device linked with Router **Can** access to internet. Disable—device **Can NOT** access to internet via Router.	Enable
ISP	Select local ISP, if not listed here, please select ”Customer”	Customer
Network Select Type	Choose mobile network type	HSDPA (or GPRS)
APN	APN parameters provided by **Local ISP, you can set TWO different group of dialup parameters (APN/Username/Password) and set one as backup**	cmnet/uninet
Access Number	Dialup parameters provided by **Local ISP**	“*99#”“*99***1#” or #777
Username	Dialup parameters provided by **Local ISP**	“GPRS” or ”CDMA”
Password	Dialup parameters provided by **Local ISP**	“GPRS” or ”CDMA”
Primary Profile Retries	After retries and dialup still failed, router will try backup dialup parameters (if you have set two IPSec tunnels and one as backup, router will also stop the main one and try another, more details please see at “VPN” → “IPSec”)	0 (always use main parameters and never use backup)
Static IP	Enable Static IP if your SIM card can get static IP address	Disable
Connection Mode	Optional Always Online,	Always Online
Redial Interval	When Dial fails, InRouter will redial after the interval	30 seconds
Show Advanced Options	Enable configure advanced options	Disabled
Initial Commands	Used for advanced parameters	Blank
Dial Timeout	Set dial timeout (IR6x1 will reboot after timeout)	120 seconds
MTU	Set max transmit unit	1500
MRU	Set max receive unit	1500
TX Queue Length	Set length of transmit queue	3
Enable IP header compression	Enable IP header compression	Disabled
Use default asyncmap	Enable default asyncmap, PPP advanced option	Disabled
Using Peer DNS	Click Enable to accept the peer DNS	Enabled

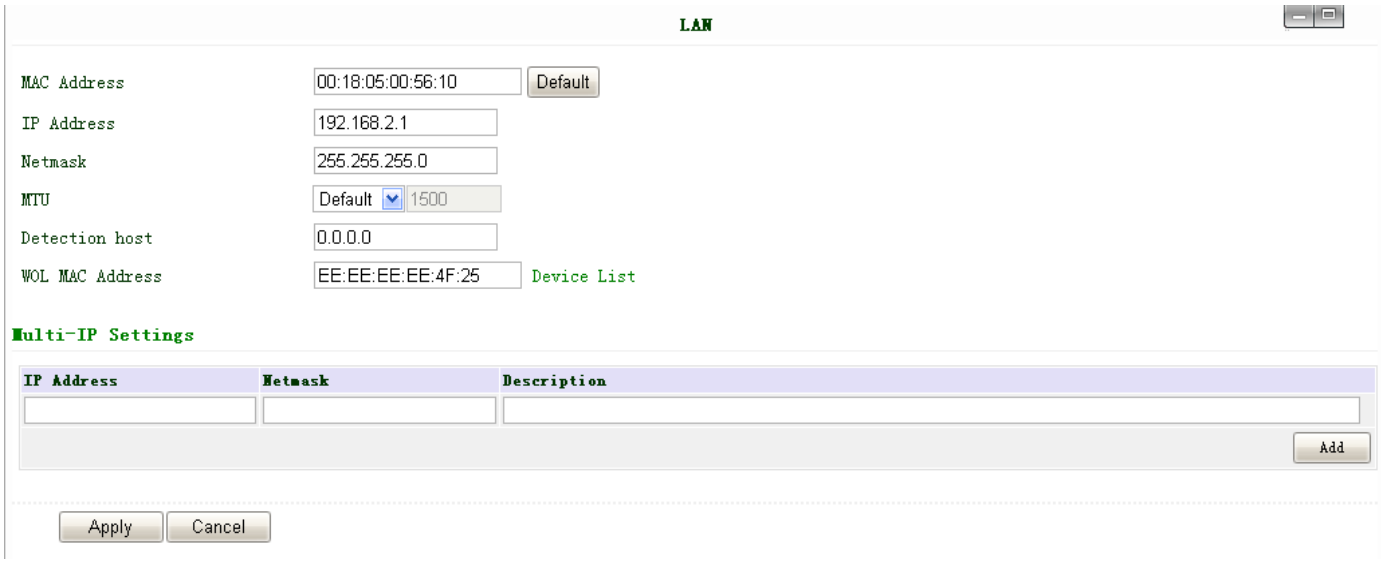
Link Detection Interval	Set Link Detection Interval	30 seconds
Link Detection Max Retries	Set the max retries if link detection failed	3
Debug	Enable debug mode	Enable
Expert Option	Provide extra PPP parameters, normally user needn't set this.	Blank
ICMP Detection Mode	MONITOR TRAFFIC When InRouter detected there are "business" data (DTU, IPSec) receive or transmit, InRouter will not send ICMP probe packet. When detected without business data, InRouter will send ICPM probe packet	Ignore Traffic
	IGNORE TRAFFIC No matter whether InRouter have some data receive or transmit(DUT, IPSec data), InRouter always send the ICMP probe packet.	
	HANDOVER ONLY InRouter send the ICMP probe Packet when the field change from a base station to other station.	
ICMP Detection Server	Set ICMP Detection Server, blank represents none	Blank
ICMP Detection Interval	Set ICMP Detection Interval	30 seconds
ICMP Detection Timeout	Set ICMP Detection Timeout (IR6X1 will reboot if ICMP time out)	5 seconds
ICMP Detection Max Retries	Set the max number of retries if ICMP failed	5

Dialup----Time Schedule Management:



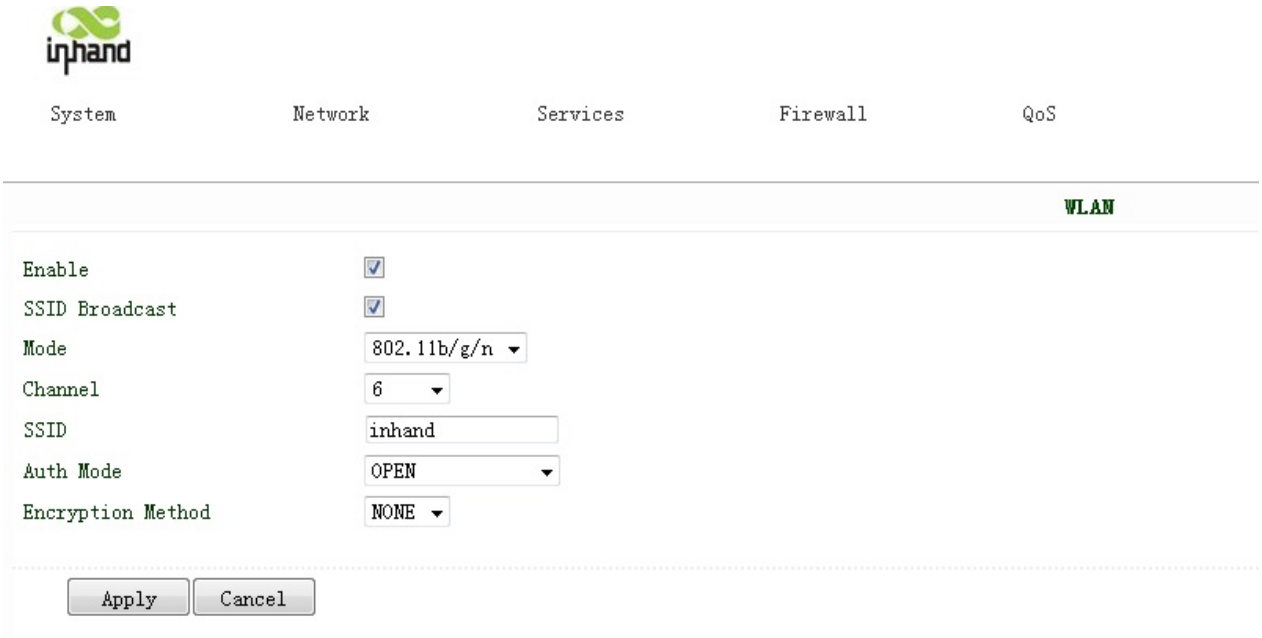
Name	Description	Default
Name	Name the schedule	schedule 1
Sunday		Blank
Monday		Enable
Tuesday		Enable
Wednesday		Enable
Thursday		Enable
Friday		Enable
Saturday		Blank
Time Range 1	Set Time Range 1	9:00-12:00
Time Range 2	Set Time Range 2	14:00-18:00
Time Range 3	Set Time Range 3	0:00-0:00
Description	Describe configuration	Blank

(2) LAN



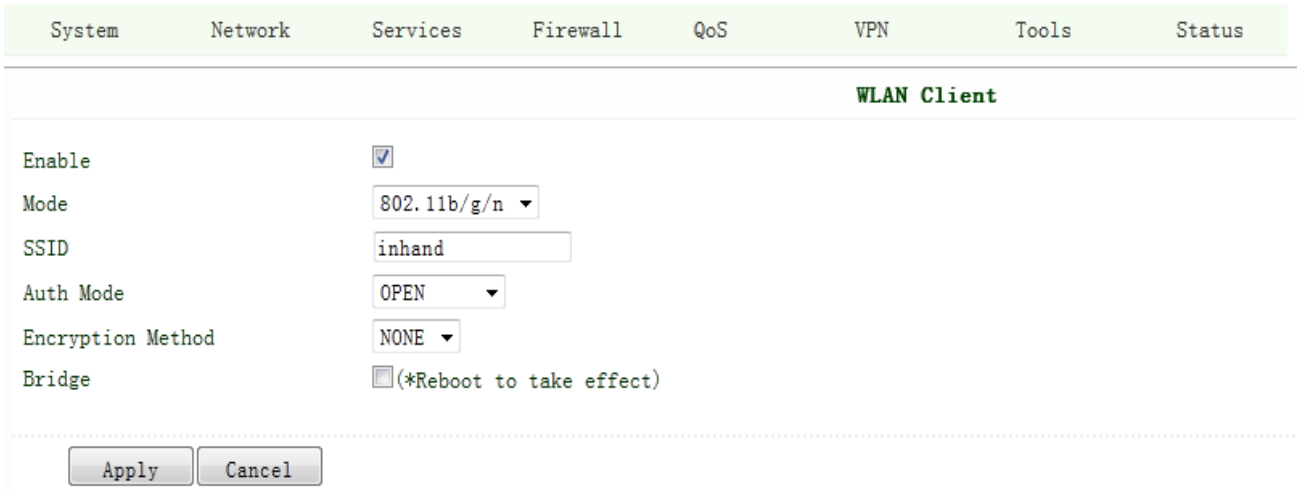
Name	Description	Default
MAC Address	The MAC address in LAN	00:10:A1:86:95:02 (Provided by InHand) , for manufactures
IP Address	Set IP Address in LAN	192.168.2.1 (If Changed, you need to input the new address for entering the configuration web)
Net Mask	Set Net Mask of LAN	255.255.255.0
MTU	Set MTU length, optional between Default and Manual	1500
Detection Host	Set Detection Host Address	0.0.0.0
WOL MAC Address	Set the MAC of PC in the LAN of router, for Wakeup Over LAN (WOL) function, you should also set "Networks"→ "Dialup" and change dialup mode into "Trigger by SMS".	Blank
Multi-IP Settings (Support additional 8 IP addresses at the most)		
IP Address	Set additional IP Address of LAN	Blank
Description	Description about this IP address	Blank

(3) WLAN (Only AP Series)



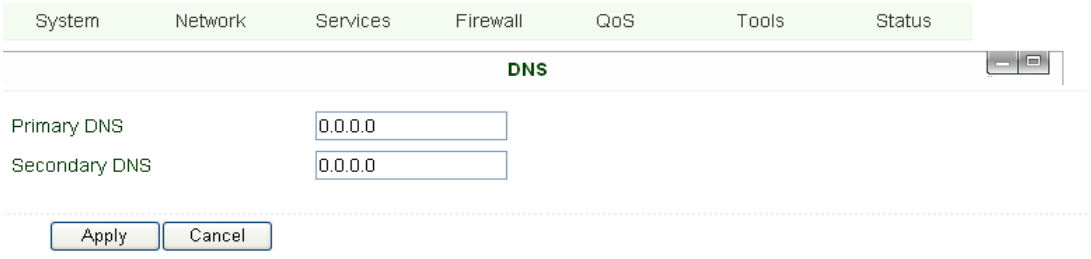
WLAN		
Description: Support WIFI, provide wireless LAN access and wireless user identification authentication services on customer field.		
Name	**Description**	**Default**
Enable	Enable “WLAN” port	Enable
SSID Broadcast	Enable “SSID Broadcast”, user can search wireless network by SSID name.	Enable
Mode Selection	Support 802.11b/g/n modes, etc.	802.11b/g/n
Channel Selection	Select channel	6
SSID	Self-define SSID name	Inhand
Authentication Method	Support Open, Shared Key, and Auto Select WEP, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA/WPA2, WPAPSK/WPA2PSK.	Open
Encryption Scheme	Based on authentication method, support NONE, WEP, TKIP, AES, and TKIP/AES. Different authentication method uses different encryption scheme and may need network key and corresponding authentication parameters, which will not be listed here.	NONE

(4) WLAN Client (Only STA Series)



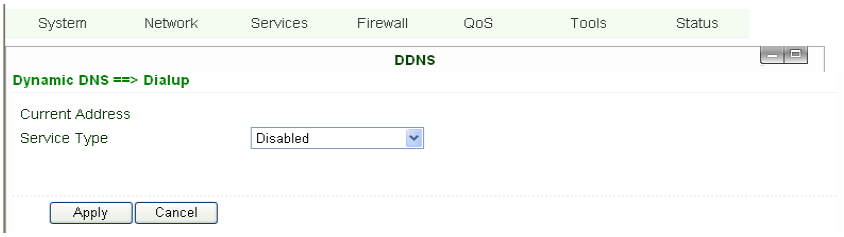
WLAN Client		
Description: Provide WIFI access for your Ethernet device		
Name	**Description**	**Default**
Enable	Enable “WLAN Client” port	Enable
Mode	Support 802.11b/g/n modes, etc.	Enable
SSID	Fill in the accessed SSID name.	inhand
Auth Mode	Support Open, Shared, WPA-PSK , WPA2-PSK,	Open
Encryption Method	Support NONE, WEP, TKIP, AES	NONE
Bridge	Enable bridge, the Access Point will assign a local IP address for your device.	NONE

(5) DNS

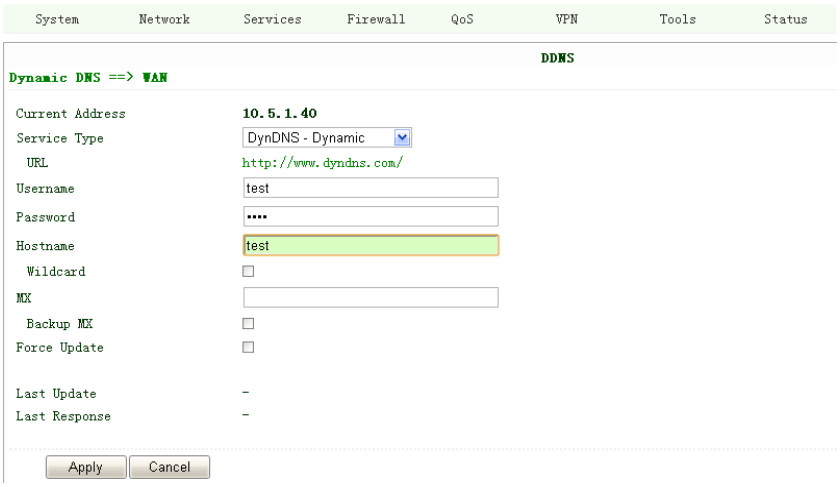


Name	Description	Default
Primary DNS	Set Primary DNS	Blank
Secondary DNS	Set Secondary DNS	Blank

(6) DDNS (Dynamic DNS)

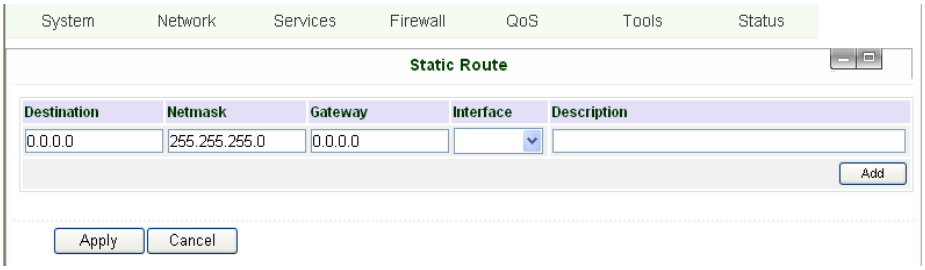


Name	Description	Default
Current Address	Show the current IP address	Blank
Service Type	Select DDNS Provider	Disabled



Name	Description	Default
Service Type	DynDNS - Dynamic	
URL	http://www.dyndns.com/	
Username	Registered username for DDNS	
Password	Registered password for DDNS	
Hostname	Registered hostname for DDNS	

(7) Static Route

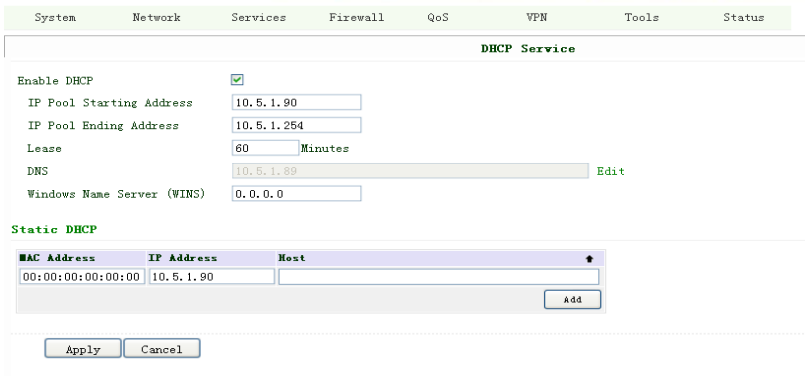


Name	Description	Default
Destination	Set IP address of destination	Blank
Net Mask	Set subnet Mask of destination	255.255.255.0
Gateway	Set the gateway of destination	Blank
Interface	Optional LAN/WAN port access to destination	Blank
Description	Describe static route	Blank

3.1.4 Service

Service settings include DHCP Service, DNS Forwarding, VRRP and other related parameters.

(1) DHCP Service



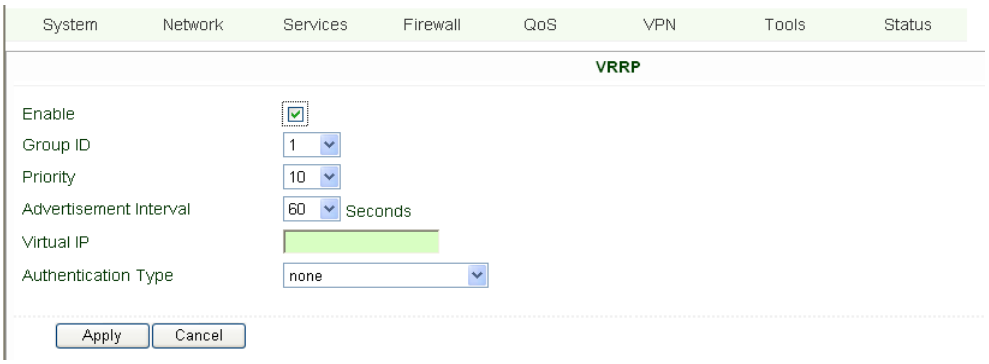
Name	Description	Default
Enable DHCP	Click to enable DHCP	Enable
IP Pool Starting Address	Set the starting IP address of DHCP pool	192.168.2.2
IP Pool Ending Address	Set the ending IP address of DHCP pool	192.168.2.100
Lease	Set the valid time lease of IP address obtained by DHCP	60 minutes
DNS	Set DNS Server	192.168.2.1
Windows Name Server (WINS)	Set WINS	Blank
Static DHCP (can set 20 designated IP address at the most)		
MAC Address	Set the MAC address of a designated IP address	Blank
IP address	Set the static IP address	192.168.2.2
Host	Set the hostname	Blank

(2) DNS Relay

Name	Description	Default
Enable DNS Relay	Click to enable DNS Relay	Disabled
Designate IP address<=>DNS couples (20 at the most)		
IP Address	Set IP address <=> DNS couples	Blank
Host	Set the name of IP address <=> DNS couples	Blank

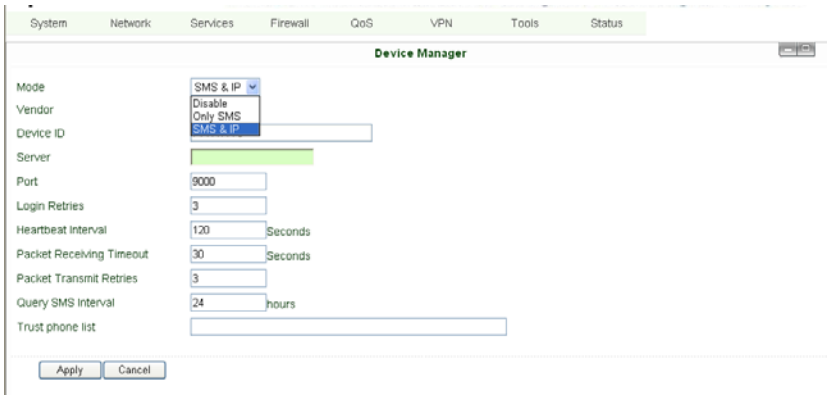
Description	Describe IP address <=> DNS couples	Blank

(3) VRRP

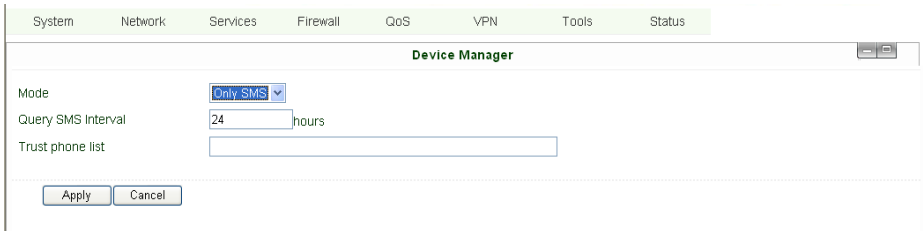


Name	Description	Default
Enable	Select to enable VRRP	Disable
Group ID	Select group id of routers (range 1-255)	1
Priority	Select priority for router (range 1—254)	10 (bigger number stands for higher priority)
Advertisement Interval	Set ad interval	60 sec
Virtual IP	Set Virtual IP	Blank
Authentication Type	Optional: None/Password type	None

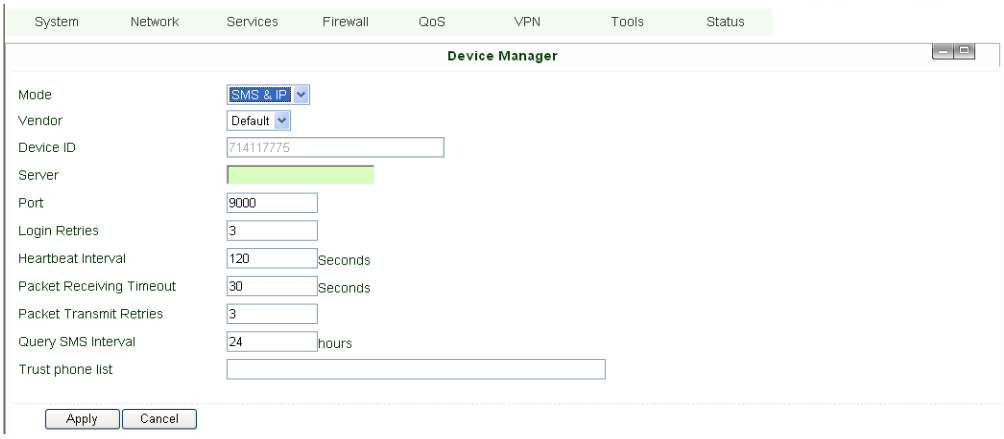
(4) Device Manager



Name	Description	Default
Mode	Disabled/Only SMS/SMS+IP	Disable

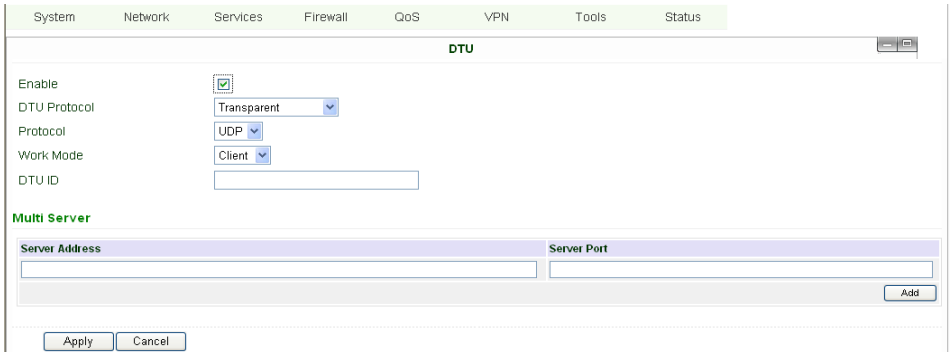


Name	Description	Default
Mode	Only SMS	
Query SMS Interval	Set how long to check SMS	24 hours
Trust Phone List	Add trust Cell Phone List	



Name	Description	Default
Mode	SMS+IP Mode	
Vendor	Set Vendor Name	Default
Device ID	Set Device ID	
Server	Set Device Manager Server IP	
Port	Set Port For DM	9000
Login Retries	Set login retries	3
Heartbeat Interval	Set interval of heartbeat	120
Packet Receiving Timeout	Set packet receiving timeout	30
Packet Transmit Retries	Set packet transmit reties	3
Query SMS Interval	Set how long to check SMS	24
Trust phone list	Set trust cell phone list	

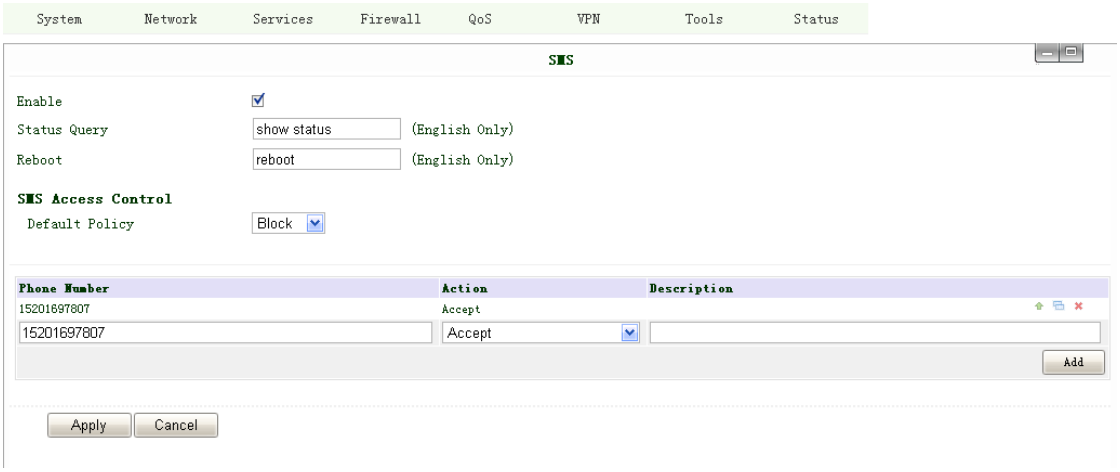
(5) DTU



Name	Description	Default
Enable	Click to enable DTU	Disable
DTU Protocol	Set DTU protocol, Please see more in related Quick Guide	Transparent
Protocol	Optional between TCP/UDP	UDP
Mode	Set DTU as client or server	Client
Frame Interval	Set Frame Interval	100
Serial Buffer Frames	Set Serial Buffer Frames	4

Multi-Server Policy	Optional between Parallel/Poll	Parallel
Min Reconnect interval	Set Min Reconnect interval	15
Max Reconnect interval	Set Max Reconnect interval	180
DTU ID	Set ID of DTU	Blank
Source IP	Set Source IP	Blank
Multi Server	Set the IP address and Port of server to receive data.	Blank

(6) SMS



Name	Description	Default
Enable	Click to enable SMS control	Disable
Status Query	Set Status Query SMS, and you can see status of router by send SMS (e.g.: show status).	
Reboot	Let the router reboot	
SMS Access Control		
Default Policy	Block or Accept control SMS from certain Phone	Block
Phone List	Include phone numbers accepted or blocked to send SMS to router	

Notice: Before using this function, please make sure you have a SIM card in the router that has SMS function. Otherwise, please contact local mobile operator to get one.

SMS you will get in your mobile phone:

Host: (SN);

Uptime: (the uptime of router for this time of reboot);

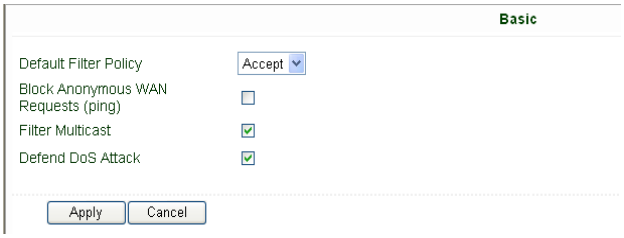
State: (Online/Offline) (Cellular WAN IP)

LAN: (Up) (LAN IP)

3.1.5 Firewall

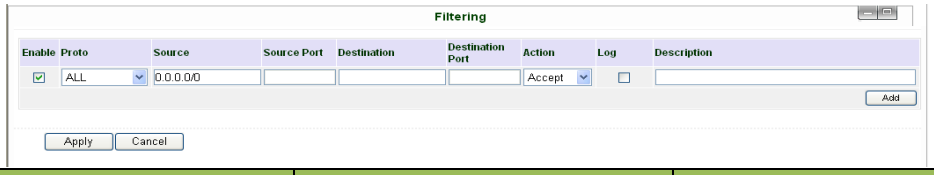
This page is to configure the firewall parameters.

(1) Basic Configuration



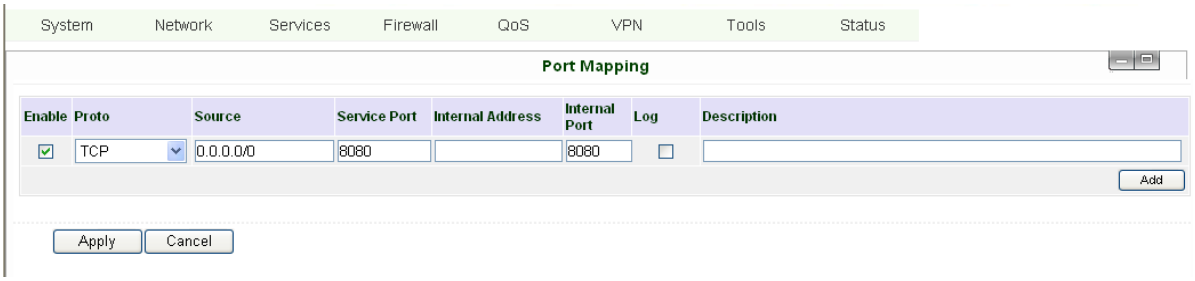
Name	Description	Default
Default Filter Policy	Optional between Accept /Refused	Accept
Block Anonymous WAN Request (ping)	Click to enable filer ping request	Disable
Filter Multicast	Click to enable filter multicast	Enable
Defend DoS Attack	Click to enable Defend DoS Attack	Enable

(2) Filtering



Name	Description	Default
Enable	Click to enable filtering	Blank
Protocol	Optional among TCP/UDP/ICMP	All
Source IP address	Set Source IP address	Blank
Source Port	Set Source Port	Blank
Destination IP	Set destination IP	Blank
Destination Port	Set destination port	Blank
Action	Accept/Deny	Accept
Log	Click to enable login	Disable
Description	Describe your configuration	Blank

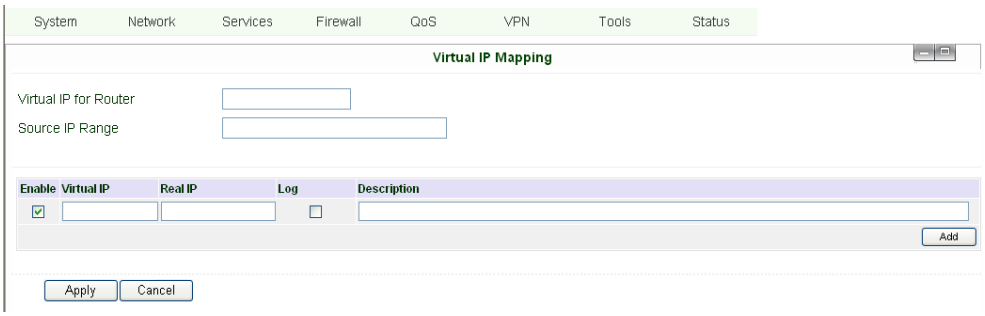
(3) Port Mapping



Name	Description	Default
Enable	Click Enable Port Mapping	Disable
Source	To fill with source IP	0.0.0.0/0
Service Port	Fill the port of service	8080

Internal Address	Set the internal IP for mapping	Blank
Internal Port	Set the Port mapping to internal	8080
Log	Click to enable log about port mapping.	Disable
Description	Describe meanings of each mapping	Blank

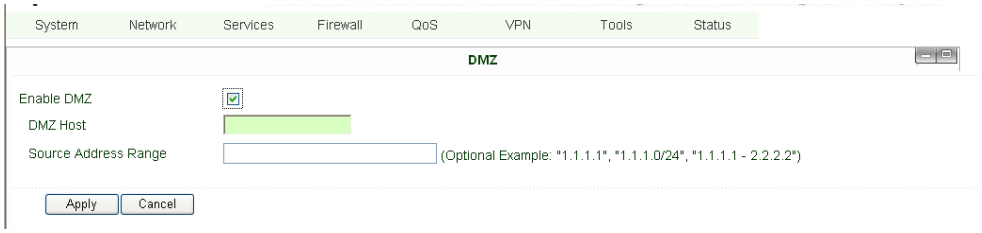
(4) Virtual IP Mapping



An internal PC's IP can match to a virtual IP, and external network can access the internal PC via this virtual IP address.

Name	Description	Default
Virtual IP for Router	Set Virtual IP for Router	Blank
Source IP Range	Set range of source IP address	Blank
Virtual IP	Set virtual IP	Blank
Real IP	Set real IP	Blank
Log	Enable logging concerned with virtual IP	Disable
Description	Describe this configuration	Blank

(5) DMZ (All Port Mapping)

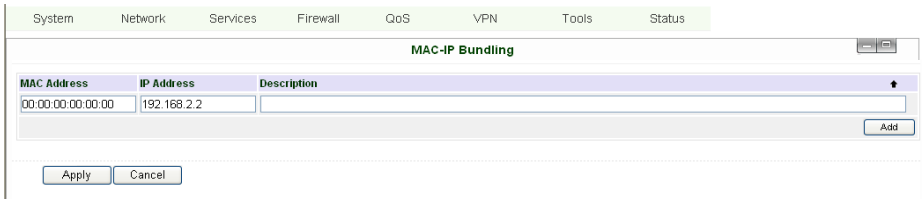


Mapping all the ports then external PC can access all the ports of internal devices behind IR6X1.

Attention: This function cannot map the admin port of IRx1 (e.g.: 80 TCP) to the device's port.

Name	Description	Default
Enable DMZ	Click to Enable DMZ	Disable
DMZ Host	Set host IP of DMZ	Blank
Source Address Range	Set IP address with restrict IP access	Blank

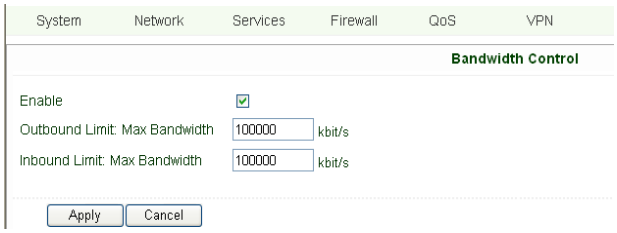
(6) MAC-IP Bundling



When firewall denies all access to the external network, only PC with MAC-IP Bundling can access external network

Name	Description	Default
MAC Address	Set Bundling Mac address	Blank
IP Address	Set Bundling IP address	192.168.2.2
Description	Describe this configuration	Blank

3.1.6 QoS



Name	Description	Default
Enable	Click to enable	Disable
Outbound Limit Max Bandwidth	Set the limit speed of out- bound bandwidth	100000kbit/s
Inbound Limit Max Bandwidth	Set the limit speed of inbound bandwidth	100000kbit/s

3.1.7 VPN

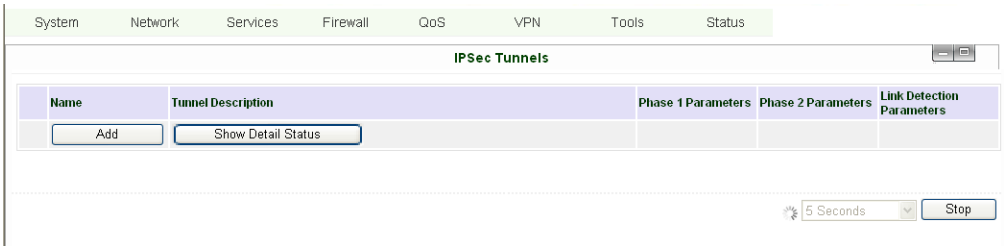
(1) IPSec Settings

To build an IPSec VPN Tunnel, you need to first set IPSec properties in this page, then go to IPSec Tunnels to add your VPN:

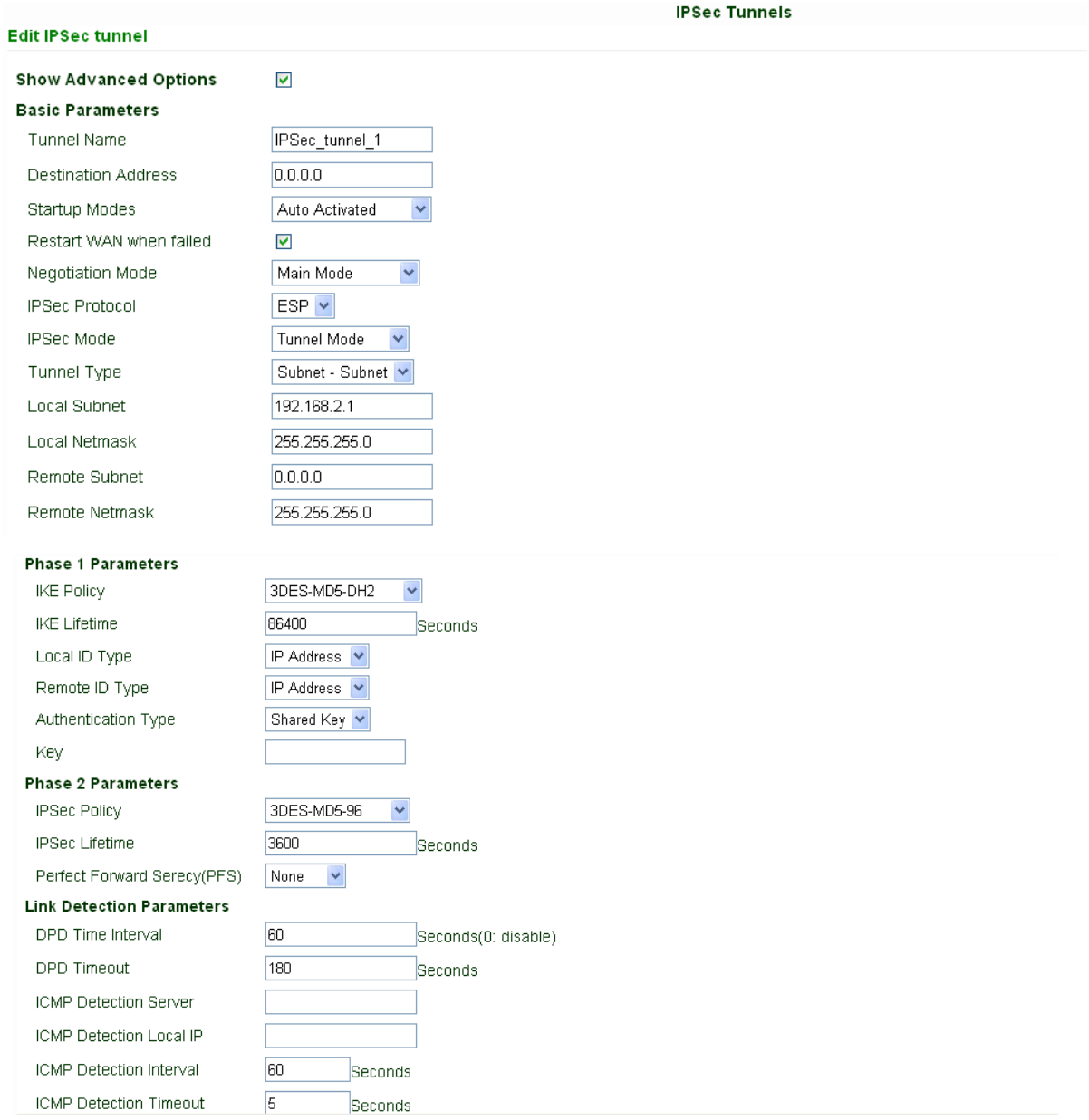
IPSec Settings		
Description: 1. Select to Enable or Disable NATT, normally we need to enable, unless you ensure there is no NAT routers in the network. 2. Select to enable Compression Mode or Debug		
Name	**Description**	**Default**
Enable NAT Transversal (NATT)	Click to enable NATT	Enable
Keep alive time interval of NATT	Set live time for NATT	60 sec

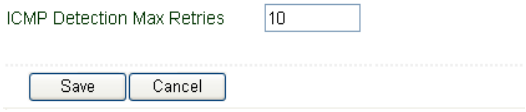
Enable Compression	Click to enable	Enable
Enable Debug	Click to enable	Disable
Force NATT	Click to enable	Disable

(2) IPSec Tunnels



Click “Add” to enter the configuration page:

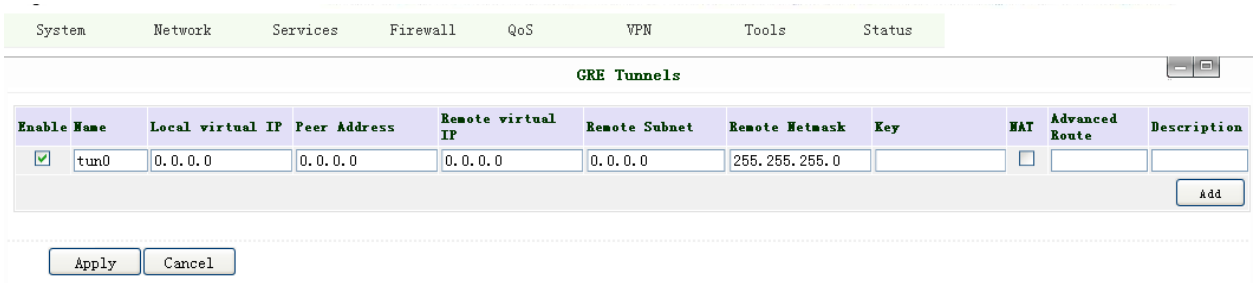




Name	Description	Default
Show Advanced Options	Click to enable advanced options	Disable
Basic Parameters		
Tunnel Name	To name the tunnel	IPSec_tunnel_1
Destination Address	Set the destination address of IPSec VPN Server	Blank
Startup Mode	Auto Activate/Trigged by Data/Passive/Manually Activated	Enable
Negotiation Mode	Optional: Main Mode or Aggressive Mode	Main Mode
IPSec Mode (Enable Advanced options)	Optional: ESP or AH	ESP
IPSec Mode (Enable Advanced options)	Optional: Tunnel Mode or Transport Mode	Tunnel Mode
Tunnel Type	Optional: Host——Host, Host——Subnet, Subnet——Host, Subnet——Subnet	Subnet——Subnet Mode
Local Subnet	Set IPSec Local Protected Subnet	192.168.2.1
Local Subnet Net Mask	Set IPSec Local Protected Subnet Net Mask	255.255.255.0
Remote Subnet Address	Set IPSec Remote Protected Subnet	Blank
Remote Subnet Net Mask	Set IPSec Remote Protected Subnet Net Mask	255.255.255.0
Phase 1 Parameters		
IKE Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IKE Lifetime	Set IKE 的 Lifetime	86400 sec
Local ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Local ID (Only for FQDN 和 USERFQDN)	Set the ID according to ID type	Blank
Remote ID Type	Optional: FQDN, USERFQDN, or IP Address	IP Address
Remote ID (Only for FQDN and USERFQDN)	Set the ID according to ID type	Blank
Authentication Type	Optional: Shared Key or Certificate	Shared Key
Key (While choosing Shared Key Authentication Type)	Set IPSec VPN Negotiation Key	Blank
Phase 2 Parameters		
IPSec Policy	Optional: 3DES-MD5-96 or AES-MD5-96	3DES-MD5-96
IPSec Lifetime	Set IPSec Lifetime	3600sec
Perfect Forward Secrecy (PFS)	Optional: Disable, GROUP1, GROUP2, GROUP5	Disable ((Enable Advanced options)
Link Detection Parameters (Enable Advanced options)		
DPD Time Interval	Set DPD Time Interval	60sec
DPD Timeout	Set DPD Timeout	180sec
ICMP Detection Server	Set ICMP Detection Server	Blank
ICMP Detection Local IP	Set ICMP Detection Local IP	
ICMP Detection Interval	Set ICMP Detection Interval	30sec

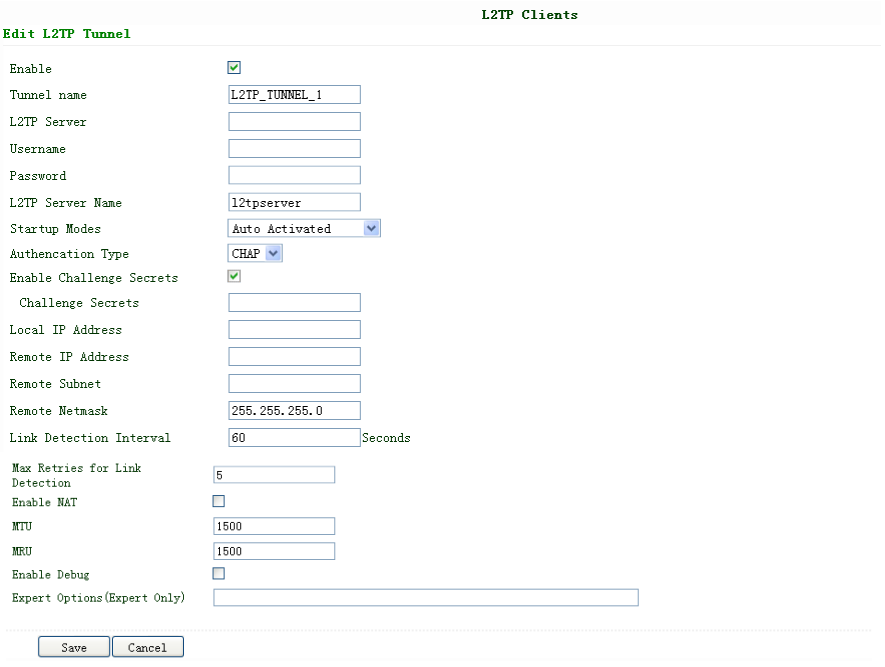
ICMP Detection Timeout	Set ICMP Detection Interval	5sec
ICMP Detection Max Retries	Set ICMP Detection Max Retries	3

(3) GRE Tunnels



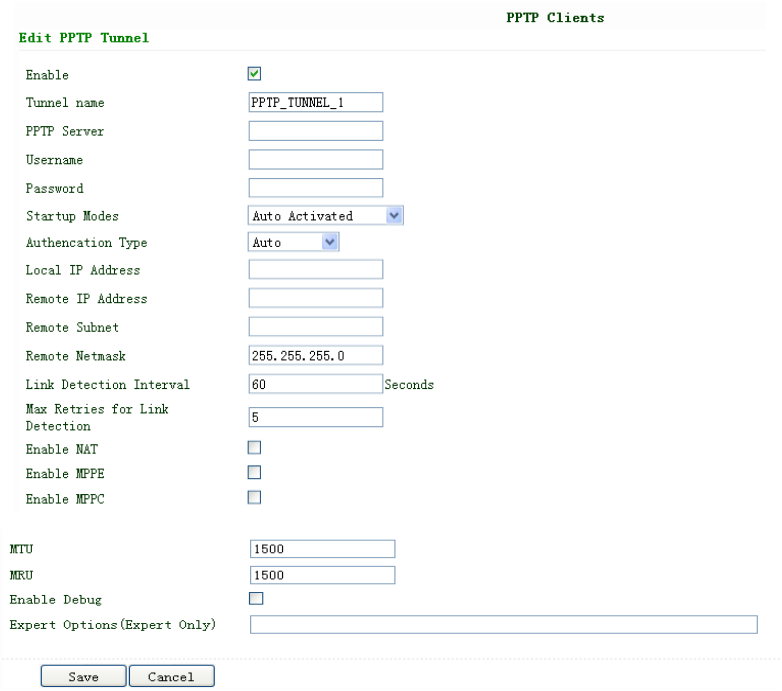
GRE Tunnels		
Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set GRE Tunnel Name	tun0
Local Virtual IP	Set Local Virtual IP	0.0.0.0
Remote Address	Set Remote Address	0.0.0.0
Remote Virtual IP	Set Remote Virtual IP	0.0.0.0
Remote Subnet Address	Set Remote Subnet Address	0.0.0.0
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Key	Set Tunnel Key	Blank
NAT	Click Enable NAT Function	Disable
Description	Add Description	Blank

(4) L2TP Clients



Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	L2TP_TUNNEL_1
L2TP Server	SetL2TP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server Password	Blank
Server Name	Set Server Name	l2tpserver
Startup Modes	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP	CHAP
Enable Challenge secrets	Set to enable Challenge secrets	Disable
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Disable
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Disable
Expert Options	Set Expert Options	Blank

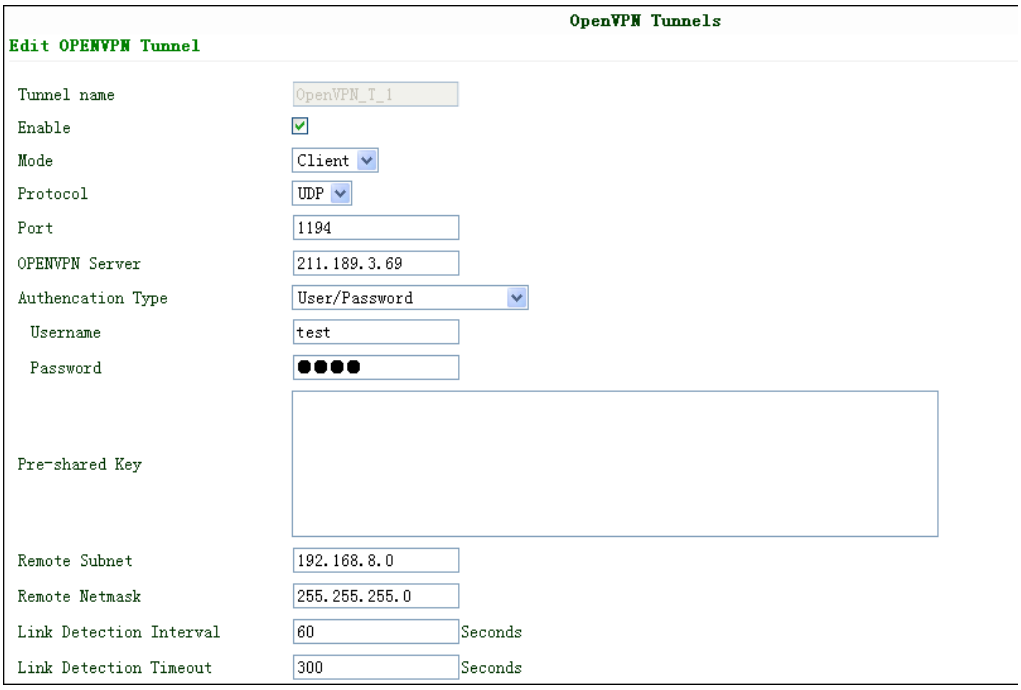
(5) PPTP Clients

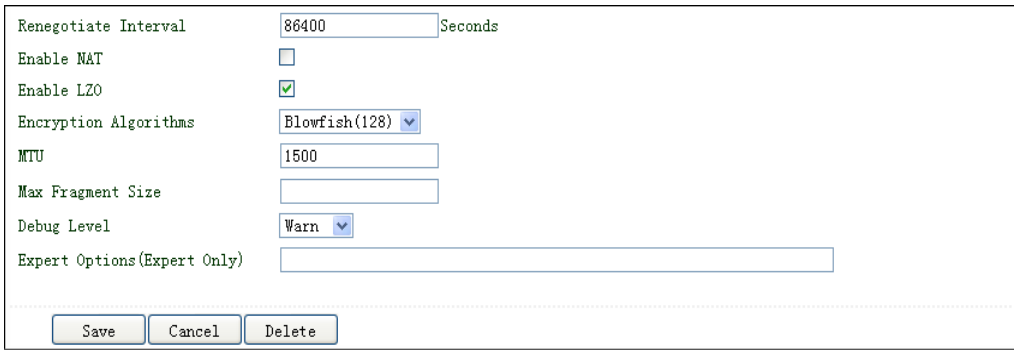


Name	Description	Default
Enable	Click Enable	Enable

Tunnel Name	Set Tunnel Name	PPTP_TUNNEL_1
PPTP Server	Set PPTP Server Address	Blank
Username	Set Server Username	Blank
Password	Set Server's Password	Blank
Startup Mode:	Set Startup Modes: Auto Activated, Trigged by Data, Manually Activated	Auto Activated
Authencation Type	Set Authencation Type: CHAP, PAP, MS-CHAPv1, MS-CHAPv2	Auto
Local IP Address	Set Local IP Address	Blank
Remote IP Address	Set Remote IP Address	Blank
Remote Subnet	Set Remote Subnet	Blank
Remote Subnet Net Mask	Set Remote Subnet Net Mask	255.255.255.0
Link Detection Interval	Set Link Detection Interval	60
Max Retries for Link Detection	Set Max Retries for Link Detection	5
Enable NAT	Click Enable NAT	Blank
Enable MPPE	Click Enable MPPE	Blank
Enable MPPC	Click Enable MPPC	Blank
MTU	Set MTU parameters	1500
MRU	Set MRU parameters	1500
Enable Debug Mode	Click Enable Debug Mode	Blank
Expert Options	For InHand R&D only	Blank

(6) OpenVPN Settings

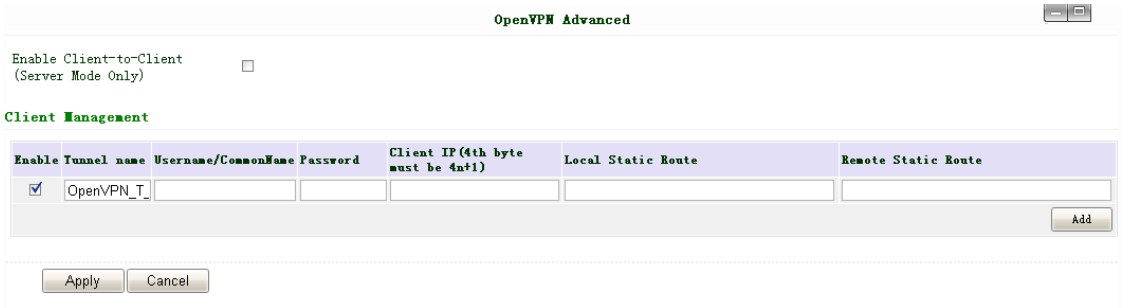




This page is to configure the OpenVPN settings, including Tunnel Name, Work Mode, Protocol, Port No. and other items.

Name	Description
Tunnel name	default
Enable	Enable this configuration
Mode	Client or Server
Protocol	UDP or TCP
Port	Import or Export Certificate (CRL)
OPEN VPN Server	OPEN VPN Server's IP or DNS
Authencation Type	(1) None ----- for host to host connection (not available when 700 as server) (2) Pre-shared Key ----- for host to host connection (not available when 700 as server) (3) User/Password ----- For multi users to access CA needed: Client: root CA (ca.crt) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key) (4) X.509 Cert (multi-client) ----- CA mode for multi users to access CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key) (5) X.509 Cert -----CA mode for host to host tunnel CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key) (6) User+X.509 mode------username + password + CA certificate CA needed: Client: root CA (ca.crt), public key (pub.crt), private key (pri.key) Server: root CA (ca.crt), public key (pub.crt), private key (pri.key)
Pre-shared Key	Set shared key or TLS-AUTH static password
Remote Subnet, Remote Net mask	Set the static route of the router, always towards the subnet of its peer
Link Detection Interval, Link Detection Timeout	Always use default
Renegotiate Interval	Always use default
Enable NAT	Set NAT mode, meanwhile it will disable route mode
Enable MPPE	Enable MPPE, always set in server
Enable LZO	Enable LZO compression
Encryption Algorithms	Set encryption algorithms, must match with the server
MTU, Max Fragment Size	Always use default

(7) OpenVPN Advanced Settings

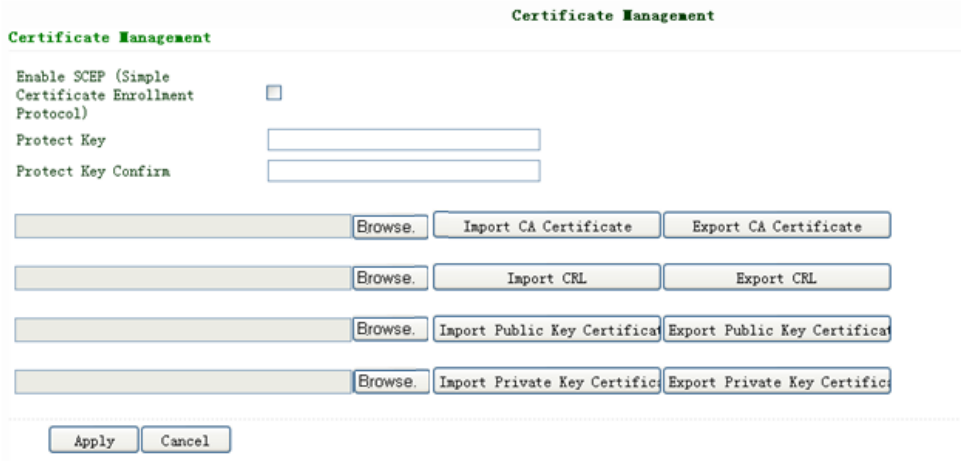


This page is to configure the OpenVPN advanced settings.

Name	Description
Enable Client-to-Client	Enable client access to other clients
Client Management	
Tunnel Name	Tunnel Name of the Client
Username/Common Name	Username (using Username/password mode) or Common Name in CA (CA mode)
Local Static Route	The client subnet
Remote Static Route	The server subnet

Attention: CA can only be produced by customer's PC; InRouter cannot produce CA.

(8) Certificate Management of OpenVPN Settings



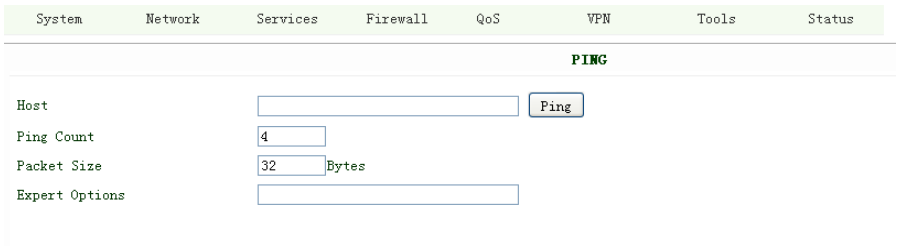
Name	Description	Default
Enable SCEP (Simple Certificate Enrollment Protocol)	Click Enable	
Certificate Protected Key	SetCertificate Protected Key	Blank
Certificate Protected Key Confirm	Confirm Certificate Protected Key	Blank
Import/Export CACertificate	Import orExport (CA) Certificate	Blank
Import/Export Certificate (CRL)	Import orExport Certificate (CRL)	Blank
Import/Export Public Key Certificate	Import orExport Public Key Certificate	Blank

Import/Export Private Key Certificate	Import orExport Private Certificate	Blank

3.1.8 Tools

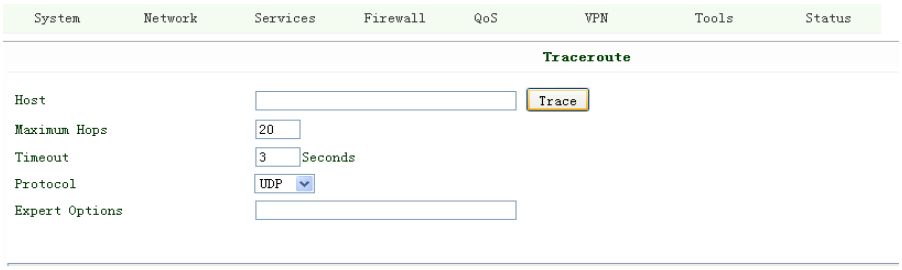
Tools contain PING Detection, Route Trace, Link Speed Test and etc.

(1) PING



Name	Description	Default
Host	Destination for PING	Blank
Ping Count	Set PING Counts	4 times
Packet Size	Set PING Packet Size	32 Bytes
Expert Options	Advanced parameters	Blank

(2) Trace Route



Name	Description	Default
Host	Destination for Trace Route	Blank
Max Hops	Set Max Hops	20

Time Out	Set Time Out	3 sec
Protocol	Optional: ICMP/UDP	UDP
Expert Options	Advanced parameters	Blank

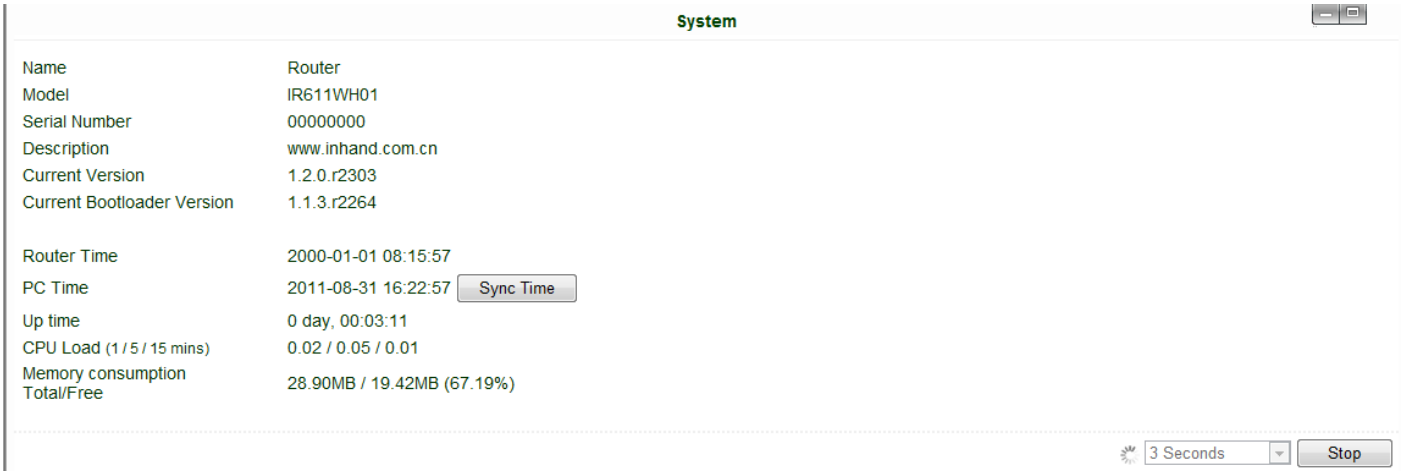
(3) Link Speed Test

Test link speed via upload or download.

3.1.9 Status

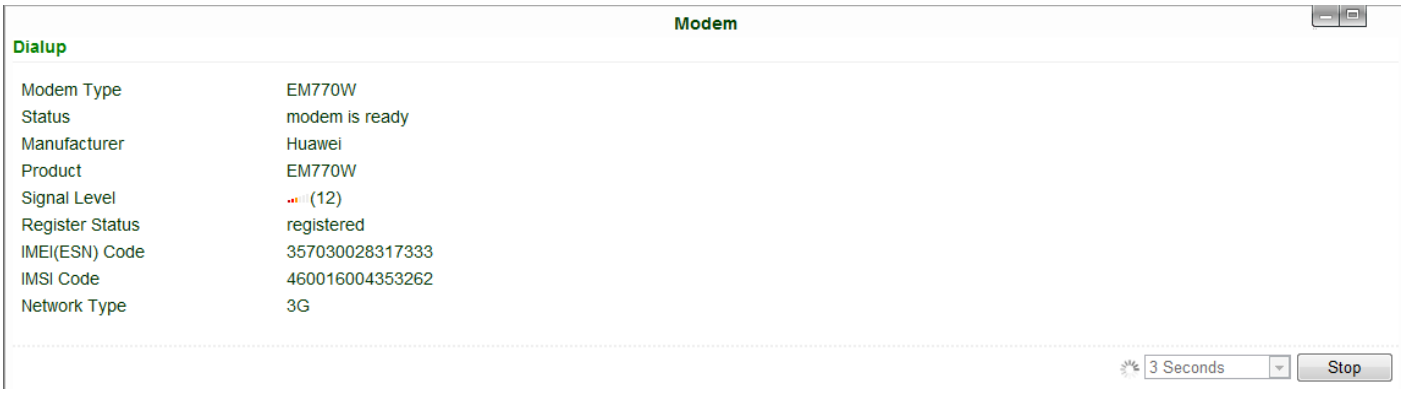
Status contains System, Modem, WLAN, Network Connections, Route Table, Device List and Log.

(1) System Status



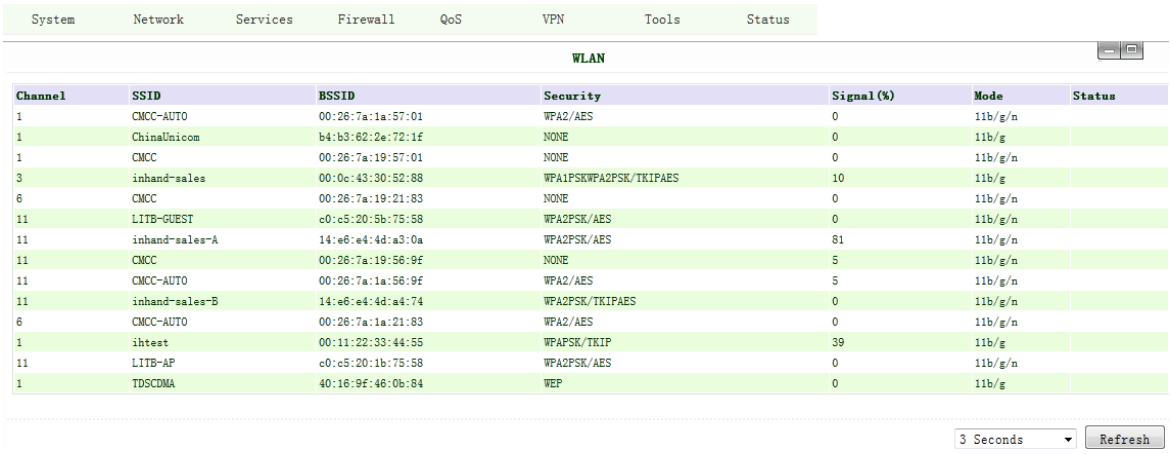
This page shows the status of system, including Name, Model Type, Current Version and etc.

(2) Modem Status



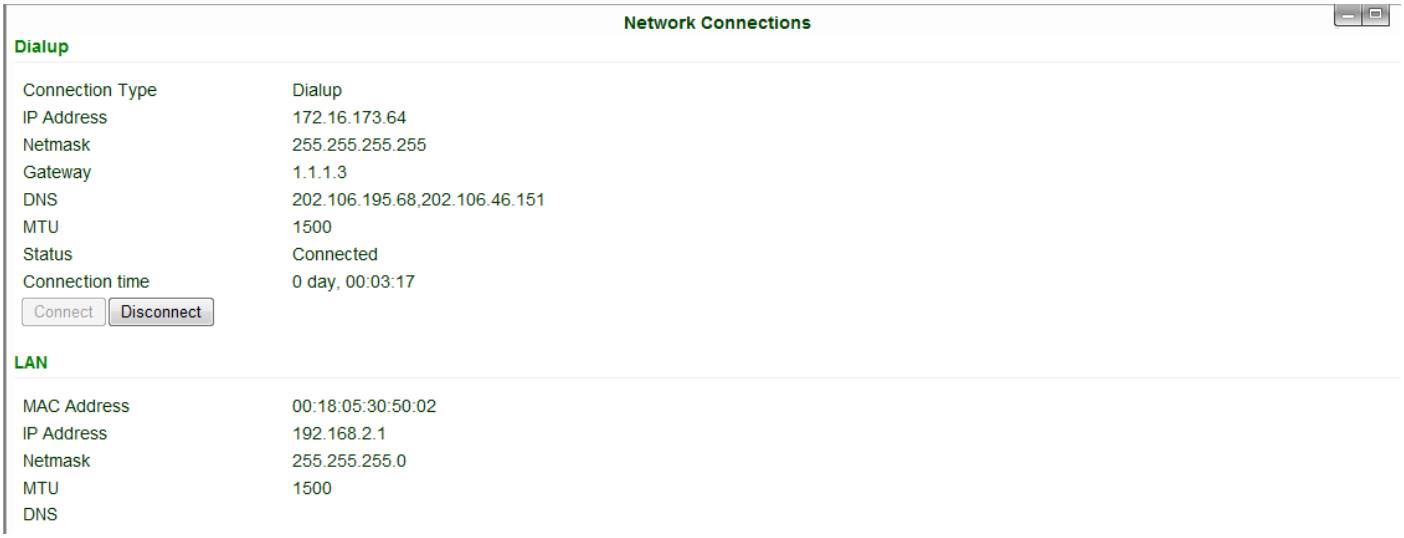
This page shows the status of Modem, including signal level.

(3) WLAN (Only STA series)



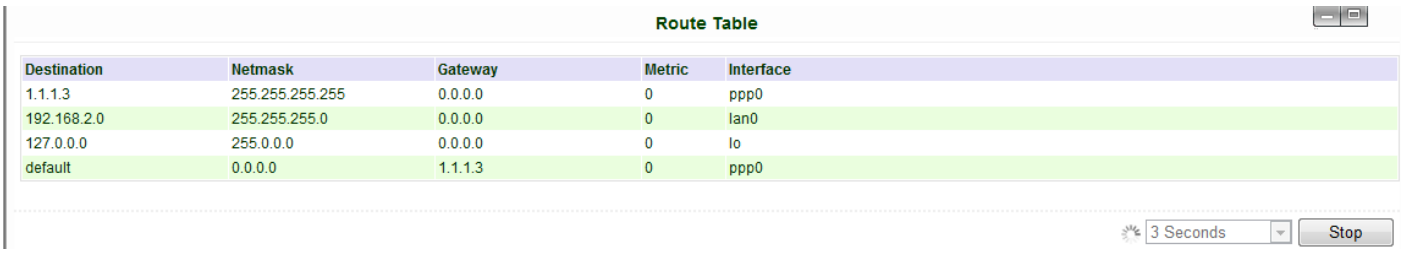
This page show joinable access point.

(4) Network Connections



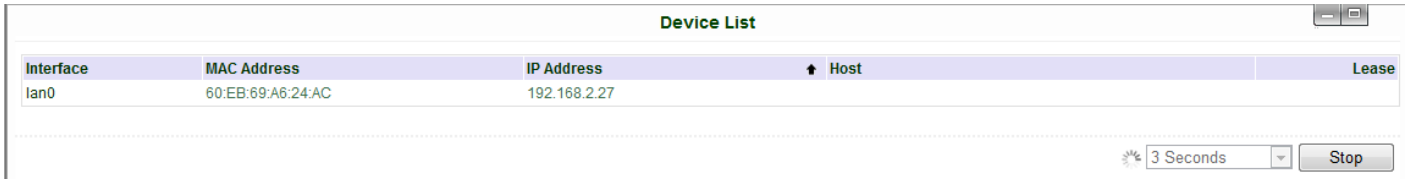
This page shows the network connection via WAN or LAN

(5) Route Table



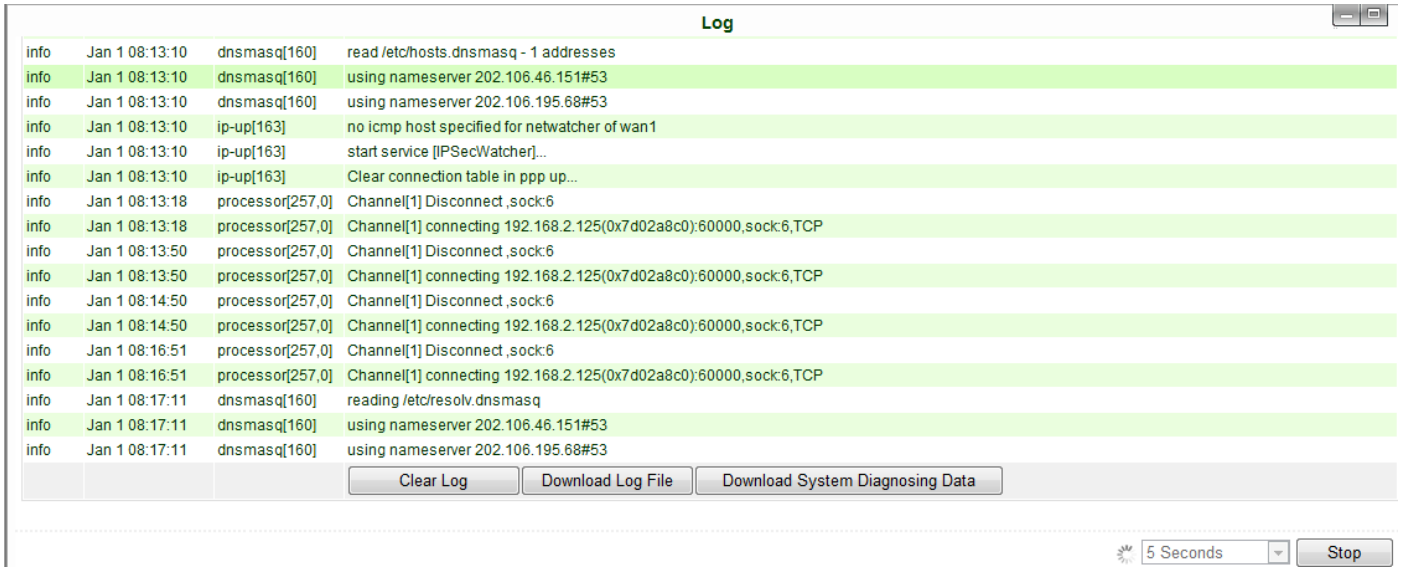
This page shows the route table of IR6x1.

(6) Device List



This page shows the devices linked with IR6x1.

(7) Log



This page shows the log of system, including download log file.

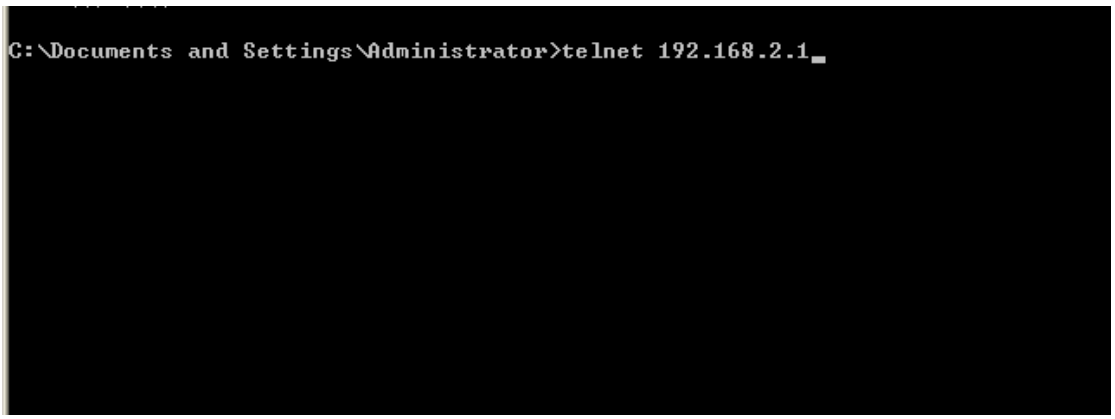
Under certain situation when there’re problems that can’t be diagnosed at the moment, you’ll be asked to provide the diagnose log to InHand engineers, you may click “Download System Diagnosing Data” and then send the diagnose log to us.

3.2 CLI Configuration

This chapter will show you how to configure via CLI.

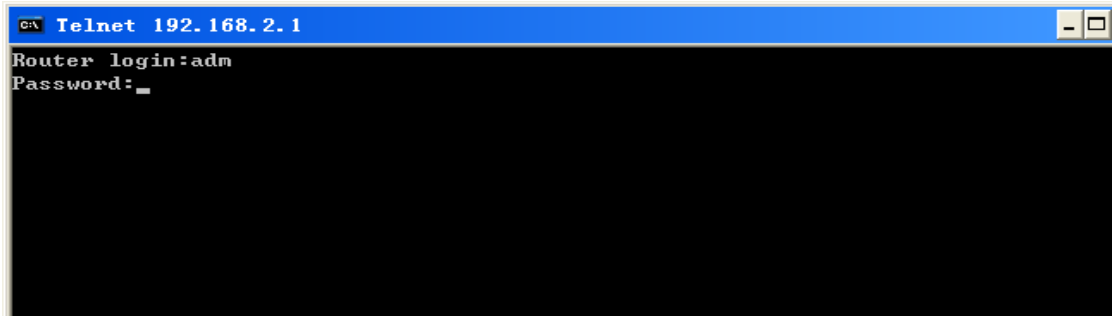
3.2.1 CLI Operation

Step 1: Input telnet LAN IP to login CLI configuration. For example:

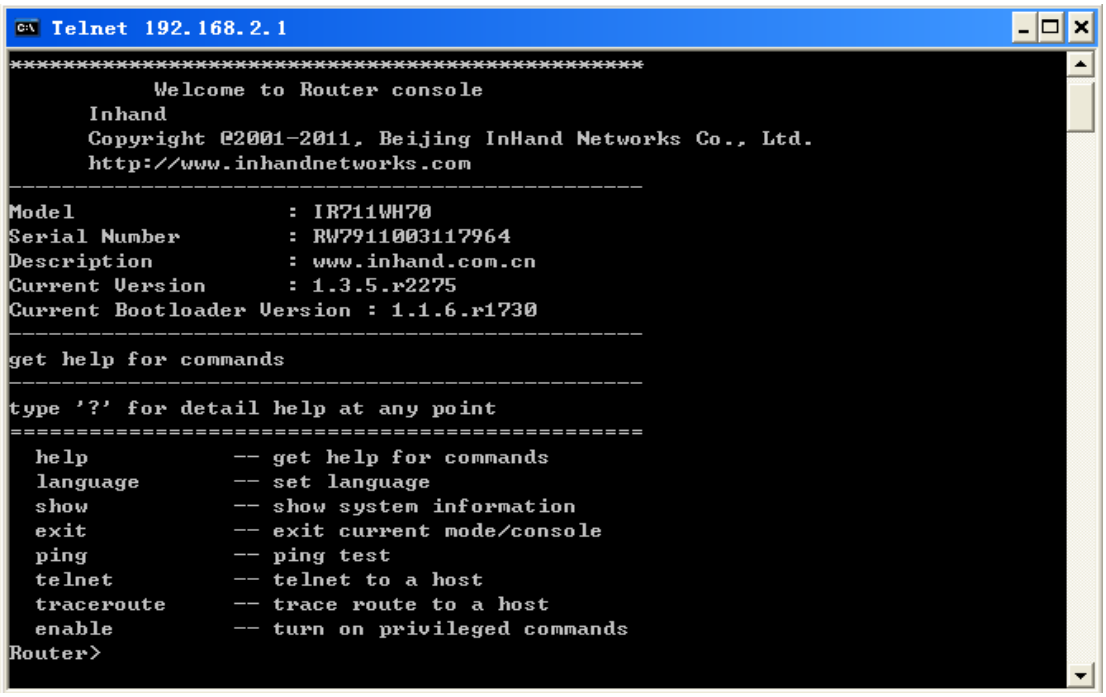


Step 2: After connection is succeed, input username and password of IR6x1. The default username/password is adm/123456

Attention: password will not be showed.

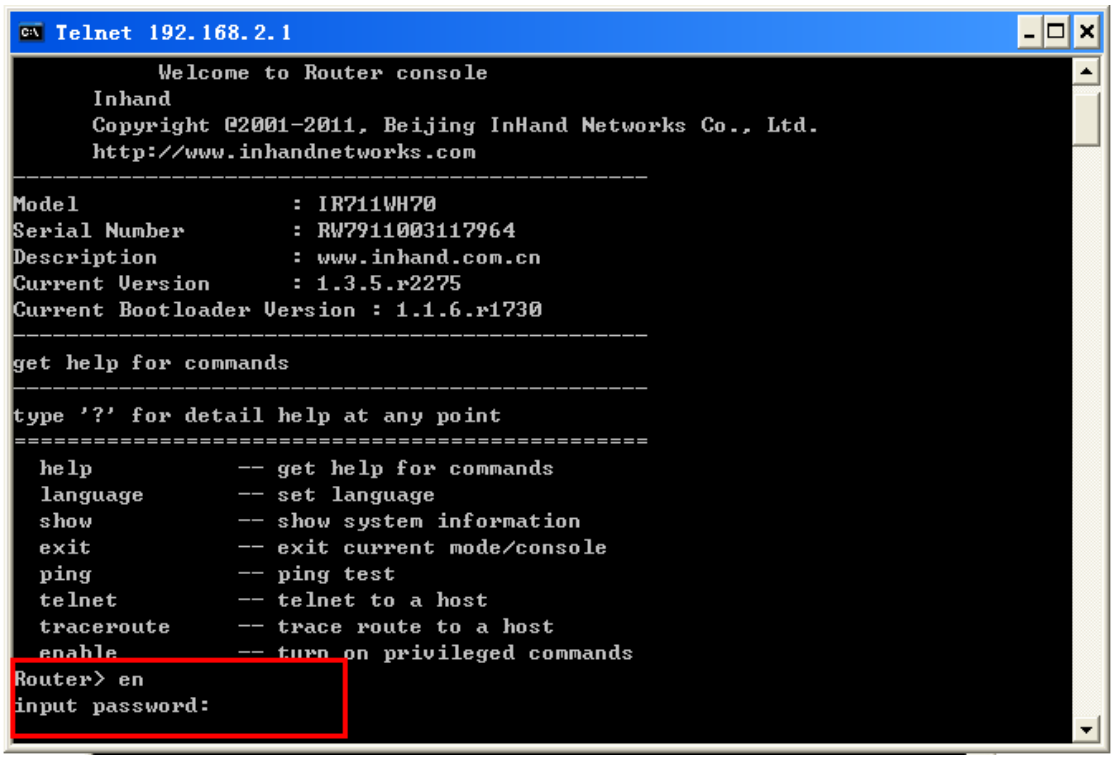


Step 3: Login to User Mode



This screenshot is the config-view of IR700.

Step 4: enter privileged mode, password is 123456



Step 5: Login to privileged mode successfully

```
Router#
Router#
Router#
Router#
Router#
Router#
Router#
Router#
```

Step 6: Enter configured mode, then you could configure parameters you want to set up.

```
Router# conf terminal
Router(config)#
```

3.2.2 CLI command

Configure username and password

```
Router(config)# nvram set adm_user adm
set adm_user=adm
Router(config)# nvram set adm_passwd 123456
set adm_passwd=123456
Router(config)#
```

Enable serial function

```
Router(config)# nvram set console_enable 1
set console_enable=1
```

Configure serial port parameters, like baudrate, parity, stop bit and so on.

```
Router(config)# nvram set com4_config 192008n1
set com4_config=192008n1
```

Enable advanced options of dialup

```
Router(config)# nvram set advanced 1
set advanced=1
```

Configure ICMP server

```
Router(config)# nvram set wan1_icmp_host www.sina.com
set wan1_icmp_host=www.sina.com
```

Configure LAN IP

```
Router(config)# nvram set lan0_ip 192.168.2.1
set lan0_ip=192.168.2.1
```

Enable DHCP function

```
Router(config)# nvram set dhcpd_enable 1
set dhcpd_enable=1
```

Configure DHCP IP pool: 192.168.2.10-192.168.2.20

```
Router(config)# nvram set dhcpd_start 192.168.2.10
set dhcpd_start=192.168.2.10
Router(config)# nvram set dhcpd_end 192.168.2.20
set dhcpd_end=192.168.2.20
```

Enable HTTP function

```
Router(config)# nvram set http_enable 1
set http_enable=1
```

Configure HTTP service port

```
Router(config)# nvram set http_port 80
set http_port=80
```

Enable HTTP local access

```
Router(config)# nvram set http_local 1
set http_local=1
```

Enable HTTP remote access

```
Router(config)# nvram set http_remote 1
set http_remote=1
```

Check device ID

```
Router(config)# nvram get ovdp_device_id
ovdp_device_id=711122732
```

After configuration, please don’t forget to commit and reboot router!

```
Router(config)# nvram commit
% command ok!
Router(config)# reboot
are you sure to reboot system?[Y:N] y
```

FAQ

1. InRouter is powered on, but can`t access Internet through it?

Please check：

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

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

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

3. Forget the setting after revising IP address and can`t configure InRouter?

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

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

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

Please check:

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

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

Please check:

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

6. After InRouter establishes VPN with the VPN server, your PC under InRouter can connect to the server, but the center can`t connect to your PC under InRouter?

Please make sure the firewall of your computer is disabled.

7. After InRouter establishes VPN with the VPN server, Your PC can`t connect to the server?

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

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

- ✧ Check if the protective tube is burn out.

- ✧ Check the power supply voltage range and if the positive and negative electrodes are correctly connected.

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

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

10. InRouter is powered on, when connected with PC, the Network LED is normal but can`t have a ping detection to the InRouter?

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

11. InRouter is powered on, but can`t configure through the web interface?

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

12. The InRouter dialup always fails, I can`t find out why?

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

13. How to restore InRouter to factory default settings?

- IR6x1 routers:

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

Support

In case you have problems with the installation and use, please address them to us by e-mail: support@inhandnetworks.com.

InHand Networks

Headquarters
West Wing, 11th Floor, QiMing International Mansion
Wang Jing Science Park, Chao Yang District
Beijing, 100102, China
T:+86-10-6439-1099
F:+86-10-8417-0089
info@inhandnetworks.com

US Office
7926 Jones Branch Dr. Suite 110
McLean, Virginia,22102
USA
T: +1-703-348-2988
F:+1-703-348-2988
www.inhandnetworks.com