

InRouter 700 Series User's Manual

Fifth Edition, August, 2011

(For Firmware Version: 1.3.5.v2275)



© 2011 InHand Networks, All rights reserved.
Republication without permission is prohibited.

InRouter 700 Series User's Manual

Copyright Notice

Copyright © 2011 InHand Networks

All rights reserved.

Reproduction without permission is prohibited.

Trademarks

InHand is a registered trademark of InHand Networks. Other registered marks cited in this manual represented their respective companies.

Disclaimer

Information in this document is subject to change without notice and does not represent an obligation on the part of InHand Networks.

This user manual may include intentional technical or typographical errors. Changes are periodically made to the manual to correct such errors, and these changes are not informed in new editions.

Technical Support Contact Information

InHand Networks, China

Tel: +86-010-64391099

Fax: +86-010-64399872

Email: support@inhand.com.cn

Release Notes

2011. 3. 24th: Add description for functions:

1. WOL (Wakeup Over LAN) at "Networks" → "LAN";
2. SMS control (reboot/show status) at "Service" → "SMS";
3. "User+X.509" mode for OpenVPN client;

Add Notice:

1. WAN/LAN settings: don't set the WAN/LAN IP as 192.168.3.1 (the default IP of DMZ port);

2011.8.21st: Add description for functions:

1. "Double Dialup", set backup parameters for PPP dialup at "Networks" → "Dialup";
2. "Double IPSec", set backup IPSec tunnel at "VPN" → "IPSec Tunnels";
3. "DHCP Relay" at "Service" → "DHCP Relay";
4. "DNS Relay" at "Service" → "DNS Relay";
5. Enable "SSH configuration";
6. Disable "Multi Manager" function at "System" → "Admin Access";
7. "Loopback" at "Networks" → "Loopback";
8. "Port Mirror" at "Networks" → "Port Mirror";

Contents

Contents.....	3
Introduction to InRouter 700 Series	0
1.1 Overview	1
1.2 Package Checklist.....	3
1.3 Product Features	4
1.3.1 Interfaces	4
1.3.2 Functions	5
1.3.3 Environmental Limits	6
1.3.4 Power Requirements	6
1.3.5 Physical Characteristics	6
1.3.6 Advanced Industrial Features	6
1.3.7 Device Management Software.....	7
1.3.8 Warranty	7
1.4 Product Models.....	8
Quick Installation Guide.....	9
2.1 Typical Application.....	10
2.2 Panel Layout	10
2.3 Quick Connection to Internet	12
2.3.1 Insert SIM Card	12
2.3.2 Antenna Installation.....	13
2.3.3 Power Supply.....	13
2.3.4 Connect.....	13
2.3.5 First Connect InRouter with Your PC	13
2.3.6 Start to configure your InRouter 700(Optional)	16
2.3.7 Connect InRouter with Internet	17
2.4 Quick IPsec VPN Configuration.....	18
2.5 Reset to Factory Defaults	20
2.5.1 Hardware Method	20
2.5.2 Web Method	21
Advanced Configuration	22
3.1 Configuration on Web.....	23
3.1.1 Preparation.....	23
3.1.2 System	24
3.1.3 Network.....	29
3.1.4 Service	37
3.1.5 Firewall.....	42
3.1.6 QoS.....	44
3.1.7 VPN	45
3.1.8 Tools	52
3.1.9 Status	53
3.2 Support	56

I

Introduction to InRouter 700 Series

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

1.1 Overview



InRouter 700 series industrial grade routers provide users with stable and high speed connection between remote devices and customer's center via 2.5G/3G networks. They allow wide voltage power supply (9-48V DC), large range operating temperature from -25 °C to 70 °C (-10 ~ 158F)/ humidity: 95% RH, and fully satisfy various EMC verifications, which ensure stability and reliability under harsh industrial conditions. The InRouter 700 can be placed on a desktop or DIN-mounted.

InRouter 700 series products support VPN (IPSec/PPTP/ L2TP/GRE/SSL VPN), which create high-security links between remote equipment and customer's center.

In Addition, InRouter 700 series products support the Device Manager remote device manage platform, which realizes remote operation including remote control, remote monitor, parameters configure, firmware upgrade, log/alarm management, information statistics/display, batch configuration/update and etc.

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.

RF safety distance

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

Warning

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

WEEE Notice

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

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

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



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

equipment, or manufacturer of the equipment.

1.2 Package Checklist

We put each InRouter 700 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
InRouter 700 Serials Wireless Router	1
Cable	1 Cross line,CAT-5,1.5M
Document and Software CD	1
Antenna	5m Cellular Antenna
Power Supply	
	Power Adapter, 100-265V AC in, 12V DC out (included in IR7xx)
	Power plug, American Standard (included in IR7xx)

Optional Antennas:

Picture	Type	Description
	GSM/GPRS Cellular Antennas	GPRS Quad-band (included in IR7xxGS55)
	UMTS/HSDPA/WCDMA Cellular Antennas	WCDMA Quad-band (included in IR7xxWH01)
	Anti-thief antenna	WCDMA Quad-band (Optional for IR7xxWH01)
	Stick antenna	WCDMA Quad-band (Optional for IR7xxWH01)
	Anti-thief antenna	WCDMA Quad-band (Optional for IR7xxWH01)

1.3 Product Features

1.3.1 Interfaces

WAN

Cellular WAN:

Band Options:

HSUPA /HSDPA/WCDMA

850/900/1900/2100MHz

GSM/GPRS/EDGE

850/900/1800/1900MHz

Ethernet WAN:

Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX

Magnetic Isolation Protection: 1.5 KV built-in

LAN

IR701/711/791:

Number of Ports: 1

Ethernet: 10/100 Mbps, RJ45 connector, Auto MDI/MDIX

Magnetic Isolation Protection: 1.5 KV built-in

IR704/714/794:

Number of Ports: 4

Ethernet: 10/100 Mbps, RJ45 connector, auto MDI/MDIX

Magnetic Isolation Protection: 1.5 KV built-in

Serial

A. Serial Type: RS232/485

B. Data bit: 5/6/7/8

C. Stop bit: 1/2

D. Check bit: N/O/D

E. Baud rate: 1,200bit/s~ 115,200bit/s

SIM Interface

SIM Control: 3 V

1.3.2 Functions

PPP

Supported VPDN/APN, fast access to virtual private dial-up network (VPDN) provided by mobile operator, ensure high-security data transmission.

Support PPPoE (Point to Point Protocol over Ethernet) Protocol.

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

Dynamic IP

Support DHCP, applied as Server/Client

Dynamic DNS

Support Dynamic DNS-IP Binding

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 (not available for IR701/704)

IPSec VPN

L2TP VPN

PPTP VPN

GRE

SSL VPN (for IR791/794 only)

Link Backup

VRRP

Support VRRP protocols, realizing immediate link backup

Hot Link Backup (for IR704/714/794 only)

Support Wireless Hot Link Backup for cable link via only one device

DNS Forwarding

Support DNS Forwarding, support DNS record

Network tools

Support Ping, Trace Route and Telnet

Wakeup Over LAN (WOL)

Support Wakeup over LAN, to wakeup industrial PC over Eth. after receives SMS.

RSSI + Cell ID Display

1.3.3 Environmental Limits

Operating Temperature: -25 to 70 °C (-10 to 158 °F)

Operating Humidity: 5 to 95% RH

Storage Temperature: -40 to 85 °C (-40 to 167 °F)

1.3.4 Power Requirements

Power Inputs: 1 terminal block, including power jack and serial.

Input Voltage: 9 -48 VDC

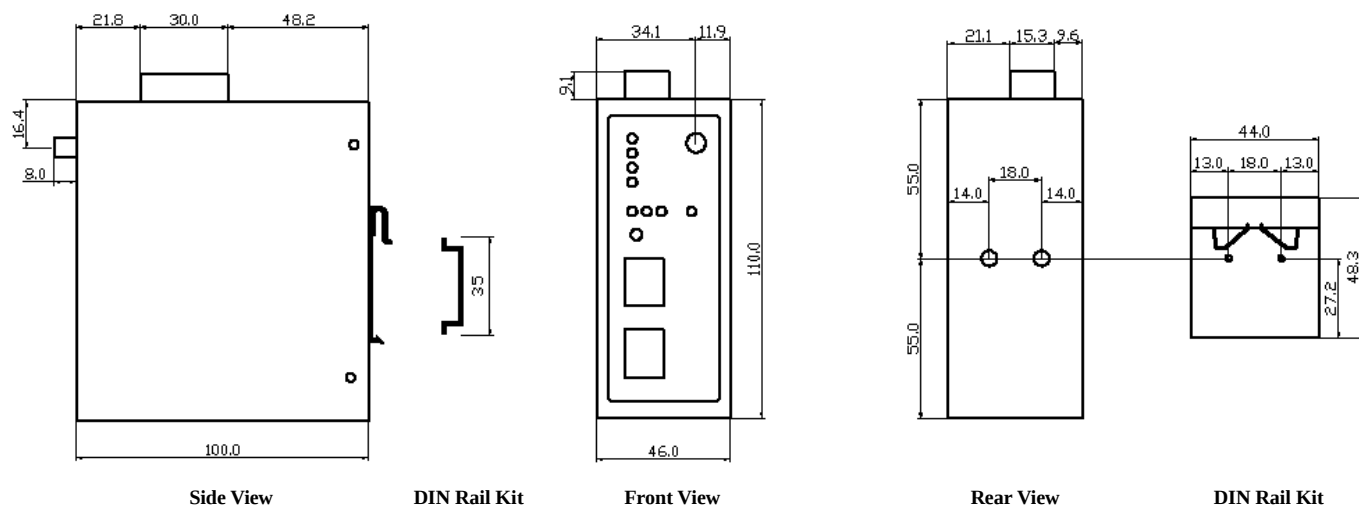
1.3.5 Physical Characteristics

Housing: Steel, providing IP30 protection

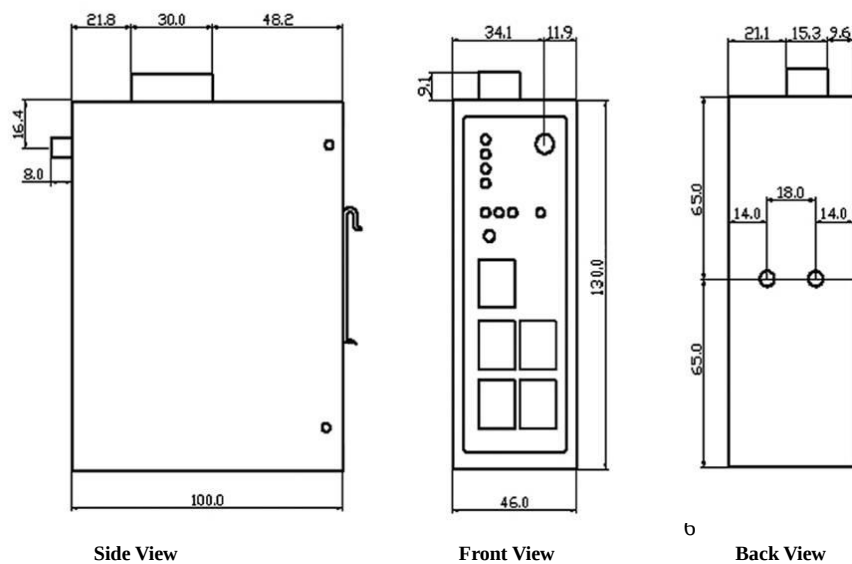
Weight: 490g

Dimensions (mm)

IR701/711/791:



IR704/714/794:



RF Electromagnetic Field Immunity: EN61000-4-3, Level 3

RF conducted interference: EN61000-4-6, Level 3

Damped oscillation Immunity: EN61000-4-12, Level 3

Power-frequency electromagnetic fields Immunity: EN61000-4-8, Level 5

Anti-shock: IEC60068-2-27

Drop: IEC60068-2-32

Vibration: IEC60068-2-6

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 current models of InRouter 700 Series include: InRouter 701/711/791GS55, InRouter 701/711/791WH01, InRouter 704/714/794WH01.

The models are classified according to main difference including cellular network, VPN support and interface for device.

Model	Serial	LAN	Cellular WAN	Ethernet WAN	VPN	CA X.509 base64
GPRS						
IR701GS55	RS232/485	1 RJ45	GSM/GPRS 850/ 900/1800/1900 MHz	N/A	N/A	N/A
IR711GS55	RS232/485	1 RJ45	GSM/GPRS 850/ 900/1800/1900 MHz	N/A	IPSec/PPTP/L2TP/GRE	N/A
IR791GS55	RS232/485	1 RJ45	GSM/GPRS 850/ 900/1800/1900 MHz	N/A	IPSec/PPTP/L2TP/GRE/SSL	Support
UTMS						
IR701WH01	RS232/485	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	N/A	N/A
IR711WH01	RS232/485	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	IPSec/PPTP/L2TP/GRE	N/A
IR791WH01	RS232/485	1 RJ45	HSUPA /HSDPA/WCDMA: 850/900/1900/2100MHz GSM/GPRS/EDGE: , 850/900/1800/1900MHz	N/A	IPSec/PPTP/L2TP/GRE/SSL	Support
IR704WH01	RS232/485	4 RJ45	WCDMA/HSUPA 850/900/1900/2100MHz	ADSL/DHCP/ PPPoE/Static IP	N/A	N/A
IR714WH01	RS232/485	4 RJ45	WCDMA/HSUPA 850/900/1900/2100MHz	ADSL/DHCP/ PPPoE/Static IP	IPSec/PPTP/L2TP/GRE	N/A
IR794WH01	RS232/485	4 RJ45	WCDMA/HSUPA 850/900/1900/2100MHz	ADSL/DHCP/ PPPoE/Static IP	IPSec/PPTP/L2TP/GRE/SSL	Support
USB Modem						
IR701UE	RS232/485	1 RJ45	USB Modem	N/A	N/A	N/A
IR711UE	RS232/485	1 RJ45	USB Modem	N/A	IPSec/PPTP/L2TP/GRE	N/A
IR791UE	RS232/485	1 RJ45	USB Modem	N/A	IPSec/PPTP/L2TP/GRE/SSL	Support
IR704UE	RS232/485	4 RJ45	USB Modem	ADSL/DHCP/ PPPoE/Static IP	N/A	N/A
IR714UE	RS232/485	4 RJ45	USB Modem	ADSL/DHCP/ PPPoE/Static IP	IPSec/PPTP/L2TP/GRE	N/A

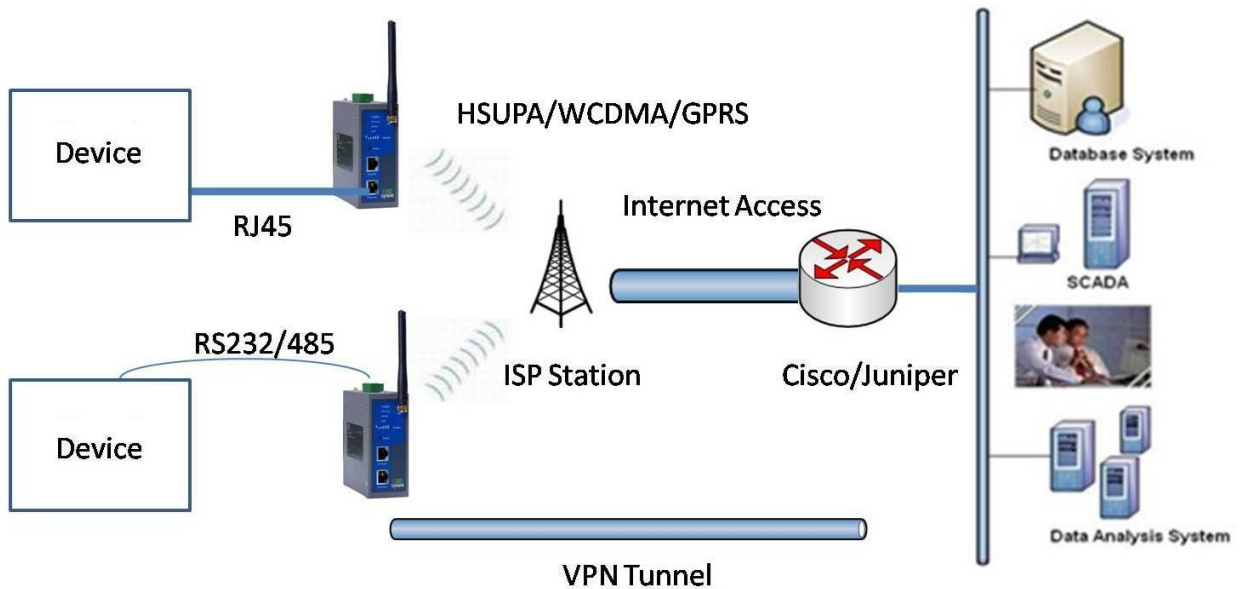
IR794UE	RS232/485	4 RJ45	USB Modem	ADSL/DHCP/ PPPoE/Static IP	IPSec/PPTP/L2TP/GRE/SSL	Support
---------	-----------	--------	-----------	-------------------------------	-------------------------	---------

II

Quick Installation Guide

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

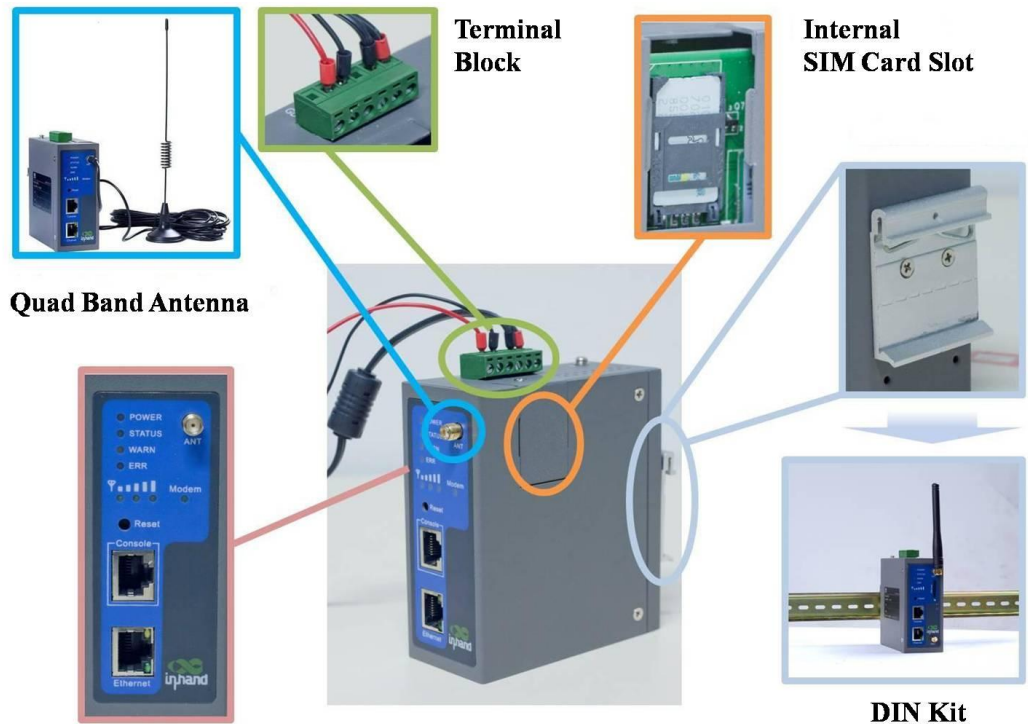
2.1 Typical Application



InRouter 700 series can be used to connect your device (with RS232/485/Ethernet Interface) to internet via GPRS/HSUPA cellular. Meanwhile, to ensure the security and access, InRouter 700 series support VPN, enabling remote access and secure data transmission through internet.

2.2 Panel Layout

IR701/711/791:



IR704/714/794:



Interface	Description
Power Interface	Access 9-48 V DC Power Supply
Serial	Access to the serial line, realizing
Ethernet Ports	One 10/100Base-TX RJ45 Port (IR701/711/791GS55, IR701/711/791WH01, IR701/711/791UE) Four 10/100Base-TX RJ45 Ports, (IR704/714/794UE, IR704/714/794WH01)
ANTENNA	2.5G/3G antenna
SIM Card Connector	Put 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 (bad signal level, route cannot work, please check the antenna and local signal level)



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



Signal: 20-31 (Perfect signal level)

2.3 Quick Connection to Internet

2.3.1 Insert SIM Card



Open InRouter SIM/UIM card case at the button, insert the SIM card and close the case.



For the external USB modem type, insert the USB card into the USB port.

2.3.2 Antenna Installation

After install the IR700, connect the interface of enhanced antenna and the interface of skin antenna and screw closely. Put the amplifier of enhanced antenna to where there receives good signal.

Attention: The position and angle may influence the quality of signal.

2.3.3 Power Supply

Link the power supply in the product package with InRouter, watch where the InRouter Power LED on the panel is light up. If not, please connect with InHand for technical supports.

You can configure IR700 after the Power LED lights up.

2.3.4 Connect

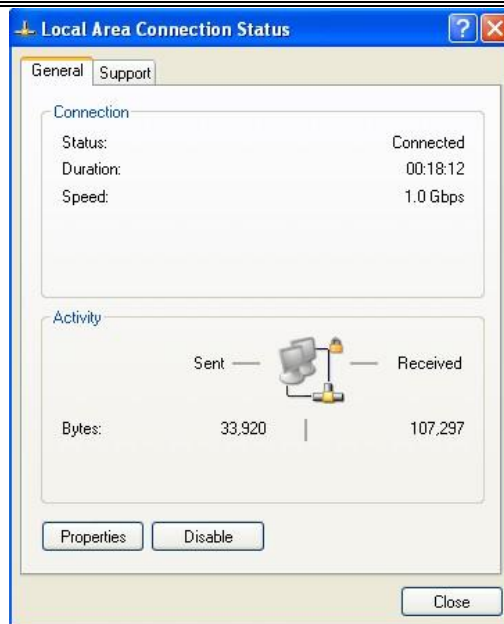
Link the IR700 with PC:

- (1) Using the cable to link IR700 with PC;
- (2) After the connection, you can see one LED of RJ45 Interface turns green and the other flashes.

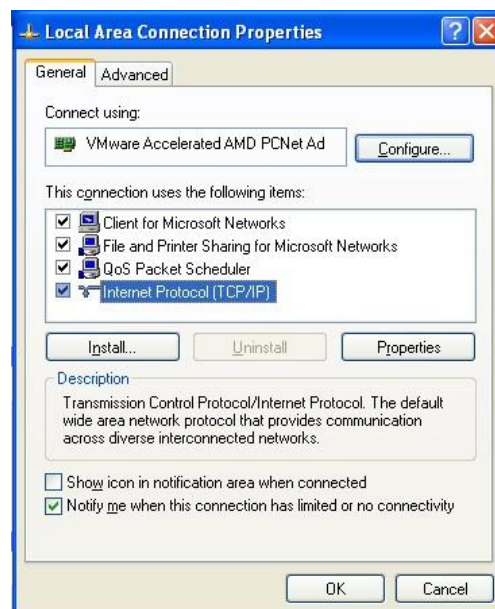
2.3.5 First Connect InRouter with Your PC

IR700 Router can auto-distribute IP address for PC. Please set the PC to automatically obtain IP address via DHCP. (Based on the Windows operation system):

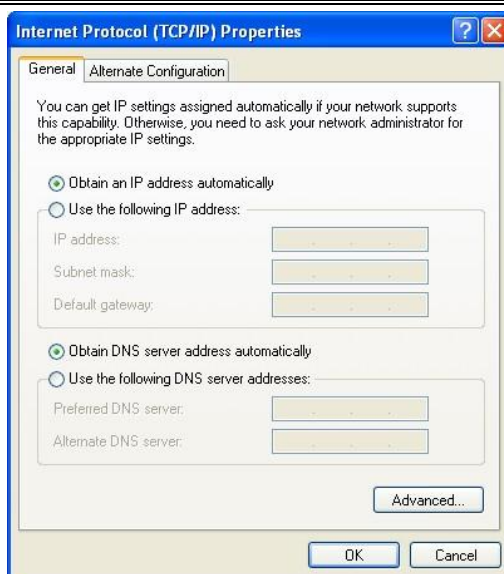
- 1) Open "Control Panel", double click "Network Connections" icon, and enter "Network Connections" Screen.
- 2) Double click "Local Area Connection", enter "Local Area Connection Status" screen:



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



Choose “Internet Protocol (TCP/IP)”, click “properties” button, 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 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 IR700).

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

Ping 192.168.2.1

If the screen shows:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\inhand>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time=1ms TTL=128
Reply from 192.168.2.1: bytes=32 time<1ms TTL=128

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Documents and Settings\inhand>ping 192.168.2.1
```

Then the link between the PC and Router is correct connected. Else if it shows:

```
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\inhand>ping 192.168.2.1

Pinging 192.168.2.1 with 32 bytes of data:

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.2.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Documents and Settings\inhand>
```

Then the connection seems not build, and you need to check thoroughly following the former instructions.

2.3.6 Start to configure your InRouter 700(Optional)

After you have finished the former steps, you can configure the Router:

- 1) Open IE browser, input the default IP address of the Router: <http://192.168.2.1>, you can see the login web below:

Router Login

Username

Password

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

- 2) Change the IP configuration:

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

If you want to set your own IP of InRouter 700, please follow the instructions below:

System	Network	Services	Firewall	QoS	VPN	Tools	Status
System Status							
Name	Router						
Model	IR711VZ30						
Serial Number	RZ7110911116349						
Description	www.inhand.com.cn						
Current Version	1.3.0.r1729(test)						
Current Bootloader Version	1.1.6.r1572						
Router Time	2010-04-06 16:47:16						
PC Time	2010-04-06 16:47:59 Sync Time						
Up time	0 day, 00:03:10						
CPU Load (1 / 5 / 15 mins)	0.01 / 0.00 / 0.00						
Memory consumption	13.35MB / 3,860.00KB (28.24%)						
Total/Free							
3 Seconds Stop							

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

System	Network	Services	Firewall	QoS
MAC Address 00:18:05:00:45:C6 Default IP Address 192.168.1.254 Netmask 255.255.255.0 MTU Default 1500 Detection host 0.0.0.0 LAN Mode Auto Negotiation				

- 3) Click “Apply”, then you will see:



Now the IP address of IR700 has been reset, and in order to enter the configuration web, you need set your PC in the same subnet, for example: 192.168.1.10/24 then input the changed IP address (192.168.1.254) in your IE Browser.

2.3.7 Connect InRouter with Internet

Following the configuration steps below to enable IR700 to connect with the internet.

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

InHand Networks

System Network Services Firewall QoS VPN Tools Status

Dialup

Enable ☒

Time schedule **ALL** Schedule Management

Shared Connection(NAT) ☒

Network Provider (ISP) **Custom** Manage

APN

Access Number

Username

Password

Primary Profile Retries (0: always)

Network Select Type **Auto**

Band **ALL**

Static IP ☐

Connection Mode **Always Online**

Redial Interval Seconds

Show Advanced Options ☐

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

Dialup Number, Username and Password are provided by local mobile operator. You can contact them for more details.

The following example shows parameters provided by China Mobile, Vodafone and Cingular. 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

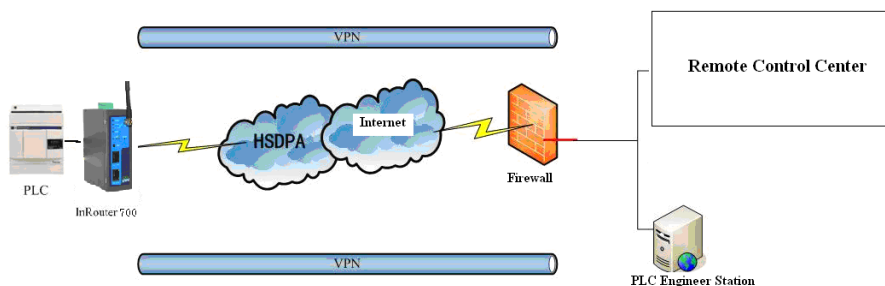
After correct configuration, InRouter 700 can now connect with Internet. Open IE Browser, input www.google.com, you can see the Google web as below:



[Google Search](#) [I'm Feeling Lucky](#)
[Advanced Search](#)
[Language Tools](#)
[Advertising Programs](#) [Business Solutions](#) [About Google](#) [Go to Google China](#)
© 2010 - [Privacy](#)

2.4 Quick IPSec VPN Configuration

If you need to build a VPN tunnel to realize access to your PLC far away through internet or you need ensure the security by using VPN. Here's a quick configuration guide of IPSec for InRouter 700 Series.



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

System	Network	Services	Firewall	QoS	VPN
IPSec Settings					
Enable NAT-Traversal (NATT) ☒ Keep alive time interval of NATT 60 Seconds Enable Compression ☒ Debug ☐ Force NATT ☐					
Apply Cancel					

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 concrete situation.

Click “Apply” to finish configuration.

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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
IPSec Tunnels							
Name		Tunnel Description		Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters	
Add		Show Detail Status					
Stop							

Click “Add” to add a new IPSec Tunnel:



System	Network	Services	Firewall	QoS	VPN	Tools	Status
IPSec Tunnels							
Edit IPSec tunnel							
Show Advanced Options ☒							
Basic Parameters							
Tunnel Name		IPSec_tunnel_1					
Destination Address		23.34.45.56					
Startup Modes		Auto Activated					
Restart WAN when failed		☒					
Negotiation Mode		Main Mode					
IPSec Protocol		ESP					
IPSec Mode		Tunnel Mode					
Tunnel Type		Subnet - Subnet					
Local Subnet		192.168.2.1					
Local Netmask		255.255.255.0					
Remote Subnet		0.0.0.0					
Remote Netmask		255.255.255.0					

Basic Parameters: set 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: configure parameters during the 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: configure parameters during the 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:

System	Network	Services	Firewall	QoS	VPN	Tools	Status
IPSec Tunnels							
	Name	Tunnel Description	Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters		
	IPSec_tunnel_1	192.168.2.1/255.255.255.0===router...0.0.0.0===0.0.0.0/255.255.255.0 ESP, Tunnel Mode, Main Mode, Auto Activated	Authentication Type: Shared Key Policy: 3des-md5-modp1024 Lifetime: 86400Seconds Disabled Perfect Forward Secrecy(PFS)	Policy: 3des-md5-96 Lifetime: 3600Seconds	Enable DPD, Interval: 60Seconds, Timeout: 180Seconds Disabled ICMP Detection		
Add		Show Detail Status					
5 Seconds Stop							

You can click “Show Detail Status” to observe the specific connection details, or click “Add” to add a new tunnel. Now you succeed to build 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 web will show:

IPSec Tunnels				
Name	Tunnel Description	Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters
IPSec_tunnel_1	192.168.220.0/255.255.255.0===router...===192.168.123.0/255.255.255.0 ESP; Tunnel Mode; Aggressive Mode; Auto Activated 500 STATE_QUICK_I2 (sent Q12, IPsec SA established): EVENT_SA_REPLACE in 2494s: newest IPSEC: croute owner: isakmp#1; idle: import:admin initiate esp fe37d11b0... esp dc8a9687010.5.1.40 tun.0010.5.1.40 ref=0 ref=0 ref=0 ref=0 ref=0 500 STATE_AGRU_I2 (sent A12, ISAKMP SA established): EVENT_SA_REPLACE in 85293s: newest ISAKMP: lastdpd=60s(seq in:19415 out:0); idle: import:admin initiate	Authentication Type: Shared Key Policy: 3des-md5-modp1024 Lifetime: 86400Seconds Enable Perfect Forward Secrecy(PFS): Group 1	Policy: 3des-md5-96 Lifetime: 3600Seconds	Enable DPD, Interval: 60Seconds, Timeout: 180Seconds Disabled ICMP Detection
Add		Show Detail Status		

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:

```
C:\Documents and Settings\Jason Hu>ping 192.168.123.250

Pinging 192.168.123.250 with 32 bytes of data:

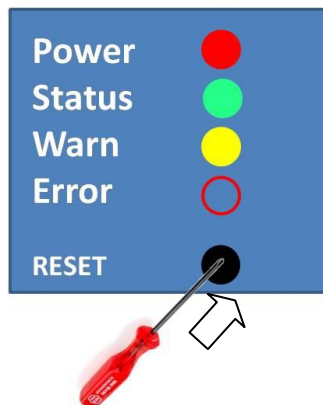
Reply from 192.168.123.250: bytes=32 time=428ms TTL=63
Reply from 192.168.123.250: bytes=32 time=395ms TTL=63
Reply from 192.168.123.250: bytes=32 time=397ms TTL=63
Reply from 192.168.123.250: bytes=32 time=393ms TTL=63
```

2.5 Reset to Factory Defaults

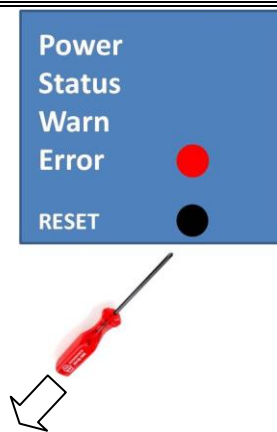
2.5.1 Hardware Method

Legend: On--● Off--○ Blink--⚡

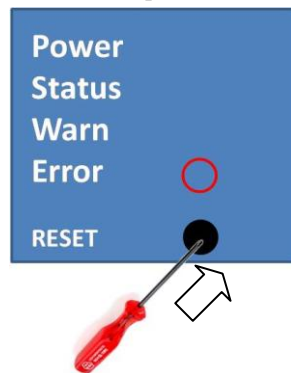
1) Push RESET button while powering on IR700:



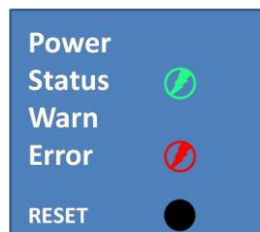
2) When you see ERROR LED turns on (about 10 seconds after powering on), stop push RESET button:



3) After a few seconds, the ERROR LED then turns off, now push RESET button again:



4) Then you will see ERROR and STATUS blinking, which means reset to factory defaults successfully!



Factory default settings:

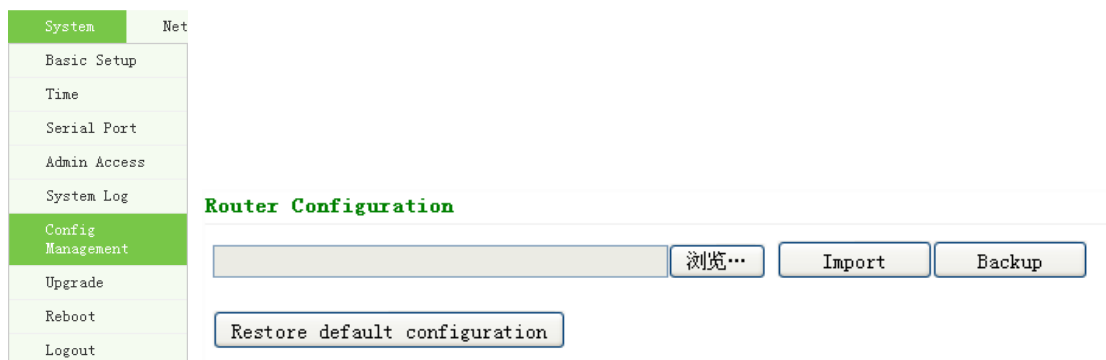
IP: 192.168.2.1

Net Mask: 255.255.255.0

Serial parameter: 19200-8-N-1

2.5.2 Web Method

1) Login the web interface of IR700, select “System”→”Config Management”:



2) Click “Restore default configuration” to Reset IR700.

III

Advanced Configuration

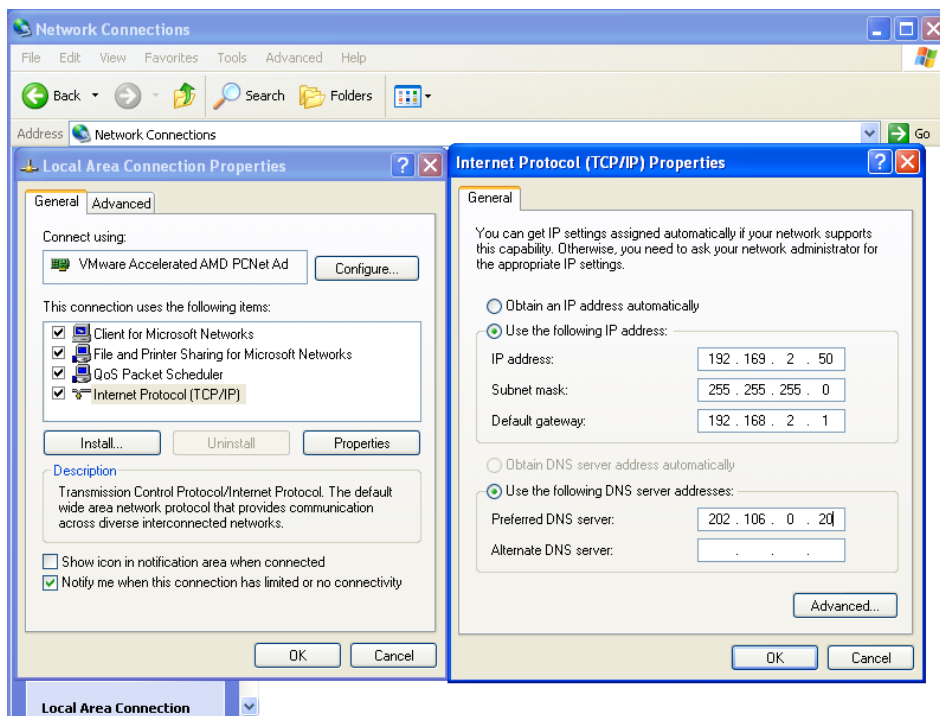
- ◆ Configuration on Web

3.1 Configuration on Web

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

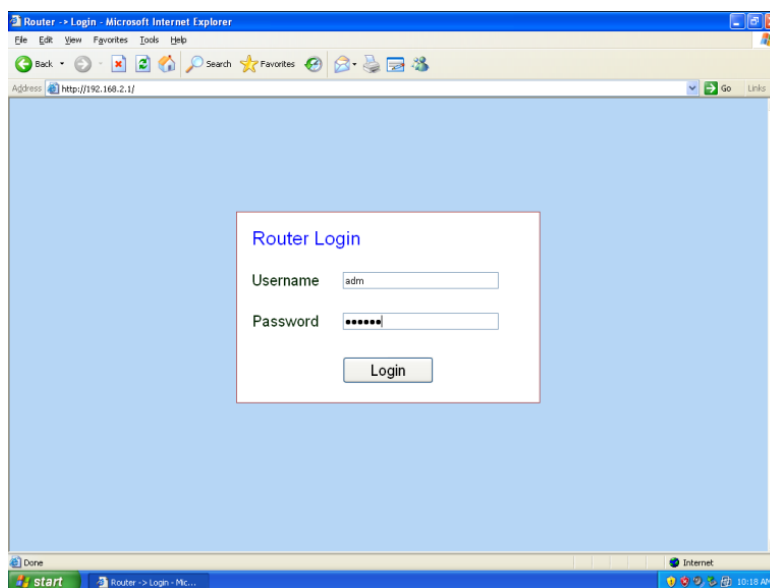
3.1.1 Preparation

Firstly, connect your devices with IR700 by cable or HUB (switch), then set the IP of PC and IR700 in the same subnet, for example: Set PC IP to 192.168.2.50, net mask: 255.255.255.0, gateway (default IP of IR700: 192.168.2.1):



Open IE browser, input the IP address of IR700: <http://192.168.2.1> (default IP of IR700).

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



Click "Login" to enter configure web:

Router -> Cellular Router

InHand Networks

System Network Services Firewall QoS VPN Tools Status

System Status

Name	Router
Model	IR794VZ30-LP
Serial Number	RZ7141005119560
Description	www.inhand.com.cn
Current Version	1.3.4.r2101
Current Bootloader Version	1.1.6.r1742
Router Time	2011-03-22 15:37:16
PC Time	2011-03-22 15:37:17 Sync Time
Up time	0 day, 00:01:30
CPU Load (1 / 5 / 15 mins)	0.13 / 0.05 / 0.01
Memory consumption	13.35MB / 2,756.00KB (20.16%)
Total/Free	

3.1.2 System

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

(1) Basic Setup

System Network Services Firewall QoS VPN Tools Status

Basic Setup

Language

Router Name

Hostname

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 IR700	Router	My InRouter

(2) Time

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Time							
Router Time		2010-04-12 10:55:23					
PC Time		2010-04-12 10:55:22 Sync Time					
Timezone		Custom v					
Custom TZ String		CST-8					
Auto Update Time		On startup v					
NTP Time Servers		114.80.81.1					
		pool.ntp.org					
Apply		Cancel					

Name	Description	Default
Router Time	Display router time	1970-1-1 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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Serial Port							
Baudrate	19200 ▾						
Data Bits	8 ▾						
Parity	None ▾						
Stop Bit	1 ▾						
Hardware Flow Control	☐						
Software Flow Control	☐						
Apply Cancel							

Name	Description	Default
Baud Rate	Serial baud rate	19200
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

Admin Access

Username / Password

Username
 Old Password
 New Password
 Confirm New Password

Management

Enable	Service Type	Service Port	Local access	Remote access	Allowed addresses from WAN (Optional)	Description
☒	HTTP	80	☒	☒		
☐	HTTPS	443	☒	☒		
☒	TELNET	23	☒	☒		
☐	SSHD	22	☒	☒		
☒	Console					

Non-privileged users

Username	Password

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 IR700 by WAN. (e.g.: HTTP) Disable—forbid to manage IR700 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 IR700)	
Other Parameters		
Log Timeout	Set the Log Timeout, configuration web will be disconnected after timeout	500 seconds

(5) System Log

System	Network	Services	Firewall	QoS	VPN	Tools	Status
System Log							
Log to Remote System ☒							
IP Address / Port(UDP) 192.168.2.23 514							
Apply Cancel							
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					

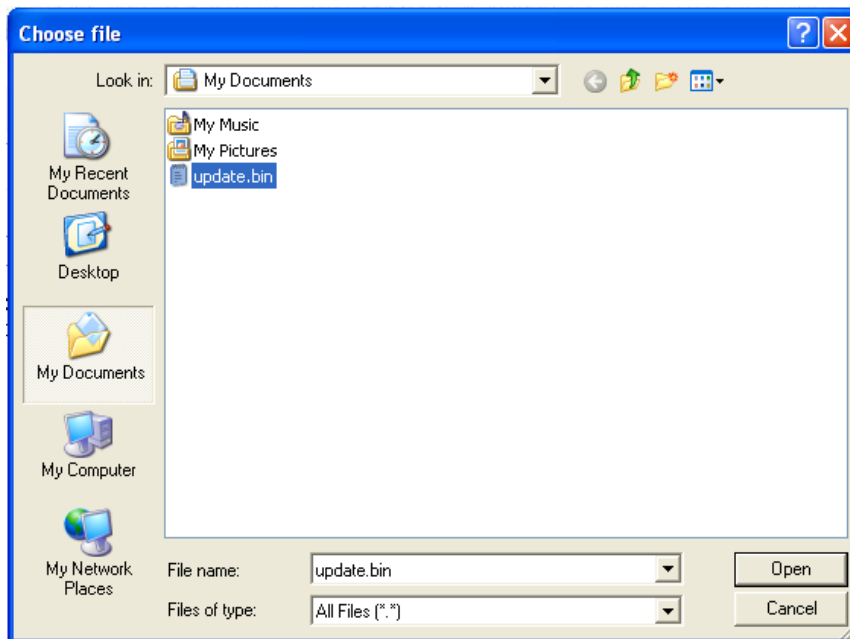
(6) Config Management

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Config Management							
Router Configuration							
Browse... Import Backup							
Restore default configuration							
Network Provider (ISP)							
Browse... Import Backup							
Name	Description						
Router Configuration	Import/Backup configuration file						
Restore default configuration	Click to reset IR700 (to enable RESET, you need to reboot IR700)						
Network Provider (ISP)	Used to configure the APN, username, password and other parameters of major operators						

(7) System Upgrade

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Upgrade							
Select the file to use: Browse... Upgrade							
Current Version : 1.3.0.r1733 Current Bootloader Version : 1.1.6.r1624							

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



Click “update”, and then click “sure” to begin update as it shows below.

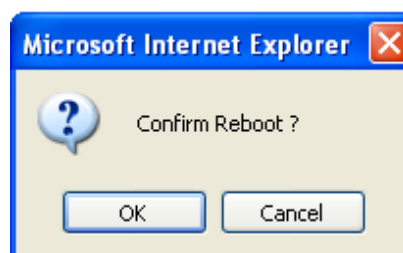
⌚ 0:01

Upgrading system...
It will take about 1-5 minutes depending on network. Please wait and don't interrupt!

Upgrade firmware succeed, and click “reboot” to restart IR700.

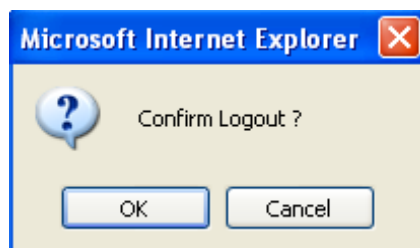
(8) Reboot

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 configurations of Dialup, LAN, DNS, DDNS, Static Route, and etc.

(1) Dialup



System	Network	Services	Firewall	QoS	VPN	Tools	Status
Dialup							
Enable	☒						
Time schedule	ALL Schedule Management						
Shared Connection(NAT)	☒						
Network Provider (ISP)	Custom Manage						
APN	uninet						
Access Number	*99***1#						
Username	gprs						
Password							
Primary Profile Retries	0 (0: always)						
Network Select Type	Auto						
Band	ALL						
Static IP	☐						
Connection Mode	Always Online						
Redial Interval	30 Seconds						
Show Advanced Options ☒							
Initial Commands							
PIN Code							
Dial Timeout	120 Seconds						
MTU	1500						
MRU	1500						
TX Queue Length	64						
Authentication Type	Auto						
Enable IP head compression	☒						
Use default asyncmap	☐						
Use Peer DNS	☒						
Link Detection Interval	55 Seconds(0: disable)						
Link Detection Max Retries	3						
Debug	☐						
Expert Options	nomppe nomppc nodeflate nobsdcomp novj novjccomp						
ICMP Detection Server							
ICMP Detection Interval	30 Seconds						
ICMP Detection Timeout	5 Seconds						
ICMP Detection Max Retries	5						
Apply Cancel							

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 (IR700 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 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 (IR700 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:

System Network Services Firewall QoS VPN Tools Status

Schedule Management

Dialup

Name	Sunday	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Time Range 1	Time Range 2	Time Range 3	Description
schedule_1	☐	☒	☒	☒	☒	☒	☐	9:00-12:00	14:00-18:00	0:00-0:00	

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) WAN (for InRouter704/714/794 only)

The screenshot shows the WAN configuration page with tabs for System, Network, Services, Firewall, QoS, Tools, and Status. The 'WAN' tab is active. Under the 'Type' label, a dropdown menu is open, showing options: Disabled, Static IP, Dynamic Address (DHCP), ADSL Dialup (PPPoE), and Disabled (highlighted). Below the dropdown are 'Apply' and 'Cancel' buttons.

This page is to set the type of WAN port:

Name	Description	Default
Type	Static IP; Dynamic Address(DHCP); ADSL Dialup(PPPoE); Disabled	Disabled

Attention: There can only be one WAN type at one time, enabling one type WAN will disabled another.

WAN—Static IP

The screenshot shows the WAN Static IP configuration page. The 'Type' is set to 'Static IP'. The 'SHARED' checkbox is checked. The 'MAC Address' is 00:18:05:00:51:44, with 'Default' and 'Clone' buttons. The 'IP Address' is 192.168.1.29, 'Netmask' is 255.255.255.0, and 'Gateway' is 192.168.1.1. The 'MTU' is set to 'Default' with a value of 1500. Below these fields is the 'Multi-IP Settings' section with a table for adding additional IP addresses. The table has columns for IP Address, Netmask, and Description. An 'Add' button is at the bottom right of the table. 'Apply' and 'Cancel' buttons are at the bottom of the page.

Notice: please **DO NOT** set WAN address as: 192.168.3.x (an IP for DMZ port).

Name	Description	Default
Type	Static IP	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
IP Address	Set WAN port IP	192.168.1.29
Net Mask	Set WAN port Net Mask	255.255.255.0
Gateway	Set WAN Gateway	192.168.1.1
MTU	Set Max Transmission Unit, optional between default and manual	1500
Multi-IP Settings(can set 8 additional IP address at the most)		
IP address	Set the additional IP address of LAN	Blank
Net Mask	Set Net Mask	Blank
Description	Describe the settings	Blank

WAN—Dynamic Address (DHCP)

WAN

Type: Dynamic Address (DHCP)

SHARED: ☒

MAC Address: 00:18:05:00:51:44 Default Clone

MTU: Default 1500

Apply Cancel

Name	Description	Default
Type	Dynamic Address (DHCP)	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
MTU	Set Max transmission unit, optional between default and manual	1500

WAN --ADSL

WAN

Type: ADSL Dialup (PPPoE)

SHARED: ☒

MAC Address: 00:18:05:00:51:44 Default Clone

MTU: Default 1492

ADSL Dialup (PPPoE) Settings

Username:

Password:

Static IP: ☒

IP Address:

Peer Address: 0.0.0.0

Connection Mode: Always Online

Show Advanced Options ☒

Service Name:

TX Queue Length: 3

Enable IP head compression: ☐

Use Peer DNS: ☒

Link Detection Interval: 55 Seconds

Link Detection Max Retries: 10

Debug: ☐

Expert Options:

ICMP Detection Server:

ICMP Detection Interval: 30 Seconds

ICMP Detection Timeout: 3 Seconds

ICMP Detection Max Retries: 3

Apply Cancel

Name	Description	Default
Type	ADSL Dialup (PPPoE)	
SHARED	Enabled—the local device linked with Router can get access to internet. Disable—the local device can't get access to internet via Router.	Enable
MAC Address	Set MAC Address	
MTU	Set Max Transmission Unit, optional between default and manual	1500
ADSL Dialup (PPPoE) Settings		

Username	Set username for dialing up	Blank
Password	Set password for dialing up	Blank
Static IP	Enable Static IP	Disabled
IP address	Static IP Address	Blank
Peer IP	Set Peer IP	Blank
Connection Mode	Set connection mode (Connect on Demand/Always Online/ Manual)	Always Online
Advanced Options		
Show advanced options	Enable advanced configuration	Disabled
Service Name	Name the service	Blank
TX Queue Length	Set TX Queue Length	3
Enable IP head compression	Click to enable IP head compression	Disabled
User Peer DNS	Enable User Peer DNS	Disabled
Link Detection Interval	Set link detection interval	55 seconds
Link Detection Max Retries	Set link detection max retries	10 (times)
Debug	Select to enable debug-mode	Disabled
Expert Options	Set expert parameters	Blank
ICMP Detection Server	Set ICMP Detection Server	Blank
ICMP Detection Time	Set ICMP Detection Time	30
ICMP Detection Timeout	Set ICMP Detection Timeout	3
ICMP Detection Max Reties	Set ICMP Detection Max Reties	3

(3) Link Backup (for IR704/714/794 only)

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Link Backup							
Enable		☒					
Main Link		WAN					
ICMP Detection Server							
ICMP Detection Interval		10 Seconds					
ICMP Detection Timeout		3 Seconds					
ICMP Detection Max Retries		3					
Backup Link		WAN					
Apply		Cancel					

Link Backup, to realize link backup between Cellular WAN and Ethernet WAN, when one fails, IR700 will try the other

Name	Description	Default
Enable	Enable Link Backup service	Disabled
Main Link	InRouter will choose this for normal WAN connection	WAN (Ethernet WAN)
ICMP Detection Server	ICMP can ensure a link to certain destination	
ICMP Detection Interval	Time interval between ICMP packages	10
ICMP Detection Timeout	Timeout for each ICMP package	3 (seconds)
ICMP Detection Max Retries	After the retries if no ICMP succeed, dialup will try the backup link	3
Backup Link	Select the backup link	WAN

(4) LAN

LAN

MAC Address Default

IP Address

Netmask

MTU Default 1500

Detection host

WOL MAC Address Device List

Multi-IP Settings

IP Address	Netmask	Description

Add

Apply Cancel

Notice: please **DO NOT** set LAN address as: 192.168.3.x (an IP for DMZ port).

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

(5) Loopback

Loopback

IP Address

Netmask

Multi-IP Settings

IP Address	Netmask	Description

Apply Cancel

Name	Description	Default
IP Address	The IP Address for loopback	127.0.0.1
Net Mask	Set Net Mask of loopback host	255.0.0.0
Multi-IP Settings (Support additional 8 IP addresses at the most)		
IP Address/Net mask	Set additional IP/Net mask of loopback host	Blank
Description	Description about this IP address	Blank

(6) DMZ Port (for InRouter704/714/794 only)

Configure this page after select WAN-DMZ-LAN mode in Port Mode page.

Name	Description	Default
MAC Address	Set MAC address of DMZ port	(Provided by Manufacture: InHand)
IP Address	Set IP Address of DMZ port	192.168.3.1
Net Mask	Set Net Mask of DMZ port	255.255.255.0
MTU	Optional between Default & Manual	Default (1500)
Multi-IP Settings (8 additional IP address at the most)		
IP Address	Set additional IP address for DMZ port	Blank
Net Mask	Set Net Mask	Blank
Description	Description of additional IP address	Blank

(7) Port Mode (for InRouter704/714/794 only)

Notice: please **DO NOT** set WAN IP/LAN IP/DMZ IP the same; it will disable your link to internet!

Name	Descriptions	Default
Port Mode	LAN (four LAN ports)	WAN-DMZ-LAN
	WAN-LAN (3 LAN ports and 1 WAN port)	

(8) Port Mirror (for InRouter704/714/794 only)

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Port Mirror							
Enable	☒						
Destination Port	Port 1						
Port 1	None						
Port 2	None						
Port 3	Both						
Port 4	None						
Apply Cancel							

This function is used for Engineer capture packages of different ports of IR700.

Destination Port: the port to which you want to send the copied packages.

Here we set Port 3 as example, after you set Port 1 as destination port, and Port 3“Both”, you can link your PC to Port 1 and get the packages sent and received by Port 3.

(9) DNS

System	Network	Services	Firewall	QoS	Tools	Status
DNS						
Primary DNS	0.0.0.0					
Secondary DNS	0.0.0.0					
Apply Cancel						

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

(10) DDNS (Dynamic DNS)

System	Network	Services	Firewall	QoS	Tools	Status
DDNS						
Dynamic DNS ==> Dialup						
Current Address						
Service Type	Disabled					
Apply Cancel						

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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
DDNS							
Dynamic DNS ==> WAN							
Current Address	10.5.1.40						
Service Type	DynDNS - Dynamic						
URL	http://www.dyndns.com/						
Username	test						
Password							
Hostname	test						
Wildcard	☐						
MX							
Backup MX	☐						
Force Update	☐						
Last Update	-						
Last Response	-						
Apply Cancel							

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	

(11) Static Route

System	Network	Services	Firewall	QoS	Tools	Status
Static Route						
Destination	Netmask	Gateway	Interface	Description		
0.0.0.0	255.255.255.0	0.0.0.0				
Add						
Apply Cancel						

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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
DHCP Service							
Enable DHCP		☒					
IP Pool Starting Address		10.5.1.90					
IP Pool Ending Address		10.5.1.254					
Lease		60 Minutes					
DNS		10.5.1.89					Edit
Windows Name Server (WINS)		0.0.0.0					
Static DHCP							
MAC Address		IP Address		Host			
00:00:00:00:00:00		10.5.1.90					
Add							
Apply Cancel							

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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
DNS Relay							
Enable DNS Relay		☒					
Static [IP address <=> Domain Name] Pairing							
IP Address		Host		Description			
Add							
Apply Cancel							

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) DHCP Relay


System Network Services Firewall QoS VPN Tools Status

DHCP Relay

Enable ☒

DHCP Server

Source IP

This function can realize DHCP relay and send relay packages to LAN interface of router.

Name	Description	Default
Enable DHCP Relay	Click to enable DHCP Relay	Enable (after enable DHCP)
DHCP Server	Set the DHCP Server's address, always you need ensure DHCP server is in the same LAN or VPN subnet as IR700's LAN	Blank
Source IP	The interface IR700 will forward the DHCP acknowledge packages (always set the LAN IP of IR700)	Blank

(4) VRRP

System Network Services Firewall QoS VPN Tools Status

VRRP

Enable ☒

Group ID

Priority

Advertisement Interval Seconds

Virtual IP

Authentication Type

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

(5) Device Manager

System Network Services Firewall QoS VPN Tools Status

Device Manager

Mode: SMS & IP

Vendor: Disable

Device ID: Only SMS

Server: SMS & IP

Port: 9000

Login Retries: 3

Heartbeat Interval: 120 Seconds

Packet Receiving Timeout: 30 Seconds

Packet Transmit Retries: 3

Query SMS Interval: 24 hours

Trust phone list:

Apply Cancel

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

System Network Services Firewall QoS VPN Tools Status

Device Manager

Mode: Only SMS

Query SMS Interval: 24 hours

Trust phone list:

Apply Cancel

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	

System Network Services Firewall QoS VPN Tools Status

Device Manager

Mode: SMS & IP

Vendor: Default

Device ID: 714117775

Server:

Port: 9000

Login Retries: 3

Heartbeat Interval: 120 Seconds

Packet Receiving Timeout: 30 Seconds

Packet Transmit Retries: 3

Query SMS Interval: 24 hours

Trust phone list:

Apply Cancel

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 retries	3
Query SMS Interval	Set how long to check SMS	24
Trust phone list	Set trust cell phone list	

(6) 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
Work Mode	Set DTU as client or server	Client
DTU ID	Set ID of DTU	Blank
Multi Server	Set the IP address and Port of server to receive data.	Blank

(7) 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 notice you have a SIM card with SMS function in the router, else, please contact local mobile operator.

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)

(8) LLDP (Link Layer Discovery Protocol)

System	Network	Services	Firewall	QoS	VPN	Tools	Status
LLDP							
Enable ☒ Tx Interval 60 Seconds Apply Cancel							
Name	Description	Default					
Enable	Click to enable LLDP	Disable					
Tx Interval	Set DTU protocol	Transparent					

3.1.5 Firewall

This page is to set parameters concerned with firewall.

(1) Basic Configuration

Basic		
Default Filter Policy	Accept	
Block Anonymous WAN Requests (ping)	☐	
Filter Multicast	☒	
Defend DoS Attack	☒	
Apply Cancel		
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

Filtering								
Enable	Proto	Source	Source Port	Destination	Destination Port	Action	Log	Description
☒	ALL	0.0.0.0				Accept	☐	
Add								
Apply Cancel								
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 to 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 and then external PC can get access to all the ports of internal device behind IR700.

Attention: this function cannot help to map the admin port of IR700 (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 to 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

This page introduces the parameters set in InRouter 700's Web.

(1) IPSec Settings (For IR711/791/714/794 only)

To build an IPSec VPN Tunnel, you need first set IPSec properties in this page, then turn 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 (For IR711/791/714/794 only)

Name	Tunnel Description	Phase 1 Parameters	Phase 2 Parameters	Link Detection Parameters
Add	Show Detail Status			

5 Seconds [Stop](#)

Click "Add" and enter the configuration web:

IPSec Tunnels

Edit IPSec tunnel

Show Advanced Options



Basic Parameters

Tunnel Name	IPSec_tunnel_1
Destination Address	0.0.0.0
Startup Modes	Auto Activated
Restart WAN when failed	☒
Negotiation Mode	Main Mode
IPSec Protocol	ESP
IPSec Mode	Tunnel Mode
Tunnel Type	Subnet - Subnet
Local Subnet	192.168.2.1
Local Netmask	255.255.255.0
Remote Subnet	0.0.0.0
Remote Netmask	255.255.255.0

Phase 1 Parameters

IKE Policy	3DES-MD5-DH2
IKE Lifetime	86400 Seconds
Local ID Type	IP Address
Remote ID Type	IP Address
Authentication Type	Shared Key
Key	

Phase 2 Parameters

IPSec Policy	3DES-MD5-96
IPSec Lifetime	3600 Seconds
Perfect Forward Serecy(PFS)	None

Link Detection Parameters

DPD Time Interval	60 Seconds(0: disable)
DPD Timeout	180 Seconds
ICMP Detection Server	
ICMP Detection Local IP	
ICMP Detection Interval	60 Seconds
ICMP Detection Timeout	5 Seconds
ICMP Detection Max Retries	10

Save

Cancel

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/Triggered 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	Optional: Tunnel Mode or Transport Mode	Tunnel Mode

(Enable Advanced options)		
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 (For IR711/791/714/794 only)

System	Network	Services	Firewall	QoS	VPN	Tools	Status			
GRE Tunnels										
Enable	Name	Local virtual IP	Peer Address	Remote virtual IP	Remote Subnet	Remote Netmask	Key	NAT	Advanced Route	Description
☒	tun0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	255.255.255.0		☐		
Add										
Apply Cancel										

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 (For IR711/791/714/794 only)

L2TP Clients

Edit L2TP Tunnel

Enable	☒
Tunnel name	L2TP_TUNNEL_1
L2TP Server	
Username	
Password	
L2TP Server Name	l2tpserver
Startup Modes	Auto Activated
Authentication Type	CHAP
Enable Challenge Secrets	☒
Challenge Secrets	
Local IP Address	
Remote IP Address	
Remote Subnet	
Remote Netmask	255.255.255.0
Link Detection Interval	60 Seconds
Max Retries for Link Detection	5
Enable NAT	☐
MTU	1500
MFRU	1500
Enable Debug	☐
Expert Options (Expert Only)	

Name	Description	Default
Enable	Click Enable	Enable
Tunnel Name	Set Tunnel Name	L2TP_TUNNEL_1
L2TP Server	Set L2TP 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, Triggered by Data, Manually Activated	Auto Activated
Authentication Type	Set Authentication 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 (For IR711/791/714/794 only)

PPTP Clients

Edit PPTP Tunnel

Enable ☒

Tunnel name

PPTP Server

Username

Password

Startup Modes

Authentication Type

Local IP Address

Remote IP Address

Remote Subnet

Remote Netmask

Link Detection Interval Seconds

Max Retries for Link Detection

Enable NAT ☐

Enable MPPE ☐

Enable MPPC ☐

MTU

MRU

Enable Debug ☐

Expert Options (Expert Only)

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, Triggered by Data, Manually Activated	Auto Activated
Authentication Type	Set Authentication 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) Open VPN Tunnels (for IR791/794 only)

In the configuration WEB of 700, select “VPN”=> “Open VPN Tunnels” as below:

Click “Add” to add a new Open VPN tunnel:

Name	Description
Tunnel name	Can't be set
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
Authentication 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) Open VPN Advanced (for IR791/794 only)

This configuration page is only used for the Open VPN Server.

OpenVPN Advanced ⌵ ⌵ ⌵

Enable Client-to-Client (Server Mode Only) ☐

Client Management

Enable	Tunnel name	Username/CommonName	Password	Client IP (4th byte must be 4nt1)	Local Static Route	Remote Static Route
☒	OpenVPN_T_					

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 700 cannot produce CA.

(8) Certificate Management (for IR791/794 only)

Name	Description	Default
Enable SCEP (Simple Certificate Enrollment Protocol)	Click Enable	
Certificate Protected Key	Set Certificate Protected Key	Blank
Certificate Protected Key Confirm	Confirm Certificate Protected Key	Blank
Import/Export CA Certificate	Import or Export (CA) Certificate	Blank
Import/Export Certificate (CRL)	Import or Export Certificate (CRL)	Blank
Import/Export Public Key Certificate	Import or Export Public Key Certificate	Blank
Import/Export Private Key Certificate	Import or Export 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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Traceroute							
Host				Trace			
Maximum Hops	20						
Timeout	3 Seconds						
Protocol	UDP						
Expert Options							

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

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Link Speed Test							
				Browse		upload download	

Test link speed via unload or download

3.1.9 Status

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

(1) System Status

System	Network	Services	Firewall	QoS	VPN	Tools	Status
System							
Name	Router						
Model	IR794VZ30						
Serial Number	RZ7941005119560						
Description	www.inhand.com.cn						
Current Version	1.3.0.r1773						
Current Bootloader Version	1.1.6.r1730						
Router Time	2010-06-19 13:00:32						
PC Time	2010-06-19 13:00:48 Sync Time						
Up time	0 day, 17:21:52						
CPU Load (1 / 5 / 15 mins)	0.00 / 0.00 / 0.00						
Memory consumption	13.35MB / 1,120.00KB (8.19%)						
Total/Free							
3 Seconds Stop							

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

(2) Modem Status

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Modem							
Dialup							
Modem Type	Auto detect						
Status	unknown						
Manufacturer							
Product							
Signal Level	- (0)						
Register Status	no registered						
IMEI Code							
IMSI Code							
Network Type							
							3 Seconds

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

(3) Network Connections

Network Connections	
WAN	
MAC Address	00:18:05:00:56:10
Connection Type	Static IP
IP Address	203.86.43.190
Netmask	255.255.255.0
Gateway	203.86.43.185
DNS	
MTU	1500
Status	Connected
Connection time	0 day, 17:26:19
Dialup	
Connection Type	Disabled
IP Address	0.0.0.0
Netmask	0.0.0.0
Gateway	0.0.0.0
DNS	0.0.0.0
MTU	1500
Status	Disconnected

This page shows the network connections via WAN or LAN

(4) Route Table

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Route Table							
Destination	Netmask	Gateway	Metric	Interface			
10.8.0.2	255.255.255.255	0.0.0.0	0	tun0			
192.168.5.0	255.255.255.0	0.0.0.0	0	lan0			
192.168.3.0	255.255.255.0	10.8.0.2	0	tun0			
203.86.43.0	255.255.255.0	0.0.0.0	0	wan0			
10.8.0.0	255.255.255.0	10.8.0.2	0	tun0			
192.168.9.0	255.255.255.0	10.8.0.2	0	tun0			
127.0.0.0	255.0.0.0	0.0.0.0	0	lo			
default	0.0.0.0	203.86.43.185	0	wan0			
							Manual Refresh
							Refresh

This page shows the route table of IR700.

(5) Device List

System	Network	Services	Firewall	QoS	VPN	Tools	Status
Device List							 
Interface	MAC Address	IP Address	Host				Lease
wan0	00:16:46:B7:CD:FF	203.86.43.185					

This page shows the devices linked with IR700.

(6) Log

Log			
Level	Time	Module	Content
			Too many logs, old logs are not displayed. Please download log file to check more logs!
debug	Jun 19 13:06:49	InAgent	IMSI:0123456789ABCDE
info	Jun 19 13:06:49	InAgent	Firmware Version(1.3.0.r1773):Entity Config Timestamp(a-1275632533021):Sysconfig Timestamp(0000000000000000)
info	Jun 19 13:06:59	InAgent	Try to login(9th/10)
info	Jun 19 13:06:59	InAgent	nvrnm sysconf_timestamp not found!
debug	Jun 19 13:06:59	InAgent	IMSI:0123456789ABCDE
info	Jun 19 13:06:59	InAgent	Firmware Version(1.3.0.r1773):Entity Config Timestamp(a-1275632533021):Sysconfig Timestamp(0000000000000000)
info	Jun 19 13:07:09	InAgent	Try to login(10th/10)
info	Jun 19 13:07:09	InAgent	nvrnm sysconf_timestamp not found!
debug	Jun 19 13:07:09	InAgent	IMSI:0123456789ABCDE
info	Jun 19 13:07:09	InAgent	Firmware Version(1.3.0.r1773):Entity Config Timestamp(a-1275632533021):Sysconfig Timestamp(0000000000000000)
info	Jun 19 13:07:19	InAgent	Try to connect OVPD AP(10.8.0.6:9000)
info	Jun 19 13:07:19	InAgent	Try to login(1th/10)
info	Jun 19 13:07:19	InAgent	nvrnm sysconf_timestamp not found!
debug	Jun 19 13:07:19	InAgent	IMSI:0123456789ABCDE
info	Jun 19 13:07:19	InAgent	Firmware Version(1.3.0.r1773):Entity Config Timestamp(a-1275632533021):Sysconfig Timestamp(0000000000000000)
info	Jun 19 13:07:29	InAgent	Try to login(2th/10)
info	Jun 19 13:07:29	InAgent	nvrnm sysconf_timestamp not found!
debug	Jun 19 13:07:29	InAgent	IMSI:0123456789ABCDE
info	Jun 19 13:07:29	InAgent	Firmware Version(1.3.0.r1773):Entity Config Timestamp(a-1275632533021):Sysconfig Timestamp(0000000000000000)
Clear Log Download Log File Download System Diagnosing Data			

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

For some situation when there're some problems that can't be diagnosed at the moment, you'll be asked to provide the diagnose log to InHand engineers, you can click "Download System Diagnosing Data" then send the diagnose log to us.

3.2 Support

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

support@inhandnetworks.com.



Copyright © 2010 InHand Networks, All rights reserved.

Tel: 86-10-64391099-8022

Fax: 86-10-64399872

Address: Wangjing Science Park, Road Lizezhonger, Chaoyang District, Beijing, P. R. C, 100102

Website: <http://www.inhandnetworks.com>

Email: info@inhandnetworks.com

Subject to alterations without notice.