

User Manual

FT412

Catalogue

Introduction	4
1.1 Overview	4
1.2 Features	5
Quick start guide	6
2.1 Product Display	7
2.4 LED indicators	7
2.5 Accessories	8
Preparation	9
3.1 Out of the box	9
3.2 Installation and wiring	9
3.2.1 SIM card installation	9
3.2.2 Antenna installation	10
3.3 Log in the Web UI of router	10
3.3.1 Computer network configuration	10
3.3.2 Login to device	11
Network Configuration	13
4.1 Network Configuration	13
4.1.1 Ethernet WWAN Configuration	13
4.1.2 WAN	15
4.1.3 Break the line and restart	16
4.1.4 Break line detection	17
4.1.2 LAN Configuration	17
4.1.3 DHCP Server	18
1、DHCP Server Configuration	18
2、DHCP List of clients	18
3、DHCP Address Bind	19
4.1.4 DTU	19
1、DTU server	19
2、DTU Client	20
4.1.5 Network detection tool	21
4.2 VPN	22
4.2.1 PPTP settings	22
PPTP Server	22
4.2.2 L2TP	24
4.2.3 IPSEC	25
1、Connect Status and Control	25
2、New IPSEC security policy	26
3、Add the IKE security policies	26
4.2.4 GRE	27
4.3 Firewall settings	28
4.3.1 Port mapping	28

4.3.2 DMZ settings	29
4.4 System Settings	30
4.4.1 Management Settings	30
1、 Password setting	30
2、 Language settings	30
4.4.2 Configuration management	31
4.4.3 Firmware	31
4.4.4 Reboot	31
5 FCC Warning:	32

1.1 Overview

FT412 series routing provides one RS232 or RS485 serial port, four 100 million Ethernet LAN, one 100 million Ethernet WAN port to connect serial devices, Ethernet devices enabling transparent data transmission and routing functions.

The product has the advantages of rapid deployment and easy management, advanced software features and a fully industrial hardware design platform, enabling enterprises to quickly build large-scale industrial equipment networks with minimal investment, providing multi-service services including data, voice and video. Especially suitable for large-scale machine networking, such as self-help selling machine, bank ATM, multimedia advertising equipment, industrial automation equipment, intelligent medical equipment, robots, field machinery, oil and gas exploration equipment, digital production equipment and other machine networking and information construction, its excellent hardware performance, easy to deploy and perfect remote management function .

1.2 Features

Industrial-grade application design

- Adopt the industrial communication module
- With a high-performance 32-bit communication processor
- Support low power mode, including sleep mode, timing up and down mode and timing switch mode (special version only)
- With metal case, protection class IP30. The metal shell and the system are safely isolated, especially suitable for industrial control field applications
- Design of wide voltage input: 9~36V

Stable and reliable

- Double watchdog design to ensure the stability of the system
- Adopt a complete anti-drop mechanism to ensure that the data terminal is always online.
- The Ethernet interface is built-in 1.5KV electromagnetic isolation protection
- The RS232 / RS485 interface has a built-in 1.5KV ESD protection
- The SIM / UIM interface has a built-in 1.5KV ESD protection
- Power-interface built-in reverse voltage protection and overvoltage protection
- Lightning protection of antenna interface (optional)

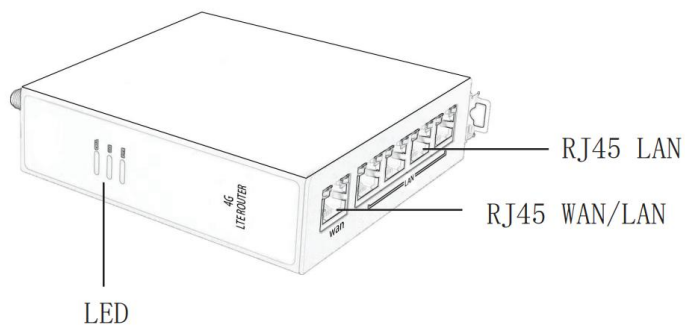
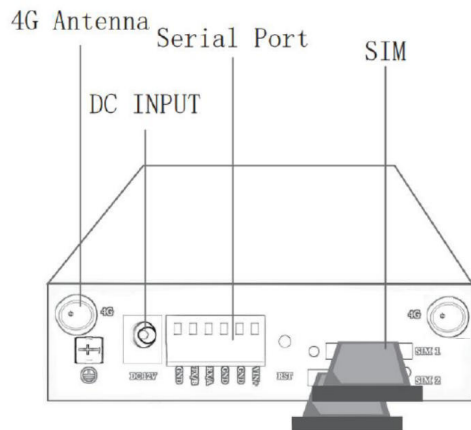
Standard easy to use

- Standard RS232 / RS485, Ethernet interfaces are provided, connecting directly to serial port devices, Ethernet devices devices
- Provide standard limited WAN port (supporting standard PPPOE protocol) to connect to ADSL devices directly
- Intelligent data terminal, power on can enter the data transmission state
- Provide powerful central management software to facilitate equipment management (optional)
- Easy to use, flexible, a variety of working mode selection
- Convenient system configuration and maintenance interface (including local, remote WEB and platform management)

powerful

- Various WAN connection modes are supported, including static IP, DHCP, L 2 TP, PPTP, PPP OE, 3G / HSPA / 4G.
- Support for mobile network and wired WAN dual-link intelligent switching backup function (optional)
- Support for VPN client (PPTP / L 2 TP / IPSEC / GRE)
- Support for remote management, SYSLOG / SNMP / TELNET / HTTP and other functions
- Support for local and remote online upgrades, and import and export profiles
- support NTP
- Support for the APN / VPDN
- Support multi-channel DHCP Server and DHCP Client, DHCP bundled MAC address, DDNS, firewall, NAT, DMZ host traffic statistics and other functions
- Support for TCP / IP, UDP, FTP (optional), HTTP and other network protocols
- Support for SNMP V1.V2.V3

2.1 Product Display



2.4 LED indicators

name	state	description
System lamp (SYS)	twinkle	It indicates that the power supply is normal and it is starting
	Often bright	Note that the system is running abnormally
	Often bright	System operation
Power lamp (PWR)	Often bright	The equipment is in normal power supply
	extinct	The equipment has abnormal power supply
Network Lamp (LINK)	Often bright	Indicates that the router has successfully dialed up to the network
	twinkle	Indicates that the router is currently connecting to a dial-up connection

2.5 Accessories

Accessories name	quantity	remarks
FT412	1	
4G antenna	1	
Power adapter	1	
Quick start guide	1	
Industrial guide rail buckle	1	

Preparation

3.1 Out of the box

After the whole package of equipment arrives at the site, it is necessary to open the box and check whether the accessories are complete according to the product accessories list. Please keep the packing materials well after opening the box, for later use.

3.2 Installation and wiring

3.2.1 SIM card installation

During the normal installation process, the product needs to install SIM in the SIM card slot in the SIM slot on the right side of the front panel.

Step 1 Gently press the yellow button on the SIM holder with a sharp object to pop the holder:



Step 2 insert the SIM metal face up and into the holder with the missing end facing the outside. Then push the card holder into the card slot:



3.2.2 Antenna installation

Rotate the antenna into the antenna connector accordingly.

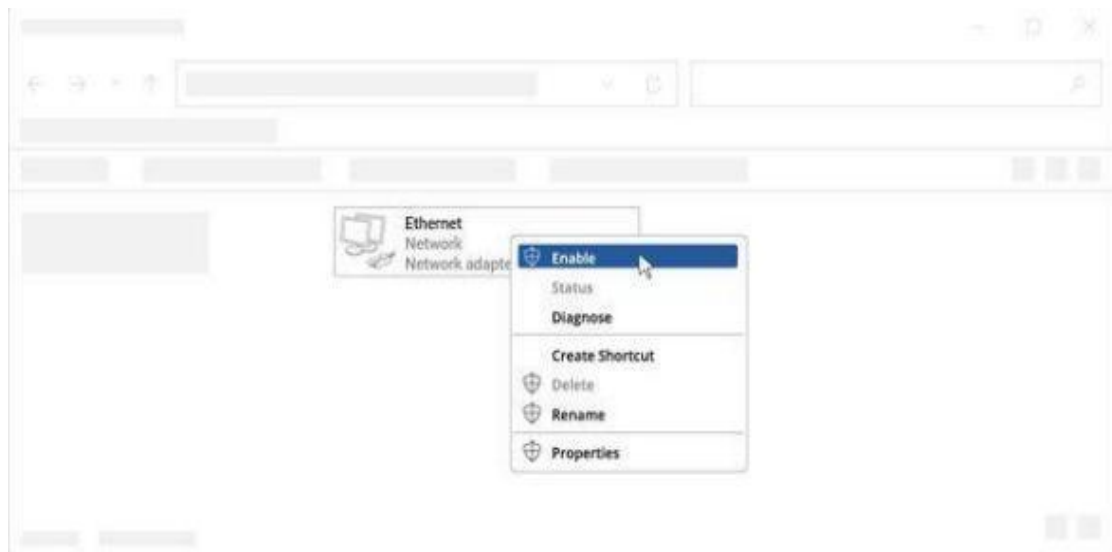
The external antenna should be installed vertically always on a site with a good signal.

3.3 Log in the Web UI of router

This product has built-in WEB interface, management and debugging tools. Users should configure relevant parameters before using the router, and they can flexibly change the relevant parameters, software upgrade and conduct simple tests.

3.3.1 Computer network configuration

1、 Ensure the Wireless network connection is Enabled. Go to Start — Control Panel — Network and Internet — Network and Sharing Center. Click on the Change adapter settings in the left panel, then right-click on Wireless Network Adapter, and select Enable.

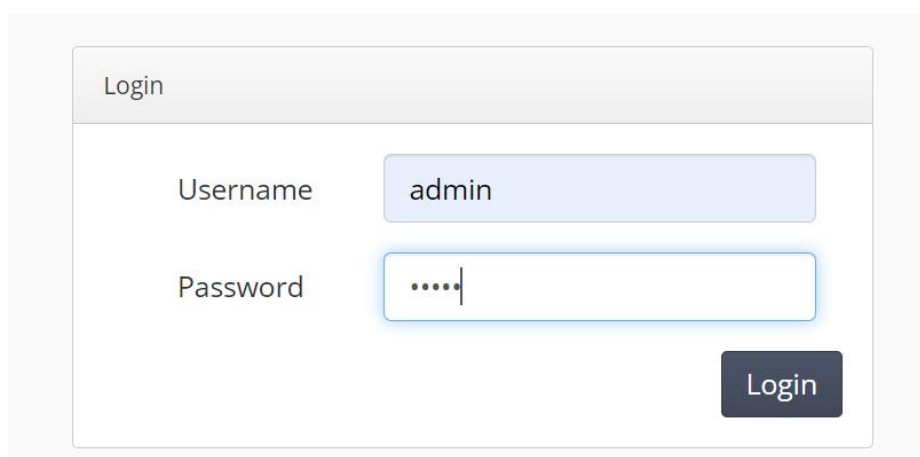


2、 Check if IP and DNS are obtained automatically. Right-click on Wireless Network Adapter and select Properties. Then select Internet Protocol Version 4 and click Properties.



3.3.2 Login to device

- 1、 Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.10.1, and press Enter on your keyboard.
- 2、 When the first login, please enter the default user name: admin, password: iradm



- 1、 After you login the WebUI, you can view system information and perform configuration on the router.

FT205L

- Status ^
- System
- Internet Status
- Network v
- VPN v
- Firewall v
- System v
- Logout

Home / System

Device Information

Device Model	FT205L
System Version	3.8.4 (240403111216)
RunTime	0Day0Hour24Minutes
Device SN	KO0C010W0004

LAN Status

IP Address	192.168.10.1
IPv6 Address	fd4c:1234:abcd::1/48
Netmask	255.255.255.0
MAC Address	BC:14:EF:BB:A8:FC
DHCP Client Count	0

Internet access traffic analysis

Interface WWAN	Transmit:129.6 KiB	Receive:0.0 B
Interface WAN	Transmit:123.4 KiB	Receive:0.0 B
Interface LAN	Transmit:162.9 KiB	Receive:208.5 KiB

Network Configuration

4.1 Network Configuration

This section explains how to connect FT412 to network via WAN connection or cellular.

4.1.1 Ethernet WWAN Configuration

1、 The default system is 4G wireless Internet access mode, insert 4G service card, the router will automatically identify the main card (SIM1) for dial-up Internet access.

WWAN	Wired WAN	Disconnect Reboot	WWAN ICMP Check
Link Type	Auto		
REG	0		
APN			
Auth Type	None		
Username			
Password			
PIN Code			
Dial Number			
LCP echo failure threshold	10		
LCP echo interval	5		
MTU	1490		
DNS Server1			
DNS Server2			
Dial Time	5		
Dial Interval	1		
Main SIM	SIM1 13		
Backup SIM1	SIM2 13		
AutoSwitch	<input type="checkbox"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

2、 If you need to realize the dual card switching function, please install the two 4G charge cards in SIM1 and SIM2 respectively. After you configure the main card and standby card, check "Auto cut card" and save it.

WWAN Wired WAN Disconnect Reboot WWAN ICMP Check

Link Type	Auto
REG	0
APN	
Auth Type	None
Username	
Password	
PIN Code	
Dial Number	
LCP echo failure threshold	10
LCP echo interval	5
MTU	1490
DNS Server1	
DNS Server2	
Dial Time	5
Dial Interval	1
Main SIM	SIM1 13
Backup SIM1	SIM2 13
AutoSwitch	<input checked="" type="checkbox"/>

Save Cancel

3、 If you are using a 4G private network card, please fill in the corresponding parameters through the relevant APN information provided by the operator and save it.

WWAN Wired WAN Disconnect Reboot WWAN ICMP Check

Link Type Auto

REG 0

APN shenzhen123456789@gd.com

Auth Type CHAP

Username username

Password password

PIN Code

Dial Number

LCP echo failure threshold 10

LCP echo interval 5

MTU 1490

DNS Server1

DNS Server2

Dial Time 5

Dial Interval 1

Main SIM SIM1 13

Backup SIM1 SIM2 13

AutoSwitch

Save Cancel

4.1.2 WAN

Wired connection WAN includes: DHCP client, static IP, PPPOE:
PPPOE parameter configuration, as shown in the figure below:

WWAN Wired WAN Disconnect Reboot WWAN ICMP Check

Link Type PPPOE

Username 075501234567@gd

Password password

Service Name Service Name

Max Demand(Minute)

MAC Address BC:14:EF:BB:A8:FB

MTU 1500

Save Cancel

Configure according to the example of the above figure, input the correct broadband dial account and password, and click "Save".

Static address parameter configuration, as shown below:

[WWAN](#) | [Wired WAN](#) | [Disconnect Reboot](#) | [WWAN ICMP Check](#)

Link Type	Static IP
IP Address	192.168.15.100
Netmask	255.255.255.0
Gateway	192.168.15.1
DNS Server1	114.114.114.114
DNS Server2	8.8.8.8
MAC Address	BC:14:EF:BB:A8:FB
MTU	1500

Configure according to the example above, and click "Save".

DHCP client parameter configuration, as shown below:

[WWAN](#) | [Wired WAN](#) | [Disconnect Reboot](#) | [WWAN ICMP Check](#)

Link Type	DHCP Auto
MAC Address	BC:14:EF:BB:A8:FB
MTU	1500

Configure according to the example above, and click "Save".

4.1.3 Break the line and restart

[WWAN](#) | [Wired WAN](#) | [Disconnect Reboot](#) | [WWAN ICMP Check](#)

Enable Reboot When Disconnect	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Period	60 Senond
Interval	600 Senond
IP Address1	114.114.114.114
IP Address2	

After the disconnection restart function is enabled, the system will automatically perform PING operation on the IP address in the settings.

The detection time is the cumulative packet loss time; the detection interval is how long for the PING function once; the IP address is the target address of the system for the PING function. If the PING pass IP address fails during the detection time period, the system will automatically restart the operation.

4.1.4 Break line detection

WWAN Wired WAN Disconnect Reboot WWAN ICMP Check

Enable WWAN Disconnect Check Enabled Disabled

Interval Minutes

Protect Sleep Minutes

Usual Using Address WWAN DNS WWAN Gateway

Custom domain name ip address

Custom domain name ip addressV6

Save Cancel

After the disconnection detection function is enabled, the system will automatically operate the PING on the IP address in the settings.

The detection time is the cumulative packet loss time; the detection interval is how long for the PING function once; the IP address is the target address of the system for the PING function. If the PING IP address is failed during the detection time limit, the system will automatically re-dial the operation.

4.1.2 LAN Configuration

Local area network (Local Area Network, LAN) is a group of computers connected by multiple computers in a certain area. Routers can assign IP addresses to devices within the LAN, enabling them to communicate with each other and access the Internet.

IP Address	<input type="text" value="192.168.10.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
MTU	<input type="text" value="1500"/>
MAC Address	<input type="text" value="BC:14:EF:BB:A8:FC"/>

4.1.3 DHCP Server

DHCP (Dynamic Host Configuration Protocol, Dynamic Host Configuration Protocol) is a LAN network protocol using UDP protocol and has two main uses: automatically assigning IP addresses to the internal network or network service providers, and to users or internal network administrators as a means of central management of all computers.

1、DHCP Server Configuration

Used to set the DHCP server open or close, and DHCP gateway, starting address, lease duration, etc., generally open by default.

DHCP Server Setting DHCP Client List DHCP Bind

DHCP Service	<input checked="" type="radio"/> Enabled <input type="radio"/> Disabled
Start Address	<input type="text" value="192.168.10.100"/>
DHCP Max IP	<input type="text" value="150"/>
Netmask	<input type="text" value="255.255.255.0"/>
Gateway	<input type="text" value="192.168.10.1"/>
DNS Server1	<input type="text"/>
DNS Server2	<input type="text"/>
DHCP Lease Time	<input type="text" value="720"/> Minutes

2、DHCP List of clients

Displays the device currently using the assigned address.

DHCP服务器设置			
DHCP客户端列表			DHCP地址绑定
客户端信息			
IP地址	MAC地址	主机名	剩余租期(秒)
192.168.199.227	74:e5:0b:37:a7:f9	wangzhenjiang-PC 01:74:e5:0b:37:a7:f9	36074秒
192.168.199.171	14:75:90:f8:81:47	jane-THINK 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47	36815秒
192.168.199.136	5c:8d:4e:ca:b2:4c	iPhone-2 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c	36158秒
192.168.199.145	44:74:6c:ae:a7:3f	android-b75bd5f004c534b 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f	25465秒
192.168.199.186	68:17:29:a5:e2:22	think 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22	29738秒
192.168.199.105	54:ea:a8:09:24:1f	zphone 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f	29660秒
192.168.199.187	fc:3d:93:1b:ab:83	android-3dd1505bcdca9e 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f*	43184秒
192.168.199.133	48:5b:39:49:9e:cf	Flyinkr 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f* 01:48:5b:39:49:9e:cf	33228秒
192.168.199.150	20:08:ed:40:cc:ba	android-612262cb48025f1f 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f* 01:48:5b:39:49:9e:cf*	34310秒
192.168.199.173	ec:55:f9:c3:ee:cf	2015-0130-0036 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f* 01:48:5b:39:49:9e:cf* 01:ec:55:f9:c3:ee:cf	32298秒
192.168.199.148	ac:17:f3:cb:44:86	Mi2S-xiaomishouji 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f* 01:48:5b:39:49:9e:cf* 01:ec:55:f9:c3:ee:cf*	26817秒
192.168.199.226	74:e5:0b:37:a7:f8	* 01:74:e5:0b:37:a7:f9 01:14:75:90:f8:81:47 01:5c:8d:4e:ca:b2:4c 01:44:74:6c:ae:a7:3f 01:68:17:29:a5:e2:22 01:54:ea:a8:09:24:1f* 01:48:5b:39:49:9e:cf* 01:ec:55:f9:c3:ee:cf* 01:74:e5:0b:37:a7:f8	29425秒

3、DHCP Address Bind

Specify the IP address according on its MAC address.

DHCP Server Setting		DHCP Client List	DHCP Bind
Add DHCP Bind			
Host Name	<input type="text" value="test"/>		
IP Address	<input type="text" value="192.168.10.100"/>		
MAC Address	<input type="text" value="00:11:22:33:44:55"/>		
<input type="button" value="Save"/> <input type="button" value="Cancel"/>			

4.1.4 DTU

The DTU setting is closed by default, and it is divided into two modes: server and client.

DTU Type

Disabled

Disabled

Server

Client

DTU tty Transmit To Mobile tty

SeaNet Cloud

1、DTU server

Description of the Server Mode settings:

DTU Type	<input type="text" value="Server"/>
Protocol	<input type="text" value="TCP"/>
Port	<input type="text" value="9900"/>
Baudrate	<input type="text" value="115200"/>
Data bits	<input type="text" value="8"/>
Stop bits	<input type="text" value="1"/>
Parity	<input type="text" value="None"/>
Flow Control	<input type="text" value="None"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

DTU type: Server mode

Agreement: Support for TCP, UDP.

Port: The port number used by the server.

Baud rate: Baud rate of the serial port, supported by: 9600,19200,38400,57600,115200.

Data bit: Serial port data bit setting, supported by: 8,7,6,5.

Stop bit: serial port stop bit setting, support: 1,2.

Check bit: serial port check bit setting, support: None, Odd, Event, Mark, Space.

Flow control: serial port flow control options, support: None, RTS / CTS, XON / XOFF.

2、 DTU Client

Description of the client-side mode setting:

DTU Type	Client
Protocol	TCP
IP Address	47.115.208.32
Port	9900
IP Address2	47.115.208.32
Port2	9901
Baudrate	115200
Data bits	8
Stop bits	1
Parity	None
Flow Control	None
Heartbeat Interval	60
Register Package	String
Content	123
Heartbeat Package	String
Content	abc

Agreement: Support for TCP, UDP.

IP address: the IP address or domain name of the server.

Port: The port number used by the server.

Baud rate: Baud rate of the serial port, supported by: 9600,19200,38400,57600,115200.

Data bit: Serial port data bit setting, supported by: 8,7,6,5.

Stop bit: serial port stop bit setting, support: 1,2.

Check bit: serial port check bit setting, support: None, Odd, Event, Mark, Space.

Flow control: serial port flow control options, support: None, RTS / CTS, XON / XOFF.

Heartbeat interval: The heartbeat packet sends the heartbeat content to the server according to the time set by the heartbeat interval.

Registration package: The DTU is sent once when it is connected to the server.

Heartbeat packet: When there is no data sent by the serial port, the data will be sent to the server regularly to keep the link smooth.

4.1.5 Network detection tool

Cooperate with the tester to monitor the line status of the whole network in real time, and take corresponding measures.

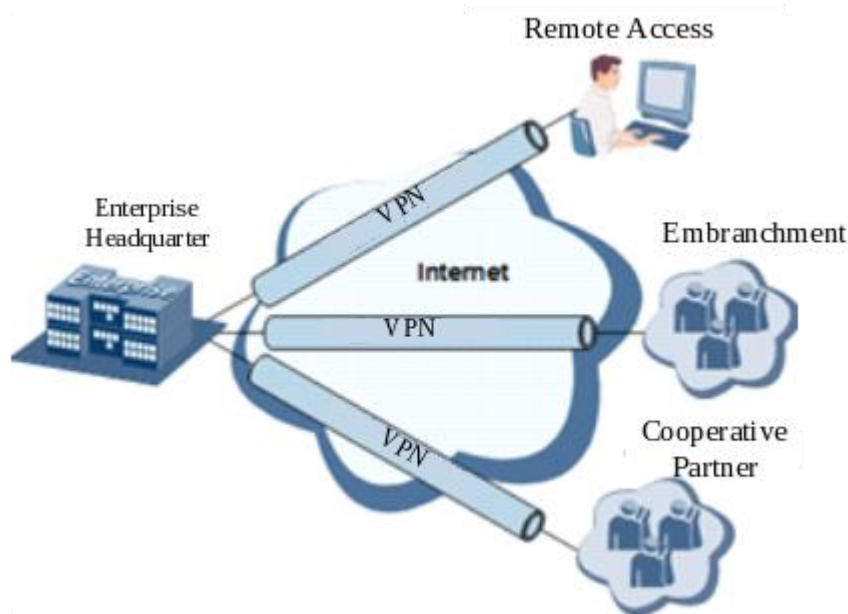
PING TRACEROUTE

IP or Domain name	<input type="text" value="114.114.114.114"/>
Source internet interface	<input type="text" value="Auto"/>
Times	<input type="text" value="10"/>

```
PING 114.114.114.114 (114.114.114.114): 56 data bytes
```

4.2 VPN

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



4.2.1 PPTP settings

PPTP (Point to Point Tunneling Protocol), namely, the point-to-point tunneling protocol. This protocol is a new enhanced security protocol developed on the basis of PPP protocol, supporting multi-protocol virtual private network (VPN), which can be enhanced by password authentication protocol (PAP), scalable authentication protocol (EAP) and other methods. It enables remote users to securely access enterprise networks by dialing into the ISP, through direct connection to Internet or other networks.

PPTP Server

Build the PPTP server

PPTP Server PPTPUser

PPTPServer Enabled Disabled

Local IP 192.168.0.1

Remote IP 192.168.0.10-30

Save Cancel

As shown above: Open the PPTP server button and configure the PPTP virtual IP address field:

Username	<input type="text" value="pptptest"/>
Password	<input type="password" value="password"/>
Remote Subnet	<input type="text" value="192.168.10.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
IP Address	<input type="text" value="192.168.10.10"/>

User name: the name of the new user

Password: Password for the new user

Remote subnet: the local gateway IP of the PPTP client

Subnet mask: Subnet mask of the PPTP client

IP address: Virtual IP address assigned to the changed user

PPTP Client

In the figure below, click-new PPTP client in PPTP client to add a new PPTP connection.

PPTP Client

Client Information					
Name	Server Address	Username	Status	IP Address	Action

Click to see the following setting options:

PPTP Client

PPTP Client Enabled Disabled

Name

Server Address

Username

Password

Remote Subnet

Netmask

Local End IP

Remote End IP

Refuse

<input checked="" type="checkbox"/> refuse-pap	<input checked="" type="checkbox"/> refuse-chap
<input checked="" type="checkbox"/> refuse-eap	<input checked="" type="checkbox"/> refuse-mschap

MPPE Enabled Disabled

Default Route Enabled Disabled

MTU

Name: The name of this client connection that can be customized.

Server address: Fill in the address of the PPTP server here, which can be the domain name or the IP address.

Username: User name to login PPTP Server

Password: Password to log into PPTP Server.

Remote Subnet: The network of the remote PPTP server Remote

Net Mask: Subnet mask of remote PPTP server

MPPE Encryption: Enable or disable Microsoft Point-to-Point Encryption。

MTU : Maximum Transmission Unit

4.2.2 L2TP

The L 2 TP is an industry-standard Internet tunnel protocol, functioning roughly similar to the PPTP protocol, such as enabling the same encryption of network data streams. However, there are differences, such as PPTP requires IP network; L 2 TP requires packet point-to-point connection; PPTP uses single tunnel; L 2 TP uses multiple tunnel; L 2 TP provides Baotou compression and tunnel verification, while PPTP does not support.

Create a new L 2 TP client connection

In the figure below, click in the L 2 TP client-a new L 2 TP client to add a new L 2 TP connection.



Click to see the following setting options:

L2TP Client Enabled Disabled

Name

Server Address

Username

Password

Local End IP

Netmask

Default Route Enabled Disabled

MTU

Name: The name of this client connection that can be customized.

Server address: Fill in the address of the L2TP server here, which can be the domain name or the IP address.

Username: User name to login L2TP Server

Password: Password to log into L2TP Server.

Local end IP: The network of the remote L2TP server Remote

Net Mask: Subnet mask of remote L2TP server

MTU : Maximum Transmission Unit

4.2.3 IPSEC

The IPsec protocol works on the third layer of the OSI model, making it suitable to protect TCP or UDP-based protocols when used alone (such as the socket sublayer (SSL) cannot protect the UDP layer). This means that the IPsec protocol must deal with reliability and fragmentation issues compared to the transport layer or higher level, which also increases its complexity and processing overhead. In contrast, SSL / TLS relies on a higher level TCP (layer 4 of OSI) to manage reliability and sharding.

1、 Connect Status and Control

Existing IPSEC connection status information is displayed here. In the figure below, click on the new IPSEC connection in the IPSEC list to add a new IPSEC connection.

Name	Mode	Remote Address	Remote Subnet	Status	Comment	Action
------	------	----------------	---------------	--------	---------	--------

Click to see the following setting options:

Name	test
Mode	<input checked="" type="radio"/> Main <input type="radio"/> Aggressive
IPSEC Type	Net To Net
Work Mode	Add
Local ID	
Local Subnet	192.168.10.0/24
Remote Address	27.191.236.69
Remote ID	
Remote Subnet	10.0.1.0/24
IKE Version	IKEv1
IKE Policy	2
IPSEC Policy	1
Verification Type	IKE-PSK
PSK	8239904
DPD Action	none
ICMP ID	27.191.236.69
Comment	

Name: IKE policy name, use plain English or English numbers.
 Mode: Optional main mode, savage mode.
 IPSEC networking type: support network to network mode.
 Working mode: Optionally not enabled, active connection, automatic discovery, waiting for the connection.
 Local ID: IPSEC ID may not be set or set to pure English custom name.
 Local subnet: the local subnet address.
 Distal address: the IP address or domain name of the opposite-end IPSEC.
 Distal ID: the IPSEC ID name of the opposite end.
 Distal subnet: the opposite-end subnet address.
 IKE version: optional version IKEv 1 or IKEv 2.
 The IKE security policy: The IKE security policy needs to be added to the IKE security policy first.
 The IPSEC security policy: The IPSEC security policy needs to be added to the IPSEC security policy first.
 Tunnel Certification: Optional Mode IKE-PSK, IKE-XAUTH-PSK, NEVER.
 PSK: the PSK key for the IPSEC connection.
 DPD mode: optional none, clean, hold, restart.
 Note: Comments about this link.

2、New IPSEC security policy

In the figure below, click on the new IPSEC security policy in the IPSEC Security Policy to add a new IPSEC security policy.



Click to see the following setting options:

Name

Protocol

AH Verification Algorithms

Name: IKE policy name, use plain English or English numbers.
 Agreement: Optional AH, ESP.
 AH validation algorithm: optional MD5, SHA 1.

3、Add the IKE security policies

In the figure below, click on the-new IKE security policy in the IKE security policy to add a new IKE security policy.

IPSEC Policy IPSEC Policy IKE Policy

Add IKE Policy

IKE Policy					
Name	Verification Algorithms	Encryption Algorithm	DH Group	IKE Life time	Action

Click to see the following setting options:

Name

Encryption Algorithm

Verification Algorithms

DH Group

IKE Life time Hour

Name: IKE policy name, use plain English or English numbers.

Encryption algorithm: optional DES, 3 DES, AES128, AES192, AES256.

Validation algorithm: select SHA 1, MD5.

DH group: select DH 1, DH 2, DH 5, DH 14, DH 15, DH 16, DH 17, DH 18.

IKE survival cycle: a minimum value of 1 hour.

4.2.4 GRE

GRE (Generic Routing Encapsulation), the general routing encapsulation protocol, is the encapsulation of some network layer protocols (such as IP and IPX), enabling these encapsulated datagram to be transmitted in another network layer protocol (such as IP). GRE is the third layer tunnel protocol of VPN (Virtual Private Network), where a technology called Tunnel (tunnel) is used between the protocol layers.

Existing GRE connection status information is displayed here.

In the figure below, click on the-new GRE connection in the GRE to add a new GRE tunnel connection.

Add GRE Link

GRE						
Name	Tunnel Address	Remote Address	Remote Subnet/Mask	Status	Action	

Click to see the following setting options:

GRE Link Enabled Disabled

Name

Tunnel Address

Remote Address

Remote Subnet/Mask

Password

MTU

TTL

Name: GRE tunnel name

Tunnel address: the IP address of the GRE tunnel.

Distal address: the IP address of the distal GRE connection.

Distal subnet / mask: the subnet and mask of the distal GRE.

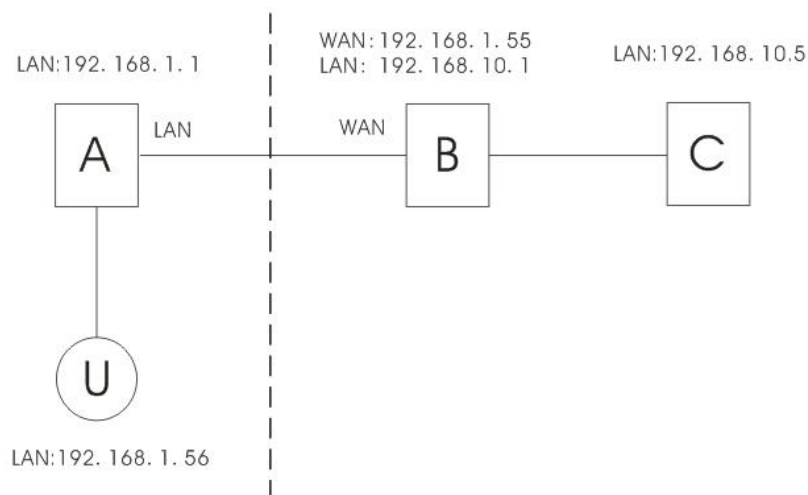
Password: the connection password for the GRE tunnel

The MTU value: the MTU value of the GRE tunnel.

TTL: the TTL cycle of the GRE tunnel.

4.3 Firewall settings

4.3.1 Port mapping



As shown in the figure: there are three routers: A, B (IR 1 equipment) and C, and U is the user end. A and U are in the same LAN, the IP address of A is 192.168.1.1, and the IP address of U is 192.168.1.56. B and C are in another LAN, IP addresses are 192.168.10.1, 192.168.10.5. The WAN port of router B is connected to the LAN port of

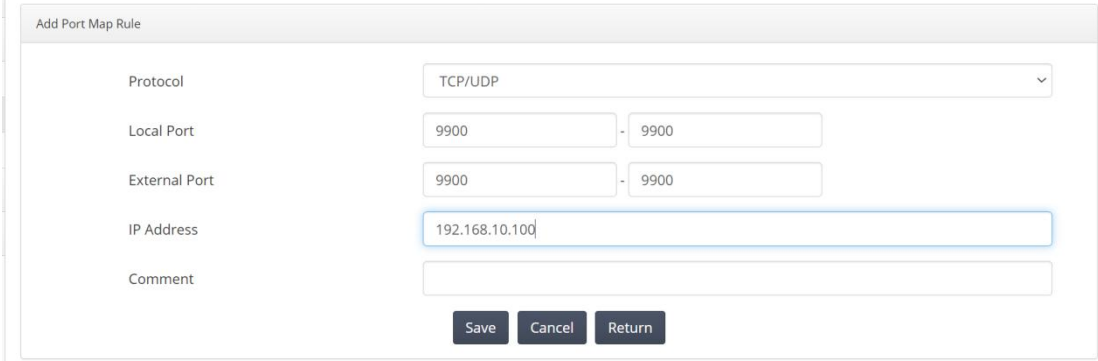
router A, and the WAN address is 192.168.1.55.

The virtual server is defined as: user U accessing router B through A across the network, and router B automatically transfers the service request to the server (router) C.

Here, the connection mode and setting of B are very important. The connection mode is required as follows:

1. B Connect to the external network with the WAN port.
- 2, B, connect C with the LAN port.

Setting mode: Enter the setting interface of router B-firewall-commodity mapping, and the setting parameters are as follows:



The screenshot shows a web-based configuration window titled "Add Port Map Rule". It contains the following fields and controls:

- Protocol:** A dropdown menu set to "TCP/UDP".
- Local Port:** Two input boxes, both containing "9900", separated by a hyphen.
- External Port:** Two input boxes, both containing "9900", separated by a hyphen.
- IP Address:** A text input box containing "192.168.10.100".
- Comment:** An empty text input box.
- Buttons:** Three buttons labeled "Save", "Cancel", and "Return" are located at the bottom right of the form.

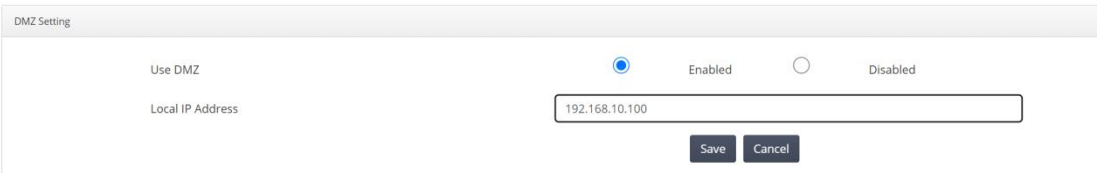
Among them, the external port can be filled in at will, and the internal port should be consistent with the corresponding service port of the server (router) C (port 80 is the WEB configuration interface port of the router C).

Fill in according to the above content, and save it.

Now, we connect to router A through the client U, and input: `http://192.168.10.100:9900` in the address bar, then the browser directly enters the Settings interface of router C.

4.3.2 DMZ settings

DMZ is short for the English word "demilitarized zone", and the Chinese name is "isolation zone", also called "demilitarized zone". It is a buffer between the non-secure system and the security system to solve the problem that the external network access users cannot access the internal network server after installing the firewall. The buffer is located in a small network area between the enterprise internal network and the external network. In this small network area, you can place some necessary public server facilities, such as enterprise Web server, FTP server, and forum. On the other hand, through such a DMZ region, the internal network is more effectively protected. Because this kind of network deployment, compared to the general firewall scheme, for the attacker from the external network and another level.



The screenshot shows a web-based configuration window titled "DMZ Setting". It contains the following fields and controls:

- Use DMZ:** A radio button selection with "Enabled" selected and "Disabled" unselected.
- Local IP Address:** A text input box containing "192.168.10.100".
- Buttons:** Two buttons labeled "Save" and "Cancel" are located at the bottom right of the form.

4.4 System Settings

4.4.1 Management Settings

Used to manage the router interface language and password security.

1、 Password setting

Manage the router login password, save and restart the effective.

The screenshot shows the 'Password Setting' page. It has three tabs: 'Password Setting' (selected), 'Language Setting', and 'Web Port Setting'. There are three input fields for passwords: 'Current Password', 'New Password', and 'Confirm Password'. Each field contains a series of dots representing masked text. Below the fields are two buttons: 'Save' and 'Cancel'.

2、 Language settings

Language : Set up the Router page shows the type of language, including simplified Chinese and English.

The screenshot shows the 'Language Setting' page. On the left is a navigation menu with items: Status, Network, Wireless, VPN, Route, Firewall, System, Admin, Config, Upgrade Firmware, Reboot, and Logout. The main content area has three tabs: 'Password Setting', 'Language Setting' (selected), and 'Web Port Setting'. Below the tabs is a 'Choose Language' label and a dropdown menu showing 'English'. A 'Save' button is located below the dropdown. At the bottom of the page, there is a copyright notice: '© 2015 - Industry Cellular&Wireless Router (SL-IR1)'.

4.4.2 Configuration management

You can save the current configuration information locally, or import previous backup files locally.

[Home](#) /

Backup Config

Download Backup

Factory Reset

Confirm

Import Config

选择文件 未选择任何文件

Confirm

4.4.3 Firmware

Firmware Upgrade : New firmware versions are posted at [www..com](#) and can be downloaded. If the Router is not experiencing difficulties, then there is no need to download amore recent firmware version, unless that version has a new feature that you want to use.

[Home](#) / Upgrade

Device Model

FT205L

System Version

3.8.4 240403111216

Upload Progress



Upgrade Firmware

选择文件 未选择任何文件

Factory Reset

Confirm

4.4.4 Reboot

This item can set the timing restart of the device.

Reboot Now

[Reboot Timer](#)

Reboot Now

Confirm

You can schedule regular reboots for the router: Regularly after xxx Minutes.

Reboot Now Reboot Timer

Enabled Reboot Timer Enabled Disabled

Reboot Timer Interval Minutes

Save Cancel

5 FCC Warning:

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Caution: Any changes or modifications to this device not explicitly approved by manufacturer could void your authority to operate this 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.

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 and your body.