

F-DPU110 Distributed Processing Unit User Manual	Document Version	Page
	V1.0.0	
	Product Name: : F-DPU110	Totall: 94

F-DPU110 Distributed Processing Unit User Manual

The user manual is suitable for the following model:

Model	Product Type



Xiamen Four-Faith Communication Technology Co., Ltd.

Add: 11th Floor, A-06 Area, No. 370, Chengyi Street, Jimei,
Xiamen, Fujian, China.

Hotline: 400-8838-199

Tel: +86 592-6300320

Fax: +86 592-5912735

Web: en.four-faith.com




Files Revised Record

Date	Version	Remark	Author
2020-06-03	V1.0.0	Initial version	WHC

Copyright Notice

All contents in the files are protected by copyright law, and all copyrights are reserved by Xiamen Four-Faith Communication Technology Co., Ltd. Without written permission, all commercial use of the files from Four-Faith are forbidden, such as copy, distribute, reproduce the files, etc., but non-commercial purpose, downloaded or printed by individual (all files shall be not revised, and the copyright and other proprietorship notice shall be reserved) are welcome.

Trademark Notice

Four-Faith、四信、、、 are all registered trademarks of Xiamen Four-Faith Communication Technology Co., Ltd., illegal use of the name of Four-Faith, trademarks and other marks of Four-Faith is forbidden, unless written permission is authorized in advance.



Contents

Chapter 1 Brief Introduction of Product.....	7
1.1 General.....	7
1.2 Features and Benefits.....	7
1.3 Working Principle.....	9
1.4 Specifications.....	9
LoRa Specification (optional)	10
Chapter 2 Installation Introduction.....	13
2.1 General.....	13
2.2 Encasement List.....	13
2.3 Installation and Cable Connection.....	13
2.3.1 Dimensions.....	13
2.3.2 Installation of antenna:.....	14
2.3.3 Installation of SIM/UIM card.....	14
2.3.4 Installation of cable.....	15
2.3.5 Connection RS232/RS485.....	15
2.3.6 Connection 8 isolated digital input and 2 12VDC power output.....	17
2.3.7 Connection 4 digital output lines.....	18
2.4 Power.....	18
2.5 Indicator Lights Introduction.....	19
2.6 Reset Button Introduction.....	20
Chapter 3 Configuration and Management.....	20
3.1 Configuration Connection.....	20
3.2 Access the Configuration Web Page.....	21
3.2.1 PC IP address setting (two ways).....	21
3.2.2 Access the Configuration Web Page.....	22
3.3 Management and configuration.....	24
3.3.1 Setting.....	24
3.3.1.1 Basic Setting.....	24
3.3.1.2 Dynamic DNS(DDNS).....	30
3.3.1.3 Clone MAC Address.....	31
3.3.1.4 Advanced Router.....	31
3.3.1.5 VLANs.....	32
3.3.1.6 Networking.....	33
3.3.2 Wireless.....	36
3.3.2.1 Basic Settings.....	36
3.3.2.2 Wireless Security.....	38
3.3.3 Services.....	40
3.3.4 VPN.....	43
3.3.4.1 PPTP.....	43

3.3.4.2 L2TP.....	45
3.3.4.3 OPENVPN.....	46
3.3.4.4 IPSEC.....	51
3.3.4.5 GRE.....	53
3.3.5 Security.....	54
3.3.5.1 Firewall.....	54
3.3.6 Access Restrictions.....	57
3.3.6.1 WAN Access.....	57
3.3.6.2 URLFilter.....	60
3.3.6.3 Packet Filter.....	61
3.3.7 NAT.....	62
3.3.7.1 Port Forwarding.....	62
3.3.7.2 Port Range Forward.....	62
3.3.7.3 DMZ.....	64
3.3.8 QoS Setting.....	64
3.3.8.1 Basis.....	64
3.3.8.2 Classify.....	65
3.3.9 Applications.....	66
3.3.9.1 Serial Applications.....	66
3.3.9.2 Communication Gateway.....	68
3.3.10Administration.....	75
3.3.10.1 Management.....	75
3.3.10.2 Keep Alive.....	77
3.3.10.3 Commands.....	78
3.3.10.4 Factory Defaults.....	78
3.3.10.5 Firmware Upgrade.....	79
3.3.10.6 BackUP.....	79
3.3.11 Status.....	80
3.3.11.1 F-DPU110.....	80
3.3.11.2 WAN.....	82
3.3.11.3 LAN.....	84
3.3.11.4 Wireless.....	87
3.3.11.5 Bandwidth.....	88
3.3.11.6 Sys-Info.....	90
Appendix.....	93

Chapter 1 Brief Introduction of Product

1.1 General

F-DPU110 Distributed Processing Unit is a kind of cellular terminal device that provides Protocol integration and data transfer function by public cellular network.

It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232/RS485, Ethernet and WIFI port that can conveniently and transparently connect one device to a cellular network, allowing you to connect to your existing serial, Ethernet and WIFI devices with only basic configuration.

It has been widely used on M2M fields, Such as photo-voltaic power, substation and other electric industries, urban building energy management, the management of enterprise energy consumption and so on.



1.2 Features and Benefits

Design for Industrial Application

- ◆ High-powered industrial cellular module

- ◆ High-powered industrial 32bits CPU
- ◆ Support low-consumption mode, including sleep mode, scheduled online/offline mode
- ◆ Housing: iron, providing IP30 protection.
- ◆ Power range: (85~265VAC/DC)

Stability and Reliability

- ◆ Support hardware and software WDT
- ◆ Support auto recovery mechanism, including online detect, auto redial when offline to make device always online
- ◆ Ethernet port: 1.5KV magnetic isolation protection
- ◆ RS232/RS485 port: 15KV ESD protection
- ◆ SIM/UIM port: 15KV ESD protection
- ◆ Power port: reverse-voltage and over voltage protection
- ◆ Antenna port: lightning protection(optional)

Standard and Convenience

- ◆ Support standard RS232/RS485, Ethernet and WIFI port that can connect to serial, Ethernet and WIFI devices directly
- ◆ Support standard WAN port and PPPOE protocol that can connect to ADSL directly
- ◆ Support intellectual mode, enter into communication state automatically when powered
- ◆ Provide management software for remote management
- ◆ Support several work modes
- ◆ Convenient configuration and maintenance interface (WEB or CLI)

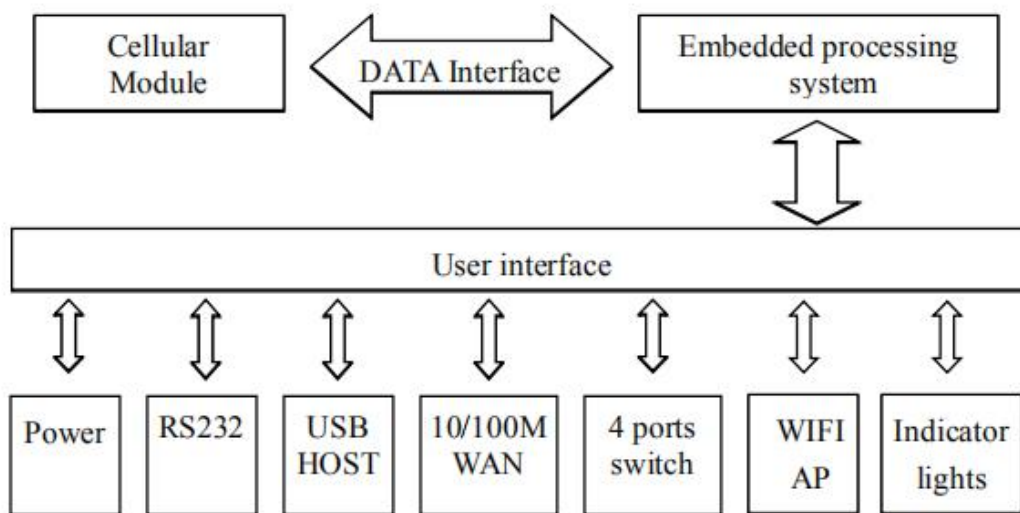
High-performance

- ◆ Ultra-large capacity flash memory, storing tens of thousands of protocols, compatible with different systems and platform protocols of various manufacturers
- ◆ Support multiple WAN access methods, including static IP, DHCP, L2TP, PPTP,PPPOE,2.5G/3G/4G
- ◆ Support double link backup between Cellular and WAN (optional)
- ◆ Support VPN client(PPTP,L2TP,IPSEC)(Note: Only for VPN version)
- ◆ Support VPN sever(PPTP,L2TP,IPSEC)(Note: Only for VPN version)
- ◆ Support remote management, SYSLOG、SNMP、TELNET、SSHD,HTTPS etc.
- ◆ Support local and remote firmware upgrade,import and export configure file
- ◆ Support NTP, RTC embedded
- ◆ Support multiple DDNS provider service
- ◆ Support MAC address clone, PPPOE server
- ◆ Support rack installation.
- ◆ WIFI support 802.11b/g/n, support WIFI AP、AP Client, repeater, repeater bridge mode etc. (Optional)
- ◆ WIFI support WEP,WPA,WPA2 encryption, support MAC address filter
- ◆ Support multiple online and offline trigger ways, including SMS, phone call, serial data and network data
- ◆ Support APN/VPDN

- ◆ Support multichannel DHCP server and DHCP client,DHCP bind MAC address, DDNS, firewall,NAT,DMZ
- host,QOS,traffic statistics, real-time display of data transmission rate etc.
- ◆ Support TCP/IP、 UDP、 FTP(Optional)、 HTTP etc.
- ◆ Support SPI firewall,VPN traversing, access control,URL filtration etc.
- ◆ Timed online and offline function.
- ◆ Support USB3.0, backward compatible with USB2.0
- ◆ Local storage supports flash memory, TF card
- ◆ Support multi-protocol conversion

1.3 Working Principle

The principle chart of the F-DPU110 is as following:



1.4 Specifications

Product Specification

Cellular Specification	
Item	Content
F-DPU110	
Standard and Band	Support band (optional): TDD-LTE、 FDD-LTE、 EVDO、 WCDMA、 TD-SCDMA、 CDMA1X、 GPRS/EDGE
Bandwidth	LTE FDD : download speed 100Mbps,upload speed 50Mbps LTE TDD : download speed 61Mbps,upload speed 18Mbps

	CDMA2000 1X EVDO Rev A : download speed 3.1Mbps,upload speed 1.8Mbps WCDMA : download speed 42Mbps,upload speed 5.76Mbps TD-SCDMA : download speed 4.2Mbps,upload speed 2.2Mbps
TX power	<23dBm
RX sensitivity	<-93.3dBm

WIFI Specification

Item	Content
Standard and Band	Support IEEE802.11b/g/n, 2.4G, 2*2 MIMO, support AP mode, Station mode (optional) Support IEEE802.11ac, 5.8G, 2*2 MIMO, support AP mode, Station mode (optional)
Bandwidth	IEEE802.11b/g: the highest rate reaches 108Mbps IEEE802.11n: the highest rate reaches 300Mbps IEEE802.11ac: the highest speed up to 780Mbps
Secure encryption	Support WEP, WPA, WPA2 and other encryption methods, optional WPS function
RX sensitivity	26dBm (11b) , 21.5dBm (11g) , 20dBm (11n) , 16dBm (11ac)

LoRa Specification (optional)

Item	Content
Communication standards and frequency bands	support multiple frequency bands around the world (433/470/780/868/915 MHz)
Indoor/urban communication distance	2km
Outdoor/line-of-sight communication distance	9km
Tx power	<30dBm
RX sensitivity	<-140dBm
Communication theoretical rate	6 levels adjustable (0.3, 0.6, 1.0, 1.8, 3.1, 5.5Kbps)

Hardware System

Item	Content
CPU	Dual-core 880MHZ processor
FLASH	64MB SPIflash/512MB Nandflash

DDR3	512MB
TF	8GB/32GB, optional

Interface type	
Item	Content
WAN	1*10/100M Ethernet port (RJ45 socket), auto MDI/MDIX, 1.5KV magnetic isolation protection
LAN	4*10/100M Ethernet ports(RJ45 socket), auto MDI/MDIX, 1.5KV magnetic isolation protection
Serial port	2 RS232/RS485 port, 6RS485 port 15KV ESD protection Data bit: 5、6、7、8 Stop bit: 1、1.5(Optional)、2 Parity: none, even, odd, space(optional), mark(optional) Baud rate:2400~115200bits/s
indicator	"PWR"、"SYS"、"LAN"、"WAN"、"NET"、"Signal Strength"
I/O port	8 channels with isolated digital input, Applicable types: passive empty contact, active contact, open collector Input high level: 5~30 VDC Input low level: 0~3 VDC Input current range: DC2~20mA Resolution: 100mS 4 digital outputs Output type: relay output Contact capacity: 5A 250V AC/30V DC 2 channels 12VDC power output Output type: 12V/1A output, controllable
Antenna	Cellular: 2* Standard SMA female interface, 50 ohm WIFI/GPS: 2 *Standard SMA male interface, 50 ohm, Lora: 1 *Standard SMA male interface, 50 ohm(optional)
SIM/UIM	2 standard drawer type 3V/1.8V user card interface, 15KV ESD protection
Power	3-core terminal power socket with built-in reverse power protection Working voltage: 85~265VAC/DC Overload protection, reverse connection protection, redundancy protection
USB	Standard USB3.0 interface, support various USB storage
TF	Standard TF card interface, support various TF cards
Reset	Restore the router to its original factory default settings

Power supply	
Item	Content

Standard Power	AC220V
Power range	85~265VAC/DC

Power

Item	Content
Communication status	7.8W

Physical Characteristics

Item	Content
Housing	Metal, IP30
Dimensions	482.6*180*44mm(Without antenna and mounting parts)
Weight	1.53kg(Without external expansion)

Other parameters

Item	Content
Operating Temperature	-35~+75°C (-31~+167°F)
Storage Temperature	-40~+85°C (-40~+185°F)
Operating Humidity	95%(unfreezing)

Ordering Information

Model No.	Description	Note
F-DPU110	Distributed Processing Unit	



Chapter 2 Installation Introduction

2.1 General

The F-DPU110 must be installed correctly to make it work properly.

Warning: Forbid to install the F-DPU110 when powered!

2.2 Encasement List

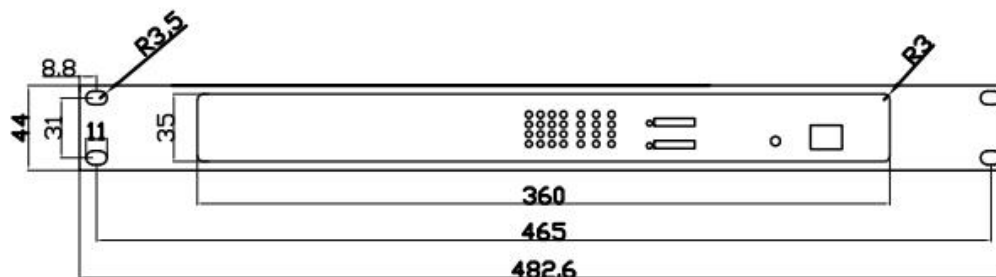
When you open the box, please keep the packing materials, so that you can use it in the future. The list is as follows:

Name	Quantity	Remark
F-DPU110	1	
Cellular antenna (Male SMA)	2	
WIFI antenna (Female SMA)	2	
Network cable	1	
Console cable	1	
Power adapter	1	
8PIN 5.08mm Terminal Block	1	
7PIN 3.5mm Terminal Block	2	
11PIN 3.5mm Terminal Block	2	
Certification card	1	
Maintenance card	1	

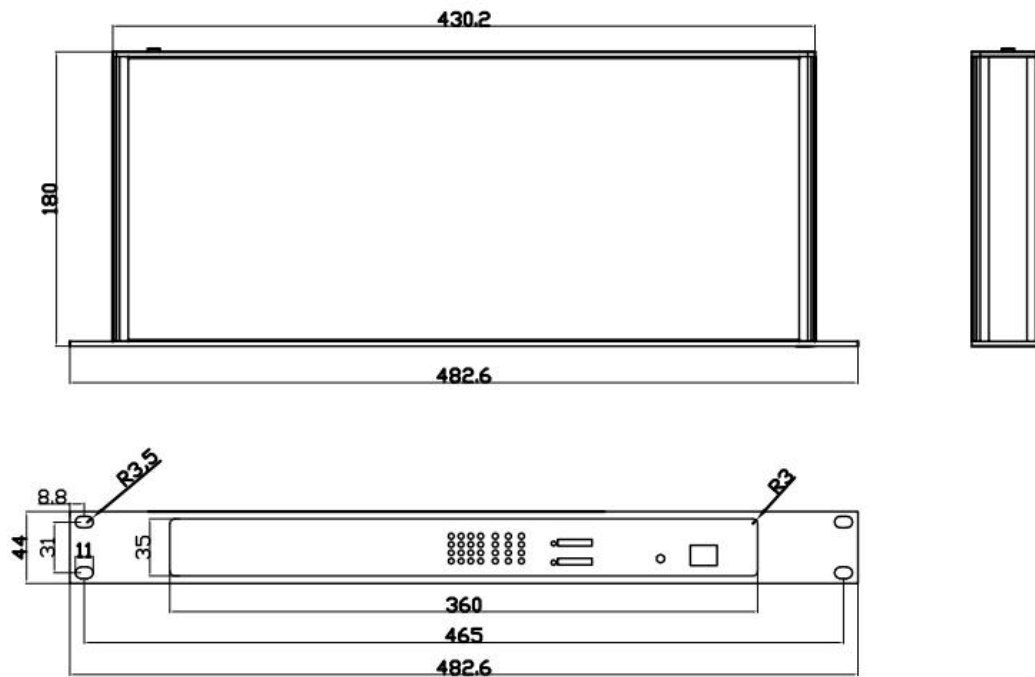
2.3 Installation and Cable Connection

2.3.1 Dimensions

Dimensions as shown below.(Unit: mm)



Fixed size



DPU110 size

Note: The screw used to install the DPU110 with the fixing piece is M3, and the depth of the screw lock into the DPU110 is 3~4mm.

2.3.2 Installation of antenna:

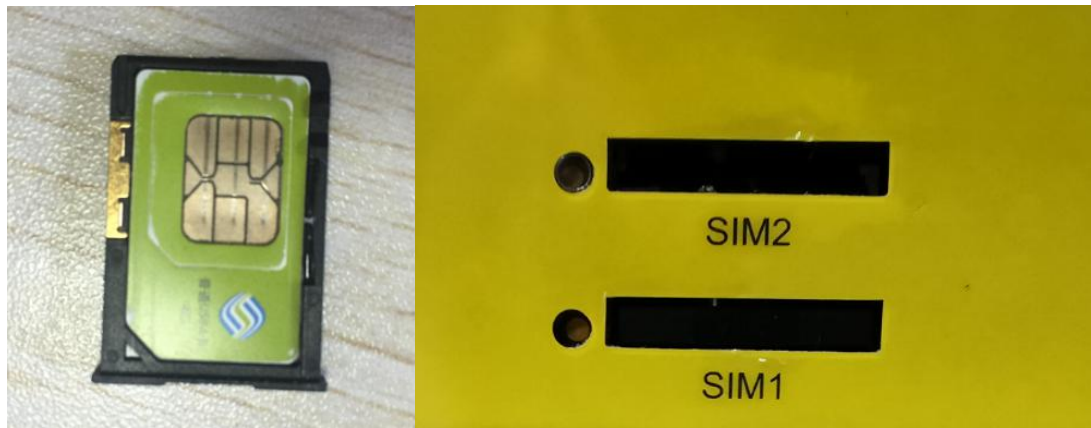
Screw the SMA male pin of the cellular antenna to the female SMA interface of the F-DPU110 with sign “ANT-M” and “ANT-A”.

Screw the SMA female pin of the WIFI antenna to the male SMA interface of the F-DPU110 with sign “WIFI”.

Warning: The cellular antenna and the WIFI antenna can not be connected wrongly. And the antennas must be screwed tightly, or the signal quality of antenna

2.3.3 Installation of SIM/UID card

When installing or removing the SIM/UID card, first use a pointed object to gently hold the eject button (the small round dot on the left side of the SIM/UID), and the SIM/UID card sleeve will pop out. When installing SIM/UID card, put SIM/UID card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UID card outlet.



2.3.4 Installation of cable

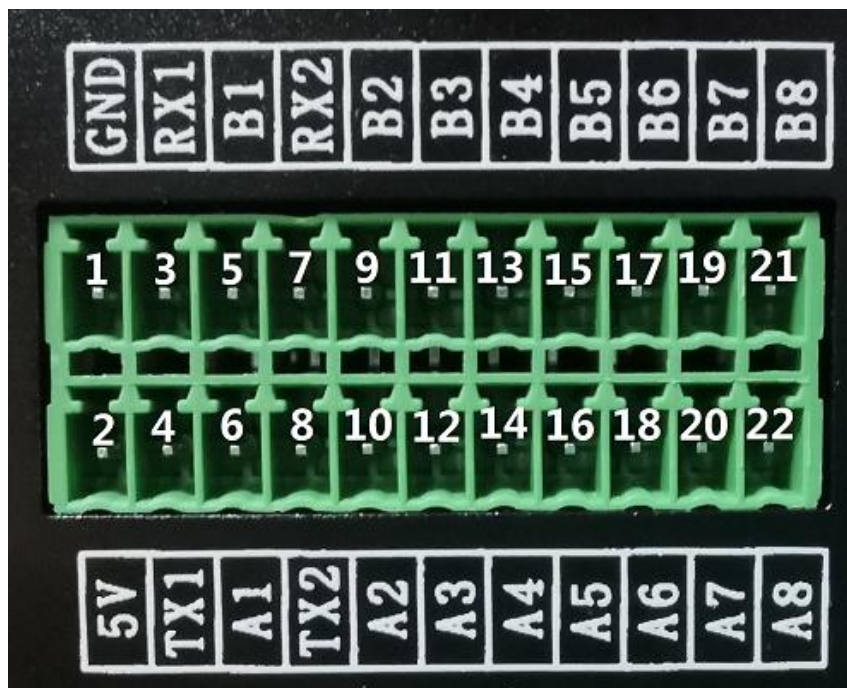
Insert one end of the network cable into the switch interface with sign “Local Network”, and insert the other end into the Ethernet interface of user’s device. The signal connection of network direct cable is as follows:

RJ45-1	RJ45-2	Color
1	1	White/Orange
2	2	Orange
3	3	White/Green
4	4	Blue
5	5	White/Blue
6	6	Green
7	7	White/Brown
8	8	Brown



2.3.5 Connection RS232/RS485

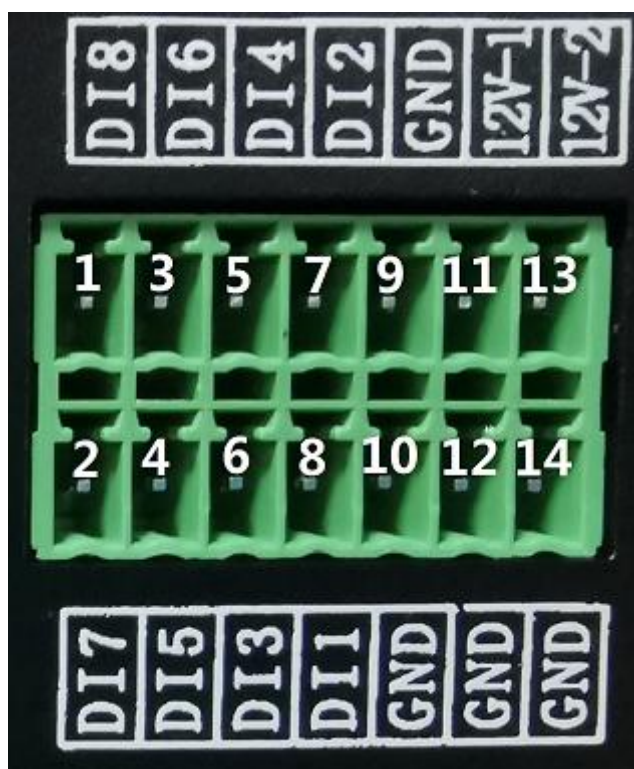
Plug the RS232 and RS485 line ends into the 14PIN interface of DPU110, and the lead out RS232/RS485 line to the RS232/RS485 serial interface of the user equipment, the interface signal connection is as follows:



21PIN	Signal	Description	Dir (F-DPU110)
1	GND	Ground	Output
2	5V	5VPower (1W)	Output
3	RX1	232 RXD1	Input
4	TX1	232 TXD1	Output
5	B1	485B1	Input/Output
6	A1	485A1	Input/Output
7	RX2	232 RXD2	Input
8	TX2	232 TXD2	Output
9	B2	485B2	Input/Output
10	A2	485A2	Input/Output
11	B3	485B3	Input/Output
12	A3	485A3	Input/Output
13	B4	485B4	Input/Output
14	A4	485A4	Input/Output
15	B5	485B5	Input/Output
16	A5	485A5	Input/Output
17	B6	485B6	Input/Output
18	A6	485A6	Input/Output
19	B7	485B7	Input/Output
20	A7	485A7	Input/Output
21	B8	485B8	Input/Output
22	A8	485A8	Input/Output

2.3.6 Connection 8 isolated digital input and 2 12VDC power output

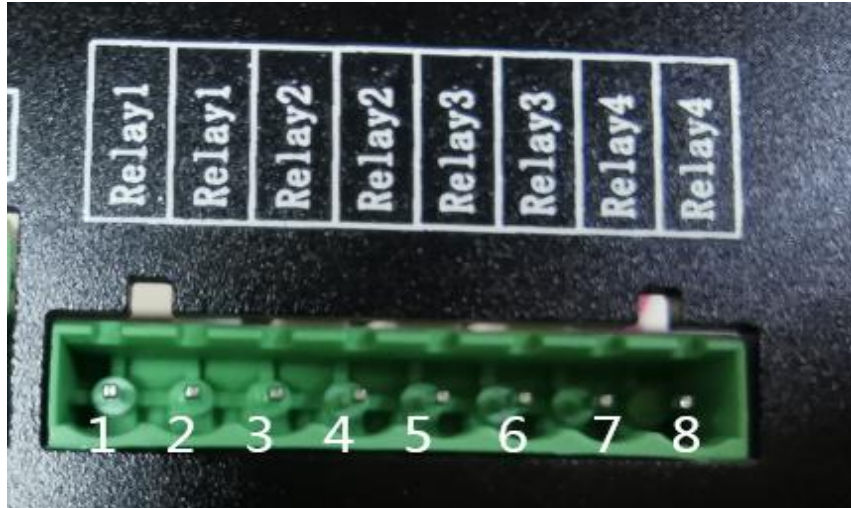
Plug 8 channels of isolated digital input and 2 channels of 12VDC power output line ends into the 14PIN interface of DPU110, 8 channels of data input connect to the data output of the user equipment, 12VDC connect to the 12VDC power input of the user equipment, to the user equipment For power supply, the interface signal connections are as follows:



14PIN	Signal	Description	Dir (F-DPU110)
1	DI8	Digital 8	Input
2	DI7	Digital 7	Input
3	DI6	Digital 6	Input
4	DI5	Digital 5	Input
5	DI4	Digital 4	Input
6	DI3	Digital 3	Input
7	DI2	Digital 2	Input
8	DI1	Digital 1	Input
9	GND	Power-Ground	Output
10	GND	Power-Ground	Output
11	12V-1	12V Power 1 (1A)	Output
12	GND	Power-Ground	Output
13	12V-2	12V Power 2 (1A)	Output
14	GND	Power-Ground	Output

2.3.7 Connection 4 digital output lines

Plug the 4-channel digital output line end into the 8PIN interface of DPU110, the 4-channel digital output type is relay output, and connect to the data input of the user equipment. The interface signal connection is as follows:



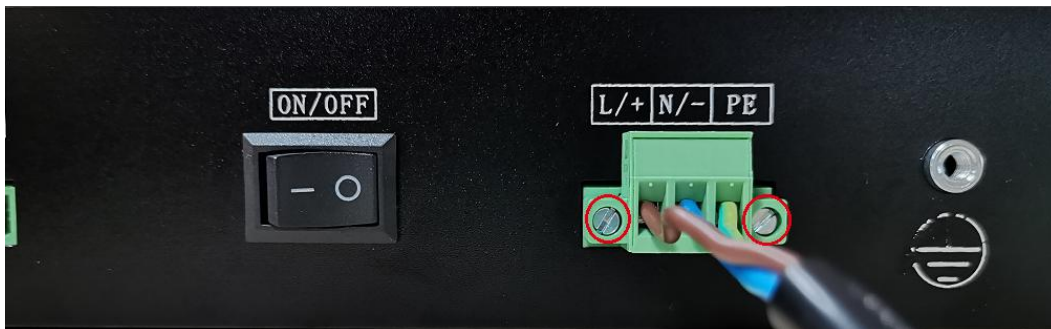
8PIN	Signal	Description	Dir (F-DPU110)
1	Relay1	Relay Output1 NO1	Output
2	Relay1	Relay Output1 NC1	Output
3	Relay2	Relay Output2 NO2	Output
4	Relay2	Relay Output2 NC2	Output
5	Relay3	Relay Output3 NO3	Output
6	Relay3	Relay Output3 NC3	Output
7	Relay4	Relay Output4 NO4	Output
8	Relay4	Relay Output4 NC4	Output

2.4 Power

DPU110 is usually used in complex external environments. In order to adapt to the complex application environment and improve the stability of the system, DPU110 uses advanced power supply technology. Users can directly use 85~265VAC/DC to supply power to DPU110. It is recommended to use the standard power cord. Insert the terminal block into the power input port and tighten the two screws of the terminal block.



Standard power line



Power line connection

2.5 Indicator Lights Introduction

The F-DPU110 provides following indicator lights: "PWR", "SYS", "Online", "SIM", "LAN1~LAN4", "WAN", "WIFI", "Signal Strength". Indicator is as follows:

Indicator	State	Introduction
Power	On	DPU110 is powered on
	Off	F-DPU110 is powered off
System	Blink	System works properly
	Off	System does not work
Online	On	F-DPU110 has logged on network
	Off	F-DPU110 hasn't logged on network
SIM	On	The SIM card has been identified
	Off	The SIM card is not recognized
LAN1~LAN4	Off	The corresponding interface of switch is not connected
	On/Blink	The corresponding interface of switch is connected /Communicating
WAN	Off	The interface of WAN is not connected
	On/Blink	The interface of WAN is connected /Communicating
WIFI	Off	WIFI is not active
	On	WIFI is active

Signal Strength	One Light ON	Signal strength is weak(less -90dbm)
	Two Light ON	Signal strength is medium(-70dbm~-90dbm)
	Three Light ON	Signal strength is good(Over-70dbm)
Serial port indicator	Off	serial port is not connected/not communicating
	On	serial port is connected/ communicating

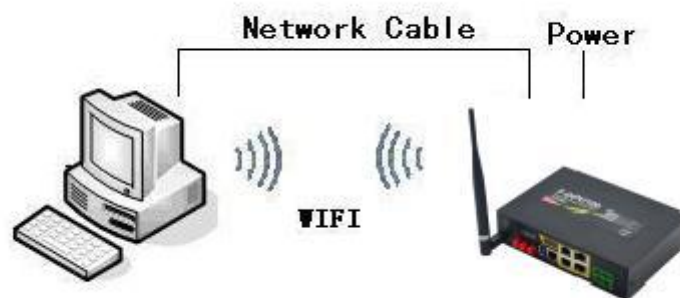
2.6 Reset Button Introduction

The Device has a “Reset” button to restore it to its original factory default settings. When user press the “Reset” button for up to 15s, the device will restore to its original factory default settings and restart automatically.(The automatic restart phenomenon is as follows: the "System" indicator turns off for about 10 seconds, and then it works normally).

Chapter 3 Configuration and Management

3.1 Configuration Connection

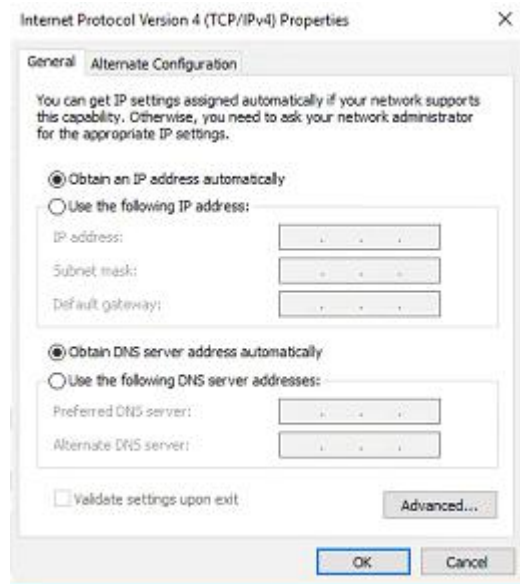
Before configuration, you should connect the F-DPU110 and your configuration PC with the supplied network cable or WIFI . Plug the cable’s one end into the Local Network port of the F-DPU110, and another end into your configure PC’s Ethernet port. When connected with WIFI, the factory default SSID of DPU110 is "FOUR-FAITH", no password verification is required.The connection diagram is as following:



3.2 Access the Configuration Web Page

3.2.1 PC IP address setting (two ways)

First way: get an IP address automatically



Second way: specify the IP address

Set the PC's IP address to 192.168.4.9 (or other IP addresses in the 192.168.4.1 network segment), the subnet mask to: 255.255.255.0, and the default gateway to: 192.168.4.1. DNS is set to a local available DNS server.



3.2.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connect users' PC to the F-DPU110. There are eleven main pages: Setting, Wireless, Service, VPN, Security, Access Restrictions, NAT, QoS Setting, Applications, Management and Status. Users enable to browse slave pages by click one main page..

Users can open IE or other explorers and enter the F-DPU110's default IP address of 192.168.4.1 on address bar, then press the bottom of Enter to visit page Web management tool of the F-DPU110. The users login in the web page at the first name, there will display a page shows as blow to tip users to modify the default user name and password of the F-DPU110. Users have to click "change password" to make it work if they modify user name and password.

Router Management

Your Router is currently not protected and uses an unsafe default username and password combination, please change it using the following dialog!

Router Password

Router Username	<input type="text" value="admin"/>
Router Password	<input type="password" value="••••"/>
Re-enter to confirm	<input type="password" value="••••"/>

After access to the information main page

Setup	Wireless	Services	VPN	Security	NAT	Access Restrictions	QoS	App	Admin	Status
System Information										
Router										
Router Name	Four-Faith									
Router Model	Four-Faith Router									
LAN MAC	00:0C:43:BB:EB:92									
WAN MAC	00:0C:43:BB:EB:93									
Wireless MAC	00:0C:43:BB:EB:94									
WAN IP	120.42.46.98									
LAN IP	192.168.8.1									
Services										
DHCP Server	Enabled									
ff-radauth	Disabled									
USB Support	Enabled									
Memory										
Total Available	501.2 MB / 512.0 MB									
Free	441.1 MB / 501.2 MB									
Used	60.0 MB / 501.2 MB									
Buffers	4.7 MB / 60.0 MB									
Cached	15.4 MB / 60.0 MB									
Active	8.8 MB / 60.0 MB									
Inactive	15.3 MB / 60.0 MB									
Wireless										
Wireless Packet Info										
Radio	Radio is On									
Mode	AP									
Network	Mixed									
SSID	ff-fourfaith									
Channel	13 (2472 MHz)									
TX Power	100 mW									
Rate	150 Mb/s									
Received (RX)	0 OK, no error									
Transmitted (TX)	0 OK, no error									
Wireless										
Clients										
MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality		
- None -										
DHCP										
DHCP Clients										
Host Name	IP Address	MAC Address	Client Lease Time							

Users need to input user name and password if it is their first time to login.



Input correct user name and password to visit relevant menu page. Default user name is admin, password is admin. (available to modify user name and password on management page, then click submit)

3.3 Management and configuration

3.3.1 Setting

The first page opened by clicking "Settings" is the basic settings. Through this page, you can follow the prompts to change the basic settings, click the "Save Settings" button to change but not take effect, click the "Apply" button to make the changes take effect, or click the "Cancel Changes" button to cancel change.

3.3.1.1 Basic Setting

WAN Connection Type

Seven Ways: Disabled, Static IP, Automatic Configuration-DHCP, PPPOE, 3G/UNMTS/4G/LTE, DHCP-4G.

Disabled

Connection Type Disabled

Forbid the setting of WAN port connection type

Static IP

WAN Connection Type

Connection Type	Static IP
WAN IP Address	0 . 0 . 0 . 0
Subnet Mask	0 . 0 . 0 . 0
Gateway	0 . 0 . 0 . 0
Static DNS 1	0 . 0 . 0 . 0
Static DNS 2	0 . 0 . 0 . 0
Static DNS 3	0 . 0 . 0 . 0
Wan Nat	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

WAN IP Address: Users set IP address by their own or ISP assigns

Subnet Mask: Users set subnet mask by their own or ISP assigns

Gateway: Users set gateway by their own or ISP assigns

Static DNS1/DNS2/DNS3: Users set static DNS by their own or ISP assigns

Automatic Configuration-DHCP

Connection Type	Automatic Configuration - DHCP
-----------------	--------------------------------

IP address of WAN port gets automatic via DHCP

PPPOE

Connection Type	PPPoE
User Name	<input type="text"/>
Password	<input type="text"/> <input type="checkbox"/> Unmask

User Name: login the Internet

Password: login the Internet

3G/UMTS/4G/LTE

Connection Type	3G/UMTS/4G/LTE
User Name	<input type="text"/>
Password	<input type="text"/> <input type="checkbox"/> Unmask
Dial String	*99***1# (UMTS/3G/3.5G)
APN	<input type="text"/>
PIN	<input type="text"/> <input type="checkbox"/> Unmask

User Name: login users' ISP(Internet Service Provider)

Password: login users' ISP

Dial String: dial number of users' ISP

APN: access point name of users' ISP

PIN: PIN code of users' SIM card

Connection type

Connection type

Connection type: Auto, Force 3G, Force 2G, Prefer 3G, Prefer 2G options. If using 4G module, there has 4G network option. Users select different mode depending on their need

DHCP-4G

Connection Type

IP address of WAN port gets automatic via DHCP-4G

Keep Online

Keep Online Detection

Detection Interval Sec.

Primary Detection Server IP

Backup Detection Server IP

This function is used to detect whether the Internet connection is active, if users set it and when the Router detect the connection is inactive, it will redial to users' ISP immediately to make the connection active. If the network is busy or the user is in private network, we recommend that Router mode will be better.

Detection Method:

None: do not set this function

Ping: Send ping packet to detect the connection, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

Route: Detect connection with route method, when choose this method, users should also configure "Detection Interval", "Primary Detection Server IP" and "Backup Detection Server IP" items.

PPP: Detect connection with PPP method, when choose this method, users should also configure "Detection Interval" item.

Detection Interval: time interval between two detections, unit is second

Primary Detection Server IP: the server used to response the Router's detection packet. This item is only valid for method "Ping" and "Route".

Backup Detection Server IP: the server used to response the Router's detection packet. This item is valid for method "Ping" and "Route".

Note: When users choose the "Route" or "Ping" method, it's quite important to make sure that the "Primary Detection Server IP" and "Backup Detection Server IP" are usable and stable, because they have to response the detection packet frequently.

Force reconnect ☒ Enable ☐ Disable

Time

Force reconnect: this option schedules the pppoe or 3G reconnection by killing the pppd daemon and restart it.

Time: needed time to reconnect

STP

STP ☐ Enable ☒ Disable

STP (Spaning Tree Protocol) can be applied to loop network. Through certain algorithm achieves path redundancy, and loop network cuts to tree-based network without loop in the meantime, thus to avoid the hyperplasia and infinite circulation of a message in the loop network

Optional Settings

Optional Settings

Router Name	<input type="text" value="Four-Faith"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
MTU	<input type="text" value="Auto"/> <input type="text" value="1500"/>
Force Net Card Mode	<input type="text" value="Auto"/>

Optional Settings

Optional Settings

Router Name	<input type="text" value="Four-Faith"/>
Host Name	<input type="text"/>
Domain Name	<input type="text"/>
MTU	<input type="text" value="Auto"/> <input type="text" value="1500"/>
Force Net Card Mode	<input type="text" value="Auto"/>

Router Name: set Router name

Host Name: ISP provides

Domain Name: ISP provides

MTU: auto (1500) and manual (1200-1492 in PPPOE/PPTP/L2TP mode, 576-16320 in other modes)

Router Internal Network Settings

Router IP

Local IP Address	192	.	168	.	1	.	1
Subnet Mask	255	.	255	.	255	.	0
Gateway	0	.	0	.	0	.	0
Local DNS	0	.	0	.	0	.	0

Local IP Address: IP address of the Router

Subnet Mask: the subnet mask of the Router

Gateway: set internal gateway of the Router. If default, internal gateway is the address of the Router

Local DNS: DNS server is auto assigned by network operator server. Users enable to use their own DNS server or other stable DNS servers, if not, keep it default

Network Address Server Settings (DHCP)

These settings for the Router's Dynamic Host Configuration Protocol (DHCP) server functionality configuration. The Router can serve as a network DHCP server. DHCP server automatically assigns an IP address for each computer in the network. If they choose to enable the Router's DHCP server option, users can set all the computers on the LAN to automatically obtain an IP address and DNS, and make sure no other DHCP server in the network.

DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1. 100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	0.0.0.0
Static DNS 2	0.0.0.0
Static DNS 3	0.0.0.0
WINS	0.0.0.0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

DHCP Type: DHCP Server and DHCP Forwarder

Enter DHCP Server if set DHCP Type to DHCP Forwarder as blow:

DHCP Type	<input type="button" value="DHCP Forwarder"/>
DHCP Server	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>

DHCP Server: keep the default Enable to enable the Router's DHCP server option. If users have already have a DHCP server on their network or users do not want a DHCP server, then select Disable

Start IP Address: enter a numerical value for the DHCP server to start with when issuing IP addresses. Do not start with 192.168.1.1 (the Router's own IP address).

Maximum DHCP Users: enter the maximum number of PCs that users want the DHCP server to assign IP addresses to. The absolute maximum is 253 if 192.168.1.2 is users' starting IP address.

Client Lease Time: the Client Lease Time is the amount of time a network user will be allowed connection to the Router with their current dynamic IP address. Enter the amount of time, in minutes, that the user will be "leased" this dynamic IP address.

Static DNS (1-3): the Domain Name System (DNS) is how the Internet translates domain or website names into Internet addresses or URLs. Users' ISP will provide them with at least one DNS Server IP address. If users wish to utilize another, enter that IP address in one of these fields. Users can enter up to three DNS Server IP addresses here. The Router will utilize them for quicker access to functioning DNS servers.

WINS: the Windows Internet Naming Service (WINS) manages each PC's interaction with the Internet. If users use a WINS server, enter that server's IP address here. Otherwise, leave it blank.

DNSMasq: users' domain name in the field of local search, increase the expansion of the host option, to adopt DNSMasq can assign IP addresses and DNS for the subnet, if select DNSMasq, dhcpd service is used for the subnet IP address and DNS.

Time Settings

Select time zone of your location. To use local time, leave the checkmark in the box next to Use local time.

NTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone	<input type="button" value="UTC+08:00"/>
Summer Time (DST)	<input type="button" value="last Sun Mar - last Sun Oct"/>
Server IP/Name	<input type="text"/>

NTP Client: Get the system time from NTP server

Time Zone: Time zone options

Summer Time (DST): set it depends on users' location

Server IP/Name: IP address of NTP server, up to 32 characters. If blank, the system will find a server by default

Adjust Time

Time	<input type="text" value="2012"/> - <input type="text" value="3"/> - <input type="text" value="15"/> <input type="text" value="9"/> : <input type="text" value="16"/> : <input type="text" value="20"/>	<input type="button" value="Get"/>	<input type="button" value="Set"/>
------	---	------------------------------------	------------------------------------

To adjust time by the system and refresh to get the time of the web, user can set to modify the time

of the system. They can change to adjust time by manual to achieve adjust time by the system if the system fails to get NTP server

3.3.1.2 Dynamic DNS(DDNS)

If user's network has a permanently assigned IP address, users can register a domain name and have that name linked with their IP address by public Domain Name Servers (DNS). However, if their Internet account uses a dynamically assigned IP address, users will not know in advance what their IP address will be, and the address can change frequently. In this case, users can use a commercial dynamic DNS service, which allows them to register their domain to their IP address, and will forward traffic directed at their domain to their frequently-changing IP address.

DDNS Service: Router currently support DynDNS, freedns, Zoneedit, NO-IP, 3322, easyDNS, TZO, DynSIP and Custom based on the user.

DDNS Service	<input type="text" value="3322.org"/>	<input type="button" value="v"/>
User Name	<input type="text"/>	
Password	<input type="text"/>	<input type="checkbox"/> Unmask
Host Name	<input type="text"/>	
Type	<input type="text" value="Dynamic"/>	
Wildcard	<input type="checkbox"/>	
Do not use external ip check	<input checked="" type="radio"/> Yes <input type="radio"/> No	

User Name: users register in DDNS server, up to 64 characteristic

Password: password for the user name that users register in DDNS server, up to 32 characteristic

Host Name: users register in DDNS server, no limited for input characteristic for now

Type: depends on the server

Wildcard: support wildcard or not, the default is OFF. ON means *.host.3322.org is equal to host.3322.org

Do not use external ip check: enable or disable the function of 'do not use external ip check'

Force Update Interval	<input type="text" value="10"/>	(Default: 10 Days, Range: 1 - 60)
-----------------------	---------------------------------	-----------------------------------

Force Update Interval: unit is day, try forcing the update dynamic DNS to the server by setted days

Status

DDNS Status

```
Fri Nov 25 13:58:32 2011: INADYN: Started 'INADYN Advanced version 1.96-ADV' - dynamic DNS updater.
Fri Nov 25 13:58:32 2011: INADYN: IP read from cache file is '192.168.8.222'. No update required.
Fri Nov 25 13:58:32 2011: I:INADYN: IP address for alias 'testsixin.3322.org' needs update to '192.168.8.38'
Fri Nov 25 13:58:33 2011: I:INADYN: Alias 'testsixin.3322.org' to IP '192.168.8.38' updated successfully.
```

3.3.1.3 Clone MAC Address

Some ISP need the users to register their MAC address. The users can clone the Router MAC address to their MAC address registered in ISP if they do not want to re-register their MAC address

☒ Enable ☐ Disable

Clone LAN MAC

00 : AA : BB : CC : DD : 43

Clone WAN MAC

00 : AA : BB : CC : DD : 44

[Get Current PC MAC Address](#)

Clone Wireless MAC

00 : AA : BB : CC : DD : 45

Clone MAC address can clone three parts: Clone LAN MAC, Clone WAN MAC, Clone Wireless MAC.

Noted that one MAC address is 48 characteristic, can not be set to the multicast address, the first byte must be even. And MAC address value of network bridge br0 is determined by the smaller value of wireless MAC address and LAN port MAC address.

3.3.1.4 Advanced Router

Operating Mode: Gateway and Router

Operating Mode

Operating Mode

Gateway ▼

If the Router is hosting users' Internet connection, select Gateway mode. If another Router exists on their network, select Router mode.

Dynamic Routing

Dynamic Routing

Interface

Disable ▼

Dynamic Routing enables the Router to automatically adjust to physical changes in the network's layout and exchange routing tables with other Routers. The Router determines the network packets' route

based on the fewest number of hops between the source and destination.

To enable the Dynamic Routing feature for the WAN side, select WAN. To enable this feature for the LAN and wireless side, select LAN&WLAN. To enable the feature for both the WAN and LAN, select Both. To disable the Dynamic Routing feature for all data transmissions, keep the default setting, Disable.

Note: Dynamic Routing is not available in Gateway mode

Static Routing

Static Routing

Select set number
1 ()
Delete

Route Name

Metric
0

Destination LAN NET
0.0.0.0

Subnet Mask
0.0.0.0

Gateway
0.0.0.0

Interface
LAN & WLAN

Show Routing Table

Select set number: 1-50

Route Name: defined routing name by users, up to 25 characters

Metric: 0-9999

Destination LAN NET: the Destination IP Address is the address of the network or host to which users want to assign a static route

Subnet Mask: the Subnet Mask determines which portion of an IP address is the network portion, and which portion is the host portion

Gateway: IP address of the gateway device that allows for contact between the Router and the network or host.

Interface: indicate users whether the Destination IP Address is on the LAN & WLAN (internal wired and wireless networks), the WAN (Internet), or Loopback (a dummy network in which one PC acts like a network, necessary for certain software programs)

Show Routing Table

Routing Table Entry List			
Destination LAN NET	Subnet Mask	Gateway	Interface
192.168.1.1	255.255.255.255	0.0.0.0	WAN
192.168.1.0	255.255.255.0	0.0.0.0	LAN & WLAN
192.168.1.0	255.255.255.0	0.0.0.0	WAN
169.254.0.0	255.255.0.0	0.0.0.0	WAN
0.0.0.0	0.0.0.0	192.168.1.1	LAN & WLAN

Refresh
Close

3.3.1.5 VLANs

VLAN

VLAN	Port					Assigned To Bridge
	W	1	2	3	4	
1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	LAN <input type="button" value="v"/>
2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN <input type="button" value="v"/>
4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN <input type="button" value="v"/>
5	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	LAN <input type="button" value="v"/>
6	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
7	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
8	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
9	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
10	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
11	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
12	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
13	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
14	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>
15	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	None <input type="button" value="v"/>

VLANs function is to divide different VLAN ports by users' will. The system supports 15 VLAN port from VLAN1-VLAN15. However there is only 5 time ports (1 WAN port and 4 LAN port) divided by users themselves, and LAN port and WAN port disable to divide into one VLAN port meanwhile.

3.3.1.6 Networking

Bridging

Create Bridge

Bridge 0

br0

STP

Off

Prio

32768

MTU

1500

Add

Assign to Bridge

Add

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0 ra0

Auto Refresh

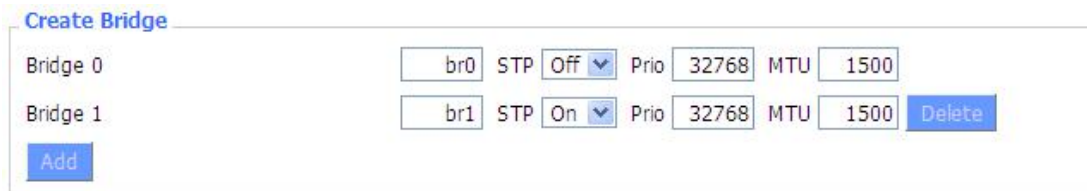
Bridging-Create Bridge: creates a new empty network bridge for later use. STP means Spanning Tree Protocol and with PRIO users are able to set the bridge priority order. The lowest number has the highest priority.

Bridging - Assign to Bridge: allows users to assign any valid interface to a network bridge. Consider setting the Wireless Interface options to Bridged if they want to assign any Wireless Interface here. Any system specific bridge setting can be overridden here in this field.

Current Bridging Table: shows current bridging table


Create steps as below:

Click 'Add' to create a new bridge, configuration is as below:



The 'Create Bridge' form contains a table with two rows for Bridge 0 and Bridge 1. Each row has input fields for the bridge name (br0, br1), STP status (Off, On), Priority (32768), and MTU (1500). There is a 'Delete' button for Bridge 1 and an 'Add' button at the bottom left.

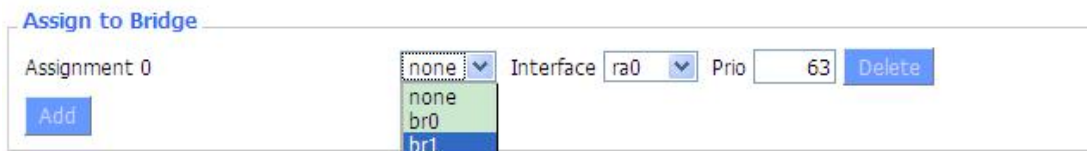
Create bridge option: the first br0 means bridge name. STP means to on/off spanning tree protocol. Prio means priority level of STP, the smaller the number, the higher the level. MTU means maximum transfer unit, default is 1500, delete if it is not need. And then click 'Save' or 'Add'. Bridge properties is as below:



This version of the 'Create Bridge' form includes additional fields for IP Address and Subnet Mask, each with four input boxes for the octets. It also includes 'Delete' buttons for both Bridge 0 and Bridge 1, and an 'Add' button at the bottom left.

Enter relevant bridge IP address and subnet mask, click 'Add' to create a bridge.

Note: Only create a bridge can apply it.



The 'Assign to Bridge' form has a dropdown menu for selecting a bridge (none, br0, br1), an 'Interface' dropdown (ra0), a 'Priority' input field (63), and a 'Delete' button. An 'Add' button is at the bottom left.

Assign to Bridge option: to assign different ports to created bridge. For example: assign port (wireless port) is ra0 in br1 bridge as below:

Prio means priority level: work if multiple ports are within the same bridge. The smaller the number, the higher the level. Click 'Add' to take it effect.

Note: corresponding interface of WAN ports interface should not be binding, this bridge function is basically used for LAN port, and should not be binding with WAN port

If bind success, bridge binding list in the list of current bridging table is as below:

Current Bridging Table

Bridge Name	STP enabled	Interfaces
br0	no	vlan0
br1	yes	ra0

Auto Refresh is On

To make br1 bridge has the same function with DHCP assigned address, users need to set multiple DHCP function, see the introduction of multi-channel DHCPD:

Port Setup

Network Configuration eth2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration vlan0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration ra0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration apcli0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds1	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds3	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration br0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default

Port Setup: Set the port property, the default is not set

Network Configuration ra0	<input checked="" type="radio"/> Unbridged	<input type="radio"/> Default
MTU	<input type="text" value="1500"/>	
Multicast forwarding	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable
Masquerade / NAT	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
IP Address	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	
Subnet Mask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>	

Choose not bridge to set the port's own properties, detailed properties are as below:

MTU: maximum transfer unit

Multicast forwarding: enable or disable multicast forwarding

Masquerade/NAT: enable or disable Masquerade/NAT

IP Address: set ra0's IP address, and do not conflict with other ports or bridge

Subnet Mask: set the port's subnet mask

Multiple DHCP Server

DHCP 0	ra0	On	Start	100	Max	50	Leasetime	3600
<input type="button" value="Delete"/> <input type="button" value="Add"/>								

Multiple DHCPD: using multiple DHCP service. Click 'Add' in multiple DHCP server to appear relevant configuration. The first means the name of port or bridge (do not be configured as eth0), the second means whether to on DHCP. Start means start address, Max means maximum assigned DHCP clients, Leasetime means the client lease time, the unit is second, click 'Save' or 'Apply' to put it into effect after setting.

Note: Only configure and click 'Save' can configure the next, can not configure multiple DHCP at the same time.

3.3.2 Wireless

3.3.2.1 Basic Settings

Wireless Physical Interface wl0 [2.4 GHz]

Wireless Network ☒ Enable ☐ Disable

Physical Interface ra0 - SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Wireless Mode

Wireless Network Mode

802.11n Transmission Mode

Wireless Network Name (SSID)

Wireless Channel

Channel Width

Extension Channel

Wireless SSID Broadcast ☒ Enable ☐ Disable

Network Configuration ☐ Unbridged ☒ Bridged

Virtual Interfaces

Wireless Network: "Eanble", radio on.

“Disable”, radio off.

Wireless Mode: AP, Client, Adhoc, Repeater, Repeater Bridge four options.

Wireless Network Mode:

Mixed: Support 802.11b, 802.11g, 802.11n wireless devices.

BG-Mixed: Support 802.11b, 802.11g wireless devices.

B-only: Only supports the 802.11b standard wireless devices.

B-only: Only supports the 802.11b standard wireless devices.

G-only: Only supports the 802.11g standard wireless devices.

NG-Mixed: Support 802.11g, 802.11n wireless devices.

N-only: Only supports the 802.11g standard wireless devices.

802.11n Transmission Mode : In the wireless network mode to "N-only" choose to transfer its transmission mode.

Greenfield: When you determine the surrounding environment, there is no other 802.11a/b/g devices use the same channel, use this mode to increase throughput. Other 802.11a/b/g devices use the same channel in the environment, the information you send may generate an error, re-issued.

Mixed: This mode is contrary to the green mode, but will reduce the throughput.

Wireless Network Name(SSID): The SSID is the network name shared among all devices in a wireless network. The SSID must be identical for all devices in the wireless network. It is case-sensitive and must not exceed 32 alphanumeric characters, which may be any keyboard character. Make sure this setting is the same for all devices in your wireless network. .

Wireless Channel : A total of 1-13 channels to choose more than one wireless device environment, please try to avoid using the same channel with other devices. .

Channel Width: 20MHZ and 40MHZ. .

Extension Channel: Channel for 40MHZ, you can choose upper or lower.

Wireless SSID Broadcast:

Enable: SSID broadcasting.

Disable: Hidden SSID.

Network Configuration:

Bridged: Bridge to the Router, under normal circumstances, please select the bridge.

Unbridged: There is no bridge to the Router, IP addresses need to manually configure.

Network Configuration	<input checked="" type="radio"/> Unbridged <input type="radio"/> Bridged
Multicast forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Masquerade / NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Address	192 . 168 . 1 . 1
Subnet Mask	255 . 255 . 0 . 0

Virtual Interfaces: Click Add to add a virtual interface. Add successfully, click on the remove, you can remove the virtual interface. .

Virtual Interfaces

Virtual Interfaces ra1 SSID [dd-wrt_vap] HWAddr [00:AA:BB:CC:DD:16]

Wireless Network Name (SSID)	<input type="text" value="dd-wrt_vap"/>
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged

AP Isolation : This setting isolates wireless clients so access to and from other wireless clients are stopped.

Note: Save your changes, after changing the "Wireless Mode", "Wireless Network Mode", "wireless width", "broadband" option, please click on this button, and then configure the other options.

3.3.2.2 Wireless Security

Wireless security options used to configure the security of your wireless network. This route is a total of seven kinds of wireless security mode. Disabled by default, not safe mode is enabled. Such as changes in Safe Mode, click Apply to take effect immediately.

Wireless Security wl0

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	<input type="text" value="Disabled"/> ▼
---------------	---

Wireless Security w10

Physical Interface ra0 SSID [four-faith] HWAddr [00:0C:43:30:52:79]

Security Mode	WEP
Authentication Type	<input checked="" type="radio"/> Open <input type="radio"/> Shared Key
Default Transmit Key	<input checked="" type="radio"/> 1 <input type="radio"/> 2 <input type="radio"/> 3 <input type="radio"/> 4
Encryption	64 bits 10 hex digits/5 ASCII
ASCII/HEX	<input type="radio"/> ASCII <input checked="" type="radio"/> HEX
Passphrase	1111111111111111 <input type="button" value="Generate"/>
Key 1	2627F68597
Key 2	15AD1DD294
Key 3	DDC4761939
Key 4	31F1ADB558

WEP: Is a basic encryption algorithm is less secure than WPA. Use of WEP is discouraged due to security weaknesses, and one of the WPA modes should be used whenever possible. Only use WEP if you have clients that can only support WEP (usually older, 802.11b-only clients).

Authentication Type: Open or shared key.

Default Transmit Key: Select the key form Key 1 - Key 4 key.

Encryption: There are two levels of WEP encryption, 64-bit (40-bit) and 128-bit. To utilize WEP, select the desired encryption bit, and enter a passphrase or up to four WEP key in hexadecimal format. If you are using 64-bit (40-bit), then each key must consist of exactly 10 hexadecimal characters or 5 ASCII characters. For 128-bit, each key must consist of exactly 26 hexadecimal characters. Valid hexadecimal characters are "0"-"9" and "A"-"F".

ASCII/HEX: ASCII, the keys is 5 bit ASCII characters/13bit ASCII characters.

HEX, the keys is 10bit/26 bit hex digits.

Passphrase: The letters and numbers used to generate a key.

Key1-Key4: Manually fill out or generated according to input the pass phrase.

Wireless Security w10

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	WPA Personal
WPA Algorithms	AES
WPA Shared Key <input type="checkbox"/> Unmask
Key Renewal Interval (in seconds)	3600 (Default: 3600, Range: 1 - 99999)

WPA Personal/WPA2 Personal/WPA2 Person Mixed: , TKIP/AES/TKIP+AES, dynamic encryption

keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allow WPA Personal and WPA2 Personal client mix.

WPA Shared Key: Between 8 and 63 ASCII character or hexadecimal digits.。

Key Renewal Interval (in seconds) : 1-99999。

Wireless Security w10

Physical Interface ra0 SSID [dd-junjinlee] HWAddr [00:AA:BB:CC:DD:15]

Security Mode	WPA Enterprise ▼
WPA Algorithms	AES ▼
Radius Auth Server Address	192 . 168 . 1 . 110
Radius Auth Server Port	1812 (Default: 1812)
Radius Auth Shared Secret	<input style="width: 80%;" type="password"/> <input type="checkbox"/> Unmask
Key Renewal Interval (in seconds)	3600

WPA Enterprise/WPA2 Enterprise/WPA2 Enterprise Mixed: WPA Enterprise uses an external RADIUS server to perform user authentication.

WPA Algorithms: AES/TKIP/TPIP+AES.

Radius Auth Sever Address: The IP address of the RADIUS server.

Radius Auth Server Port: The RADIUS Port (default is 1812)。

Radius Auth Shared Secret: The shared secret from the RADIUS server.。

Key Renewal Interva(in seconds): 1-99999.。

3.3.3 Services

DHCP Server

DHCPd assigns IP addresses to users local devices. While the main configuration is on the setup page users can program some nifty special functions here.

DHCP Server

Use JFFS2 for client lease DB (Not mounted)
Use NVRAM for client lease DB ☐
Used Domain WAN
LAN Domain
Additional DHCPd Options

Static Leases			
MAC Address	Host Name	IP Address	Client Lease Time
			minutes

Add
Remove

Use NVRAM for client lease DB: users can store data to the system NVRAM area is enabled

Used domain: users can select here which domain the DHCP clients should get as their local domain. This can be the WAN domain set on the Setup screen or the LAN domain which can be set here.

LAN Domain: users can define here their local LAN domain which is used as local domain for DNSmasq and DHCP service if chose above.

Static Leases: if users want to assign certain hosts a specific address then they can define them here. This is also the way to add hosts with a fixed address to the Router's local DNS service (DNSmasq).

Additional DHCPd Options: some extra options users can set by entering them

DNSMasq

DNSmasq is a local DNS server. It will resolve all host names known to the Router from dhcp (dynamic and static) as well as forwarding and caching DNS entries from remote DNS servers. Local DNS enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames.

DNSMasq

DNSMasq ☒ Enable ☐ Disable
Local DNS ☐ Enable ☒ Disable
No DNS Rebind ☒ Enable ☐ Disable
Additional DNSMasq Options

Local DNS: enables DHCP clients on the LAN to resolve static and dynamic DHCP hostnames

No DNS Rebind: when enabled, it can prevent an external attacker to access the Router's internal Web interface. It is a security measure

Additional DNSMasq Options: some extra options users can set by entering them in Additional DNS Options.

For example:

static allocation: dhcp-host=AB:CD:EF:11:22:33,192.168.0.10,myhost,myhost.domain,12h

max lease number: dhcp-lease-max=2

DHCP server IP range: dhcp-range=192.168.0.110,192.168.0.111,12h

SNMP

SNMP
☒ Enable ☐ Disable

Location	Unknown
Contact	root
Name	four-faith
RO Community	public
RW Community	private

Location: equipment location

Contact: contact this equipment management

Name: device name

RO Community: SNMP RO community name, the default is public, Only to read.

RW Community: SNMP RW community name, the default is private, Read-write permissions

SSHD

Enabling SSHd allows users to access the Linux OS of their Router with an SSH client

Secure Shell
☒ Enable ☐ Disable

SSHd	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SSH TCP Forwarding	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Password Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Port	22 (Default: 22)
Authorized Keys	

SSH TCP Forwarding: enable or disable to support the TCP forwarding

Password Login: allows login with the Router password (username is admin)

Port: port number for SSHd (default is 22)

Authorized Keys: here users paste their public keys to enable key-based login (more secure than a simple password)

System log

Enable Syslogd to capture system messages. By default they will be collected in the local file /var/log/messages. To send them to another system, enter the IP address of a remote syslog server.

System Log

Syslogd ☒ Enable ☐ Disable

Syslog Out Mode ☒ Net ☐ Console

Remote Server

Syslog Out Mode: two log mode

Net: the log information output to a syslog server

Console: the log information output to console port

Remote Server: if choose net mode, users should input a syslog server's IP Address and run a syslog server program on it.

Telnet

Telnet

Telnet ☒ Enable ☐ Disable

Telnet: enable a telnet server to connect to the Router with telnet. The username is **admin** and the password is the Router's password.

Note: If users use the Router in an untrusted environment (for example as a public hotspot), it is strongly recommended to use SSHd and deactivate telnet.

WAN Traffic Counter

WAN Traffic Counter

ttraff Daemon ☒ Enable ☐ Disable

Ttraff Daemon: enable or disable wan traffic counter function

3.3.4 VPN

3.3.4.1 PPTP

PPTP Server

PPTP Server

PPTP Server ☒ Enable ☐ Disable

Broadcast support ☐ Enable ☒ Disable

Force MPPE Encryption ☒ Enable ☐ Disable

DNS1

DNS2

WINS1

WINS2

Server IP

Client IP(s)

CHAP-Secrets

Broadcast support: enable or disable broadcast support of PPTP server

Force MPPE Encryption: enable or disable force MPPE encryption of PPTP data

DNS1/DNS2/WINS1/WINS2: set DNS1/DNS2/WINS1/WINS2

Server IP: input IP address of the Router as PPTP server, differ from LAN address

Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx

CHAP Secrets: user name and password of the client using PPTP service

Note: client IP must be different with IP assigned by Router DHCP.

The format of CHAP Secrets is user * password *.

PPTP Client

PPTP Client

PPTP Client Options ☒ Enable ☐ Disable

Server IP or DNS Name

Remote Subnet

Remote Subnet Mask

MPPE Encryption

MTU (Default: 1450)

MRU (Default: 1450)

NAT ☒ Enable ☐ Disable

User Name

Password ☐ Unmask

Server IP or DNS Name: PPTP server's IP Address or DNS Name

Remote Subnet: the network of the remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption.

MTU: maximum Transmission Unit

MRU: maximum Receive Unit

NAT: network Address Translation

User Name: user name to login PPTP Server.

Password: password to log into PPTP Server.

3.3.4.2 L2TP

L2TP Server

L2TP Server

L2TP Server Options

Force MPPE Encryption

Server IP

Client IP(s)

CHAP-Secrets

☒ Enable
 ☐ Disable

☒ Enable
 ☐ Disable

Force MPPE Encryption: enable or disable force MPPE encryption of L2TP data

Server IP: input IP address of the Router as PPTP server, differ from LAN address

Client IP(s): IP address assigns to the client, the format is xxx.xxx.xxx.xxx-xxx.xxx.xxx.xxx

CHAP Secrets: user name and password of the client using L2TP service

Note: client IP must be different with IP assigned by Router DHCP.

The format of CHAP Secrets is user * password *.

L2TP Client

L2TP Client

L2TP Client Options ☒ Enable ☐ Disable

User Name

Password ☐ Unmask

Gateway (L2TP Server)

Remote Subnet

Remote Subnet Mask

MPPE Encryption

MTU (Default: 1450)

MRU (Default: 1450)

NAT ☒ Enable ☐ Disable

Require CHAP ☒ Yes ☐ No

Refuse PAP ☒ Yes ☐ No

Require Authentication ☒ Yes ☐ No

Gateway(L2TP Server): L2TP server's IP Address or DNS Name

Remote Subnet: the network of remote PPTP server

Remote Subnet Mask: subnet mask of remote PPTP server

MPPE Encryption: enable or disable Microsoft Point-to-Point Encryption

MTU: maximum transmission unit

MRU: maximum receive unit

NAT: network address translation

User Name: user name to login L2TP Server

Password: password to login L2TP Server

Require CHAP: enable or disable support chap authentication protocol

Refuse PAP: enable or disable refuse to support the pap authentication

Require Authentication: enable or disable support authentication protocol

3.3.4.3 OPENVPN

OPENVPN Server

Start Type ☐ WAN Up ☒ System

Config via ☒ GUI ☐ Config File

Server mode ☒ Router (TUN) ☐ Bridge (TAP)

Config via: GUI----Page configuration, Config File----config File configuration

Server mode: Router (TUN)-route mode, Bridge (TAP)----bridge mode

Router (TUN):

Network	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>

Network: network address allowed by OPENVPN server

Netmask: netmask allowed by OPENVPN server

Bridge (TAP):

DHCP-Proxy mode	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Pool start IP	<input type="text" value="0.0.0.0"/>
Pool end IP	<input type="text" value="0.0.0.0"/>
Gateway	<input type="text" value="0.0.0.0"/>
Netmask	<input type="text" value="0.0.0.0"/>

DHCP-Proxy mode: enable or disable DHCP-Proxy mode

Pool start IP: pool start IP of the client allowed by OPENVPN server

Pool end IP: pool end IP of the client allowed by OPENVPN server

Gateway: the gateway of the client allowed by OPENVPN server

Netmask: netmask of the client allowed by OPENVPN server

Port	<input type="text" value="1194"/>	(Default: 1194)
Tunnel Protocol	<input type="text" value="UDP"/>	
Encryption Cipher	<input type="text" value="Blowfish CBC"/>	
Hash Algorithm	<input type="text" value="SHA1"/>	

Port: listen port of OPENVPN server

Tunnel Protocol: UCP or TCP of OPENVPN tunnel protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1 , SHA256, SHA512, MD5

Advanced Options

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Redirect default Gateway	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Allow Client to Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Allow duplicate cn	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
TUN MTU Setting	<input type="text" value="1500"/>	(Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/>	(Default: Disable)
TLS Cipher	<input type="text" value="Disable"/>	
Client connect script	<input type="text"/>	

Use LZO Compression: enable or disable use LZO compression for data transfer

Redirect default Gateway: enable or disable redirect default gateway

Allow Client to Client: enable or disable allow client to client

Allow duplicate cn: enable or disable allow duplicate cn

TUN MTU Setting: set the value of TUN MTU

TCP MSS: MSS of TCP data

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

Client connect script: define some client script by user self

CA Cert	<input type="text"/>
CA Cert: CA certificate	
Public Server Cert	<input type="text"/>
Public Server Cert: server certificate	
Private Server Key	<input type="text"/>
DH PEM	<input type="text"/>

Private Server Key: the key seted by the server

DH PEM: PEM of the server

Additional Config

CCD-Dir DEFAULT file

TLS Auth Key

Certificate Revoke List

Additional Config: additional configurations of the server

CCD-Dir DEFAULT file: other file approaches

TLS Auth Key: authority key of Transport Layer Security

Certificate Revoke List: configure some revoke certificates

OPENVPN Client

Server IP/Name

Port

(Default: 1194)

Tunnel Device

Tunnel Protocol

Encryption Cipher

Hash Algorithm

nsCertType verification

☐

Server IP/Name: IP address or domain name of OPENVPN server

Port: listen port of OPENVPN client

Tunnel Device: TUN----Router mode, TAP----Bridge mode

Tunnel Protocol: UDP and TCP protocol

Encryption Cipher: Blowfish CBC, AES-128 CBC, AES-192 CBC, AES-256 CBC, AES-512 CBC

Hash Algorithm: Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, MD5

nsCertType verification: support ns certificate type

Advanced Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use LZO Compression	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
NAT	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Bridge TAP to br0	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
Local IP Address	<input type="text"/>	
TUN MTU Setting	<input type="text" value="1500"/>	(Default: 1500)
MSS-Fix/Fragment across the tunnel	<input type="text"/>	(Default: Disable)
TLS Cipher	<input type="text" value="Disable"/>	
TLS Auth Key	<input type="text"/>	
Additional Config	<input type="text"/>	
Policy based Routing	<input type="text"/>	

Use LZO Compression: enable or disable use LZO compression for data transfer

NAT: enable or disable NAT through function

Bridge TAP to br0: enable or disable bridge TAP to br0

Local IP Address: set IP address of local OPENVPN client

TUN MTU Setting: set MTU value of the tunnel

TCP MSS: mss of TCP data

TLS Cipher: TLS (Transport Layer Security) encryption standard supports AES-128 SHA and AES-256 SHA

TLS Auth Key: authority key of Transport Layer Security

Additional Config: additional configurations of OPENVPN server

Policy based Routing: input some defined routing policy

CA Cert	<input type="text"/>
Public Client Cert	<input type="text"/>
Private Client Key	<input type="text"/>

CA Cert: CA certificate

Public Client Cert: client certificate

Private Client Key: client key

3.3.4.4 IPSEC

Connect Status and Control

Show IPSEC connection and status of current router on IPSEC page.

Connection status and control				
Name	Type	Common Name	status	Action
Add				

Name: the name of IPSEC connection

Type: The type and function of current IPSEC connection

Common name: local subnet, local address, opposite end address and opposite end subnet of current connection

Status: connection status: closed, negotiating, establish

Closed: this connection does not launch a connection request to opposite end

Negotiating: this connection launch a request to opposite end, is under negotiating, the connection has not been established yet

Establish: the connection has been established, enabled to use this tunnel

Action: the action of this connection, current is to delete, edit, reconnect and enable

Delete: to delete the connection, also will delete IPSEC if IPSEC has set up

Edit: to edit the configure information of this connection, reload this connection to make the configuration effect after edit

Reconnect: this action will remove current tunnel, and re-launch tunnel establish request

Enable: when the connection is enable, it will launch tunnel establish request when the system reboot or reconnect, otherwise the connection will not do it

Add: to add a new IPSEC connection

Add IPSEC connection or edit IPSEC connection

Type: to choose IPSEC mode and relevant functions in this part, supports tunnel mode client, tunnel mode server and transfer mode currently

Type	Net-to-Net Virtual Private Network
IPSEC role	<input checked="" type="radio"/> Client <input type="radio"/> Server

Connection: this part contains basic address information of the tunnel

Connection

Name	<input type="text"/>	Enabled	<input checked="" type="checkbox"/>
Local WAN Interface	vlan1 <input type="button" value="v"/>	Remote Host address	<input type="text"/>
Local Subnet	<input type="text"/>	Remote subnet	<input type="text"/>
Local Id	<input type="text"/>	Remote ID	<input type="text"/>

Name: to indicate this connection name, must be unique

Enabled: If enable, the connection will send tunnel connection request when it is reboot or re-connection, otherwise it is no need if disable

Local WAN Interface: local addresss of the tunnel

Remote Host Address: IP/domain name of end opposite; this option can not fill in if using tunnel mode server

Local Subnet: IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode

Remote Subnet: IPSec opposite end protects subnet and subnet mask, i.e.192.168.7.0/24; this option can not fill in if using transfer mode

Local ID: tunnel local end identification, IP and domain name are available

Remote ID: tunnel opposite end identification, IP and domain name are available

Detection: this part contains configure information of connection detection

Detection

Enable DPD Detection ☒

Time Interval (S) Timeout (S) Action

Enable Connection Detection ☒

Enable DPD Detection: enable or disable this function, tick means enable

Time Interval: set time interval of connect detection (DPD)

Timeout: set the timeout of connect detection

Action: set the action of connect detection

Advanced Settings: this part contains relevant setting of IKE, ESP, negotiation mode, etc.

Advanced Settings

Enable advanced settings ☒

IKE Encryption IKE Integrity IKE Groupype

IKE Lifetime hours

ESP Encryption ESP Integrity

ESP Keylife hours

☐ IKE+ESP: Use only proposed settings.

☐ IKE aggressive mode allowed. Avoid if possible (preshared key is transmitted in clear text)!

☒ Perfect Forward Secrecy (PFS)

☐ Negotiate payload compression

Enable Advanced Settings: enable to configure 1st and 2nd phase information, otherwise it will automic negotiation according to opposite end

IKE Encryption: IKE phased encryption mode

IKE Integrity: IKE phased integrity solution

IKE Groupype: DH exchange algorithm

IKE Lifetime: set IKE lifetime, current unit is hour, the default is 0

ESP Encryption: ESP encryption type

ESP Integrity: ESP integrity solution

ESP Keylife: set ESP keylife, current unit is hour, the default is 0

IKE aggressive mode allowed: negotiation mode adopt aggressive mode if tick; it is main mode if non-tick

Negotiate payload compression: Tick to enable PFS, non-tick to diable PFS

Authentication: choose use share encryption option or certificate authentication option. Current is only to choose use share encryption option.

Authentication

☒ Use a Pre-Shared Key:

☐ Generate and use the X.509 certificate

3.3.4.5 GRE

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a network layer protocol (such as IP and IPX) data packets are encapsulated, so these encapsulated data packets to another network layer protocol (IP)transmission. GRE Tunnel (tunnel) technology, Layer Two Tunneling Protocol VPN (Virtual Private Network).

GRE Tunnel

GRE Tunnel ☐ Enable ☒ Disable

GRE Tunnel: enable or disable GRE function

Number	1 (fff) ▼	Delete
Status	Enable ▼	
Name	fff	
Through	PPP ▼	
Peer Wan IP Addr	120.42.46.98	
Peer Subnet	192.168.5.0/24	(eg:192.168.1.0/24)
Peer Tunnel IP	200.200.200.1	
Local Tunnel IP	200.200.200.5	
Local Netmask	255.255.255.0	

Number: Switch on/off GRE tunnel app

Status: Switch on/off someone GRE tunnel app

Name: GRE tunnel name

Through: The GRE packet transmit interface

Peer Wan IP Addr: The remote WAN address

Peer Subnet: The remote gateway local subnet, eg: 192.168.1.0/24

Peer Tunnel IP: The remote tunnel ip address

Local Tunnel IP: The local tunnel ip address

Local Netmask: Netmask of local network

Keepalive	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Retry times	<input type="text"/>
Interval	<input type="text"/>
Fail Action	Hold ▼

Keepalive: Enable or disable GRE Keepalive function

Retry times: GRE keepalive detect fail retries

Interval: The time interval of GRE keepalive packet sent

Fail Action: The action would be exec after keeping alive failed

Click on “**View GRE tunnels**” keys can view the information of GRE

GRE Tunnels list												
Number	Name	Enable	Through	Peer Wan IP Addr	Peer Subnet	Peer Tunnel IP	Local Tunnel IP	Local Netmask	Keepalive	Retry times	Interval	Fail Action
1	fff	Yes	PPP	120.42.46.98	192.168.5.0/24	200.200.200.1	200.200.200.5	255.255.255.0	No	0	0	Hold

[Refresh](#)
[Close](#)

3.3.5 Security

3.3.5.1 Firewall

You can enable or disable the firewall, filter specific Internet data types, and prevent anonymous Internet requests, ultimately enhance network security.

Firewall Protection

Firewall Protection

SPI Firewall
☒ Enable
☐ Disable

Firewall enhance network security and use SPI to check the packets into the network. To use firewall protection, choose to enable otherwise disabled. Only enable the SPI firewall, you can use other firewall functions: filtering proxy, block WAN requests, etc.

Additional Filters

Additional Filters

☐ Filter Proxy
☐ Filter Cookies
☐ Filter Java Applets
☐ Filter ActiveX

Filter Proxy: Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

Filter Cookies: Cookies are the website of data the data stored on your computer. When you interact with the site, the cookies will be used. Click the check box to enable the function otherwise disabled.

Filter Java Applets: If refuse to Java, you may not be able to open web pages using the Java programming. Click the check box to enable the function otherwise disabled.

Filter ActiveX: If refuse to ActiveX, you may not be able to open web pages using the ActiveX programming. Click the check box to enable the function otherwise disabled.

Prevent WAN Request

Block WAN Requests

☒ Block Anonymous WAN Requests (ping)
☒ Filter IDENT (Port 113)
☒ Block WAN SNMP access

Block Anonymous WAN Requests (ping): By selecting “Block Anonymous WAN Requests (ping)” box to enable this feature, you can prevent your network from the Ping or detection of other Internet users. so that make More difficult to break into your network. The default state of this feature is enabled, choose to disable allow anonymous Internet requests.

Filter IDENT (Port 113): Enable this feature can prevent port 113 from being scanned from outside. Click the check box to enable the function otherwise disabled.

Block WAN SNMP access: This feature prevents the SNMP connection requests from the WAN. After Complete the changes, click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

Impede WAN DoS/Bruteforce

Impede WAN DoS/Bruteforce

☐ Limit SSH Access
☐ Limit Telnet Access
☐ Limit PPTP Server Access
☐ Limit L2TP Server Access

Limit ssh Access: This feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit Telnet Access: This feature limits the access request from the WAN by Telnet, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Limit PPTP Server Access: When build a PPTP Server in the Router,this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP . Any new access request will be automatically dropped.

Limit L2TP Server Access: When build a L2TP Server in the Router, this feature limits the access request from the WAN by ssh, and per minute up to accept two connection requests on the same IP. Any new access request will be automatically dropped.

Log Management

The Router can keep logs of all incoming or outgoing traffic for your Internet connection.

Log

Log

☐ Enable
 ☒ Disable

Log: To keep activity logs, select Enable. To stop logging, select Disable. When select enable, the following page will appear.

Log

Log

☒ Enable
 ☐ Disable

Log Level

High

Options

Dropped

Disable

Rejected

Enable

Accepted

Enable

Log Level: Set this to the required log level. Set Log Level higher to log more actions.

Options: When select Enable, the corresponding connection will be recorded in the journal, the disabled are not recorded.

Incoming Log: To see a temporary log of the Router's most recent incoming traffic, click the Incoming Log button.

Incoming Log Table

Source IP	Protocol	Destination Port Number	Rule
<div>Refresh Close</div>			

Outgoing Log: To see a temporary log of the Router's most recent outgoing traffic, click the Outgoing Log button.

Outgoing Log Table

LAN IP	Destination URL/IP	Protocol	Service/Port Number	Rule
192.168.1.164	223.203.188.56	TCP	www	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted
192.168.1.164	112.95.240.183	UDP	8000	Accepted
192.168.1.164	183.60.49.245	UDP	8000	Accepted
192.168.1.164	119.147.32.204	UDP	8000	Accepted
192.168.1.164	112.90.86.244	UDP	8000	Accepted
192.168.1.164	119.147.45.157	UDP	8000	Accepted
192.168.1.164	183.60.49.15	UDP	8000	Accepted
192.168.1.164	183.60.16.70	UDP	8000	Accepted
192.168.1.164	183.60.16.200	UDP	8000	Accepted
192.168.1.164	183.60.48.60	UDP	8000	Accepted

Click the **Save Settings** button to save your changes. Click the **Cancel Changes** button to cancel unsaved changes.

3.3.6 Access Restrictions

3.3.6.1 WAN Access

Use access restrictions, you can block or allow specific types of Internet applications.

You can set specific PC-based Internet access policies.

Access Policy

Policy

1 ()

Delete

Summary

Status

☐ Enable
☒ Disable

Policy Name

PCs

Edit List of clients

☐ Deny
☒ Filter

Internet access during selected days and hours.

There are two options of "filter" and "deny" in the default policy rules. If you select "deny", you will deny specific computers from accessing any Internet service during a specific time period; if you select "filter", you will block specific computers from a specific time period

Access to a specific website; you can set 10 Internet access policies to filter the Internet services accessed by a specific PC during a specific time period.

Policy: You may define up to 10 access policies. Click Delete to delete a policy or Summary to see a summary of the policy.

Status: Enable or disable a policy.

Policy Name: You may assign a name to your policy.

PCs: The part is used to edit client list, the strategy is only effective for the PC in the list.

Days

Everyday	Sun	Mon	Tue	Wed	Thu	Fri	Sat
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Times

24 Hours
☒

From
☐

0:00

To

0:00

Days: Choose the day of the week you would like your policy to be applied.

Times: Enter the time of the day you would like your policy to be applied.

Website Blocking by URL Address

Website Blocking by Keyword

Website Blocking by URL Address: You can block access to certain websites by entering their URL.

Website Blocking by Keyword: You can block access to certain website by the keywords contained in their webpage

List of clients	
Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx	
MAC 01	00:AA:BB:CC:DD:EE
MAC 02	00:00:00:00:00:00
MAC 03	00:00:00:00:00:00
MAC 04	00:00:00:00:00:00
MAC 05	00:00:00:00:00:00
MAC 06	00:00:00:00:00:00
MAC 07	00:00:00:00:00:00
MAC 08	00:00:00:00:00:00
Enter the IP Address of the clients	
IP 01	192.168.1. 15
IP 02	192.168.1. 0
IP 03	192.168.1. 0
IP 04	192.168.1. 0
IP 05	192.168.1. 0
IP 06	192.168.1. 0
Enter the IP Range of the clients	
IP Range 01	192. 168. 1. 19 ~ 192. 168. 1. 30
IP Range 02	0. 0. 0. 0 ~ 0. 0. 0. 0

Set up Internet access policy

1. Select one from the "Internet Access Policy" drop-down menu.
2. To enable this policy, click the radio button next to "Enable".
3. Enter the policy name in the field provided.
4. Click the "Edit PC List" button, the "PC List" page appears, enter the PC to which the policy is applied, and you can use the MAC address or PC address to specify the PC. If you want this policy to be applied to a group of PCs, you can enter a group of IP address ranges. After completing the page modification, click "Save Settings" to save the changes, or click "Cancel Changes" to complete the modification. Then close this window.
5. Determine when this strategy will take effect. Select the specific date when this strategy takes effect or select "every day", and then enter the specific time range during which this strategy takes effect, or

select "24 hours".

6. If you deny or only allow access to websites with specific URL addresses, enter each URL address in a separate field next to "Website URL Address".

7. If you want to refuse or only allow access to websites with specific keywords, enter each keyword in a separate field in the narration of "Site Keywords".

8. Click the "Save Settings" button to save the social child of the strategy. If you want to cancel the settings of the strategy, click the "Cancel Changes" button.

Note:

1. The default policy rule factory value is "Filter". If the user selects the default policy rule as "Reject", edit the relevant policy to save or save the settings directly. If the strategy you edited is the first one, it will automatically become the second one after saving. If it is not the first one, it will be saved with the original number.

2. The communication management machine itself does not have a battery to keep the clock running. Turning off the communication management machine power or restarting the communication management machine will cause the communication management machine clock to temporarily fail. After the communication management machine fails, if the NTP time server cannot be automatically synchronized, the time needs to be recalibrated To ensure the correct execution of the relevant "control by time period" functions.

3.3.6.2 URL Filter

If you want to prevent certain client access to specific network domain name, such as www.sina.com. We can achieved it through the function of URL filter.

URL filtering function

Url Filter

Url Filter Setting

Enable Url Filter ☐ Enable ☒ Disable

Policy Discard packets conform to the following rules ▼

Del	Num	URL
<input type="checkbox"/>	1	www.sina.com

Add Filter Rule

Type URL ▼

Add

Discard packets conform to the following rules: only discard the matching URL address in the list .

Accept only the data packets conform to the following rules: receive only with custom rules of network address, discarded all other URL address.

3.3.6.3 Packet Filter

If you want to prevent certain data packets from entering the Internet through the communication management machine, or to prevent certain data packets from the Internet, you can implement filters.

Packet Filter



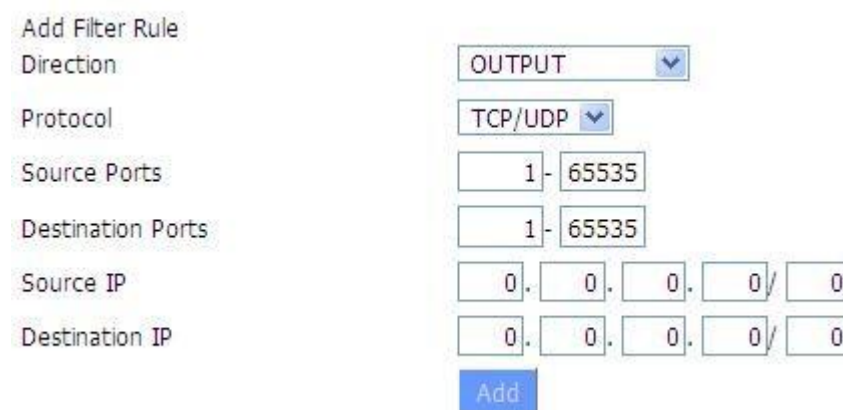
Enable Packet Filter: Enable or disable “packet filter” function

Policy: The filter rule’s policy, you can choose the following options

Discard The Following--Discard packets conform to the following rules, Accept all other packets

Only Accept The Following-- Accept only the data packets conform to the following rules, Discard all other packets

The custom packet filter rule list will list the packet filter rules that have been set. If you want to delete one of them, select the corresponding item, check the "Delete" button, and then click the "Save" button.



Add filter rules

Add custom packet filtering rules. "Source port", "Destination port", "Source address", "Destination address" must be filled in at least one item.

Direction

input: packet from WAN to LAN

output: packet from LAN to WAN

Protocol: packet protocol type

Source Ports: packet's source port **Destination Ports:** packet's destination port **Source IP:** packet's source IP address **Destination IP:** packet's destination IP address.

3.3.7 NAT

3.3.7.1 Port Forwarding

Port forwarding is used to set up public services on the network, such as web servers, ftp servers, or other dedicated internet applications (dedicated Internet applications refer to any applications that use internet access to use functions).

Forwards

Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
web	TCP	192.168.8.11	8000	192.168.1.12	80	<input checked="" type="checkbox"/>
ftp	Both	192.168.8.12	24	192.168.1.12	21	<input checked="" type="checkbox"/>

Application: Enter the name of the application in the field provided.

Protocol: Chose the right protocol TCP,UDP or Both. Set this to what the application requires.

Source Net: Forward only if sender matches this ip/net (example 192.168.1.0/24).

Port from: Enter the number of the external port (the port number seen by users on the Internet).

IP Address: Enter the IP Address of the PC running the application.

Port to: Enter the number of the internal port (the port number used by the application).

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.7.2 Port Range Forward

Port Range Forwarding allows you to set up public services on your network, such as web servers, ftp servers, e-mail servers, or other specialized Internet applications. Specialized Internet applications are any applications that use Internet access to perform functions such as videoconferencing or online gaming. When users send this type of request to your network via

the Internet, the F-DPU100 will forward those requests to the appropriate PC. If you only want to forward a single port, see Port Forwarding.

Port Range Forward

Forwards

Application	Start	End	Protocol	IP Address	Enable
web-tftp	800	8100	Both ▼	192.168.1.16	<input checked="" type="checkbox"/>
game	9000	10000	Both ▼	192.168.1.16	<input checked="" type="checkbox"/>

Add
Remove

Application: Enter the name of the application in the field provided.

Start: Enter the number of the first port of the range you want to be seen by users on the Internet and forwarded to your PC.

End: Enter the number of the last port of the range you want to be seen by users on the Internet and forwarded to your PC.

Protocol: Choose the right protocol TCP,UDP or Both. Set this to what the application requires.

IP Address: Enter the IP Address of the PC running the application.

Enable: Click the Enable checkbox to enable port forwarding for the application.

Check all values and click **Save Settings** to save your settings. Click the **Cancel changes** button to cancel your unsaved changes.

3.3.7.3 DMZ

The DMZ (DeMilitarized Zone) hosting feature allows one local user to be exposed to the Internet for use of a special-purpose service such as Internet gaming or videoconferencing. DMZ hosting forwards all the ports at the same time to one PC. The Port Forwarding feature is more secure because it only opens the ports you want to have opened, while DMZ hosting opens all the ports of one computer, exposing the computer so the Internet can see it.



The screenshot shows a configuration window titled "Demilitarized Zone (DMZ)". Inside the window, there is a section labeled "DMZ". Within this section, there is a "Use DMZ" checkbox and two radio buttons: "Enable" (which is selected) and "Disable". Below these controls, there is a "DMZ Host IP Address" field. The IP address "192.168.8.166" is entered into this field.

To enable the DMZ function, select Enable, and then enter the computer's IP address in the "DMZ host IP address" field.

After finishing the page modification, click the **"Save Settings"** button to save the changes, or click the **"Cancel Changes"** button to cancel the modification, the help information is on the right. For more information, click "More".

3.3.8 QoS Setting

3.3.8.1 Basis

Use the QoS function to limit the upload and download traffic respectively, and assign priority to a specific IP or MAC.

Uplink (kbps): In order to use bandwidth management (QoS) you must enter bandwidth values for your uplink. These are generally 80% to 90% of your maximum bandwidth.

Downlink (kbps): In order to use bandwidth management (QoS) you must enter bandwidth values for your downlink. These are generally 80% to 90% of your maximum bandwidth.

3.3.8.2 Classify

Netmask Priority

You may specify priority for all traffic from a given IP address or IP Range.

Priority description: The system provides five priority levels, among which the "unrestricted" priority level is independent of the other four priority levels. The other four priority levels are: high priority (Premium), priority (Express), Standard (Standard), low (Bulk).

Unrestricted: The bandwidth of the data stream at the unrestricted (Exempt) level is limited only by the hardware. The relationship between the unrestricted bandwidth and the other four priorities is as follows:

Suppose the total upload bandwidth is Max_Up, the total download bandwidth is Max_Down, the upload limit in "QOS Settings" is Uplink, the download limit is Downlink, and the flow rates of unrestricted data streams are Exempt_Rate_Up and Exempt_Rate_Do.

Then the total upload bandwidth of other priorities is: $\min(\text{Max_Up} - \text{Exempt_Rate_Up}, \text{Uplink})$;

The total download bandwidth for other priority levels is: $\min(\text{Max_Downlink} - \text{Exempt_Rate_Do}, \text{Downlink})$.

The remaining four priorities

After the unrestricted data stream is sent, the remaining bandwidth of the system is allocated by the remaining four priority data streams according to a certain proportion. Assume that the remaining upload bandwidth is 1000kbps, and the download is 1000kbps. At this time, there are four data streams, which have priority. The levels are high priority, priority, standard, and low. Then the upload and download bandwidths of each data stream are as follows:

High priority: $(75/100) * \text{Uplink}$; $(75/100) * \text{Downlink}$

Priority: $(15/100) * \text{Uplink}$; $(15/100) * \text{Downlink}$

Standard: $(10/100) * \text{Uplink}$; $(10/100) * \text{Downlink}$

Low: 1000bit (almost 0); 1000bit (almost 0);

For low priority, the upload and download rates are both 1000bit, and it is its turn when other priority data streams are sent;

When there is only one level of data stream, the bandwidth of the data stream is only limited by the upload and download restrictions in "QOS Settings";

Note: When a connection meets the control conditions in MAC priority and netmask priority at the same time, the rule added first shall prevail.

3.3.9 Applications

3.3.9.1 Serial Applications

The Console port of the communication management machine is usually used as a console. The Console port can also be configured as a common serial port, and the communication management machine has a built-in serial port to TCP/IP program. Through configuration, the console port of the communication management machine is used as a serial port protocol conversion device, or it is completely equivalent to a four-trust DTU device.

Serial Applications

Serial Applications ☒ Enable ☐ Disable

Baudrate 115200 ▼

Databit 8 ▼

Stopbit 1 ▼

Parity None ▼

Flow Control None ▼

Protocol TCP(DTU) ▼

Server Address 120.42.46.98

Server Port 55501

Device Number 12345678901

Device Id 12345678

Heartbeat Interval 60

Baudrate: Baud rate indicates the number of bytes per second transported by device, commonly used baud rate is 115200, 57600, 38400, 19200.

Databit: the data bits can be 4, 5, 6, 7, 8, constitute a character. The ASCII code is usually used. Starting from the most significant bit is transmitted.

Stopbit: it marks the end of a character data. It is a high level of 1, 1.5, 2.

Parity: use a set of data to check the data error.

Flow control: including the hardware part and software part in two ways.

Protocol Type

UDP(DTU): Data transmit with UDP protocol, work as a Four-Faith IP client. server.

MODEM device which has application protocol and hear beat mechanism.

Pure UDP: Data transmit with standard UDP protocol.

TCP(DTU): Data transmit with TCP protocol, work as a Four-Faith P MODEM device which has application protocol and hear beat mechanism.

Pure TCP: Data transmit with standard TCP protocol, F-DPU100 is the

TCP Server: Data transmit with standard TCP protocol, F-DPU100 is the TCST -- Data transmit with TCP protocol, Using a custom data

Server Address: The data service center's IP Address or domain name.

Server Port: The data service center's listening port.

Device ID: The F-DPU100's identity ID.

Device Number: The F-DPU100's phone number.

Heartbeat Interval: The time interval to send heart beat packet. This item is valid only when you choose UDP(DTU) or TCP(DTU) protocol type.

TCP Server Listen Port: This item is valid when Protocol Type is “TCP Server”

Custom Heartbeat Packet : This item is valid when Protocol Type is “TCST” Custom

Registration Packets: This item is valid when Protocol Type is “TCST”

3.3.9.2 Communication Gateway

Communication management

Communication management ☒ Enable ☐ Disable

Select Channel

Select Channel 1 ▾

Com Enable ☒ Enable ☐ Disable

Acquisition service

Acquisition service ☒ Enable ☐ Disable

Protocol Modbus RTU ▾

Byte Order small end ▾

Acq intv(s) 40

Retransmission timeout(s) 10

Retransmission times 3

Modbus Configure

SN	Slave Address	Data Name	Function code	Start Addr	Count	Data Type	Delete
1	1	chn0.mdb.s.coil	1	100	32	bit ▾	Delete
2	1	chn0.mdb.s.disc	2	200	24	bit ▾	Delete
3	1	mdbs.hold	3	300	4	short ▾	Delete
4	1	chn0.mdb.s.input	4	400	4	short ▾	Delete
5	2	chn0.dev2.coil	1	100	32	bit ▾	Delete

Add

Port TCP Client ▾

Server Addr 192.168.7.127

Server Port 502

Data service

Data service ☐ Enable ☒ Disable

Save

Apply

Select Channel:Select the channels that need to be used, each of which can be used as a collection service or a data service mode.

Baudrate	115200 ▼
Databit	8 ▼
Stopbit	1 ▼
Parity	None ▼
Flow Control	None ▼

Port description

Whether to enable: Control whether the serial port is enabled.

Use serial ports: There are a total of four serial ports available.

Baud rate: indicates the number of bytes transmitted by the device per second. Commonly used baud rates are 115200, 57600, 38400, 19200, etc.

Data bits: The number of data bits can be 4, 5, 6, 7, 8, etc. to form a character. ASCII code is usually used. Start transmission from the lowest bit and locate by clock.

Stop bit: It is the end sign of a character data. It can be a high level of 1 bit, 1.5 bits, and 2 bits.

Inspection: indicates the data error checking method adopted by a group of data. There are two ways of parity check.

Flow control: It includes two methods: hardware part and software part.

Port	TCP Client ▼
Server Addr	192.168.7.127
Server Port	502

Server address: The IP address or domain name of the data service center that communicates with the communication management machine serial port to TCP program.

Server port number: the port that the data service center program listens to.

Listening port: The device acts as the monitoring port of the data service center program.

Port	UDP ▼
Server Addr	
Server Port	

Working mode: There are two main types, collection service and data service.

Collection service: collect information from connected devices.

Data service: The device acts as a slave or server to provide collected information.

Protocol: The protocol used for communication between devices. The supported protocols are: modbus RTU, modbus ASCII, Modbus TCP, bacnet mstp, bacnet BIP, IEC101, IEC104.

Work Mode	Acquisition service ▼
Acquisition service	
Acquisition service	<input type="radio"/> Enable <input type="radio"/> Disable
Protocol	Modbus TCP ▼
Byte Order	small endian ▼
Acq intv(ms)	<input type="text"/>
Retransmission timeout(ms)	<input type="text"/>
Retransmission times	<input type="text"/>

Description of the Modbus protocol

Slave address: the address of the device that needs to be accessed. (0~255).

Data name: Create data points for interconversion between different protocols.

Read coils (function code 1): Each bit in the response message is divided into a coil according to each bit in the data domain. The indicated state is 1= ON and 0= OFF. The LSB (minimum valid bit) of the first data byte includes the addressable output in the query. The other coils are analogous in turn, until the high end of the byte, and the order from the low to the high in the subsequent bytes. If the number of outputs returned is not a multiple of eight, the remaining bits in the last data bytes will be filled with zero (all the way to the high end of the byte). The number of bytes explains the complete number of bytes of the data.

Read discrete quantity (function code 2): according to each bit of the data domain, the input of the discrete quantity input in the response message is divided into one input. The indicated state is 1= ON and 0= OFF. The LSB (minimum valid bit) of the first data byte includes the input that is addressed in the inquiry. The other inputs are analogous in turn, until the high end of the byte, and the order from the low to the high in the subsequent bytes. If the number of inputs returned is not a multiple of eight, the remaining bits in the final data bytes will be filled with zero (all the way to the high end of the byte). The number of bytes explains the complete number of bytes of the data. Read hold register(the function code is 3: in a remote device that uses this function code to read the content of the continuous block of the hold register.

Read input register (function code 4): in a remote device, the function code is used to read the content of the continuous block of the input register.

Start address: the start address of the register.

Quantity: the number of registers

Protocol	Bacnet BIP ▼
MSTP MAC(0~254)	<input type="text"/>
Device Number(0~2^32)	<input type="text"/>

BACTNE

MSTP MAC:the address of the device that needs to be accessed. (0~255).

Device Number:Indicate the number of the device.

The IEC power agreement

Protocol	IEC60870_5_101 ▼
Link Addr	<input type="text"/>
Common Address	<input type="text"/>
Reson Byte Length	1 ▼
ASDU Common Addr Length	1 ▼
Infomation Addr Length	1 ▼
Time period(s)	<input type="text"/>
Fullcall cycle(s)	<input type="text"/>
Usr2call cycle(s)	<input type="text"/>
Electricity Call cycle(s)	<input type="text"/>
Link Test cycle(s)	<input type="text"/>
T1(104)	<input type="text"/>
T2(104)	<input type="text"/>
T3(104)	<input type="text"/>
Retransmission timeout(s)	<input type="text"/>
Retransmission times	<input type="text"/>

Link Addr:Used for equipment addressing.

Common address:The same as the link address, as the terminal address.

Reson Byte Length:The 101 protocol is generally 1 bytes, and the 104 protocol is generally 2 bytes.

ASDU Common Addr Length:The 101 protocol is generally 1 bytes, and the 104 protocol is generally 2 bytes.

Infomation Addr Length:The 101 protocol is generally 2 bytes, and the 104 protocol is generally 3 bytes.

Time period:The period of clock synchronization between the main station and the sub station. Fullcall cycle:After the call control station is initialized, the control station must obtain all the state signals of the field equipment and all the analog data.

Usr2call cycle:Teleconnection and telemetry are usually circulatory.

Electricity Call cycle: Get data tiring regularly.

Link Test cycle:When the link does not interact with the data, it is necessary to send the link test message regularly to see if the detection link is disconnected.

T1: control message confirms the timeout and sends the test frame.

T2:The monitoring message responds to the timeout, sending the S confirmation frame.

T3:Long time idle timeout, send test frames.

Retransmission timeout:The timeout time of the message is repeated.

Retransmission times:The number of times the message is re sent.

Device management											
SN	Device Number	Device Number	Device Type	Telesignalling count	undefined	Remote control count	Pluse count	Telesignalling flag	Telemetry flag	Pulse flag	Delete
1	001	1									Delete

Add

Collection content					
SN	Device Number	Collection Address	Collection Type	Data Name	Delete
1	1 ▼		Telemetry ▼		Delete

Add

Device management: add configuration of terminal equipment, can be configured as well as queries, these parameters include the number of devices, the device address, type of equipment, a number of remote communication, remote control number, to measure the number of pulses, telesignalling telemetry flag, flag, flag pulse.

Collection of content: create data points and relate to the device.

UDP: Standard serial port to UDP connection.

Data service

The configuration items of the data service part are roughly the same as the collection part, mainly providing forwarding data services.

Protocol: The protocol used for communication between devices. The supported protocols are: modbus RTU, modbus ASCII, Modbus TCP, bacnet mstp, bacnet BIP, IEC101, IEC104.

Modbus protocol part

Data service

Data service
☒ Enable
☐ Disable

Protocol
Modbus RTU

Slave Address
2

Data Configure					
SN	Data Address	Data Name	Function code	Data Value	Delete
1	2000	chn0.mdb.s.coil	Read Coils	bit	Delete
2	3000	chn0.mdb.s.disc	Read Discrete	bit	Delete
3	4000	chn0.mdb.s.coil	Read Hold	short	Delete
4	5000	chn0.mdb.s.input	Read Input	short	Delete

Add

Port
TCP Server

Listening Port
2404

Data configuration items: mainly related to data points according to different function codes of Modbus protocol. The main configuration items are data address (Modbus starting address), data name (that is, point to provide collection), function code, and data type.

IEC protocol part

Data service ☒ Enable ☐ Disable

Protocol IEC60870_5_101 ▼

Link Addr 2

Reson Byte Length 1 ▼

ASDU Common Addr Length 2 ▼

Infomation Addr Length 3 ▼

Link Test cycle(s) 30

Common Address 2

T1(104) 20

T2(104) 20

T3(104) 30

Data Configure					
SN	Data Address	Data Name	Data Type	Data Value	Delete
1	2000	chn0.mdb.s.coil ▼	Telesignalling ▼	bit ▼	Delete
2	2001	chn0.mdb.s.coil ▼	Telesignalling ▼	bit ▼	Delete
3	2002	chn0.mdb.s.coil ▼	Telesignalling ▼	bit ▼	Delete
4	2003	chn0.mdb.s.coil ▼	Telesignalling ▼	bit ▼	Delete
5	1000	mdbs.hold ▼	Telemetry ▼	short ▼	Delete
6	1001	mdbs.hold ▼	Telemetry ▼	short ▼	Delete
7	1002	mdbs.hold ▼	Telemetry ▼	short ▼	Delete
8	1003	mdbs.hold ▼	Telemetry ▼	short ▼	Delete
9	3000	chn0.mdb.s.input ▼	Electric pulse ▼	int ▼	Delete
10	3001	chn0.mdb.s.input ▼	Electric pulse ▼	int ▼	Delete
11	2004	chn0.dev2.coil ▼	Telesignalling ▼	bit ▼	Delete
12	2005	chn0.dev2.coil ▼	Telesignalling ▼	bit ▼	Delete

Public address: Same as the link address, it is the terminal address.

Send reason byte length: 101 protocol is generally 1 byte, 104 protocol is generally 2 bytes.

ASDU public address byte length: 101 protocol is generally 1 byte, 104 protocol is generally 2 bytes.

Message body byte length: The 101 protocol is generally 2 bytes, and the 104 protocol is generally 3 bytes.

Link test cycle: When there is no data exchange on the link, it is necessary to send link test messages regularly to detect whether the link is disconnected.

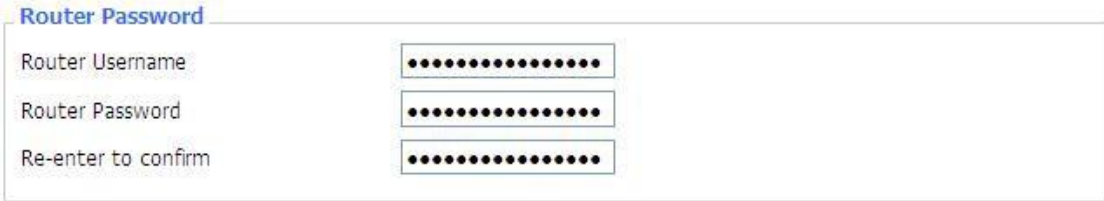
Data configuration: used to create a point table, configure the message body address, associate

forwarding data, and configure frame types and data types.

3.3.10 Administration

3.3.10.1 Management

The Management screen allows you to change the F-DPU100's settings. On this page you will find most of the configurable items of the F-DPU100 code.



The image shows a web form titled "Router Password". It contains three input fields, each with a masked password (dots): "Router Username", "Router Password", and "Re-enter to confirm".

The new password must not exceed 32 characters in length and must not include any spaces.

Enter the new password a second time to confirm it.

Note:

Default username is admin.

It is strongly recommended that you change the factory default password of the F-DPU100, which is admin. All users who try to access the F-DPU100's web-based utility or Setup Wizard will be prompted for the F-DPU100's password.

Web Access



The image shows a web form titled "Web Access". It contains four settings: "Protocol" with checkboxes for "HTTP" (checked) and "HTTPS"; "Auto-Refresh (in seconds)" with a text box containing "3"; "Enable Info Site" with radio buttons for "Enable" (selected) and "Disable"; and "Info Site Password Protection" with a checkbox for "Enabled".

This feature allows you to manage the F-DPU100 using either HTTP protocol or the HTTPS protocol. If you choose to disable this feature, a manual reboot will be required. You can also activate or not the F-DPU100 information web page. It's now possible to password protect this page (same username and password than above).

Protocol: This feature allows you to manage the F-DPU100 using either HTTP protocol or the HTTPS protocol

Auto-Refresh: Adjusts the Web GUI automatic refresh interval. 0 disables this feature completely

Enable Info Site: Enable or disable the login system information page

Info Site Password Protection : Enable or disable the password protection feature of the system information page

Remote Access

Web GUI Management	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Use HTTPS	<input type="checkbox"/>	
Web GUI Port	<input type="text" value="8080"/>	(Default: 8080, Range: 1 - 65535)
SSH Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
SSH Remote Port	<input type="text" value="22"/>	(Default: 22, Range: 1 - 65535)
Telnet Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	

Web interface management: This feature allows you to manage the F-DPU100 from a remote location, via the Internet. To disable this feature, keep the default setting, Disable. To enable this feature, select Enable, and use the specified port (default is 8080) on your PC to remotely manage the F-DPU100. You must also change the F-DPU100's default password to one of your own, if you haven't already. To remotely manage the F-DPU100, enter `http://xxx.xxx.xxx.xxx:8080` (the x's represent the F-DPU100's Internet IP address, and 8080 represents the specified port) in your web browser's address field. You will be asked for the F-DPU100's password.

If you use https you need to specify the url as `https://xxx.xxx.xxx.xxx:8080` (not all firmwares does support this without rebuilding with SSL support).

SSH Management: You can also enable SSH to remotely access the F-DPU100 by Secure Shell. Note that SSH daemon needs to be enable in Services page.

Warning:

If the Remote F-DPU100 Access feature is enabled, anyone who knows the F-DPU100's Internet IP address and password will be able to alter the F-DPU100's settings.

Telnet Management: Enable or disable remote Telnet function

Cron

Cron	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Additional Cron Jobs	<input type="text"/>

Cron: The cron subsystem schedules execution of Linux commands. You'll need to use the command line or startup scripts to actually use this.

Language Selection

Language	<input type="text" value="English"/>
----------	--------------------------------------

Language: Set up the F-DPU100 page shows the type of language, including simplified Chinese and English.

Device Management

Device Management ☒ Enable ☐ Disable

Device Management Server IP

Device Management Server Listen Port (Default: 40001, Range: 1 - 65535)

Heart Interval (Default: 60Sec, Range: 1 - 999)

Device Number

Device Phone Number

Device Type Description

Remote Upgrade: custom-developed remote management server for this station F-DPU100 monitoring and management, configuration parameters, WIFI advertising updates.

3.3.10.2 Keep Alive

Schedule Boot&Shutdown

Schedule Boot&Shutdown

Schedule Boot&Shutdown ☒ Enable ☐ Disable

Match ☒ Day ☐ Weekday ☐ Days ☐ Weekdays

Shutdown Time

Shutdown Date

Boot Time

Boot Date

The user can set the startup or shutdown time:

For example, the user wants to set the start time at 8:07 and boot time at 9:07.

Schedule Boot&Shutdown

Schedule Boot&Shutdown ☒ Enable ☐ Disable

Match ☒ Day ☐ Weekday ☐ Days ☐ Weekdays

Shutdown Time

Shutdown Date

Boot Time

Boot Date

Schedule Reboot

Schedule Reboot

Schedule Reboot ☒ Enable ☐ Disable

Interval (in seconds) ☒

At a set Time ☐ :

You can schedule regular reboots for the F-DPU100 :

Regularly after xxx seconds.

At a specific date time each week or everyday.

Note:

For date based reboots Cron must be activated. See Management for Cron activation.

3.3.10.3 Commands

Commands: You are able to run command lines directly via the Webinterface.

Command Shell

Commands

Run Commands
Save Startup
Save Shutdown
Save Firewall

Save Custom Script

Run Command: You can run command lines via the web interface. Fill the text area with your command and click Run Commands to submit.

Startup: You can save some command lines to be executed at startup's F-DPU100. Fill the text area with commands (only one command by row) and click Save Startup.

Shutdown: You can save some command lines to be executed at shutdown's F-DPU100. Fill the text area with commands (only one command by row) and click Save Shutdown.

Firewall: Each time the firewall is started, it can run some custom iptables instructions. Fill the text area with firewall's instructions (only one command by row) and click Save Firewall.

Custom Script: Custom script is stored in /tmp/custom.sh file. You can run it manually or use cron to call it. Fill the text area with script's instructions (only one command by row) and click Save Custom Script.

3.3.10.4 Factory Defaults

Factory Defaults

Reset router settings

Restore Factory Defaults ☐ Yes ☒ No

Restore factory defaults Click the "Yes" button and save the settings, reset all configurations to factory defaults. When you restore to the default settings, all settings you made will be lost. The default configuration of this feature is "No". For more information, please click "More"

3.3.10.5 Firmware Upgrade



The Firmware Upgrade interface includes a title bar 'Firmware Upgrade'. Below it, there is a label 'After flashing, reset to' followed by a dropdown menu currently set to 'Don't reset'. Underneath, a label 'Please select a file to upgrade' is followed by a file selection input field and a '浏览...' (Browse...) button.

Firmware upgrade: new firmware can be loaded onto the communication management machine. The new firmware version will be posted on www.four-faith.com

It can be downloaded for free. If there is no problem with the communication manager, there is no need to download the updated firmware version unless

The new version contains the new features you want to use.

Note: When upgrading the firmware of the communication management machine, its configuration settings may be lost. Therefore, please ensure that before upgrading the firmware,

Back up the setting information of the communication management machine first.

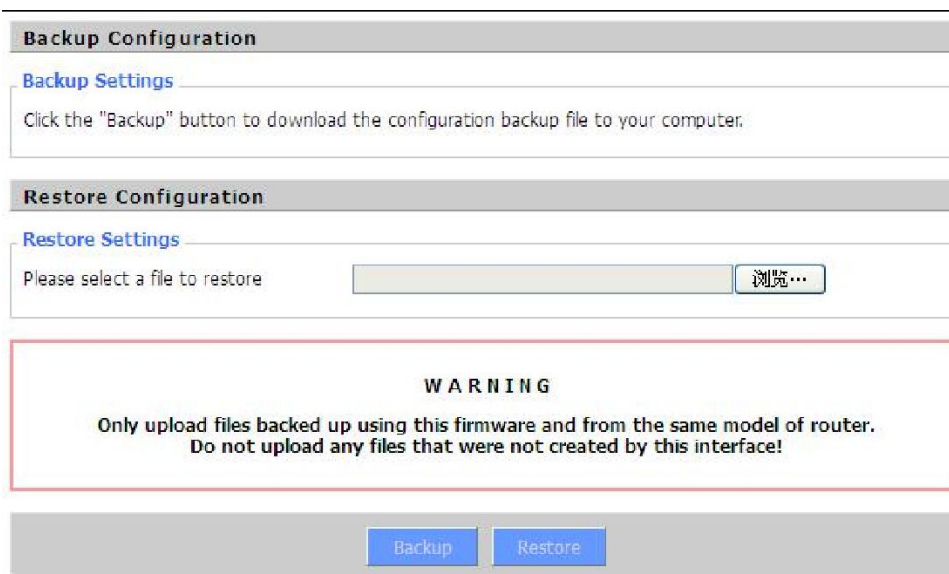
After refreshing, reset to: If you want to reset the default settings of the firmware version of the communication management machine after the upgrade, please click the preset settings option.

Click Browse: select the firmware file to be upgraded, and then click the upgrade button to start the firmware upgrade. It costs money to upgrade the firmware

For a few minutes, please do not turn off the power or press the reset button.

3.3.10.6 BackUP

This page is used to backup or restore the configuration file of the communication management machine.



The interface is divided into two main sections: 'Backup Configuration' and 'Restore Configuration'. The 'Backup Configuration' section has a 'Backup Settings' link and a text instruction: 'Click the "Backup" button to download the configuration backup file to your computer.' The 'Restore Configuration' section has a 'Restore Settings' link, a label 'Please select a file to restore', a file selection input field, and a '浏览...' (Browse...) button. Below these sections is a red-bordered warning box with the text: 'WARNING Only upload files backed up using this firmware and from the same model of router. Do not upload any files that were not created by this interface!'. At the bottom, there are two buttons: 'Backup' and 'Restore'.

If you want to back up the configuration file of the communication management machine, click the "**Backup**" button. After that, follow the instructions on the screen.

If you want to restore the configuration file of the communication management machine, click the "**Browse**" button. After you find the backup file, follow the instructions on the screen. Select the backup file and click the "**Restore**" button.

3.3.11 Status

3.3.11.1 F-DPU110

System	
Router Name	Four-Faith
Router Model	Four-Faith Router
Firmware Version	FXXXX v1.0 (01/10/12) std - build 94
MAC Address	<u>00:AA:BB:CC:DD:44</u>
Host Name	
WAN Domain Name	
LAN Domain Name	
Current Time	Sat, 01 Jan 2000 00:51:29
Uptime	51 min,

F-DPU110 Name: name of the F-DPU110, setting→basic setting to modify

F-DPU110 Model: model of the F-DPU110, unavailable to modify

Firmware Version: software version information

MAC Address: MAC address of WAN, setting→Clone MAC Address to modify

Host Name: host name of the F-DPU110, setting→basic setting to modify

WAN Domain Name: domain name of WAN, setting→basic setting to modify

LAN Domain Name: domain name of LAN, unavailable to modify

Current Time: local time of the system

Uptime: operating uptime as long as the system is powered on

Communication gateway

Communication gateway status		Enabled			
Channel SN	Work mode	Collection service	Data service	Protocol type	Connection status
1	Disabled	None	Modbus TCP	DisConnected	
2	Disabled	None		DisConnected	
3	Disabled	None		DisConnected	
4	Disabled	None		DisConnected	
5	Disabled	None		DisConnected	
6	Disabled	None		DisConnected	
7	Disabled	None		DisConnected	
8	Disabled	None		DisConnected	
9	Disabled	None		DisConnected	

Work mode: channel enabled or disabled

Collection service: Show collection service on or off

Data service: show data service on or off

Communication protocol: show the communication protocol

Connection state: show the state of connection

Memory

Total Available	125192 kB / 131072 kB	<div><div></div></div> 96%
Free	94884 kB / 125192 kB	<div><div></div></div> 76%
Used	30308 kB / 125192 kB	<div><div></div></div> 24%
Buffers	3412 kB / 30308 kB	<div><div></div></div> 11%
Cached	11936 kB / 30308 kB	<div><div></div></div> 39%
Active	10528 kB / 30308 kB	<div><div></div></div> 35%
Inactive	6512 kB / 30308 kB	<div><div></div></div> 21%

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the F-DPU110 will reboot if the memory is less than 500kB

Used: used memory, total available memory minus free memory

Buffers: used memory for buffers,

Cached: the memory used by high-speed cache memory

Active: active use of buffer or cache memory page file size

Inactive: not often used in a buffer or cache memory page file size

Network

IP Filter Maximum Ports	4096	
Active IP Connections	43	<div><div></div></div> 1%

IP Filter Maximum Ports: preset is 4096, available to re-management

Active IP Connections: real time monitor active IP connections of the system, click to see the table as blow:

Active IP Connections

53

No.	Protocol	Timeout (s)	Source Address	Remote Address	Service Name	State
1	TCP	60	192.168.1.120	192.168.1.1	80	TIME_WAIT
2	TCP	30	192.168.1.120	192.168.1.1	80	TIME_WAIT
3	TCP	65	192.168.1.120	192.168.1.1	80	TIME_WAIT
4	TCP	96	192.168.1.120	192.168.1.1	80	TIME_WAIT
5	TCP	99	192.168.1.120	192.168.1.1	80	TIME_WAIT
6	TCP	70	192.168.1.120	192.168.1.1	80	TIME_WAIT
7	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
8	TCP	115	192.168.1.120	192.168.1.1	80	TIME_WAIT
9	TCP	84	192.168.1.120	192.168.1.1	80	TIME_WAIT
10	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
11	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
12	TCP	108	192.168.1.120	192.168.1.1	80	TIME_WAIT
13	TCP	3600	192.168.1.120	192.168.1.1	80	ESTABLISHED
14	TCP	93	192.168.1.120	192.168.1.1	80	TIME_WAIT
15	TCP	102	192.168.1.120	192.168.1.1	80	TIME_WAIT
16	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
17	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
18	TCP	15	192.168.1.120	192.168.1.1	80	TIME_WAIT
19	TCP	25	192.168.1.120	192.168.1.1	80	TIME_WAIT
20	TCP	90	192.168.1.120	192.168.1.1	80	TIME_WAIT
21	UDP	26	192.168.8.119	255.255.255.255	1947	UNREPLIED
22	TCP	77	192.168.1.120	192.168.1.1	80	TIME_WAIT
23	TCP	35	192.168.1.120	192.168.1.1	80	TIME_WAIT
24	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
25	TCP	40	192.168.1.120	192.168.1.1	80	TIME_WAIT
26	TCP	3599	192.168.1.120	192.168.1.1	80	ESTABLISHED
27	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
28	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT
29	TCP	4	192.168.1.120	192.168.1.1	80	TIME_WAIT
30	UDP	31	192.168.8.160	224.0.0.1	9166	UNREPLIED
31	TCP	74	192.168.1.120	192.168.1.1	80	TIME_WAIT

Active IP Connections: total active IP connections

Protocol: connection protocol

Timeouts: connection timeouts, unit is second

Source Address: source IP address

Remote Address: remote IP address

Service Name: connecting service port

Status: displayed status

3.3.11.2 WAN

Connection Type Automatic Configuration - DHCP

Connection Uptime Not available

Connection Type: disabled, static IP, automatic configuration-DHCP, PPPOE, PPTP, L2TP, 3G/UMTS

Connection Uptime: connecting uptime; If disconnect, display Not available

IP Address	0.0.0.0
Subnet Mask	0.0.0.0
Gateway	0.0.0.0
DNS 1	
DNS 2	
DNS 3	

IP Address: IP address of F-DPU110 WAN

Subnet Mask: subnet mask of F-DPU110 WAN

Gateway: the gateway of F-DPU110 WAN

DNS1, DNS2, DNS3: DNS1/DNS2/DNS3 of F-DPU110 WAN

Remaining Lease Time	0 days 23:38:43
<div><div>DHCP Release</div><div>DHCP Renew</div></div>	

Remaining Lease Time: remaining lease time of IP address in DHCP way

DHCP Release: release DHCP address

DHCP Renew: renew IP address in DHCP way, default is 1 day

Login Status	Disconnected	<div>Connect</div>
--------------	--------------	--------------------

Login Status: connection status of WAN

Disconnection: disconnect

Connection: connect

Module Type	ZTE-EVDO MODULE
<div><div><div></div><div></div><div></div><div></div><div></div></div></div>	
Signal Status	-79 dBm
Network	CDMA/HDR

Module Type: module type in 3G/UMTS way

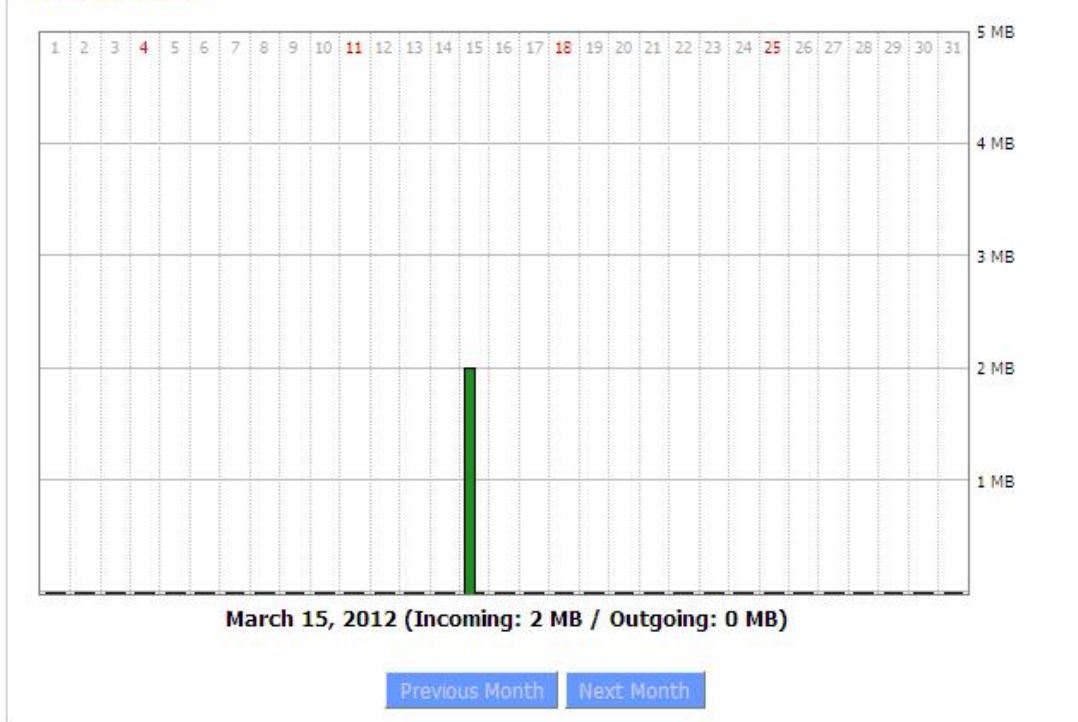
Signal Status: signal intensity of the module in 3G/UMTS way

Network: network type of the module in 3G/UMTS way

Total Traffic

Incoming (MBytes)	0
Outgoing (MBytes)	0

Traffic by Month



Total Flow: flow from power-off last time until now statistics, download and upload direction

Monthly Flow: the flow of a month, unit is MB

Last Month: the flow of last month

Next Month: the flow of next month

Data Administration

Backup Restore Delete

Backup: backup data administration

Restore: restore data administration

Delete: delete data administration

3.3.11.3 LAN

LAN Status

MAC Address	<u>00:0C:43:30:52:77</u>
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

MAC Address: MAC Address of the LAN port ethernet

IP Address: IP Address of the LAN port

Subnet Mask: Subnet Mask of the LAN port

Gateway: Gateway of the LAN port

Local DNS: DNS of the LAN port

Active Clients

Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.1.120	<u>10:78:D2:98:C9:46</u>	57	1%

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Conn. Count: connection count caused by the client

Ratio: the ratio of 4096 connection

Dynamic Host Configuration Protocol

DHCP Status

DHCP Server	Enabled
DHCP Daemon	uDHCpd
Start IP Address	192.168.1.100
End IP Address	192.168.1.149
Client Lease Time	1440 minutes

DHCP Server: enable or disable the F-DPU110 work as a DHCP server




DHCP Daemon: the agreement allocated using DHCP including DNSMasq and uDHCpd

Starting IP Address: the starting IP Address of the DHCP server's Address pool

Ending IP Address: the ending IP Address of the DHCP server's Address pool

Client Lease Time: the lease time of DHCP client

DHCP Clients

Host Name	IP Address	MAC Address	Client Lease Time	Delete
PC-201011161332	192.168.1.142	<u>00:21:5C:33:4D:29</u>	1 day 00:00:00	
jack-lincw	192.168.1.117	<u>44:37:E6:3F:45:54</u>	1 day 00:00:00	
*	192.168.1.149	<u>00:0C:E7:00:00:00</u>	1 day 00:00:00	

Host Name: host name of LAN client

IP Address: IP address of the client

MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

Delete: click to delete DHCP client

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

Interface: the interface assigned by dial-up system

User Name: user name of PPPoE client

Local IP: IP address assigned by PPPoE client

Delete: click to delete PPPoE client

Connected L2TP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local L2TP

Remote IP: tunnel IP address of L2TP server

Delete: click to disconnect L2TP

Connected L2TP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.50.2	120.42.46.98	

Interface: the interface assigned by dial-up system

User Name: user name of the client

Local IP: tunnel IP address of L2TP client

Remote IP: IP address of L2TP client

Delete: click to delete L2TP client

Connected PPTP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	


Interface: the interface assigned by dial-up system

Local IP: tunnel IP address of local PPTP

Remote IP: tunnel IP address of PPTP server

Delete: click to disconnect PPTP

Connected PPTP Clients

Interface	User Name	Local IP	Remote IP	Delete
ppp1	hometest	192.168.5.1	120.42.46.98	

Interface: the interface assigned by dial-up system

User Name: user name of the client

Local IP: tunnel IP address of PPTP client

Remote IP: IP address of PPTP client

Delete: click to delete PPTP client

3.3.11.4 Wireless

Wireless Status

MAC Address	00:0C:43:30:52:79
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	four-faith
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s
Encryption - Interface w10	Disabled
PPTP Status	Disconnected

MAC Address: MAC address of wireless client

Radio: display whether radio is on or not

Mode: wireless mode

Network: wireless network mode

SSID: wireless network name

Channel: wireless network channel

TX Power: reflection power of wireless network

Rate: reflection rate of wireless network

Encryption-Interface w10: enable or diasbal Encryption-Interface w10

PPTP Status: show wireless pptp status

Wireless Packet Info

Received (RX)	91125 OK, no error	100%
Transmitted (TX)	11957 OK, no error	100%

Received (RX): received data packet

Transmitted (TX): transmitted data packet

Wireless Nodes

Clients

MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

Neighbor's Wireless Networks

SSID	Mode	MAC Address	Channel	Rssi	Noise	beacon	Open	dtim	Rate	Join Site
tzt-3g	Unknown	00:aa:bb:cc:dd:14	2	-5	-95	0	No	0	54(b/g)	Join
four-faith	Unknown	00:0c:43:30:52:79	6	-24	-95	0	No	0	300(b/g/n)	Join
ff-old	AP	00:13:10:09:56:92	6	-55	-95	0	No	0	54(b/g)	Join

Refresh

Close

Neighbor's Wireless Network: display other networks nearby

SSID: the name of wireless network nearby

Mode: operating mode of wireless network nearby

MAC Address: MAC address of the wireless nearby

Channel: the channel of the wireless nearby

Rssi: signal intensity of the wireless nearby

Noise: the noise of the wireless nearby

Beacon: signal beacon of the wireless nearby

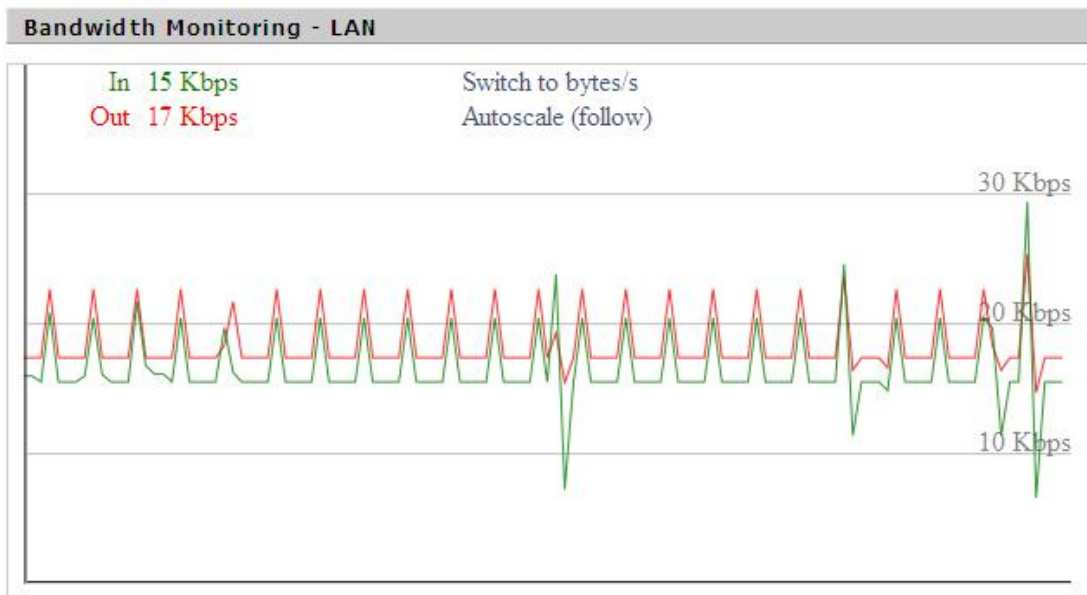
Open: the wireless nearby is open or not

Dtim: delivery traffic indication message of the wireless nearby

Rate: speed rate of the wireless nearby

Join Site: click to join wireless network nearby

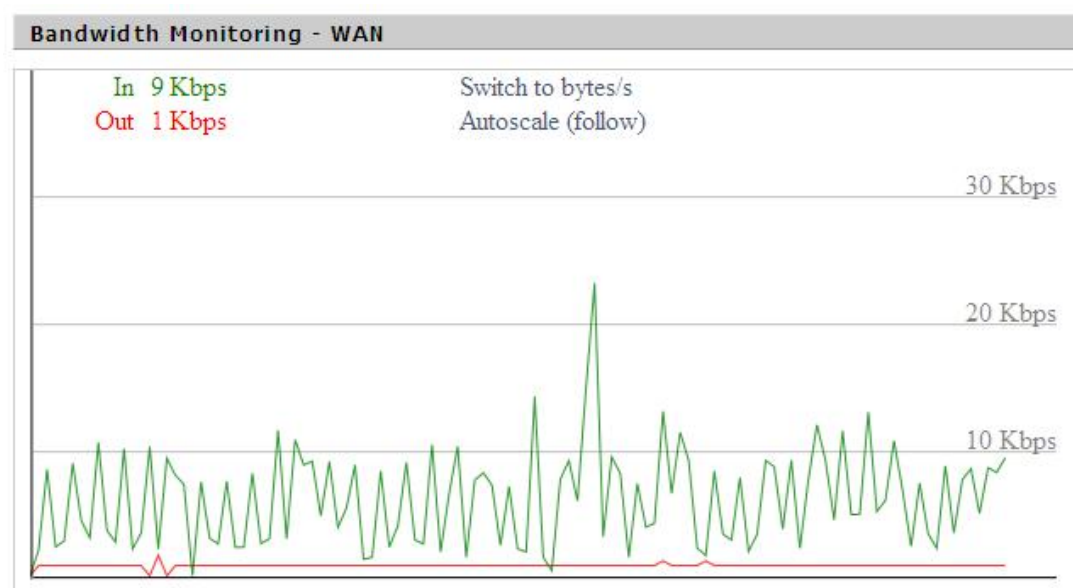
3.3.11.5 Bandwidth



Bandwidth Monitoring-LAN Graph

abscissa axis: time

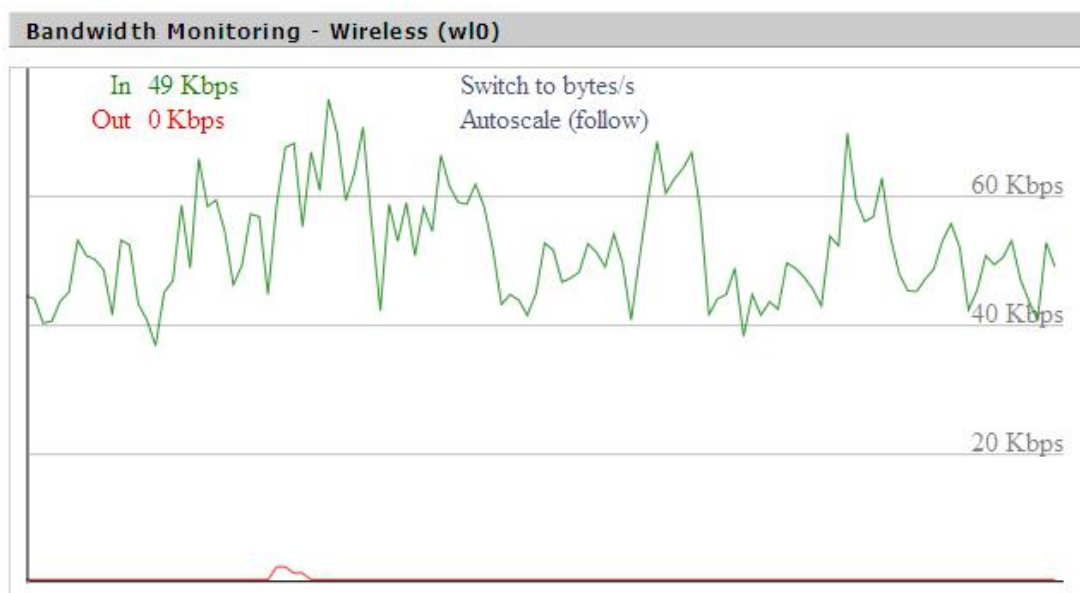
vertical axis: speed rate



Bandwidth Monitoring-WAN Graph

abscissa axis: time

vertical axis: speed rate



Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

3.3.11.6 Sys-Info

Router	
Router Name	Four-Faith
Router Model	Four-Faith Router
LAN MAC	<u>00:0C:43:30:52:77</u>
WAN MAC	<u>00:0C:43:30:52:78</u>
Wireless MAC	<u>00:0C:43:30:52:79</u>
WAN IP	10.34.107.156
LAN IP	192.168.1.1

F-DPU110 Name: the name of the F-DPU110

F-DPU110 Model: the model of the F-DPU110

LAN MAC: MAC address of LAN port

WAN MAC: MAC address of WAN port

Wireless MAC: MAC address of the wireless

WAN IP: IP address of WAN port

LAN IP: IP address of LAN port

Wireless	
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	four-faith
Channel	6 (2437 MHz)
TX Power	71 mW
Rate	72 Mb/s

Radio: display whether radio is on or not

Mode: wireless mode

Network: wireless network mode

SSID: wireless network name

Channel: wireless network channel

TX Power: reflection power of wireless network

Rate: reflection rate of wireless network

Wireless Packet Info	
Received (RX)	6982 OK, no error
Transmitted (TX)	1498 OK, no error

Received (RX): received data packet

Transmitted (TX): transmitted data packet

Wireless								
Clients								
MAC Address	Interface	Uptime	TX Rate	RX Rate	Signal	Noise	SNR	Signal Quality
- None -								

MAC Address: MAC address of wireless client

Interface: interface of wireless client

Uptime: connecting uptime of wireless client

TX Rate: transmit rate of wireless client

RX Rate: receive rate of wireless client

Signal: the signal of wireless client

Noise: the noise of wireless client

SNR: the signal to noise ratio of wireless client

Signal Quality: signal quality of wireless client

Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Disabled

DHCP Server: enabled or disabled

ff-radauth: enabled or disabled

USB Support: enabled or disabled

Memory

Total Available	122.3 MB / 128.0 MB
Free	92.6 MB / 122.3 MB
Used	29.6 MB / 122.3 MB
Buffers	3.3 MB / 29.6 MB
Cached	11.7 MB / 29.6 MB
Active	10.3 MB / 29.6 MB
Inactive	6.4 MB / 29.6 MB

Total Available: the room for total available of RAM (that is physical memory minus some reserve and the kernel of binary code bytes)

Free: free memory, the F-DPU110 will reboot if the memory is less than 500kB

Used: used memory, total available memory minus free memory

Buffers: used memory for buffers, total available memory minus allocated memory

Cached: the memory used by high-speed cache memory

Active: Active use of buffer or cache memory page file size

Inactive: Not often used in a buffer or cache memory page file size

DHCP

DHCP Clients

Host Name	IP Address	MAC Address	Expires
*	192.168.1.143	xx:xx:xx:xx:DD:45	1 day 00:00:00
four-488e1df5fa	192.168.1.125	xx:xx:xx:xx:D8:F7	1 day 00:00:00
Mycenae-PC	192.168.1.116	xx:xx:xx:xx:5E:30	1 day 00:00:00

Host Name: host name of LAN client

IP Address: IP address of the client

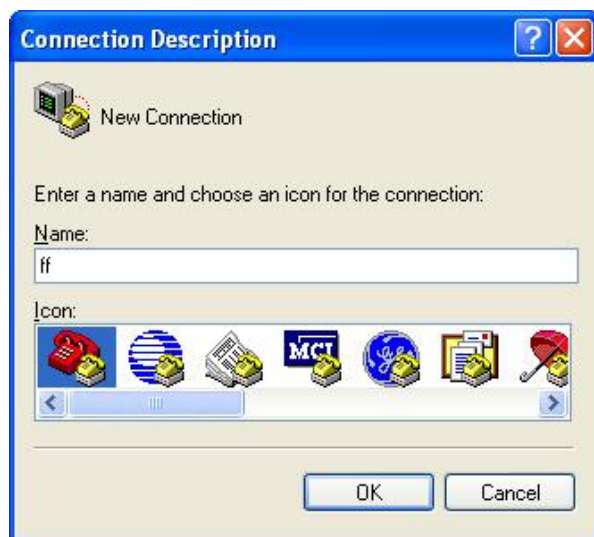
MAC Address: MAC address of the client

Expires: the expiry the client rents the IP address

Appendix

The following steps describe how to setup Windows XP Hyper Terminal.

1. Press “Start”→”Programs”→”Accessories”→”Communications”→”Hyper Terminal”



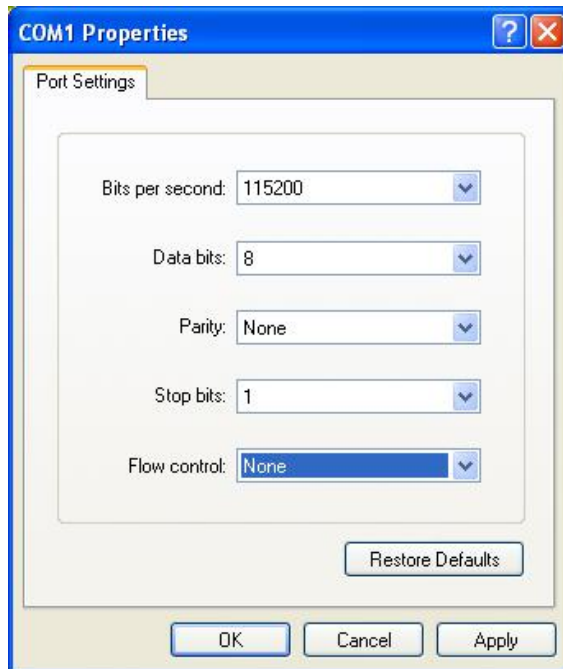
2. Input connection name, choose “OK”
3. Choose the correct COM port which connects to modem, choose “OK”



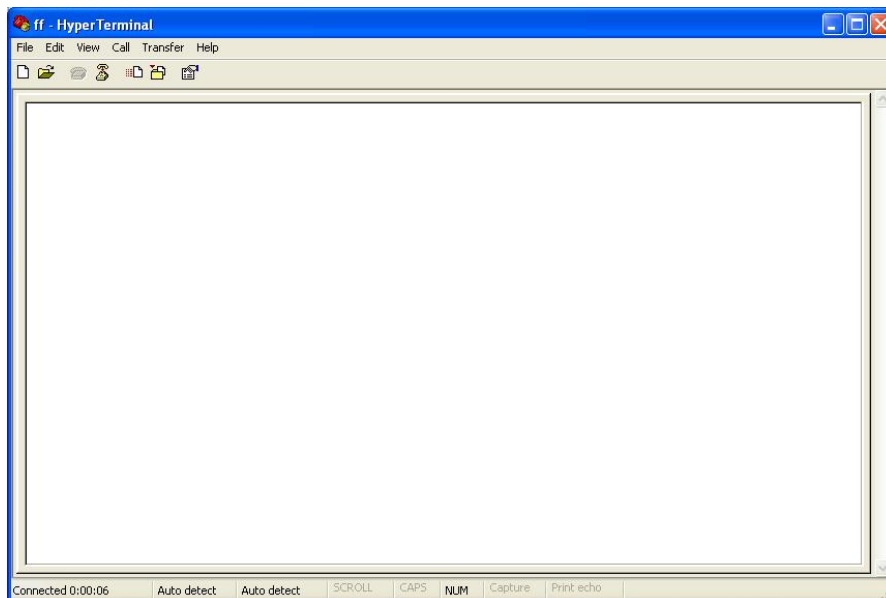
4. Configure the serial port parameters as following, choose “OK”

Bits per second: 115200

Data bits: 8
Parity: None
Stop bits: 1
Flow control: None



5. Complete Hyper Terminal operation, It runs as following



Note: If the user is using the win7 system, you can download a win7 super terminal on the internet. Universal serial interface or other similar software.