

F3X25 Series Router User Manual	Documentation No.	Product Version	Page
	Product Name:		Total:

# F3X25 Series Router User Manual

The user manual is suitable for the following model:

Model	Product Type
F3125	GPRS ROUTER
F3225	CDMA ROUTER
F3325	EDGE ROUTER
F3425	WCDMA ROUTER
F3525	TD-SCDMA ROUTER
F3625	EVDO ROUTER
F3725	LTE/TD-SCDMA ROUTER
F3825	LTE/WCDMA ROUTER
F3A25	LTE/EVDO ROUTER



**Xiamen Four-Faith Communication Technology Co., Ltd.**

**Add: J1-J3,3rd Floor,No.44,GuanRi Road,SoftWare**

**Park,XiaMen,China Zip Code:361008**

**Tel: +86 592-6300326 , 6300325, 6300324**

**Fax:+86 592-5912735**

**<http://www.fourfaith.co>**





## Files Revised Record

Date	Version	Remark	Author
2012-09-16	V1.00	Initial Draft	ZYL
2012-11-1	V1.01	Add Packet Filter	PF

## 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
Chapter 2 Installation Introduction .....	13
2.1 General .....	13
2.2 Encasement List .....	13
2.3 Installation and Cable Connection .....	13
2.4 Power .....	15
2.5 Indicator Lights Introduction .....	15
2.6 Reset Button Introduction .....	16
Chapter 3 Configuration and Management .....	17
3.1 Configuration Connection .....	17
3.2 Access the Configuration Web Page .....	17
3.3 Management and configuration .....	19
3.3.1 Setting .....	19
3.3.1.1 Basic Setting .....	19
3.3.1.2 Dynamic DNS .....	24
3.3.1.3 Clone MAC Address .....	25
3.3.1.4 Advanced Router .....	25
3.3.2 Services .....	27
3.3.2.1 Services .....	27
3.3.2.2 PPPoE Server .....	30
3.3.3 VPN .....	31
3.3.3.1 PPTP .....	31
3.3.3.2 L2TP .....	33
3.3.3.3 OPENVPN .....	34
3.3.3.4 IPSEC .....	39
3.3.3.5 GRE .....	41
3.3.4 Security .....	43
3.3.4.1 Firewall .....	43
3.3.4.2 VPN Passthrough .....	45
3.3.5 Access Restrictions .....	46
3.3.5.1 WAN Access .....	46
3.3.5.2 Packet Filter .....	49
3.3.6 NAT .....	50
3.3.6.1 Port Forwarding .....	50
3.3.6.2 Port Range Forward .....	50
3.3.6.3 Port Triggering .....	51

---

3.3.6.4	DMZ.....	52
3.3.7	QoS Setting.....	52
3.3.7.1	Basic.....	52
3.3.7.2	Classify.....	53
3.3.8	Applications.....	53
3.3.8.1	Serial Applications .....	53
3.3.9	Administration.....	55
3.3.9.1	Management.....	55
3.3.9.2	Keep Alive.....	57
3.3.9.3	Commands.....	57
3.3.9.4	Factory Defaults .....	58
3.3.9.5	Firmware Upgrade.....	58
3.3.9.6	Backup.....	59
3.3.10	Status.....	60
3.3.10.1	Router .....	60
3.3.10.2	WAN.....	62
3.3.10.3	LAN.....	63
3.3.10.4	Bandwidth .....	66
3.3.10.5	Sys-Info .....	67
Chapter 4	Appendix .....	69

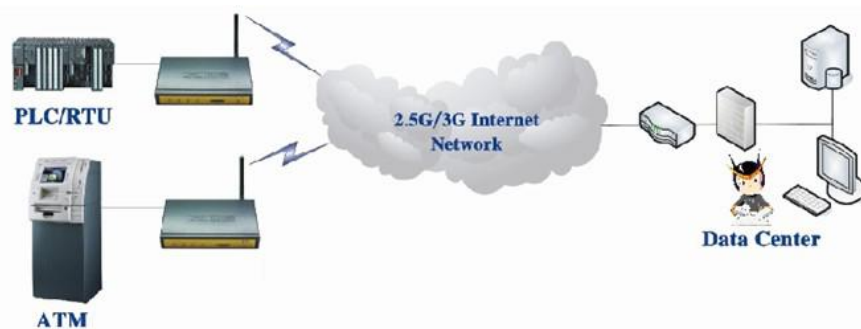
## Chapter 1 Brief Introduction of Product

### 1.1 General

F3X25 series ROUTER is a kind of cellular terminal device that provides data transfer function by public cellular network.

It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232 (or RS485/RS422), Ethernet port that can conveniently and transparently connect one device to a cellular network, allowing you to connect to your existing serial, Ethernet devices with only basic configuration.

It has been widely used on M2M fields, such as intelligent transportation, smart grid, industrial automation, telemetry, finance, POS, water supply, environment protection, post, weather, 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, scheduled power-on/power-off mode(optional)
- ◆ Housing: iron, providing IP30 protection.
- ◆ Power range: DC 5~35V

#### Stability and Reliability

- ◆ Support hardware and software WDT
- ◆ Support auto recovery mechanism, including online detect, auto redial when offline to make router always online
- ◆ Ethernet port: 1.5KV magnetic isolation protection

- ◆ RS232/RS485/RS422 port: 15KV ESD protection
- ◆ SIM/UIM port: 15KV ESD protection
- ◆ Power port: reverse-voltage and overvoltage protection
- ◆ Antenna port: lightning protection(optional)

**Standard and Convenience**

- ◆ Support standard RS232(or RS485/RS422), Ethernet port that can connect to serial, Ethernet devices 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)

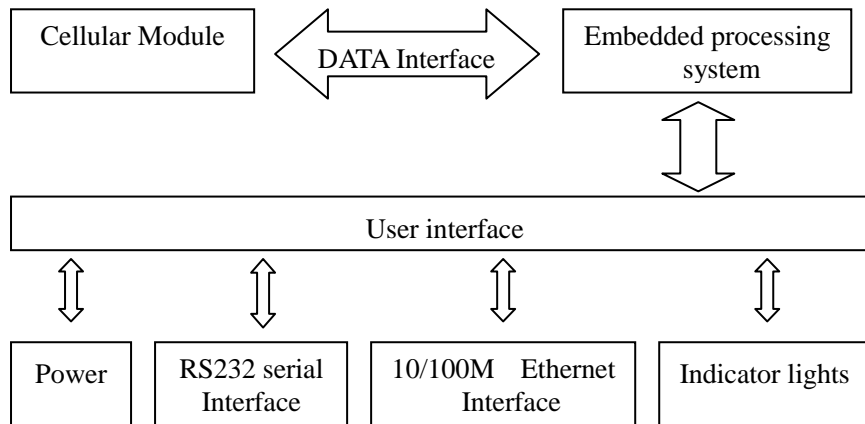
**High-performance**

- ◆ Support 3G/HSPA/4G WAN access methods.
- ◆ Support VPN client(PPTP, L2TP, OPENVPN, IPSEC and GRE)(only for VPN version)
- ◆ Support VPN server(PPTP, L2TP, OPENVPN, IPSEC and GRE)(only for VPN version)
- ◆ 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 multi online trigger ways, including SMS, ring and data. Support link disconnection when timeout
- ◆ Support APN/VPDN
- ◆ Support DHCP server and client, firewall, NAT, DMZ host , URL block, QoS, ttraff,statistics, real time link speed statistics etc.
- ◆ Full protocol support , such as TCP/IP, UDP, ICMP, SMTP, HTTP, POP3, OICQ, TELNET, FTP, SNMP, SSHD, etc.
- ◆ Schedule Reboot, Schedule Online and Offline,etc.



## 1.3 Working Principle

The principle chart of the router is as following:



## 1.4 Specifications

### Cellular Specification

Standard and Band	Bandwidth	TX power	RX sensitivity
<b>F3125 GPRS ROUTER</b>			
EGSM900/GSM1800MHz, GSM850/900/1800/1900MHz (optional) Compliant to GSM phase 2/2+ GPRS class 10, class 12(optional)	85.6Kbps	GSM850/900: <33dBm  GSM1800/1900: <30dBm	<-107 dBm
<b>F3225 CDMA ROUTER</b>			
CDMA2000 1xRTT 800MHz 800/1900MHz(optional) 450MHz(optional)	153.6Kbps	<30dBm	<-104 dBm
<b>F3325 EDGE ROUTER</b>			
GSM850/900/1800/1900MHz GPRS/EDGE Class 12	236.8Kbps	GSM850/900: <33dBm  GSM1800/1900: <30dBm	<-106 dBm
<b>F3425 WCDMA&amp;HSDPA&amp;HSUPA ROUTER</b>			
UMTS/WCDMA/HSDPA/HSUPA /HSPA+ 850/1900/2100MHz	HSUPA:5.76Mbps (Upload speed)	<24dBm	<-109 dBm

850/900/1900/2100MHz(optional) GSM850/900/1800/1900MHz GPRS/EDGE CLASS 12	HSDPA:7.2Mbps (Download speed)  UMTS:384Kbps (DL/UL) HSPA+: 21 Mbps (Download speed) 5.76Mbps (Upload speed)		
<b>F3525 TD-SCDMA ROUTER</b>			
TD-SCDMA/HSDPA/HSUPA /LTE 1880-1920/2010-2025MHz GSM850/900/1800/1900MHz GPRS/EDGE CLASS 12	Download speed:2.8Mbps upload speed:2.2Mbps  LTE(Download speed:100Mbps, upload speed:50Mbps)	<24dBm	<-108 dBm
<b>F3625 CDMA2000 1X EVDO</b>			
CDMA2000 1X EVDO Rev A 800MHz,800/1900MHz(optional) 450MHz (optional) EVDO Rev B 800/1900MHz(optional) CDMA2000 1X RTT, IS-95 A/B	Download speed:3.1Mbps upload speed:1.8Mbps EVDO Rev B(optional) Download speed:14.7Mbps upload speed:5.4Mbps	<23dBm	<-104 dBm
<b>F3725 LTE/TD-SCMA ROUTER</b>			
LTE TDD 2600/2300MHz. DC-HSPA+/HSPA+/HSUPA/HSD PA/UMTS 2100/900MHz EDGE/GPRS/GSM 850/900/1800/1900MHz	LTE(Download speed:68Mbps, upload speed:17Mbps)  HSUPA:5.76Mbps(upl oad speed) HSDPA:14.4Mbps(Do wnload speed) HSPA+: 28Mbps(Download speed)	<24dBm	<-106dBm
<b>F3825 LTE/WCDMA ROUTER</b>			
LTE FDD 2600/2100/1800/900/800MHz, 700/1700/2100MHz(optional)  HSPA+/HSDPA/HSUPA/WCDM A /UMTS900/2100MHz,	LTE(DL:100Mbps,UL :50Mbps) HSUPA:5.76Mbps(Up load speed) HSDPA:7.2Mbps(Do wnload speed)	<32dBm	<-93.3dBm

800/850/1900/2100MHz(optional) EDGE/GPRS/GSM 900/1800/1900MHz  GPRS CLASS 10 GPRS CLASS 12	UMTS:384Kbps (DL/UL)  HSPA+: 21Mbps(Download speed) 5.76Mbps(Upload speed)		
<b>F3A25 LTE&amp;EVDO ROUTER</b>			
LTE 700MHz CDMA 1XRTT/EV 800/1900MHz	LTE(DL:100Mbps, UL:50Mbps)/ CDMA2000 1X EVDO Rev A (DL:3.1Mbps, UL:1.8Mbps)	<24dBm	<-93.3dBm

### Hardware System

Item	Content
CPU	Industrial 32bits CPU
FLASH	8MB(Extendable to 64MB)
SDRAM	64MB

### Interface Type

Item	Content
Ethernet	1 10/100 Mbps Ethernet port(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
Serial	1 RS232(or RS485/RS422) port, 15KV ESD protection Data bits: 5, 6, 7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, (space, mark) (optional) Baud rate: 2400~115200 bps
Indicator	"Power", "System", "Online", "Link/ACT ", "Alarm","Signal Strength"
Antenna	Standard SMA female interface, 50 ohm, lightning protection(optional)
SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
Power	Standard 3-PIN power jack, reverse-voltage and overvoltage protection
Reset	Restore the router to its original factory default settings



### Power Input

Item	Content
Standard Power	DC 12V/1.5A
Power Range	DC 5~35V
Consumption	<450mA (12V)

### Physical Characteristics

Item	Content
Housing	Iron, providing IP30 protection
Dimensions	157x97x25 mm
Weight	440g

### Environmental Limits

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

## Chapter 2 Installation Introduction

### 2.1 General

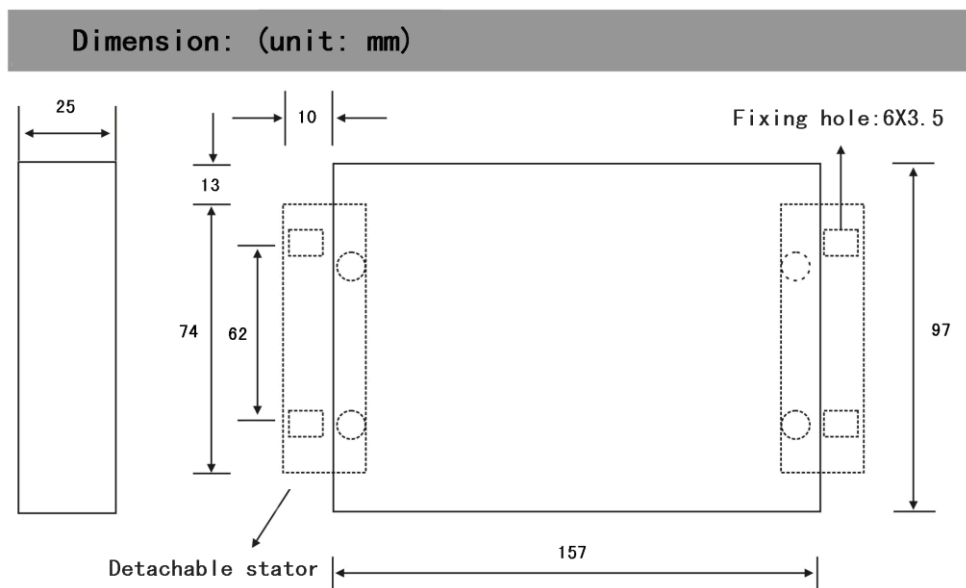
The router must be installed correctly to make it work properly.

Warning: Forbid to install the router when powered!

### 2.2 Encasement List

Name	Quantity	Remark
Router host	1	
Cellular antenna (Male SMA)	1	
Network cable	1	
Console cable	1	optional
Power adapter	1	
Manual CD	1	
Certification card	1	
Maintenance card	1	

### 2.3 Installation and Cable Connection



#### Installation of SIM/UIM card:

Firstly power off the router, and press the out button of the SIM/UIM card outlet with a needle object. Then the SIM/UIM card sheath will flick out at once. Put SIM/UIM card into the card sheath (Pay attention to put the side which has metal point outside), and insert card sheath back to the SIM/UIM card outlet.

**Warning:** Forbid to install SIM/UIM card when powered!

### Installation of antenna:

Screw the SMA male pin of the cellular antenna to the female SMA interface of the router with sign “WWAN”.

### 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
1	1
2	2
3	3
4	4
5	5
6	6
7	7
8	8

Insert the RJ45 end of the console cable into the RJ45 outlet with sign “console”, and insert the DB9F end of the console cable into the RS232 serial interface of user’s device.

The signal connection of the console cable is as follows:

RJ45	DB9F
1	8
2	6
3	2
4	1
5	5
6	3
7	4
8	7

The signal definition of the DB9F serial communication interface is as follows:

Pin	RS232 signal name	The direction for Router
1	DCD	output
2	RXD	output

3	TXD	input
4	DTR	input
5	GND	
6	DSR	output
7	RTS	input
8	CTS	output

## 2.4 Power

The power range of the router is DC 5~35V.

Warning: When we use other power, we should make sure that the power can supply power above 7W.

We recommend user to use the standard DC 12V/1.5A power.

## 2.5 Indicator Lights Introduction

The router provides following indicator lights: “Power”, “System”, “Online”, “Link/ACT”, “Alarm”, “Signal Strength”.

Indicator Light	State	Introduction
Power	ON	Router is powered on
	OFF	Router is powered off
System	BLINK	System works properly
	OFF	System does not work
Online	ON	Router has logged on network
	OFF	Router hasn't logged on network
Link/ACT	OFF	The corresponding interface of switch is not connected
	ON / BLINK	The corresponding interface of switch is connected /Communicating
Alarm	OFF	Router has no alarm
	ON	SIM/UIM card does not work or the signal of the antenna is week
Signal Strength	One Light ON	Signal strength is weak

	Two Lights ON	Signal strength is medium
	Three Lights ON	Signal strength is good

## 2.6 Reset Button Introduction

The router has a “Reset” button to restore it to its original factory default settings. When user press the “Reset” button for up to 15s, the router will restore to its original factory default settings and restart automatically.

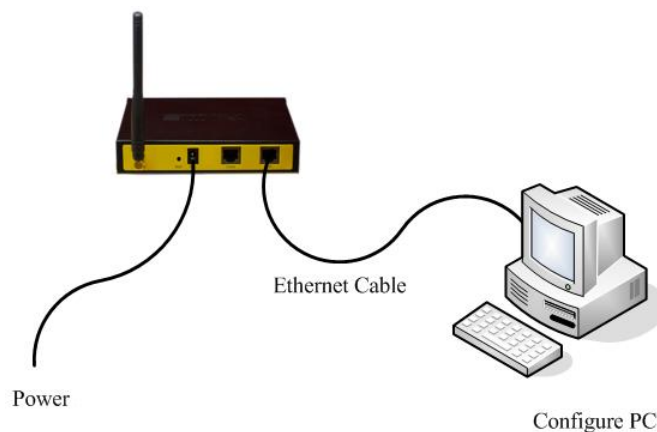


## Chapter 3 Configuration and Management

This chapter describes how to configure and manage the router.

### 3.1 Configuration Connection

Before configuration, you should connect the router and your configuration PC with the supplied network cable. Plug the cable's one end into the Local Network port of the router, and another end into your configure PC's Ethernet port. The connection diagram is as following:



Please modify the IP address of PC as the same network segment address of the router, for instance, 192.168.1.9. Modify the mask code of PC as 255.255.255.0 and set the default gateway of PC as the router's IP address (192.168.1.2).

### 3.2 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 router. 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 router's default IP address of 192.168.1.2 on address bar, then press the bottom of Enter to visit page Web management tool of the router. 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 router. 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:

Router Password:

Re-enter to confirm:

After access to the information main page



**Wireless Mobile Router**

GPRS/GDMA/EDGE/WGDMA/HDR/HSDPA/HSUPA/TD-SCDMA/HSPA+/LTE

Firmware: F3x25 v1.0 (Dec 3 2012 11:19:03) std  
 Time: 15:03:12 up 3 min, load average: 0.02, 0.04, 0.01  
 WAN IP: 192.168.13.93

---

**Menu**

- [Setup](#)
- [Services](#)
- [VPN](#)
- [Security](#)
- [Access Restrictions](#)
- [NAT](#)
- [QoS Setting](#)
- [Applications](#)
- [Administration](#)
- [Status](#)

**System Information**

Router		Services	
Router Name	Four-Faith	DHCP Server	Enabled
Router Model	Four-Faith Router	ff-radauth	Disabled
LAN MAC	00:0C:43:30:52:77	USB Support	Enabled
WAN MAC	00:0C:43:30:52:78	<b>Memory</b>	
WAN IP	192.168.13.93	Total Available	59.2 MB / 64.0 MB
LAN IP	192.168.1.2	Free	38.9 MB / 59.2 MB
		Used	20.3 MB / 59.2 MB
		Buffers	2.5 MB / 20.3 MB
		Cached	8.2 MB / 20.3 MB
		Active	1.3 MB / 20.3 MB
		Inactive	1.8 MB / 20.3 MB

**DHCP**

**DHCP Clients**

Host Name	IP Address	MAC Address	Client Lease Time
- None -			

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 Setup screen is the first screen users will see when accessing the router. Most users will be able to configure the router and get it work properly using only the settings on this screen. Some Internet Service Providers (ISPs) will require users to enter specific information, such as User Name, Password, IP Address, Default Gateway Address, or DNS IP Address. These information can be obtained from your ISP, if required.

##### 3.3.1.1 Basic Setting

WAN Connection Type

Seven Ways: Disabled, 3G/UNMTS/4G/LTE

**Disabled**

Connection Type

Forbid the setting of WAN port connection type

### 3G/UMTS/4G/LTE

Connection Type	<input type="text" value="3G/UMTS/4G/LTE"/>	
User Name	<input type="text"/>	
Password	<input type="text"/>	<input type="checkbox"/> Unmask
Dial String	<input type="text" value="*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

### Keep Online

Keep Online Detection	<input type="text" value="Ping"/>
Detection Interval	<input type="text" value="60"/> Sec.
Primary Detection Server IP	<input type="text" value="166"/> . <input type="text" value="111"/> . <input type="text" value="8"/> . <input type="text" value="238"/>
Backup Detection Server IP	<input type="text" value="202"/> . <input type="text" value="119"/> . <input type="text" value="32"/> . <input type="text" value="102"/>

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.

#### 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 Configuration

Router Name

Host Name

Domain Name

MTU

**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	<input type="text" value="192"/>	<input type="text" value="168"/>	<input type="text" value="1"/>	<input type="text" value="1"/>
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>
Local DNS	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="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	<input type="text" value="DHCP Server"/>
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1. <input type="text" value="100"/>
Maximum DHCP Users	<input type="text" value="50"/>
Client Lease Time	<input type="text" value="1440"/> minutes
Static DNS 1	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Static DNS 2	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Static DNS 3	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
WINS	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="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="text" 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 192.168.1.2 (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	UTC+08:00 ▾
Summer Time (DST)	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

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:** Four-Faith 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.
    
```

DDNS Status shows connection log information

### 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

#### MAC Clone

Enable
  Disable

---

Clone LAN(VLAN) MAC

---

Clone WAN MAC

**Clone MAC address** can clone two parts: Clone LAN MAC, Clone WAN MAC

**Noted** that one MAC address is 48 characteristic, can not be set to the multicast address, the first byte must be even.

### 3.3.1.4 Advanced Router

**Operating Mode:** Gateway and Router

#### Operating Mode

Operating Mode

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

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 ( )

Route Name:

Metric:

Destination LAN NET: ...

Subnet Mask: ...

Gateway: ...

Interface: LAN & WLAN

**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

## 3.3.2 Services

### 3.3.2.1 Services

#### DHCP Client

**DHCP Client**

Set Vendorclass	<input type="text"/>
Request IP	<input type="text"/>

**Set Vendorclass:** the DHCP server can automatically identify the specific identifier of the computer running certain operating systems to send, such as the DHCP server can identify the DHCP client running the operating system is Windows 2000 or Windows 98. Identification identifier DHCP option can be assigned to DHCP clients based on specific operating system.

**Request IP:** IP address of the request

#### 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

LAN Domain

Additional DHCPd Options

Static Leases			
MAC Address	Host Name	IP Address	Client Lease Time
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/> minutes

**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**

SNMP  Enable  Disable

Location

Contact

Name

RO Community

RW Community

**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**

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	<input type="text" value="22"/>	(Default: 22)
Authorized Keys	<input type="text"/>	

**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	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Syslog Out Mode	<input checked="" type="radio"/> Net	<input type="radio"/> Console
Remote Server	<input type="text"/>	

**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	<input checked="" type="radio"/> Enable	<input type="radio"/> 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

### 3.3.2.2 PPPoE Server

#### PPPoE Server

**PPPoE Server**

RP-PPPoE Server Daemon  Enable  Disable

**RP-PPPoEServer Daemon:** enable or disable PPPoE server

#### RP-PPPoEServer Options

**RP-PPPoE Server Options**

RP-PPPoE Server Interface

Client IP(s)

Deflate Compression

BSD Compression

LZS Stac Compression

MPPC Compression

MPPE PPPoE Encryption

Session Limit per MAC  (Default: 10)

LCP Echo Interval  (Default: 5)

LCP Echo Failure  (Default: 12)

Idle Time  (Default: 0 = Deactivate)

Authentication  Radius  Local User Management (CHAP Secrets)

**PPPOE Server Interface:** PPPoE server interface to the outside, only to support the LAN port

**Client IP(s):** IP range assigns to the PPPoE client in the format: xxx.xxx.xxx.xxx-xxx

**Deflate Compression:** enable or disable Deflate Compression

**BSD Compression:** enable or disable BSD Compression

**LZS Stac Compression:** enable or disable LZS Stac Compression

**MPPC Compression:** enable or disable MPPC Compression

**MPPE PPPoE Encryption:** enable or disable MPPE PPPoE Encryption

**Session Limit per MAC:** default is 10

**LCP Echo Interval:** time interval to set the the LCP calibration phase response

**LCP Echo Failure:** release PPPoE over failure times, the PPPoE client will need to reconnect

**Idle Time:** set idle time, idle time at the appropriate time to release the PPPoE

**Authentication:** including local and Radius (Remote Authentication Dial In User)

### Local User Management (CHAP Secrets)

Local User Management (CHAP Secrets)

User	Password	IP Address	Enable
<input type="text"/>	<input type="text"/>	<input type="text" value="0.0.0.0"/>	<input type="checkbox"/>

**User:** set PPPOE client's user name

**Password:** set PPPOE client's user password

**IP Address:** set PPPOE client's user IP address

**Enable:** enable or disable this setting

### Radius

Radius Authentication

Radius Server IP	<input type="text" value="192.168.1.1"/>	
Radius Authentication Port	<input type="text" value="1812"/>	(Default: 1812)
Radius Accounting Port	<input type="text" value="1813"/>	(Default: 1813)
Radius Shared Key	<input type="text" value="••••••••••"/>	

**Radius Server IP:** set the Remote Authentication Dial In User-Server IP

**Radius Authentication Port:** set the Remote Authentication Dial in User-Authentication Port

**Radius Accounting Port:** set the Remote Authentication Dial in User-Accounting Port

**Radius Shared Key:** transactions between the client and RADIUS accounting server are authenticated through the use of a shared secret, which is never sent over the network.

## 3.3.3 VPN

### 3.3.3.1 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.

### 3.3.3.2 L2TP

#### L2TP Server

**L2TP Server**

L2TP Server Options  Enable  Disable

Force MPPE Encryption  Enable  Disable

Server IP

Client IP(s)

CHAP-Secrets

**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

### 3.3.3.3 OPENVPN

#### OPENVPN Server

Start Type  WAN Up  System

**Start Type:** WAN UP----start after on-line, System----start when boot up

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   
 Netmask

**Network:** network address allowed by OPENVPN server

**Netmask:** netmask allowed by OPENVPN server

**Bridge (TAP):**

DHCP-Proxy mode  Enable  Disable  
 Pool start IP   
 Pool end IP   
 Gateway   
 Netmask

**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  (Default: 1194)  
 Tunnel Protocol   
 Encryption Cipher   
 Hash Algorithm

**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

### 3.3.3.4 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
<input type="button" value="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	
Type	Net-to-Net Virtual Private Network <input type="button" value="v"/>
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	<input checked="" type="checkbox"/>
Time Interval	<input type="text" value="60"/> (S) Timeout <input type="text" value="60"/> (S) Action <input type="button" value="hold"/> <input type="button" value="v"/>
Enable Connection Detection	<input checked="" type="checkbox"/>

**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 Grouptype

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 1<sup>st</sup> and 2<sup>nd</sup> phase information, otherwise it will automatic negotiation according to opposite end

**IKE Encryption:** IKE phased encryption mode

**IKE Integrity:** IKE phased integrity solution

**IKE Grouptype:** 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

### 3.3.3.5 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	<input type="text" value="1 (fff)"/>	<input type="button" value="Delete"/>
Status	<input type="text" value="Enable"/>	
Name	<input type="text" value="fff"/>	
Through	<input type="text" value="PPP"/>	
Peer Wan IP Addr	<input type="text" value="120.42.46.98"/>	
Peer Subnet	<input type="text" value="192.168.5.0/24"/>	(eg:192.168.1.0/24)
Peer Tunnel IP	<input type="text" value="200.200.200.1"/>	
Local Tunnel IP	<input type="text" value="200.200.200.5"/>	
Local Netmask	<input type="text" value="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	<input type="text" value="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

### 3.3.4 Security

#### 3.3.4.1 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

---

**Options**

Dropped

Rejected

Accepted

**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
<input type="button" value="Refresh"/> <input type="button" value="Close"/>			

**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	183.60.49.20	UDP	8000	Accepted

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

### 3.3.4.2 VPN Passthrough

Virtual Private Networking (VPN) is typically used for work-related networking. For VPN tunnels, the router supports OPENVPN Passthrough, PPTP Passthrough and L2TP Passthrough.

## Virtual Private Network (VPN)

### VPN Passthrough

IPSec Passthrough	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
PPTP Passthrough	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
L2TP Passthrough	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable

**IPSec Passthrough:** Internet Protocol Security (IPSec) is a suite of protocols used to implement secure exchange of packets at the IP layer. To allow IPSec tunnels to pass through the router, IPSec Passthrough is enabled by default. To disable IPSec Passthrough, select Disable.

**PPTP Passthrough:** Point-to-Point Tunneling Protocol is the method used to enable VPN sessions to a Windows NT 4.0 or 2000 server. To allow PPTP tunnels to pass through the router, PPTP Passthrough is enabled by default. To disable PPTP Passthrough, select Disable.

**L2TP Passthrough:** Layer Two (2) Tunneling Protocol, an extension to the PPP protocol that enables ISPs to operate Virtual Private Networks (VPNs). L2TP merges the best features of two other tunneling protocols: PPTP from Microsoft and L2F from Cisco Systems. To allow L2TP tunnels to pass through the router, L2TP Passthrough is enabled by default. To disable L2TP Passthrough, select Disable.

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

## 3.3.5 Access Restrictions

### 3.3.5.1 WAN Access

Use access restrictions, you can block or allow specific types of Internet applications. You can set specific PC-based Internet access policies. This feature allows you to customize up to ten different Internet Access Policies for particular PCs, which are identified by their IP or MAC addresses.

#### Access Policy

Policy	1 ( )	Delete	Summary
Status	<input type="radio"/> Enable	<input checked="" type="radio"/> Disable	
Policy Name	<input type="text"/>		
PCs	Edit List of clients		
<input type="radio"/> Deny	Internet access during selected days and hours.		
<input checked="" type="radio"/> Filter			

Two options in the default policy rules: "Filter" and "reject". If select "Deny", you will deny specific computers to access any Internet service at a particular time period. If you choose to

"filter", It will block specific computers to access the specific sites at a specific time period. You can set up 10 Internet access policies filtering specific PCs access Internet services at a particular time period.

**Access 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  00:00 To 00:00

**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**

<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>

**Website Blocking by Keyword**

<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>

**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 the policy number (1-10) in the drop-down menu.
2. For this policy is enabled, click the radio button next to "Enable"
3. Enter a name in the Policy Name field.
4. Click the Edit List of PCs button.
5. On the List of PCs screen, specify PCs by IP address or MAC address. Enter the appropriate IP addresses into the IP fields. If you have a range of IP addresses to filter, complete the appropriate IP Range fields. Enter the appropriate MAC addresses into the MAC fields.
6. Click the Apply button to save your changes. Click the Cancel button to cancel your unsaved changes. Click the Close button to return to the Filters screen.
7. If you want to block the listed PCs from Internet access during the designated days and time, then keep the default setting, Deny. If you want the listed PCs to have Internet filtered during the designated days and time, then click the radio button next to Filter.
8. Set the days when access will be filtered. Select Everyday or the appropriate days of the week.
9. Set the time when access will be filtered. Select 24 Hours, or check the box next to From and



use the drop-down boxes to designate a specific time period.

10. Click the Add to Policy button to save your changes and active it.
11. To create or edit additional policies, repeat steps 1-9.
12. To delete an Internet Access Policy, select the policy number, and click the Delete button.

**Note:**

- 1) The default factory value of policy rules is "filtered". If the user chooses the default policy rules for "refuse", and editing strategies to save or directly to save the settings. If the strategy edited is the first, it will be automatically saved into the second, if not the first, keep the original number.
- 2) Turn off the power of the router or reboot the router can cause a temporary failure. After the failure of the router, if can not automatically synchronized NTP time server, you need to recalibrate to ensure the correct implementation of the relevant period control function.

### 3.3.5.2 Packet Filter

To block some packets getting Internet access or block some Internet packets getting local network access, you can configure filter items to block these packets.

#### Packet Filter

Packet filter function is realized based on IP address or port of packets.

Enable Packet Filter  Enable  Disable

Policy  ▼

**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

Add Filter Rule

Direction  ▼

Protocol  ▼

Source Ports  -

Destination Ports  -

Source IP  .  .  .  /

Destination IP  .  .  .  /

#### 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

Note: "Source Port" ,"Destination Port" ,"Source IP" ,"Destination IP" could not be all empty ,you have to input at least one of these four parameters.

## 3.3.6 NAT

### 3.3.6.1 Port Forwarding

Port 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 router will forward those requests to the appropriate PC. If you want to forward a whole range of ports, see [Port Range Forwarding](#).

**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.

### 3.3.6.2 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 router 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"/>

**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.

### 3.3.6.3 Port Triggering

Port Triggering allows you to do port forwarding without setting a fixed PC. By setting Port Triggering rules, you can allow inbound traffic to arrive at a specific LAN host, using ports different than those used for the outbound traffic. This is called port triggering since the outbound traffic triggers to which ports inbound traffic is directed.

**Port Triggering**

**Forwards**

Application	Triggered Port Range		Protocol	Forwarded Port Range		Enable
	Start	End		Start	End	
web	8000	10000	Both ▾	20	800	<input checked="" type="checkbox"/>

If you want to forward ports to a PC with a static IP address, see [Port Forwarding](#) or [Port Range Forwarding](#).

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

**Triggered Port Range:** Enter the number of the first and the last port of the range, which should

be triggered. If a PC sends outbound traffic from those ports, incoming traffic on the Forwarded Range will be forwarded to that PC.

**Forwarded Port Range:** Enter the number of the first and the last port of the range, which should be forwarded from the Internet to the PC, which has triggered the Triggered Range.

**Enable :** Click the Enable checkbox to enable port triggering for the application.

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

### 3.3.6.4 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.

**Demilitarized Zone (DMZ)**

---

**DMZ**

Use DMZ  Enable  Disable

DMZ Host IP Address 192.168.8.

Any PC whose port is being forwarded must should have a new static IP address assigned to it because its IP address may change when using the DHCP function.

**DMZ Host IP Address:** To expose one PC to the Internet, select Enable and enter the computer's IP address in the DMZ Host IP Address field. To disable the DMZ, keep the default setting: Disable

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

## 3.3.7 QoS Setting

### 3.3.7.1 Basic

Bandwidth management prioritizes the traffic on your router. Interactive traffic (telephony, browsing, telnet, etc.) gets priority and bulk traffic (file transfer, P2P) gets low priority. The main goal is to allow both types to live side-by side without unimportant traffic disturbing more critical things. All of this is more or less automatic.

QoS allows control of the bandwidth allocation to different services, netmasks, MAC addresses and the four LAN ports.

#### Main WAN QoS Settings

Start QoS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Port	WAN ▾
Packet Scheduler	HTB ▾
Uplink (kbps)	0
Downlink (kbps)	0

#### Bkup WAN QoS Settings

Start QoS	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Port	WAN ▾
Packet Scheduler	HTB ▾
Uplink (kbps)	0
Downlink (kbps)	0

**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.

### 3.3.7.2 Classify

#### Netmask Priority

##### Netmask Priority

Delete	IP/Mask	Priority
<input type="checkbox"/>	192.168.1.1/24	Exempt ▾
<input type="checkbox"/>	192.168.2.3/24	Standard ▾
<input type="checkbox"/>	192.168.3.4/32	Express ▾
<input type="checkbox"/>	192.168.4.5/32	Bulk ▾
	<input type="button" value="Add"/> <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> / <input type="text" value="0"/>	

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

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

## 3.3.8 Applications

### 3.3.8.1 Serial Applications

There is a console port on Four-Faith router. Normally, this port is used to debug the router. This port can also be used as a serial port. The router has embedded a serial to TCP program. The data sent to the serial port is encapsulated by TCP/IP protocol stack and then is sent to the destination server. This function can work as a Four-Faith DTU (Data Terminal Unit). Please refer [www.four-faith.com](http://www.four-faith.com) for more information about this product.

**Serial Applications**

Serial Applications  Enable  Disable

Baudrate

Databit

Stopbit

Parity

Flow Control

Protocol

Server Address

Server Port

Device Number

Device Id

Heartbeat Interval

**Baudrate:** The serial port's baudrate

**Databit:** The serial port's databit

**Parity:** The serial port's parity

**Stopbit:** The serial port's stopbit

**Flow Control:** The serial port's flow control type.

**Enable Serial TCP Function:** Enable the serial to TCP function

**Protocol Type:** The protocol type to transmit data.

UDP(DTU) – Data transmit with UDP protocol , work as a Four-Faith DTU 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 DTU which has application protocol and hear beat mechanism.

Pure TCP -- Data transmit with standard TCP protocol, router is the client.

TCP Server -- Data transmit with standard TCP protocol, router is the server.

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 router's identity ID.

**Device Number:** The router'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 Administration

#### 3.3.9.1 Management

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

**Router Password**

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

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 router, which is admin. All users who try to access the router's web-based utility or Setup Wizard will be prompted for the router's password.

**Web Access**

This feature allows you to manage the router 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 router information web page. It's now possible to password protect this page (same username and password than above).

**Web Access**

Protocol	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Auto-Refresh (in seconds)	<input type="text" value="3"/>
Enable Info Site	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Info Site Password Protection	<input type="checkbox"/> Enabled

**Protocol:** This feature allows you to manage the router 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 checked="" type="radio"/> Enable <input 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	

**Remote Access:** This feature allows you to manage the router 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 router. You must also change the router's default password to one of your own, if you haven't already.

To remotely manage the router, enter `http://xxx.xxx.xxx.xxx:8080` (the x's represent the router's Internet IP address, and 8080 represents the specified port) in your web browser's address field. You will be asked for the router'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 router by Secure Shell. Note that SSH daemon needs to be enable in Services page.

#### Note:

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

#### 802.1x

802.1x	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
--------	---

**802.1x:** A limited 802.1x server needed to fulfill WPA handshake requirements to allow Windows XP clients to work with WPA.



**Routing**

Routing  Enable  Disable

**Routing:** Routing enables the OSPF and RIP routing daemons if you have set up OSPF or RIP routing in the Advanced Routing page.

**Language Selection**

Language

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

**IP Filter Settings (adjust these for P2P)**

TCP Congestion Control	<input type="text" value="vegas"/>	
Maximum Ports	<input type="text" value="4096"/>	(Default: 4096, Range: 256 - 4096)
TCP Timeout (in seconds)	<input type="text" value="3600"/>	(Default: 3600, Range: 1 - 86400)
UDP Timeout (in seconds)	<input type="text" value="120"/>	(Default: 120, Range: 1 - 86400)

**IP Filter Settings (adjust these for P2P):** If you have any peer-to-peer (P2P) applications running on your network please increase the maximum ports and lower the TCP/UDP timeouts. This is necessary to maintain router stability because peer-to-peer applications open many connections and don't close them properly. Consider using these:

**Maximum Ports:** 4096

**TCP Timeout:** 3600 sec

**UDP Timeout:** 120 sec

### 3.3.9.2 Keep Alive

#### Schedule Reboot

**Schedule Reboot**

Schedule Reboot  Enable  Disable

Interval (in seconds)

At a set Time   :

**You can schedule regular reboots for the router :**

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.

### 3.3.9.3 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 router. 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 router. 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.

### 3.3.9.4 Factory Defaults

**Factory Defaults**

**Reset router settings**

Restore Factory Defaults  Yes  No

**Reset router settings:** Click the Yes button to reset all configuration settings to their default values. Then click the Apply Settings button.

**Note:**

Any settings you have saved will be lost when the default settings are restored. After restoring the router is accessible under the default IP address 192.168.1.2 and the default password admin.

### 3.3.9.5 Firmware Upgrade

#### Firmware Upgrade

After flashing, reset to

Please select a file to upgrade

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

**Note:**

When you upgrade the Router's firmware, you lose its configuration settings, so make sure you write down the Router settings before you upgrade its firmware.

**To upgrade the Router's firmware:**

1. Download the firmware upgrade file from the website.
2. Click the Browse... button and chose the firmware upgrade file.
3. Click the Upgrade button and wait until the upgrade is finished.

**Note:**

Upgrading firmware may take a few minutes.

Do not turn off the power or press the reset button!

**After flashing, reset to:** If you want to reset the router to the default settings for the firmware version you are upgrading to, click the Firmware Defaults option.

### 3.3.9.6 Backup

**Backup Configuration**

**Backup Settings**

Click the "Backup" button to download the configuration backup file to your computer.

**Restore Configuration**

**Restore Settings**

Please select a file to restore

**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!

**Backup Settings:** You may backup your current configuration in case you need to reset the router back to its factory default settings. Click the Backup button to backup your current configuration.

**Restore Settings:** Click the Browse... button to browse for a configuration file that is currently saved on your PC. Click the Restore button to overwrite all current configurations with the ones in

the configuration file.

**Note:**

Only restore configurations with files backed up using the same firmware and the same model of router.

### 3.3.10 Status

#### 3.3.10.1 Router

**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,

**Router Name:** name of the router, setting→basic setting to modify

**Router Model:** model of the router, 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 router, 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

**Memory**

Total Available	28880 kB / 32768 kB	88%
Free	12436 kB / 28880 kB	43%
Used	16444 kB / 28880 kB	57%
Buffers	1660 kB / 16444 kB	10%
Cached	5708 kB / 16444 kB	35%
Active	963 kB / 16444 kB	6%
Inactive	1118 kB / 16444 kB	7%

**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 router will reboot if the memory is less than 500kB

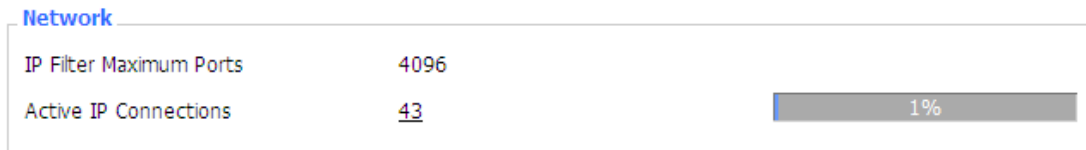
**Used:** used memory, total available memory minus free memory

**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



**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

### 3.3.10.2 WAN

Connection Type 3G/UMTS

**Connection Type:** disabled, 3G/UMTS

Connection Uptime 0:28:24

**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 router WAN

**Subnet Mask:** subnet mask of router WAN

**Gateway:** the gateway of router WAN

**DNS1, DNS2, DNS3:** DNS1/DNS2/DNS3 of router WAN

Login Status Disconnected

**Login Status:** connection status of WAN

**Disconnection:** disconnect

**Connection:** connect

Module Type ZTE-EVDO MODULE



Signal Status -79 dBm

Network CDMA/HDR

**Module Type:** module type in 3G/UMTS way

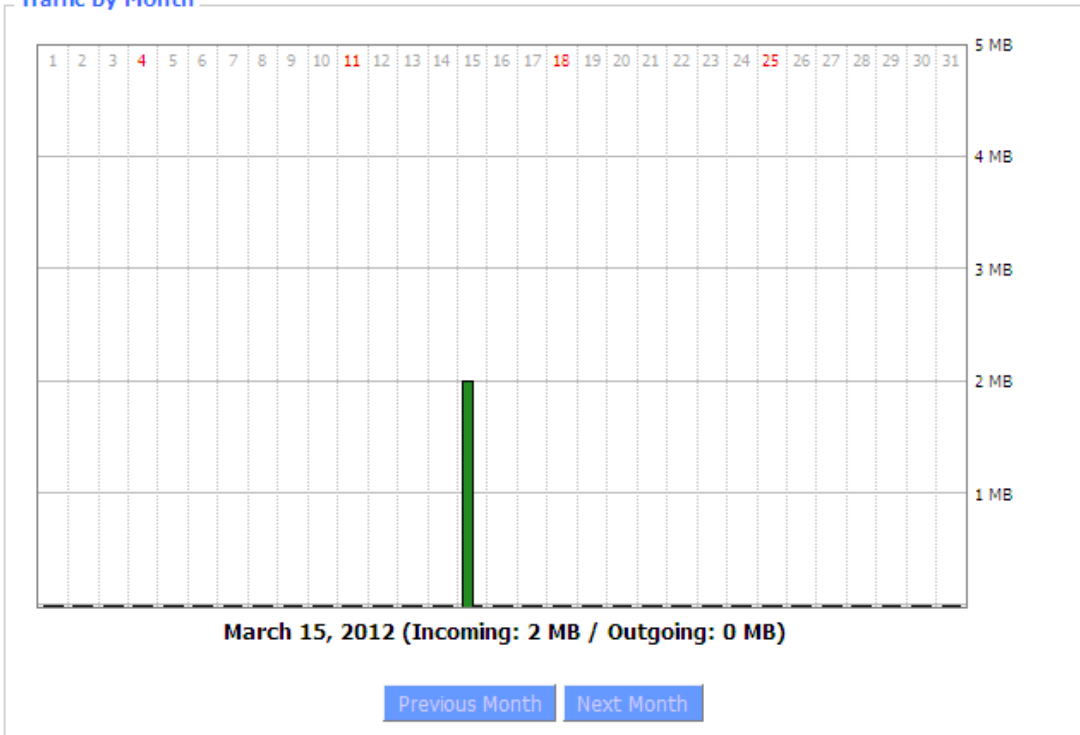
**Signal Status:** signal intensity of the module in 3G/UMTS way

**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

**3.3.10.3 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 router 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

#### 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

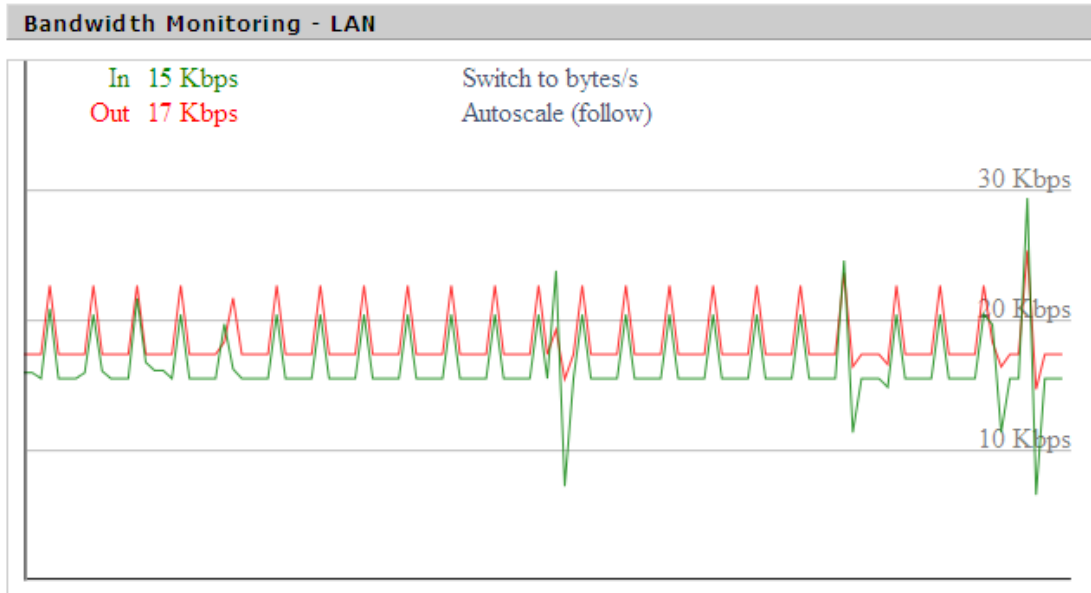
**User Name:** user name of the client

**Local IP:** tunnel IP address of PPTP client

**Remote IP:** IP address of PPTP client

**Delete:** click to delete PPTP client

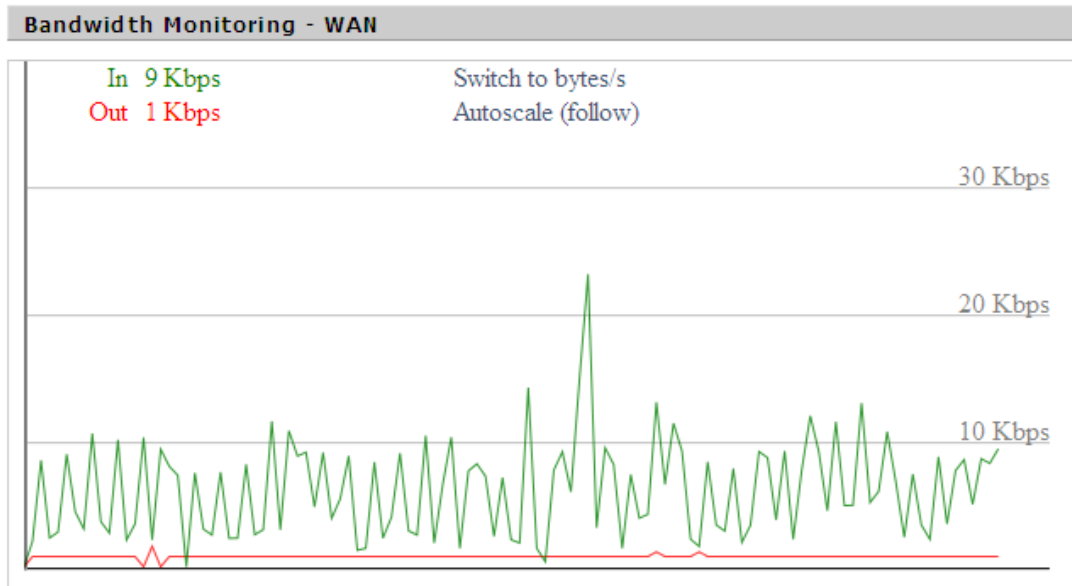
### 3.3.10.4 Bandwidth



Bandwidth Monitoring-LAN Graph

**abscissa axis:** time

**vertical axis:** speed rate



Bandwidth Monitoring-WAN Graph

**abscissa axis:** time

**vertical axis:** speed rate

### 3.3.10.5 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>
WAN IP	192.168.13.93
LAN IP	192.168.1.2

**Router Name:** the name of the router

**Router Model:** the model of the router

**LAN MAC:** MAC address of LAN port

**WAN MAC:** MAC address of WAN port

**WAN IP:** IP address of WAN port

**LAN IP:** IP address of LAN port

### 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	28.2 MB / 32.0 MB
Free	11.2 MB / 28.2 MB
Used	17.0 MB / 28.2 MB
Buffers	1.8 MB / 17.0 MB
Cached	6.3 MB / 17.0 MB
Active	1.5 MB / 17.0 MB
Inactive	0.8 MB / 17.0 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 router 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

## Chapter 4 Appendix

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

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



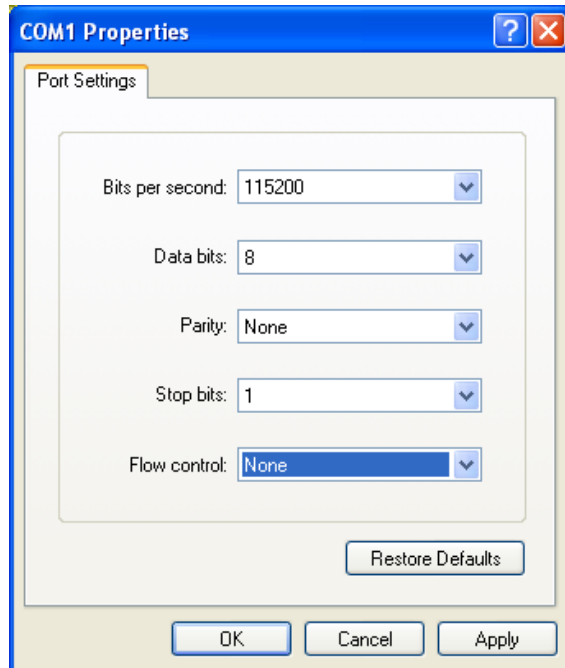
2. Input connection name, choose “OK”
3. Choose the correct COM port which connects to modem, choose “OK”



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

