

F3936 Router User Manual	Documentation No.	Product Version	Page
		V1.0	
	Product Name: F3936		Total:77

# F3936 Router User Manual

## Files Revised Record

Date	Version	Remark	Author
2014-9-28	V1.00	Initial version	wonder
2015-3-26	V1.10	Modified	wonder



# Contents

Chapter 1 Brief Introduction of Product.....	6
1.1 General.....	6
1.2 Features and Benefits.....	6
1.3 Working Principle.....	9
1.4 Product Specifications.....	9
Chapter 2 Installation Introduction.....	12
2.1 General.....	12
2.2 Encasement List.....	12
2.3 Installation and Cable Connection.....	12
2.4 Power.....	14
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.....	26
3.3.1.3 Clone MAC Address.....	27
3.3.1.4 Advanced Router.....	27
3.3.1.5 VLANs.....	29
3.3.1.6 Networking.....	30
3.3.2 Wireless.....	33
3.3.2.1 Basic Settings.....	33
3.3.2.2 Wireless Security.....	35
3.3.3 Services.....	37
3.3.3.1 USB.....	40
3.3.3.2 FTP Server.....	40
3.3.3.3 Hotspot.....	41
3.3.4 Security.....	43
3.3.4.1 Firewall.....	43
3.3.5 Access Restrictions.....	45
3.3.5.1 WAN Access.....	45
3.3.5.2 Packet Filter.....	48
3.3.6 NAT.....	49
3.3.6.1 Port Forwarding.....	49
3.3.6.2 Port Range Forward.....	50
3.3.6.3 DMZ.....	51
3.3.7 QoS Setting.....	51
3.3.7.1 Basic.....	51
3.3.8 Applications.....	52

3.3.8.1	Serial Applications.....	52
3.3.8.2	GPS Settings(Optional).....	54
3.3.9	Administration.....	55
3.3.9.1	Management.....	55
3.3.9.2	Keep Alive.....	58
3.3.9.3	Commands.....	59
3.3.9.4	Factory Defaults.....	59
3.3.9.5	Firmware Upgrade.....	60
3.3.9.6	Backup.....	60
3.3.10	Status.....	61
3.3.10.1	Router.....	61
3.3.10.2	WAN.....	63
3.3.10.3	LAN.....	66
3.3.10.4	Wireless.....	68
3.3.10.5	Device Management.....	70
3.3.10.6	Bandwidth.....	71
3.3.10.7	Sys-Info.....	72
Appendix.....		75

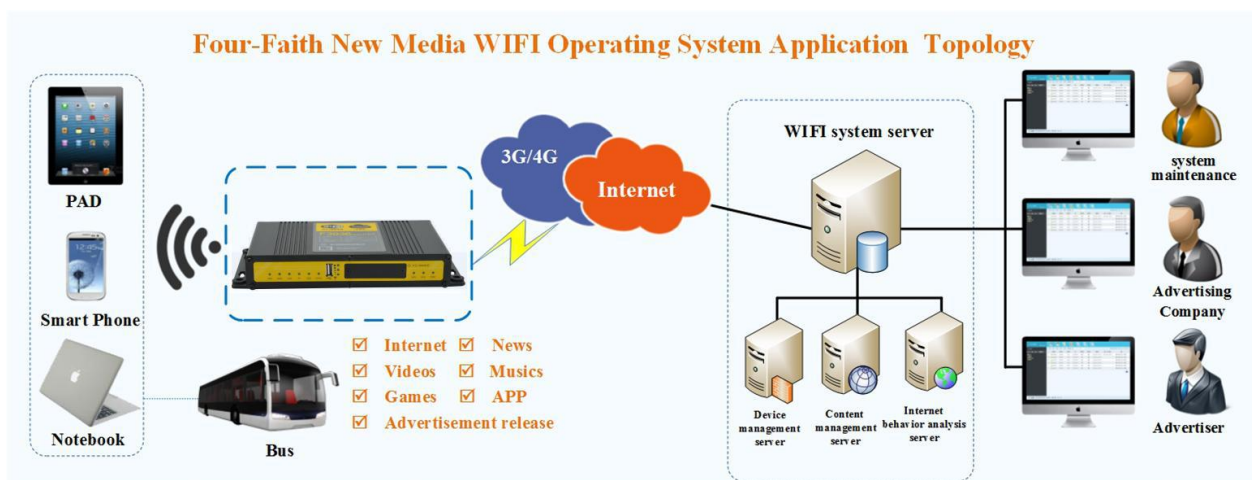
# Chapter 1 Brief Introduction of Product

## 1.1 General

F3936 is a vehicle WIFI new media operating terminal and it integrates the advanced 3G/4G/WIFI communication GPS/beidou(optional) positioning technology, local large-capacity storage and multimedia advertising push technology. The passengers can use smart phones, PAD and notebook to enjoy freely the local videos, news, music, games, and quickly connecting the Internet, etc. And media operators may carry out more value added services.

F3936 has been already widely used in public transportation, tourism, finance and medical industries, such as urban public transport, customized bus, bus stations, tour bus, long-distance passenger bus, tourist attractions, bank, hospital and so on.

## Application Topology



## 1.2 Features and Benefits

### Design for Vehicle Application

- High-powered 32bits CPU
- Vehicle power supply design, support under-voltage, over-voltage, over-current, reverse connection, short circuit, surge protection
- Wide Power range: DC 9~36V
- Wide Operating Temperature(-35~+75°C)
- Aviation plug for power input
- Metal shell, high heat radiating and anti collision performance

- Shockproof design,suitable for vehicle vibrating environment
- Security structure design for TF/SIM card

## Stability and Reliability

- Support hardware and software WDT to ensure the stability of the system
- Support auto recovery mechanism, including online detect, auto redial when offline to make router always online
- Data storage with SSD, ensure the data security and stability on high speed read and write
- Ethernet port: 1.5KV magnetic isolation protection
- RS232/RS485/RS422 port: 15KV ESD protection
- SIM/UIM port: 15KV ESD protection
- Antenna port: lightning protection(optional)

## Standard and Convenience

- Support all kinds of the Intelligent WIFI terminals
- Smart data terminal, enter into communication state automatically when powered
- Provides standard wired network and wireless 3G/4G network
- Small size device,rapid establishment of wireless network to use
- Provide powerful business platform for equipment management, content management and release, report management, user behavior statistics analysis, authority management, alarm management, billing system (optional) and other functions

## High-performance

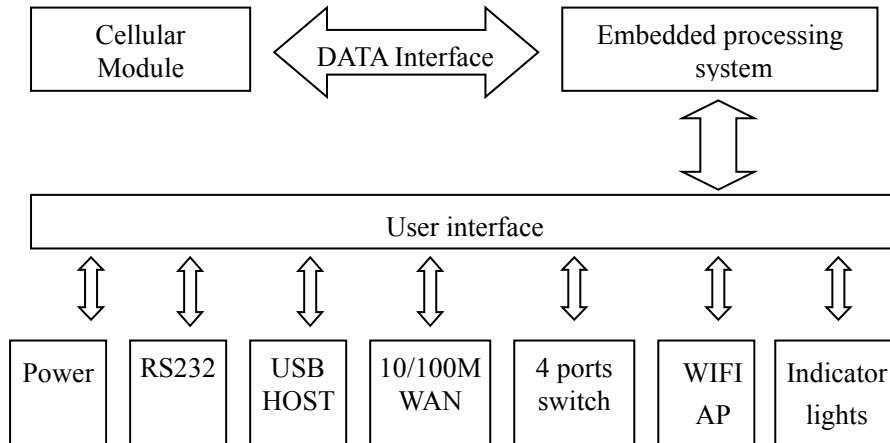
- Support website redirection, local captive portal, remote captive portal(optional)
- Support various authentication ways, including mobile phone number authentication, Wechat authentication, Weibo authentication, QQ authentication and without authentication.
- Support WIFI channel hopping for anti-interference
- Support English SSID
- Support SSD(Solid State Disk) and TF card for local storage(TF card is optional)
- WIFI TX power is configurable for optimized wireless coverage
- Support WEB server. Supports PHP, XML, and database storage(optional)

- Support WIFI inspector
- Support black/white list of URL, account, IP address, MAC address
- Support traffic statistics. Support monitoring of device traffic, user traffic and online duration monitoring.
- Support user's surfing behavior record, local PV/UV statistics and transmit these data to server at real time for data statistics analysis.
- Support real time log auditing based on user's URL access
- Local information contains advertisement, news, APP, video, music, etc. Support various video formats and streaming media delivery
- Local information update support whole update and incremental update, support grouping update, support break-point resume and outage resume, support A/B backup, support update via 3G/4G, FTP, station WIFI(optional) and U disk upgrades(optional)
- Support remote firmware upgrade, including upgrade on single device, devices in patch and automatic upgrade(optional), support break-point resume, outage resume(optional), U disk upgrades (optional)
- Support remote terminal parameters configuration, can be a single, batch configuration, custom configuration, at the same time support online/offline equipment configuration and U disk field configuration (optional)
- Support monitoring device status at real time, including CPU, memory, signal strength, network status, storage and alarm
- Supports completed functionality of router
- Support SPI firewall, access restriction, URL filter, QoS, NAT, etc
- Support NTP, schedule reboot and schedule boot/shutdown with in built RTC
- Support various WAN connection types, including static IP, DHCP, PPPoE, 3G / 4G, etc
- Support 3G/4G network and Ethernet WAN for backup(optional)
- Support VPN client and VPN server(PPTP, L2TP, OPENVPN, IPSEC and GRE(only VPN version supports))
- Support the GPS/beidou positioning function (optional)



### 1.3 Working Principle

The principle chart of the router is as following:



### 1.4 Product Specifications

#### Cellular Specification

Item	Content
Cellular Module	High-performance cellular module (optional single module, double module or no module)
Standard	Can support: TDD-LTE/FDD-LTE/EVDO/WCDMA/TD-SCDMA/CDMA1X/GPRS/EDGE Optional support:single-mode,multi-mode or All network communication
Bandwidth	FDD LTE(DL:100Mbps,UL:50Mbps) TDD LTE(DL:61Mbps,UL:18Mbps) CDMA2000 1X EVDO Rev A (DL:3.1Mbps,UL:1.8Mbps) WCDMA(DL:42Mbps,UL:5.76Mbps) TD-SCDMA(DL:4.2Mbps,UL:2.2Mbps)
TX power	<24dBm
RX sensitivity	<-109dBm

#### GPS Specification

Item	Content
GPS Module	Industrial GPS module(optional beidou module)
Receiver Type	50-channle GPS L1(1575.42MHz)C/A code SBAS: WAAS,EGNOS,MSAS,GAGAN

Max. update rate	5 Hz
Accuracy	Position: 2.5m CPE SBAS: 2.0m CPE
Sensitivity	Tracking: -160dBm Reacquisition: -160dBm Cold starts: -146dBm

### WIFI Specification

Item	Content
Standard	IEEE802.11b/g/n, 2.4G, 2*2 MIMO, AP model, Station model(optional)
Bandwidth	IEEE802.11b/g: 108Mbps (max) IEEE802.11n: 300Mbps (max)
Security	WEP, WPA, WPA2, etc. WPS (optional)
TX power	20dBm (11n), 21.5dBm (11g), 26dBm (11b)
RX sensitivity	<-75dBm@54Mbps

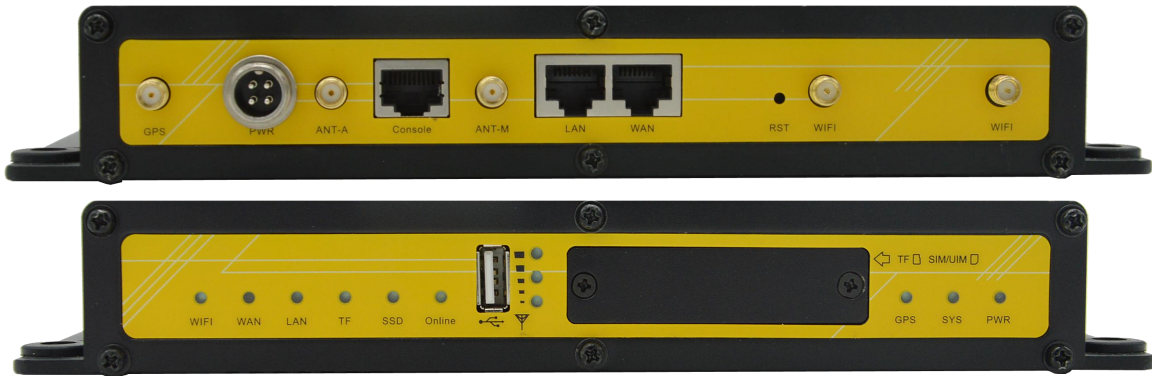
### Hardware System

Item	Content
CPU	High-performance 32bits CPU
FLASH	32MB(Extendable to 64MB)
DDR2	256MB
SSD	128GB(optional, Extendable to 2TB)
TF	32GB(optional)

### Interface Type

Item	Content
WAN	1 10/100 Mbps WAN port(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
LAN	1 10/100 Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
Serial	1 RS232(or RS485/RS422) port, 15KV ESD protection Data bits: 8(optional 5, 6, 7) Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space(optional), mark(optional) Baud rate: 2400~115200 bps
Indicator	"PWR", "SYS", "SIM", "GPS", "Online", "SSD", "TF", "LAN", "WAN", "WIFI", "Signal Strength"(Indicator according to the configuration)
Antenna	Cellular: Standard SMA female interface, 50 ohm, lightning protection(optional one, two or not) GPS: One standard SMA female interface, 50 ohm, lightning protection(optional)

	WIFI: Two standard SMA male interface, 50 ohm, lightning protection
SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
USB	Standard A type USB host interface, support USB 2.0 High-speed
TF	Standard TF card interface
Power	Aviation plug or vehicle power jack, reverse-voltage and overvoltage protection
Reset	Restore the router to its original factory default settings



### Power Supply

Item	Content
Standard Power	DC 12V/1.5A
Power range	DC 9~36V
Working current	3G : <750mA (12V)      4G : <850mA (12V)
Standby current	3G : <450mA (12V)      4G : <500mA (12V)

### Physical Characteristics

Item	Content
Housing	Metal shell, shock proof design
Dimensions	244x139x36 mm
Weight	940g

### Other Specification

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

## 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

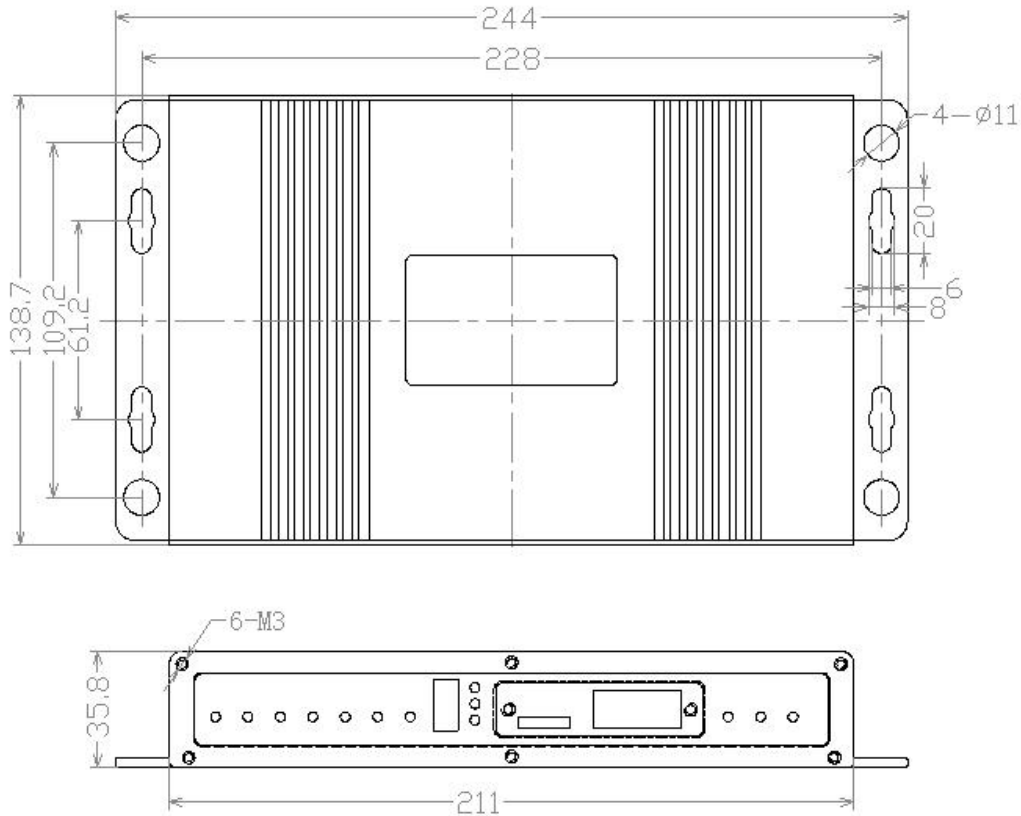
Name	Quantity	Remark
Router host	1	
Cellular antenna (Male SMA)	1(Notes 1)	
GPS antenna (Male SMA)	1	optional
WIFI antenna (Female SMA)	2	
Aviation plug power cord	1	
Network cable	1	
Console cable	1	optional
Power adapter	1	optional
Manual CD	1	
Certification card	1	
Maintenance card	1	

Note1: Cellular antenna (Male SMA) 1 pcs for 3G configuration and 2 pcs for 4G configuration.

### 2.3 Installation and Cable Connection

#### Overall dimensions:

The dimensions below. (unit: mm)



### Installation of antenna:

Screw the SMA male pin of the cellular antenna to the female SMA interface of the router with sign “ANT-M”, “ANT-A” or “ANT”.

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

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

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

### 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 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 9~36V.

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: “PWR”, “SYS”, “SIM”, “GPS”, “Online”, “SSD”, “TF”, “LAN”, “WAN”, “WIFI”, “Signal Strength”.

Indicator Light	State	Introduction
PWR	ON	Router is powered on
	OFF	Router is powered off or in the shutdown period of schedule boot&shutdown
SYS	BLINK	System works properly
	OFF	System does not work
SIM	ON	Router identification to SIM card
	OFF	Router has not identification to SIM card
GPS	ON	GPS interface connected/is data communication
	OFF	GPS interface does not connected
Online	ON	Router has logged on network
	BLINK	Router not connected on the network platform
	OFF	Router hasn't logged on network
SSD	ON	Router identification to hard disk
	BLINK	Router reading or writing hard disk data
	OFF	Router has not identified to hard disk
TF	ON	Router identification to TF card
	OFF	Router has not identification to TF card
LAN	OFF	The corresponding interface of switch is not connected
	BLINK	The corresponding interface of switch is communication
	ON / BLINK	The corresponding interface of switch is connected /communicating
WAN	OFF	The interface of WAN is not connected
	BLINK	The interface of WAN is communicating
	ON	The interface of WAN is connected /communicating
WIFI	OFF	WIFI is not active
	ON	WIFI is active
Signal Strength	One Light ON	Signal strength is weak

	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.

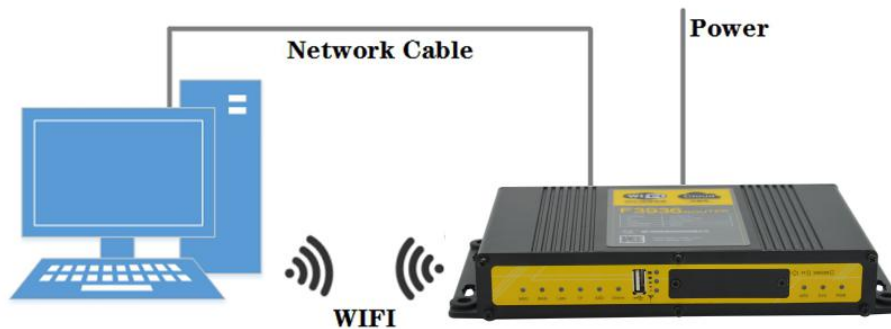


## Chapter 3 Configuration and Management

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 (192.168.1.1).

### 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 192.168.1.1:90 on address bar, then press the botton 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	<input type="text" value="admin"/>
Router Password	<input type="password" value="••••"/>
Re-enter to confirm	<input type="password" value="••••"/>

Change Password

After access to the information main page

<p><b>Menu</b></p> <ul style="list-style-type: none"> <li><a href="#">Setup</a></li> <li><a href="#">Wireless</a></li> <li><a href="#">Services</a></li> <li><a href="#">Security</a></li> <li><a href="#">NAT</a></li> <li><a href="#">Access Restrictions</a></li> <li><a href="#">QoS Setting</a></li> <li><a href="#">Applications</a></li> <li><a href="#">Administration</a></li> <li><a href="#">Status</a></li> </ul>	<p><b>System Information</b></p> <p><b>Router</b></p> <table> <tr><td>Router Name</td><td>Four-Faith</td></tr> <tr><td>Router Model</td><td>Four-Faith Router</td></tr> <tr><td>LAN MAC</td><td>00:0C:43:AD:B9:16</td></tr> <tr><td>WAN MAC</td><td>00:0C:43:AD:B9:16</td></tr> <tr><td>Wireless MAC</td><td>00:0C:43:AD:B9:18</td></tr> <tr><td>WAN IP</td><td>192.168.9.99</td></tr> <tr><td>LAN IP</td><td>192.168.1.1</td></tr> </table> <p><b>Wireless</b></p> <table> <tr><td>Radio</td><td>Radio is On</td></tr> <tr><td>Mode</td><td>AP</td></tr> <tr><td>Network</td><td>Mixed</td></tr> <tr><td>SSID</td><td>SSID</td></tr> <tr><td>Channel</td><td>10 (2457 MHz)</td></tr> <tr><td>TX Power</td><td>100 mW</td></tr> <tr><td>Rate</td><td>300 Mb/s</td></tr> </table> <p><b>Wireless Packet Info</b></p> <table> <tr><td>Received (RX)</td><td>0 OK, no error</td></tr> <tr><td>Transmitted (TX)</td><td>0 OK, no error</td></tr> </table>	Router Name	Four-Faith	Router Model	Four-Faith Router	LAN MAC	00:0C:43:AD:B9:16	WAN MAC	00:0C:43:AD:B9:16	Wireless MAC	00:0C:43:AD:B9:18	WAN IP	192.168.9.99	LAN IP	192.168.1.1	Radio	Radio is On	Mode	AP	Network	Mixed	SSID	SSID	Channel	10 (2457 MHz)	TX Power	100 mW	Rate	300 Mb/s	Received (RX)	0 OK, no error	Transmitted (TX)	0 OK, no error	<p><b>Services</b></p> <table> <tr><td>DHCP Server</td><td>Enabled</td></tr> <tr><td>ff-radauth</td><td>Disabled</td></tr> <tr><td>USB Support</td><td>Enabled</td></tr> </table> <p><b>Memory</b></p> <table> <tr><td>Total Available</td><td>249.2 MB / 256.0 MB</td></tr> <tr><td>Free</td><td>184.4 MB / 249.2 MB</td></tr> <tr><td>Used</td><td>64.8 MB / 249.2 MB</td></tr> <tr><td>Buffers</td><td>37.9 MB / 64.8 MB</td></tr> <tr><td>Cached</td><td>8.3 MB / 64.8 MB</td></tr> <tr><td>Active</td><td>15.6 MB / 64.8 MB</td></tr> <tr><td>Inactive</td><td>32.9 MB / 64.8 MB</td></tr> </table>	DHCP Server	Enabled	ff-radauth	Disabled	USB Support	Enabled	Total Available	249.2 MB / 256.0 MB	Free	184.4 MB / 249.2 MB	Used	64.8 MB / 249.2 MB	Buffers	37.9 MB / 64.8 MB	Cached	8.3 MB / 64.8 MB	Active	15.6 MB / 64.8 MB	Inactive	32.9 MB / 64.8 MB
Router Name	Four-Faith																																																					
Router Model	Four-Faith Router																																																					
LAN MAC	00:0C:43:AD:B9:16																																																					
WAN MAC	00:0C:43:AD:B9:16																																																					
Wireless MAC	00:0C:43:AD:B9:18																																																					
WAN IP	192.168.9.99																																																					
LAN IP	192.168.1.1																																																					
Radio	Radio is On																																																					
Mode	AP																																																					
Network	Mixed																																																					
SSID	SSID																																																					
Channel	10 (2457 MHz)																																																					
TX Power	100 mW																																																					
Rate	300 Mb/s																																																					
Received (RX)	0 OK, no error																																																					
Transmitted (TX)	0 OK, no error																																																					
DHCP Server	Enabled																																																					
ff-radauth	Disabled																																																					
USB Support	Enabled																																																					
Total Available	249.2 MB / 256.0 MB																																																					
Free	184.4 MB / 249.2 MB																																																					
Used	64.8 MB / 249.2 MB																																																					
Buffers	37.9 MB / 64.8 MB																																																					
Cached	8.3 MB / 64.8 MB																																																					
Active	15.6 MB / 64.8 MB																																																					
Inactive	32.9 MB / 64.8 MB																																																					

<p><b>Menu</b></p> <ul style="list-style-type: none"> <li><a href="#">Setup</a></li> <li><a href="#">Wireless</a></li> <li><a href="#">Services</a></li> <li><a href="#">Security</a></li> <li><a href="#">NAT</a></li> <li><a href="#">Access Restrictions</a></li> <li><a href="#">QoS Setting</a></li> <li><a href="#">Applications</a></li> <li><a href="#">Administration</a></li> <li><a href="#">Status</a></li> </ul>	<p><b>System Information</b></p> <p><b>Router</b></p> <table> <tr><td>Router Name</td><td>Four-Faith</td></tr> <tr><td>Router Model</td><td>Four-Faith Router</td></tr> <tr><td>LAN MAC</td><td>00:0C:43:AD:B9:16</td></tr> <tr><td>WAN MAC</td><td>00:0C:43:AD:B9:16</td></tr> <tr><td>Wireless MAC</td><td>00:0C:43:AD:B9:18</td></tr> <tr><td>WAN IP</td><td>192.168.9.99</td></tr> <tr><td>LAN IP</td><td>192.168.1.1</td></tr> </table> <p><b>Wireless</b></p> <table> <tr><td>Radio</td><td>Radio is On</td></tr> <tr><td>Mode</td><td>AP</td></tr> <tr><td>Network</td><td>Mixed</td></tr> <tr><td>SSID</td><td>SSID</td></tr> <tr><td>Channel</td><td>10 (2457 MHz)</td></tr> <tr><td>TX Power</td><td>100 mW</td></tr> <tr><td>Rate</td><td>300 Mb/s</td></tr> </table> <p><b>Wireless Packet Info</b></p> <table> <tr><td>Received (RX)</td><td>0 OK, no error</td></tr> <tr><td>Transmitted (TX)</td><td>0 OK, no error</td></tr> </table>	Router Name	Four-Faith	Router Model	Four-Faith Router	LAN MAC	00:0C:43:AD:B9:16	WAN MAC	00:0C:43:AD:B9:16	Wireless MAC	00:0C:43:AD:B9:18	WAN IP	192.168.9.99	LAN IP	192.168.1.1	Radio	Radio is On	Mode	AP	Network	Mixed	SSID	SSID	Channel	10 (2457 MHz)	TX Power	100 mW	Rate	300 Mb/s	Received (RX)	0 OK, no error	Transmitted (TX)	0 OK, no error	<p><b>Services</b></p> <table> <tr><td>DHCP Server</td><td>Enabled</td></tr> <tr><td>ff-radauth</td><td>Disabled</td></tr> <tr><td>USB Support</td><td>Enabled</td></tr> </table> <p><b>Memory</b></p> <table> <tr><td>Total Available</td><td>249.2 MB / 256.0 MB</td></tr> <tr><td>Free</td><td>184.4 MB / 249.2 MB</td></tr> <tr><td>Used</td><td>64.8 MB / 249.2 MB</td></tr> <tr><td>Buffers</td><td>37.9 MB / 64.8 MB</td></tr> <tr><td>Cached</td><td>8.3 MB / 64.8 MB</td></tr> <tr><td>Active</td><td>15.6 MB / 64.8 MB</td></tr> <tr><td>Inactive</td><td>32.9 MB / 64.8 MB</td></tr> </table>	DHCP Server	Enabled	ff-radauth	Disabled	USB Support	Enabled	Total Available	249.2 MB / 256.0 MB	Free	184.4 MB / 249.2 MB	Used	64.8 MB / 249.2 MB	Buffers	37.9 MB / 64.8 MB	Cached	8.3 MB / 64.8 MB	Active	15.6 MB / 64.8 MB	Inactive	32.9 MB / 64.8 MB
Router Name	Four-Faith																																																					
Router Model	Four-Faith Router																																																					
LAN MAC	00:0C:43:AD:B9:16																																																					
WAN MAC	00:0C:43:AD:B9:16																																																					
Wireless MAC	00:0C:43:AD:B9:18																																																					
WAN IP	192.168.9.99																																																					
LAN IP	192.168.1.1																																																					
Radio	Radio is On																																																					
Mode	AP																																																					
Network	Mixed																																																					
SSID	SSID																																																					
Channel	10 (2457 MHz)																																																					
TX Power	100 mW																																																					
Rate	300 Mb/s																																																					
Received (RX)	0 OK, no error																																																					
Transmitted (TX)	0 OK, no error																																																					
DHCP Server	Enabled																																																					
ff-radauth	Disabled																																																					
USB Support	Enabled																																																					
Total Available	249.2 MB / 256.0 MB																																																					
Free	184.4 MB / 249.2 MB																																																					
Used	64.8 MB / 249.2 MB																																																					
Buffers	37.9 MB / 64.8 MB																																																					
Cached	8.3 MB / 64.8 MB																																																					
Active	15.6 MB / 64.8 MB																																																					
Inactive	32.9 MB / 64.8 MB																																																					

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

Six Ways: Disabled, Static IP, Automatic DHCP, PPPOE, 3G/UNMTS/4G/LTE(Optional),dhcp-4G(Optional).

### Disabled

Connection Type

Forbid the setting of WAN port connection type

### Static IP

Connection Type

WAN IP Address

Subnet Mask

Gateway

Static DNS 1

Static DNS 2

Static DNS 3

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

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

**Gateway:** Users set gateway by their own or ISP assigns

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

### Automatic Configuration-DHCP

Connection Type

IP address of WAN port gets automatic via DHCP

### PPPOE

Connection Type

User Name

Password   Unmask

Service Name

PPP Compression (MPPC)  Enable  Disable

T-Home VDSL VLAN 7/8 Tagging  Enable  Disable

MPPE Encryption

Single Line Multi Link

**User Name:** login the Internet

**Password:** login the Internet

**Service Name:** provided by ISP server, if not, keep it null

**PPP Compression (MPPC):** provides a method to negotiation and use of compressed in PPP encapsulation link protocol

**T-Home VDSL VLAN 7/8 Tagging:** enable to support the front of the modem is vdsl

**MPPE Encryption:** Microsoft point to point encryption. It is used to encrypt the point-to-point link connection agreement of the encrypted data packet

**Single Line Multi Link:** enable single line link or disable multi link

### 3G/UMTS/4G/LTE (可选)

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	<input type="text" value="Auto"/>
-----------------	-----------------------------------

**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.

### Connection Strategy

Connection Strategy  Connect on Demand: Max Idle Time  Min.  Keep Alive: Redial Period  Sec.

**Connection Strategy:** one way is Connect on Demand, that is the link turnoff automatic under the situation that the ready link is idle and idle time meets users' configuration requirement, but it will connect again if users visit Internet. The other way is to keep alive, that is the link enable to dial again when reaching the re-dial period users set after disconnection.

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 (Spanning 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



## Dhcp-4G (可选)

### WAN Connection Type

Connection Type	dhcp-4G		
User Name	card		
Password	••••	<input type="checkbox"/> Unmask	
Keep Online Detection	Ping		
Detection Interval	120 Sec.		
Primary Detection Server IP	208	67	222
Backup Detection Server IP	208	67	220
Wan Nat	<input checked="" type="radio"/> Enable <input type="radio"/> Disable		
STP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable		

### 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.

**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".

### Optional Configuration

Router Name	Four-Faith
Host Name	
Domain Name	
MTU	Auto 1500

**Router Name:** set router name

**Host Name:** ISP provides

**Domain Name:** ISP provides

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

**Router Internal Network Settings**

**Router IP**

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

**Local IP Address:** IP address of the router

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

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

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

**Network Address Server Settings (DHCP)**

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

DHCP Type	DHCP Server
DHCP Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Start IP Address	192.168.1.100
Maximum DHCP Users	50
Client Lease Time	1440 minutes
Static DNS 1	0.0.0.0
Static DNS 2	0.0.0.0
Static DNS 3	0.0.0.0
WINS	0.0.0.0
Use DNSMasq for DHCP	<input checked="" type="checkbox"/>
Use DNSMasq for DNS	<input checked="" type="checkbox"/>
DHCP-Authoritative	<input checked="" type="checkbox"/>

**DHCP Type:** DHCP Server and DHCP Forwarder

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



DHCP Type DHCP Forwarder

DHCP Server 0 . 0 . 0 . 0

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

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

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

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

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

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

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

**Time Settings**

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

NTP Client  Enable  Disable

Time Zone UTC+08:00

Summer Time (DST) last Sun Mar - last Sun Oct

Server IP/Name

**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 2012 - 3 - 15 9:16:20 Get 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:** router currently support DynDNS, freedns, Zonedit, 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

Enable
  Disable

---

Clone LAN MAC 00 : AA : BB : CC : DD : 43

---

Clone WAN MAC 00 : AA : BB : CC : DD : 44

[Get Current PC MAC Address](#)

---

Clone Wireless MAC 00 : AA : BB : CC : DD : 45

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

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

**3.3.1.4 Advanced Router**

**Operating Mode:** Gateway and Router

**Operating Mode**

Operating Mode Gateway ▼

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

### Dynamic Routing

**Dynamic Routing**

Interface Disable ▾

Dynamic Routing enables the router to automatically adjust to physical changes in the network's layout and exchange routing tables with other routers. The router determines the network packets' route based on the fewest number of hops between the source and destination.

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

**Note:** Dynamic Routing is not available in Gateway mode

### Static Routing

**Static Routing**

Select set number 1 ( ) ▾ Delete

Route Name

Metric

Destination LAN NET ...

Subnet Mask ...

Gateway ...

Interface LAN & WLAN ▾

Show Routing Table

**Select set number:** 1-50

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

**Metric:** 0-9999

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

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

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

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

**Show Routing Table**

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

### 3.3.1.5 VLANs

#### VLAN

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

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

### 3.3.1.6 Networking

**Bridging**

**Create Bridge**

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500
----------	-----	-----	-----	------	-------	-----	------

[Add](#)

**Assign to Bridge**

[Add](#)

**Current Bridging Table**

Bridge Name	STP.enabled	Interfaces
br0	no	vlan1 ra0

[Add/Delete/Refresh](#)

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

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

**Current Bridging Table:** shows current bridging table

**Create steps as below:**

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

**Create Bridge**

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500
Bridge 1	br1	STP	On	Prio	32768	MTU	1500

[Add](#) [Delete](#)

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



**Create Bridge**

Bridge 0	br0	STP	Off	Prio	32768	MTU	1500	Delete
Bridge 1	br1	STP	On	Prio	32768	MTU	1500	Delete
IP Address	0 . 0 . 0 . 0							
Subnet Mask	0 . 0 . 0 . 0							
<input type="button" value="Add"/>								

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

**Note:** Only create a bridge can apply it.

**Assign to Bridge**

Assignment 0	none	Interface	ra0	Prio	63	Delete
<input type="button" value="Add"/>						

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

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

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

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

**Current Bridging Table**

Bridge Name	STP enabled	Interfaces
br0	no	vlan1
br1	no	ra0

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

Port Setup

Network Configuration eth2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration vlan1	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration ra0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration apcli0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds1	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds2	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration wds3	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default
Network Configuration br0	<input type="radio"/> Unbridged	<input checked="" type="radio"/> Default

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

Network Configuration ra0  Unbridged  Default

MTU

Multicast forwarding  Enable  Disable

Masquerade / NAT  Enable  Disable

IP Address ...

Subnet Mask ...

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

MTU: maximum transfer unit

Multicast forwarding: enable or disable multicast forwarding

Masquerade/NAT: enable or disable Masquerade/NAT

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

Subnet Mask: set the port's subnet mask

**Multiple DHCP Server**

DHCP 0   Start  Max  Leasetime

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

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



### 3.3.2 Wireless

#### 3.3.2.1 Basic Settings

**Wireless Physical Interface wl0 [2.4 GHz]**

Wireless Network  Enable  Disable

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

Wireless Mode	AP
Wireless Network Mode	N-Only
802.11n Transmission Mode	Mixed
Wireless Network Name (SSID)	dd-junjinlee
Wireless Channel	11 - 2.462 GHz
Channel Width	40 MHz
Extension Channel	upper
Wireless SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Network Configuration	<input type="radio"/> Unbridged <input checked="" type="radio"/> Bridged

**Virtual Interfaces**

**Wireless Network:** “Eanble”, radio on.  
 “Disable”, radio off.

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

**Wireless Network Mode:**

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

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

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

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

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

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

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

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

transmission mode.

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

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

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

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

**Channel Width:** 20MHZ and 40MHZ.。

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

**Wireless SSID Broadcast:**

**Enable:** SSID broadcasting.

**Disable:** Hidden SSID.

**Network Configuration:**

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

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

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

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

**Virtual Interfaces**

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

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

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

**Note :** Save your changes, after changing the "Wireless Mode", "Wireless Network Mode",

"wireless width", "broadband" option, please click on this button, and then configure the other options.

### 3.3.2.2 Wireless Security

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

**Wireless Security w10**

---

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

Security Mode Disabled

Save
Apply Settings

**Wireless Security w10**

---

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

Security Mode WEP

Authentication Type  Open  Shared Key

Default Transmit Key  1  2  3  4

Encryption 64 bits 10 hex digits/5 ASCII

ASCII/HEX  ASCII  HEX

Passphrase 1111111111111111 Generate

Key 1 2627F68597

Key 2 15AD1DD294

Key 3 DDC4761939

Key 4 31F1ADB558

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

**Authentication Type:** Open or shared key.

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

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

characters. Valid hexadecimal characters are "0"- "9" and "A"- "F".

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

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

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

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

**Wireless Security w10**

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

Security Mode: WPA Personal

WPA Algorithms: AES

WPA Shared Key: [masked]  Unmask

Key Renewal Interval (in seconds): 3600 (Default: 3600, Range: 1 - 99999)

Save Apply Settings

**WPA Personal/WPA2 Personal/WPA2 Person Mixed:** , TKIP/AES/TKIP+AES , dynamic encryption keys. TKIP + AES, self-applicable TKIP or AES. WPA Person Mixed, allow WPA Personal and WPA2 Personal client mix.

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

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

**Wireless Security w10**

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

Security Mode: WPA Enterprise

WPA Algorithms: AES

Radius Auth Server Address: 192, 168, 1, 110

Radius Auth Server Port: 1812 (Default: 1812)

Radius Auth Shared Secret: [masked]  Unmask

Key Renewal Interval (in seconds): 3600

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

**WPA Algorithms:** AES/TKIP/TPIP+AES.

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

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

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

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

### 3.3.3 Services

#### DHCP Client

**DHCP Client**

Set Vendorclass

Request IP

**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	<input type="radio"/> Web	<input type="radio"/> USB Storage
Remote Server	<input type="text"/>			

**Syslog Out Mode:** four log mode

**Net:** the log information output to a syslog server

**Console:** the log information output to console port

**Web:** the log will be shown in the web page(Starus->Weblog)

**USB Storage:** the log will be saved in the USB device for access

**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



**Ttraff Daemon:** enable or disable wan traffic counter function

### 3.3.3.1 USB

Enable the service to identify the U disk connected to the router, TF card or SD memory card, and use these types of storage media. Specific setup instructions screenshot below



**Storage Media Priority :** used to choose which storage media to storage files.

**Storage List :** list the storage media that the router recognized

### 3.3.3.2 FTP Server

Enable the service to use the router as a simple FTP application server, the user can do an FTP client to upload or download files to an external router U disk, TF card or SD memory card inside.



FTP Server		Help
<p><b>FTP Server</b></p> <p>FTPD <input checked="" type="radio"/> Enable <input type="radio"/> Disable</p> <p>Server Port <input type="text" value="21"/> (Default: 21)</p> <p>Login TimeOut <input type="text" value="20"/> (Default: 20)</p> <p>IDLE TimeOut <input type="text" value="240"/> (Default: 240)</p> <p>admin <input type="text" value="admin"/> (Default: admin)</p> <p>Password <input type="text" value="admin"/> (Default: admin)</p> <p>Confirm <input type="text" value="admin"/> (Default: admin)</p> <p>Anonymous Login <input type="radio"/> Enable <input checked="" type="radio"/> Disable (Default: Disable)</p> <p><a href="#">Manage Account</a></p>		<p><b>Help</b> <a href="#">more...</a></p> <p><b>FTPD:</b> enable/disable ftp server</p> <hr/> <p><b>Server Port:</b> ftp server port</p> <hr/> <p><b>Login TimeOut:</b> Login timeout</p> <hr/> <p><b>IDLE TimeOut:</b> idle timeout</p> <hr/> <p><b>Manage Account:</b> add/delete/account,manage account</p>

**Server Port:** Router as a local FTP server listening port, the default is 21

**admin:** Log in to the router FTP server administrator account, the default user name “admin” router WEB configuration management


**Password:** Log on to the FTP server to the router's administrator password, the default is “admin”

### 3.3.3.3 Hotspot

The service will enable wireless WIFI router for the bus, chain business model and other companies to provide customers with free internet access after authentication, while in play before certification can be played online business advertising and promotional activities specified function.

**Hotspot Portal**

**Wifidog**



**Wifidog**  
A captive portal suite

Wifidog daemon	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Gateway ID	<input type="text" value="57419230"/>	
Web Server Name	<input type="text" value="WiFiDog"/>	
Port	<input type="text" value="2060"/>	(Default: 2060, Range: 1 - 65535)
Max Users	<input type="text" value="50"/>	(Default: 10, Range: 1 - 50)
Check Interval (in sec.)	<input type="text" value="180"/>	(Default: 60, Range: 1 - 3600)
Client Timeout	<input type="text" value="10"/>	(Default: 5, Range: 1 - 99)
Trusted MAC List	<input type="text"/>	
AuthServer Hostname	<input type="text" value="192.168.6.1"/>	
AuthServer SSL Available	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
AuthServer HTTP Port	<input type="text" value="80"/>	(Default: 80, Range: 1 - 65535)
AuthServer Path	<input type="text" value="/"/>	
HTTP Server Authentication Support	<input type="radio"/> Enable <input checked="" type="radio"/> Disable	
HTML Message File for Wifidog	<input type="text"/>	
Firewall Ruleset	<div style="border: 1px solid #ccc; height: 40px; width: 100%;"></div>	

**Gateway ID:** hotspot remote / local authentication server that uniquely identifies the default is 57419230

**Port:** default 2060, range: 1 - 65535 Please note that no special circumstances do not arbitrarily modify

**Max Users:** limit the number of customers connected to the local WIFI Internet access, the default factory setting is 50

**Check Interval (in sec.):** Detection WIFI wireless client terminals (computers, mobile phones, etc.) and link status time interval of this station router, the default is 180 seconds

**Client Timeout (minutes):** detects the connection at the maximum timeout this station WIFI wireless router client terminals (computers, mobile phones, etc.) did not have the Internet to communicate, think 10 minutes by default. After this time customers need to re-authenticate login.

**AuthServer Hostname:** remote / local hotspot server host domain name or IP, if the authentication or jump in our station carried the router, please fill out this station router's LAN IP network segment

**AuthServer Path:** Remote / local server storage WIFI hotspot jump page advertisements path, the default is "/"

## 3.3.4 Security

### 3.3.4.1 Firewall

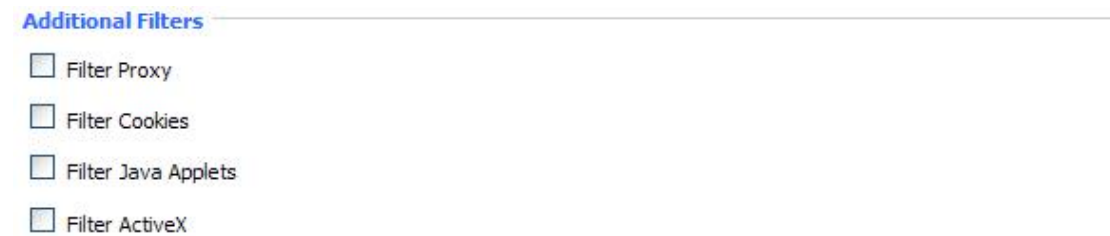
You can enable or disable the firewall, filter specific Internet data types, and prevent anonymous Internet requests, ultimately enhance network security.

#### Firewall Protection



Firewall 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



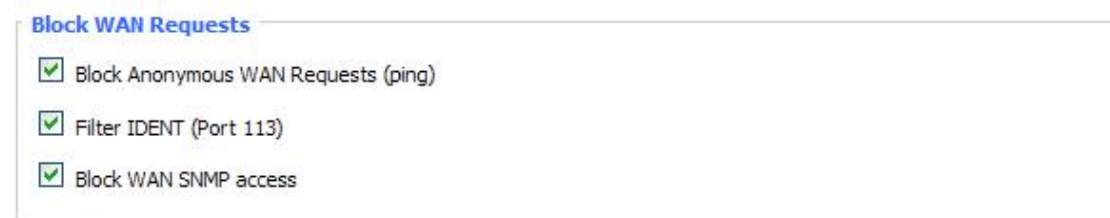
**Filter Proxy:** Wan proxy server may reduce the security of the gateway, Filtering Proxy will refuse any access to any wan proxy server. Click the check box to enable the function otherwise disabled.

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

this feature is enabled ,choose to disable allow anonymous Internet requests.

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

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

### Impede WAN DoS/Bruteforce

**Impede WAN DoS/Bruteforce**

Limit SSH Access

Limit Telnet Access

Limit PPTP Server Access

Limit L2TP Server Access

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

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

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

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

### Log Management

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

**Log**

Log  Enable  Disable

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

**Log**

Log  Enable  Disable

Log Level High

---

**Options**

Dropped Disable

Rejected Enable

Accepted Enable

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

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

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

**Incoming Log Table**

Source IP	Protocol	Destination Port Number	Rule
<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	183.60.48.60	UDP	8000	Accepted

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

### 3.3.5 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 ( )

Status:  Enable  Disable

Policy Name:

PCs:

Deny  Filter

Internet access during selected days and hours.

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  0 : 00 To 0 : 00

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

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



Website Blocking by URL Address

<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	<input type="text" value="00:AA:BB:CC:DD:EE"/>
MAC 02	<input type="text" value="00:00:00:00:00:00"/>
MAC 03	<input type="text" value="00:00:00:00:00:00"/>
MAC 04	<input type="text" value="00:00:00:00:00:00"/>
MAC 05	<input type="text" value="00:00:00:00:00:00"/>
MAC 06	<input type="text" value="00:00:00:00:00:00"/>
MAC 07	<input type="text" value="00:00:00:00:00:00"/>
MAC 08	<input type="text" value="00:00:00:00:00:00"/>
Enter the IP Address of the clients	
IP 01	192.168.1. <input type="text" value="15"/>
IP 02	192.168.1. <input type="text" value="0"/>
IP 03	192.168.1. <input type="text" value="0"/>
IP 04	192.168.1. <input type="text" value="0"/>
IP 05	192.168.1. <input type="text" value="0"/>
IP 06	192.168.1. <input type="text" value="0"/>
Enter the IP Range of the clients	
IP Range 01	<input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="19"/> ~ <input type="text" value="192"/> . <input type="text" value="168"/> . <input type="text" value="1"/> . <input type="text" value="30"/>
IP Range 02	<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"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="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,

Page 48 of 77

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 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 seen by users on the Internet and forwarded to your PC.

**Protocol:** Chose 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 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

QoS function can control the upload traffic and download traffic to balance the traffic, beside the block video is also a useful function.

**QoS Setting**

Start QoS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Uplink (kbps)	<input type="text" value="1000"/>
Downlink (kbps)	<input type="text" value="1000"/>
Max up rate for per user(kbps)	<input type="text" value="100"/>
Max down rate for per user(kbps)	<input type="text" value="100"/>

**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.

**Video Blacklist Settings**

Enable Video Restrictions  Enable Video/Flash Restrictions  Disable Video/Flash Restrictions

**Enable Video Restrictions :** Restrict the video access that connected to the router, like the MP4,MKV,AVI format and other common video format

**Enable Video and Flash Restriction :** Besides the common Video Format restriction ,it can also restrict the Flash format video.

### 3.3.8 Applications

#### 3.3.8.1 Serial Applications

There is a console port on 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 DTU (Data Terminal Unit).

**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 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 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"

### 3.3.8.2 GPS Settings(Optional)

Enable GPS	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
GPS Output Interface	<input checked="" type="checkbox"/> Net <input checked="" type="checkbox"/> Console
Protocol	TCP <input type="button" value="v"/>
GPS Center Address	<input type="text" value="0.0.0.0"/>
GPS Center Listening Port	<input type="text" value="5001"/>
GPS Information Update Interval	<input type="text" value="60"/>
GPS Speed Threshold	<input type="text" value="0"/>
Device ID	<input type="text" value="12345678"/> <input checked="" type="checkbox"/> Append the device ID to the tail of gps information
GPS Information Contents	<input checked="" type="checkbox"/> GPRMC <input checked="" type="checkbox"/> GPWGA <input checked="" type="checkbox"/> GPVTG <input checked="" type="checkbox"/> GPGSA <input checked="" type="checkbox"/> GPGSV <input checked="" type="checkbox"/> GPGLL

**Enable GPS:** Enable or disable GPS function

**GPS Output Interface:** This item selects the GPS output interface including network and serial port

**Protocol:** TCP mode or UDP mode

**GPS Center Address:** The GPS center’s IP Address or domain name

**GPS Center Listening Port:** The GPS center’s listening port.

**GPS Information Update Interval:** The time interval between two GPS information update, unit is second

**GPS Speed Threshold:** The GPS speed threshold of update gps information

**Device ID:** The ID of this device

**Append the device ID to the tail of gps information:** Whether append the ID to the GPS information

**GPS Information Contents:** GPS contents selection

When GPS output interface is serial port, we should set the following serial port settings:

Baudrate	<input type="text" value="115200"/> <input type="button" value="v"/>
Databit	<input type="text" value="8"/> <input type="button" value="v"/>
Stopbit	<input type="text" value="1"/> <input type="button" value="v"/>
Parity	None <input type="button" value="v"/>
Flow Control	None <input type="button" value="v"/>



### 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" value="....."/>
Router Password	<input type="password" value="....."/>
Re-enter to confirm	<input type="password" value="....."/>

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.

**Language Selection**

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

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

### Remote Upgrade

Remote Upgrade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Remote Server IP	<input type="text" value="xmsx0618.f3322.org"/>	
Remote Server Listen Port	<input type="text" value="8189"/>	(Default: 40001, Range: 1 - 65535)
Heart Interval	<input type="text" value="60"/>	(Default: 60Sec, Range: 1 - 999)
3G Flow Upload Interval	<input type="text" value="600"/>	(Default: 600Sec, Range: 1 - 86400)
AD Calc Upload Interval	<input type="text" value="600"/>	(Default: 600Sec, Range: 1 - 86400)
Device Number	<input type="text" value="11111115"/>	
Device Phone Number	<input type="text" value="13888888888"/>	
Device Type Description	<input type="text" value="Router"/>	
Customized Local Domain	<input type="text" value="m.16wifi.com"/>	
Advertising storage Type	<input checked="" type="radio"/> Local Storage (U-Disk / TF card) <input type="radio"/> WEB remote terminal server	
Local Auth Mode	<input checked="" type="radio"/> User Name And Password <input type="radio"/> Login without authentication	
Use Remote Authentication	<input type="radio"/> Yes <input checked="" type="radio"/> No	

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

### Remote Management Login Server

Remote Management Login Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Remote Login Server IP	<input type="text" value="192.168.8.234"/>	
Remote Login Server Port	<input type="text" value="9001"/>	(Default: 44008, Range: 1 - 65535)

**Remote Management Login Server:** In the case of more than one servers, the remote management login server is a general server. Connect the router to this login server, the login server will assign an available server IP and port for the router to connect for remote management.

### Firmware Upgrade

Firmware Upgrade	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	
Upgrade Server IP	<input type="text" value="xmsx0618.f3322.org"/>	
Upgrade Server Port	<input type="text" value="882"/>	(Default: 882, Range: 1 - 65535)

**Firmware Upgrade:** custom-developed remote server for this station router upgrading firmware.

**Users Internet Records Reported**

Users Internet Records Reported	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Server IP Address/Domain Name:	<input type="text" value="42.121.16.56"/>
Server Port:	<input type="text" value="50001"/> (Default: 50001, Range: 1 - 65535)
Heartbeat Interval:	<input type="text" value="60"/> (Default: 60Sec.Range: 1 - 999)

**User Internet Records Reported:** the router clients’ webpages record submitted to the remote server center.

### 3.3.9.2 Keep Alive

#### Schedule Boot&Shutdown

The user can set the startup or shutdown time:

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

**Schedule Boot&Shutdown**

Schedule Boot&Shutdown	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Match	<input checked="" type="radio"/> Day <input type="radio"/> Weekday <input type="radio"/> Days <input type="radio"/> Weekdays
Shutdown Time	<input type="text" value="08"/> : <input type="text" value="07"/>
Shutdown Date	* <input type="text" value="01"/> Sunday <input type="text" value="Sunday"/>
Boot Time	<input type="text" value="09"/> : <input type="text" value="07"/>
Boot Date	* <input type="text" value="01"/> Sunday <input type="text" value="Sunday"/>

#### Schedule Reboot

**Schedule Reboot**

Schedule Reboot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Interval (in seconds)	<input checked="" type="radio"/> <input type="text" value="3600"/>
At a set Time	<input type="radio"/> <input type="text" value="00"/> : <input type="text" value="00"/> Sunday

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

Regularly after xxx seconds.

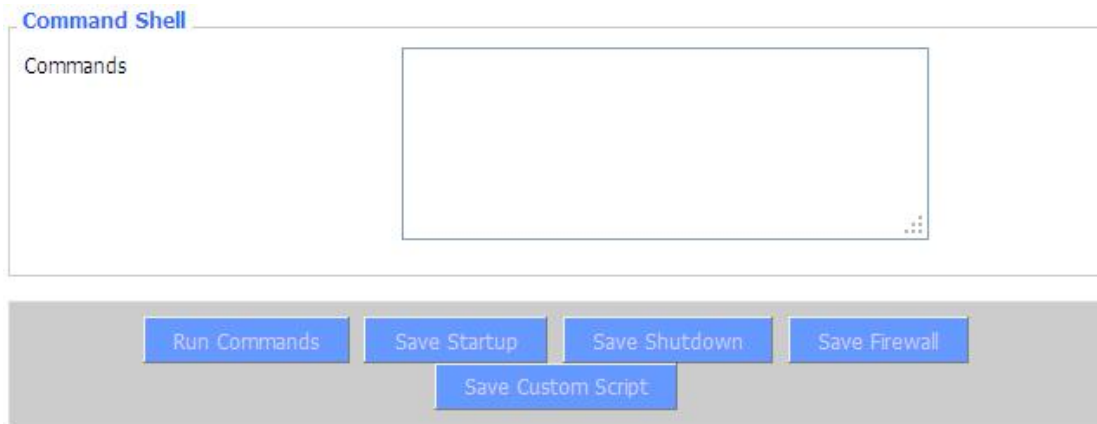
At a specific date time each week or everyday.

**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.



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

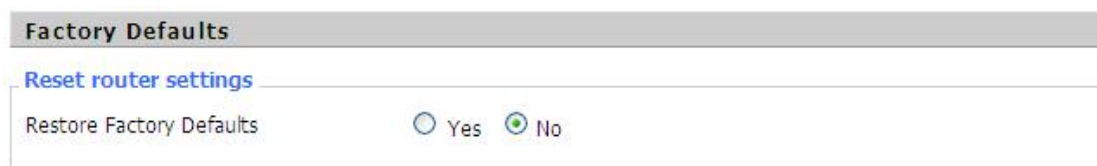
**Startup:** You can save some command lines to be executed at startup's router. Fill the text area with commands (only one command by row) and click Save Startup.

**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



**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 192.168.1.1 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	255172 kB / 262144 kB	 97%
Free	188020 kB / 255172 kB	 74%
Used	67152 kB / 255172 kB	 26%
Buffers	38872 kB / 67152 kB	 58%
Cached	8924 kB / 67152 kB	 13%
Active	16640 kB / 67152 kB	 25%
Inactive	33504 kB / 67152 kB	 50%

**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

Network

IP Filter Max Connections	16384	
Active IP Connections	<u>96</u>	 1%

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

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

Active IP Connections

53

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

**Active IP Connections:** total active IP connections

**Protocol:** connection protocol

**Timeouts:** connection timeouts, unit is second

**Source Address:** source IP address

**Remote Address:** remote IP address

**Service Name:** connecting service port

**Status:** displayed status

### 3.3.10.2 WAN

Connection Type                      Automatic Configuration - DHCP

Connection Uptime                      Not available

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

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

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

**IP Address:** IP address of router WAN

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

**Gateway:** the gateway of router WAN

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

Remaining Lease Time 0 days 23:38:43

DHCP Release

DHCP Renew

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

**DHCP Release:** release DHCP address

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

Login Status

Disconnected

Connect

**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

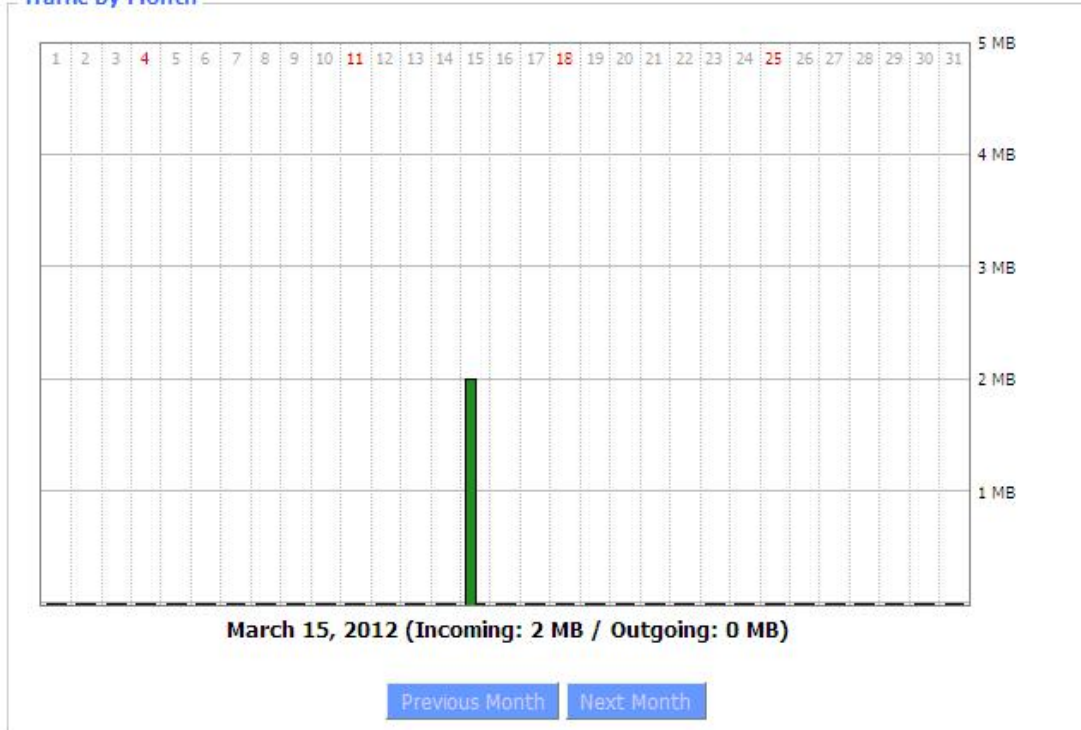
**Signal Status:** signal intensity of the module in 3G/UMTS way

**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	00:21:5C:33:4D:29	1 day 00:00:00	
jack-lincw	192.168.1.117	44:37:E6:3F:45:54	1 day 00:00:00	
*	192.168.1.149	00:0C:E7:00:00:00	1 day 00:00:00	

**Host Name:** host name of LAN client

**IP Address:** IP address of the client

**MAC Address:** MAC address of the client

**Expires:** the expiry the client rents the IP address

**Delete:** click to delete DHCP client

Connected PPPOE Clients

Interface	User Name	Local IP	Delete
ppp0	hometest	192.168.10.10	

**Interface:** the interface assigned by dial-up system

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

**Local IP:** IP address assigned by PPPoE client

**Delete:** click to delete PPPoE client

Connected L2TP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	

**Interface:** the interface assigned by dial-up system

**Local IP:** tunnel IP address of local L2TP

**Remote IP:** tunnel IP address of L2TP server

**Delete:** click to disconnect L2TP

Connected L2TP Clients

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

**Interface:** the interface assigned by dial-up system

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

**Local IP:** tunnel IP address of L2TP client

**Remote IP:** IP address of L2TP client

**Delete:** click to delete L2TP client

Connected PPTP Server

Interface	Local IP	Remote IP	Delete
ppp0	172.168.8.2	172.168.8.1	



**Interface:** the interface assigned by dial-up system

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

**Remote IP:** tunnel IP address of PPTP server

**Delete:** click to disconnect PPTP

**Connected PPTP Clients**

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

**Interface:** the interface assigned by dial-up system

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

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

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

**Delete:** click to delete PPTP client

### 3.3.10.4 Wireless

**Wireless Status**

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

**MAC Address:** MAC address of wireless client

**Radio:** display whether radio is on or not

**Mode:** wireless mode

**Network:** wireless network mode

**SSID:** wireless network name

**Channel:** wireless network channel

**TX Power:** reflection power of wireless network

**Rate:** reflection rate of wireless network

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

**PPTP Status:** show wireless pptp status



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

**Received (RX):** received data packet

**Transmitted (TX):** transmitted data packet

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

**MAC Address:** MAC address of wireless client

**Interface:** interface of wireless client

**Uptime:** connecting uptime of wireless client

**TX Rate:** transmit rate of wireless client

**RX Rate:** receive rate of wireless client

**Signal:** the signal of wireless client

**Noise:** the noise of wireless client

**SNR:** the signal to noise ratio of wireless client

**Signal Quality:** signal quality of wireless client

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

[Refresh](#)   [Close](#)

**Neighbor's Wireless Network:** display other networks nearby

**SSID:** the name of wireless network nearby

**Mode:** operating mode of wireless network nearby

**MAC Address:** MAC address of the wireless nearby

**Channel:** the channel of the wireless nearby

**Rssi:** signal intensity of the wireless nearby

**Noise:** the noise of the wireless nearby

**Beacon:** signal beacon of the wireless nearby

**Open:** the wireless nearby is open or not

**Dtim:** delivery traffic indication message of the wireless nearby

**Rate:** speed rate of the wireless nearby

**Join Site:** click to join wireless network nearby

### 3.3.10.5 Device Management

#### Device Management

##### Connection Status

Status	Enabled
Server Ip And Port	192.168.8.234:9100
Connection status	Connecting to Server...
Active Time	

**Connection Status:**display the connection status with the management platform.

**Status:**if the device management function is opened or not.

**Server Ip And Port:**the ip address and port of the management server.

**Connection status:**show if the device is connected to the server.

**Active Time:**show the during time that connected to server.

#### Fireware Upgrade

##### Upgrade Status

Status	no update, waiting...
Server Ip And Port	42.121.16.56:882
update version	
upgrade progress	

**Upgrade Status:** show the status of the firmware upgrade.

**Status:**show if the new firmware is in update.

**Server Ip And Port:**show the firmware upgrade server's ip and port.

**update version:**show the version in upgrading.

**upgrade progress:**show the progress of the upgrading firmware.

#### rsync update local ad file

##### rsync update status

Status	no update, waiting...
update info	
update progress	

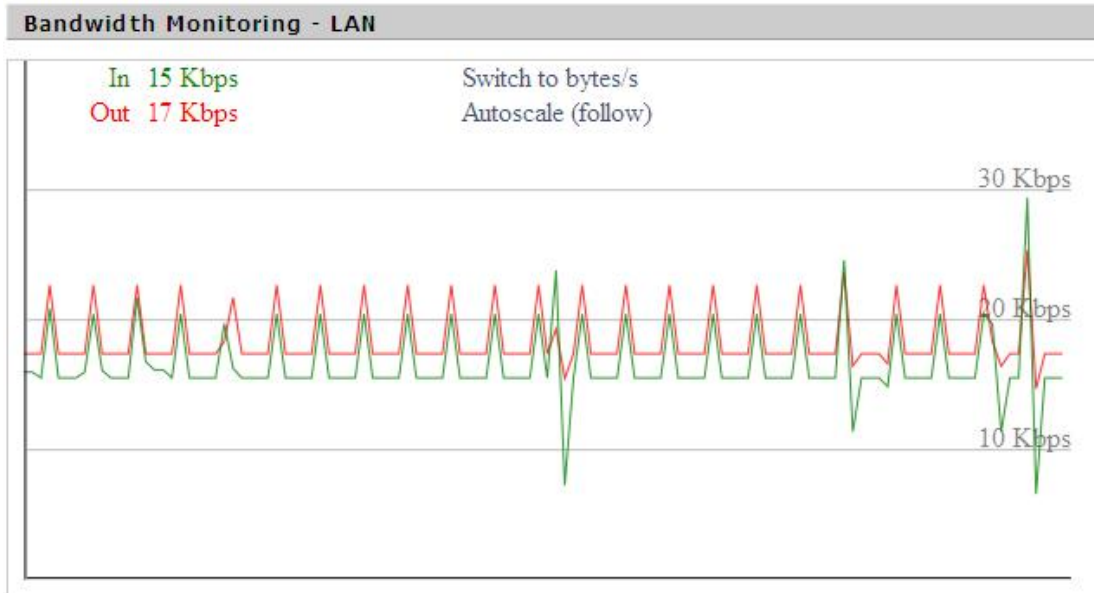
**rsync update status:**show the status of the rsync update

**Status:**show if the rsync is updating.

**Update info:**show the info of the update status.

Update progress:show the progress of the rsync update.

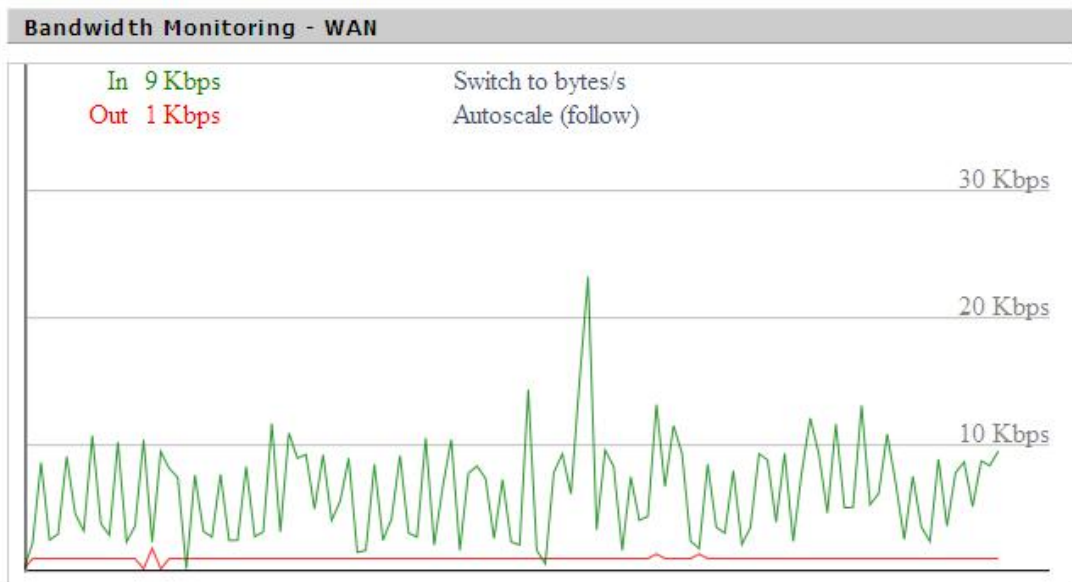
### 3.3.10.6 Bandwidth



Bandwidth Monitoring-LAN Graph

**abscissa axis:** time

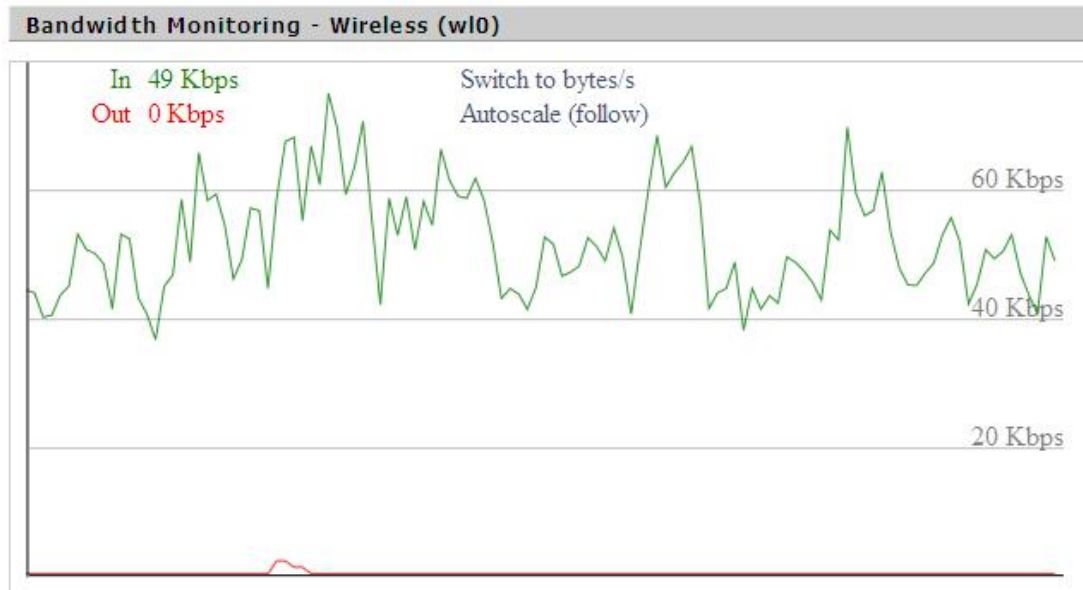
**vertical axis:** speed rate



Bandwidth Monitoring-WAN Graph

**abscissa axis:** time

vertical axis: speed rate



Bandwidth Monitoring-Wireless (W10) Graph

abscissa axis: time

vertical axis: speed rate

### 3.3.10.7 Sys-Info

#### Router

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

**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

**Wireless MAC:** MAC address of the wireless

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

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

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

**Radio:** display whether radio is on or not

**Mode:** wireless mode

**Network:** wireless network mode

**SSID:** wireless network name

**Channel:** wireless network channel

**TX Power:** reflection power of wireless network

**Rate:** reflection rate of wireless network

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

**Received (RX):** received data packet

**Transmitted (TX):** transmitted data packet

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

**MAC Address:** MAC address of wireless client

**Interface:** interface of wireless client

**Uptime:** connecting uptime of wireless client

**TX Rate:** transmit rate of wireless client

**RX Rate:** receive rate of wireless client

**Signal:** the signal of wireless client

**Noise:** the noise of wireless client

**SNR:** the signal to noise ratio of wireless client

**Signal Quality:** signal quality of wireless client

#### Services

DHCP Server	Enabled
ff-radauth	Disabled
USB Support	Disabled

**DHCP Server:** enabled or disabled

**ff-radauth:** enabled or disabled

**USB Support:** enabled or disabled

#### Memory

Total Available	249.2 MB / 256.0 MB
Free	183.4 MB / 249.2 MB
Used	65.7 MB / 249.2 MB
Buffers	38.0 MB / 65.7 MB
Cached	8.7 MB / 65.7 MB
Active	16.4 MB / 65.7 MB
Inactive	32.6 MB / 65.7 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

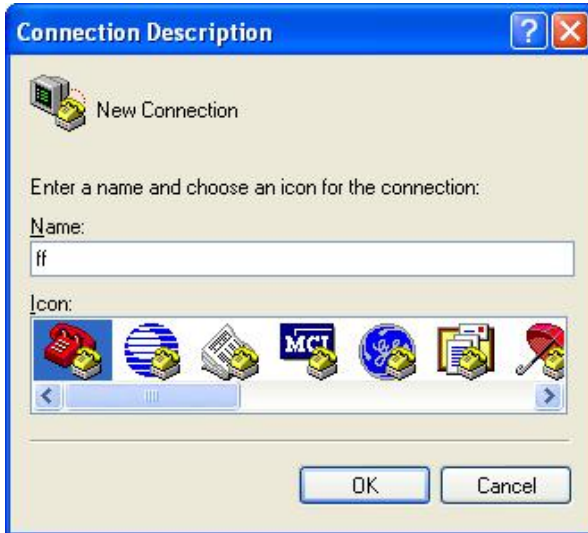
**Expires:** the expiry the client rents the IP address

## 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”

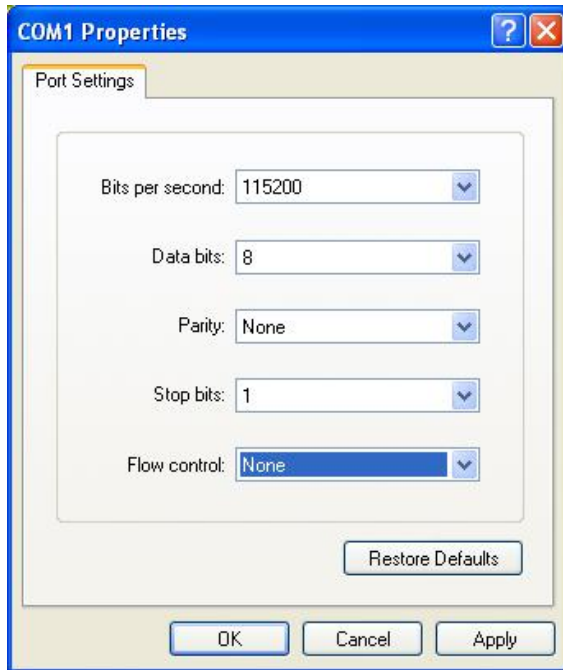
Bits per second: 115200

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None



5. Complete Hyper Terminal operation, It runs as following

