

# AR7088 Router User Manual

## Applicable Models:

Product Type	Model	Product Name
Enhanced	AR7088-W	WCDMA WIFI ROUTER
	AR7088-E	EVDO WIFI ROUTER
	AR7088-F	FDD-LTE WIFI ROUTER
	AR7088-T	TDD-LTE WIFI ROUTER
	AR7088-D	TDD/FDD-LTE WIFI ROUTER
Standard	AR7088-WSTD	WCDMA Router
	AR7088-ESTD	EVDO Router
	AR7088-FSTD	FDD-LTE Router
	AR7088-TSTD	TDD-LTE Router
	AR7088-DSTD	TDD/FDD-LTE Router



Xiamen Alotcer Communication Technology Co., Ltd.

Tel:+86 592-6195619

Fax:+86 592-6195620

Web:[en.alotcer.com](http://en.alotcer.com)

E-mail:[anne@alotcer.com](mailto:anne@alotcer.com)

Add:NO.146-148, 2nd XingBei Road, JiMei District,  
XiaMen,China.



## Contents

Contents.....	3
Chapter 1 Brief Introduction.....	5
1.1 General.....	5
1.2 Product Feature.....	6
1.3 Block Diagram.....	7
1.4 Product SPEC.....	7
1.5 Ordering Information.....	9
Chapter 2 Installation Introduction.....	9
.....	9
2.1 General.....	9
2.2 Encasement List.....	10
2.3 Installation and Cable Connection.....	10
2.4 Power.....	13
2.5 Indicator Lights Introduction.....	13
2.6 Reset Button Introduction.....	14
Chapter 3 Configuration and Management.....	14
.....	14
3.1 Configuration Connection.....	14
3.2 Access the Configuration Web Page.....	15
3.2.1 IP Address Setting.....	15
3.2.2 Access the Configuration Web Page.....	16
3.3 Basic.....	18
3.3.1 WAN.....	18
3.3.2 WAN Status.....	21
3.3.3 LAN.....	21
3.3.4 LAN Status.....	23
3.4 Advanced.....	24
3.4.1 Statically Assigned.....	24
3.4.2 Advanced Router.....	24
3.4.3 MAC Address Clone.....	25
3.4.4 SDNS.....	25
3.5 Wireless.....	26
3.5.1 Basic Settings.....	26
3.5.2 Wireless Security.....	27
3.5.3 Wireless Status.....	28
3.6 VPN.....	29
3.6.1 PPTP.....	29
3.6.2 L2TP.....	30

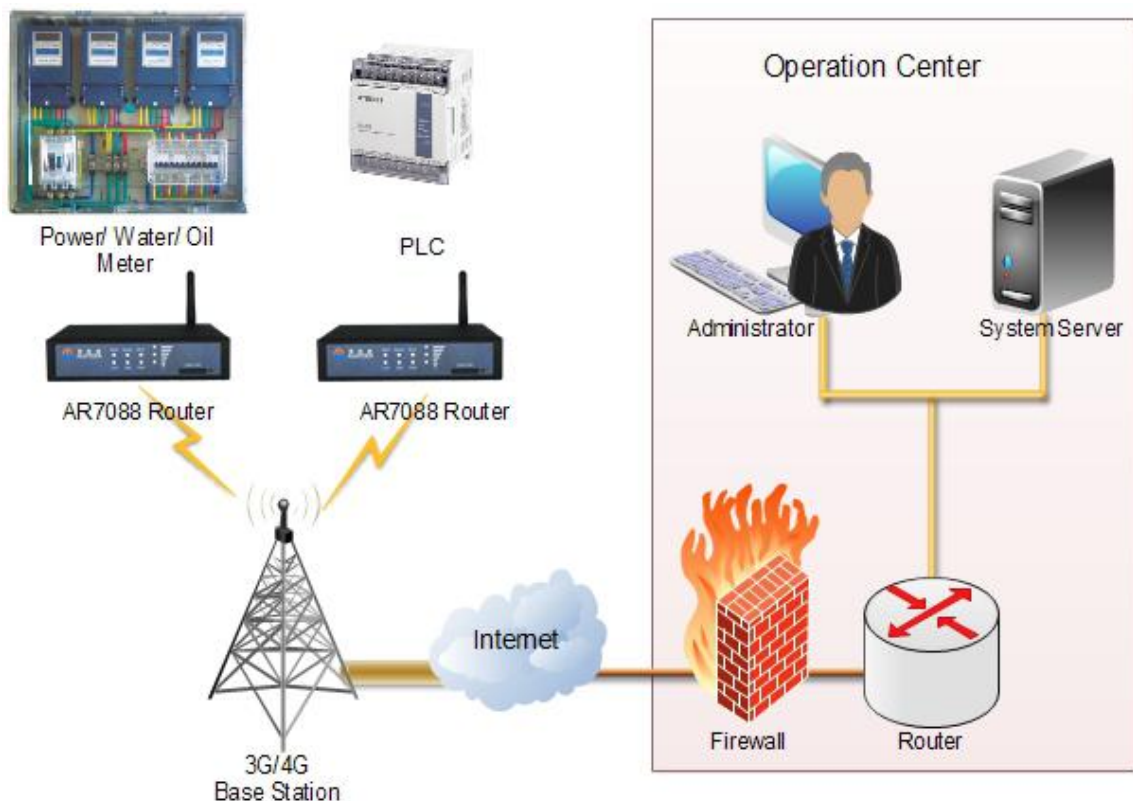
3.6.3 IPSEC.....	30
3.6.4 GRE.....	31
3.7 Security.....	32
3.7.1 Firewall.....	32
3.7.2 Access Restriction.....	33
3.7.3 MAC Filter.....	36
3.7.4 Packet Filter.....	36
3.8 Forwarding.....	37
3.8.1 Port Forwarding.....	37
3.8.2 Port Range.....	37
3.8.3 Port Triggering.....	38
3.8.4 DMZ.....	38
3.9 QoS Setting.....	39
3.9.1 Traffic monitoring.....	39
3.10 M2M.....	39
3.10.1 Serial.....	39
3.10.2 SMS.....	41
3.11 Administration.....	41
3.11.1 Language and Reboot.....	41
3.11.2 Password.....	41
3.11.3 Management.....	42
3.11.4 System Time.....	43
3.11.5 Configure.....	44
3.11.6 Upgrade.....	45
3.11.7 DDNS.....	45
3.11.8 Syslog.....	46

## Chapter 1 Brief Introduction

### 1.1 General

AR7088 ROUTER is a kind of terminal device that developed based on 2G/3G/4G, WIFI, VPN technology. It adopts high-powered industrial 32-bits CPU and embedded real time operating system. It supports RS232 (or RS485), Ethernet and WIFI port that can conveniently and transparently connect one device to a cellular network, allowing to connect to existing serial, Ethernet and WIFI devices with only basic configuration.

It has been widely used on M2M fields, such as intelligent transportation, smart grid, postal services, industrial automation, telemetry, finance, POS, water supply, environment protection, post, weather, and so on.



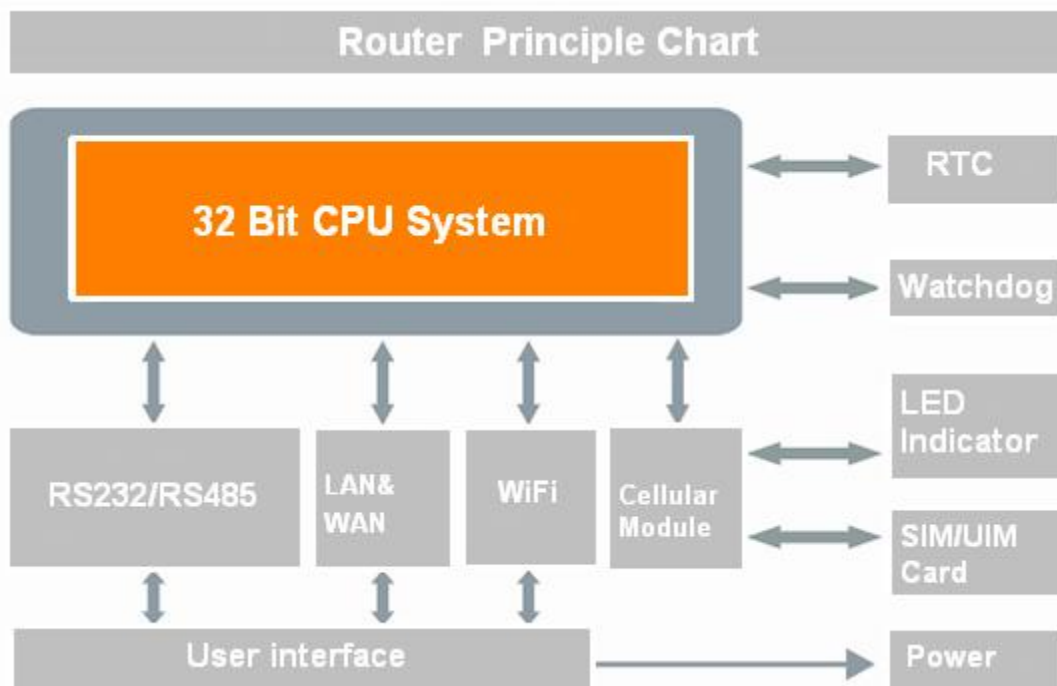
**Router Application Topology**

## 1.2 Product Feature

Items	Contents
<b>Industrial Design</b>	High-powered industrial cellular module
	High-powered industrial 32bits CPU
	Housing: iron, providing IP30 protection.
	Power range: DC 5~35V
<b>High Reliability</b>	Support hardware and software WDT
	Support auto recovery mechanism to make router always online
	Ethernet port: 1.5KV magnetic isolation protection
	RS232/RS485 port: 15KV ESD protection
	SIM/UIM port: 15KV ESD protection
	Power port: reverse-voltage and over voltage protection
	Antenna port: lightning protection(optional)
<b>Standard and Convenience</b>	Support standard RS232(or RS485), Ethernet and WIFI port that can connect to serial, Ethernet and WIFI devices directly
	Support standard WAN port and PPPOE protocol that can connect to ADSL directly
	Support intellectual mode, enter into communication state automatically when powered
	Support several work modes
	Convenient configuration and maintenance interface (WEB or CLI)
<b>High-performance and Security</b>	Support multiple WAN access methods, including static IP, DHCP, PPPOE, 2.5G/3G/4G.
	Support double link backup between 2.5G/3G/4G and WAN (optional).
	Support VPN client(PPTP, L2TP, IPSEC and GRE)(only for VPN version).
	Support remote management, SYSLOG, SNMP, TELNET, SSH, HTTPS, etc.
	Support local and remote firmware upgrade,import and export configure file.
	Support NTP, RTC embedded.
	Support multiple DDNS provider service.
	Support MAC address cloning.
	WIFI support 802.11b/g/n. support AP, client.
WIFI support WEP,WPA,WPA2 encryption.	

	Support multiple online trigger ways, including SMS, ring and data. Support link disconnection when timeout.
	Support APN/VPDN.
	Support multiple DHCP server and DHCP client, DHCP binding MAC address, DDNS, Firewall, NAT, DMZ host, QoS, traffic statistics, real-time display data transfer rate etc.
	Support TCP/IP, UDP, FTP(optional), HTTP, etc.
	Supports SPI firewall, VPN pass-through, access control, URL filtering, etc.
	Support local log storage.

### 1.3 Block Diagram



### 1.4 Product SPEC

Items		Contents
<b>Hardware System</b>	CPU	Industrial 32bits CPU
	FLASH	16MB (Extendable to 64MB)
	SDRAM	128MB
<b>Interface</b>	WAN	1 10/100Mbps WAN port(RJ45), auto MDI/MDIX,

		1.5KV magnetic isolation protection
	LAN	1 10/100Mbps Ethernet ports(RJ45), auto MDI/MDIX, 1.5KV magnetic isolation protection
	Serial	1 RS232(or RS485/RS422) port, 15KV ESD protection Data bits: 5, 6, 7, 8 Stop bits: 1, 1.5(optional), 2 Parity: none, even, odd, space(optional), mark(optional) Baud rate: 2400~115200 bps
	Antenna	Cellular: Standard SMA female interface, 50 ohm WIFI: Standard SMA male interface, 50 ohm
	SIM/UIM	Standard 3V/1.8V user card interface, 15KV ESD protection
	Power	Standard 3-PIN power jack, reverse-voltage and over voltage protection
	Reset	Press this key for 8 seconds to restore the router to its original factory default settings
	Indicator	"Signal strength"、"PWR"、"RUN"、"SIM"、"Online"、"LAN"、"WAN"
<b>Network</b>	Wireless Network	GSM/GPRS/EDGE: 850/900/1800/1900MHz CDMA: 800/1900MHz WCDMA/HSUPA/HSPA+: 850/900/1900/2100MHz CDMA2000 1x/ EVDO Rev. A: 800/1900MHz TD-SCDMA: 1880-1920/2010-2025MHz(A/F) TDD-LTE: Band 38/39/40/41& Band 61/62 FDD-LTE: Band 1/2/3/4/5/7/8/13/17/20/25/28
	WAN	Support PPP/PPPOE
	LAN	Support APR
	Network Authentication	Support CHAP/PAP Authentication
	Network Access	Support APN/VPDN
	IP Applications	Support Ping, Trace, DHCP Server, DHCP Relay, DHCP Client, DNS relay, DDNS, Telnet
	IP Routing	Support static routing
<b>WIFI</b>	Standard	IEEE802.11b/g/n
	Bandwidth	IEEE802.11b/g: 54Mbps (max) IEEE802.11n: 150Mbps (max)
	Security	WEP, WPA, WPA2, etc. WPS (optional)



<b>Power supply</b>	Standard Power	DC 12V/1.5A
	Power range	DC 5~35V
	Consumption	<410mA (@12VDC)
<b>Physical</b>	Dimensions	136x99x28mm
	Weight	395g
<b>Environmental Limits</b>	Operating Temperature	-35~+75°C (-31~+167°F)
	Storage Temperature	-40~+85°C (-40~+185°F)
	Operating Humidity	95% (unfreezing)

## 1.5 Ordering Information

Model	Network Abbreviation
AR7088	-W: WCDMA WIFI -E: EVDO WIFI -D: TDD/FDD-LTE WIFI -T: TDD-LTE WIFI -F: FDD-LTE WIFI -WSTD: WCDMA Standard -ESTD: EVDO Standard -DSTD: TDD/FDD-LTE Standard -TSTD: TDD-LTE Standard -FSTD: FDD-LTE Standard
Example	AR7088-F: AR7088 router that support FDD-LTE &WIFI

## Chapter 2 Installation Introduction

### 2.1 General

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

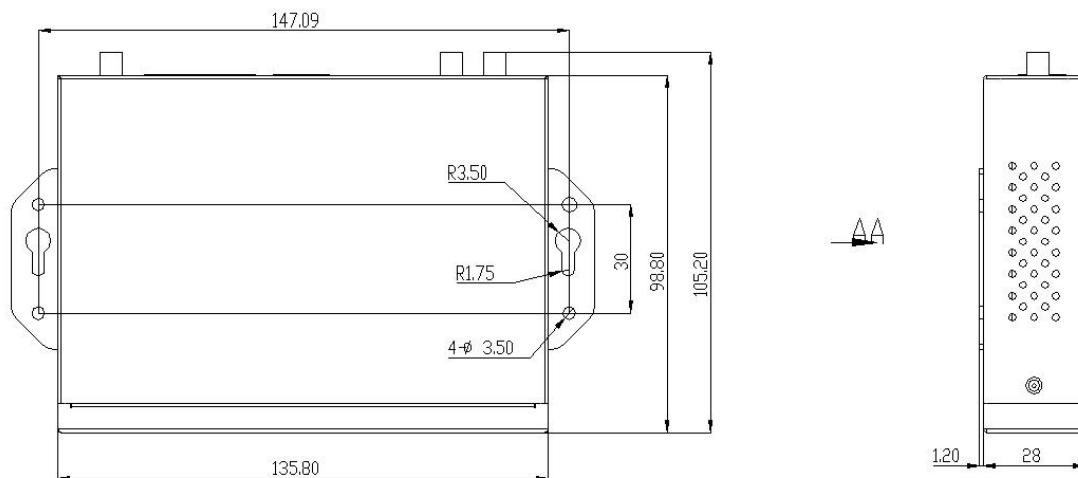
**Warning: Forbid to install the router when powered!**

## 2.2 Encasement List

Name	Quantity	Remark
Router host	1	
Cellular antenna (Male SMA)	1	
WIFI antenna (Female SMA)	1	
Network cable	1	
Power adapter	1	
Manual CD	1	
Certification card	1	
Maintenance card	1	
RS232 Console cable	1	Optional
RS485 Console cable	1	Optional

## 2.3 Installation and Cable Connection

Dimension(The fixing piece is detachable): (Unit: mm)



**Installation of antenna:**



**Cellular antenna (Standard)**

Screw the SMA male pin of the cellular antenna to the female SMA interface of the router with sign “ANT”(some models are two antennas, namely "ANT1", "ANT2").

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

**WIFI antenna (Standard)**

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

**Installation of SIM/UIM card:**

**SIM/UIM Card Installation**

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:**

**Network cable (Standard)**

**Console cable (Standard)**

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



### Power adapter (Standard)

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

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

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

## 2.5 Indicator Lights Introduction

The router provides following indicator lights: “Power”, “RUN”, “SIM”, “Online”, “LAN”, “WAN”, “Signal Strength”.

Indicator Light	State	Introduction
Power	ON	Router is powered on
	OFF	Router is powered off
RUN	BLINK	Router works properly
	OFF	Router does not work
SIM	ON	SIM/UIM card is recognized
	OFF	SIM/UIM card is not recognized
Online	ON	Router has logged on network
	OFF	Router hasn't logged on network
LAN	OFF	The corresponding interface of switch is not connected
	ON / BLINK	The corresponding interface of switch is connected /Communicating
WAN	OFF	The interface of WAN is not connected
	ON / BLINK	The interface of WAN is connected /Communicating
Signal Strength	All off	The signal is terrible

	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 8 seconds, the router will restore to its original factory default settings and restart automatically.( The auto-restart is as follows: The "RUN" indicator turns off for about 10 seconds and then functions normally)

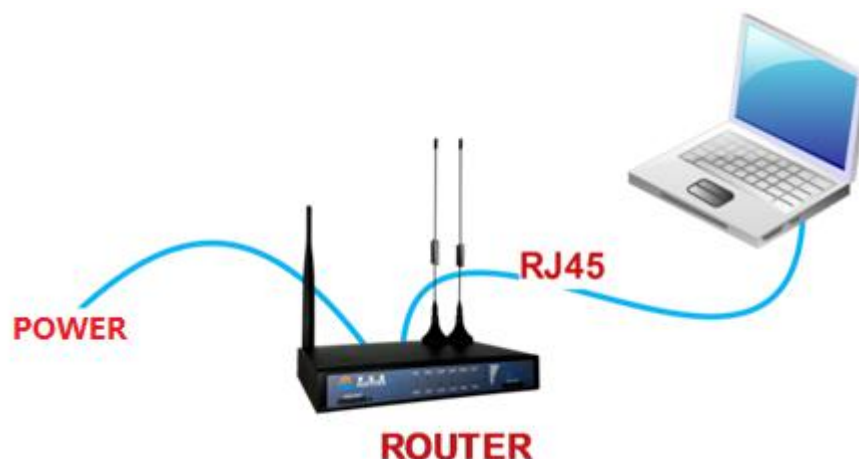
## Chapter 3 Configuration and Management

This chapter describes how to configure and manage the router.

### 3.1 Configuration Connection

Before configuration, you should connect the router and your 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 PC's Ethernet port.

The connection diagram is as following:

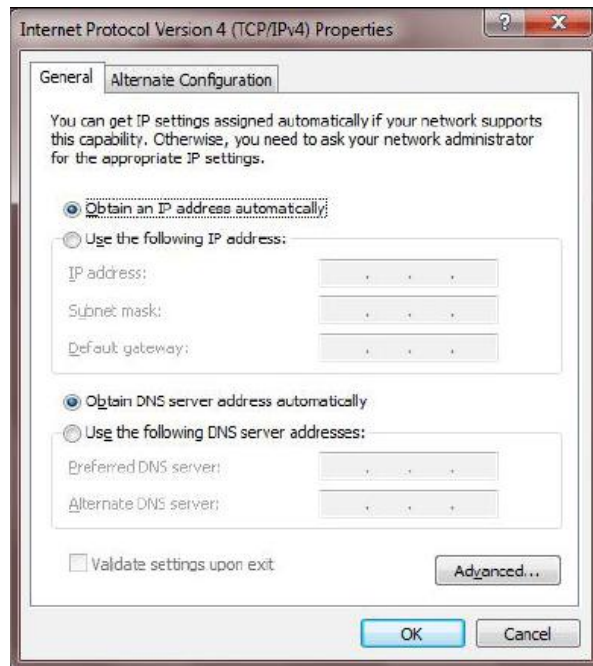


Please modify the IP address of PC the same as network segment address of the router, for instance, 192.168.1.9. Modify the mask code of PC as 255.255.255.0 and set the default gateway of PC as the router's IP address (192.168.1.1).

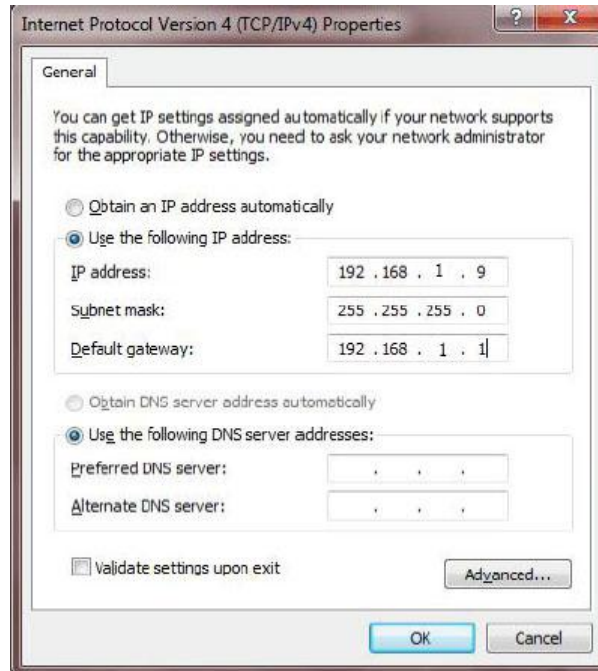
## 3.2 Access the Configuration Web Page

### 3.2.1 IP Address Setting

#### IP Address - DHCP



**IP Address - Static.** Set the IP PC address to 192.168.1.9. Set the subnet mask to 255.255.255.0. Set the default gateway to 192.168.1.1. Configure the DNS server as the local DNS server, such as 8.8.8.8.



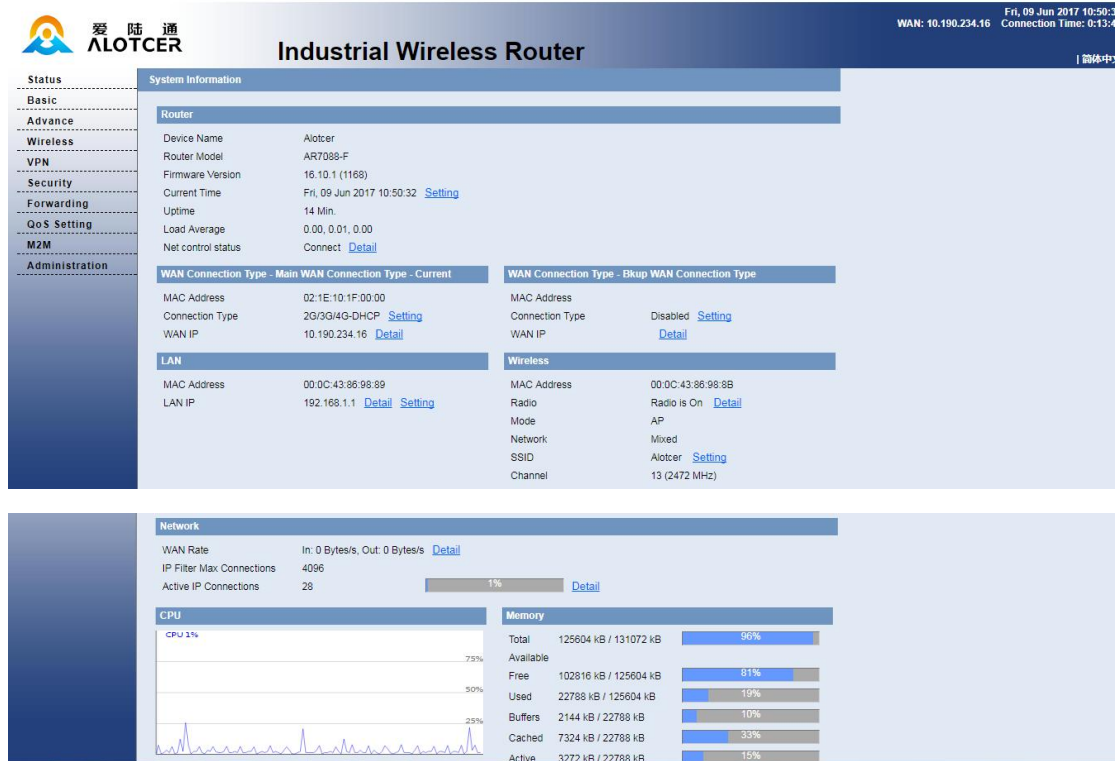
### 3.2.2 Access the Configuration Web Page

The chapter is to present main functions of each page. Users visit page tool via web browser after connect users' PC to the router.

Start a web browser and type 192.168.1.1 in the Address (URL) field (The Default IP Address of the Ethernet port is 192.168.1.1). It will prompt the Web management tool of the router. The users login in the web page, there will display a page to choose language. Users have to click "Continue" to make it work if modify language.

After access to the information main page.





The screenshot displays the ALOTCER web interface for an Industrial Wireless Router. The top navigation bar includes the ALOTCER logo, the title "Industrial Wireless Router", and system status information: WAN: 10.190.234.16, Fri, 09 Jun 2017 10:50:32, and Connection Time: 0:13:34. A sidebar on the left lists menu items: Status, Basic, Advance, Wireless, VPN, Security, Forwarding, QoS Setting, M2M, and Administration. The main content area is divided into several sections:

- Router Information:**
  - Device Name: Alotcer
  - Router Model: AR7088-F
  - Firmware Version: 16.10.1 (1168)
  - Current Time: Fri, 09 Jun 2017 10:50:32 [Setting](#)
  - Uptime: 14 Min.
  - Load Average: 0.00, 0.01, 0.00
  - Net control status: Connect [Detail](#)
- WAN Connection Type - Main WAN Connection Type - Current:**
  - MAC Address: 02:1E:10:1F:00:00
  - Connection Type: 2G/3G/4G-DHCP [Setting](#)
  - WAN IP: 10.190.234.16 [Detail](#)
- WAN Connection Type - Bkup WAN Connection Type:**
  - MAC Address: [Blank]
  - Connection Type: Disabled [Setting](#)
  - WAN IP: [Blank] [Detail](#)
- LAN:**
  - MAC Address: 00:0C:43:86:98:89
  - LAN IP: 192.168.1.1 [Detail](#) [Setting](#)
- Wireless:**
  - MAC Address: 00:0C:43:86:98:8B
  - Radio: Radio is On [Detail](#)
  - Mode: AP
  - Network: Mixed
  - SSID: Alotcer [Setting](#)
  - Channel: 13 (2472 MHz)
- Network:**
  - WAN Rate: In: 0 Bytes/s, Out: 0 Bytes/s [Detail](#)
  - IP Filter Max. Connections: 4096
  - Active IP Connections: 28 (1% of 4096) [Detail](#)
- CPU:**
  - CPU 1% (Line graph showing usage over time)
- Memory:**
  - Total: 125604 kB / 131072 kB (96%)
  - Available: [Blank]
  - Free: 102816 kB / 125604 kB (81%)
  - Used: 22788 kB / 125604 kB (19%)
  - Buffers: 2144 kB / 22788 kB (10%)
  - Cached: 7324 kB / 22788 kB (33%)
  - Active: 3272 kB / 22788 kB (15%)

The operation data and state of each module can be completely observed in the information main page, which including basic information of routing, WAN, LAN, wireless, network, CPU, memory and other basic information.

Access other pages. It will prompt a login page. The default username and password are both "admin". Please input the username and password login to access the configuration pages.



Input correct user name and password to visit relevant menu page.

## 3.3 Basic

### 3.3.1 WAN

Select the appropriate wide area networking mode according to different requirements. Set the corresponding parameters according to different connection modes.

DUAL LINK OPTION	
Dual Both Online	<input checked="" type="radio"/> Enable <input type="radio"/> Disable (Automatic return to Main)
Link Fail to Restart	<input type="text" value="10"/> minutes (0: Disabled)

**Dual Both Online:** WAN and Bkup WAN are both online. The system will automatically switch back to the main chain when the main link is available if enabled.

**Link Fail to Restart:** Time of restart system for all link fail.

Disable WAN connection

WAN Connection Type - Main WAN Connection Type	
Connection Type	<input type="text" value="Disabled"/>

Put in the IP address, subnet mask, default gateway, and DNS Server(optional) assigned by the provider.

WAN Connection Type - Main WAN Connection Type				
Connection Type	Static IP ▼			
WAN IP Address	192	168	20	100
Subnet Mask	255	255	255	0
Gateway	192	168	20	1
Static DNS 1	0	0	0	0
Static DNS 2	0	0	0	0
Static DNS 3	0	0	0	0

Normally, The Internet IP Address of the router is allocated by the ISP automatically.

WAN Connection Type - Main WAN Connection Type	
Connection Type	Automatic Configuration - DHCP ▼

You may choose "PPPoE" if you connect the WAN port to a PPPoE server. Input the correct username and password provided by ISP or administrator.

WAN Connection Type - Main WAN Connection Type	
Connection Type	PPPoE ▼
User Name	<input type="text"/>
Password	<input type="password"/> <input type="checkbox"/> Unmask
Fixed WAN IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Fixed WAN GW Address	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

If you want to access to 2G/3G/4G network, you can choose "2G/3G/4G-PPP" or "2G/3G/4G-DHCP" mode.

WAN Connection Type - Main WAN Connection Type	
Connection Type	2G/3G/4G-PPP ▼
SIM Switch/Reset	60 Sec.
User Name	<input type="text"/>
Password	<input type="password"/> <input type="checkbox"/> Unmask
Dial String	*99# (UMTS/3G/3.5G) ▼
APN	3gnet
Network Mode	Auto ▼
Permitted Authentication	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAPv2
Fixed WAN IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Fixed WAN GW Address	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

**SIM Switch/Reset:** Time of restart SIM card for dial fail.

**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

**Network Mode:** Select the appropriate network model according to the environment.

**Permitted Authentication:**Select the authentication protocol according to the requirements.

WAN Connection Type - Main WAN Connection Type	
Connection Type	2G/3G/4G-DHCP
SIM Switch/Reset	60Sec.
User Name	
Password	<input type="checkbox"/> Unmask
APN	3gnet
Network Mode	Auto
Permitted Authentication	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP

Refer to 2G/3G/4G-PPP mode.

Force reconnect	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Connect Fail	1 TimesSwitch
Dial Fail to Restart	10 minutes (0: Disabled)
Keep Alive	Ping
Keep Alive Server IP	114.114.114.114
Keep Alive Server IP2	www.baidu.com
Keep Alive Interval	60 Sec.
Keep Alive Fail	1 TimesSwitch

**Force reconnect:** Reset the connection according to the set time.

**Connect Fail:** Switch to Backup WAN after link failure times.

**Dial Fail to Restart:** Time of restart system for this link fail.

**Keep Alive:** This function is used to detect whether the Internet connection is active. It will redial to users' ISP immediately to make the connection active if users set it and when the router detect the connection is inactive. Specifies how many seconds to wait before reconnect the link after it terminates.

**None:** Do not set this function

**Ping:** Send ping packet to detect the connection, when choose this method. Users should also configure "Keep Alive Interval", "Keep Alive Server IP" and "Keep Alive Server IP2" items.

**Route:** Detect connection with route method, when choose this method. Users should also configure "Keep Alive Interval", "Keep Alive Server IP" and "Keep Alive Server IP2" items.

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


**Keep Alive Fail:** Switch to Backup WAN after keep alive fail times.

**Note:** When users choose the "Route" or "Ping" method, it's quite important to make sure that the "Keep Alive Server IP" and "Keep Alive Server IP2" are usable and stable, because they have to response the detection packet frequently.

### 3.3.2 WAN Status

**WAN**

**Module Type**

Module Type	H120F
SIM No.	SIM1
Status of SIM	OK
Signal Status	 - 59 dbm
Network	LTE
Net control status	Connect <span style="border: 1px solid #ccc; padding: 2px;">DISCONNECT</span>

**WAN - Main WAN Connection Type- Current**

**WAN - Bkup WAN Connection Type**

Connection Type	2G/3G/4G-DHCP	Connection Type	Disabled
Connection Time	0:18:35		
IP Address	10.190.234.16		
Subnet Mask	255.255.255.224		
Gateway	10.190.234.1		
DNS	218.85.157.99 218.85.152.99		
Remaining Lease Time	5 days 23:41:25		

REFRESH

The page show the specific connection details, including module information, network operators, as well as the connection of the IP address and DNS, etc., according to the different connection types.

### 3.3.3 LAN

**Router IP**

Local IP Address	192	168	1	1	
Subnet Mask	255	255	255	0	
Local DNS	0	0	0	0	(Priority is higher than DNS configured in DHCP page)

Set IP address and subnet mask of LAN. The LAN IP and WAN IP must not be in the same network segment.

**Local DNS:** You can choose to use these reliable DNS server if you have your own DNS server or other stable and reliable DNS server. Optional configuration.

**Assign WAN Port to Switch**

Assign WAN Port to Switch

**Assign WAN Port to Switch:** Use WAN port to LAN port.

Network Address Server Settings (DHCP)				
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

(Priority is higher than DNS obtained from WAN)

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

**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:** 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:** Put in 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:** 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):** 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:** 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.

Advanced	
No DNS Rebind	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Additional DNSMasq Options	<input type="text"/>

**No DNS Rebind:** When enabled, it will 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

### 3.3.4 LAN Status

LAN Status	
MAC Address	00:0C:43:30:52:77
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Gateway	0.0.0.0
Local DNS	0.0.0.0

LAN port MAC, IP and DNS and other information.

Active Clients				
Host Name	IP Address	MAC Address	Conn. Count	Ratio [4096]
*	192.168.8.200	2C:53:4A:02:2F:E3	11	0%
*	192.168.8.130	00:0C:29:7B:E4:47	1	0%

**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.

DHCP Status	
DHCP Server	Enabled
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.

**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
- None -				

**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.

## 3.4 Advanced

### 3.4.1 Statically Assigned

Static Address Setting					
Max rule number:16					
Number	Name	MAC Address	Host Name	IP Address	Client Lease Time
None					
<input type="button" value="SELECT ALL"/> <input type="button" value="DELETE"/>					
Name	<input type="text"/>				
MAC Address	<input type="text"/>	(xxxxxxxxxxxx)			
Host Name	<input type="text"/>	(optional)			
IP Address	<input type="text"/>				
Client Lease Time	<input type="text"/>	minutes	(0: Disabled)		

**Statically Assigned:** Assign the static IP address to the specified client according to MAC address.

### 3.4.2 Advanced Router

Static Routing						
Number	Name	Metric	Destination LAN NET	Subnet Mask	Gateway	Interface
None						
<input type="button" value="SELECT ALL"/> <input type="button" value="DELETE"/>						
Route Name	<input type="text"/>					
Metric	<input type="text" value="0"/>					
Destination LAN NET	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>		
Subnet Mask	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="255"/>	<input type="text" value="0"/>		
Gateway	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>	<input type="text" value="0"/>		
Interface	LAN & WLAN ▾					
<input type="button" value="SAVE"/> <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>						
Routing Table Entry List						
Destination LAN NET	Subnet Mask			Gateway	Interface	
10.37.60.212	255.255.255.252			0.0.0.0	WAN1	
192.168.8.0	255.255.255.0			0.0.0.0	LAN & WLAN	
0.0.0.0	0.0.0.0			10.37.60.214	WAN1	

**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).

### 3.4.3 MAC Address Clone

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

MAC Clone						
MAC Clone	<input checked="" type="radio"/> Enable <input type="radio"/> Disable					
Clone WAN MAC	00	0C	43	30	52	78 <a href="#">GET CURRENT PC MAC ADDRESS</a>
Clone LAN(VLAN) MAC	00	0C	43	30	52	77
Clone LAN(Wireless) MAC	00	0C	43	30	52	79

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

**Noted:** One MAC address is 48 characteristic. MAC address 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.

### 3.4.4 SDNS

Static Address Setting			
Max rule number:16			
Number	Name	Domain Name	IP Address
		None	
<a href="#">SELECT ALL</a> <a href="#">DELETE</a>			
Name	<input type="text"/>		
Domain Name	<input type="text"/>		
IP Address	<input type="text"/>		

When users host their domain names on free or commercial servers, they usually get a static IP (non-changeable IP) address for their websites, which involves the use of static name servers, or static DNS, as well. Static DNS settings will never update on their own and will remain the same, until you decide to update them. Static DNS settings are very useful, since they provide a stable service with no interruptions, and can increase the overall speed of the website.

## 3.5 Wireless

### 3.5.1 Basic Settings

Wireless Network	
Wireless Network	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Physical Interface SSID [Alotcer] HWAddr []	
Wireless Mode	AP
Network Mode	Mixed
SSID	Alotcer
Channel	Auto
Channel Width	20 MHz
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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

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

**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.

**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.

**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.

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

**Wireless SSID Broadcast:** Enable, SSID broadcasting; Disable, Hidden SSID.

Virtual Interfaces SSID [Alotcer_vap_1]	
SSID	Alotcer_vap_1
SSID Broadcast	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

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

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

### 3.5.2 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.



The screenshot shows the configuration page for a physical interface SSID. The title is "Physical Interface SSID [Alotcer] HWAddr []". The settings are as follows:

Security Mode	WPA2 Personal Mixed
WPA Algorithms	TKIP+AES
WPA Shared Key	..... <input type="checkbox"/> Unmask
Key Renewal Interval (in seconds)	3600 (Default: 3600, Range: 1 - 99999)

**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 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.

**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.

### 3.5.3 Wireless Status

Wireless Status	
MAC Address	
Radio	Radio is On
Mode	AP
Network	Mixed
SSID	Alotcer
Channel	1 (2412 MHz)
TX Power	71 mW
Rate	72 Mb/s
Encryption - Interface w10	Enabled, WPA2 Personal Mixed

**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 disable Encryption-Interface w10.

Wireless Packet Info		
Received (RX)	622820 OK, no error	100%
Transmitted (TX)	7452 OK, no error	100%

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

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

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:** 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.

## 3.6 VPN

### 3.6.1 PPTP

**PPTP Client**

PPTP Client Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Server IP or DNS Name	<input type="text" value="server.alotcer.com"/>
User Name	<input type="text" value="hd"/>
Password	<input type="password" value="••"/> <input type="checkbox"/> Unmask
Remote Subnet	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Remote Subnet Mask	<input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/> . <input type="text" value="0"/>
Permitted Authentication	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAPv2
MPPE Encryption	<input type="checkbox"/> Forced encryption <input checked="" type="checkbox"/> Stateless <input checked="" type="checkbox"/> 40 bit <input checked="" type="checkbox"/> 56 bit <input checked="" type="checkbox"/> 128 bit
MTU	<input type="text" value="1450"/> (Default: 1450)
MRU	<input type="text" value="1450"/> (Default: 1450)
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Fixed IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Keep Alive Interval	<input type="text" value="15"/> Sec.
Keep Alive Fail	<input type="text" value="3"/>
undefined	<div style="border: 1px solid #ccc; height: 20px; width: 100%;"></div>

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

**Remote Subnet:** The network of the remote PPTP server.

**Remote Subnet Mask:** Subnet mask of remote PPTP server.

**Permitted Authentication:** Select permitted authentication.

**MPPE Encryption:** Enable or disable Microsoft Point-to-Point Encryption.

**MTU:** Maximum Transmission Unit.

**MRU:** Maximum Receive Unit.

**NAT:** Network Address Translation.

**User Name:** User name to login PPTP Server.

**Password:** Password to log into PPTP Server.

### 3.6.2 L2TP

L2TP Client	
L2TP Client Options	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tunnel name	<input type="text" value="Alotcer"/>
User Name	<input type="text" value="hd"/>
Password	<input type="password" value="••"/> <input type="checkbox"/> Unmask
Tunnel Authentication	<input type="text"/> <input type="checkbox"/> Unmask
Password	<input type="text"/>
Gateway (L2TP Server)	<input type="text" value="server.alotcer.com"/>
Remote Subnet	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Remote Subnet Mask	<input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/> <input type="text" value="0"/>
Permitted Authentication	<input checked="" type="checkbox"/> Compulsory Auth <input type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP
MPPE Encryption	<input type="checkbox"/> Forced encryption <input checked="" type="checkbox"/> Stateless <input checked="" type="checkbox"/> 40 bit <input checked="" type="checkbox"/> 56 bit <input checked="" type="checkbox"/> 128 bit
MTU	<input type="text" value="1450"/> (Default: 1450)
MRU	<input type="text" value="1450"/> (Default: 1450)
NAT	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Fixed IP	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
undefined	<input type="text"/>

**User Name:** User name to login L2TP Server.

**Password:** Password to login L2TP Server.

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

**Remote Subnet:** The network of remote PPTP server.

**Remote Subnet Mask:** Subnet mask of remote PPTP server.

**Permitted Authentication:** Select permitted authentication.

**MPPE Encryption:** Enable or disable Microsoft Point-to-Point Encryption.

**MTU:** Maximum transmission unit.

**MRU:** Maximum receive unit.

**NAT:** Network address translation.

### 3.6.3 IPSEC

Connect Setting	
Name	<input type="text"/> Enable <input checked="" type="checkbox"/>
Mode	<input checked="" type="radio"/> Tunnel <input type="radio"/> Transport
Type	<input checked="" type="radio"/> Client <input type="radio"/> Server
Local WAN Interface	<input type="text" value="WAN"/>
Local Subnet	<input type="text"/>
Local Id	<input type="text"/>
Use a Pre-Shared Key:	<input type="text"/>
Peer WAN address	<input type="text"/>
Peer subnet	<input type="text"/>
Peer ID	<input type="text"/>

**Name:** Indicate this connection name, must be unique.

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

**Local WAN Interface:** Local addresss of the tunnel.

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

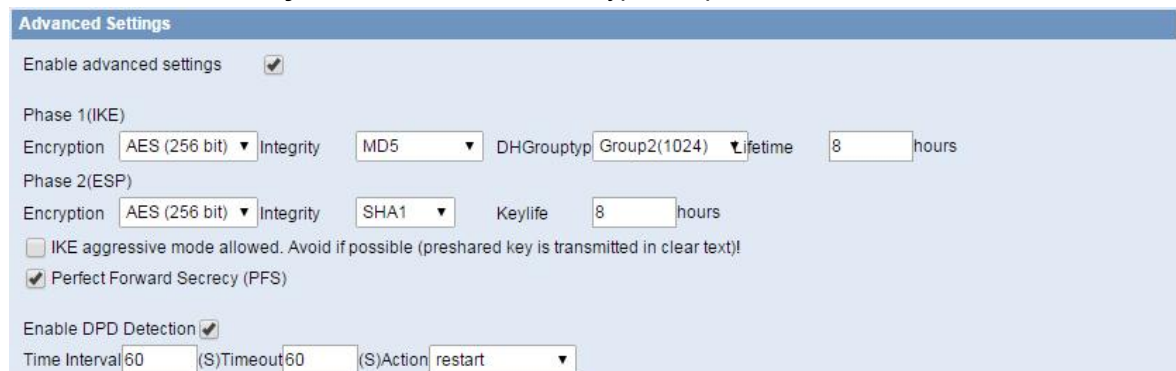
**Local Subnet:** IPSec local protects subnet and subnet mask, i.e. 192.168.1.0/24; this option can not fill in if using transfer mode.

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

**Local ID:** Tunnel local end identification, IP and domain name are available.

**Remote ID:** Tunnel opposite end identification, IP and domain name are available.

**Use a Pre-Shared Key:** Choose use share encryption option.



**Enable Advanced Settings:** Enable to configure 1<sup>st</sup> and 2<sup>nd</sup> phase information, otherwise it will auto negotiation according to opposite end.

### Phase 1(IKE)

**Encryption:** IKE phased encryption mode.

**Integrity:** IKE phased integrity solution.

**DHGroup type:** DH exchange algorithm.

**Lifetime:** Set IKE lifetime, current unit is hour, the default is 0.

### Phase 2(ESP)

**Encryption:** ESP encryption type.

**Integrity:** ESP integrity solution.

**Keylife:** Set ESP keylife, current unit is hour, the default is 0.

**IKE aggressive mode allowed:** Negotiation mode adopt aggressive mode if tick; it is main mode if non-tick.

**Perfect Forward Secrecy:** Tick to enable PFS, non-tick to disable PFS.

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

**Time Interval:** Set time interval of connect detection (DPD).

**Timeout:** Set the timeout of connect detection.

**Action:** Set the action of connect detection.

## 3.6.4 GRE

GRE (Generic Routing Encapsulation, Generic Routing Encapsulation) protocol is a

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

GRE Tunnel	
Name	<input type="text"/> Enable <input checked="" type="checkbox"/>
Through	WAN ▾
Local Tunnel IP	<input type="text"/>
Local Netmask	<input type="text"/>
Peer Wan IP Addr	<input type="text"/>
Peer Tunnel IP	<input type="text"/>
Peer Subnet	<input type="text"/> (x.x.x.0/24)

**Name:** GRE tunnel name.

**Through:** The GRE packet transmit interface.

**Local Tunnel IP:** The local tunnel ip address.

**Local Netmask:** Netmask of local network.

**Peer Wan IP Addr:** The remote WAN address.

**Peer Tunnel IP:** The remote tunnel ip address.

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

## 3.7 Security

### 3.7.1 Firewall

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

Firewall Protection	
SPI Firewall	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

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

Block WAN Requests	
<input type="checkbox"/> Block Anonymous WAN Requests (ping)	
<input checked="" type="checkbox"/> Filtered IDENT(port 113)	
<input checked="" type="checkbox"/> Block WAN SNMP access	

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

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



**Block WAN SNMP access:** This feature prevents the SNMP connection requests from the WAN.

Impede WAN DoS/Bruteforce	
<input type="checkbox"/>	Limit SSH Access
<input type="checkbox"/>	Limit Telnet 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.

Additional Filters	
<input type="checkbox"/>	Filter Proxy
<input type="checkbox"/>	Filter Cookies
<input type="checkbox"/>	Filter Java Applets
<input type="checkbox"/>	Filter ActiveX

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

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

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

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

### 3.7.2 Access Restriction

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

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

Enter MAC Address of the clients in this format: xx:xx:xx:xx:xx:xx

MAC 01	<input type="text" value="00:00:00:00:00:00"/>
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"/>

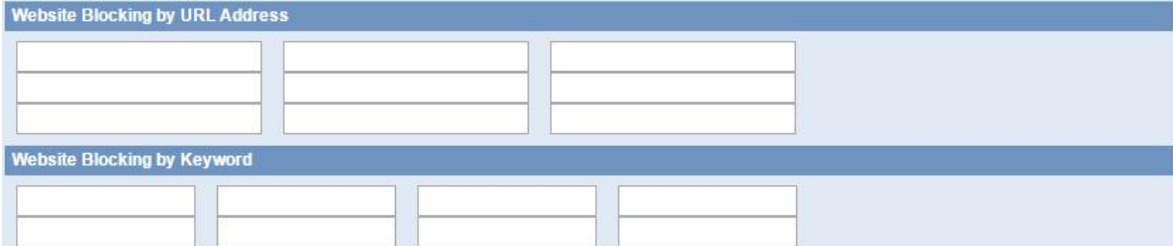
Enter the IP Address of the clients

IP 01	192.168.8.	<input type="text" value="0"/>
IP 02	192.168.8.	<input type="text" value="0"/>
IP 03	192.168.8.	<input type="text" value="0"/>
IP 04	192.168.8.	<input type="text" value="0"/>
IP 05	192.168.8.	<input type="text" value="0"/>
IP 06	192.168.8.	<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.



Website Blocking by URL Address			

Website Blocking by Keyword			

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

**Website Blocking by Keyword:** You can block access to certain website by the keywords contained in the web page.

**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, please keep the original number.

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 ensure the correct implementation of the relevant period control function.

### 3.7.3 MAC Filter

**Mac Filter Setting**

Enable Mac Filter  Enable  Disable

Policy Accept only the data packets conform to the following rules ▼

Max rule number:30

Number	Name	Enable	MAC
None			

SELECT ALL

DELETE
ENABLE
DISABLE

Add Filter Rule

Name  Enable

MAC(FF:FF:FF:FF:FF:FF)

Using MAC address for data filtering.

### 3.7.4 Packet Filter

This page can create firewall rules to protect your network from malicious attacks on Internet network viruses.

**Packet Filter Setting**

Enable Packet Filter  Enable  Disable

Policy Discard packets conform to the following rules ▼

Max rule number:30

Number	Name	Enable	Source IP	SPorts	Destination IP	DPorts	Pro	Dir
None								

SELECT ALL

DELETE
ENABLE
DISABLE

Add Filter Rule

Name  Enable

Dir INPUT/OUTPUT ▼

Pro TCP/UDP ▼

SPorts 

1	-	65535
---	---	-------

DPorts 

1	-	65535
---	---	-------

Source IP 

0.	0.	0.	0.	0/	0
----	----	----	----	----	---

Destination IP 

0.	0.	0.	0.	0/	0
----	----	----	----	----	---

**Packet filter:** Enable or disable packet filtering.

**Policy:** Select the action of the data package that does not conform to the setting rules.

**Accept only the data packets conform to the following rules:** Only access to match the address.

**Discard packets conform to the following rules:** Only receive the network address that complies with the custom rules, and drop all other addresses.

**Note:** Add filter matching rules. Source port, destination port, source address, destination address must be filled in at least one item.

**INPUT:** Data packets from WAN port to LAN port.

**OUTPUT:** Data packets from the LAN port to the WAN port.

**Pro:** Protocol type for a data packet.

**Sport:** The source port of the data package.

**Dport:** Port of destination.

**Source IP:** The source IP address of the data package.

**Destination IP:** Destination IP address.

## 3.8 Forwarding

### 3.8.1 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.

Forwards								
Delete	Num	Application	Protocol	Source Net	Port from	IP Address	Port to	Enable
<input type="checkbox"/>	1		Both ▼		0	0.0.0.0	0	<input 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 check box to enable port forwarding for the application.

### 3.8.2 Port Range

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.

Forwards							
Delete	Num	Application	Start	End	Protocol	IP Address	Enable
<input type="checkbox"/>	1		0	0	Both ▼	0.0.0.0	<input type="checkbox"/>

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

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

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

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

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

**Enable:** Click the Enable check box to enable port forwarding for the application.

### 3.8.3 Port Triggering

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

Triggering								
Delete	Num	Application	Triggered Port Range		Forwarded Port Range		Enable	
			Start	End	Protocol	Start		End
<input type="checkbox"/>	1		0	0	TCP ▾	0	0	<input type="checkbox"/>

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

**Triggered Port Range:** Enter the number of the first and the last port of the range, which should be triggered. If a PC sends outbound traffic from those ports, incoming traffic on the Forwarded Range will be forwarded to that PC.

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

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

### 3.8.4 DMZ

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

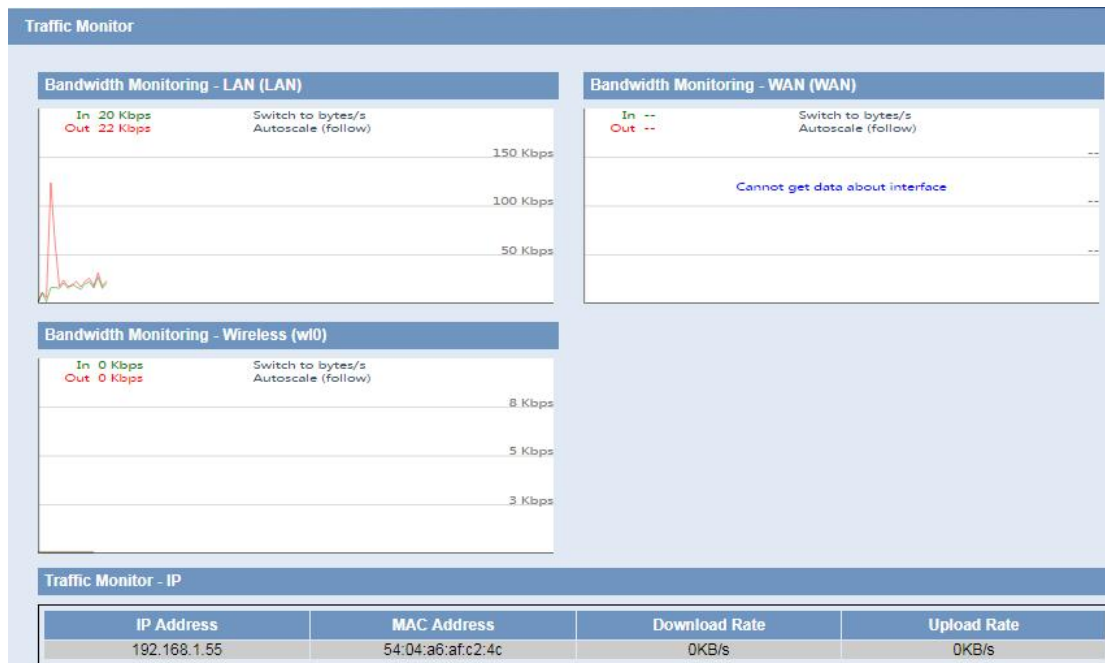
DMZ	
Use DMZ	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DMZ Host IP Address	192.168.1. <input type="text" value="0"/>

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.

## 3.9 QoS Setting

### 3.9.1 Traffic monitoring



Show the bandwidth of WAN, LAN, WIFI.

**Abscissa axis:** Time.

**Vertical axis:** Speed rate.

## 3.10 M2M

### 3.10.1 Serial

There is a console port on the router. Normally, this port is used to debug. This port can also be used for serial transmission. 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 IP Modem.

Serial Applications	
Serial Applications	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Baudrate	115200 ▼
Databit	8 ▼
Stopbit	1 ▼
Parity	None ▼
Flow Control	None ▼
Protocol	TCP(DTU) ▼
Server Address	server.alotcer.com
Server Port	6001
Device Number	18912345678
Device Id	12345678
Heartbeat Interval	60

**Baudrate:** The serial port's baud rate.

**Databit:** The serial port's data bit.

**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.

**Modbus TCP Server:** MODBUS TCP and MODBUS RTU conversion.

**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".



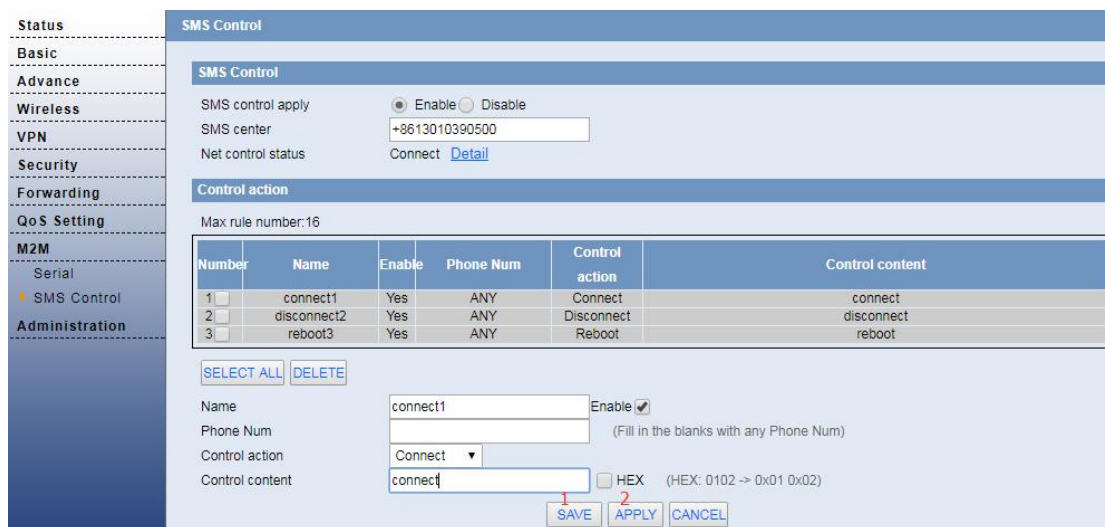
**Custom Registration Packets:** This item is valid when Protocol Type is "TCST".

### 3.10.2 SMS

For the SMS Function, support SMS to the router for Disconnect, Connect, Reboot functions.

The default state of the router is Connect. So you could configure the the below parameters for SMS control the Router.

SMS Center: Please check with the SIM card operator.



Number	Name	Enable	Phone Num	Control action	Control content
1	connect1	Yes	ANY	Connect	connect
2	disconnect2	Yes	ANY	Disconnect	disconnect
3	reboot3	Yes	ANY	Reboot	reboot

## 3.11 Administration

### 3.11.1 Language and Reboot



The upper right corner of the page provides the language switch button and reset button to set the WEB configuration page.

### 3.11.2 Password

Set the user name and password, to support the input of 32 characters.

Router Password	
Router Username	.....
Router Password	.....
Re-enter to confirm	.....

The new password must not exceed 32 characters in length and must not include any spaces. Enter the new password a second time to confirm it.

**Note:** Default username is admin.

It is strongly recommended that you change the factory default password of the 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.

### 3.11.3 Management

Configure WEB server parameters.

Web Access	
Protocol	<input checked="" type="checkbox"/> HTTP <input type="checkbox"/> HTTPS
Local Web GUI Port	<input type="text" value="80"/> (Default: 80, Range: 1 - 65535)

**Protocol:** This feature allows you to manage the router using either HTTP protocol or the HTTPS protocol.

**Local Web GUI port:** Set the access port of the WEB server. For example, when the gateway address is 192.168.1.1 and set the server port 1010, you will enter the address bar in the http://192.168.1.1:1010 to access the WEB configuration page. The default port for the server is 80.

Telnet	
Telnet	<input checked="" type="radio"/> Enable <input type="radio"/> Disable

**Telnet:** Enable or disable Telnet server.

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	<div style="border: 1px solid gray; height: 40px;"></div>

**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).

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="8088"/> (Default: 8088, Range: 1 - 65535)
SSH Management	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
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, if you haven't. 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 web browser's address field. You will be asked for the router's password.

If use https, 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:** Enable SSH to remotely access the router by Secure Shell.

**Telnet Management:** Enable SSH to remotely access the router.

**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.

SNMP	
SNMP	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Location	<input type="text" value="Unknown"/>
Contact	<input type="text" value="root"/>
Name	<input type="text" value="Alotcer"/>
RO Community	<input type="text" value="public"/>
RW Community	<input type="text" value="private"/>
SNMP Trap	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

**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.

### 3.11.4 System Time

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

Time Settings	
System Time	Tue, 06 Dec 2016 09:14:26
Time of PC	2016-12-06 09:16:08 <input checked="" type="checkbox"/> AUTO
Manual	<input type="text" value="2016"/> - <input type="text" value="12"/> - <input type="text" value="06"/> <input type="text" value="09"/> : <input type="text" value="15"/> : <input type="text" value="55"/> <input type="checkbox"/> MANUAL

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.

Time Server	
NTP Client	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Time Zone	UTC+08:00 ▼
Summer Time (DST)	none ▼
Server IP/Name	<input type="text"/>
Interval (in seconds)	<input type="text" value="3600"/>
Last Time updated:	Not available

**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.

### 3.11.5 Configure

Reset router settings	
Restore Factory Defaults	<input type="radio"/> Yes <input checked="" type="radio"/> No

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

**Note:**

Any settings you have saved will be lost when the default settings are restored. After restoring the router is accessible under the default IP address 192.168.1.1 and the default password admin.

Backup Settings	
Click the "Backup" button to download the configuration backup file to your computer.	
<input type="button" value="BACKUP"/>	
Restore Configuration	
Restore Settings	
Please select a file to restore	<input type="button" value="选择文件"/> 未选择任何文件
<p><b>WARNING</b>            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!</p>	

**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.

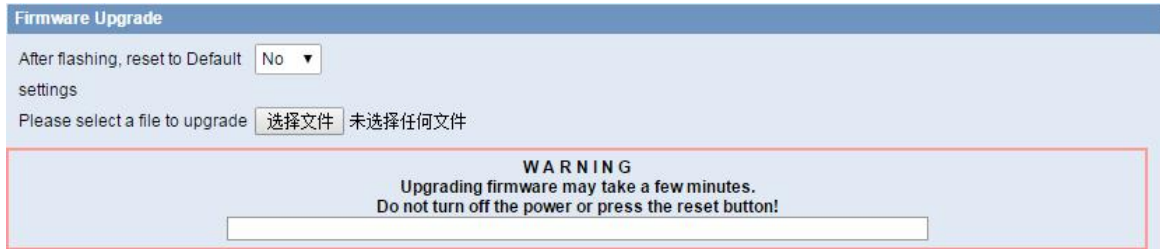
**Restore Settings:** Click the Browse button to browse for a configuration file that is currently saved on your PC. Click the Restore button to overwrite all current configurations with the ones in the configuration file.

**Note:**

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

### 3.11.6 Upgrade

Update software to get new features.



**Firmware Upgrade:** Contact us for New firmware versions. 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.
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 default:** If you want to reset the router to the default settings for the firmware version you are upgrading to, click the YES option.

### 3.11.7 DDNS

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

DDNS	
DDNS Service	DynDNS.org
User Name	<input type="text"/>
Password	<input type="password"/> <input type="checkbox"/> Unmask
Host Name	<input type="text"/>
Type	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'.

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

**Force Update Interval:** Unit is day, try forcing the update dynamic DNS to the server by settled days.

DDNS Status	
DDNS function is disabled	

DDNS Status shows connection log information.

### 3.11.8 Syslog

Alotcer router support stock log locally for at least 2 weeks. You could click the “Backup” button to download the log from the router and check the details.

Enable Syslogd to capture system 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 type="radio"/> Net <input type="radio"/> Console <input checked="" type="radio"/> Web
<input type="button" value="SAVE"/> <input type="button" value="APPLY"/> <input type="button" value="CANCEL"/>	
Log	
<input type="button" value="BACKUP"/> <input type="button" value="REFRESH"/> <input type="button" value="DELETE"/>	
<pre>07:16:21 mck[1039]: T: AT+COPS?^M &lt;6&gt;Dec 6 07:16:21 mck[1039]: R: ^M +COPS: 0,0,"CHINA TELECOM",7^M ^M OK^M &lt;8&gt;Dec 6 07:16:21 mck[1039]: T: AT+CFERG?^M</pre>	

**Syslog Out Mode:** 3 mode options.

**Net:** The log information output to a syslog server.

**Console:** The log information output to console port. (The log from the console is the most detailed, so if need to debug, could run serial port software to read and save the log). For the AD7028, the once choose

**Web:** The log information output to local web page.

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