Wireless Data Connectivity for Industrial applicatioons

4G Wireless Industrial Router

KING PIGEON

4G Wireless Router

User Manual

Ver 1.0

Date Issued: 2019-11-20

King Pigeon Hi-Tech. Co., Ltd.

www.iot-solution.com

Table of contents

【UPGRADE HISTORY】

DATE	FIRMWARE VERSION	HARDWARE VERSION	DESCRIPTION
2019.11.20	*V 1.0*	*V 1.0*	***First edition***

Model List

Model	Serial Port	WAN/LAN	LAN	WIFI	GPS
R10	1	1	1	√	×
R20	1	1	3	√	optional

1. Description

1. 1 Brief Introduction

This router is an industrial IoT high-speed router, compatible with 4G/3.5G/3G/2.5G network, flagship configuration, VPN link, industrial protection, wide temperature, wide voltage design, easy to set up high speed, stable The wireless transmission network uses the public LTE network to provide users with wireless long-distance data transmission.

The 4G router adopts high-performance industrial-grade 32-bit communication processor and industrial-grade wireless module, with embedded real-time operating system as software support platform, and provides one RS232, Ethernet LAN, Ethernet WAN and WIFI interface, which can be connected at the same time. Serial devices, Ethernet devices, and WIFI devices implement transparent data transmission and routing.

At present, industrial grade products have patented technology that maintains stable system, ensuring that the equipment is always online; the whole machine adopts metal casing, anti-interference and radiation protection, and industrial grade design on hardware; system with watchdog protection, and system monitoring protection After strict design, testing and practical application for 10 years, the product performance is stable and reliable.

1.2 Typically Applications

BTS Monitoring, Security Alarm System applications, Supervision and monitoring alarm systems, Automatic monitoring system, Vending Machines security protection, Pumping Stations, Tanks, Oil or Water levels, Buildings and Real Estate, Weather Stations, River Monitoring and Flood Control, Oil and gas pipelines, Corrosion protection, Temperatures, water leakage applications, Wellheads, boat, vehicle, Energy saving, street lights control system, Valve controls, Transformer stations, Unmanned machine rooms, Control room application, Automation System, M2M, etc.

1.3 Safety Directions

Safe Start up

Do not use the unit when using GSM/3G/4G equipment is prohibited or might bring disturbance or danger.

Interference

All wireless equipment might interfere network signals of the unit and influence its performance.

1.4 Standard Packing List

(1) Router R10 or R20 X1;

(2) 2PIN Power Terminals x 1(R20)

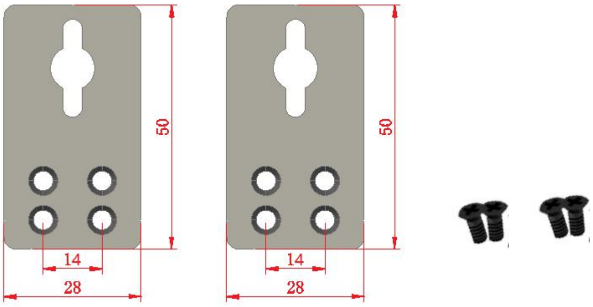
(3) 4PIN Serial Terminals x 1(R20)

(4) 12V DC Adaptor X1;

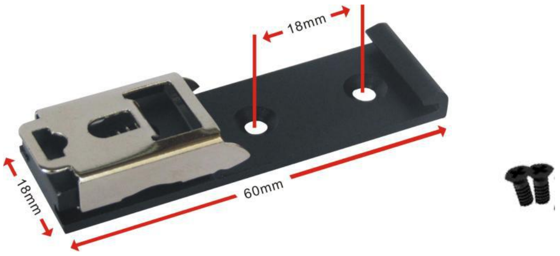
(5) GSM/3G/4G Antenna X1;

(6) 2.4G WIFI Antenna X2;

(7) Wall-mounted snap kit x 2(R20)



(8) 35mm Standard DIN rail fixed Bracket



Note: The package does not include any SIM card.

1.5 Main Features

- Support hundreds of 3G/4G wireless modules, plug and play;
- Intelligent anti-drop line, support online detection, online maintenance, automatic redial of dropped calls, ensuring that the device is always online;
- Cloud remote background management, ad push, remote upgrade and remote configuration;
- Local network PHP browsing and remote synchronization of local storage content;
- Support serial port TCP/UDP transparent data transmission or AT command transmission;
- SMS control route online and offline, short-term notification of routing status;
- Support VPN security tunneling, including PPTP, L2TP;
- Complete and robust router function, support multiple Internet access methods: automatic allocation, specified IP, PPPoE;
- Support IPTABLES firewall, various network protocols;
- Support serial port local TFTP, web software upgrade;
- Support for dynamic DDNS: support for peanut shell, 88IP and dyndns domain name service providers;

1.6 Specifications

Item	Parameter	Description
Power Supply	Input voltage	7-35VDC
	Consumption	Standby:12V/50mA; Max.:12V/150mA
	Protection	Anti-reverse connection
Ethernet	QTY	R10:1*WAN/LAN,1*LAN R20:1*WAN/LAN,3*LAN
	Type	RJ45 Integrated 10/100M,MDI/MDIX
	Function	ETH0: WAN interface / LAN interface ETH1: LAN interface ETH2: LAN interface ETH3: LAN interface
	Protection	ESD contact: 8KV, surge: 4KV (10/1000us)

Serial Port	QTY	1 channel
	Type	RS485(default)/RS232
	Baud rate	110bps-128000bps
	Data bit	7,8
	Parity Bit	None, Even, Odd
	Stop Bit	1,2
	Operating mode	AT Command mode, Transparent transmission mode
	Protection	ESD contact: 8KV, surge: 4KV (8/20us)
WIFI	Antenna port qty	2
	Antenna port type	SMA hole type
	Protocol	802.11a/b/g/n（mixed）
	Mode	AP mode, client mode
	Frequency	2.4G
	Channel	1-13
	Security	Open ,WPA,WPA2
	Encryption	AES,TKIP,TKIPAES
	Connections numbers	32 max
	Rate	300Mbps（Max）
	Transmission distance	Open space up to 100 meters
	SSID broadcast switch	Support
Cellular Network	Antenna port qty	1
	Antenna port type	SMA hole type

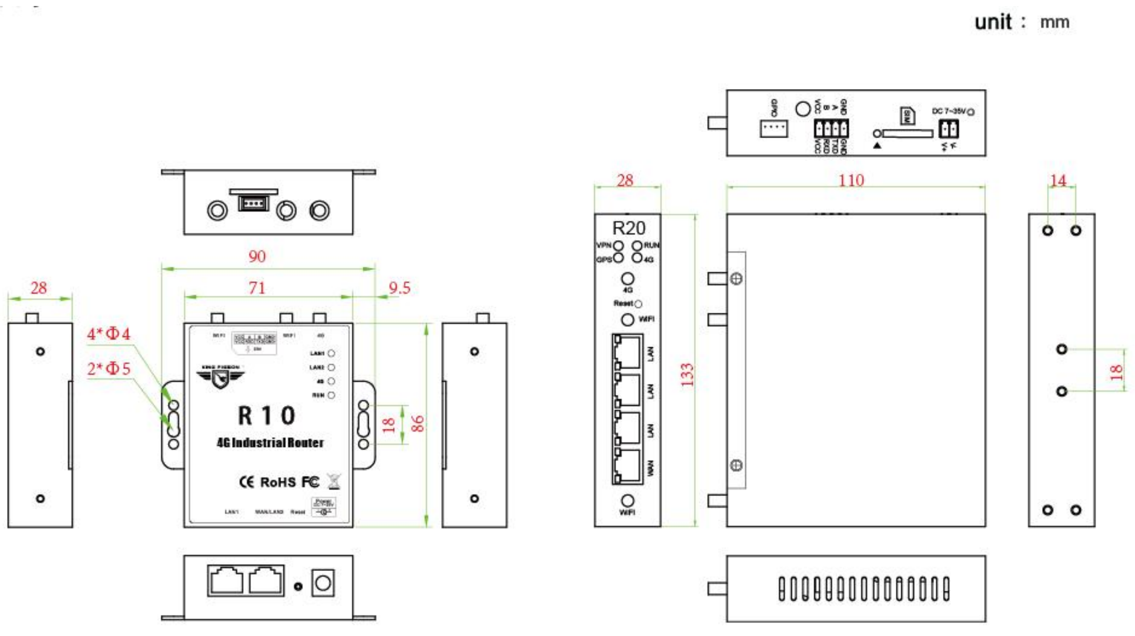
	SIM/UIM card interface	R10: Self-elastic interface;
		R20: drawer interface;
		Both support 1.8V/3V SIM/UIM card with built-in 15KV ESD protection.

	4G (E version)	GSM/EDGE：900,1800MHz WCDMA：B1,B5,B8 FDD：B1,B3,B5,B7,B8,B20 TDD：B38,B40,B41
	4G (AU version)	GSM/EDGE：850,900,1800MHz WCDMA：B1,B2,B5,B8 FDD：B1,B2,B3,B4,B5,B7,B8,B28 TDD：B40
	4G (A version)	WCDMA：B2,B4,B5 FDD：B2,B4,B12
	4G (V version)	FDD：B4,B13
	4G (J version)	WCDMA：B1,B3,B8,B18,B19，B26 FDD：B2,B4,B12 TDD: B41
	4G (CE version)	GSM/EDGE：900,1800MHz WCDMA：B1,B8 TD-SCDMA：B34,B39

		FDD：B1,B3,B8 TDD：B38,B39,B40,B41
	SIM/UIM card interface	Drawer interface / self-elastic interface Support 1.8V/3V SIM/UIM card with built-in 15KV ESD protection
GPS (Only for R20)	Antenna Port Qty	1
	Antenna Port Type	SMA
	Tracking Sensitivity	> -148 dBm
	Horizontal Accuracy	2.5M
	Protocol	NMEA-0183 V2.3
System	CPU	MIPS CPU,Clock Speed 580Mhz
	Flash	128Mbits SPI Flash
	Memory	1024Mbits DDR2
Software	Network Protocol	IPV4/TCP/IP/PPPOE/DHCP/DNS/DDNS/NAT/HTTPS/ARP/FTP/telnet/SSH
	Firewall	Support IPTABLES /DMZ/DoS defense
	VPN	PPTP/L2TP
	Remote Management	Support web remote configuration
	Port Mapping	Support
	SMS Command	Support
	System Log	Support
	Firmware Upgrade	Support serial port local TFTP/web firmware upgrade
Certificate	MTBF	≥100,000hours
	EMC	EN 55022: 2006/A1: 2007 (CE &RE) Class B
		IEC 61000-4-2 (ESD) Level 4
		IEC 61000-4-3 (RS) Level 4
		IEC 61000-4-4 (EFT) Level 4
		IEC 61000-4-5 (Surge)Level 3
		IEC 61000-4-6 (CS)Level 4
		IEC 61000-4-8 (M/S) Level 4
	others	CE/FCC/ROHS/3C
Environment	Working Temperature&Humidity	-40～85℃,5～95%RH
	Storage Temperature&Humidity	-45～105℃,5～95%RH
Others	Enclosure	Metal
	Size	R10 90*86*28 mm R20 133*110*28 mm
	IP level	IP30
	Net Weight	R10: 280g R20: 460g
	Installation	Wall-amount/ rail-amount

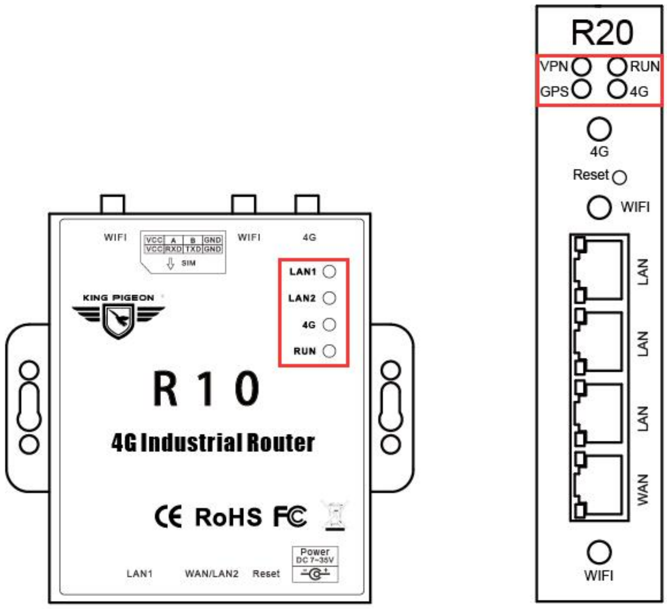
2. Physical Layout and Installation Diagram

2.1 Unit size



R10 R20

2.2 LED Indicator light

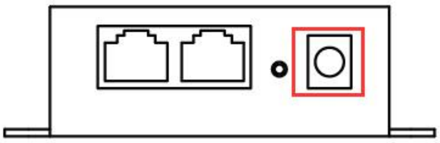


LED Indicator light		
Name	**Status**	**Description**
RUN	flick	Router is running
	off	Router stop running
VPN	on	VPN connected
	off	VPN disconnected

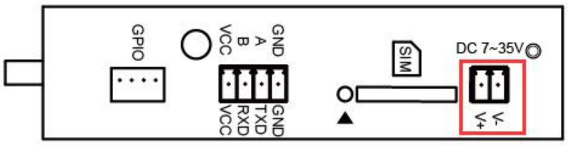
4G	on	Internet connected
	off	Internet disconnect
GPS	on	GPS location on
	off	GPS location off
LAN1	on	LAN1 connected device
	off	LAN1 disconnect device
LAN2	on	LAN2 connected device
	off	LAN2 disconnect device

2.3 Power input

R10 supports DC2.0 terminal insertion mode; R20 supports 3.5mm terminal connection mode.



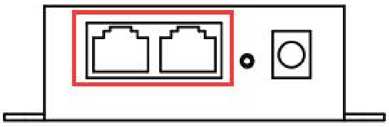
R10



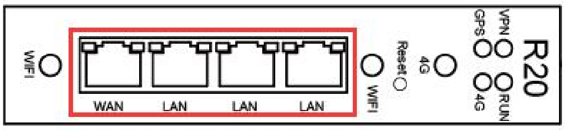
R20

2.4 Ethernet Port

R10 has 2 Ethernet ports, 1 WAN/LAN port and 1 LAN port; R20 has 4 Ethernet ports, 1 WAN/LAN port and 3 LAN ports; WAN/LAN can be used WAN port in "standard route mode",used LAN in other modes.
Note: The router default “3G/4G wireless routing mode” and the WAN/LAN port defaults is LAN.



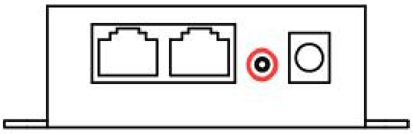
R10



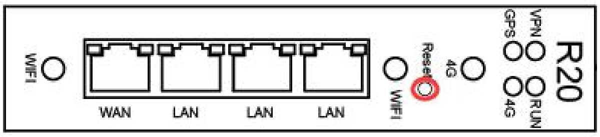
R20

2.5 Reset

Press this button for 5 seconds when it is in running state , the RUN light will be flashing quickly, After that ,



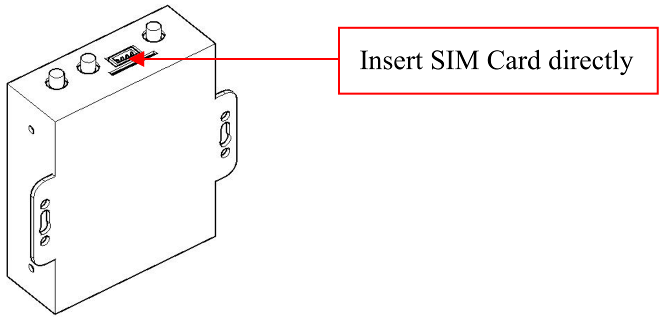
R10



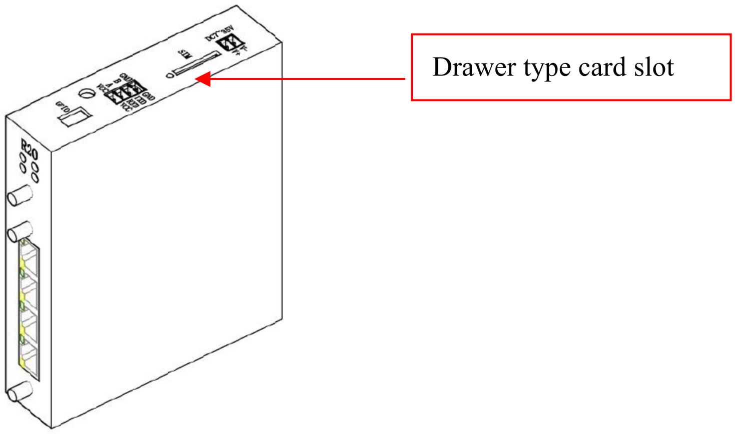
R20

2.6 SIM Card

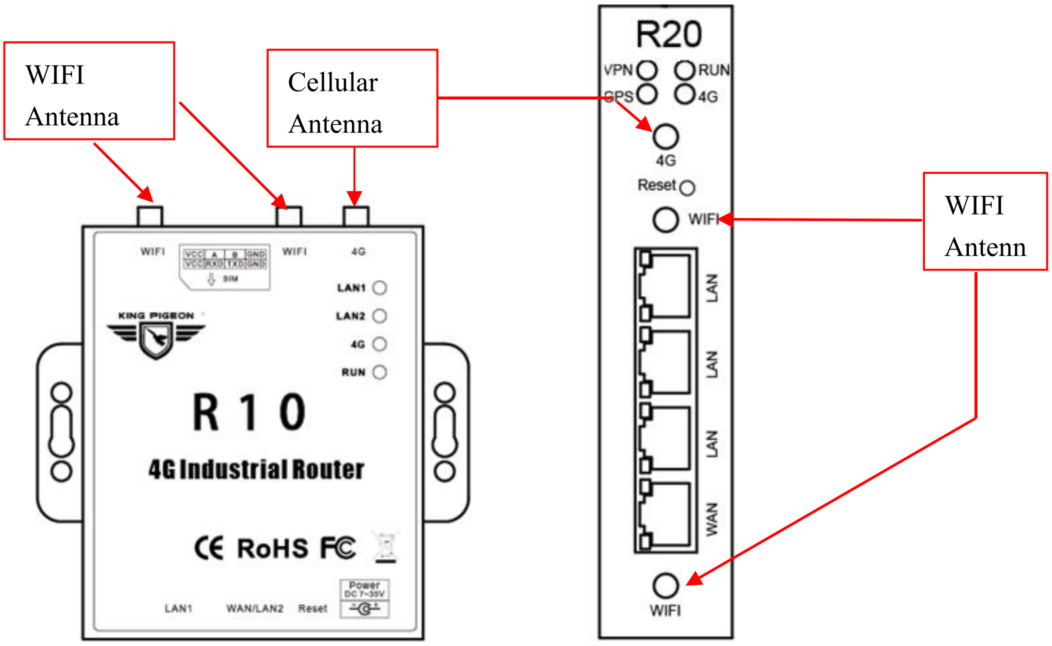
When inserting/removing the SIM card, make sure the device is turned off.
R10 supports self-elastic card slot interface:



R20 supports drawer type card slot interface:

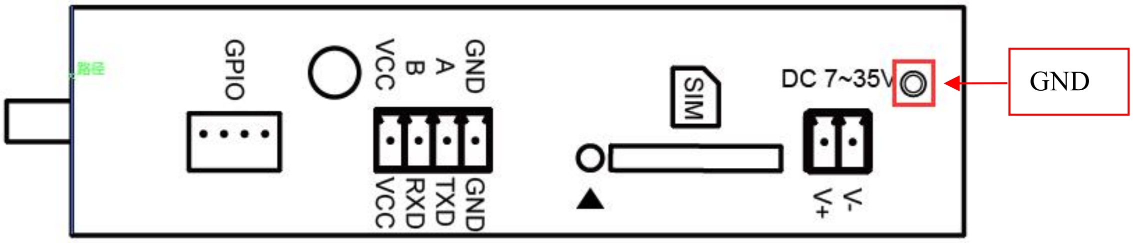


2.7 External Antenna Connection



2.8 Router GND

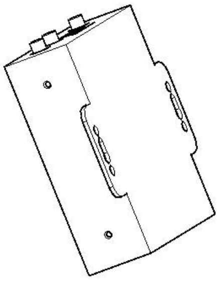
The router ground wire helps prevent electromagnetic interference. This product should be mounted on a well-grounded device surface such as a metal plate.



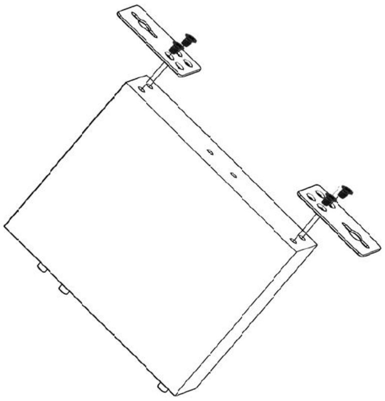
3. Installation

This device supports horizontal desktop placement, wall mounting and rail mounting

3.1 Wall-mounted

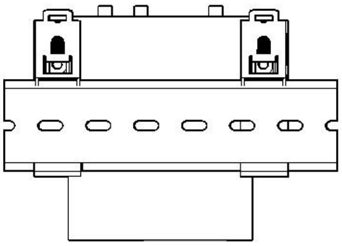


(R10)

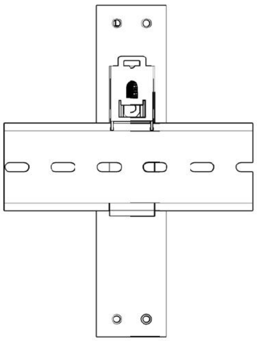


(R20)

3.2 Rail installation

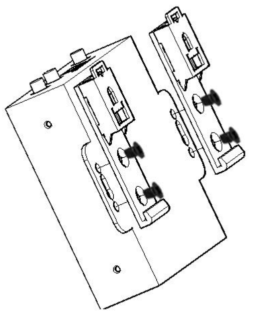


(R10)

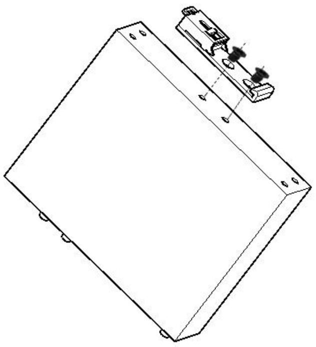


(R20)

3.3 Buckle installation



(R10)



(R20)

4. Parameter Configuration

The router supports web page configuration. supports IE6.0 or above, Google and Firefox, Linux 2.6 and above, Mac OS 10.3.7 and above, Windows XP/ Vista/7/ 8 /10 and so on.

There are two ways to connect to the router, one is through a wired connection, through an external repeater/hub connection, or directly to the computer;Another way is WIFI connection.

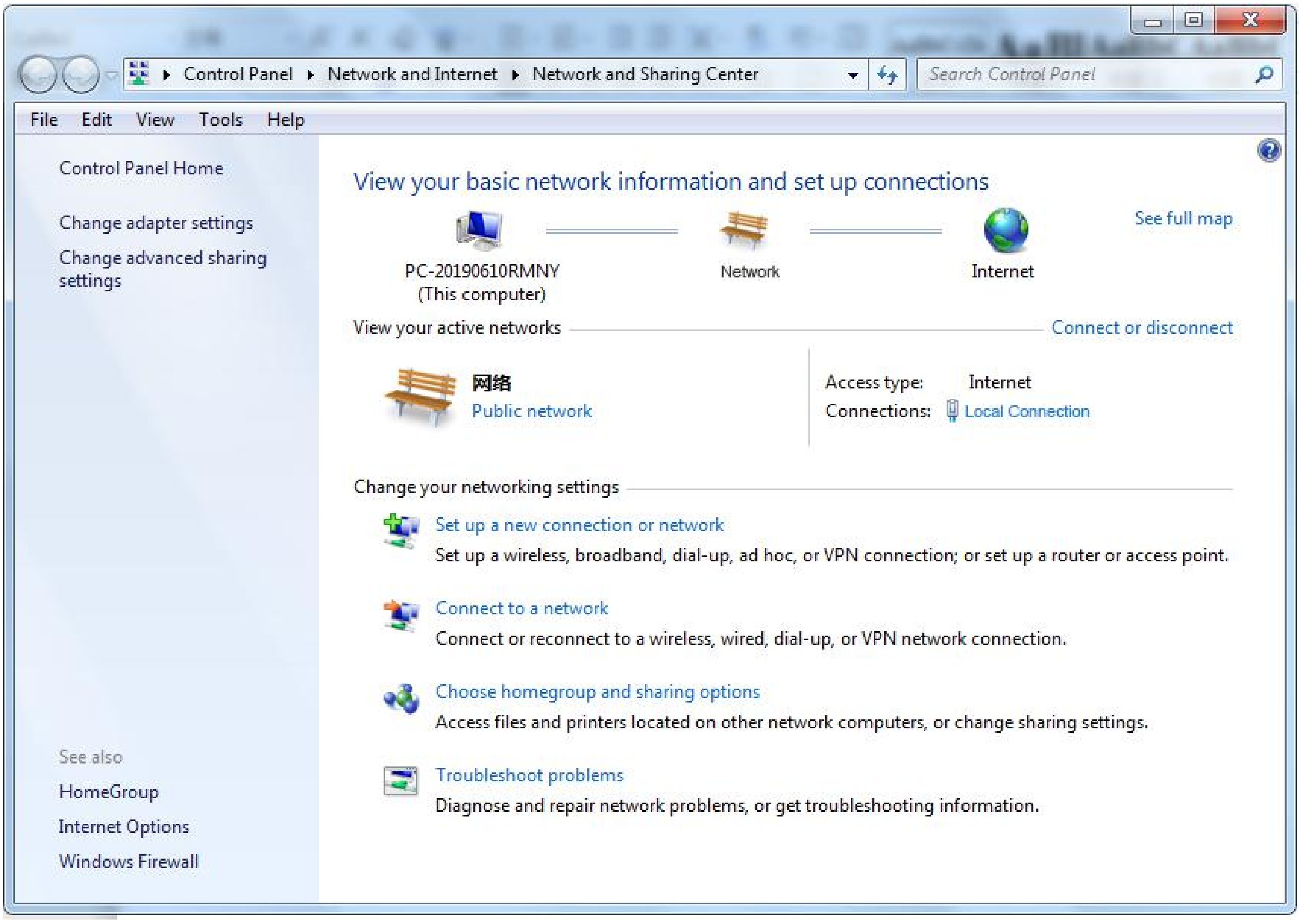
When the router is directly connected to the Ethernet port of the computer, if the router acts as a DHCP server, the computer can obtain the IP directly from the router.The computer can also set the static IP with the router in the same network segment, so that the computer and the router form a small local area network.After the computer and the router connected successfully , enter the default login address of the device on the computer browser to login the router.

4.1 Wired Connection

There are two ways to configure the IP address; one is to automatically obtain an IP address on the local connection of the PC, and the other is to configure a static IP address on the same subnet as the router on the local connection of the PC.

Following example is Windows 7 system configuring.Windows system is similar:

Step1: Click Start - Control Panel - Network and Sharing Center, then double-click Local Connection



View your basic network information and set up connections

View your active networks

网络
Public network

Access type: Internet
Connections: Local Connection

Change your networking settings

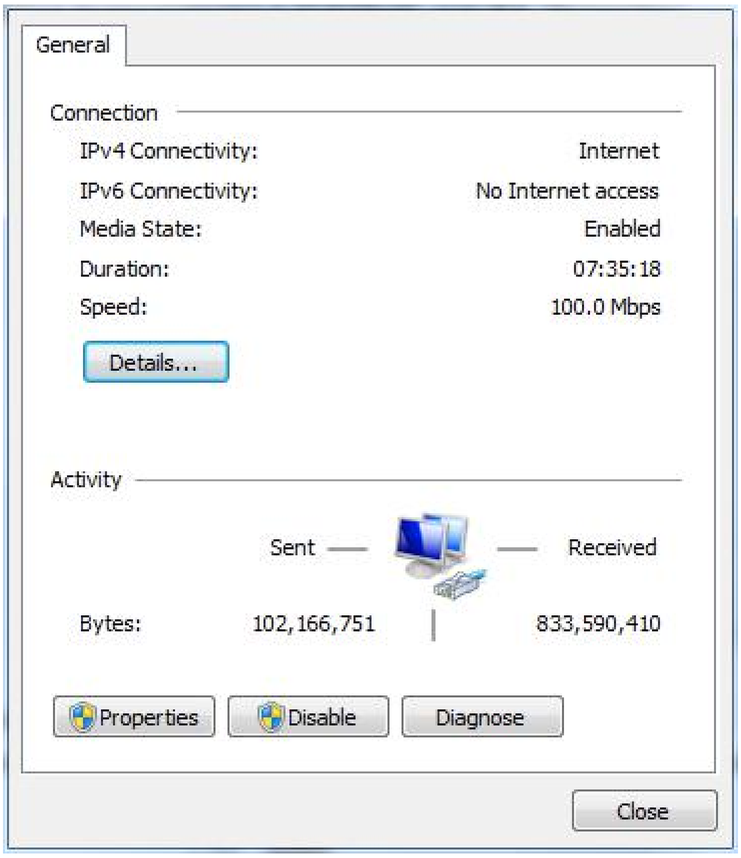
Set up a new connection or network
Set up a wireless, broadband, dial-up, ad hoc, or VPN connection; or set up a router or access point.

Connect to a network
Connect or reconnect to a wireless, wired, dial-up, or VPN network connection.

Choose homegroup and sharing options
Access files and printers located on other network computers, or change sharing settings.

Troubleshoot problems
Diagnose and repair network problems, or get troubleshooting information.

Step2: In the "Local Connection Status" window, click Properties.



General

Connection

IPv4 Connectivity:	Internet
IPv6 Connectivity:	No Internet access
Media State:	Enabled
Duration:	07:35:18
Speed:	100.0 Mbps

Details...

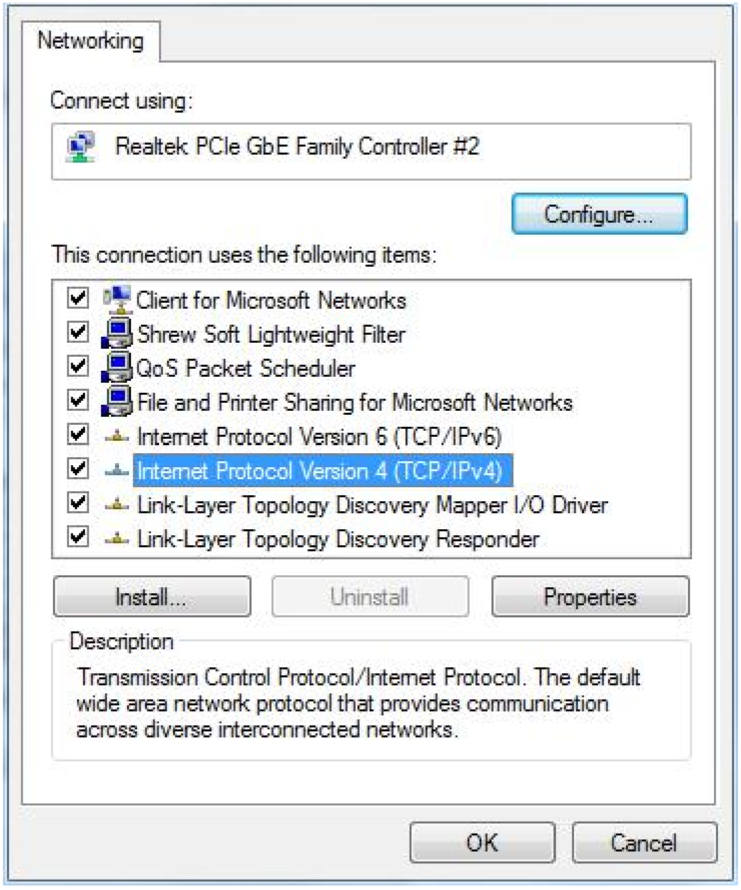
Activity

	Sent	Received
Bytes:	102,166,751	833,590,410

Properties | Disable | Diagnose

Close

Step3: **Select "Internet Protocol Version 4 (TCP/IPv4)" and click "Properties".**



Networking

Connect using:

Realtek PCIe GbE Family Controller #2

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ Shrew Soft Lightweight Filter
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Install... | Uninstall | Properties

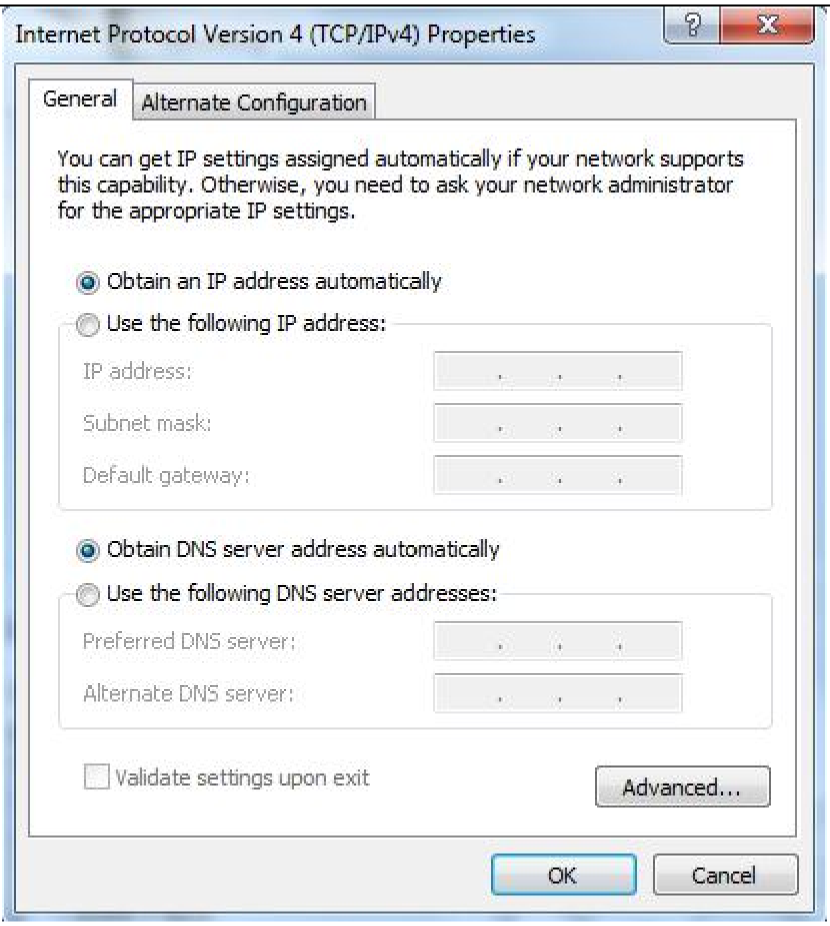
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

OK | Cancel

Step4: **Two ways to configure the IP address**

Obtain an IP address automatically from the DHCP server and click "Obtain an IP address automatically";



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

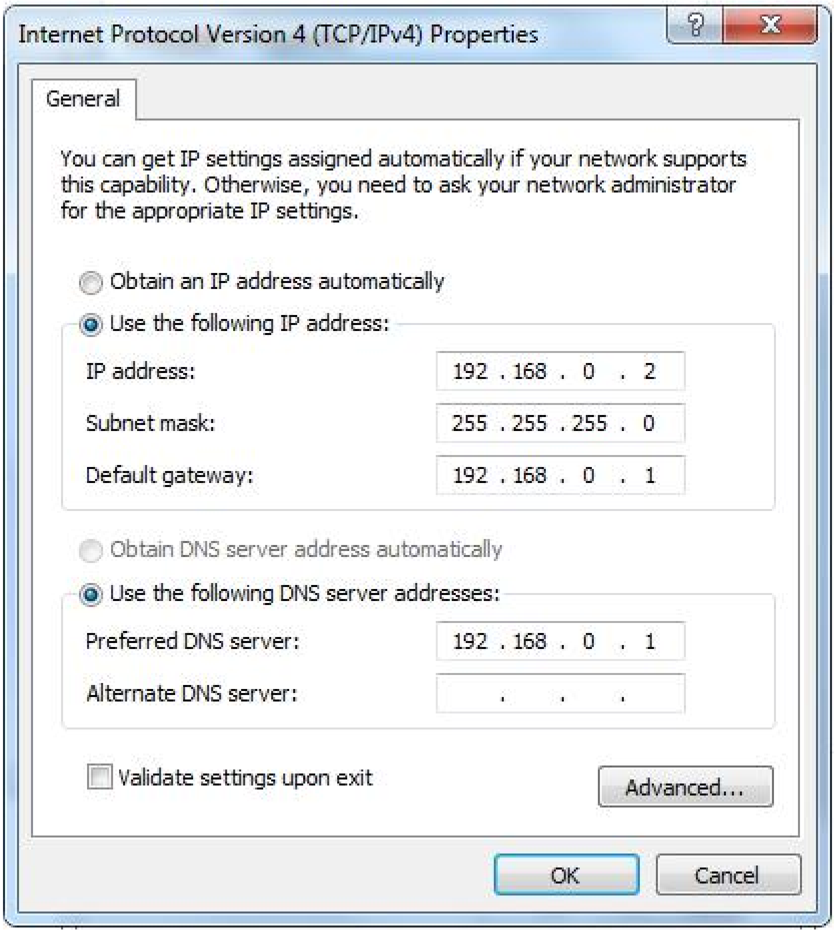
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Manually configure the PC with a static IP address on the same subnet as the router address, click and configure "Use the following IP address".



Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

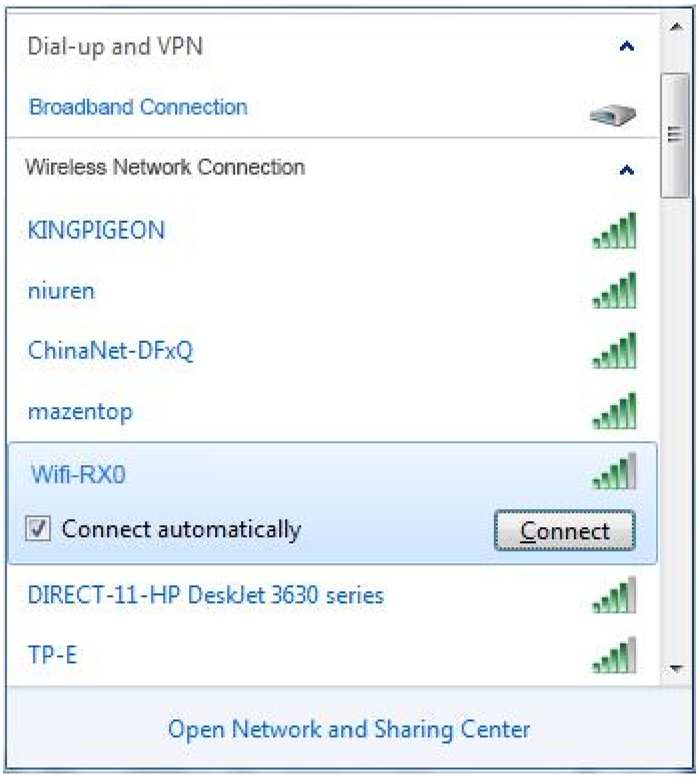
Alternate DNS server: . . .

□ Validate settings upon exit

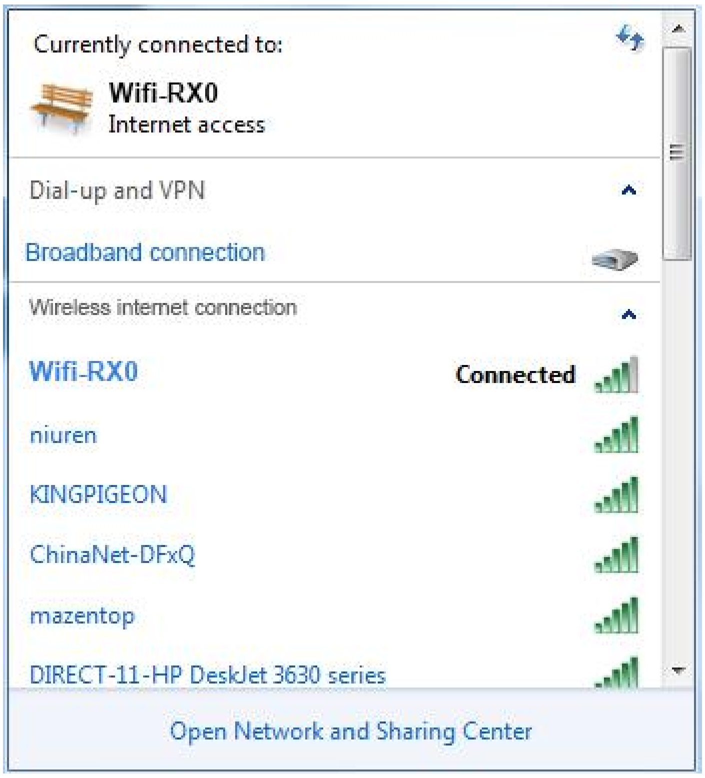
Step5: **Click "OK" to complete the configuration**

4.2 Wifi Connection

Step1: **Detect Router Wireless Network Connection**



Step2: **Click “connect” to establish a connection**



4.3 Default Setting

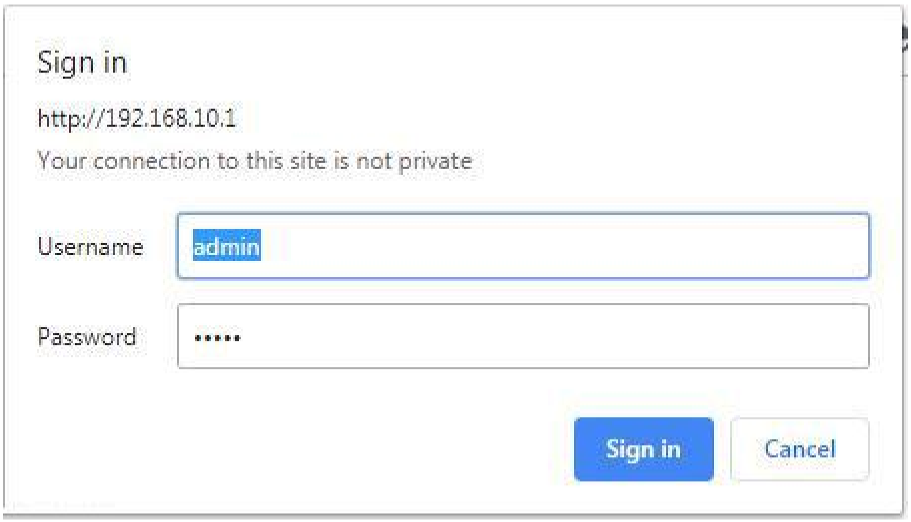
Before logging the configuration page, please check the default settings as below:

Item	Description
User name	admin
Password	admin
DHCP server	open
WIFI	AP mode SSID： Wifi-xxxx-xxxx KEY : 12345678

4.4 Enter web setting

(1).Open a browser, such as IE, Google, etc. and enter IP address: http://192.168.10.1

(2).Enter username and password, user name: admin   Password: admin



Sign in

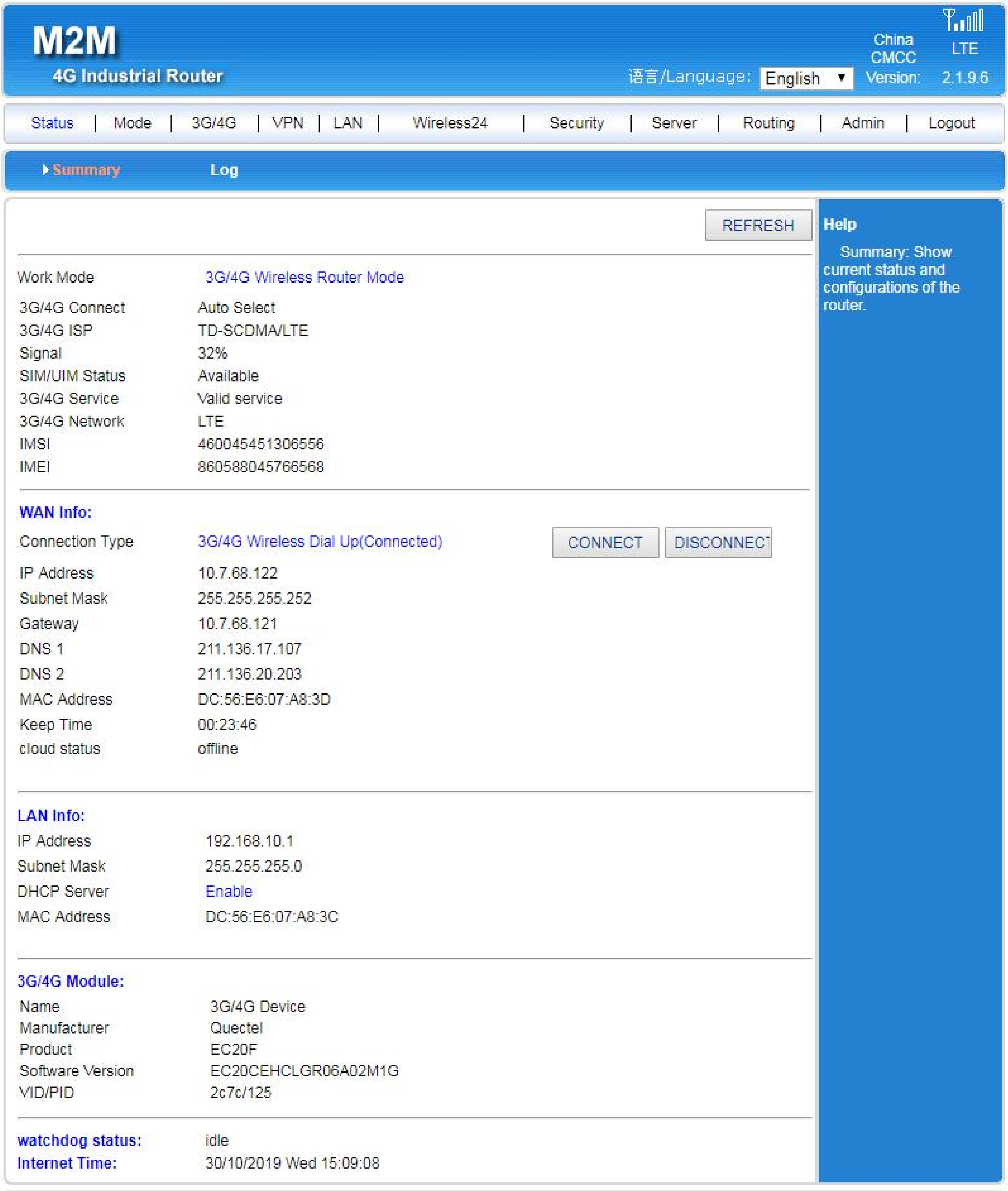
http://192.168.10.1

Your connection to this site is not private

Username: admin

Password: •••••

After successfully login the R10/R20 router, the page is displayed as below:



Help

Summary: Show current status and configurations of the router.

Work Mode	3G/4G Wireless Router Mode
3G/4G Connect	Auto Select
3G/4G ISP	TD-SCDMA/LTE
Signal	32%
SIM/UIM Status	Available
3G/4G Service	Valid service
3G/4G Network	LTE
IMSI	460045451306556
IMEI	860588045766568

WAN Info:

Connection Type	3G/4G Wireless Dial Up(Connected)
IP Address	10.7.68.122
Subnet Mask	255.255.255.252
Gateway	10.7.68.121
DNS 1	211.136.17.107
DNS 2	211.136.20.203
MAC Address	DC:56:E6:07:A8:3D
Keep Time	00:23:46
cloud status	offline

LAN Info:

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	DC:56:E6:07:A8:3C

3G/4G Module:

Name	3G/4G Device
Manufacturer	Quectel
Product	EC20F
Software Version	EC20CEHCLGR06A02M1G
VID/PID	2c7c/125

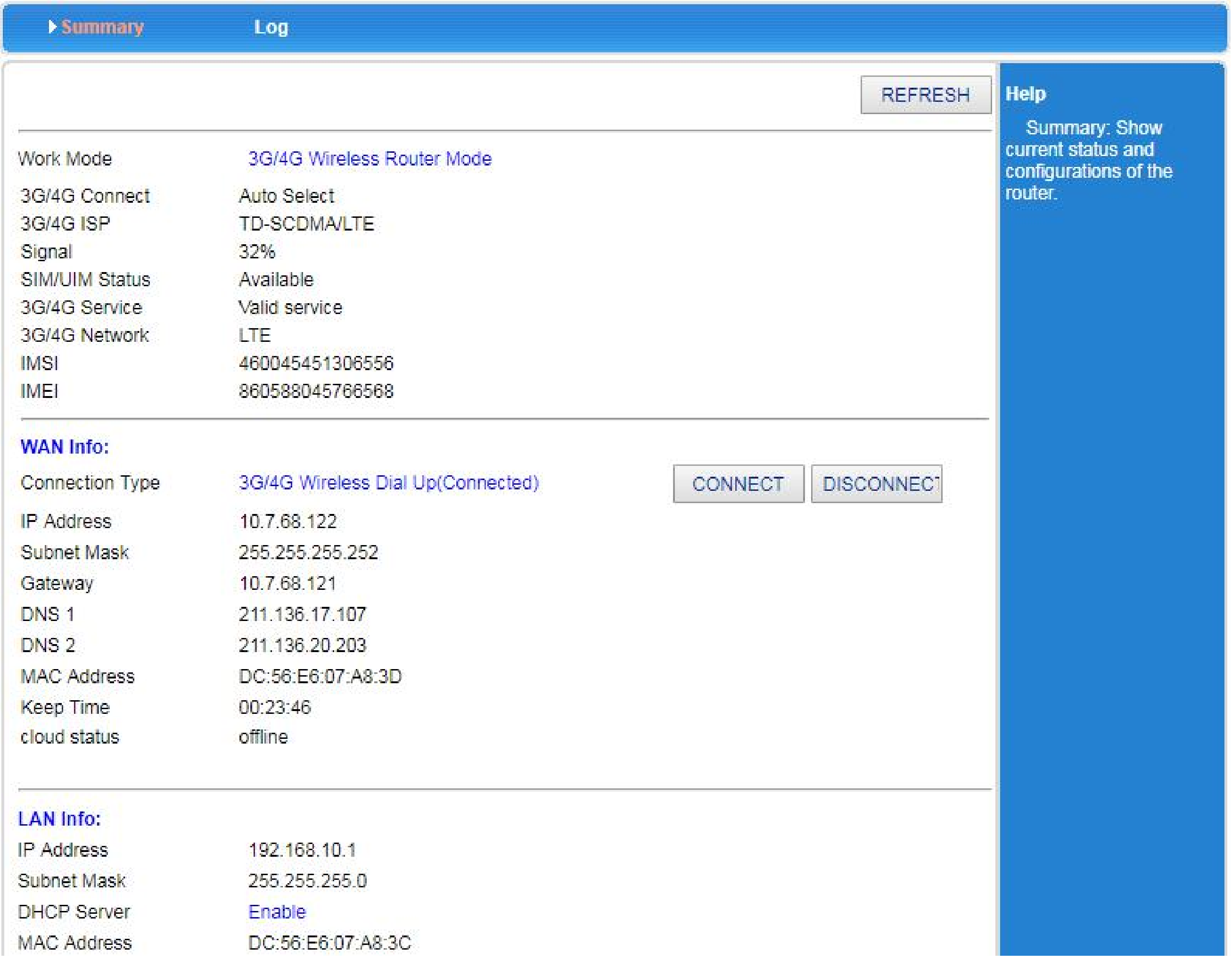
watchdog status:	idle
Internet Time:	30/10/2019 Wed 15:09:08

5. *Router Setting*

5.1 *Current status*

System status

Display current system running status



Help

Summary: Show current status and configurations of the router.

Work Mode 3G/4G Wireless Router Mode

3G/4G Connect	Auto Select
3G/4G ISP	TD-SCDMA/LTE
Signal	32%
SIM/UIM Status	Available
3G/4G Service	Valid service
3G/4G Network	LTE
IMSI	460045451306556
IMEI	860588045766568

WAN Info:

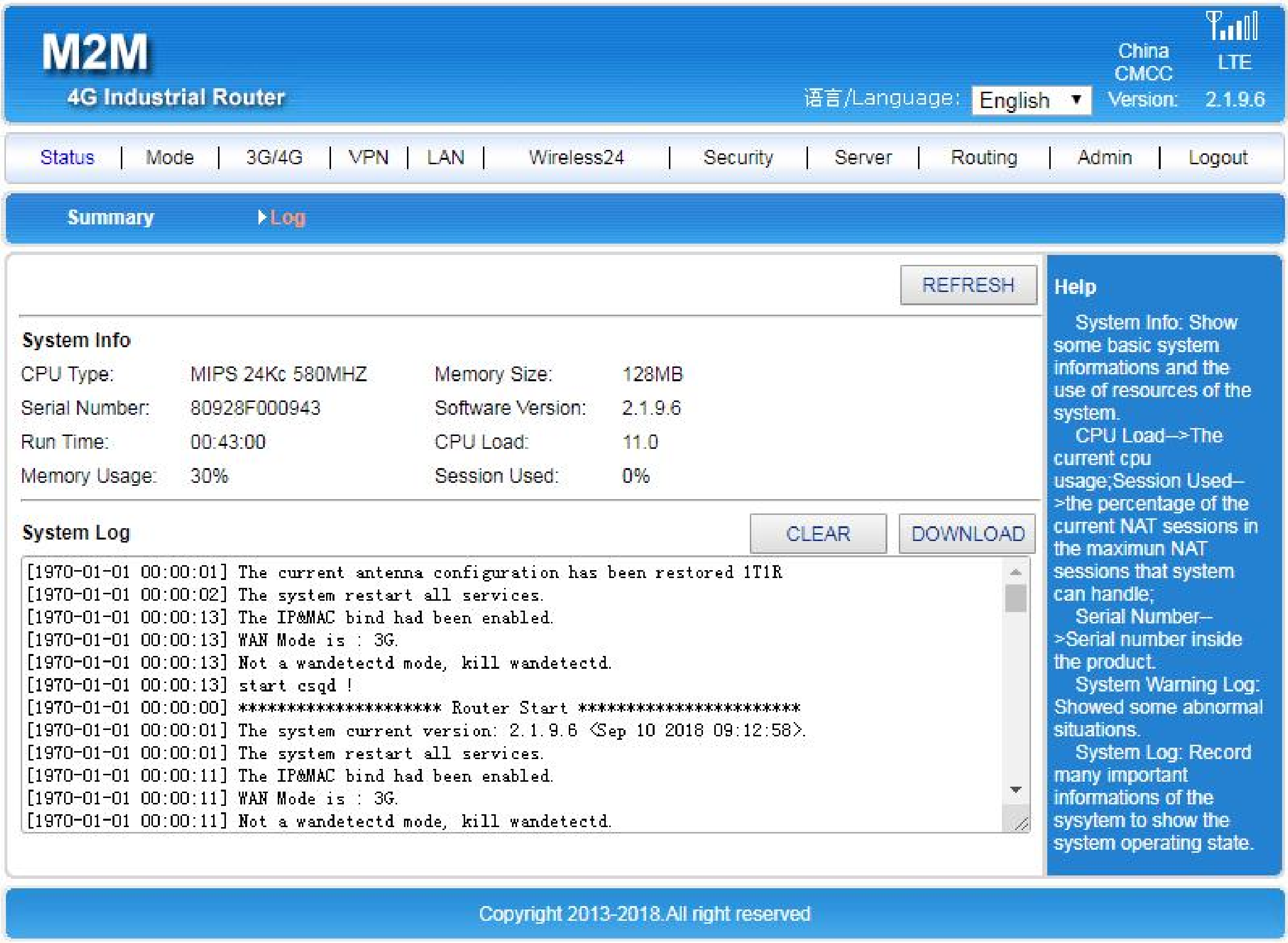
Connection Type	3G/4G Wireless Dial Up(Connected)
IP Address	10.7.68.122
Subnet Mask	255.255.255.252
Gateway	10.7.68.121
DNS 1	211.136.17.107
DNS 2	211.136.20.203
MAC Address	DC:56:E6:07:A8:3D
Keep Time	00:23:46
cloud status	offline

LAN Info:

IP Address	192.168.10.1
Subnet Mask	255.255.255.0
DHCP Server	Enable
MAC Address	DC:56:E6:07:A8:3C

System Status		
Item	**Description**	**Default**
WAN Info	The current connection mode and status, obtained IP address, gateway address, and DNS server address. Based on these, you can judge whether the router is working properly.	--
LAN Info	LAN IP address, whether the DHCP server is started, and the range of IP addresses that can be assigned.	--
3G/4G module	Whether 3G/4G devices is connected and the device names, manufacturers, types, and IDs etc..	--
Internet Time	The Internet time of system.	--

Log


M2M
4G Industrial Router
China CMCC
LTE
语言/Language: English
Version: 2.1.9.6
Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Summary
Log
REFRESH
CLEAR
DOWNLOAD
Copyright 2013-2018.All right reserved

System Info

CPU Type:	MIPS 24Kc 580MHZ	Memory Size:	128MB
Serial Number:	80928F000943	Software Version:	2.1.9.6
Run Time:	00:43:00	CPU Load:	11.0
Memory Usage:	30%	Session Used:	0%

System Log

```
[1970-01-01 00:00:01] The current antenna configuration has been restored 1T1R
[1970-01-01 00:00:02] The system restart all services.
[1970-01-01 00:00:13] The IP&MAC bind had been enabled.
[1970-01-01 00:00:13] WAN Mode is : 3G.
[1970-01-01 00:00:13] Not a wandetectd mode, kill wandetectd.
[1970-01-01 00:00:13] start csqd !
[1970-01-01 00:00:00] ********************* Router Start ***********************
[1970-01-01 00:00:01] The system current version: 2.1.9.6 <Sep 10 2018 09:12:58>.
[1970-01-01 00:00:01] The system restart all services.
[1970-01-01 00:00:11] The IP&MAC bind had been enabled.
[1970-01-01 00:00:11] WAN Mode is : 3G.
[1970-01-01 00:00:11] Not a wandetectd mode, kill wandetectd.
```

Help

System Info: Show some basic system informations and the use of resources of the system.
CPU Load-->The current cpu usage;Session Used-->the percentage of the current NAT sessions in the maximun NAT sessions that system can handle;
Serial Number-->Serial number inside the product.
System Warning Log: Showed some abnormal situations.
System Log: Record many important informations of the sysytem to show the system operating state.

Log		
Item	**Description**	**Default**
CPU Type	Device CPU model	--
Serial Number	Serial number	--
Run Time	The time of router powered on until now.	--
Memory Usage	Current memory usage	--
Memory Size	128M	--
Software Version	Current system version of the device	--
CPU Load	Current CPU usage	--
Session Used	The current number of established NAT sessions as a percentage of the maximum number of NAT sessions that the system can handle.	--
System log	Record some important information of the system, which can help you quickly locate device faults or understand network conditions, such as setting status changes and network attacks during system operation.	--

Note: After the router is restarted, all recorded logs will be lost.

File Sharing

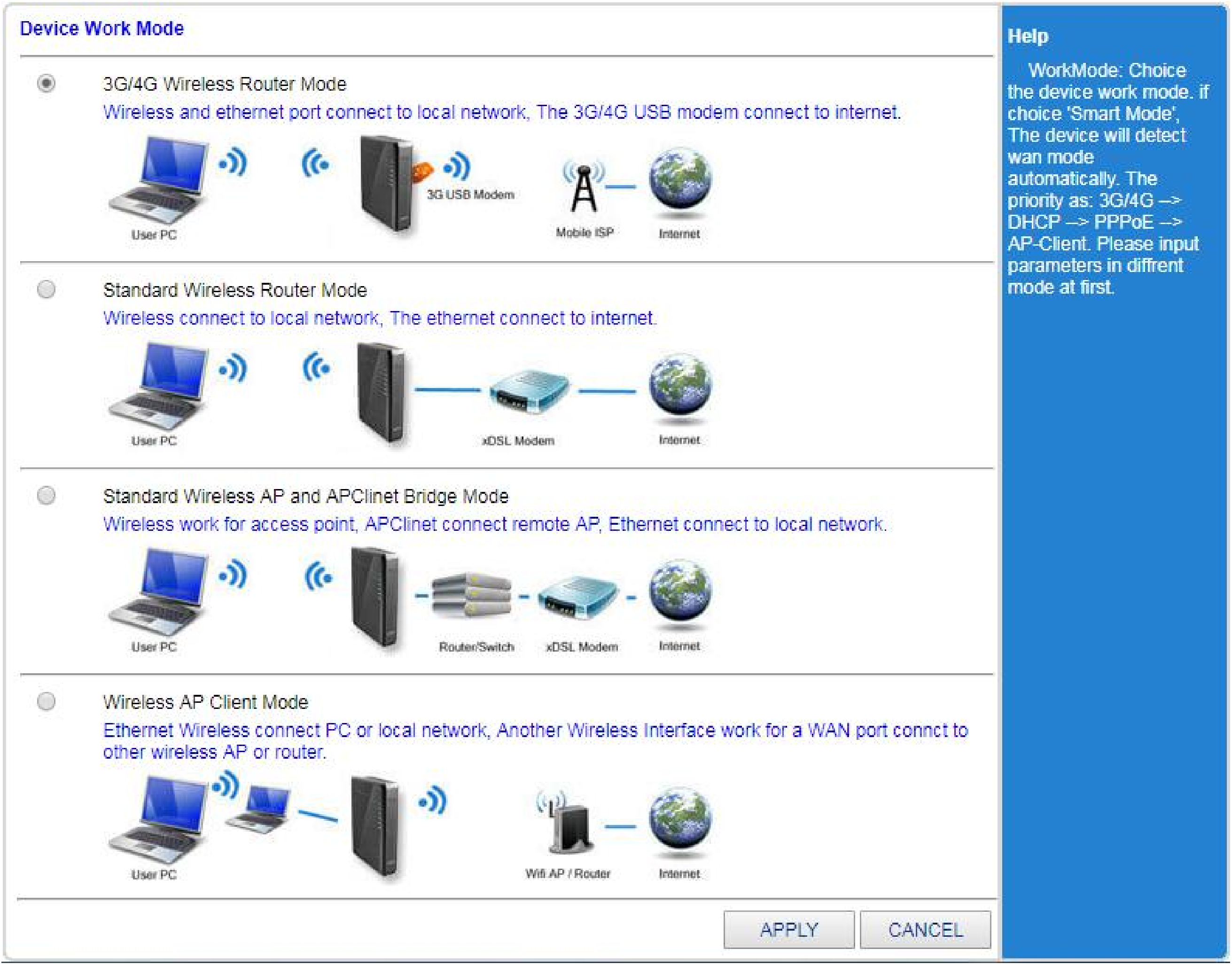
Router reserved function,unwork.

Video Surveillance

Router reserved function,unwork

5.2 Work Mode

R10/R20 supports following 4 work modes:



Device Work Mode

● 3G/4G Wireless Router Mode
Wireless and ethernet port connect to local network, The 3G/4G USB modem connect to internet.

○ Standard Wireless Router Mode
Wireless connect to local network, The ethernet connect to internet.

○ Standard Wireless AP and APClinet Bridge Mode
Wireless work for access point, APClinet connect remote AP, Ethernet connect to local network.

○ Wireless AP Client Mode
Ethernet Wireless connect PC or local network, Another Wireless Interface work for a WAN port connct to other wireless AP or router.

Help

WorkMode: Choice the device work mode. if choice 'Smart Mode', The device will detect wan mode automatically. The priority as: 3G/4G --> DHCP --> PPPoE --> AP-Client. Please input parameters in diffrent mode at first.

Work Mode		
Item	**Description**	**Default**
3G/4G Wireless Router Mode	The "3G/4G Settings" interface of the router is the WAN setting interface, and the "Internet access mode" only has 4G dial-up;	√
Standard Wireless Router Mode	The router's Internet access method is optional, static address, dynamic address and PPPoE;	x
Wireless AP And AP client Bridge Mode	Wireless and wired networks act as LAN access points, and wireless connect to remote AP by bridging;	x
Wireless AP client mode	Relay mode or WISP, the wireless interface also serves as a client to connect to other AP. Please use the information provided by your ISP to choose the appropriate Internet access method.	x

After selecting <Work Mode>, you can set in <3G/4G> or <WAN>:

- Connection type
- Break detection
- MAC clone(non 3G/4G mode)
- Dynamic domain name setting(DDNS)

- AT Command (3G/4G mode)

5.3 3G/4G Setting(WAN Setting)

5.3.1 Connection Methods

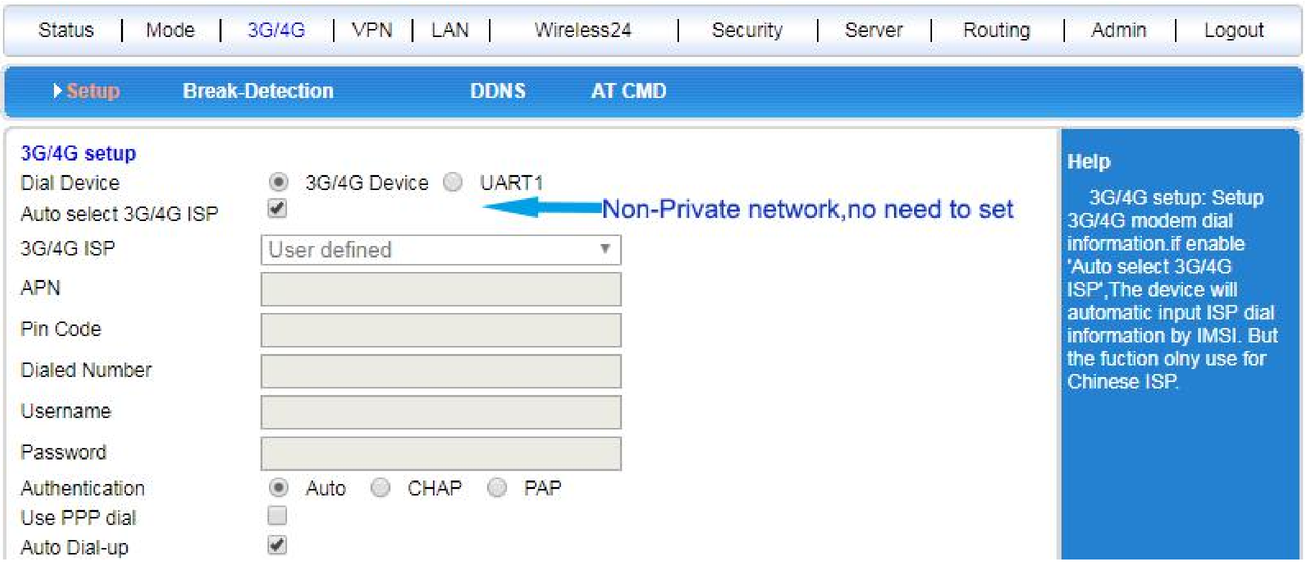
3G/4G Wireless Router Mode

•**Automatic Select Operators:**

For ordinary mobile phone SIM card or IoT SIM card, no need to set, the system automatically queries the appropriate ISP dial-up Internet.

•**VPDN Dial-up:**

For the private network tariff card, you need to set a specific APN, user name and password to achieve VPDN access. VPDN:Virtual Private Dial一up Networks or Virtual private dial-up network,It is a kind of VPN service, which is based on the virtual private dial-up network service of dial-up users.That is to use the dial-up access method to access the Internet, which is a secure virtual private network established by using the bearer function of the IP network combined with the corresponding authentication and authorization mechanism.It is a technology that has developed rapidly with the development of the Internet in recent years,Can be used for intra-regional group intranets, professional information service provider private networks, financial mass service networks, bank access service networks, etc.VPDN uses a dedicated network security and communication protocol that enables enterprises to establish a relatively secure virtual private network on a public network.VPN users can connect to the user network inside the user through the virtual secure channel through the public network, and users on the public network cannot access the resources inside the user network through the virtual channel.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Setup
Break-Detection
DDNS
AT CMD

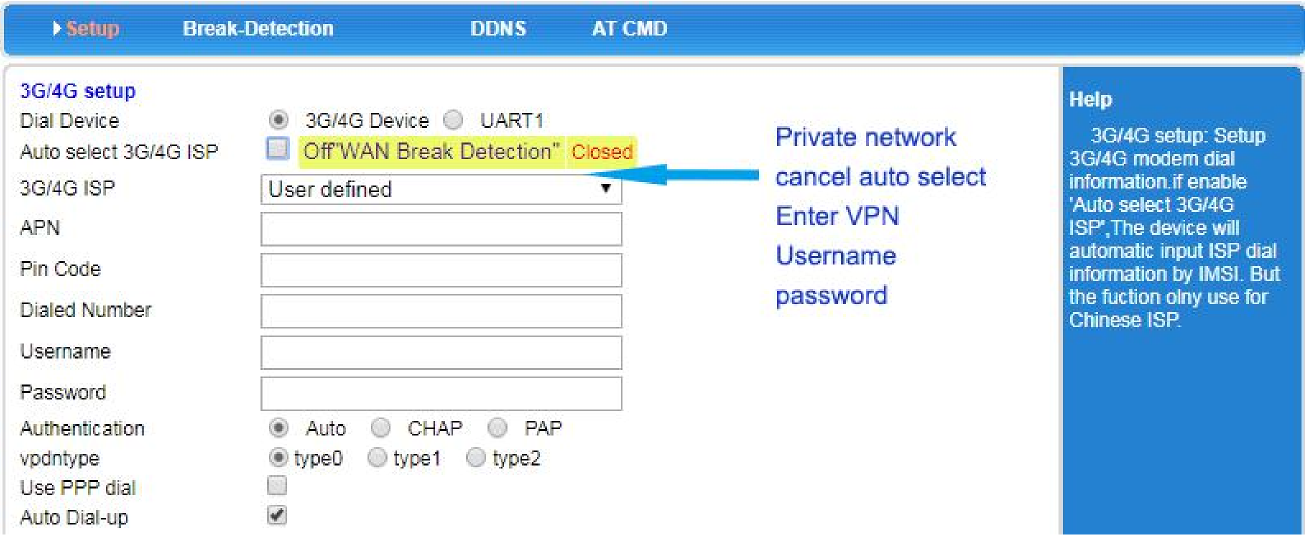
3G/4G setup

Dial Device	● 3G/4G Device ○ UART1
Auto select 3G/4G ISP	☑
3G/4G ISP	User defined
APN	
Pin Code	
Dialed Number	
Username	
Password	
Authentication	● Auto ○ CHAP ○ PAP
Use PPP dial	☐
Auto Dial-up	☑

Non-Private network,no need to set

Help

3G/4G setup: Setup 3G/4G modem dial information.if enable 'Auto select 3G/4G ISP',The device will automatic input ISP dial information by IMSI. But the fuction olny use for Chinese ISP.



3G/4G setup

Dial Device	● 3G/4G Device ○ UART1
Auto select 3G/4G ISP	□ Off"WAN Break Detection" Closed
3G/4G ISP	User defined ▾
APN	
Pin Code	
Dialed Number	
Username	
Password	
Authentication	● Auto ○ CHAP ○ PAP
vpdntype	● type0 ○ type1 ○ type2
Use PPP dial	□
Auto Dial-up	☑

Private network
cancel auto select
Enter VPN
Username
password

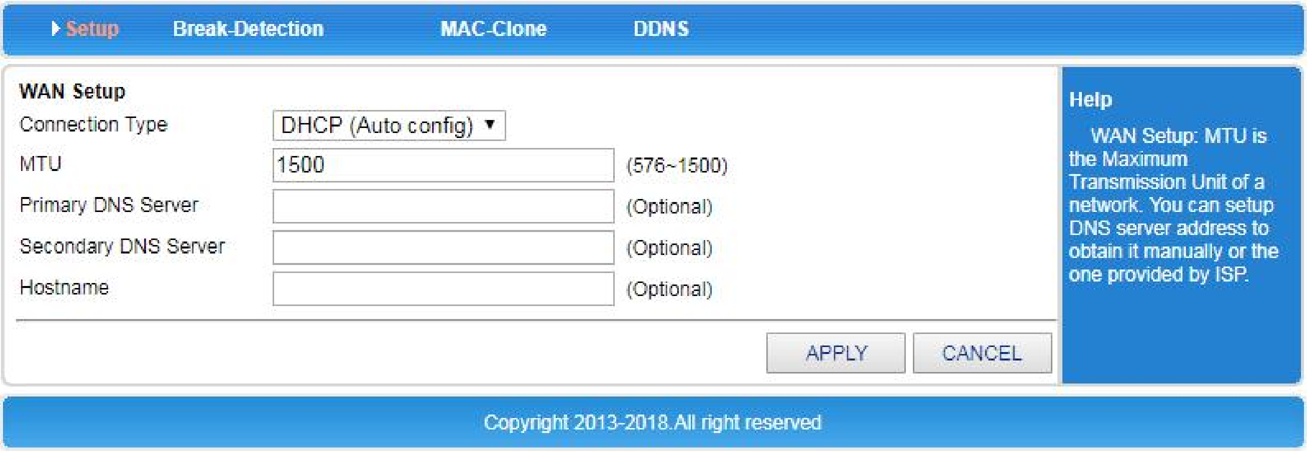
Help

3G/4G setup: Setup 3G/4G modem dial information.if enable 'Auto select 3G/4G ISP",The device will automatic input ISP dial information by IMSI. But the fuction olny use for Chinese ISP.

3G/4G Wireless Router Mode@Connection mode		
Item	**Description**	**Default**
Dial Device	Select a static address in the list.	3G/4G
Auto select 3G/4G ISP	Tick it,Will automatically choose the network operator	√
3G/4G ISP	Generally China Mobile, China Unicom, China Telecom	--
APN	Provided by the ISP. The special network card filled.	--
Pin code	SIM Card pin code	--
Dialed Number	Provided by the ISP	--
Username	Provided by the ISP	--
Password	Provided by the ISP	--
Authentication	CHAP and PAP. Chap is a three-way handshake, The two sides only transmit the username, do not transfer the password, the password is pre-configured on the router, only need to compare it.Pap is a two-way handshake. It not only transmits the username but also the password, and the password is transmitted in plain text, which is not secure.	auto
Auto Dial-up	Optional, recommend open.	√
Router will reboot after dial N times	Default is 3 times. If did not insert into the SIM card, recommend to cancel it to prevent automatic restart during the test.	3
Extra AT cmd	Manually add items that are automatically executed when AT dials.	empty

Standard Wireless Router Mode

- **Dynamic Internet Access**



WAN Setup

Connection Type	DHCP (Auto config)	
MTU	1500	(576~1500)
Primary DNS Server		(Optional)
Secondary DNS Server		(Optional)
Hostname		(Optional)

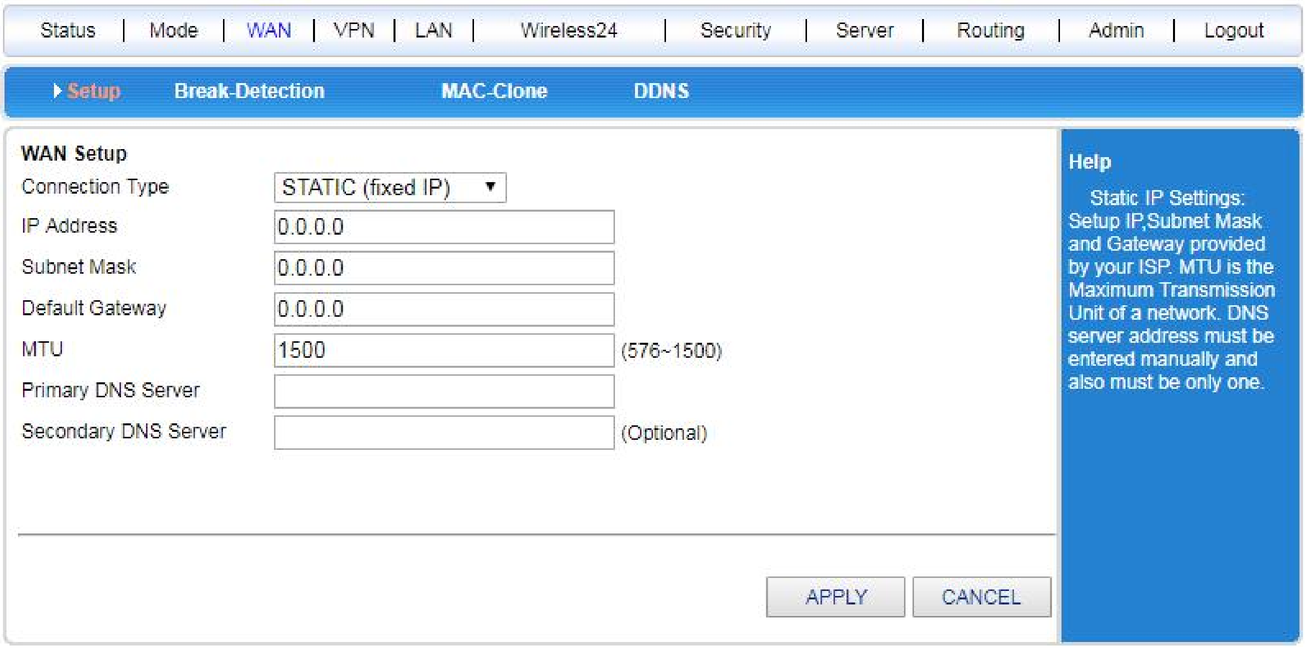
Help

WAN Setup: MTU is the Maximum Transmission Unit of a network. You can setup DNS server address to obtain it manually or the one provided by ISP.

Copyright 2013-2018.All right reserved

Dynamic Address@WAN Setting		
Item	**Description**	**Default**
Connection Type	Including: DHCP, Fixed IP, PPPOE	DHCP
MTU	Maximum Transmission Unit,is the largest unit of data that can be transmitted in a certain physical network.Range is 576～1500,unit is bite,default is 1500,recommend to keep the default value.	1500
Primary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty
Secondary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty
Host name	Optional, the device name of the PWR series seen by other devices on the network is empty by default.	empty

When the connection type is selected as "static IP", the interface is as follows:



WAN Setup

Connection Type	STATIC (fixed IP)	
IP Address	0.0.0.0	
Subnet Mask	0.0.0.0	
Default Gateway	0.0.0.0	
MTU	1500	(576~1500)
Primary DNS Server		
Secondary DNS Server		(Optional)

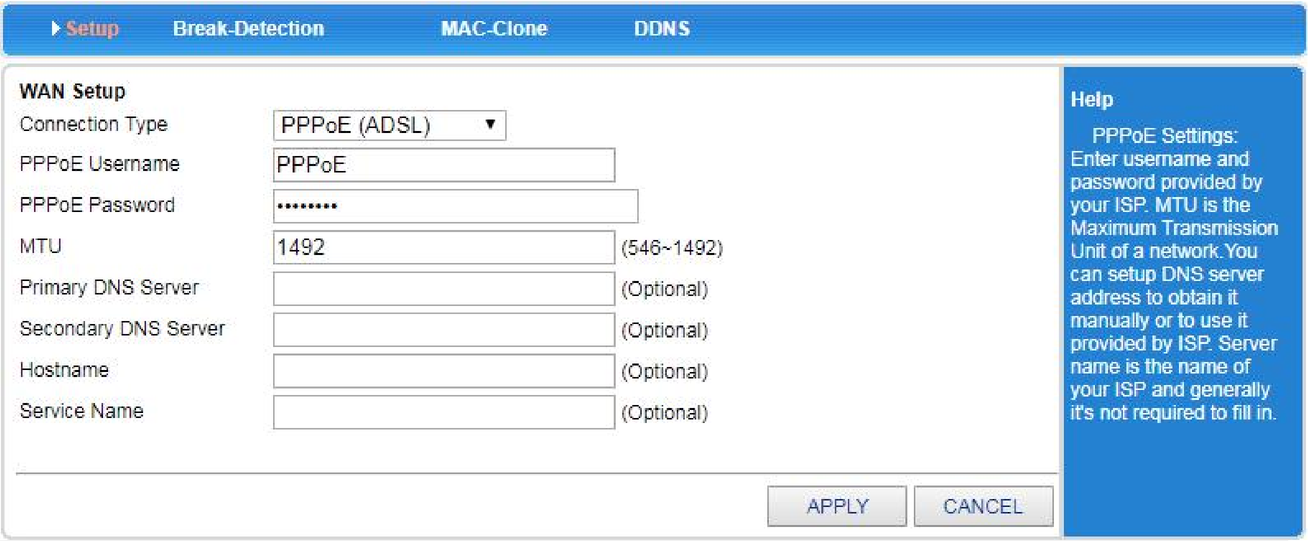
Help

Static IP Settings: Setup IP,Subnet Mask and Gateway provided by your ISP. MTU is the Maximum Transmission Unit of a network. DNS server address must be entered manually and also must be only one.

Static address@WAN Setting		
Item	**Description**	**Default**
Connection Type	Static address	DHCP
IP address	Provided by the ISP. LAN customization.	0.0.0.0
Subnet Mask	Provided by the ISP. LAN customization.	0.0.0.0
Default Gateway	Provided by the ISP. LAN customization.	0.0.0.0

MTU	Maximum Transmission Unit,is the largest unit of data that can be transmitted in a certain physical network.Range is 576～1500,unit is bite,default is 1500,recommend to keep the default value.	1500
Primary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty
Secondary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty

When the type is selected as “PPPOE”, the interface is as follows:



WAN Setup

Connection Type: PPPoE (ADSL)
PPPoE Username: PPPoE
PPPoE Password: ••••••••
MTU: 1492 (546~1492)
Primary DNS Server: (Optional)
Secondary DNS Server: (Optional)
Hostname: (Optional)
Service Name: (Optional)

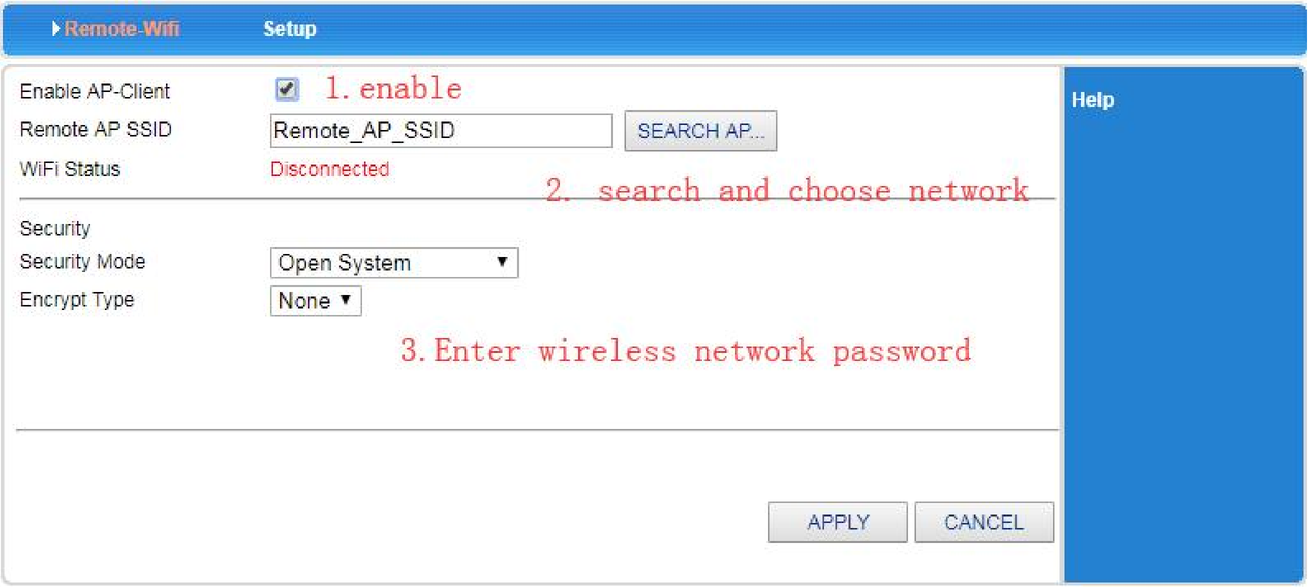
Help

PPPoE Settings: Enter username and password provided by your ISP. MTU is the Maximum Transmission Unit of a network.You can setup DNS server address to obtain it manually or to use it provided by ISP. Server name is the name of your ISP and generally it's not required to fill in.

PPPOE @WAN Setting		
Item	**Description**	**Default**
Connection Type	PPPoE	DHCP
PPPoE Username	Provided by the ISP	empty
PPPoE Password	Provided by the ISP	empty
MTU	Maximum Transmission Unit,is the largest unit of data that can be transmitted in a certain physical network.Range is 546～1492,unit is bite,default is 1492,recommend to keep the default value.	1492
Primary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty
Secondary DNS Server	Optional, provided by the local ISP operator, or you can set it yourself.	empty
Host Name	Optional, Enter the name of the PPPoE server provided by the ISP, which is not required by the ISP.	empty
Service Name	Optional, Enter the name of the PPPoE server provided by the ISP, which is not required by the ISP.	empty

Wireless AP+Client Bridge Mode

We can use the router as a bridge AP to bridge the previous level of the wireless router. Connect to the LAN interface through the network cable, enter the router <work mode>, and select the wireless AP + client mode.



Enable AP-Client ☑ 1. enable

Remote AP SSID: Remote_AP_SSID

WiFi Status: Disconnected

2. search and choose network

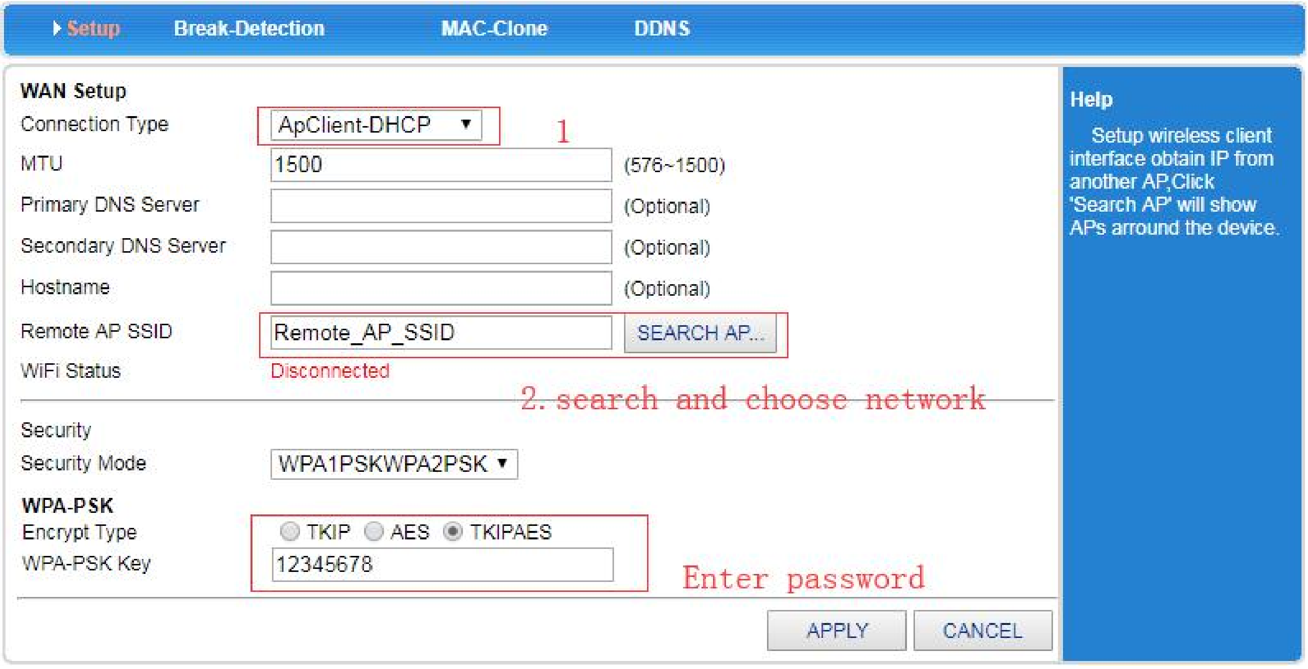
Security

Security Mode: Open System

Encrypt Type: None

3. Enter wireless network password

Wireless AP Client Mode



WAN Setup

Connection Type: ApClient-DHCP 1

MTU: 1500 (576~1500)

Primary DNS Server: (Optional)

Secondary DNS Server: (Optional)

Hostname: (Optional)

Remote AP SSID: Remote_AP_SSID

WiFi Status: Disconnected

2. search and choose network

Security

Security Mode: WPA1PSKWPA2PSK

WPA-PSK

Encrypt Type: ○ TKIP ○ AES ● TKIPAES

WPA-PSK Key: 12345678

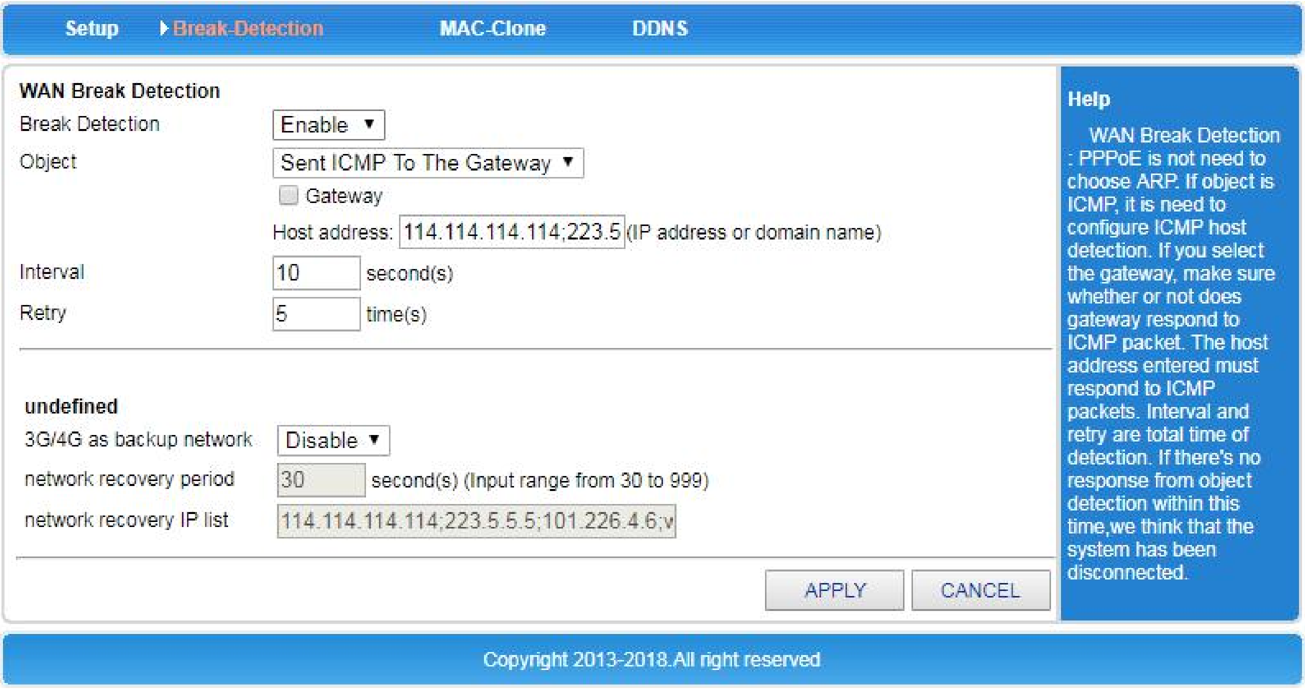
Enter password

Setup wireless client interface obtain IP from another AP,Click 'Search AP' will show APs arround the device.

5.3.2 Break Detection

WAN Break Detection:

Interval how many times to detect WAN network status and the allowed re-connection times.



Setup | ▸Break-Detection | MAC-Clone | DDNS

WAN Break Detection

Break Detection: Enable ▾

Object: Sent ICMP To The Gateway ▾

□ Gateway

Host address: 114.114.114.114;223.5 (IP address or domain name)

Interval: 10 second(s)

Retry: 5 time(s)

undefined

3G/4G as backup network: Disable ▾

network recovery period: 30 second(s) (Input range from 30 to 999)

network recovery IP list: 114.114.114.114;223.5.5.5;101.226.4.6;v

APPLY | CANCEL

Help

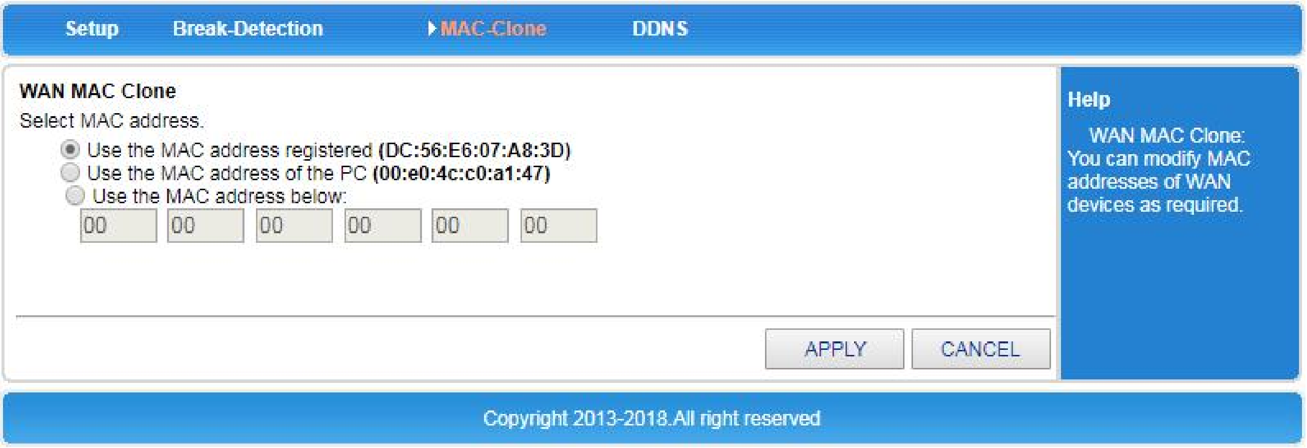
WAN Break Detection : PPPoE is not need to choose ARP. If object is ICMP, it is need to configure ICMP host detection. If you select the gateway, make sure whether or not does gateway respond to ICMP packet. The host address entered must respond to ICMP packets. Interval and retry are total time of detection. If there's no response from object detection within this time,we think that the system has been disconnected.

Copyright 2013-2018.All right reserved

5.3.3 WAN MAC Clone

Each interface (LAN, WAN port) has a default MAC address. In general, there is no need to change it.

Some ISPs require that only the registered MAC address can access the Internet. In this case, you should select "Use the manually entered MAC address below" to change the MAC address to the MAC address specified by the ISP. The setup interface is shown below.



Setup | Break-Detection | ▸MAC-Clone | DDNS

WAN MAC Clone

Select MAC address.

● Use the MAC address registered **(DC:56:E6:07:A8:3D)**

○ Use the MAC address of the PC **(00:e0:4c:c0:a1:47)**

○ Use the MAC address below:

00 | 00 | 00 | 00 | 00 | 00

APPLY | CANCEL

Help

WAN MAC Clone: You can modify MAC addresses of WAN devices as required.

Copyright 2013-2018.All right reserved

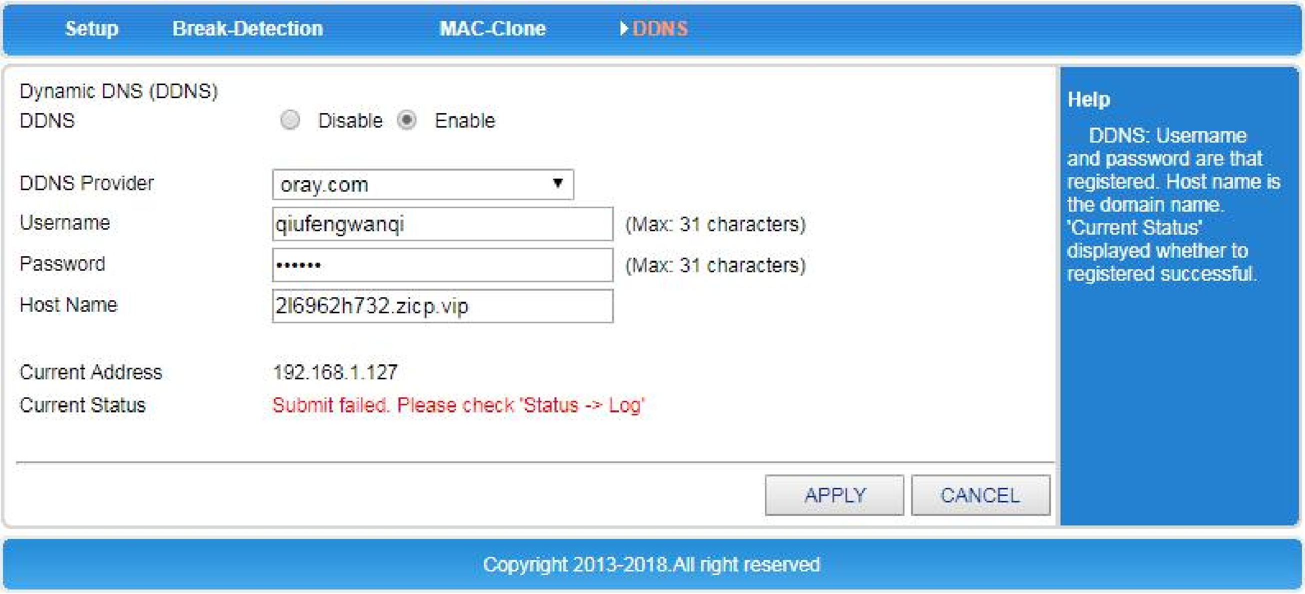
5.3.4 Dynamic Domain Name

Since the IP address obtained is not fixed when accessing the Internet through the PPPoE address, this brings great inconvenience to Internet users who want to access the LAN server.

DDNS (Dynamic Domain Name Service) can solve this problem,The router will establish a relationship table between the IP and the domain name (which needs to be pre-registered) on the DDNS server. When the IP address of the WAN port changes.The router automatically initiates an update request to the specified DDNS server. The DDNS server updates the mapping between the domain name and the IP address. Regardless of how the IP address of the router's WAN port changes, users on the Internet can still access it through the domain name.

[Example]:

If you have already registered the domain name gg.3322.org on www.3322.org, the method for establishing a dynamic correspondence between the domain name and the router's WAN port IP address is as follows:



Dynamic DNS (DDNS)

DDNS	○ Disable ● Enable	
DDNS Provider	oray.com	
Username	qiufengwanqi	(Max: 31 characters)
Password	••••••	(Max: 31 characters)
Host Name	2l6962h732.zicp.vip	
Current Address	192.168.1.127	
Current Status	Submit failed. Please check 'Status -> Log'	

Help

DDNS: Username and password are that registered. Host name is the domain name. 'Current Status' displayed whether to registered successful.

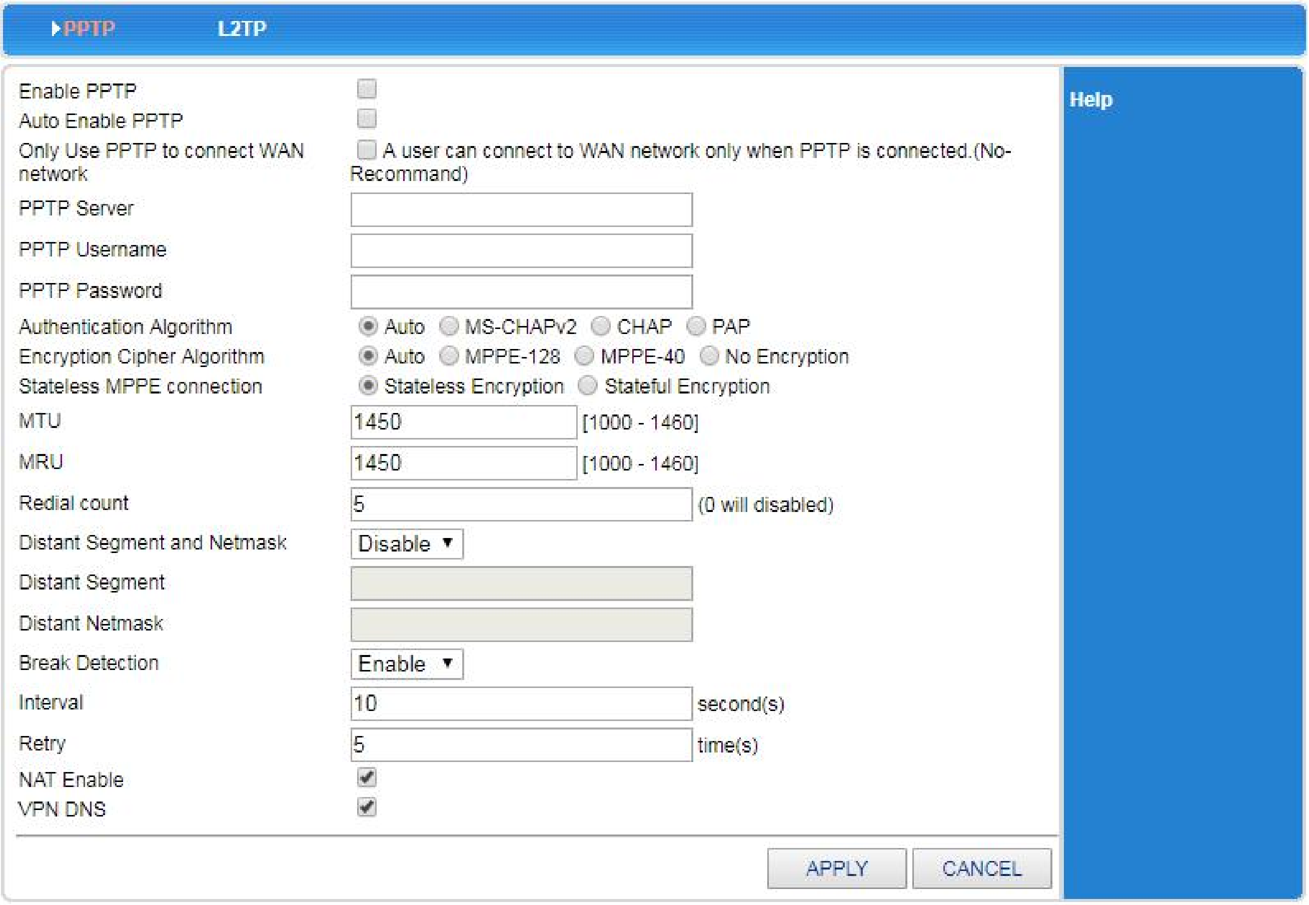
The status shows whether the connection is successful. Only the status displayed “Connected”, and the DDNS function starts normally.

5.4 *VPN Setting*

In <VPN Settings> you can set:

- PPTP settings
- L2TP settings

5.4.1 PPTP

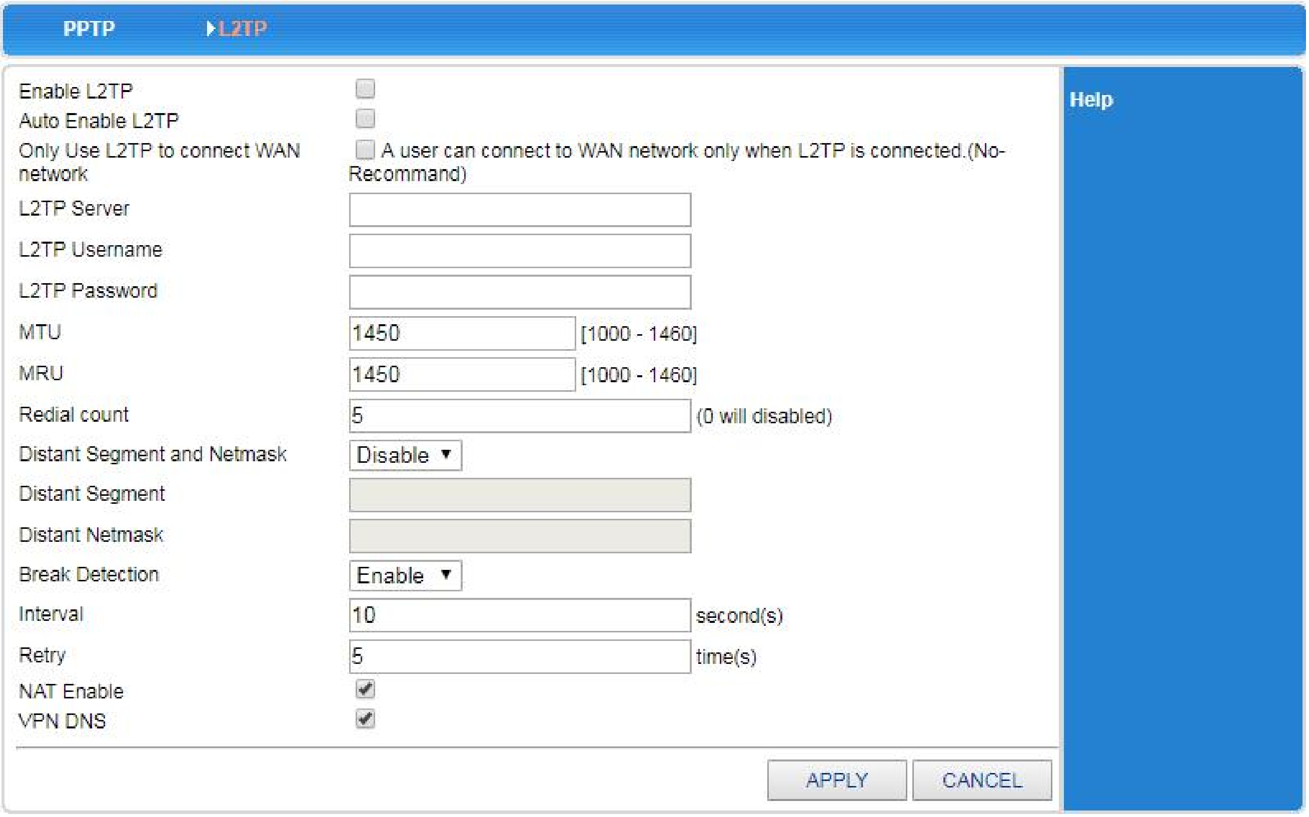


Enable PPTP	□	
Auto Enable PPTP	□	
Only Use PPTP to connect WAN network	□ A user can connect to WAN network only when PPTP is connected.(No-Recommand)	
PPTP Server		
PPTP Username		
PPTP Password		
Authentication Algorithm	● Auto ○ MS-CHAPv2 ○ CHAP ○ PAP	
Encryption Cipher Algorithm	● Auto ○ MPPE-128 ○ MPPE-40 ○ No Encryption	
Stateless MPPE connection	● Stateless Encryption ○ Stateful Encryption	
MTU	1450	[1000 - 1460]
MRU	1450	[1000 - 1460]
Redial count	5	(0 will disabled)
Distant Segment and Netmask	Disable	
Distant Segment		
Distant Netmask		
Break Detection	Enable	
Interval	10	second(s)
Retry	5	time(s)
NAT Enable	☑	
VPN DNS	☑	

PPTP@VPN Setting

Item	Description	Default
Enable PPTP	Enable PPTP function	x
Auto Enable PPTP	Automatically dial the VPN when the WAN port is connected.	x
Only use PPTP to connect WAN network	All data transmit via VPN gateway, with "VPN NAT" you can use port forwarding \DMZ	x
PPTP Server	Enter required	empty
PPTP Username	Enter required	empty
PPTP Password	Enter required	empty
MTU,MRU	Default 1450,Not recommended to change	1450
Distant Segment and Netmask	For Access VPN subnet	1450
Break Detection	Ping to detect the VPN server. If the server prohibits ping, disable this item.	open
VPN NAT	for"only use PPTP to connect to the external network" use port forwarding \DMZ	√
VPN DNS	PPTP use VPN server DNS	√

5.4.2 L2TP



Enable L2TP	□	
Auto Enable L2TP	□	
Only Use L2TP to connect WAN network	□ A user can connect to WAN network only when L2TP is connected.(No-Recommand)	
L2TP Server		
L2TP Username		
L2TP Password		
MTU	1450	[1000 - 1460]
MRU	1450	[1000 - 1460]
Redial count	5	(0 will disabled)
Distant Segment and Netmask	Disable ▾	
Distant Segment		
Distant Netmask		
Break Detection	Enable ▾	
Interval	10	second(s)
Retry	5	time(s)
NAT Enable	☑	
VPN DNS	☑	

L2TP@VPN Setting		
Item	**Description**	**Default**
Enable L2TP	Enable L2TP function	Untick
Auto Enable L2TP	Automatically dial the VPN when the WAN port is connected.	Untick
Only use L2TP to connect WAN network	All data pass the VPN gateway, work with "VPN NAT" you can use port forwarding\DMZ	Untick
L2TP Server	Required	empty

L2TP Username	Required	empty
L2TP Password	Required	empty
MTU,MRU	Default is 1450,Not recommended to change	1450
Distant Segment	Access VPN subnet	1450
Break Detection	Ping to detect the VPN server. If the server prohibits ping, disable this item.	enable
VPN NAT	work with "Only use L2TP to connect WAN network" you can use port forwarding\DMZ	ticked
VPN DNS	L2TP uses the DNS of the VPN server	ticked

5.5 LAN Setting

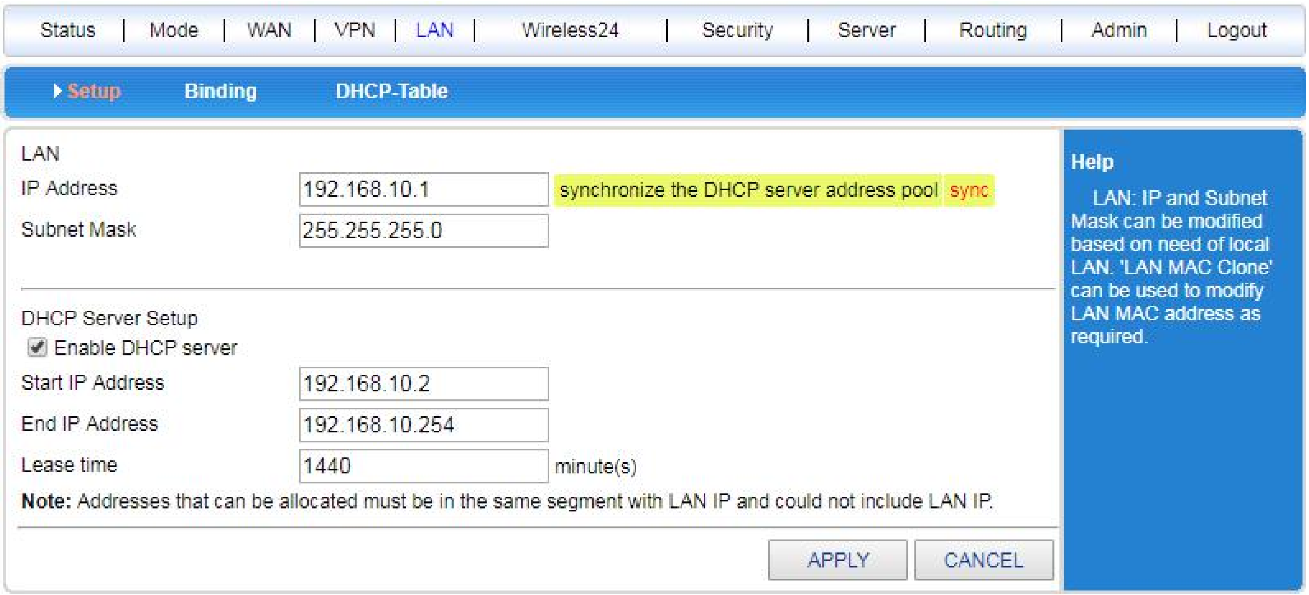
You can set:

- LAN basic settings
- IP&MAC address binding
- DHCP allocation status table

5.5.1 Basic Setting

LAN Setting

Computers on the LAN can manage the router through the LAN port IP address. As shown below:


Status | Mode | WAN | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
▸Setup
Binding
DHCP-Table
APPLY
CANCEL

LAN

IP Address 192.168.10.1 synchronize the DHCP server address pool sync

Subnet Mask 255.255.255.0

DHCP Server Setup

☑ Enable DHCP server

Start IP Address 192.168.10.2

End IP Address 192.168.10.254

Lease time 1440 minute(s)

Note: Addresses that can be allocated must be in the same segment with LAN IP and could not include LAN IP.

Help

LAN: IP and Subnet Mask can be modified based on need of local LAN. 'LAN MAC Clone' can be used to modify LAN MAC address as required.

Note: After modifying the IP address of the LAN port, you need to log in again to the new device address to continue accessing the router web interface.

LAN Setting @ Basic Setting		
Item	**Description**	**Default**
IP address	LAN port IP address. You can access the router web interface through this IP address.	192.168.10.1
Subnet mask	Subnet mask corresponding to the IP address of the LAN port	255.255.255.0

Synchronize the DHCP address pool	Default IP is 192.168.10.1,If you change to 192.168.12.1, click on the synchronous address pool, the address that can be assigned automatically changes to: 192.168.12.2-192.168.12.254	--

DHCP Server Setting

The router can act as a DHCP server to assign IP addresses to computers on the LAN.

Router's DHCP server IP address allocation mechanism:

• When the router receives a request from the DHCP client to obtain an IP address, first check the IP/MAC binding relationship table (set the path: LAN Settings→IP/MAC Binding, refer to "6.2 IP/MAC Address Binding" for details). If the computer is in the IP/MAC binding table, the corresponding IP address is assigned to the computer.

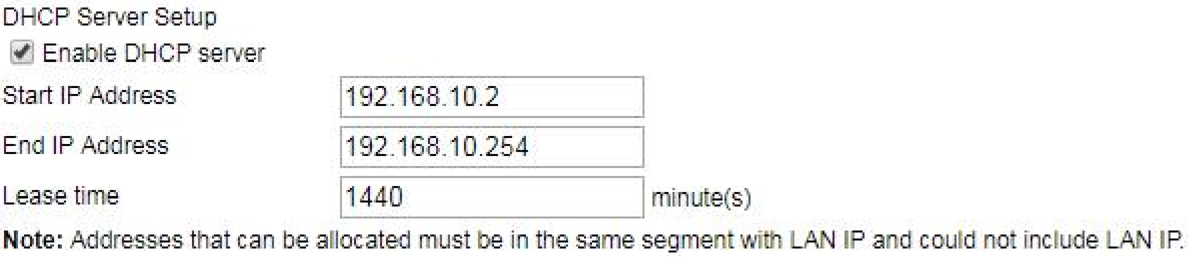
• If the computer requesting the IP address is not in the IP/MAC binding table, the router will select an IP address from the address pool that is not used in the LAN to be assigned to the computer.

• If the computer is offline (such as a shutdown), the router will not immediately assign the IP address previously assigned to it, Assign it out only if there are no other assignable IP addresses in the address pool and the lease of the offline computer IP address expires.

• If there are no assignable IP addresses in the address pool, the computer cannot get an IP address.

[Example]

Assuming the address pool range is 192.168.10.190 to 192.168.10.200, computer A sets the IP/MAC address binding, and the bound IP address is 192.168.10.210, Computer B does not set IP/MAC address binding. In this case, computer A is assigned the IP address 192.168.10.210. Computer B is assigned an IP address in the range of the address pool, such as 192.168.10.2.



DHCP Server Setup

☑ Enable DHCP server

Start IP Address: 192.168.10.2

End IP Address: 192.168.10.254

Lease time: 1440 minute(s)

Note: Addresses that can be allocated must be in the same segment with LAN IP and could not include LAN IP.

DHCP@Basic Setting		
Item	**Description**	**Default**
Enable DHCP Server	Choose this item to enable the DHCP function of PWR ,or disable it	enable
Start IP Address	The starting address of the DHCP server address pool must be in the same subnet as the LAN port.	192.168.10.2
End IP Address	The end address of the DHCP server address pool must be in the same subnet as the LAN port. The address pool end address must be greater than the address pool start address.	192.168.10.254
Lease time	Enter the lease time for assigning an IP address to the computer. After the lease time expires, the computer must re-apply to PWR once.(The computer will automatically apply). The unit is minutes.	1440

Note: If the IP address of the router LAN port is set between the DHCP start address and the end address, the router will automatically set the DHCP-assignable IP start address to the last address of the router LAN port IP address. A resulting address to avoid conflicts between the router address and the IP address assigned to the PC in the LAN.

5.5.2 IP&MAC Address Binding

<IP&MAC Binding> enabled with 3 functions:

- The DHCP server assigns an IP address based on the added IP&MAC.
- Set the static ARP cache in the ARP table of the router to prevent the ARP virus from modifying the ARP table.
- Strictly control users to modify IP or MAC addresses, control users' online behavior, and prevent DDoS attacks.

Description:

- Supports up to 254 IP/MAC binding entries, and the number supported by each model is different.
- By default, no IP/MAC address binding is done.

The IP/MAC binding function can be implemented in three ways:

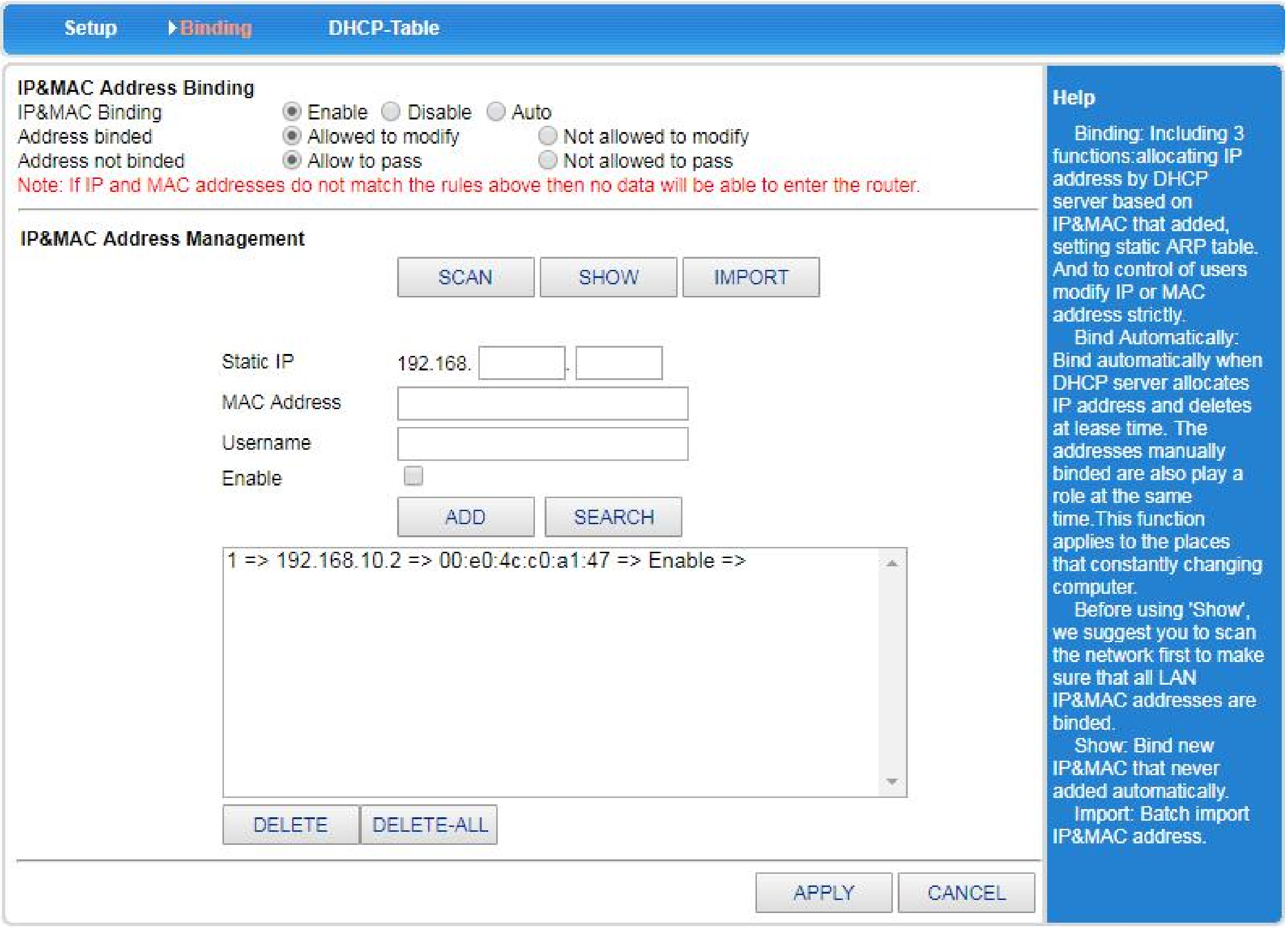
- Manually configured one by one,Click the <Add to List> button in the figure below to add the settings to the IP/MAC binding table.
- Support one-click binding function. When the network is stable and all computers are online, click the <SHOW> button to automatically bind the IP&MAC that has not been added and import it into the IP/MAC binding table.
- Write the file in the format ".cfg" first, then click the <Import> button to import.

Note: The format of the .cfg file is "MAC Address - IP Address - Username

[Example]

00:00:e8:f5:6e:3a -192.168.10.22- host

00:00:00:00:11:11- 192.168.10.111- host 1



IP&MAC Address Binding

IP&MAC Binding ● Enable ○ Disable ○ Auto

Address binded ● Allowed to modify ○ Not allowed to modify

Address not binded ● Allow to pass ○ Not allowed to pass

Note: If IP and MAC addresses do not match the rules above then no data will be able to enter the router.

IP&MAC Address Management

Static IP 192.168. ___ . ___

MAC Address

Username

Enable □

1 => 192.168.10.2 => 00:e0:4c:c0:a1:47 => Enable =>

Help

Binding: Including 3 functions:allocating IP address by DHCP server based on IP&MAC that added, setting static ARP table. And to control of users modify IP or MAC address strictly.

Bind Automatically: Bind automatically when DHCP server allocates IP address and deletes at lease time. The addresses manually binded are also play a role at the same time.This function applies to the places that constantly changing computer.

Before using 'Show', we suggest you to scan the network first to make sure that all LAN IP&MAC addresses are binded.

Show: Bind new IP&MAC that never added automatically.

Import: Batch import IP&MAC address.

IP&MAC Bind		
Item	**Description**	**Default**
IP&MAC Address Binding	Only after click<enable> can set the following related items,Click <Disable> and the router IP&MAC address binding function will be invalid.	enable
Address binded	If click <Not allowed to Modify >, the IP address corresponding to the bound MAC address cannot be modified. If it is changed, it cannot pass through the router.	Allowed to modify
Address not binded	Enable <Allow to Pass>, the unbound MAC address can pass through the router through the IP address of the LAN port segment.Conversely, if the "Not allow to Pass" is activated, the unbound IP&MAC address cannot pass through the router.	Allow to pass
Static IP	Enter the IP address of computer. The IP address may not be in the address pool assigned by the router's DHCP server, but it must be on the same subnet as the LAN port IP address.	empty
MAC address	Enter the computer MAC address	empty
Username	Enter the computer name which the IP and MAC addresses are bound.	empty
SHOW	Click this button, the router will automatically scan all the IP in the LAN, and bind the unbound MAC address to the IP&MAC address. Note：This method is suitable for network stability and all computers are online, can obtain computer IP/MAC binding entries in the LAN easily. However, in this way, some ARP cache tables are missing information about the computer due to aging of ARP entries, that is, these IP/MAC addresses are not bound. After setting this method, it is recommended to check whether the computer you want to bind is in the binding list. If not, add it manually.	--
IMPORT	Click this button to select the ARP entry to be bound. Click <OK> to import the IP/MAC binding table at the bottom of the page.	--

[Example]

In an Internet cafe, because the computer in the LAN has a virus or other reasons, ARP attack packets keep attacking the router, causing the computer in the LAN to be abnormal. Hope to achieve the following requirements:

- The computer in the LAN dynamically obtains the IP address through DHCP;
- When the computer IP address is inconsistent with the set binding relationship table, the computer cannot access the Internet, thus preventing the Internet user from modifying the IP address of the computer at random;
- External computers (such as laptops that come with users) do not have access to the Internet;
- ARP attacks on the LAN do not affect computers on the LAN from accessing the Internet.

Setting Step

Step1: Enable the router's DHCP server function (LAN Settings → Basic Settings → DHCP Server Settings), set the IP address pool range, such as 192.168.10.2 to 192.168.10.254, so that the computer in the LAN dynamically obtains the IP address. (The computer must be set to automatically obtain an IP address).

Step2: Set the IP/MAC binding relationship table to set the mapping between the IP address and MAC address of all computers on the LAN to the list. (Also refer to the "SHOW" in the above table to help the IP address of all computers in the LAN with the corresponding MAC address).

Step3: Tick <Address Binded> → <Not allowed to Modify>.

Step4: Tick < Address not binded> → <Not allowed to pass>.

Step5: Click the <APPLY> button and the configuration is complete.

5.5.3 DHCP table

From this table you can see a list of all IP addresses that the DHCP server has assigned.

5.6 Media Setting

Reserved function and is disable now.

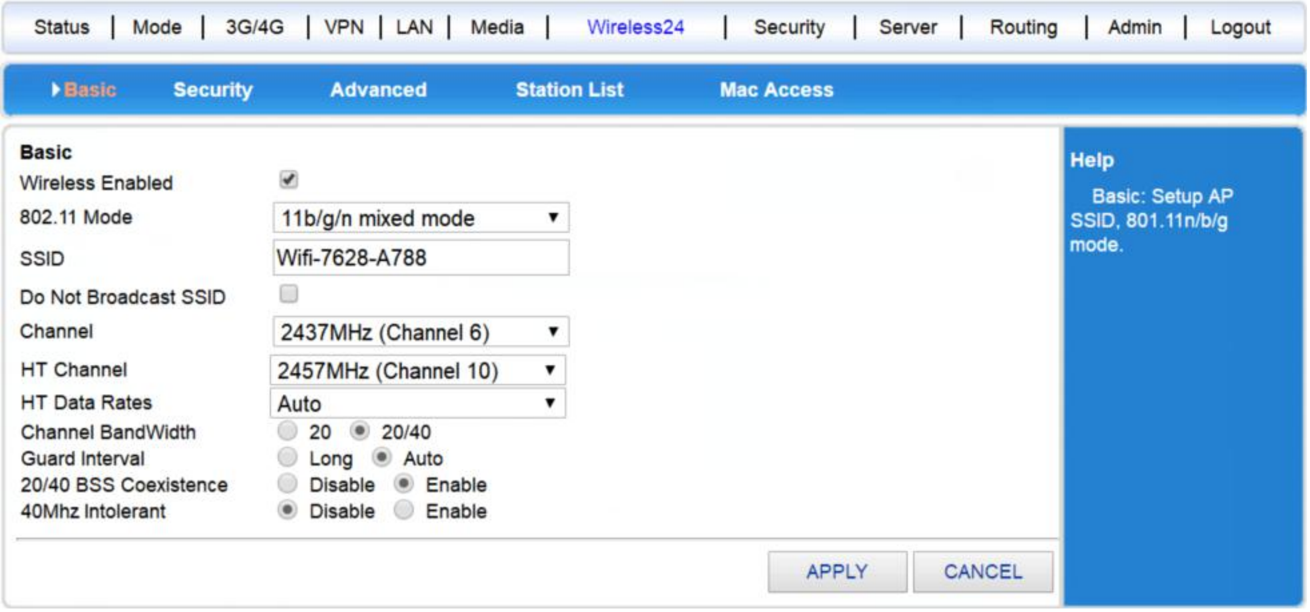
5.7 Wireless 2.4G

In <Wireless Settings>, you can set it below:

- Basic setting
- Security
- Advanced
- Station list
- MAC Access

5.7.1 Basic Setting

Set the basic information of the wireless connection. On this page, you can enable or disable the wireless function , broadcast and disable the broadcast SSID, set the SSID name, etc.


Status | Mode | 3G/4G | VPN | LAN | Media | Wireless24 | Security | Server | Routing | Admin | Logout
▸Basic Security Advanced Station List Mac Access
APPLY
CANCEL

Basic

Wireless Enabled	☑
802.11 Mode	11b/g/n mixed mode ▼
SSID	Wifi-7628-A788
Do Not Broadcast SSID	□
Channel	2437MHz (Channel 6) ▼
HT Channel	2457MHz (Channel 10) ▼
HT Data Rates	Auto ▼
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Auto
20/40 BSS Coexistence	○ Disable ● Enable
40Mhz Intolerant	● Disable ○ Enable

Help

Basic: Setup AP SSID, 801.11n/b/g mode.

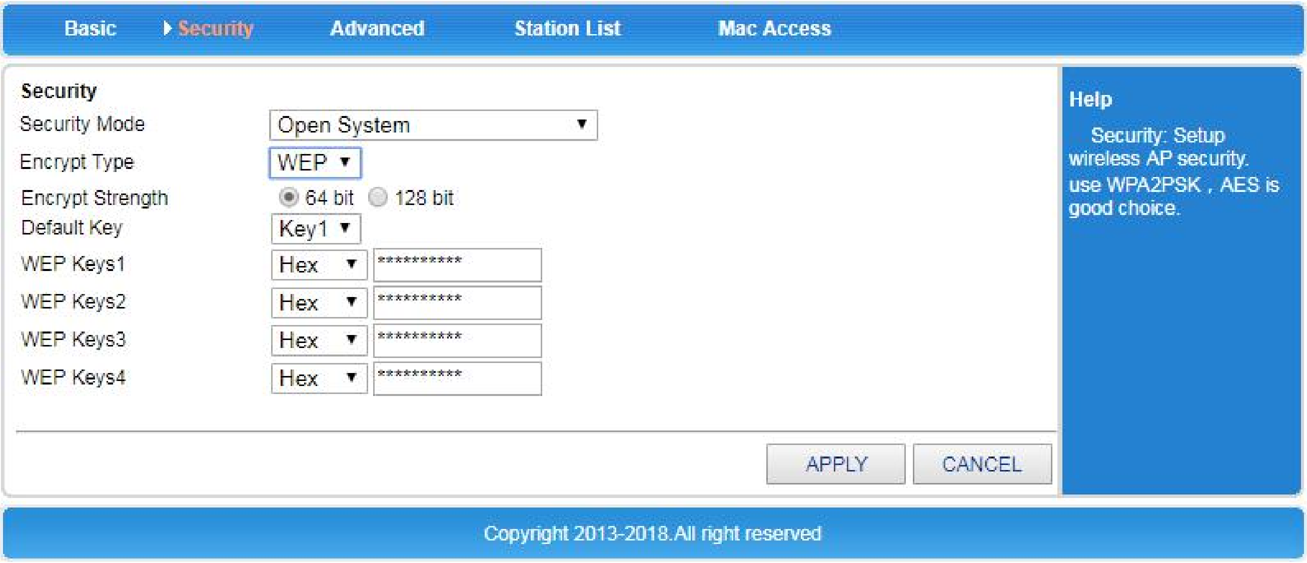
5.7.2 Security

There are several types of wireless security modes, and you can select different security modes as needed.

- Disable
- Open System
- WPA-PSK
- WPA2-PSK
- WPA-PSK/WPA2-PSK (WPA-PSK and WPA2-PSK mixed mode)

Open System

In this security mode, the encryption types are: None and WEP.



Security

Security Mode: Open System

Encrypt Type: WEP

Encrypt Strength: ● 64 bit ○ 128 bit

Default Key: Key1

WEP Keys1: Hex **********

WEP Keys2: Hex **********

WEP Keys3: Hex **********

WEP Keys4: Hex **********

Help

Security: Setup wireless AP security. use WPA2PSK , AES is good choice.

Open System @ Security		
Item	**Description**	**Default**
Encrypt type	Two encryption types are optional: None and WEP,None is Not encrypted	None
Encryption Strength	Two encryption length are optional:64bit,128bit.	64bit
Default Key	You can set up 4 keys at the same time, but only 1 key can be selected for use at the moment. This item is to select the key to be used currently.	Key 1
WEP Key	You can choose key type and set the key. There are two key types to choose: hexadecimal and character. Set different keys according to different encryption lengths and key types.	--

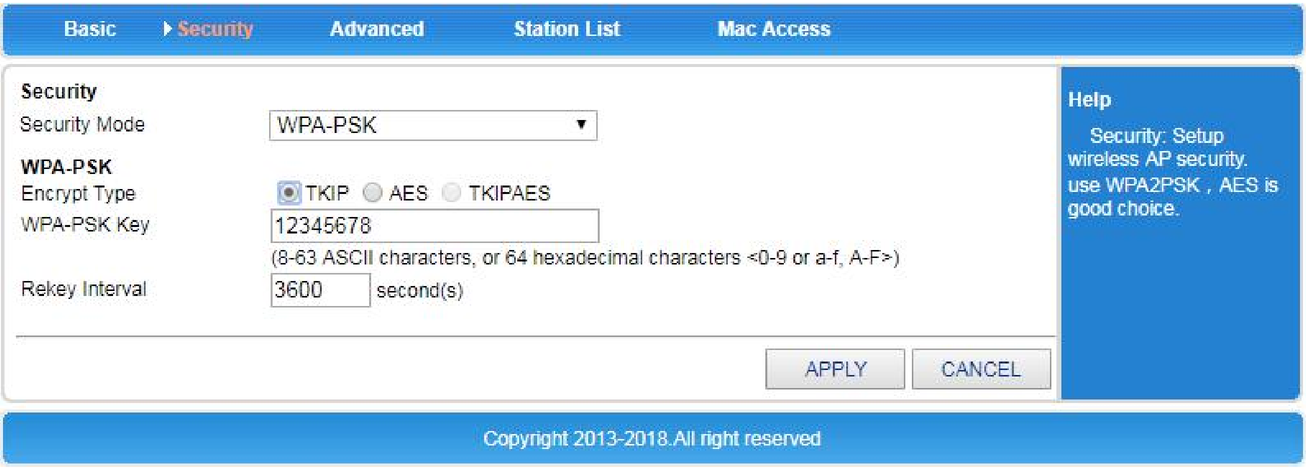
Key Setting:

64bit encrypt: 10-digit hexadecimal or 5-digit character.

128bit encrypt: 26-digit hexadecimal or 13-bit character.

WPA-PSK

This security mode is WPA-PSK encryption mode.



Security

Security Mode: WPA-PSK

WPA-PSK

Encrypt Type: ● TKIP ○ AES ○ TKIPAES

WPA-PSK Key: 12345678

(8-63 ASCII characters, or 64 hexadecimal characters <0-9 or a-f, A-F>)

Rekey Interval: 3600 second(s)

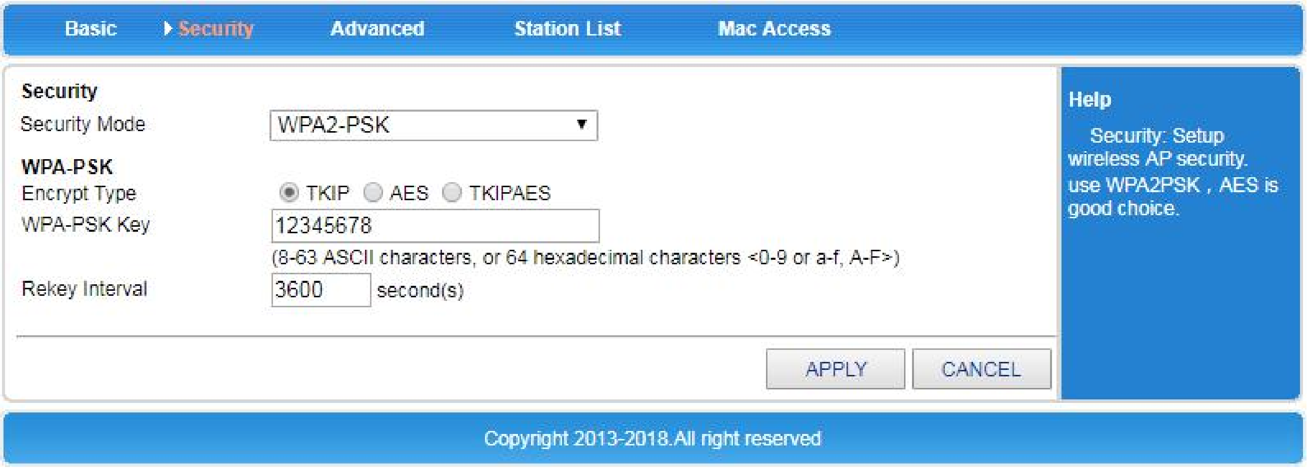
Help

Security: Setup wireless AP security. use WPA2PSK , AES is good choice.

WAP-PSK @ Security		
Item	**Description**	**Default**

Security Mode	WPA-PSK	--
Encrypt Type	TKIP,AES.	--
WPA-PSK Key	Set the key. The legal key length is 8-63 ASCII characters or 64 hexadecimal numbers (0~9, a~f or A~F).	--
Key Interval	Set key update interval time,unit is second	3600

WPA2-PSK



Security

Security Mode: WPA2-PSK

WPA-PSK

Encrypt Type: ● TKIP ○ AES ○ TKIPAES

WPA-PSK Key: 12345678

(8-63 ASCII characters, or 64 hexadecimal characters <0-9 or a-f, A-F>)

Rekey Interval: 3600 second(s)

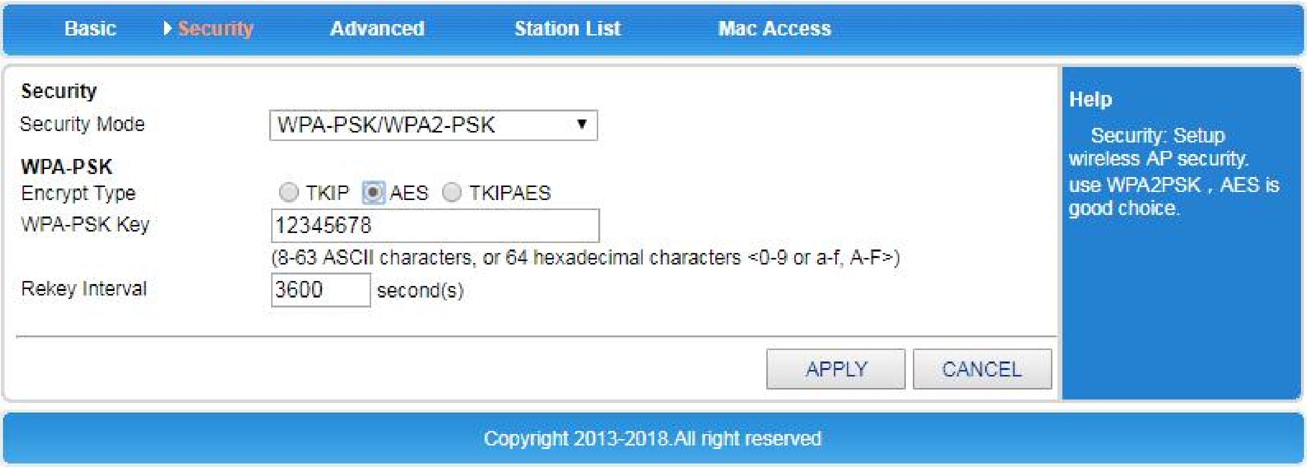
Help

Security: Setup wireless AP security. use WPA2PSK , AES is good choice.

Copyright 2013-2018.All right reserved

WAP2-PSK @Wireless Security		
Item	**Description**	**Default**
Security mode	WPA2-PSK。	--
Encrypt type	TKIP,AES.	--
WPA-PSK key	Set the key. The legal key length is 8-63 ASCII characters or 64 hexadecimal numbers (0~9, a~f or A~F).	--
Key Interval	Set key update interval time,unit is second	3600

WPA-PSK/WPA2-PSK



Security

Security Mode: WPA-PSK/WPA2-PSK

WPA-PSK

Encrypt Type: ○ TKIP ● AES ○ TKIPAES

WPA-PSK Key: 12345678

(8-63 ASCII characters, or 64 hexadecimal characters <0-9 or a-f, A-F>)

Rekey Interval: 3600 second(s)

Help

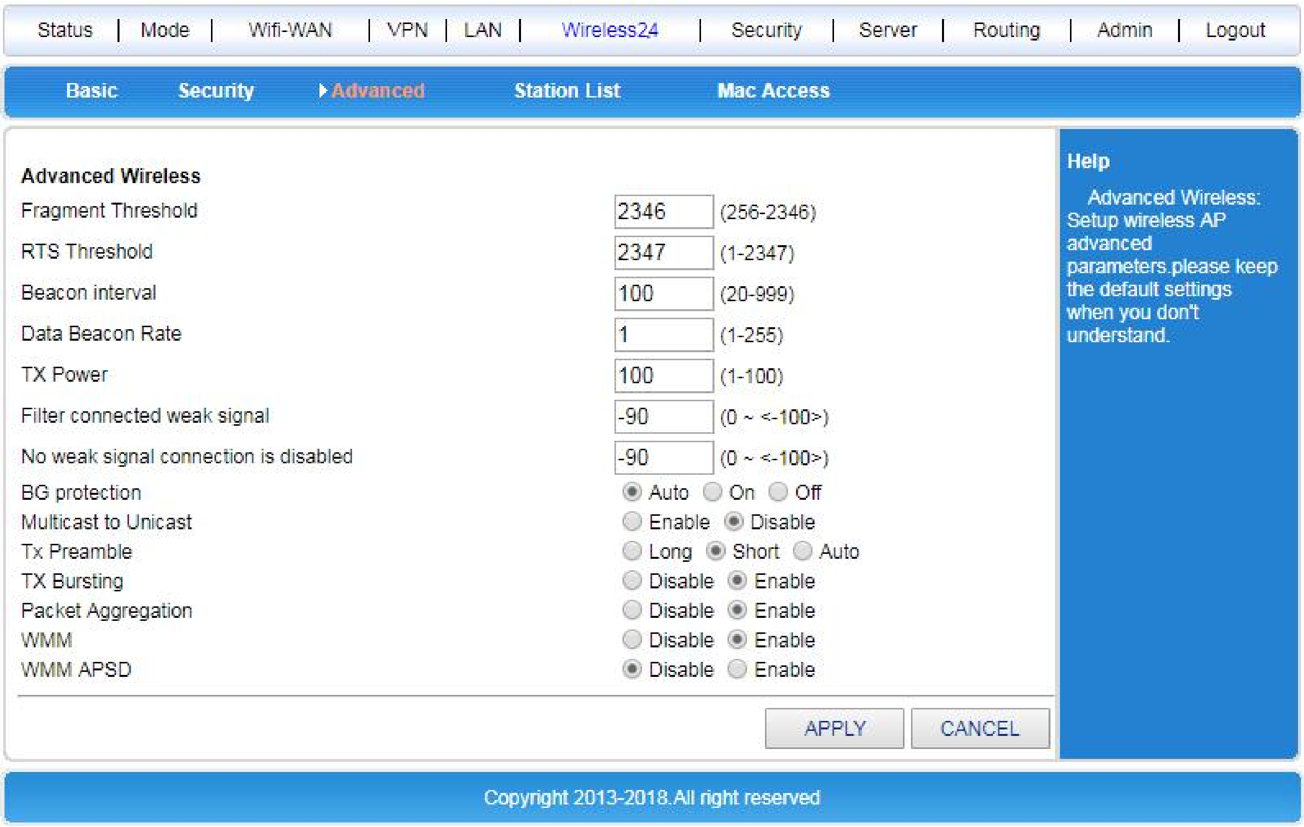
Security: Setup wireless AP security. use WPA2PSK , AES is good choice.

Copyright 2013-2018.All right reserved

WAP-PSK/WAP2-PSK @ Wireless Security		
Item	**Description**	**Default**
Security Mmode	WPA-PSK/WPA2-PSK	--

Encrypt Type	TKIP,AES	--
WPA-PSK key	Set the key. The legal key length is 8-63 ASCII characters or 64 hexadecimal numbers (0~9, a~f or A~F).	--
Key Interval	Set key update interval time,unit is second	3600

5 .7.3 Advanced


Status | Mode | Wifi-WAN | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Basic
Security
Advanced
Station List
Mac Access
APPLY
CANCEL
Copyright 2013-2018.All right reserved

Advanced Wireless

Fragment Threshold	2346	(256-2346)
RTS Threshold	2347	(1-2347)
Beacon interval	100	(20-999)
Data Beacon Rate	1	(1-255)
TX Power	100	(1-100)
Filter connected weak signal	-90	(0 ~ <-100>)
No weak signal connection is disabled	-90	(0 ~ <-100>)
BG protection	● Auto ○ On ○ Off	
Multicast to Unicast	○ Enable ● Disable	
Tx Preamble	○ Long ● Short ○ Auto	
TX Bursting	○ Disable ● Enable	
Packet Aggregation	○ Disable ● Enable	
WMM	○ Disable ● Enable	
WMM APSD	● Disable ○ Enable	

Help

Advanced Wireless: Setup wireless AP advanced parameters.please keep the default settings when you don't understand.

Advanced Settings		
Item	**Description**	**Default**
Fragment Threshold	Fragment transmission when the length of the message is greater than the set value. that is a message is split into several and sent in sequence.	2346
RTS Threshold	When the packet length exceeds the threshold, the AP sends an RTS packet to clear the channel to prevent interference.	2347
Beacon Interval	Set how long to send a beacon message	100
Data Beacon Rate	1	1
TX Power	1-100%	100
Signal connection limit	0-（-100）	-90

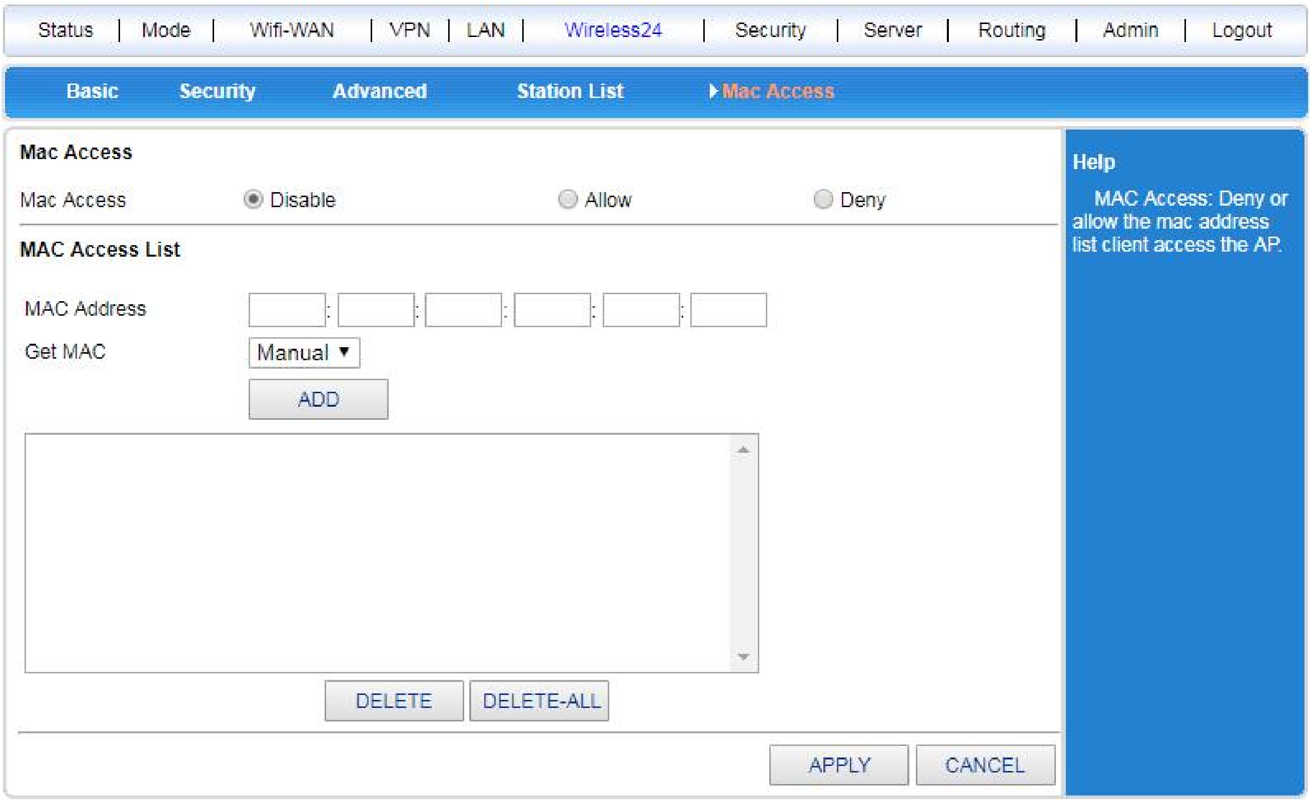
5.7.4 Station List

Can view the current wireless connection user information

5.7.5 MAC Access

MAC access can set the router's wireless white list and black list. If set to "Allow", only the MAC in the list can be connected to the wireless, and the others cannot access. If set to "Disable", the

MAC in the list cannot be connected to the wireless, and the others can.


Status | Mode | Wifi-WAN | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Basic
Security
Advanced
Station List
Mac Access
ADD
DELETE
DELETE-ALL
APPLY
CANCEL

Mac Access

Mac Access ● Disable ○ Allow ○ Deny

MAC Access List

MAC Address

Get MAC Manual

Help

MAC Access: Deny or allow the mac address list client access the AP.

MAC Access		
Item	**Description**	**Default**
Disable	Close MAC Access	Ticked
Allow	Only the MAC in the list can be connected, others can not.	untick
Deny	MAC in the list cannot be connected, others can	untick

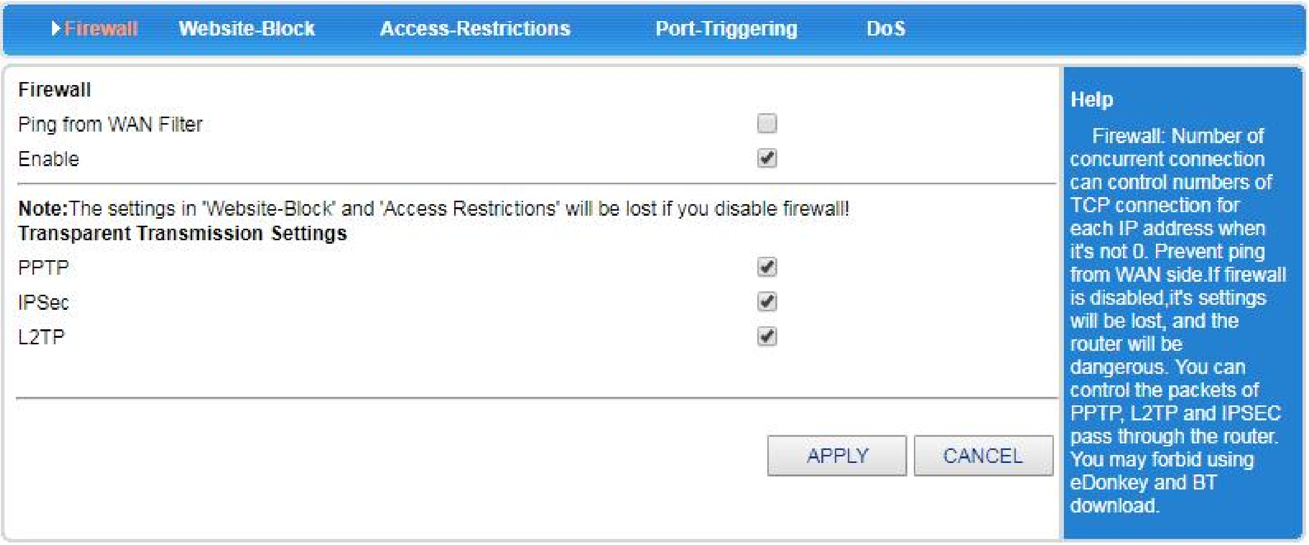
5.8 Security

Network security settings include: Firewall , Web-site Block, MAC Access,Access-Restrictions, Port-Triggering, and DOS .

5.8.1 Firewall Settings

When the firewall function is enabled, the Internet can prevent malicious attacks on the router or computers in the LAN, and ensure the safe operation of the router and the LAN computer. Especially for some open servers (such as virtual servers, DMZ hosts, etc.), enabling the router firewall function can block malicious attack sources and prevent DoS attacks.

In the firewall settings (the number of concurrent connections, if not 0), you can control the number of TCP connections per IP address to prevent PING behavior from the WAN side. If the firewall function is disabled, all firewall settings will be invalid and the router will be in danger.



Firewall

Ping from WAN Filter □

Enable ☑

Note: The settings in 'Website-Block' and 'Access Restrictions' will be lost if you disable firewall!

Transparent Transmission Settings

PPTP ☑

IPSec ☑

L2TP ☑

APPLY CANCEL

Help

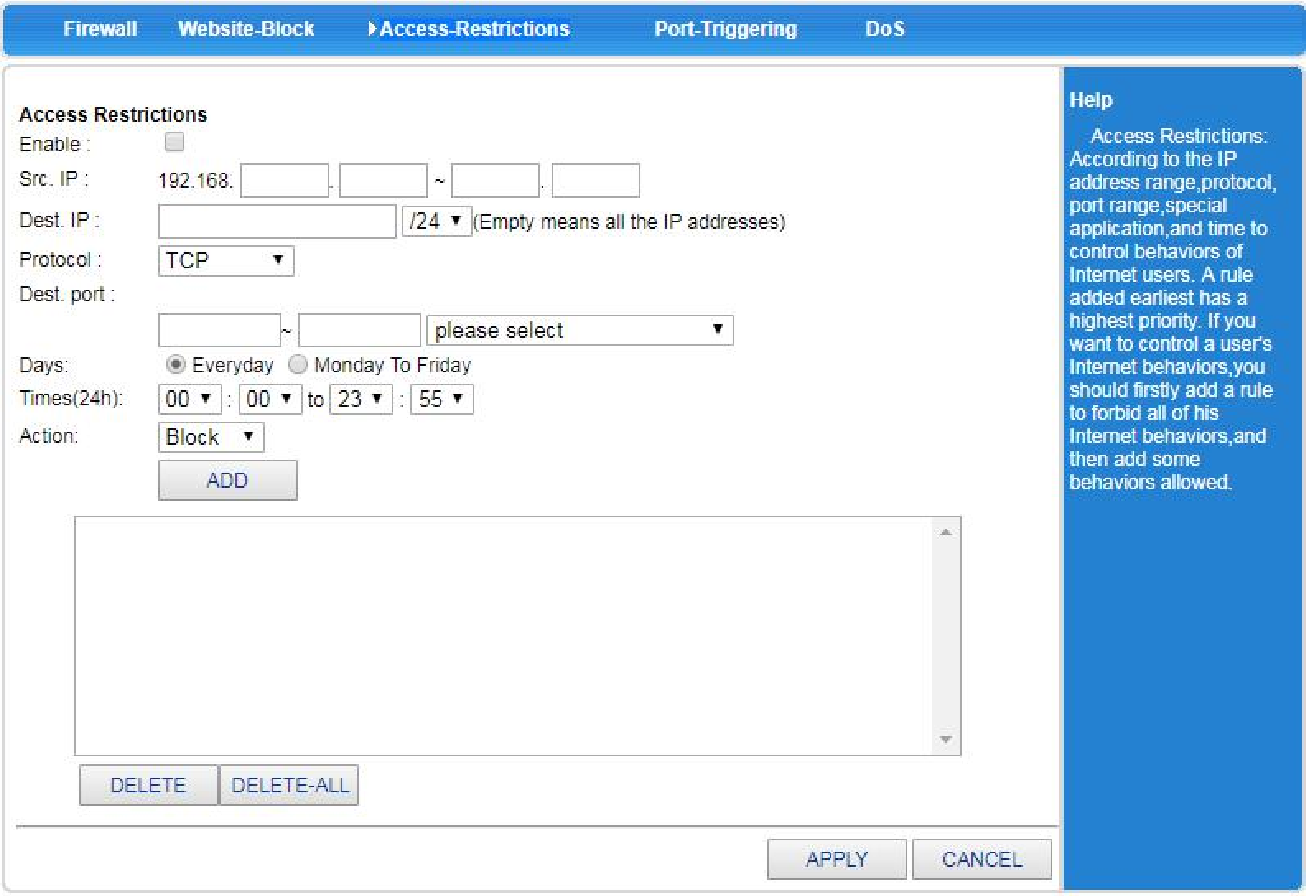
Firewall: Number of concurrent connection can control numbers of TCP connection for each IP address when it's not 0. Prevent ping from WAN side.If firewall is disabled,it's settings will be lost, and the router will be dangerous. You can control the packets of PPTP, L2TP and IPSEC pass through the router. You may forbid using eDonkey and BT download.

By setting, you can control whether PPTP, L2TP, IPSEC packets pass through the router, WAN port ping Prevention.

5.8.2 Access-Restrictions

In <Access-Restrictions>, you can control the computer in the LAN to access the Internet according to the source IP address, destination IP address, protocol type, destination port range, time period, and day of the week. You can also use the special application to access the LAN. Users control QQ, MSN and other online behaviors by time period ,It's easy and flexible to add rules to achieve the control you want.

The principle of adding rules is: the rule added first has the highest priority. The data with the highest priority, the data passing through the router is first compared with this rule. If it is met, it will no longer be compared with the later rules. It is determined by this rule whether the data is passed or blocked.



Access Restrictions

Enable : □

Src. IP : 192.168. ___ . ___ ~ ___ . ___

Dest. IP : ___ /24 ▼ (Empty means all the IP addresses)

Protocol : TCP ▼

Dest. port : ___ ~ ___ please select ▼

Days: ● Everyday ○ Monday To Friday

Times(24h): 00 ▼ : 00 ▼ to 23 ▼ : 55 ▼

Action: Block ▼

ADD

DELETE DELETE-ALL

APPLY CANCEL

Help

Access Restrictions: According to the IP address range,protocol, port range,special application,and time to control behaviors of Internet users. A rule added earliest has a highest priority. If you want to control a user's Internet behaviors,you should firstly add a rule to forbid all of his Internet behaviors,and then add some behaviors allowed.

Access-Restrictions		
Item	**Description**	**Default**
Enable	Site control will not take effect until ticked	untick
Src. IP	Enter the IP address of the computer on the LAN that you want to control. The source address must be filled in.	empty
Dest.IP	Enter the destination IP address that you want to control. If you do not need to control the destination address, then no need to fill in, indicating all IP addresses.	empty
Protocol	Select the type of protocol you want to control. There are five options for TCP, UDP, TCP/UDP, ICMP, and ALL, where ALL includes TCP, UDP, TCP/UDP, and ICMP. The default is TCP.	TCP
Dest. port	Enter the destination port number to be controlled. If you do not need to control the destination port, select <All ports 1~65535>, and the starting port number should not be greater than the terminating port number.	empty
Days	Choose daily or weekdays (Monday to Friday), the rule takes effect	everyday
Times	Select the time period during which the rule takes effect, and the time is in 24-hour format. The start time should be earlier than the end time, and 00:00 to 23:55 means that the rule takes effect at any time during the day.	--
Action	Select whether to allow matching messages (pass) or (block).	block

[Example]

We configure an application case according to the above principles, only allowing users to send and receive mail, and using MSN and QQ.

Analysis: The port number for receiving mail is TCP 110, and sending mail port is TCP 25. Since the mail server is in the domain name mode, there is also UDP port 53 of domain name resolution (DNS), Since the port number of QQ,MSN is not fixed, so it cannot be controlled by port,Should choose special application .

To achieve the purpose of this case, the host needs to be allowed to access ports 110, 25, 53 and special applications QQ, MSN, and others cannot access. . According to the rules defined above, the rules should be added as follows (This example takes the host 192.168.10.100 as an example) :

1. Allow the host 192.168.10.100 to access TCP protocol port 110 , the operation of this rule is passed.
2. Allow the host 192.168.10.100 to access TCP protocol port 25 , the operation of this rule is passed.
3. Allow the host 192.168.10.100 to access UDP protocol port 53 , the operation of this rule is passed.
4. Allow the host 192.168.10.100 to access TCP/UDP protocol special application , this operation of this rule is passed.
5. Forbid the host 192.168.10.100 to access All or TCP/UDP protocol port 1-65535 , this operation of this rule is blocked.

The rules of 1-4 should be added first, is the data allowed to pass, last add 5, is to block all data of the host 192.168.10.100. According to the above rules, the data passed the router compared with the first added rule,When the host 192.168.10.100 is sending mail, the router will look for rules that match the data.

The sending mail port is 25, so if the first rule not met, the router will continue to check.

The second one is consistent. It is determined by this rule whether the data is passed or blocked. Since the set operation is passed, this data can be sent through the router.

If the host wants to browse the web, it needs to allow the protocol to be TCP, and the data of port 80 is passed. When its data arrives at the router, the router looks for rules and compares it. It turns out that 1-4 does not match, so continue to Look down.

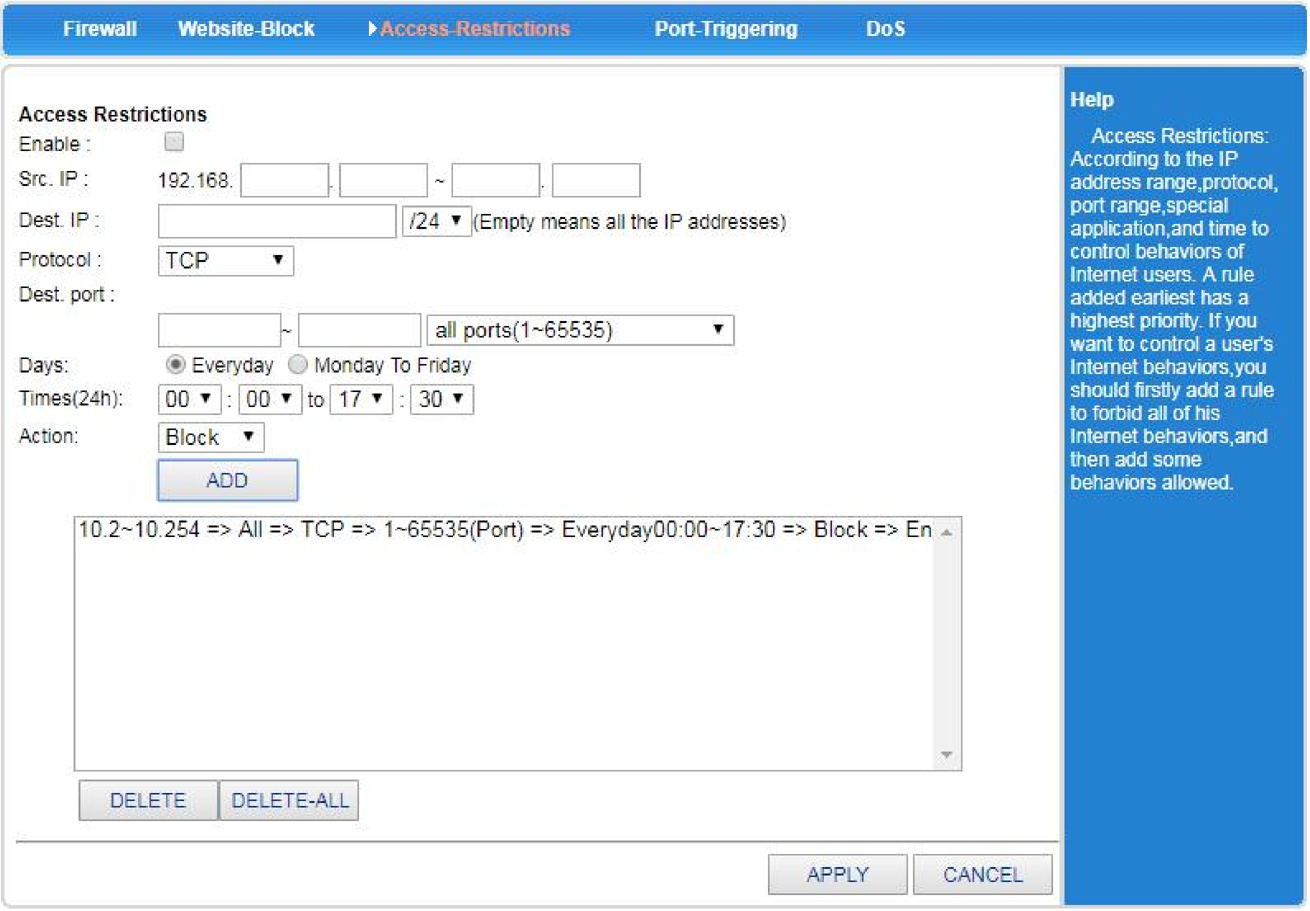
The fifth rule matches, and the operation of the rule is blocked, so the host cannot browse the web page.

The above case has no time control. If you need to control by time period, you only need to set the time range according to your needs.

[Example]

An enterprise needs to prohibit all computers in the LAN from 192.168.10.2 to 192.168.10.254, and can't access the Internet during working hours (working hours are 9:00 to 17:00, Monday to Friday), and other time is allowed.

Set as follows:



Access Restrictions

Enable : □

Src. IP : 192.168. . ~ .

Dest. IP : /24 (Empty means all the IP addresses)

Protocol : TCP

Dest. port : ~ all ports(1~65535)

Days: ● Everyday ○ Monday To Friday

Times(24h): 00 : 00 to 17 : 30

Action: Block

ADD

10.2~10.254 => All => TCP => 1~65535(Port) => Everyday00:00~17:30 => Block => En

Help

Access Restrictions: According to the IP address range,protocol, port range,special application,and time to control behaviors of Internet users. A rule added earliest has a highest priority. If you want to control a user's Internet behaviors,you should firstly add a rule to forbid all of his Internet behaviors,and then add some behaviors allowed.

After setting the selected item, click <APPLY> to complete the setting.

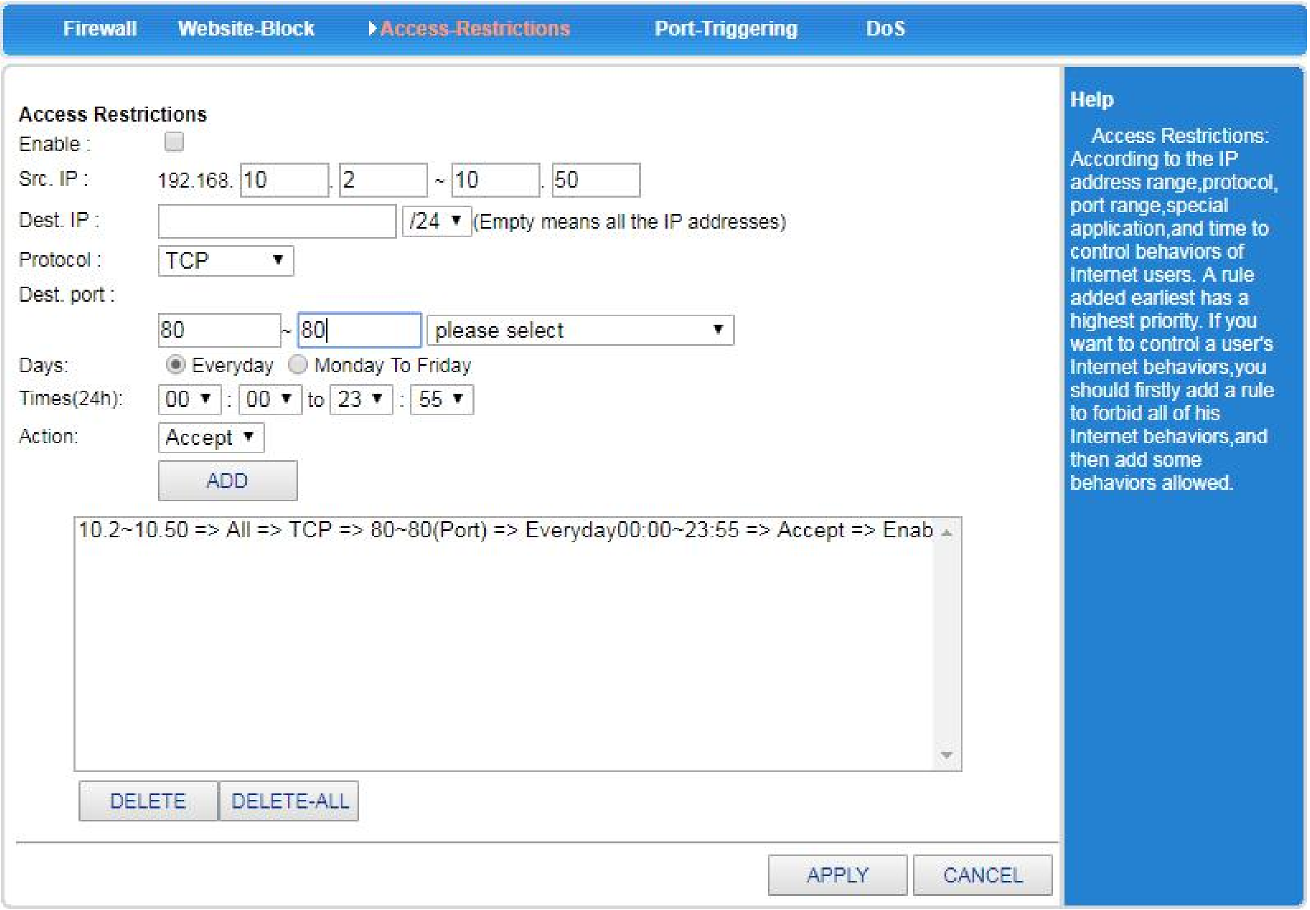
[Example]

The network administrator wants to allow only computers with IP addresses 192.168.10.2 to 192.168.10.50 to use Web services (port 80), and other computers are not allowed to access the Internet.

Note: All computer IP address is 192.168.10.2~192.168.10.254.

Set as follows:

Step1: Add an access control archive,allow computers with IP addresses 192.168.10.2 to 192.168.10.50 to access the Internet:



Access Restrictions
Enable : □
Src. IP : 192.168. 10 . 2 ~ 10 . 50
Dest. IP : /24 (Empty means all the IP addresses)
Protocol : TCP
Dest. port : 80 ~ 80 please select
Days: ● Everyday ○ Monday To Friday
Times(24h): 00 : 00 to 23 : 55
Action: Accept
ADD

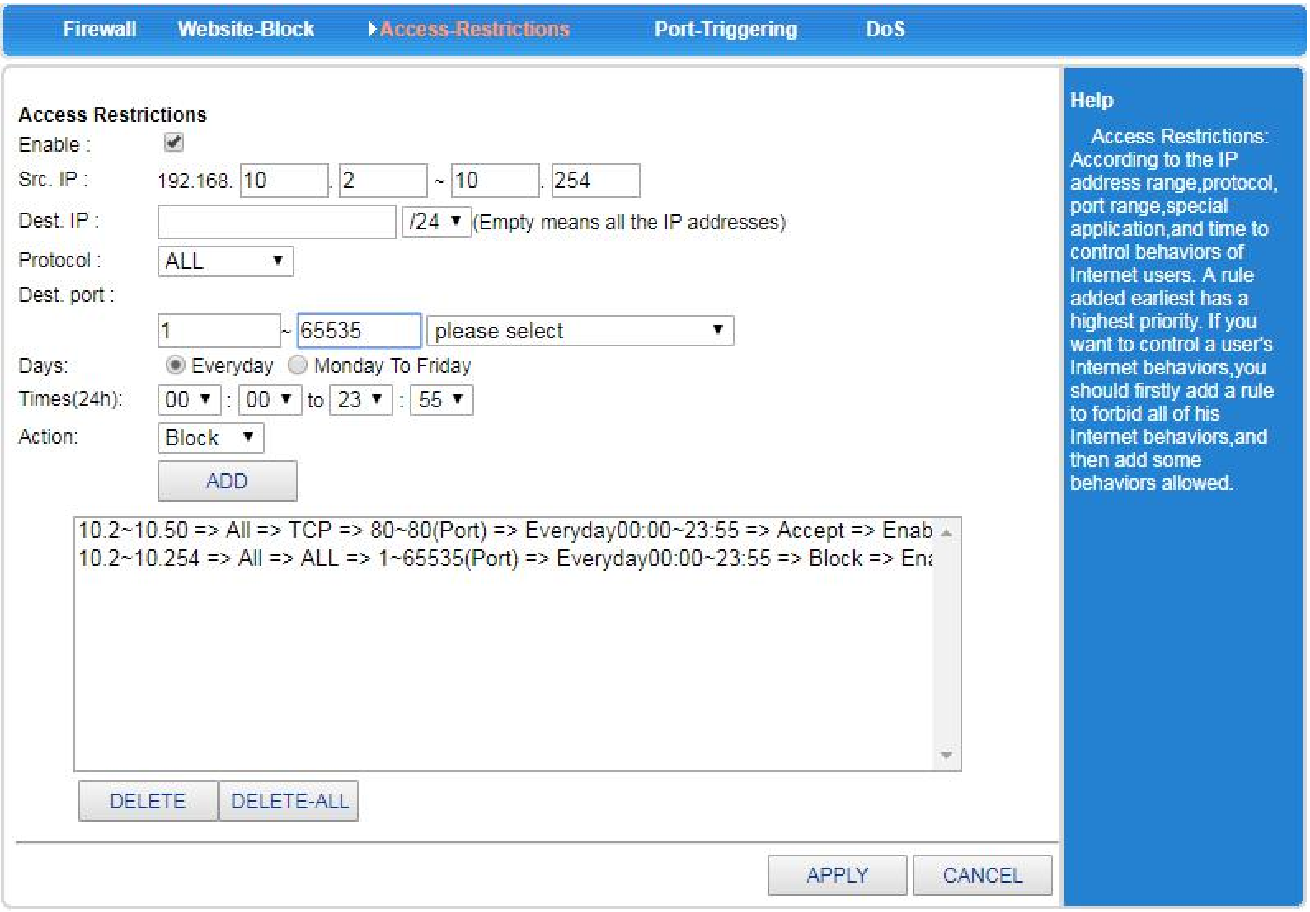
```
10.2~10.50 => All => TCP => 80~80(Port) => Everyday00:00~23:55 => Accept => Enab
```

DELETE DELETE-ALL APPLY CANCEL

Help
Access Restrictions: According to the IP address range,protocol, port range,special application,and time to control behaviors of Internet users. A rule added earliest has a highest priority. If you want to control a user's Internet behaviors,you should firstly add a rule to forbid all of his Internet behaviors,and then add some behaviors allowed.

Step2: Click <Add> to add this rule.

Step3: Prevent other computers from accessing the Internet.



Access Restrictions
Enable : ☑
Src. IP : 192.168. 10 . 2 ~ 10 . 254
Dest. IP : /24 (Empty means all the IP addresses)
Protocol : ALL
Dest. port : 1 ~ 65535 please select
Days: ● Everyday ○ Monday To Friday
Times(24h): 00 : 00 to 23 : 55
Action: Block
ADD

```
10.2~10.50 => All => TCP => 80~80(Port) => Everyday00:00~23:55 => Accept => Enab
10.2~10.254 => All => ALL => 1~65535(Port) => Everyday00:00~23:55 => Block => Ena
```

DELETE DELETE-ALL APPLY CANCEL

Help
Access Restrictions: According to the IP address range,protocol, port range,special application,and time to control behaviors of Internet users. A rule added earliest has a highest priority. If you want to control a user's Internet behaviors,you should firstly add a rule to forbid all of his Internet behaviors,and then add some behaviors allowed.

Step4: Click <Add> to add this rule.

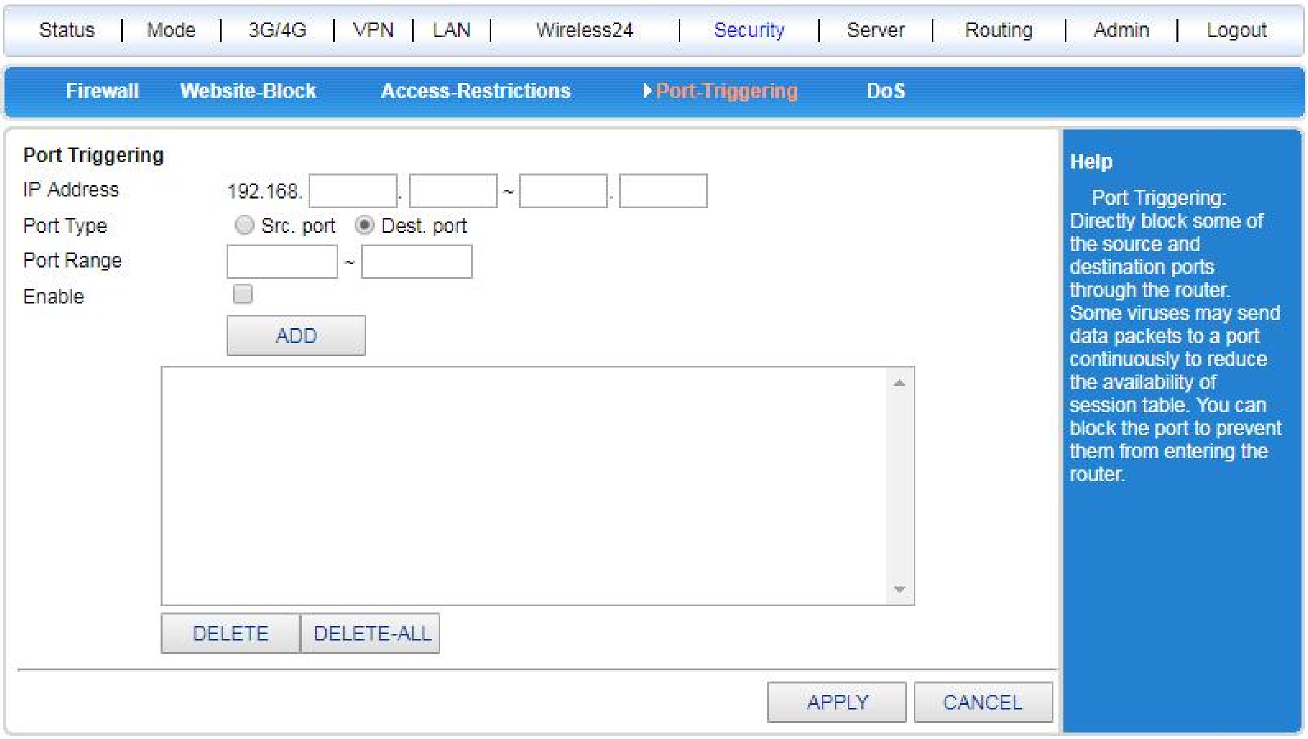
Step5: Click the <APPLY> button to complete the setting.

At this time, only computers with IP addresses of 192.168.10.2 -192.168.10.50 can use the Web service, and other computers cannot access the Internet.

5.8.3 Port Triggering

In <Port Triggering>, by controlling the port range, you can block certain ports from passing through the router, effectively blocking certain viruses from starting to connect through a port and occupying a large number of SESSION.

Note: The port here includes the source port and the destination port, so the packet will be discarded by the router regardless of whether the source port or destination port of the packet is within the range.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Firewall
Website-Block
Access-Restrictions
Port-Triggering
DoS
ADD
DELETE
DELETE-ALL
APPLY
CANCEL

Port Triggering

IP Address 192.168. [ ] . [ ] ~ [ ] . [ ]

Port Type ○ Src. port ● Dest. port

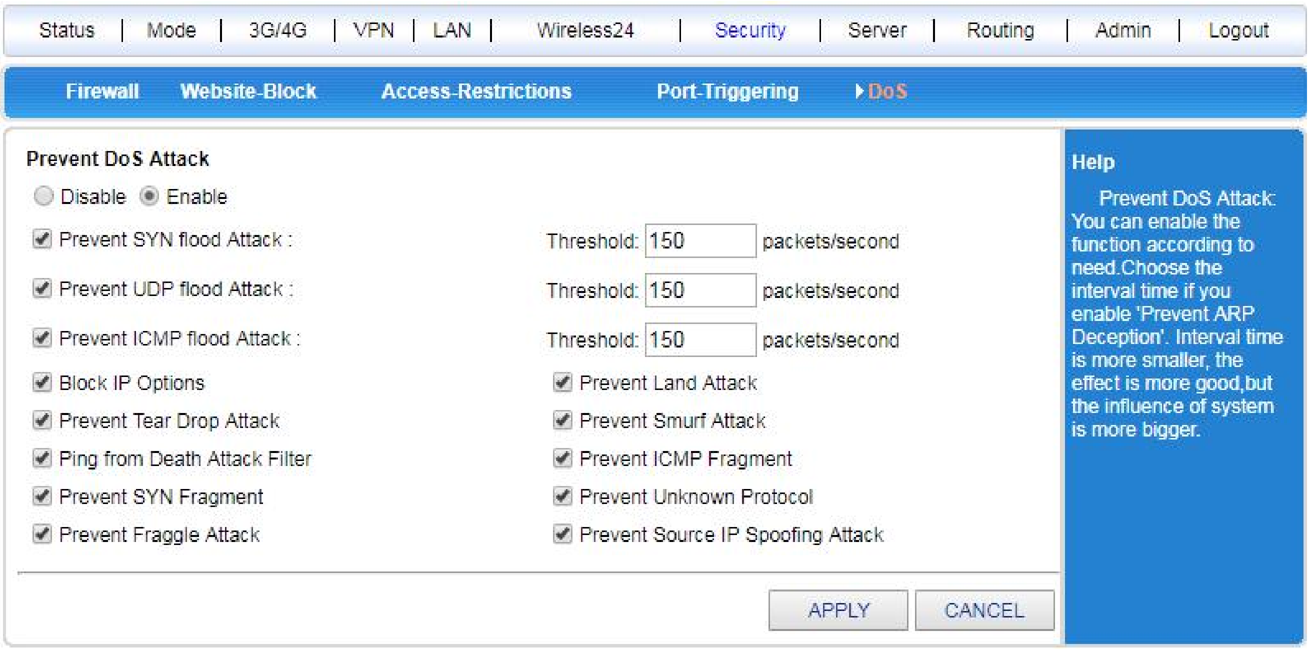
Port Range [ ] ~ [ ]

Enable □

Help

Port Triggering: Directly block some of the source and destination ports through the router. Some viruses may send data packets to a port continuously to reduce the availability of session table. You can block the port to prevent them from entering the router.

5.8.4 DOS


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Firewall
Website-Block
Access-Restrictions
Port-Triggering
DoS
APPLY
CANCEL

Prevent DoS Attack

○ Disable ● Enable

☑ Prevent SYN flood Attack : Threshold: 150 packets/second

☑ Prevent UDP flood Attack : Threshold: 150 packets/second

☑ Prevent ICMP flood Attack : Threshold: 150 packets/second

☑ Block IP Options ☑ Prevent Land Attack

☑ Prevent Tear Drop Attack ☑ Prevent Smurf Attack

☑ Ping from Death Attack Filter ☑ Prevent ICMP Fragment

☑ Prevent SYN Fragment ☑ Prevent Unknown Protocol

☑ Prevent Fraggle Attack ☑ Prevent Source IP Spoofing Attack

Help

Prevent DoS Attack: You can enable the function according to need.Choose the interval time if you enable 'Prevent ARP Deception'. Interval time is more smaller, the effect is more good,but the influence of system is more bigger.

DOS		
Item	**Description**	**Default**
Disable/Enable	Select this option to disable or enable the DOS attack prevention function of the wireless router.	enable
Prevent SYN flood attack	Enable this option and the wireless router can prevent Syn Flood attacks. The maximum Syn packet rate value can be set according to the amount of traffic under normal conditions of the server, and the threshold value is generally 150 packets/second.	enable
Prevent UDP flood attack	Enable this option, the wireless router can prevent UDP Flood attacks. The maximum UDP packet rate value can be set according to the normal access volume of the server, and the threshold value is generally 150 packets/second.	enable
Prevent ICMP flood attack	Enable this option and the wireless router can prevent ICMP Flood attacks. The maximum ICMP packet rate value can be set according to the amount of traffic under normal conditions of the server, and the threshold value is generally maintained at 150 packets/second.	enable
Block IP options	Enable it, the wireless router can prevent IP option attacks.	enable
Prevent Land attack	Enable it, the wireless router can prevent Land attacks.	enable
Prevent Tear Drop attack	Enable it, the wireless router can prevent Tear Drop attacks.	enable
Prevent Smuef attack	Enable it, the wireless router can prevent Smuef attacks.	enable
Ping from Death attack Filter	Enable it, the wireless router can prevent Ping of Death attacks.	enable
Prevent ICMP fragment	Enable it, can prevent ICMP fragments attacks.	enable
Prevent unknown protocols	Enable it, can prevent unknown protocols attacks.	enable
Prevent Fraggle Attack	Enable it, can prevent Fraggle attacks.	enable
Prevent source IP spoofing Attack	Enable it, can prevent source IP spoofing attacks.	enable
Prevent ARP spoofing	Enable it, the wireless router starts anti-ARP spoofing. The time shorter the interval is, the better the anti-ARP spoofing effect is, but the impact on the system is relatively large. Please select according to your needs.	enable

5.9 Server

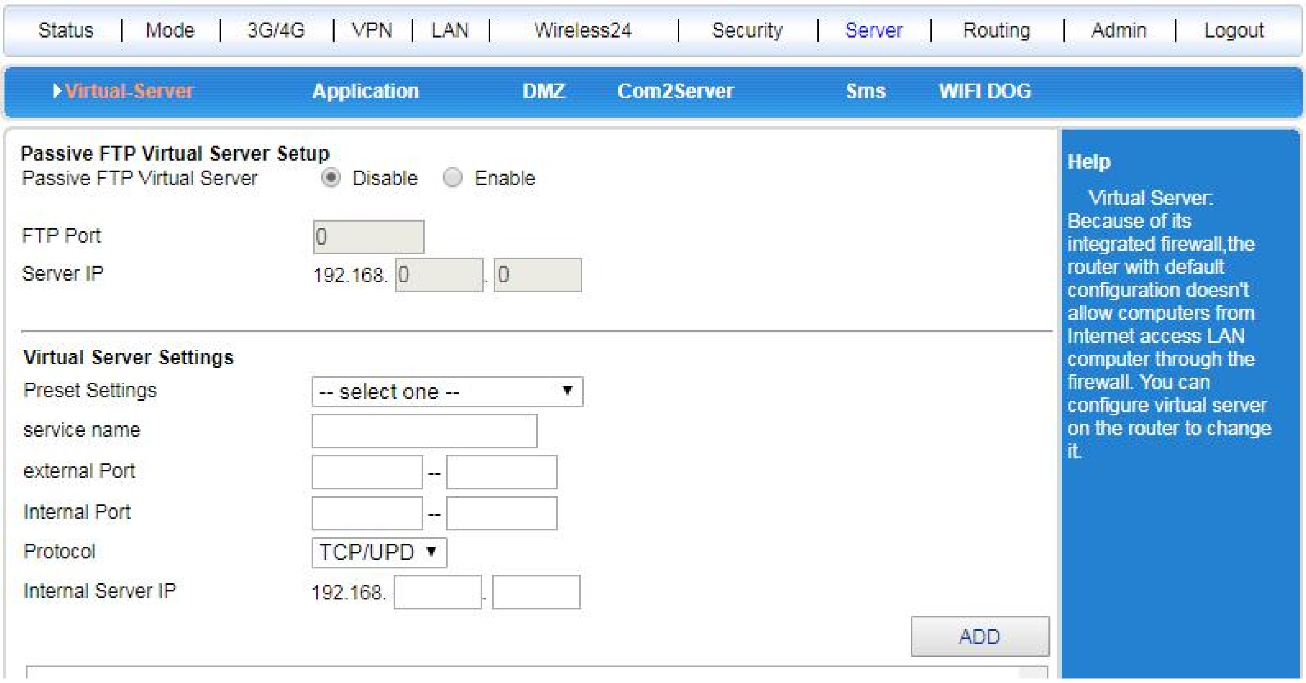
In the server, you can set:

- A virtual server that sets up an internal server to provide access to Internet users.
- DMZ (Demilitarized zone), the host of the DMZ, is actually the default virtual server. When the open port of the virtual server to be set is uncertain, it can be set as a DMZ host.
- Port triggering allows the wireless router to automatically open inbound service ports based on the LAN's access to the Internet.

5.9.1 Virtual Server

Virtual server can also be called port mapping. You can set up a virtual server to enable Internet users to access services provided by internal LAN servers, such as Web services, Email, and FTP. By default, to ensure the security of the LAN, the wireless router blocks the connection request initiated from the Internet. Therefore, if you want Internet users to access the servers in the LAN, you need to set up a virtual server.

Virtual server can mapping the WAN port IP address, the external port number, and the server IP address and internal port number in the LAN. All access to a service port of the WAN port will be redirected to the corresponding internal server of the specified LAN port.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Virtual-Server
Application
DMZ
Com2Server
Sms
WIFI DOG

Passive FTP Virtual Server Setup

Passive FTP Virtual Server ● Disable ○ Enable

FTP Port 0

Server IP 192.168. 0 . 0

Virtual Server Settings

Preset Settings -- select one --

service name

external Port --

Internal Port --

Protocol TCP/UPD

Internal Server IP 192.168. .

ADD

Help

Virtual Server: Because of its integrated firewall,the router with default configuration doesn't allow computers from Internet access LAN computer through the firewall. You can configure virtual server on the router to change it.

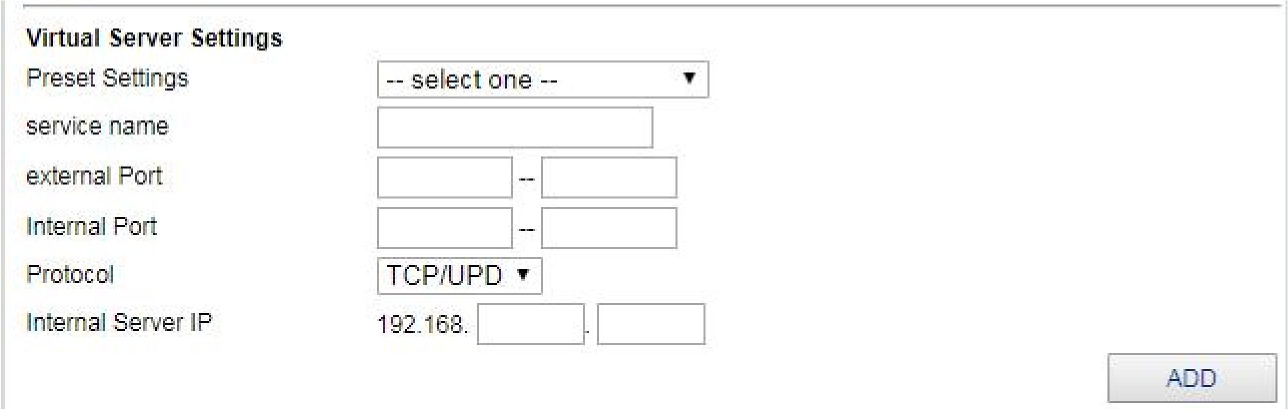
Virtual Server		
Item	**Description**	**Default**
FTP port	Passive FTP virtual server port	empty
Server IP	Passive FTP virtual server IP address	empty
Preset Settings	The system provides common service options such as FTP, Web, and more. Select a service in the drop-down list box, and the service name, external port, and internal port entries will be automatically set. Description: • If the default service provided by the wireless router does not have what you need, you can set the following service information yourself. • The port number of the default service is a common port number, which you can modify if you want.	empty
Service Name	The name of the virtual server settings item.	empty
External port	The port used by the client to access the virtual server. The value ranges is 1 ~ 65535. The port range must be from small to large. If there is only one port, fill in the same port number in both places. Note: The external port of each setting item cannot be repeated, and the number of internal ports and external ports must be the same, that is, the internal port and the external port correspond one-to-one. For example,	empty

	set up a virtual server with an external port of 100-102 and an internal port of 10-12. If the wireless router receives an access request from the external 101 port, the wireless router forwards the data packet to port 11 of the internal server.	
Internal port	A truly open service port on a virtual server. The value ranges is 1 t~65535. The port range must be from small to large. If there is only one port, fill in the same port number in both places. Note: The internal ports of each setting item are allowed to repeat, and the number of internal ports and external ports must be the same, that is, the internal port and the external port are in one-to-one correspondence.	empty
Internal server IP	Virtual server IP address	empty

[Example]

The A company's internal LAN connects to the Internet through a wireless router. There is a Web server on the LAN (IP address is 192.168.10.100, service port is 80), and the client (user on the Internet or LAN user of the company) needs to access Web server through port 8080.

Set as follows:



Virtual Server Settings

Preset Settings	-- select one --
service name	
external Port	--
Internal Port	--
Protocol	TCP/UPD
Internal Server IP	192.168. .

After the setup is complete, simply enter http://xxx.xxx.xxx.xxx:8080 in the client browser to access the web server (xxx.xxx.xxx.xxx is the current WAN port address of the wireless router).

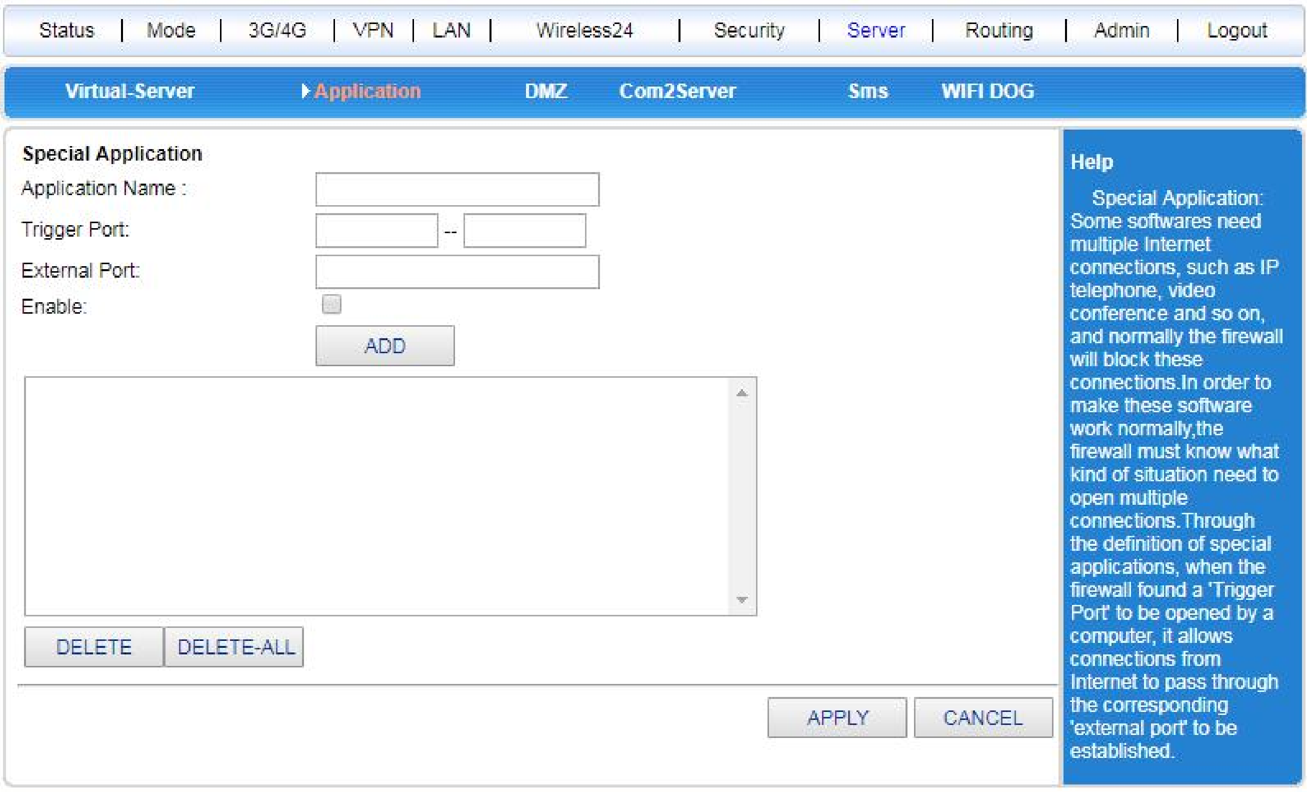
5.9.2 Special Application

The LAN client accesses the server on the Internet. For some applications, when the client initiates a connection to the server, the server also needs to initiate a connection request to the client. By default, the wireless router rejects the request of the WAN side to actively connect. This will interrupt the communication. By defining the port triggering rule, when the client accesses the server to trigger this rule, the wireless router automatically opens the port that the server needs to request from the client, thus ensuring normal communication. After the client and the wireless router have no data interaction for a period of time, the wireless router automatically closes the previously opened port, which not only ensures the normal use of the application, but also ensures the security of the local area network to the utmost extent.

Description:

- Port triggering supports up to 50 settings.
- In each setting item, the trigger port and the foreign port are allowed to overlap.
- When a computer in the LAN establishes a connection with the external network through the trigger port, its corresponding external port will also be opened, and the computer of the external network can access the LAN through these ports.

- Each defined port trigger can only be used by one computer at the same time. If more than one machine opens the same "trigger port" at the same time, the "External port" connection will only be redirected to the computer that last opened the "trigger port".



Special Application: Some softwares need multiple Internet connections, such as IP telephone, video conference and so on, and normally the firewall will block these connections.In order to make these software work normally,the firewall must know what kind of situation need to open multiple connections.Through the definition of special applications, when the firewall found a 'Trigger Port' to be opened by a computer, it allows connections from Internet to pass through the corresponding 'external port' to be established.

Special Application		
Item	**Description**	**Default**
Application name	This port triggers setting name	empty
Trigger port	The port which the LAN client initiates a request to the server. The value ranges is 1 ~ 65535. The port range must be from small to large. If there is only one port, fill in the same port number in both places.	empty
External port	The port which server needs to actively request to the client in the LAN. The value rangesis 1~65535. You can set a single port, a port range, or a combination of the two. The ports are separated by a comma ",".eg：100,200-300,400.	empty

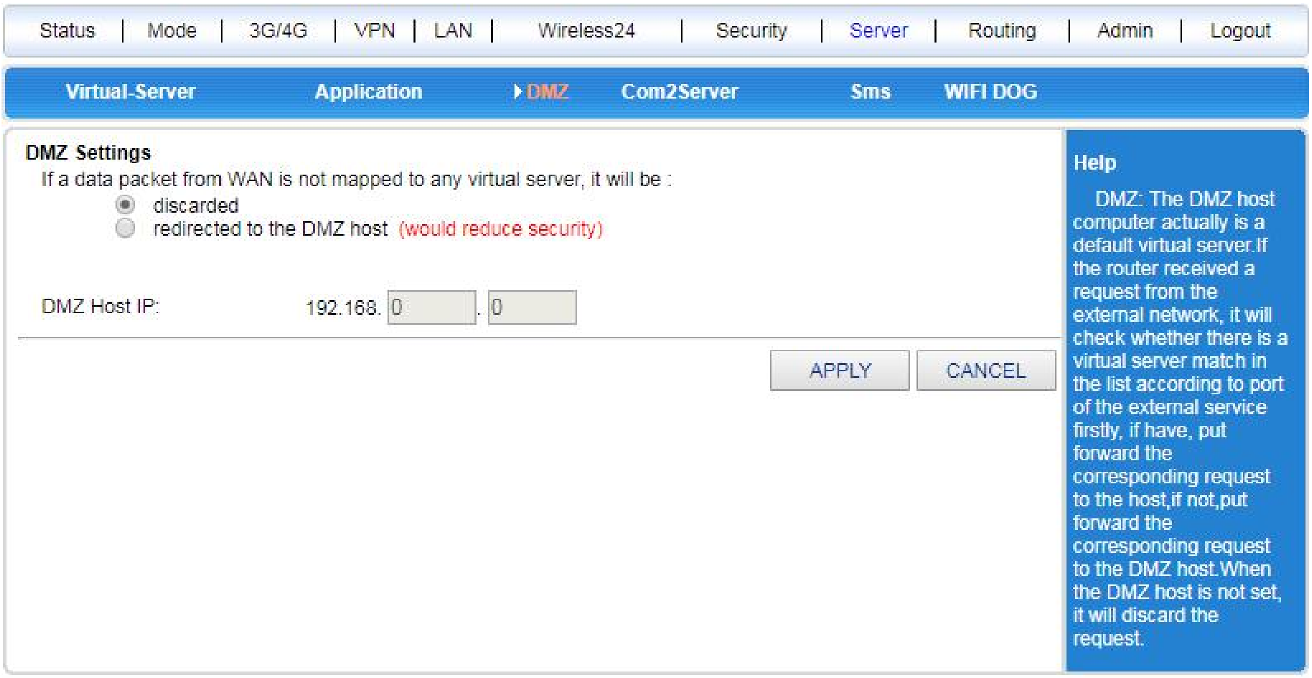
5.9.3 DMZ Setting

The DMZ host is actually a default virtual server with a lower priority than the virtual server. If the wireless router receives a connection request from the external network, it will first look up the virtual service list according to the service port number of the external request, and check if there is a matching mapping entry:

- If there is a matching entry, send the request message to the virtual server corresponding to the entry;
- If no matching entries are found, check if there is a matching DMZ host. If the DMZ host exists, forward all the request messages to the DMZ host, otherwise discard.

Description:

- After the DMZ feature is enabled, the DMZ host is exposed to the Internet and the security is reduced.
- The port number of the DMZ host should be the same as the service port number actually opened by the DMZ.



Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Virtual-Server Application DMZ Com2Server Sms WIFI DOG
APPLY
CANCEL

DMZ Settings

If a data packet from WAN is not mapped to any virtual server, it will be :

● discarded

○ redirected to the DMZ host (would reduce security)

DMZ Host IP: 192.168. 0 . 0

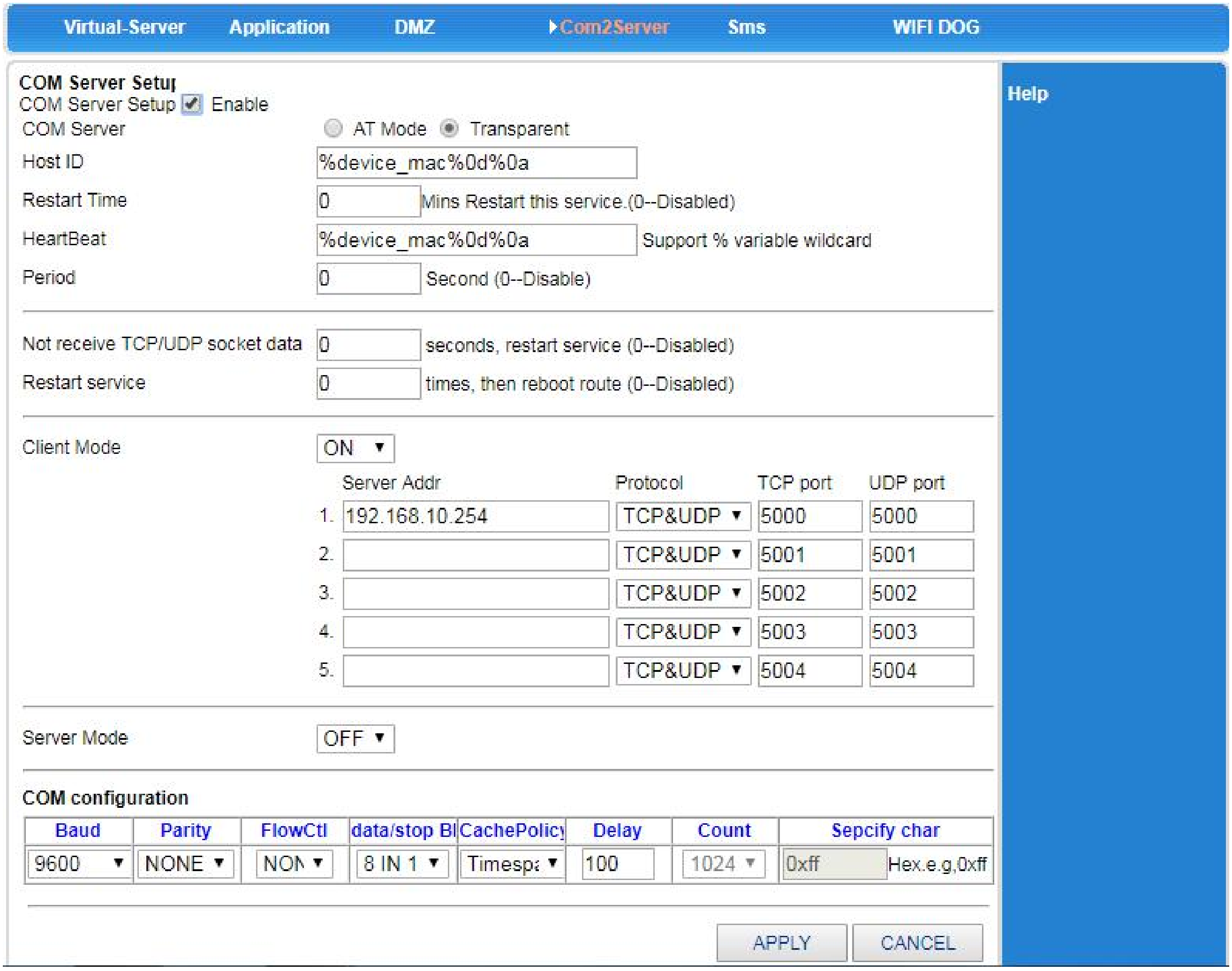
Help

DMZ: The DMZ host computer actually is a default virtual server.If the router received a request from the external network, it will check whether there is a virtual server match in the list according to port of the external service firstly, if have, put forward the corresponding request to the host,if not,put forward the corresponding request to the DMZ host.When the DMZ host is not set, it will discard the request.

DMZ Setting		
Item	**Description**	**Default**
discarded	Tick this item， When an incoming packet does not match any virtual server entry, the router discards the packet.	Ticked
Redirected to DMZ host	Tick this item,When the incoming packet does not match any virtual server entry,the router forwards the packet to the DMZ host.After ticked this item, you also need to set the "DMZ Host IP Address". If the set DMZ host IP address does not exist, the router discards the packet.	untick
DMZ Host IP	Set DMZ host IP address Note: Only one DMZ host can be set in the LAN.	empty

5.9.4 Com Server

The UART2 interface is the physical interface of the serial communication service.



COM Server Setuן

COM Server Setup ☑ Enable

COM Server ○ AT Mode ● Transparent

Host ID %device_mac%0d%0a

Restart Time 0 Mins Restart this service.(0--Disabled)

HeartBeat %device_mac%0d%0a Support % variable wildcard

Period 0 Second (0--Disable)

Not receive TCP/UDP socket data 0 seconds, restart service (0--Disabled)

Restart service 0 times, then reboot route (0--Disabled)

Client Mode ON

	Server Addr	Protocol	TCP port	UDP port
1.	192.168.10.254	TCP&UDP	5000	5000
2.		TCP&UDP	5001	5001
3.		TCP&UDP	5002	5002
4.		TCP&UDP	5003	5003
5.		TCP&UDP	5004	5004

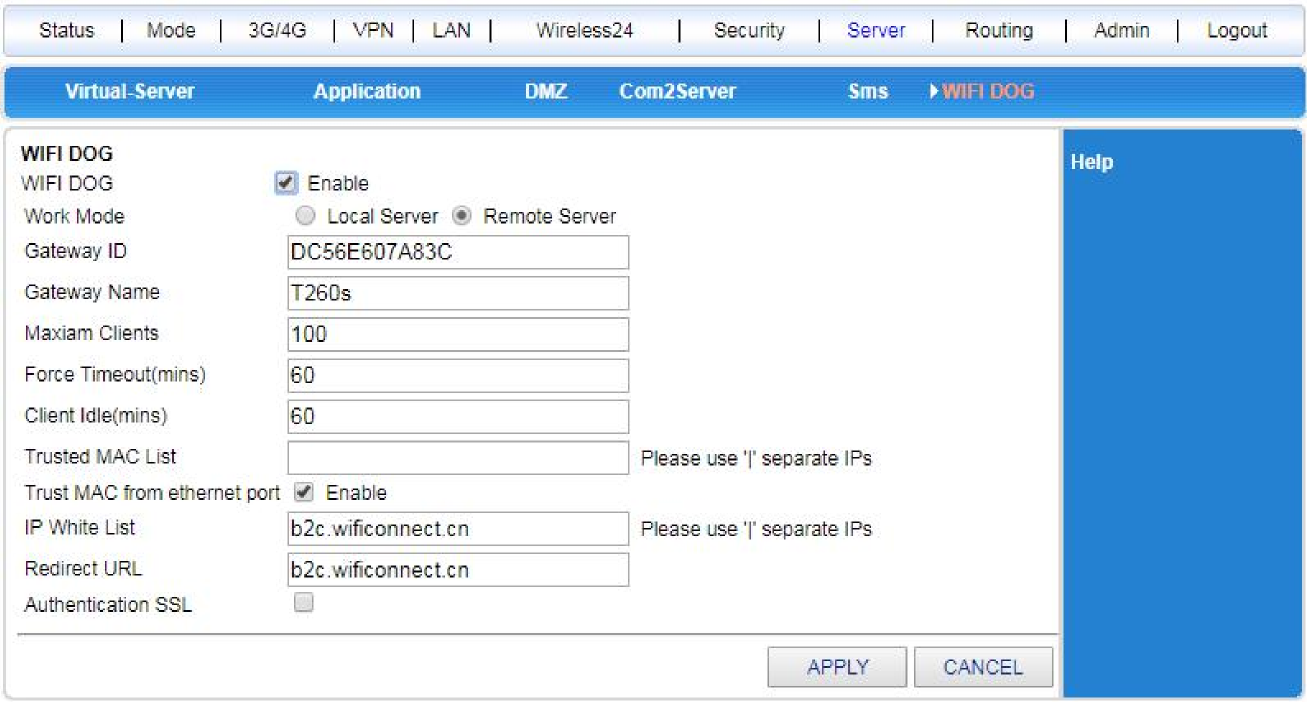
Server Mode OFF

COM configuration

Baud	Parity	FlowCtl	data/stop Bl	CachePolicy	Delay	Count	Sepcify char
9600	NONE	NON	8 IN 1	Timespa	100	1024	0xff Hex.e.g,0xff

Com Server		
Item	**Description**	**Default**
COM Server	Select the transparent transmission mode or AT mode. command switch is available: In the transparent transmission mode, enter +++ to enter the AT mode. In AT mode, enter ato into transparent mode	transparent transmission
Heartbeat	You can set the variable in nvram as the content sent by the heartbeat.	empty
Period	Set 0 is disable	empty
Client Mode	The router serial port service is used as the client, and the LAN connected device is used as the serial port server.	ON
Server Mode	Router serial port used as serial server, LAN connected device as client	OFF

5.9.5 WIFI DOG


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Virtual-Server
Application
DMZ
Com2Server
Sms
WIFI DOG
Help
APPLY
CANCEL

WIFI DOG

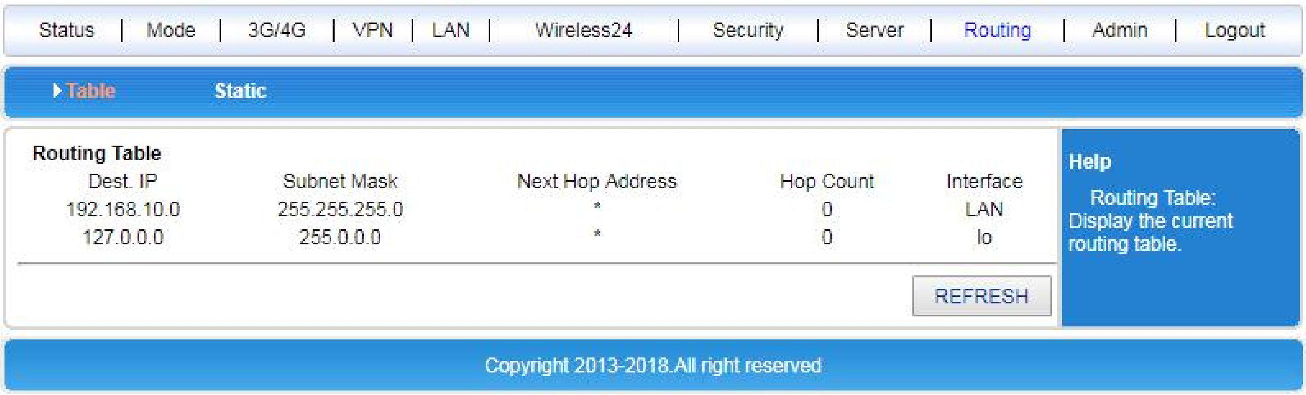
WIFI DOG	☑ Enable	
Work Mode	○ Local Server ● Remote Server	
Gateway ID	DC56E607A83C	
Gateway Name	T260s	
Maxiam Clients	100	
Force Timeout(mins)	60	
Client Idle(mins)	60	
Trusted MAC List		Please use '|' separate IPs
Trust MAC from ethernet port	☑ Enable	
IP White List	b2c.wificonnect.cn	Please use '|' separate IPs
Redirect URL	b2c.wificonnect.cn	
Authentication SSL	□	

WIFI DOG		
Item	**Description**	**Default**
Work Mode	Local Server: local authentication server Remote Server: Remote wifidog server	--
Gateway ID	Local MAC address	--
Local trust	Local wired network does not require authentication	--
Trusted MAC List	Set up a local wireless MAC that does not require authentication	--
IP White List	Set no need to authenticate when accessing a domain name or IP address	--
Authentication SSL	The server needs to support SSL. It cannot be ticked by default, otherwise the authentication cannot be enabled.	

5.10 Routing

In the routing settings, you can set a static route.

5.10.1 Routing Table


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Table
Static
REFRESH
Copyright 2013-2018.All right reserved

Routing Table

Dest. IP	Subnet Mask	Next Hop Address	Hop Count	Interface
192.168.10.0	255.255.255.0	*	0	LAN
127.0.0.0	255.0.0.0	*	0	lo

Help

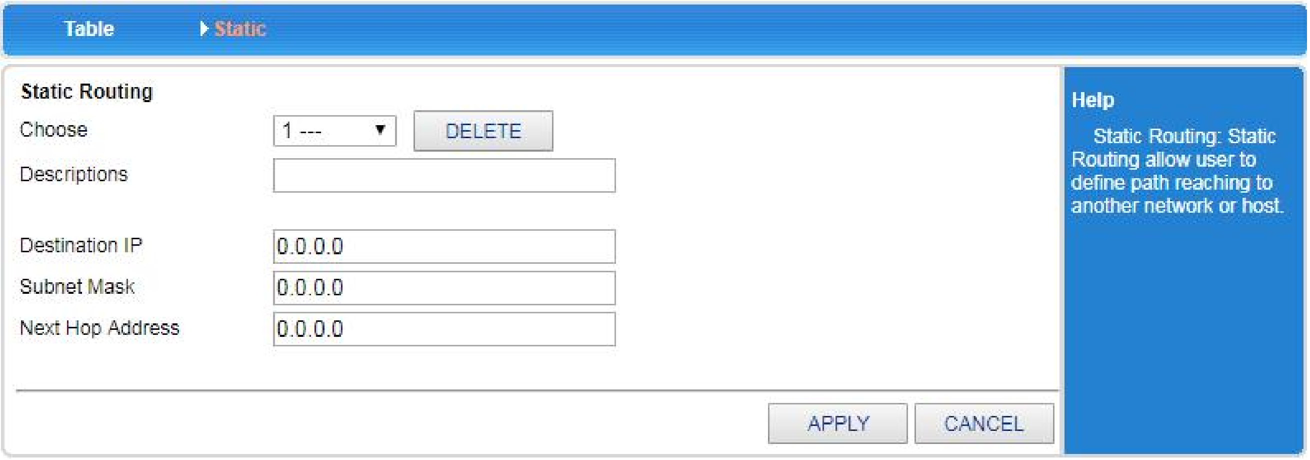
Routing Table: Display the current routing table.

5.10.2 Static

Static routes manually set the destination address, subnet mask, next hop address, and outbound interface to make the packets destined for the specified destination address go to the specified path.

The static route does not change according to the network structure. When the destination network path changes or the network is faulty, you can manually re-specify the path from the packet to the destination network by manually modifying the corresponding static routing table.

After the static route is added, click <Current Routing Table> to check whether the added static route takes effect. If the wrong route is added, it will only be displayed in the routing table in the following figure, but it will not take effect. There is no such route in the routing information table.



Static Routing

Choose	1 ---
Descriptions	
Destination IP	0.0.0.0
Subnet Mask	0.0.0.0
Next Hop Address	0.0.0.0

Help

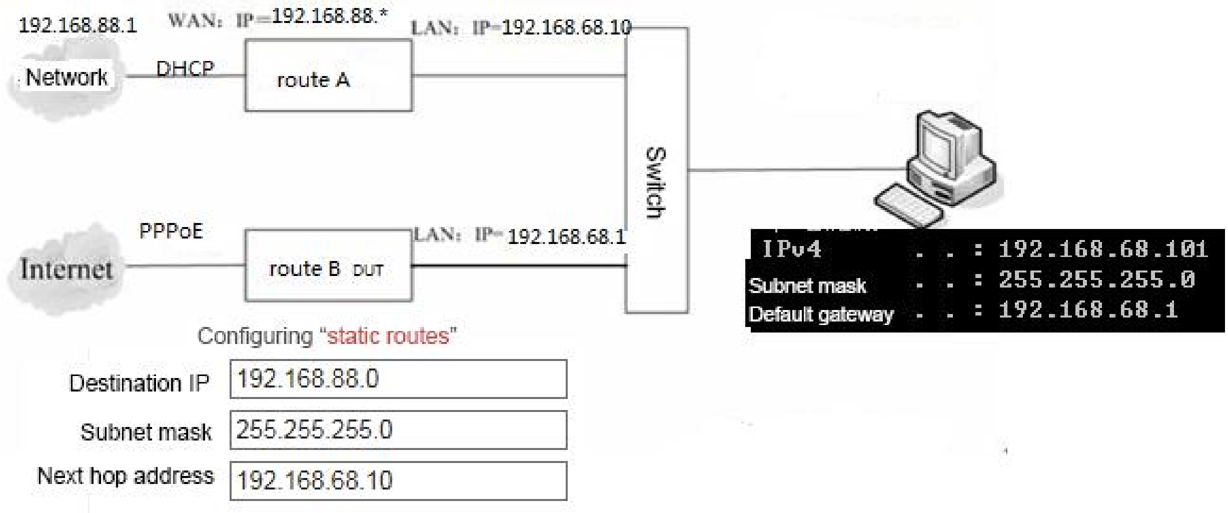
Static Routing: Static Routing allow user to define path reaching to another network or host.

Static Route		
Item	**Description**	**Default**
Selection	The router has a total of 20 static routes to choose	1
Comment	You can comment on the static route	empty
Destination address	Destination IP address	0.0.0.0
Subnet mask	The destination address subnet mask to be reached.	0.0.0.0
Next hop address	The IP address of the next router that the data needs to pass before it reaches the destination address.	0.0.0.0

NOTE: After setting, click <Routing Table> to check whether the added static route takes effect. If the wrong route is added, it will only be displayed in the routing table in the following figure, but it will not take effect. There is no such route in the routing information table.

[Example]

In company,not only can connect external network via wireless router B,but also can connect intranet server via wireless router A.The company computer needs to be able to access both the external network and the internal network server without modifying the IP address and gateway of the local connection. Configuration example is as follows:



```
IPv4            . . : 192.168.68.101
Subnet mask     . . : 255.255.255.0
Default gateway . . : 192.168.68.1
```

Configuring "static routes"

Destination IP 192.168.88.0

Subnet mask 255.255.255.0

Next hop address 192.168.68.10

By default, the PC sends data to the gateway 192.168.68.1, which is router B. After receiving the data, router B checks the destination address of the packet. If the IP address of the destination address IP is 192.168.88.0, the router adds a static routing table to send the data packets sent by the PC to the 192.168.88.0 network segment to the router A gateway. This allows the PC to directly access the company's intranet server.

5.11 Admin

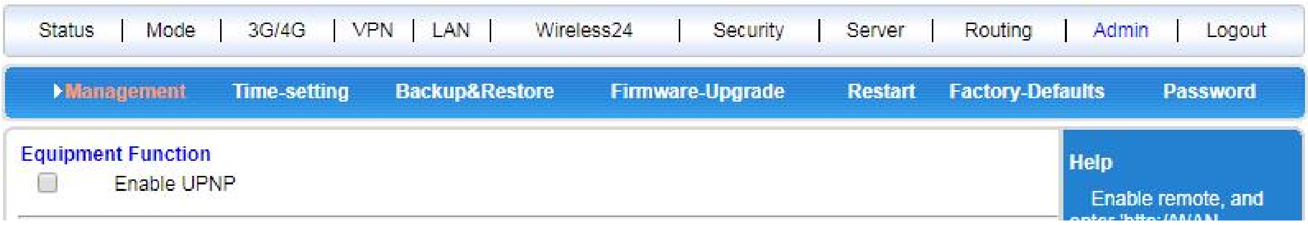
This chapter describes how to operate a wireless router through a web page. You can do the following:

- Time settings: Set the local time zone and get the real network time.
- NTP server settings: Set the address of the specified NTP server to provide time synchronization between routers, switches, and workstations.
- Backup Settings: Back up system setup information to prevent accidental loss of information.
- Restore settings from file: Restore current settings to previously backed up settings.
- Factory Defaults: Restore the wireless router to the factory default state.
- Firmware Upgrade: Upgrade the software of the wireless router through the web page.
- Remote: Allow/disable users to remotely log in to the wireless router's settings page via the WAN port to manage the wireless router.
- Restart: Restart the wireless router via the web page.
- Modify Password: Prevent unauthorized people from logging in to the web settings page.

5.11.1 Management

Equipment Function

The UPnP protocol is used by systems such as Windows ME, 2000, XP. If this feature is enabled, these operating systems will automatically find the router through this protocol.UPnP (Universal Plug and Play) is mainly used to implement intelligent inter working of devices. It can automatically discover and control various network devices from various vendors without user participation and use of the main server. When the UPnP function is enabled, the router can implement NAT traversal: when the computer in the LAN communicates with the Internet through the wireless router, the wireless router can automatically add and delete the NAT mapping table as needed, so that some traditional services (such as MSN voice and video) cannot be traversed. The problem with NAT.



Equipment Function

□ Enable UPNP

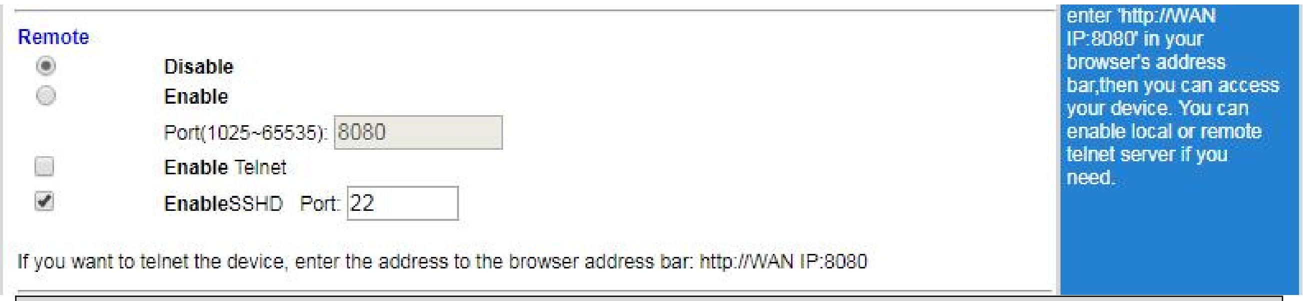
Help

Enable remote, and

Tick it and Press the <APPLY> button to complete the setting.

Remote

You can set up and manage your wireless router.



Remote

● Disable

○ Enable

Port(1025~65535): 8080

□ Enable Telnet

☑ EnableSSHD Port: 22

If you want to telnet the device, enter the address to the browser address bar: http://WAN IP:8080

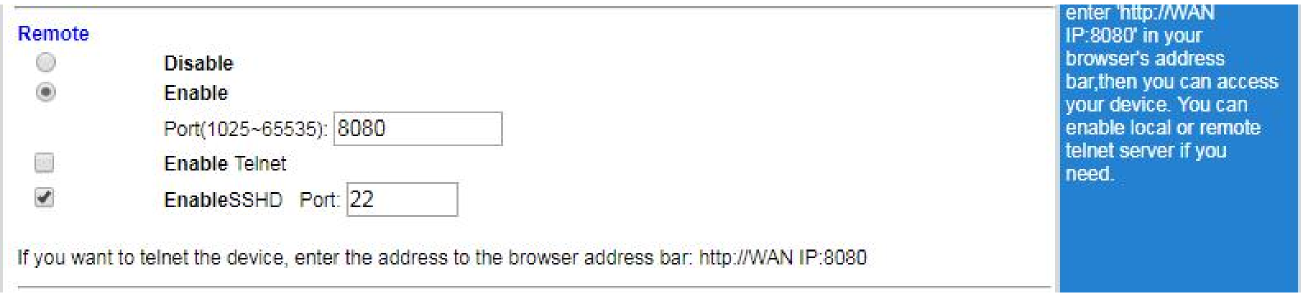
enter 'http://WAN IP:8080' in your browser's address bar,then you can access your device. You can enable local or remote telnet server if you need.

Remote @Management		
Item	**Description**	**Default**
Disable	Tick this option to disable remote management of the wireless router.	ticked
Enable Port	Tick this item to indicate that the wireless router can be remotely managed. Enter the remote management port number. The external user can log in to the wireless router's settings page to manage the router. The default is 8080.	Untick
Enable Telnet	Tick this item to remotely manage the wireless router via telnet.	Untick
Enable SSHD	Tick this item to remotely manage the wireless router via SSHD.	Ticked

[Example]

Allow a computer on the Internet to manage wireless routers through port 8080,

Set as follows:



Remote

○ Disable

● Enable

Port(1025~65535): 8080

□ Enable Telnet

☑ EnableSSHD Port: 22

If you want to telnet the device, enter the address to the browser address bar: http://WAN IP:8080

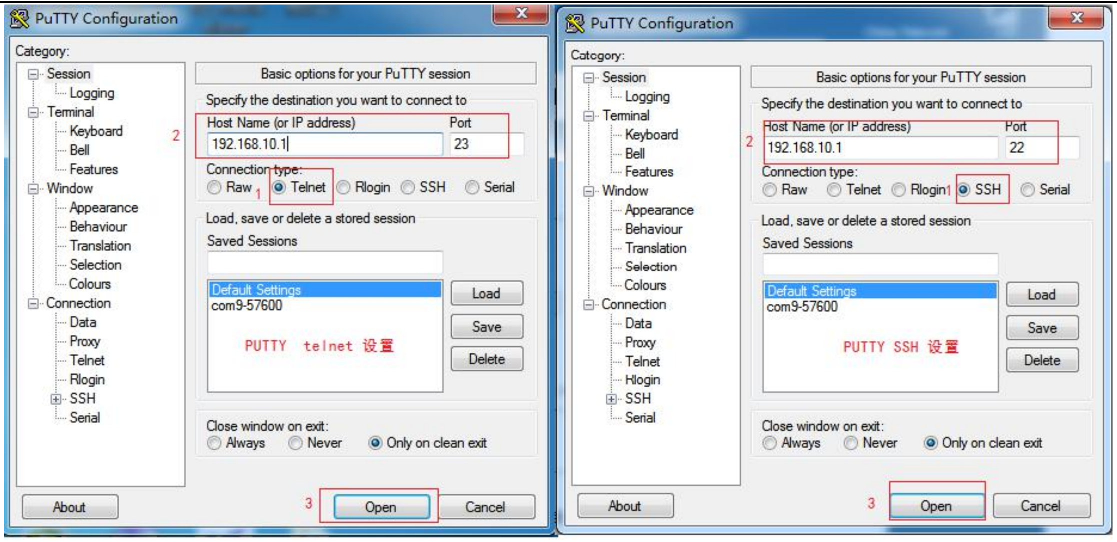
enter 'http://WAN IP:8080' in your browser's address bar,then you can access your device. You can enable local or remote telnet server if you need.

Just need enter "http://XX.XX.XX.XX:8080" in the browser address bar of this computer to log in to the wireless router, (where "XX.XX.XX.XX" is the WAN port IP of the wireless router. Address) for configuration management.

SSH default is enabled, telnet management default is disabled and needs to be manually opened.

Instructions:

Take PUTTY as an example. As shown below, you can choose one of ssh or telnet.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 192.168.10.1 Port: 23

Connection type: ○ Raw ● Telnet ○ Rlogin ○ SSH ○ Serial

Saved Sessions: Default Settings, com9-57600

PUTTY telnet 设置

Close window on exit: ○ Always ○ Never ● Only on clean exit

PuTTY Configuration

Host Name (or IP address): 192.168.10.1 Port: 22

Connection type: ○ Raw ○ Telnet ○ Rlogin ● SSH ○ Serial

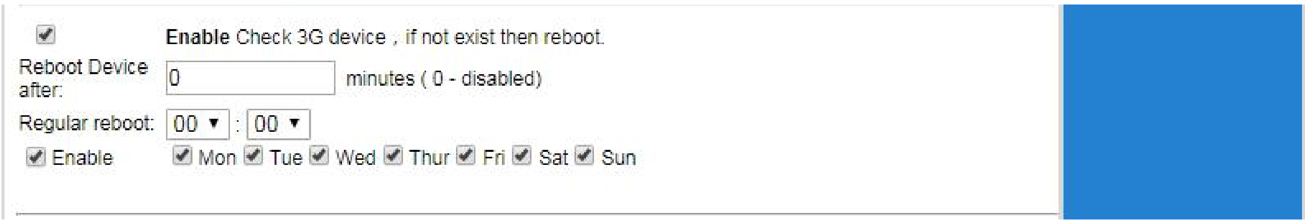
Saved Sessions: Default Settings, com9-57600

PUTTY SSH 设置

Close window on exit: ○ Always ○ Never ● Only on clean exit

Reboot Device

The system reboot is divided into a timed restart (Reboot device after x minutes) and a Regular reboot (the system reboot at one time in the day).



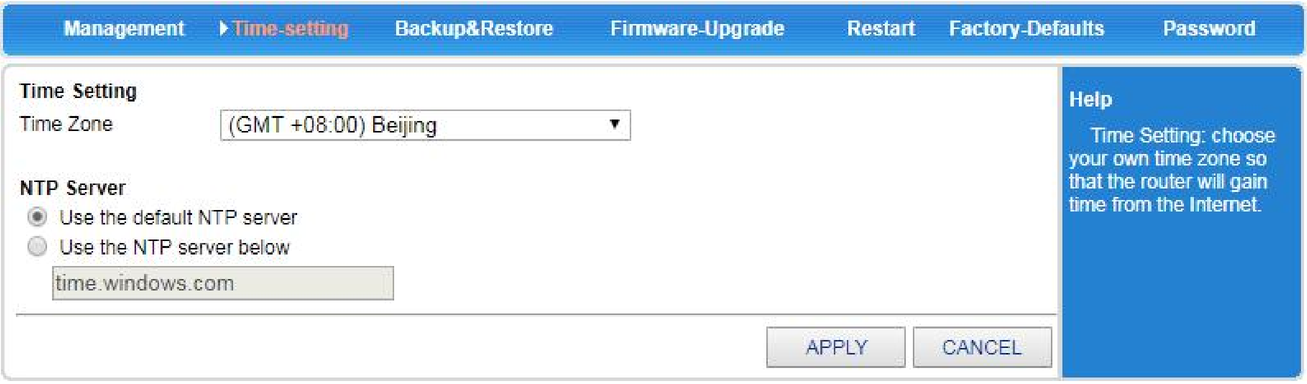
☑ Enable Check 3G device , if not exist then reboot.

Reboot Device after: 0 minutes (0 - disabled)

Regular reboot: 00 : 00

☑ Enable ☑ Mon ☑ Tue ☑ Wed ☑ Thur ☑ Fri ☑ Sat ☑ Sun

5.11.2 Time-setting



Time Setting

Time Zone: (GMT +08:00) Beijing

NTP Server

● Use the default NTP server

○ Use the NTP server below

time.windows.com

Help

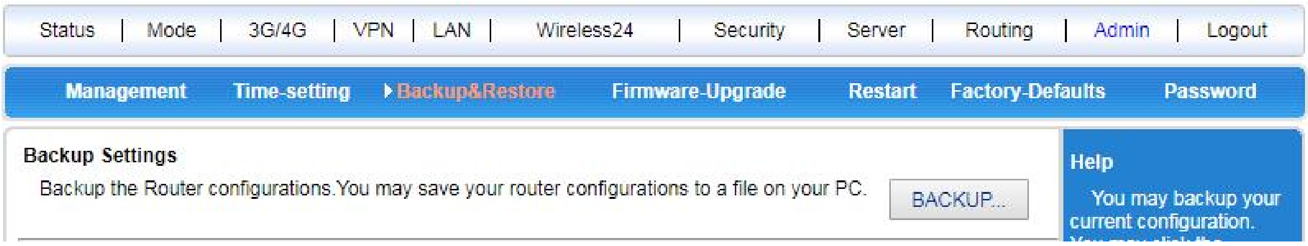
Time Setting: choose your own time zone so that the router will gain time from the Internet.

Remote @Management		
Item	**Description**	**Default**
Time Zone	Select your own time zone and the wireless router will automatically get time from the network.	Beijing
Use the default NTP server	Tick it,the wireless router updates the time from the default NTP server. By default, the wireless router's default NTP server is used.	Ticked
Use the NTP Server below	If you need to set up another NTP server, tick it and enter the address (in the form of IP address or domain name) of the NTP server in the text box. The wireless router updates the time to the specified NTP server.	Untick

5.11.3 Backup & Restore

Backup Settings

If you have previously backed up the system settings information, when a misoperation or other situation causes the wireless router's system settings information to be lost, you can restore the current settings to the previous backup settings, ensure the normal operation of the wireless router, and reduce the information loss, Backing up system setup information also helps with failure analysis.



Backup Settings

Backup the Router configurations.You may save your router configurations to a file on your PC.

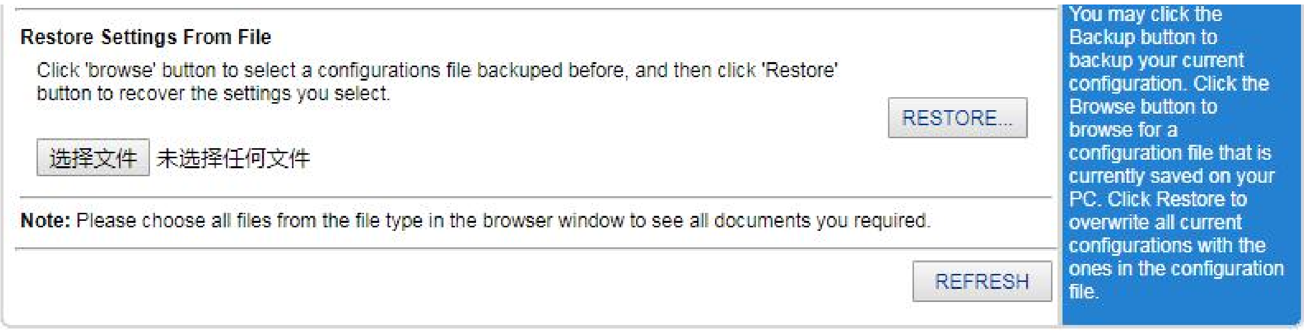
You may backup your current configuration.

Click <Backup> button, select the backup path of the setting information, click <OK> to save the current setting information of the wireless router to the computer, so that it can be restored later through the file (suffixed with .cfg).

Restore settings from file

You can restore your current settings to the settings you have previously backed up.

Note: The current settings will be lost after the settings are restored. If you do not wish to lose your current settings, please be careful to make a backup. About the backup method, refer to "5.11.3.1 Backing Up System Settings Information."



Restore Settings From File

Click 'browse' button to select a configurations file backuped before, and then click 'Restore' button to recover the settings you select.

Note: Please choose all files from the file type in the browser window to see all documents you required.

You may click the Backup button to backup your current configuration. Click the Browse button to browse for a configuration file that is currently saved on your PC. Click Restore to overwrite all current configurations with the ones in the configuration file.

Click the <Select file> button, select a previously backed up file (*.cfg) on the computer, and then click the <Restore> button to restore the settings to the state of the backup file.

Wireless router will restart during recovery setup.

5.11.4 Firmware Upgrade

You can load the latest version of the software into your router for more features and more stable performance.

Upgrade step:

Step1: Click the <Select file> button and select the software to be upgraded.

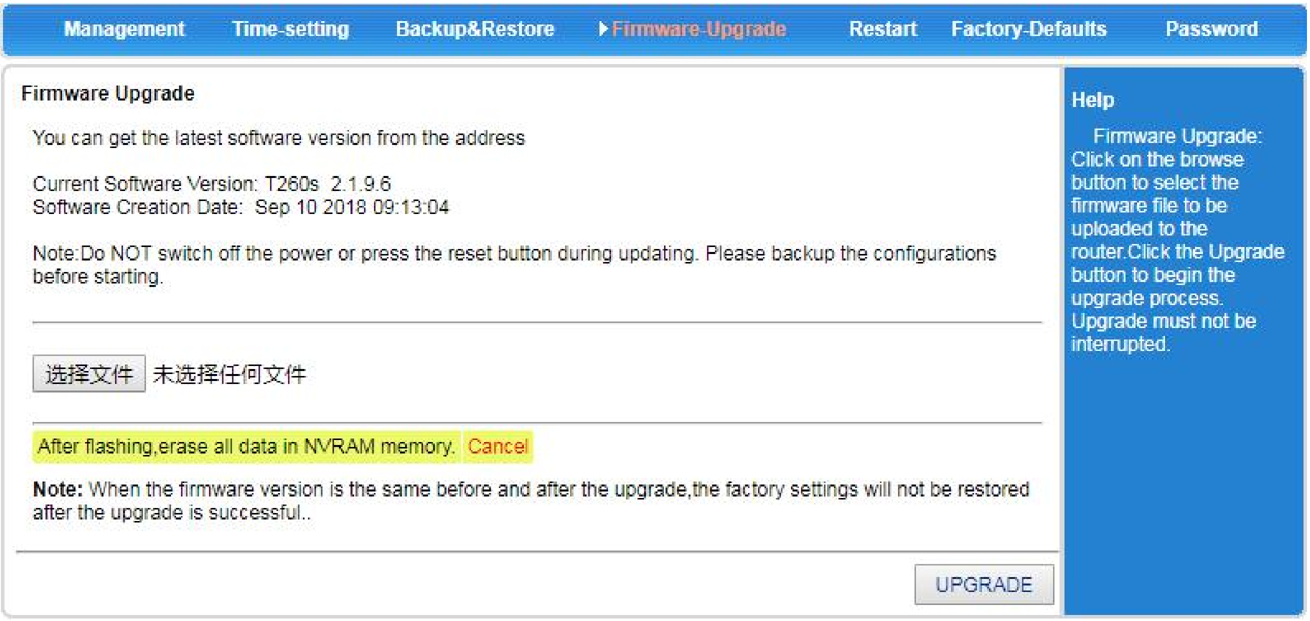
Step2: Click the <Upgrade> button to start the upgrade.

Step3: If you need to upgrade and restore the factory, click the <Factory-Defaults> button.

Note: The upgrade and factory reset must meet two conditions at the same time.

(1).Version number changes.

(2).Click the <Factory-Defaults> button during the upgrade.



Firmware Upgrade

You can get the latest software version from the address

Current Software Version: T260s 2.1.9.6
Software Creation Date: Sep 10 2018 09:13:04

Note:Do NOT switch off the power or press the reset button during updating. Please backup the configurations before starting.

选择文件 未选择任何文件

After flashing,erase all data in NVRAM memory. Cancel

Note: When the firmware version is the same before and after the upgrade,the factory settings will not be restored after the upgrade is successful..

UPGRADE

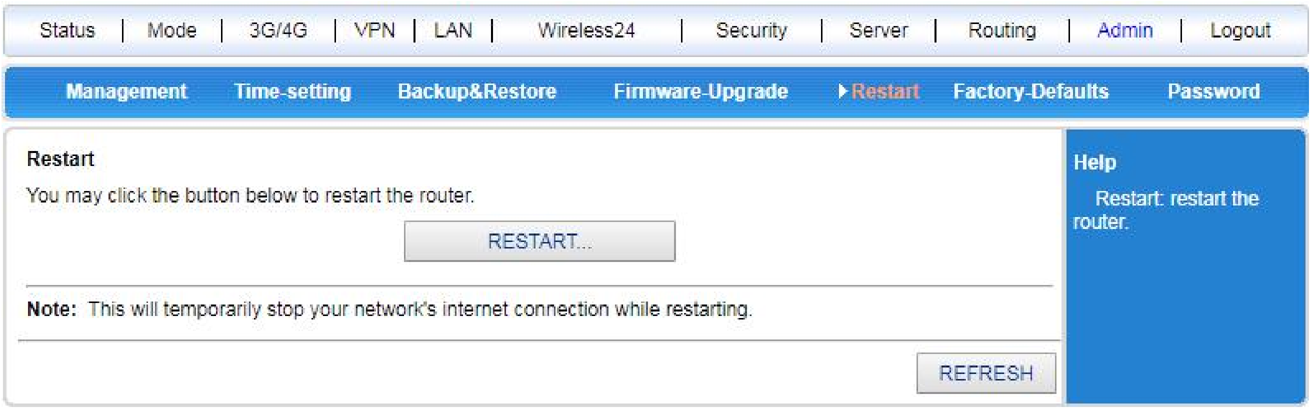
Help

Firmware Upgrade: Click on the browse button to select the firmware file to be uploaded to the router.Click the Upgrade button to begin the upgrade process. Upgrade must not be interrupted.

5.11.5 Restart

Note: Do not power off during restart.

Network communication will be temporarily interrupted during the restart.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Management
Time-setting
Backup&Restore
Firmware-Upgrade
▸Restart
Factory-Defaults
Password

Restart

You may click the button below to restart the router.

RESTART...

Note: This will temporarily stop your network's internet connection while restarting.

REFRESH

Help

Restart: restart the router.

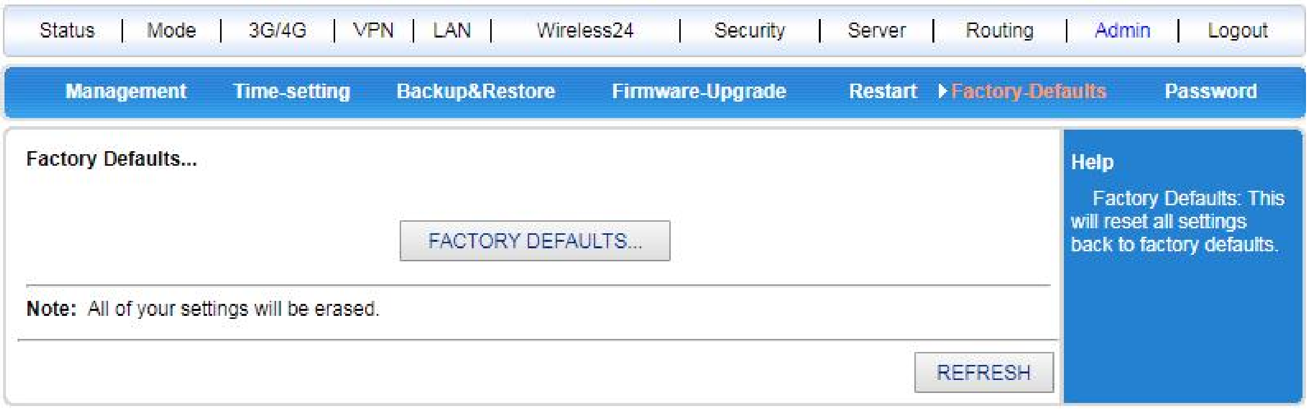
Click the <Restart> button and the wireless router restarts.

5.11.6 Factory-Defaults

Description:

- The current settings will be lost when the settings are restored. If you do not wish to lose your current settings, please be careful to make a backup. For the backup method, refer to "5.11.3.1 Backup Settings".
- The wireless router will reboot during the recovery setup.

Restoring to the factory settings will clear all settings information of the wireless router and return to the initial state. This function is generally used when the device is switched from one network environment to another. The device is restored to the factory settings and then re-set to better suit the current networking.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Management Time-setting Backup&Restore Firmware-Upgrade Restart Factory-Defaults Password
FACTORY DEFAULTS...
REFRESH

Factory Defaults...

Note: All of your settings will be erased.

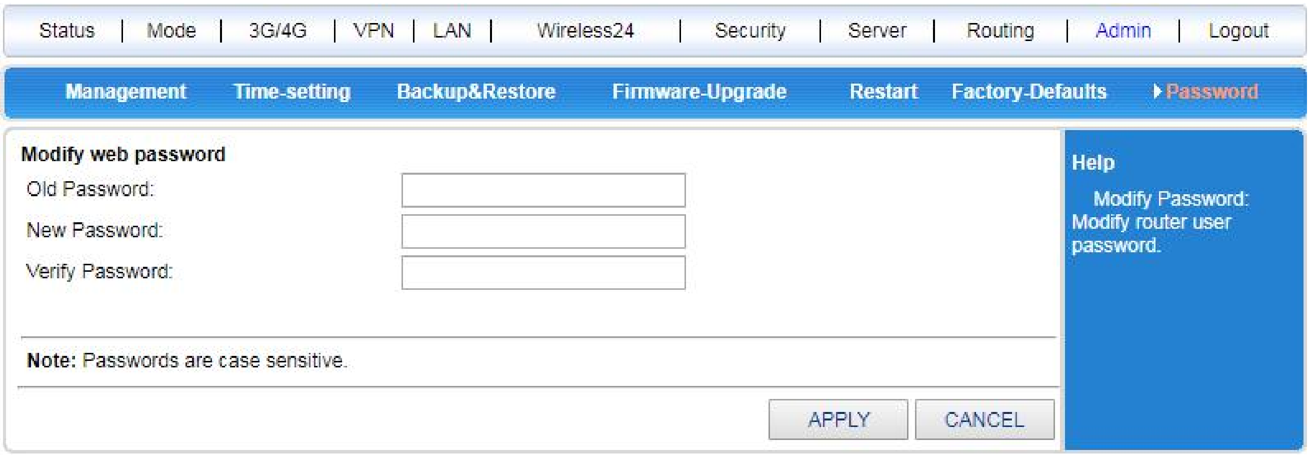
Help

Factory Defaults: This will reset all settings back to factory defaults.

Click the <Factory Defaults> button and confirm to restore the factory settings.

5.11.7 Password

Default username/password is admin, cannot be modified, password can be modified, maximum support 16 bits. For security reasons, please modify this password and save it.


Status | Mode | 3G/4G | VPN | LAN | Wireless24 | Security | Server | Routing | Admin | Logout
Management Time-setting Backup&Restore Firmware-Upgrade Restart Factory-Defaults Password
APPLY
CANCEL

Modify web password

Old Password:

New Password:

Verify Password:

Note: Passwords are case sensitive.

Help

Modify Password: Modify router user password.

Set as follows:

Step1: Enter the original password in the <Old Password> text box; enter the new password in the <New Password> text box, and re-enter the new password in the <Verify Password> text box to confirm.

Step2: Click the <APPLY> button to complete the password modification.

6. Warranty

1) This device is warranted to be free of defects in material and workmanship for one year.

2) This warranty does not extend to any defect, malfunction or failure caused by abuse or misuse by the Operating Instructions. In no event shall the manufacturer be liable for any router altered by purchasers.

The End!
Any questions please help to contact us feel free.
Http://www.IOT-SOLUTION.com