TW-LTE/4G/3G

WLAN 802.11ac

Router

User Manual

Directory

Introduction

Introduction to your Router

TW-LTE/4G/3G WLAN 802.11ac Router is a residential/small office gateway, especially designed for those who need to have the data, video and file sharing services beyond his home and office.
It is an all-in-one advanced device integrating Wireless, Ethernet, 3G/4G/LTE, and NAS (Network Attached Storage) in one unit. As well as being IPv6-capable, the router supports super-fast fiber connections via dual-WAN connectivity through a Gigabit Ethernet WAN port. Also, it also has a USB port, allowing the device to act as a print server as well as a NAS (Network Attached Storage) device. Moreover, the USB port can host a 3G/4G/LTE modem connecting to the 3G/4G/LTE network for Internet access.

Maximum wireless performance
With an integrated 802.11ac Wireless Access Point, The device supports a data rate of up to 750 Mbps and is also compatible with 802.11b/g/n/ac equipment

The Wireless Protected Access (WPA-PSK/WPA2-PSK) and Wireless Encryption Protocol (WEP) features enhance the level of transmission security and access control over wireless LAN. The router also supports the Wi-Fi Protected Setup (WPS) standard, allowing users to establish a secure wireless network by simply pushing a button. If your network requires wider coverage, the built-in Wireless Distribution System (WDS) repeater function allows you to expand your wireless network without the need for any external wires or cables.

3G/4G/LTE Mobility and Always-on Connectivity
With 3G/4G/LTE-based Internet connection (requires an additional 3G/4G/LTE USB modem plugged into the built-in USB port), user can access Internet through 3G/4G/LTE, whether you are seated at your desk or taking a cross-country trip. The auto fail-over feature ensures optimum connectivity and minimum interruption by quickly and smoothly connecting to a 3G/4G/ LTE network in the event that you ADSL/Fiber/Cable line fails. The device will then

automatically reconnect to the ADSL/Fiber/Cable connection when it is restored, reducing connection costs. These features are perfect for office situations when a constant and smooth WAN connection is critical.

IPv6 supported

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol that is designed to succeed IPv4. IPv6 has a vastly larger address space than IPv4. This results from the use of a 128-bit address, whereas IPv4 uses only 32 bits. The new address space thus supports 2128 (about 3.4×1038) addresses. This expansion provides flexibility in allocating addresses and routing traffic and eliminates the primary need for network address translation (NAT), which gained widespread deployment as an effort to alleviate IPv4 address exhaustion.

The device fully supports IPv6 (Internet Protocol Version 6), launched as the current IPv4 range is filling up, and IPv6 is gradually becoming the indispensable addressing system for savvy cloud computing users. Dual stack means the router is capable of running IPv4 and IPv6 in parallel during the transition period. With TeleWell IPv6 enabled devices.

Virtual AP

A “Virtual Access Point” is a logical entity that exists within a physical Access Point (AP). When a single physical AP supports multiple “Virtual APs”, each Virtual AP appears to stations (STAs) to be an independent physical AP, even though only a single physical AP is present. For example, multiple Virtual APs might exist within a single physical AP, each advertising a distinct SSID and capability set. Alternatively, multiple Virtual APs might advertise the same SSID but a different capability set – allowing access to be provided via Web Portal, WEP, and WPA simultaneously. Where APs are shared by multiple providers, Virtual APs provide each provider with separate authentication and accounting data for their users, as well as diagnostic information, without sharing sensitive management traffic or data between providers. You can enable the virtual AP.

Web Based GUI

It supports web based GUI for configuration and management. It is user-friendly and comes with online help. It also supports remote management capability for remote users to configure and manage this product.

Firmware Upgradeable

Device can be upgraded to the latest firmware through the WEB based GUI.

Features

Network Protocols and Features

- IPv4 or IPv4 / IPv6 Dual Stack
- Dual WAN and load sharing
- NAT, DMZ and ALG
- IPv6 Stateless / Stateful Address Auto-configuration
- IPv6 Router Advertisement
- DHCPv6
- Static Route and Policy Route
- Universal Plug and Play (UPnP) Compliant
- Dynamic Domain Name System (DDNS)
- Virtual Server, DMZ and one-to-one NAT
- SNTP, DNS relay, IGMP snooping and IGMP proxy for video service
- Management based-on IP protocol, port number and address

Firewall

- Built-in NAT Firewall
- Stateful Packet Inspection (SPI)
- DoS attack prevention
- Packet Filtering (v4/v6) - port, source IP address, destination IP address, MAC address
- URL Content Filtering (v4/v6) – string or domain name detection in URL string
- Wireless MAC Filtering

Quality of Service Control

- Supports the DiffServ approach
- Traffic prioritization and bandwidth management based-on IPv4 protocol, port number and address

IPTV Applications

- IGMP Snooping and IGMP Proxy
- Quality of Service (QoS)

Wireless LAN

- Compliant with
    - IEEE 802.11 b/g/n/ac standards
    - 2.4 and 5G radio bands for wireless
    - Up to 300 Mbps (11n) and 450Mbps (11ac) wireless operation rate

- 64/128 bits WEP supported for encryption
- WPS (Wi-Fi Protected Setup) for easy setup
- Wireless Security with WPA-PSK / WPA2-PSK support
- WDS repeater function support

USB Application Server

- 3G/4G/LTE dongle support
- FTP/Samba server
- Printer Server

Virtual Private Network (VPN)

- PPTP Client/Server
- L2TP Client/Server
- PAP / CHAP/ MS-CHAPv2 authentication for PPTP
- GRE tunnel

Management

- Web-based GUI for remote and local management (IPv4/IPv6)
- Firmware upgrades and configuration data upload and download via web-based GUI
- Embedded Telnet server for remote and local management
- Supports DHCP server / client
- Available Syslog
- Mail alert for WAN IP changed

Physical Interface

- Ethernet: 1 WAN-port 10/100/1000 Mbps auto-crossover (MDI / MDI-X) Switch
- Ethernet: 4 LAN-port 10/100/1000 Mbps auto-crossover (MDI / MDI-X) Switch
- WPS / Factory default reset button
- Power jack
- Power switch
- USB 2.0 port for storage, printer server and 3G/4G/LTE dongle
- WLAN: 3 x 5 dBi external antenna

Package Contents

- TW-LTE/4G/3G WLAN 802.11ac Router
- User Manual
- RJ-45 Cat. 5e STP Ethernet cable
- Power adapter

Important note for using this router

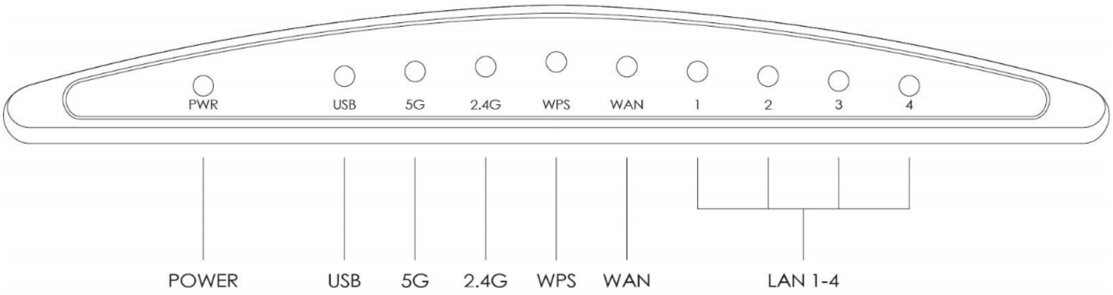
Do not use the router in high humidity or high temperatures
Do not use the same power source for the router as other equipment.
Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
Avoid using this product and all accessories outdoors

Warning

Do not use the router in high humidity or high temperatures.
Do not use the same power source for the router as other equipment.
Do not open or repair the case yourself. If the router is too hot, turn off the power immediately and have it repaired at a qualified service center.
Avoid using this product and all accessories outdoors.
Place the router on a stable surface.
Only use the power adapter that comes with the package. Using a different voltage rating power adapter may damage the router.

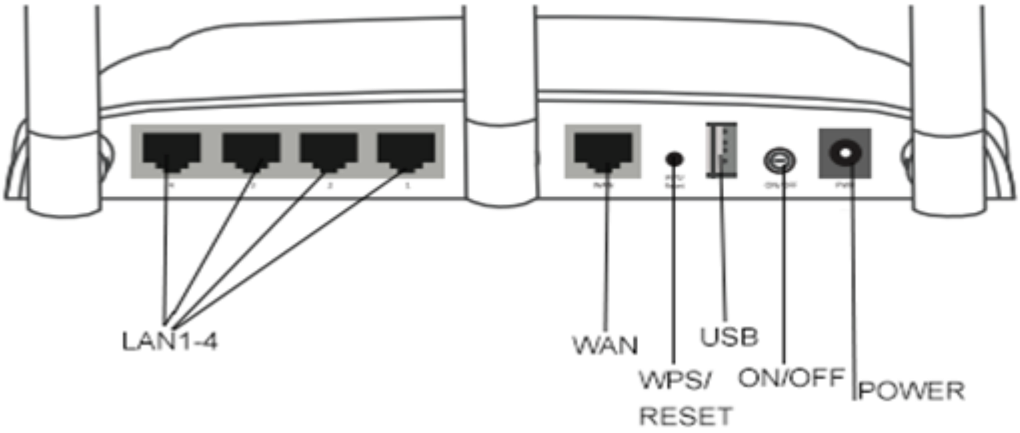
Device Description

The Front LEDs



LED	Status	Meaning
Power	Green	Power cable connected
USB	Green	When any USB device is attached
5G 2.4G	Green	Wireless module is ready and work.
	Green blinking	Sending/receiving data
WPS	Green blinking	WPS configuration being in progress
	Off	WPS process completed or WPS is off
WAN LAN 1-4	Green	Ethernet Cable connected
	Blinking	Data being transmitted/received

The Rear Ports



Port	Meaning
LAN1-4	Connect a UTP Ethernet cable (Cat-5 or Cat-5e) to one of the LAN ports when connecting to a PC or an office/home network.
WAN	Connect Ethernet cable for WAN connections
WPS / RESET	**WPS:** Press and release quickly to enable the WPS function. **RESET:** Power on device and wait for 60 seconds, then press it 5 seconds or above to restore to factory default settings.
USB	Connect the USB device (Storage, Printer, 3G/4G LTE USB modem) to this port.
ON / OFF	Power ON / OFF switch.
Power	Connect the supplied power adapter to this jack.

Basic Installation

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 8 / 7 / 98 / NT / 2000 / XP / Me / Vista, etc. The product provides an easy and user-friendly interface for configuration.

Please check your PC network components. The TCP/IP protocol stack and Ethernet network adapter must be installed. If not, please refer to your Windows-related or other operating system manuals.

There are ways to connect the router, either through an external repeater hub or connect directly to your PCs. However, make sure that your PCs have an Ethernet interface installed properly prior to connecting the router device. You ought to configure your PCs to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The default IP address of the router is 192.168.0.254 and the subnet mask is 255.255.255.0 (i.e. any attached PC must be in the same subnet, and have an IP address in the range of 192.168.0.1 to 192.168.0.253).

The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problem accessing the router web interface it is advisable to uninstall your firewall program on your PCs, as they can cause problems accessing the IP address of the router. Users should make their own decisions on what is best to protect their network.

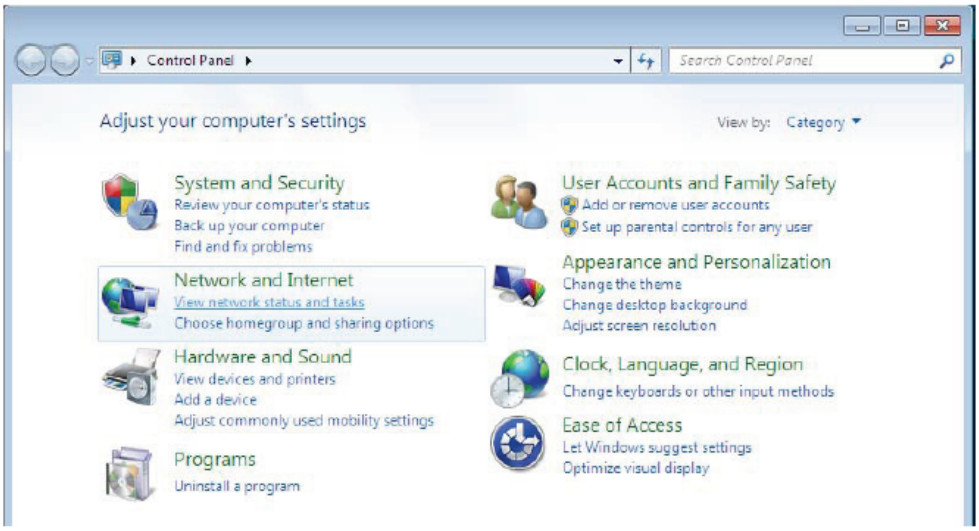
Please follow the following steps to configure your PC network environment.

Any TCP/IP capable workstation can be used to communicate with or through this router. To configure other types of workstations, please consult your manufacturer documentation.

Network Configuration

Configuring a PC in Windows 7 / 8 / 8.1 / 10

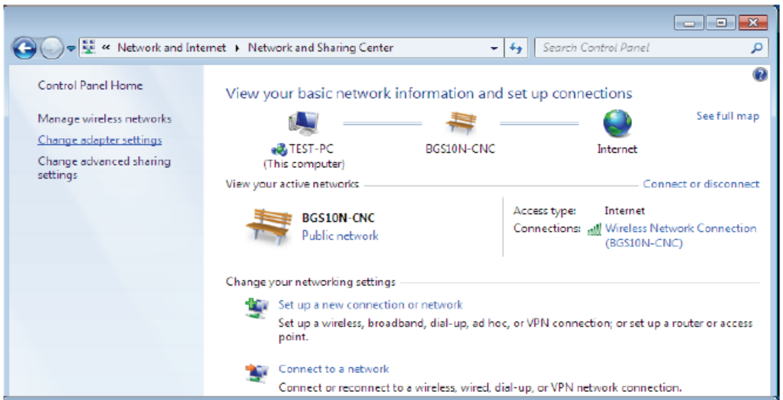
Go to Start. Click on Control Panel. Then click on Network and Internet.

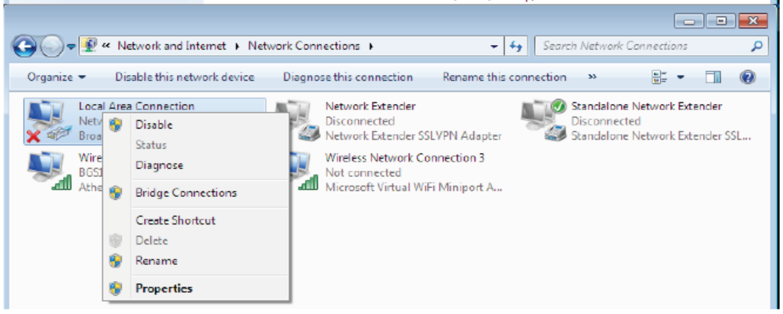

Control Panel
Search Control Panel
Adjust your computer's settings
View by: Category
System and Security
Review your computer's status
Back up your computer
Find and fix problems
Network and Internet
View network status and tasks
Choose homegroup and sharing options
Hardware and Sound
View devices and printers
Add a device
Adjust commonly used mobility settings
Programs
Uninstall a program
User Accounts and Family Safety
Add or remove user accounts
Set up parental controls for any user
Appearance and Personalization
Change the theme
Change desktop background
Adjust screen resolution
Clock, Language, and Region
Change keyboards or other input methods
Ease of Access
Let Windows suggest settings
Optimize visual display

When the Network and Sharing Center window pops up, select and click on Change adapter settings on the left window panel.

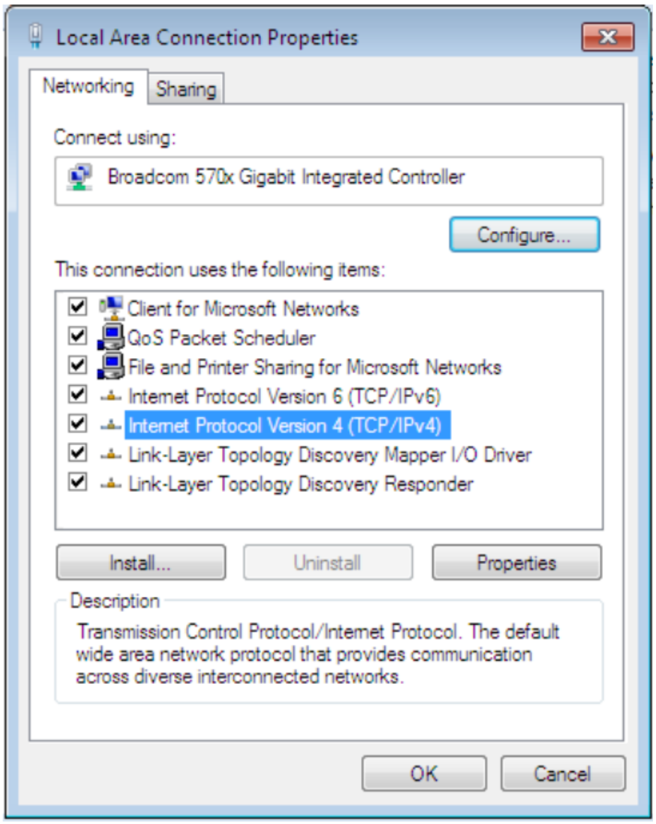
Select the Local Area Connection, and right click the icon to select Properties.

IPv4:


« Network and Internet ▸ Network and Sharing Center
Search Control Panel
Control Panel Home
Manage wireless networks
Change adapter settings
Change advanced sharing settings
View your basic network information and set up connections
See full map
TEST-PC
(This computer)
BGS10N-CNC
Internet
View your active networks
Connect or disconnect
BGS10N-CNC
Public network
Access type: Internet
Connections: Wireless Network Connection (BGS10N-CNC)
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.


« Network and Internet ▸ Network Connections ▸
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
»
Local Area Connection
Netw
Broa
Wire
BGS1
Athe
Disable
Status
Diagnose
Bridge Connections
Create Shortcut
Delete
Rename
Properties
Network Extender
Disconnected
Network Extender SSLVPN Adapter
Wireless Network Connection 3
Not connected
Microsoft Virtual WiFi Miniport A...
Standalone Network Extender
Disconnected
Standalone Network Extender SSL...

Select Internet Protocol Version 4 (TCP/IPv4) then click Properties.



Connect using:

Broadcom 570x Gigabit Integrated Controller

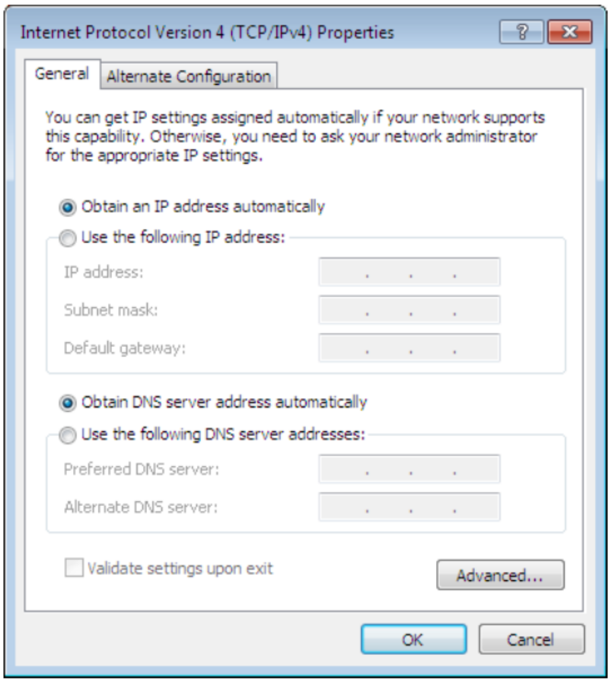
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ 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

Description

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

In the TCP/IPv4 properties window, select the Obtain an IP address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.



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:

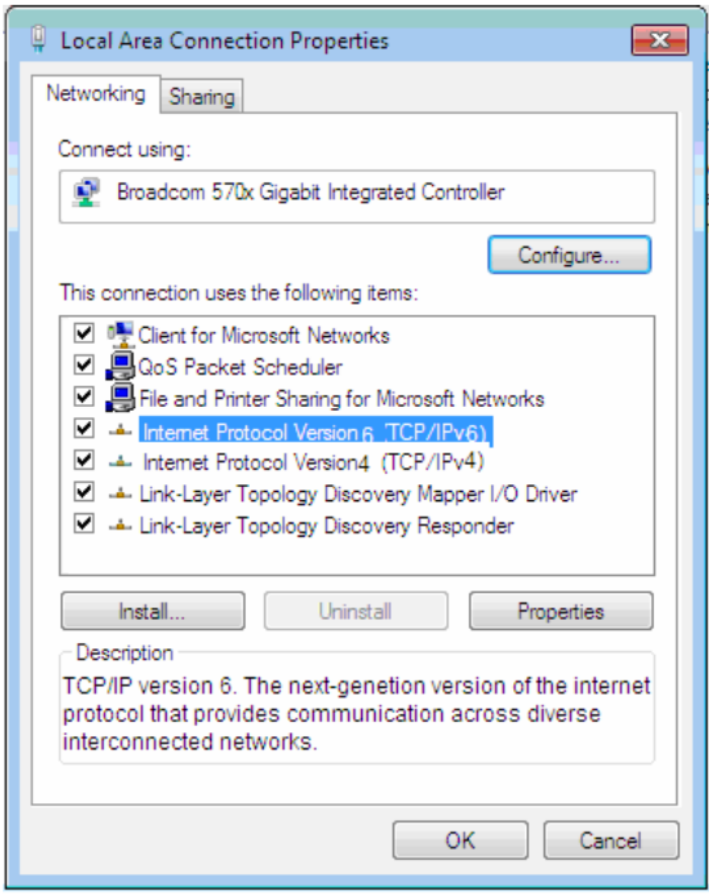
Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

IPv6:

Select Internet Protocol Version 6 (TCP/IPv6) then click Properties



Connect using:

Broadcom 570x Gigabit Integrated Controller

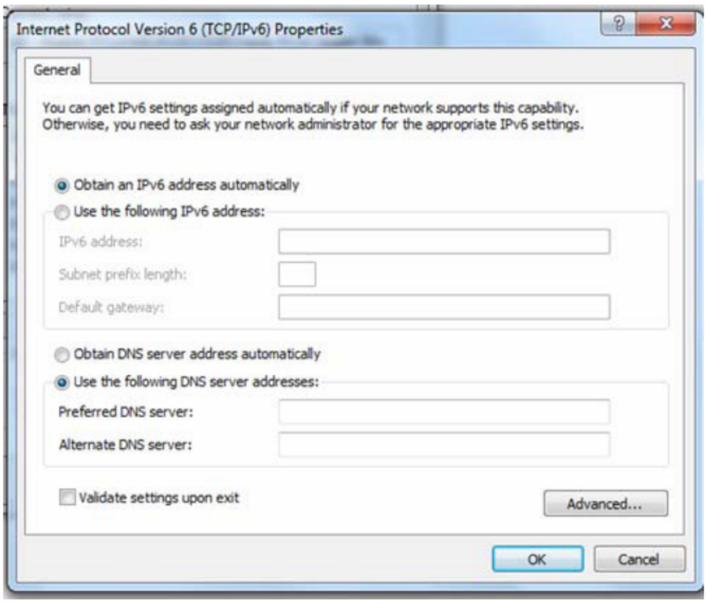
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

TCP/IP version 6. The next-genetion version of the internet protocol that provides communication across diverse interconnected networks.

In the TCP/IPv6 properties window, select the Obtain an IPv6 address automatically and Obtain DNS Server address automatically radio buttons. Then click OK to exit the setting. Click OK again in the Local Area Connection Properties window to apply the new configuration.



You can get IPv6 settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IPv6 settings.

● Obtain an IPv6 address automatically

○ Use the following IPv6 address:

IPv6 address:

Subnet prefix length:

Default gateway:

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Factory Default Settings

Before configuring your router, you need to settings.

Web Interface (Username and Password)

Administrator
Username: hallinta
Password: saimaa

Attention
If you have forgotten the username and/or password of the router, you can restore the device to its default setting by pressing the Reset Button more than 5 seconds.

Device LAN IPv4 settings

- IPv4 Address: 192.168.0.254
- Subnet Mask: 255.255.255.0

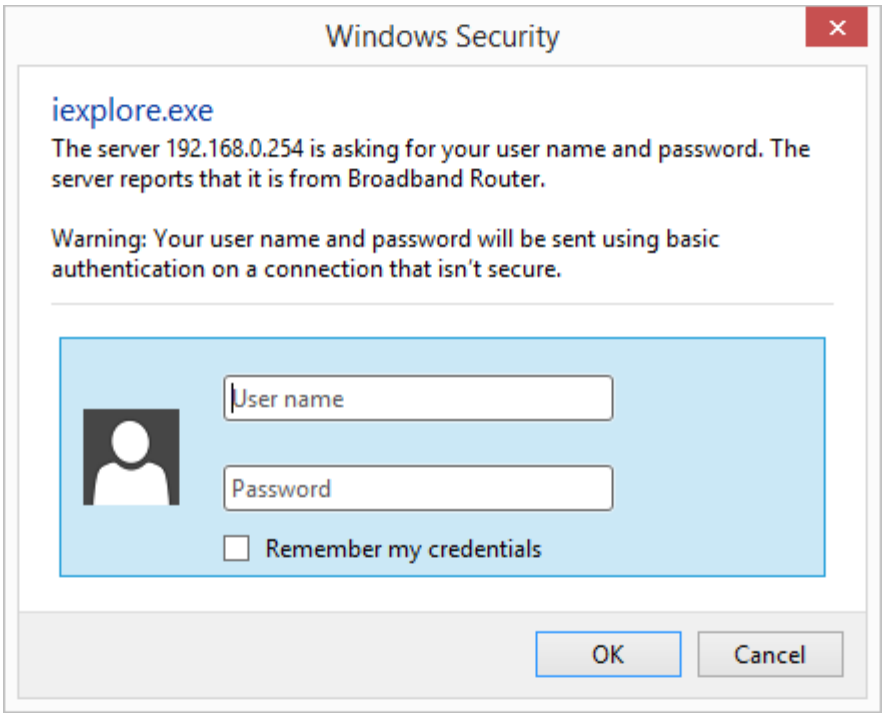
DHCP server for IPv4

- DHCP server is enabled
- Start IP Address: 192.168.0.100
- IP pool counts: 100

Configuration

Configuration via Web Interface

Open your web browser; enter the IP address of your router, which by default is 192.168.0.254, and click ok or press ‘Enter’ key on the keyboard, a login prompt window will appear. The default root username and password are “hallinta” and “saimaa” respectively.



Windows Security

iexplore.exe

The server 192.168.0.254 is asking for your user name and password. The server reports that it is from Broadband Router.

Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.

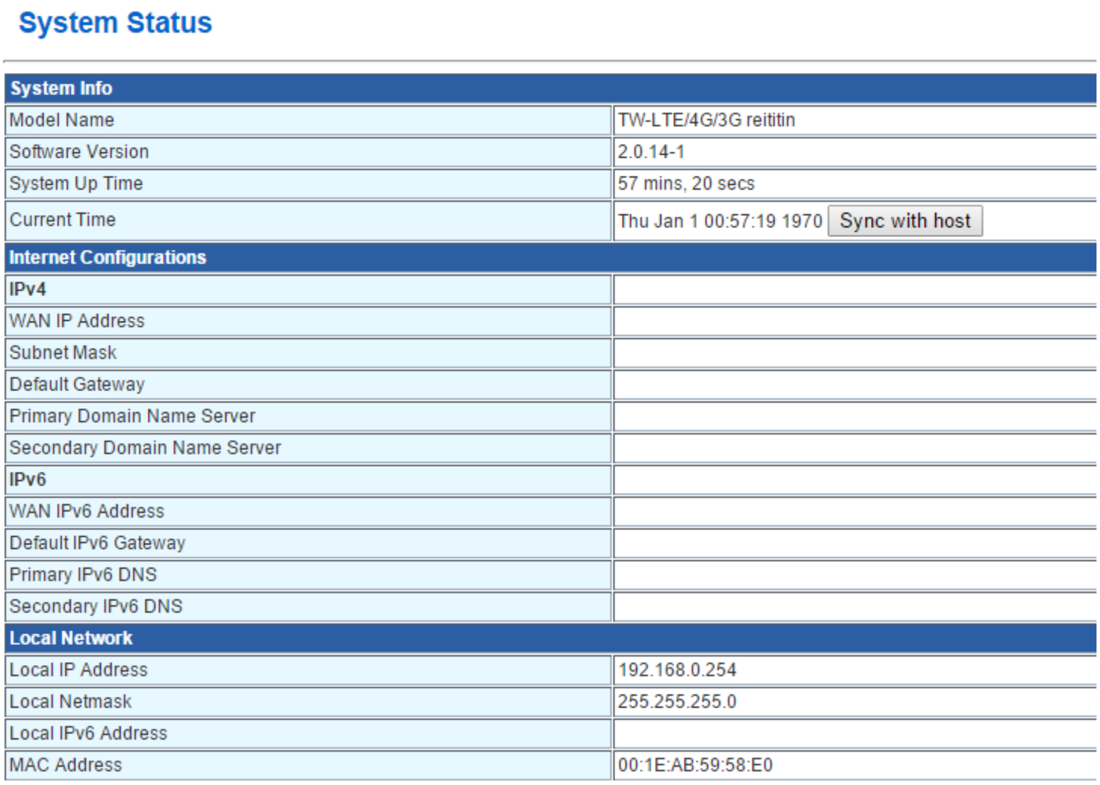
Congratulations! You are now successfully logged in to the Firewall Router!

Once you have logged on to your TeleWell TW-LTE/4G/3G WLAN 802.11ac Router via your web browser, you can begin to set it up according to your requirements. On the configuration homepage, the left navigation pane links you directly to the setup pages, which include:

Information

Status

The page below shows the basic system and WAN connection information.

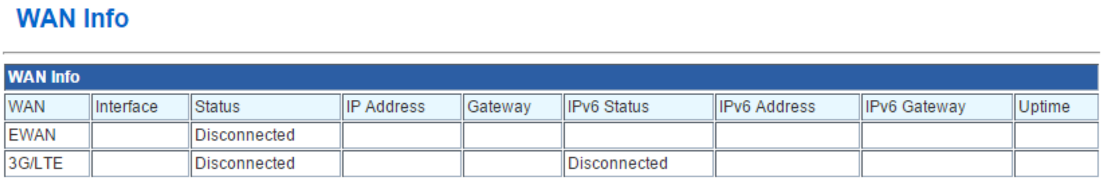


System Status

System Info	
Model Name	TW-LTE/4G/3G reititin
Software Version	2.0.14-1
System Up Time	57 mins, 20 secs
Current Time	Thu Jan 1 00:57:19 1970 Sync with host
Internet Configurations	
IPv4	
WAN IP Address	
Subnet Mask	
Default Gateway	
Primary Domain Name Server	
Secondary Domain Name Server	
IPv6	
WAN IPv6 Address	
Default IPv6 Gateway	
Primary IPv6 DNS	
Secondary IPv6 DNS	
Local Network	
Local IP Address	192.168.0.254
Local Netmask	255.255.255.0
Local IPv6 Address	
MAC Address	00:1E:AB:59:58:E0

WAN

More details of WAN information can be found here, like WAN status, gateway and Uptime.

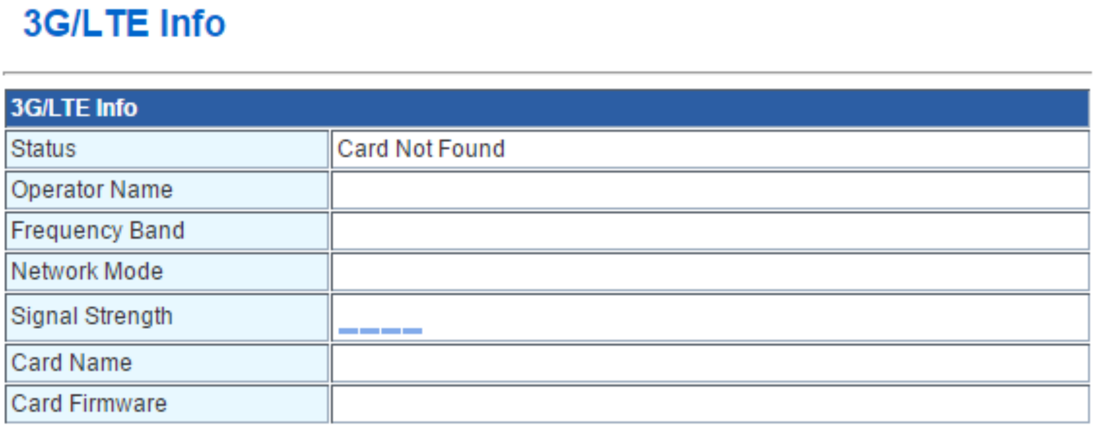


WAN Info

WAN Info								
WAN	Interface	Status	IP Address	Gateway	IPv6 Status	IPv6 Address	IPv6 Gateway	Uptime
EWAN		Disconnected						
3G/LTE		Disconnected			Disconnected			

3G/LTE Info

Details of 3G/4G dongle information will be shown here once dongle detected correctly by router.

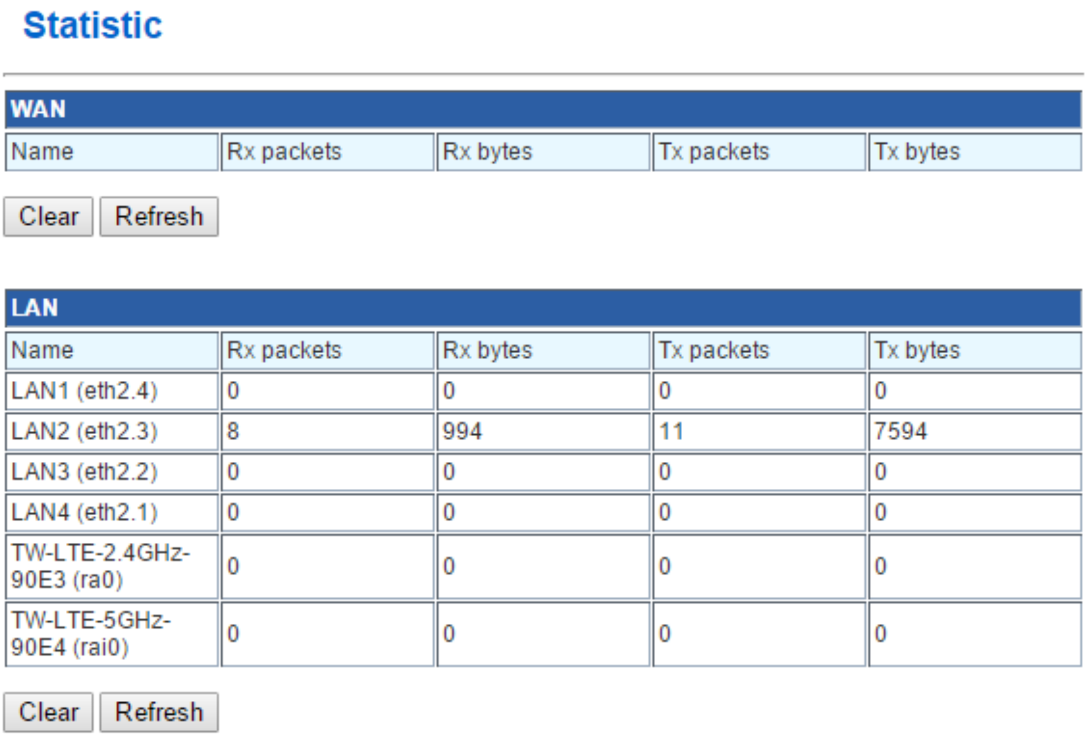


3G/LTE Info

3G/LTE Info	
Status	Card Not Found
Operator Name	
Frequency Band	
Network Mode	
Signal Strength	▬▬▬▬
Card Name	
Card Firmware	

Statistics

This page shows the statistics of each hardware interface. Click ***Clear*** button to reset counter.



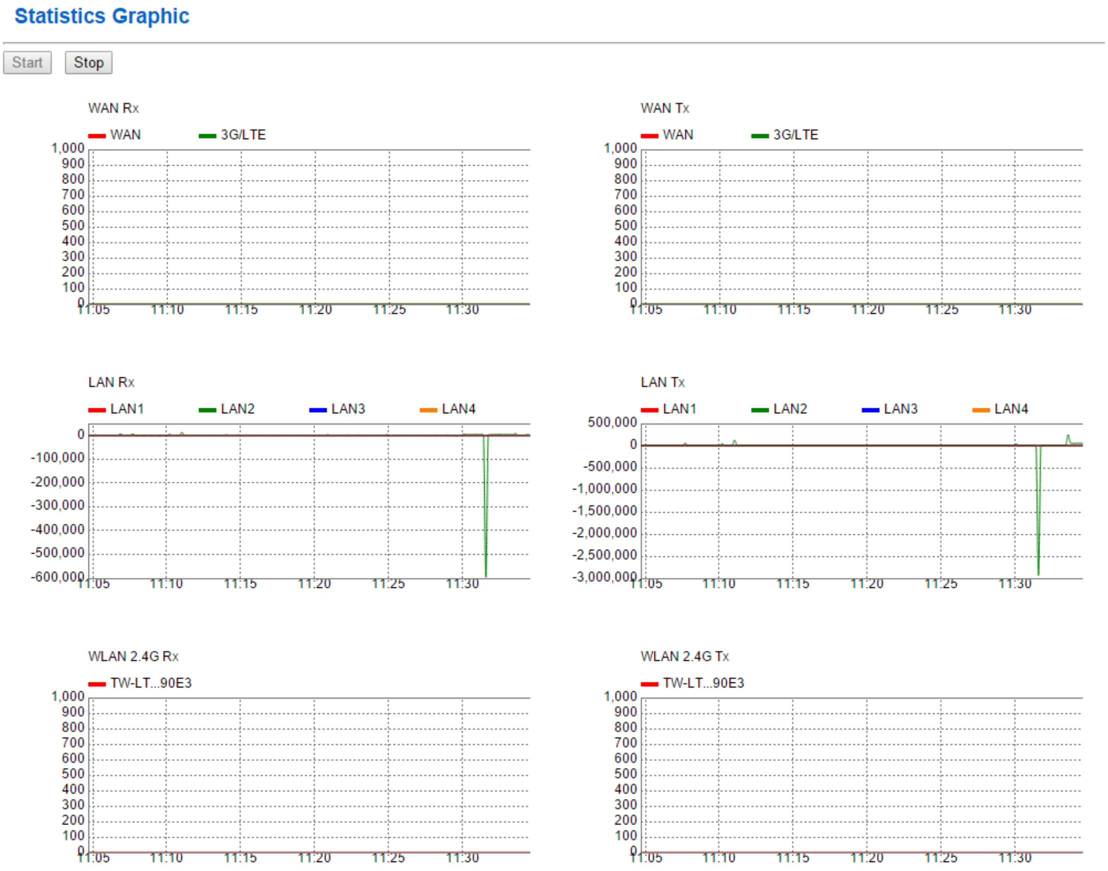
Statistic

WAN				
Name	Rx packets	Rx bytes	Tx packets	Tx bytes

LAN				
Name	Rx packets	Rx bytes	Tx packets	Tx bytes
LAN1 (eth2.4)	0	0	0	0
LAN2 (eth2.3)	8	994	11	7594
LAN3 (eth2.2)	0	0	0	0
LAN4 (eth2.1)	0	0	0	0
TW-LTE-2.4GHz-90E3 (ra0)	0	0	0	0
TW-LTE-5GHz-90E4 (rai0)	0	0	0	0

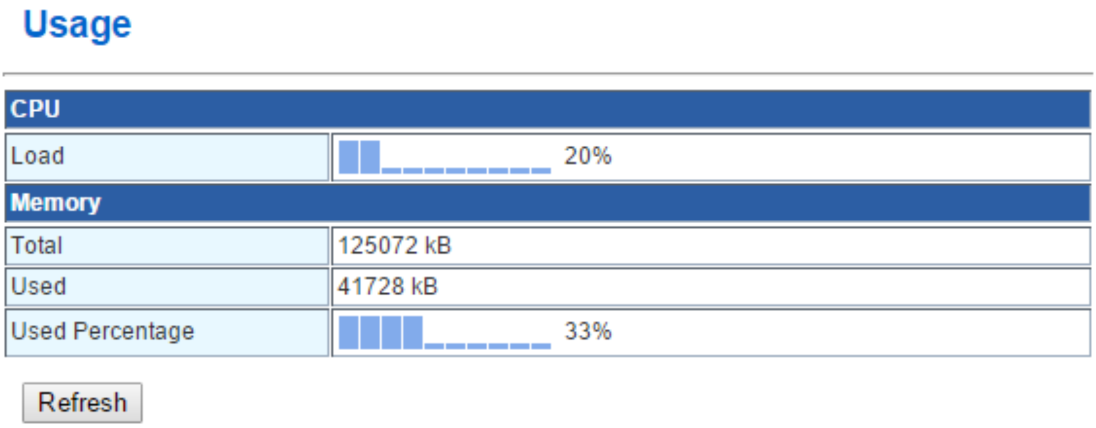
Graphic

The router also supports to show statistics with graphic display.



Usage

The usage of CPU and memory can be found here.

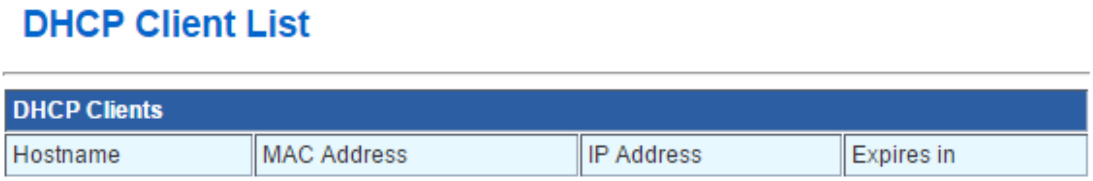


Usage

CPU	
Load	20%
Memory	
Total	125072 kB
Used	41728 kB
Used Percentage	33%

DHCP Clients

The PC which gets dynamic IP address from router will be displayed here.

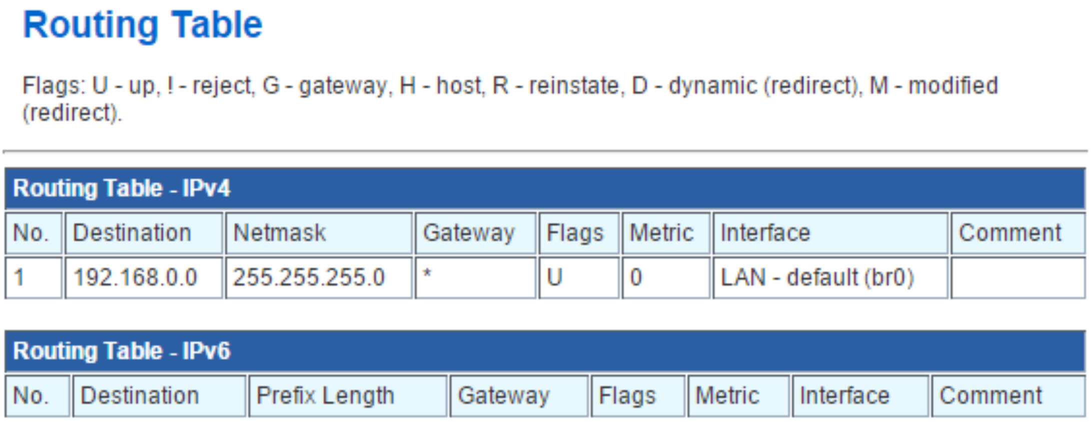


DHCP Client List

DHCP Clients			
Hostname	MAC Address	IP Address	Expires in

Routing

Details of all routing rules can be found here.



Routing Table

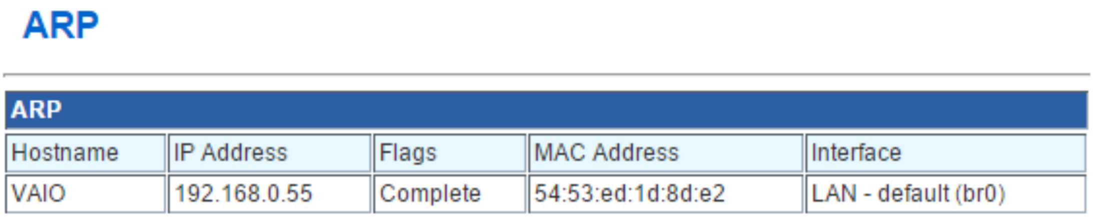
Flags: U - up, ! - reject, G - gateway, H - host, R - reinstate, D - dynamic (redirect), M - modified (redirect).

Routing Table - IPv4							
No.	Destination	Netmask	Gateway	Flags	Metric	Interface	Comment
1	192.168.0.0	255.255.255.0	*	U	0	LAN - default (br0)	

Routing Table - IPv6							
No.	Destination	Prefix Length	Gateway	Flags	Metric	Interface	Comment

ARP

Details of ARP information can be found here.



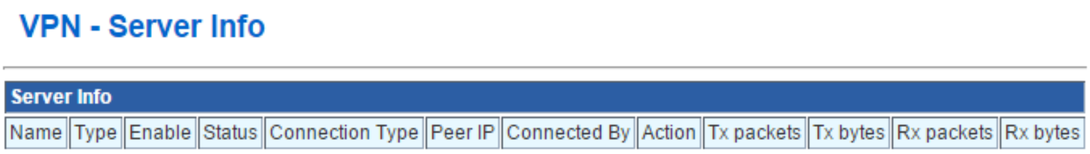
ARP

ARP				
Hostname	IP Address	Flags	MAC Address	Interface
VAIO	192.168.0.55	Complete	54:53:ed:1d:8d:e2	LAN - default (br0)

VPN

All details of VPN connection information can be found in this section.

PPTP/L2TP Server Information

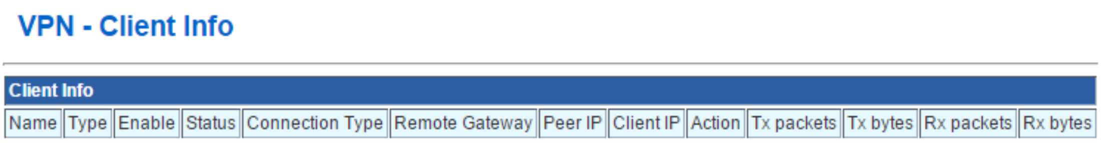


VPN - Server Info

Server Info

Name	Type	Enable	Status	Connection Type	Peer IP	Connected By	Action	Tx packets	Tx bytes	Rx packets	Rx bytes

PPTP/L2TP Client Information

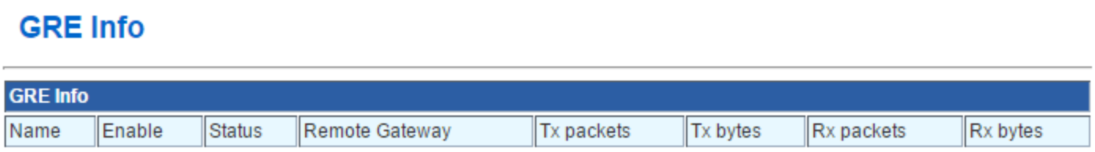


VPN - Client Info

Client Info

Name	Type	Enable	Status	Connection Type	Remote Gateway	Peer IP	Client IP	Action	Tx packets	Tx bytes	Rx packets	Rx bytes

GRE Tunnel Information



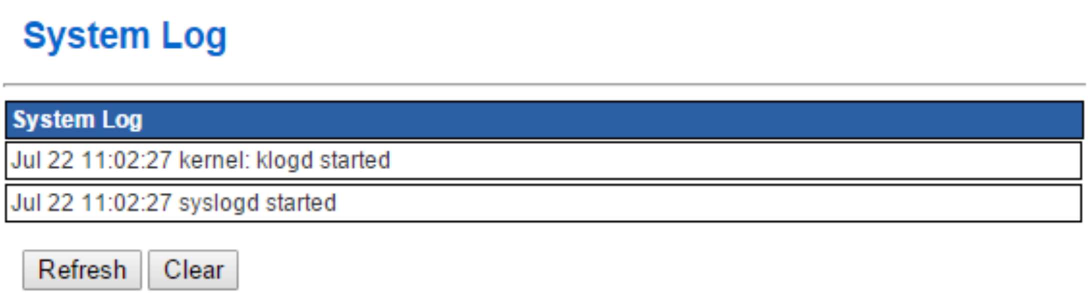
GRE Info

GRE Info

Name	Enable	Status	Remote Gateway	Tx packets	Tx bytes	Rx packets	Rx bytes

System Log

System log to help you to know what happens on your router.



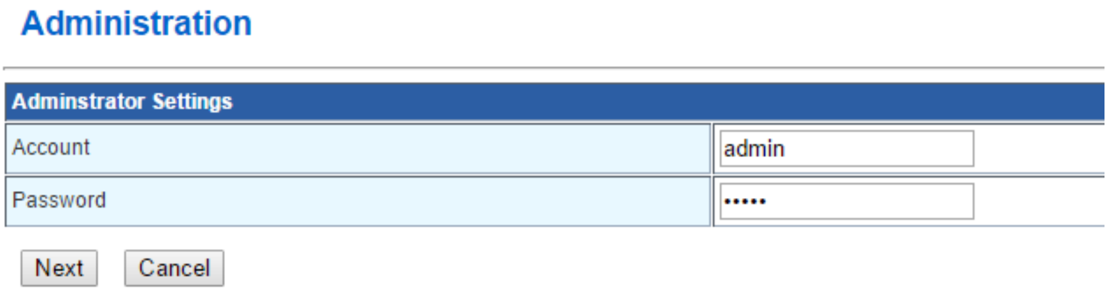
System Log

System Log

```
Jul 22 11:02:27 kernel: klogd started
Jul 22 11:02:27 syslogd started
```

Quick Setup

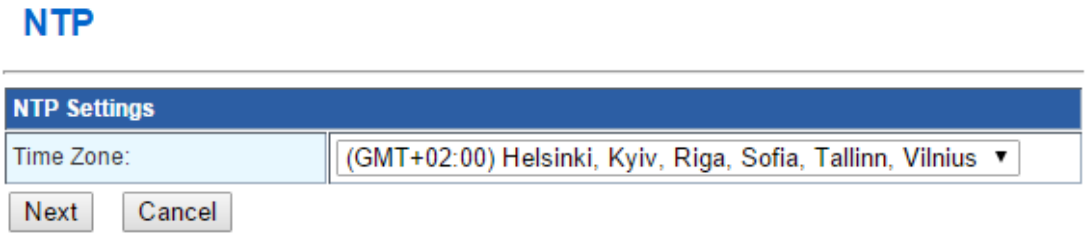
Quick Setup can guide you to setup your router step by step.



Administration

Adminstrator Settings	
Account	admin
Password	•••••

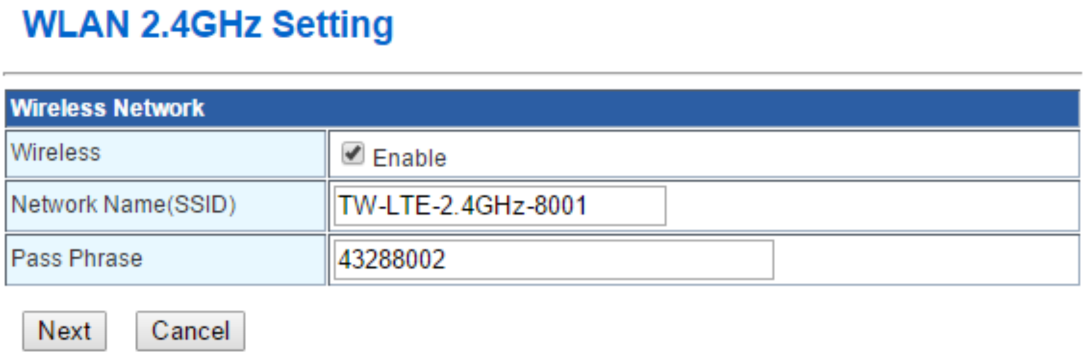
It is better to change default administrator username/password at first login.



NTP

NTP Settings	
Time Zone:	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius ▼

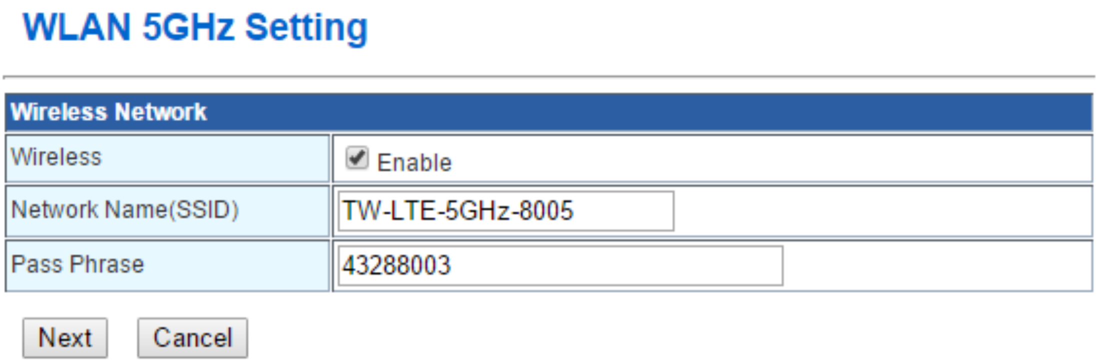
Setup your Time Zone to make system to sync with local time.



WLAN 2.4GHz Setting

Wireless Network	
Wireless	☑ Enable
Network Name(SSID)	TW-LTE-2.4GHz-8001
Pass Phrase	43288002

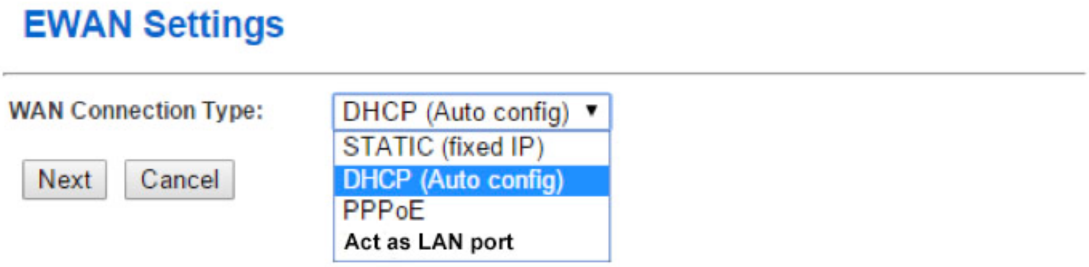
Setup SSID and WiFi key for wireless 2.4G.



WLAN 5GHz Setting

Wireless Network	
Wireless	☑ Enable
Network Name(SSID)	TW-LTE-5GHz-8005
Pass Phrase	43288003

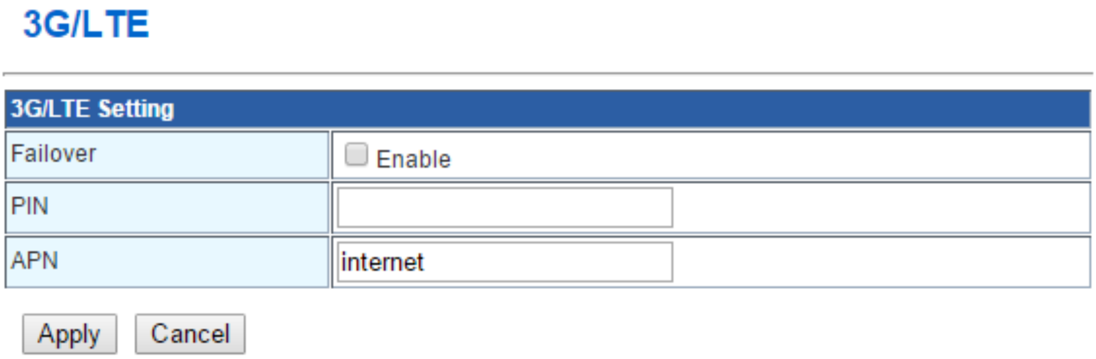
Setup SSID and WiFi key for wireless 5G.



EWAN Settings

WAN Connection Type: DHCP (Auto config)

Setup your WAN connection type.



3G/LTE

3G/LTE Setting	
Failover	☐ Enable
PIN	
APN	internet

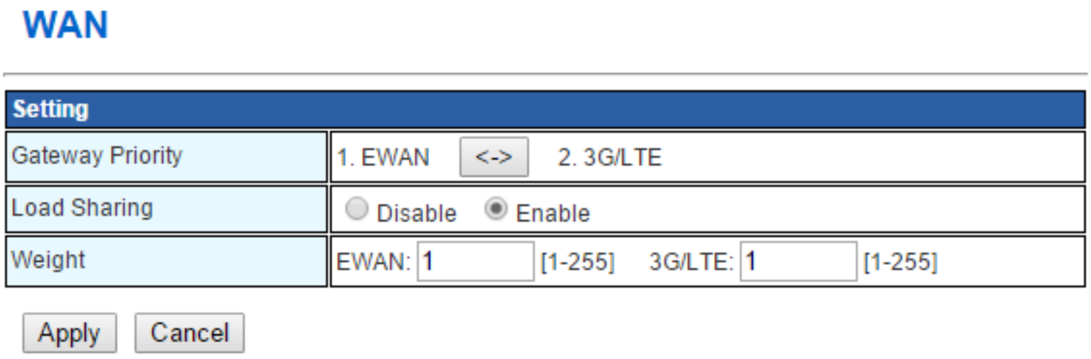
Setup 3G/LTE dongle if there is dongle plugged. Then click Apply button to finish the Quick Stup.

Internet Settings

WAN

Default Gateway

User can change the default gateway priority if dual WAN is available. Enable Load Sharing and setup the weight of each WAN connection for load sharing.



WAN

Setting	
Gateway Priority	1. EWAN <-> 2. 3G/LTE
Load Sharing	○ Disable ● Enable
Weight	EWAN: 1 [1-255] 3G/LTE: 1 [1-255]

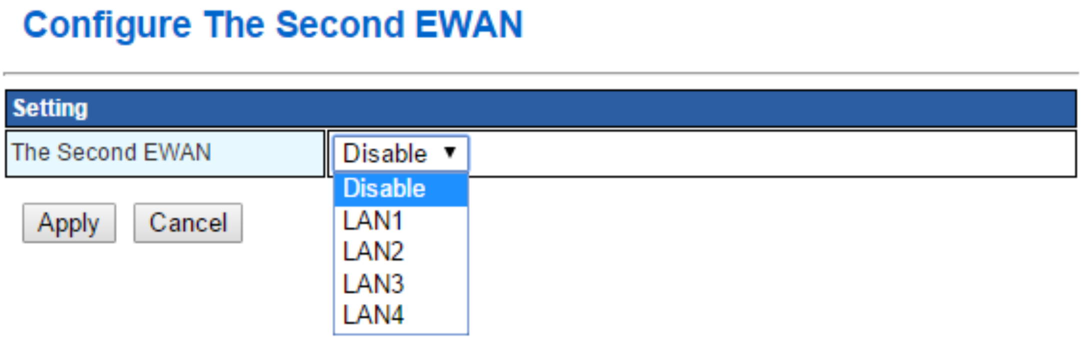
Gateway Priority: Specify which interface will be activated as default gateway when both EWAN and 3G/LTE connection up at the same time.

Load Sharing: Enable/Disable the load sharing function.

Weight: Specify the weight for EWAN and 3G/LTE connection.

The Second EWAN

This page allows to setup one of LAN Ethernet port as second EWAN interface.



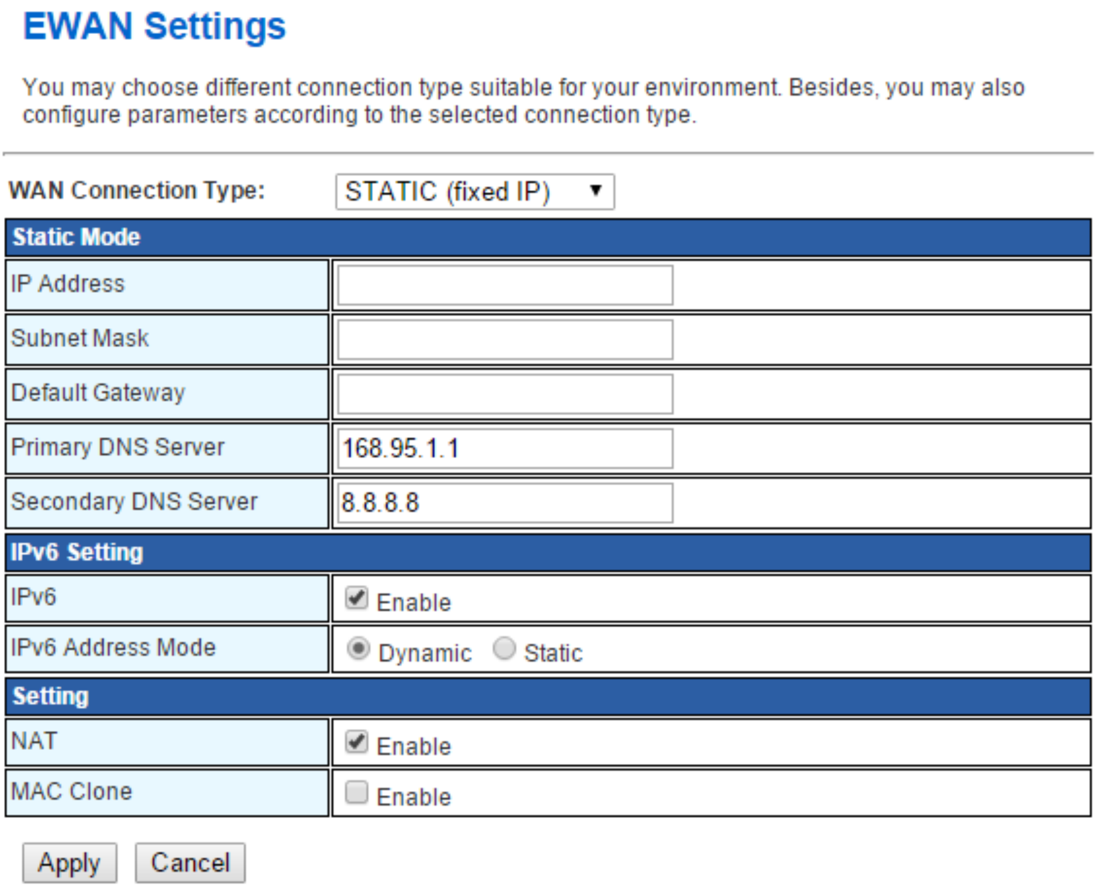
Configure The Second EWAN

Setting	
The Second EWAN	Disable ▼

The Second EWAN: Enable and specify which Ethernet LAN port is second EWAN port.

EWAN

This page allows user to setup WAN connection on Ethernet WAN port and it can support Static IP, DHCP Client, and PPPoE modes. The details of EWAN setting should follow ISP's information.



EWAN Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: STATIC (fixed IP)

Static Mode	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS Server	168.95.1.1
Secondary DNS Server	8.8.8.8
IPv6 Setting	
IPv6	☑ Enable
IPv6 Address Mode	● Dynamic ○ Static
Setting	
NAT	☑ Enable
MAC Clone	□ Enable

IP Address / Subnet Mask / Default Gateway: Enter the IP address, subnet mask and gateway address that provided by your ISP.

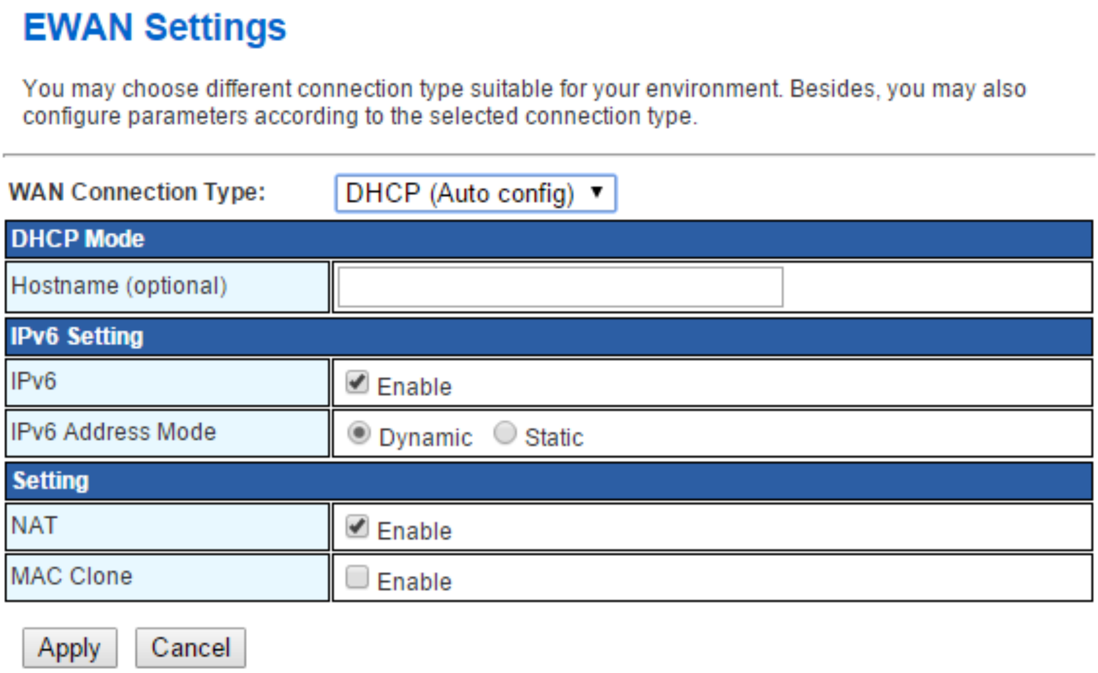
Primary DNS /Secondary DNS Server: Input the primary and secondary DNS server if necessary.

IPv6: Enable/Disable IPv6 on WAN port.

IPv6 Address Mode: Specify the mode for getting or setting IPv6 address.

NAT: Enable/Disable NAT.

MAC Clone: Enter the MAC address if your ISP requires to use specify MAC address for Internet connection.



EWAN Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: DHCP (Auto config) ▼

DHCP Mode	
Hostname (optional)	
IPv6 Setting	
IPv6	☑ Enable
IPv6 Address Mode	● Dynamic ○ Static
Setting	
NAT	☑ Enable
MAC Clone	□ Enable

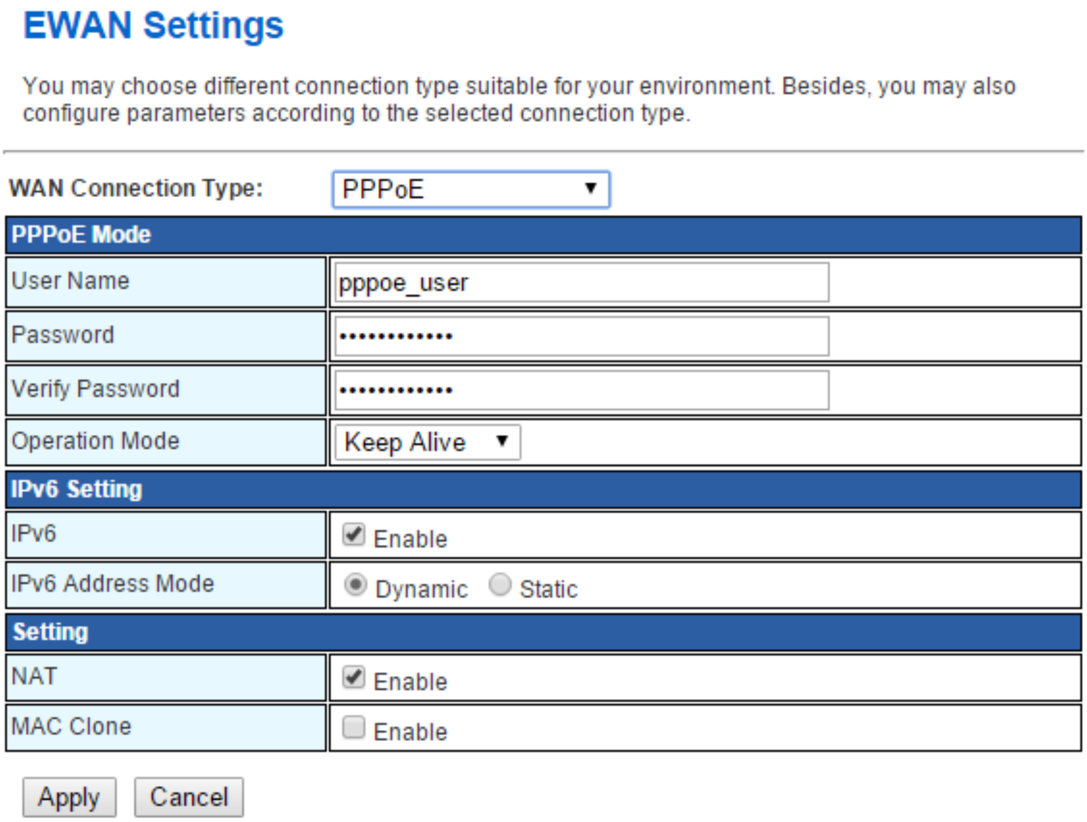
Hostname: Optional, required by some ISPs.

IPv6: Enable/Disable IPv6 on WAN port.

IPv6 Address Mode: Specify the mode for getting or setting IPv6 address.

NAT: Enable/Disable NAT.

MAC Clone: Enter the MAC address if your ISP requires to use specify MAC address for Internet connection.



EWAN Settings

You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: PPPoE ▼

PPPoE Mode	
User Name	pppoe_user
Password	••••••••••••
Verify Password	••••••••••••
Operation Mode	Keep Alive ▼
IPv6 Setting	
IPv6	☑ Enable
IPv6 Address Mode	● Dynamic ○ Static
Setting	
NAT	☑ Enable
MAC Clone	□ Enable

User Name / Password: Enter the PPPoE username/password that provided by your ISP.

Verify Password: Re-enter the password again.

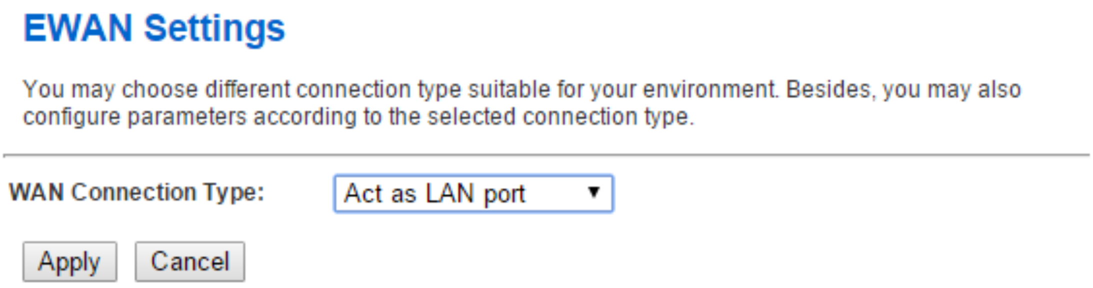
Operation Mode: Specify the PPP connection should be always on (Keep Alive) or only make connection when necessary (On Demand).

IPv6: Enable/Disable IPv6 on WAN port.

IPv6 Address Mode: Specify the mode for getting or setting IPv6 address.

NAT: Enable/Disable NAT.

MAC Clone: Enter the MAC address if your ISP requires to use specify MAC address for Internet connection.



EWAN Settings

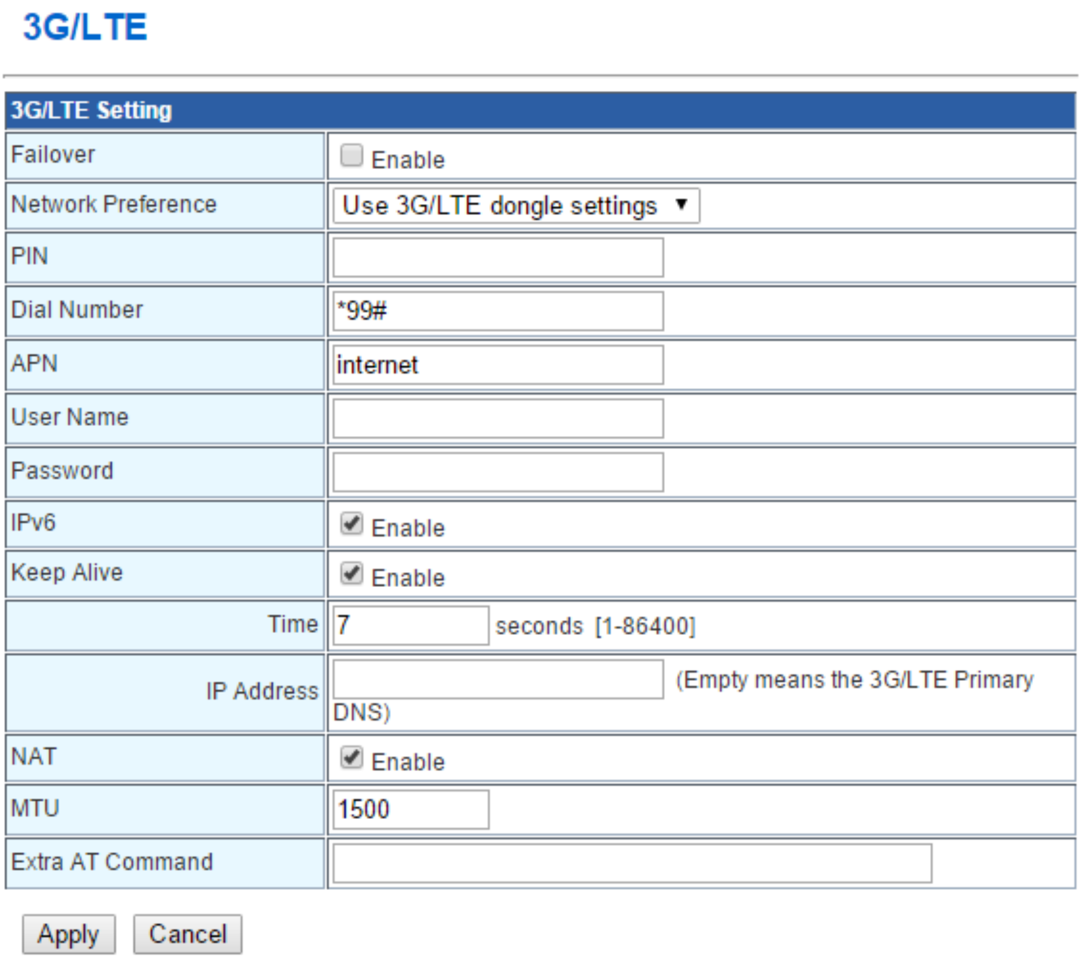
You may choose different connection type suitable for your environment. Besides, you may also configure parameters according to the selected connection type.

WAN Connection Type: Act as LAN port ▼

When WAN Connection Type set to Bridge mode, four Ethernet LAN ports and Ethernet WAN port will work as a switch.

3G/LTE

Select 3G/LTE to configure the route to enjoy the mobility. By default the 3G/LTE interface is on, user can edit the parameters to meet your own requirements.



3G/LTE

3G/LTE Setting	
Failover	☐ Enable
Network Preference	Use 3G/LTE dongle settings ▼
PIN	
Dial Number	*99#
APN	internet
User Name	
Password	
IPv6	☑ Enable
Keep Alive	☑ Enable
Time	7 seconds [1-86400]
IP Address	(Empty means the 3G/LTE Primary DNS)
NAT	☑ Enable
MTU	1500
Extra AT Command	

Failover: Enable/Disable the failover function. The 3G/LTE connection will be activated when EWAN connection is down if it is enabled.

Network Preference: Specify the network preference you preferred.

PIN: Enter the PIN code for your SIM card (optional).

Dial Number: Enter the dialed number that is provided by your ISP, the default value should work with most ISPs.

APN: Enter the APN name if required by your ISP. The default value should work with most ISPs.

Username / Password: Enter the username and password that is provided by your ISP (optional).

IPv6: Enable/Disable IPv6 for your 3G/LTE connection.

Keep Alive: Enable/Disable this feature to prevent the 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity. It may make extra charge if you are not use unlimited service.

Time: Specify the period of time to send keep alive packet.

IP Address: Specify the IP address for sending packet to keep alive.

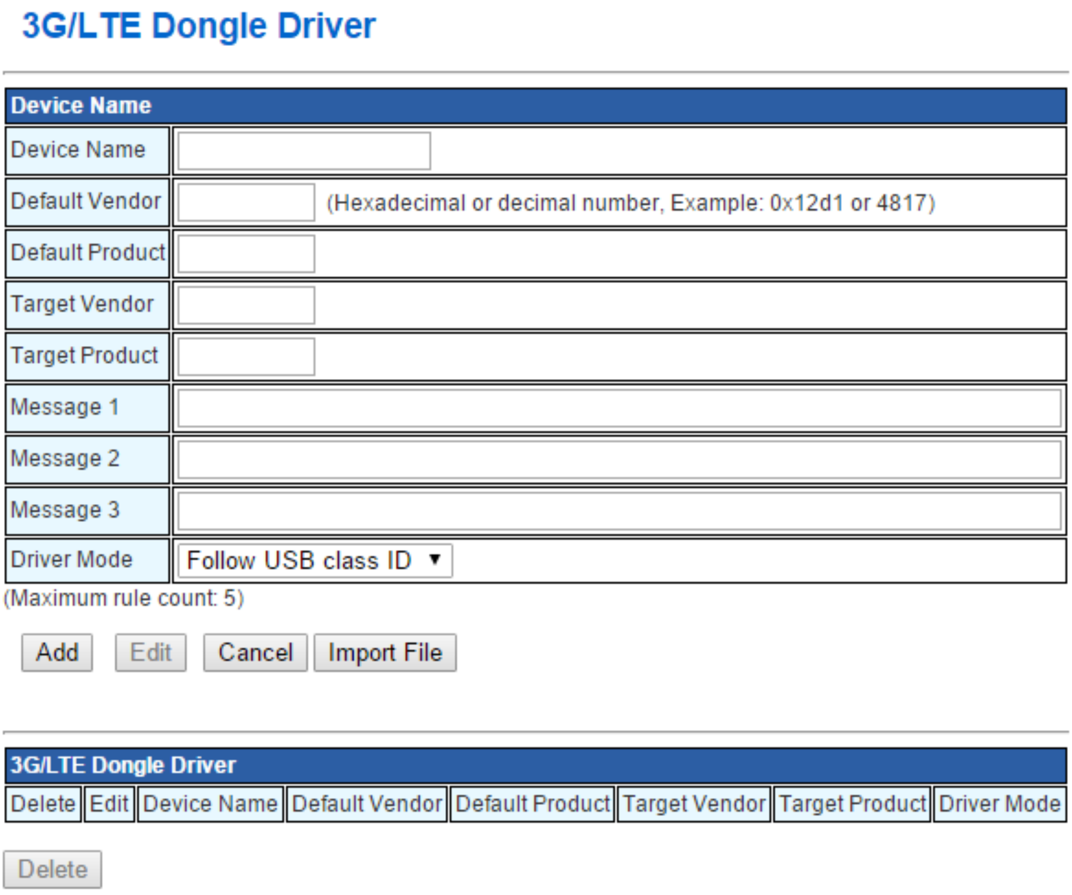
NAT: Enable/Disable the NAT.

MTU: Most ISP offers MTU value to users.

Extra AT Command: User can issue specify the AT command after 3G/LTE modem initialized.

3G/LTE Dongle Driver

This page allows user to add new 3G/LTE dongle support manually. The parameters below can refer to Linux standard usb_modeswitch database to switch dongle to modem mode. User can also choose which driver must be activated by selecting **Driver Mode** once modem mode is ready.

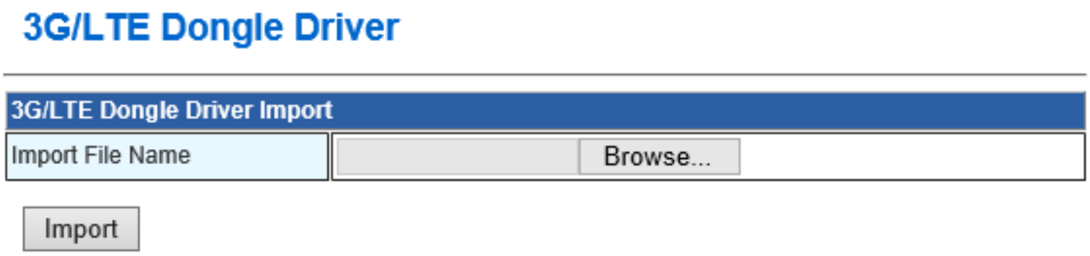


3G/LTE Dongle Driver

Device Name	
Device Name	
Default Vendor	(Hexadecimal or decimal number, Example: 0x12d1 or 4817)
Default Product	
Target Vendor	
Target Product	
Message 1	
Message 2	
Message 3	
Driver Mode	Follow USB class ID ▼

(Maximum rule count: 5)

3G/LTE Dongle Driver							
Delete	Edit	Device Name	Default Vendor	Default Product	Target Vendor	Target Product	Driver Mode



3G/LTE Dongle Driver

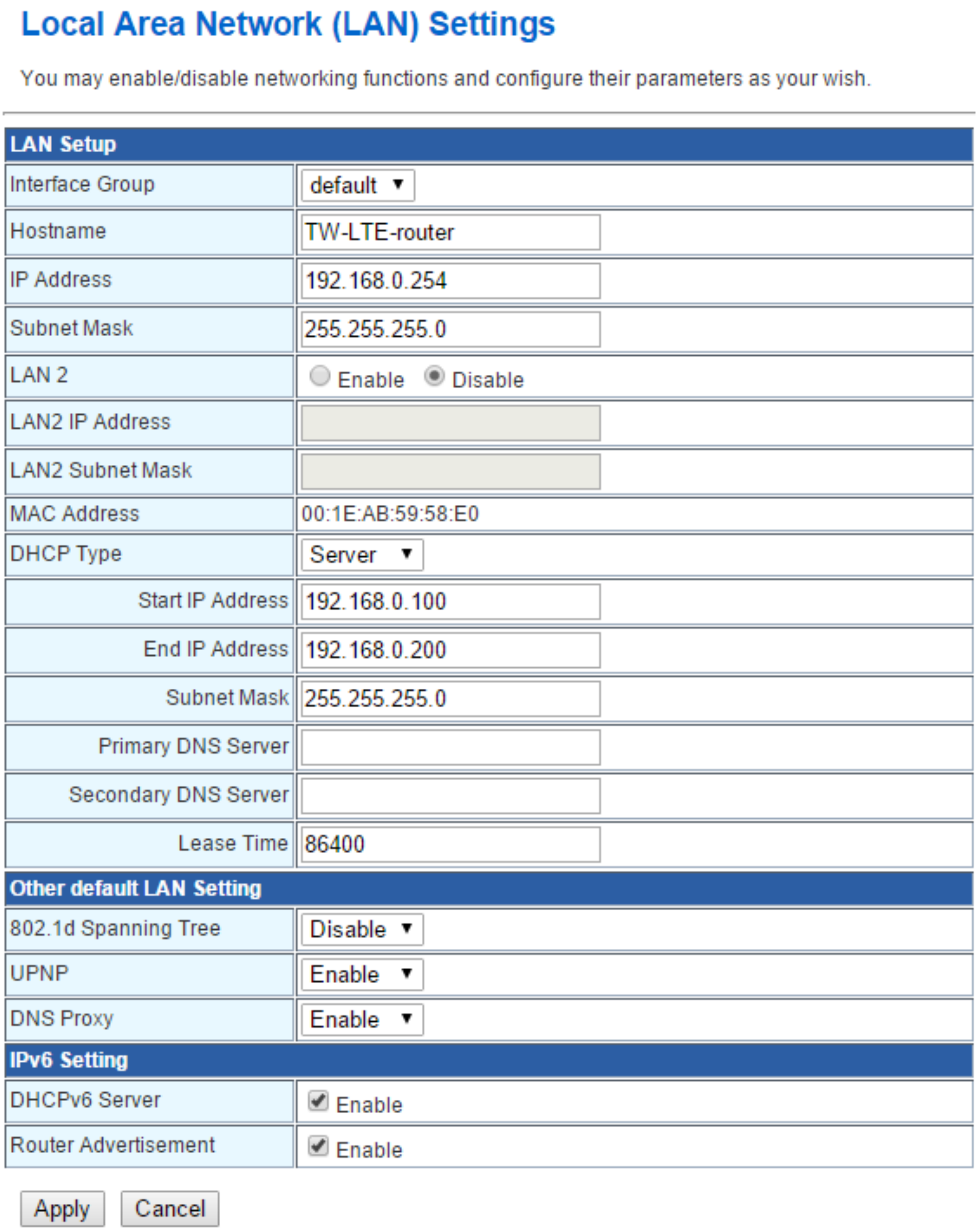
3G/LTE Dongle Driver Import	
Import File Name	Browse...

The file will be provided by TeleWell if new dongle driver support is available.

LAN

LAN

This window allows you to set up a LAN interface. When you are finished, click the **Apply** button.



Local Area Network (LAN) Settings

You may enable/disable networking functions and configure their parameters as your wish.

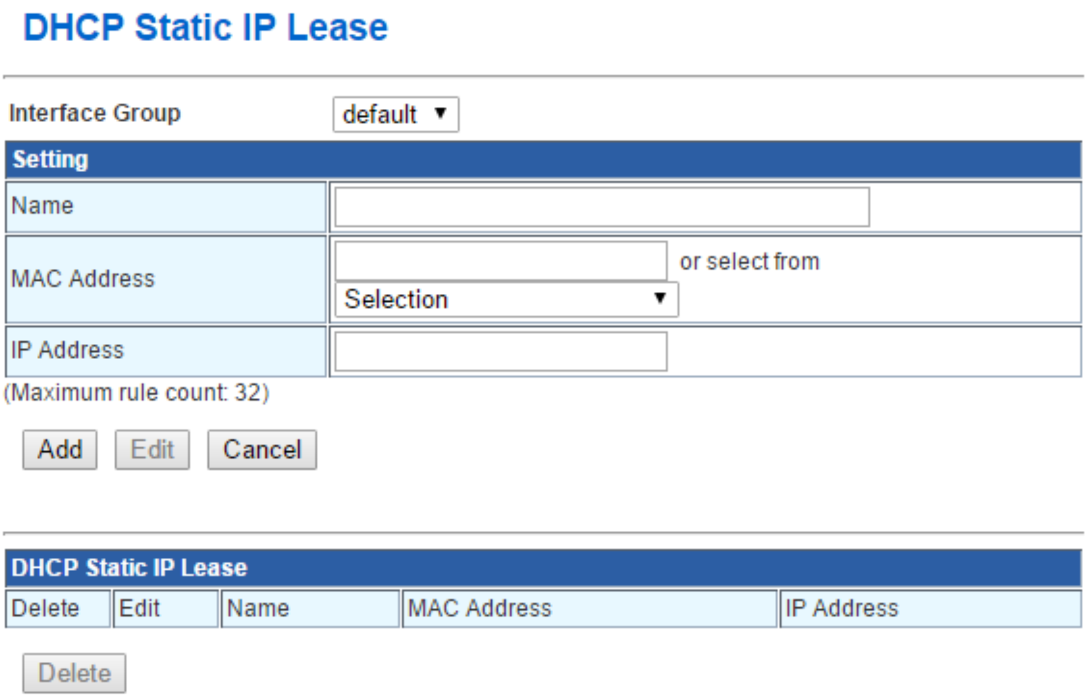
LAN Setup	
Interface Group	default ▼
Hostname	TW-LTE-router
IP Address	192.168.0.254
Subnet Mask	255.255.255.0
LAN 2	○ Enable ● Disable
LAN2 IP Address	
LAN2 Subnet Mask	
MAC Address	00:1E:AB:59:58:E0
DHCP Type	Server ▼
Start IP Address	192.168.0.100
End IP Address	192.168.0.200
Subnet Mask	255.255.255.0
Primary DNS Server	
Secondary DNS Server	
Lease Time	86400
Other default LAN Setting	
802.1d Spanning Tree	Disable ▼
UPNP	Enable ▼
DNS Proxy	Enable ▼
IPv6 Setting	
DHCPv6 Server	☑ Enable
Router Advertisement	☑ Enable

Interface Group: Select group name for detailed setting.

Hostname: Enter the host name for your local area network (optional).
IP Address / Subnet Mask: The local management IP address and mask of this device which is also the default gateway IP address for all PCs in local area network.
LAN 2: Enable/Disable second management LAN IP address.
LAN 2 IP Address / LAN 2 subnet Mask: Specify the second management IP address and mask.
MAC Address: The MAC address of this device LAN interface.
DHCP Type: Enable/Disable the DHCP server on this device.
Start IP Address / End IP Address / Subnet Mask: Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting PC. You must specify the starting / ending address of the IP address pool.
Primary DNS / Secondary DNS Server: Optional. This allows you to assign a DNS Servers to the requesting PC.
Lease Time: DHCP lease time to the DHCP client.
802.1d Spanning Tree: Enable/Disable the spanning tree if necessary.
UPNP: Enable/Disable the UPNP feature.
DNS Proxy: Enable/Disable the DNS Proxy feature.
DHCPv6 Server: Enable/Disable the DHCPv6 server for local area network.
Router Advertisement: Enable/Disable the Router Advertisement for local area network.

DHCP Static IP Lease

The specified IP will be assigned to the corresponding MAC Address listed in the following table when DHCP Server assigns IP Addresses to Clients. Enter the MAC Address, IP Address, and then click **Add** button to add it. But the IP assigned should be outside the range of 192.168.0.100-192.168.0.199.



DHCP Static IP Lease

Interface Group: default ▼

Setting	
Name	
MAC Address	or select from Selection ▼
IP Address	

(Maximum rule count: 32)

DHCP Static IP Lease				
Delete	Edit	Name	MAC Address	IP Address

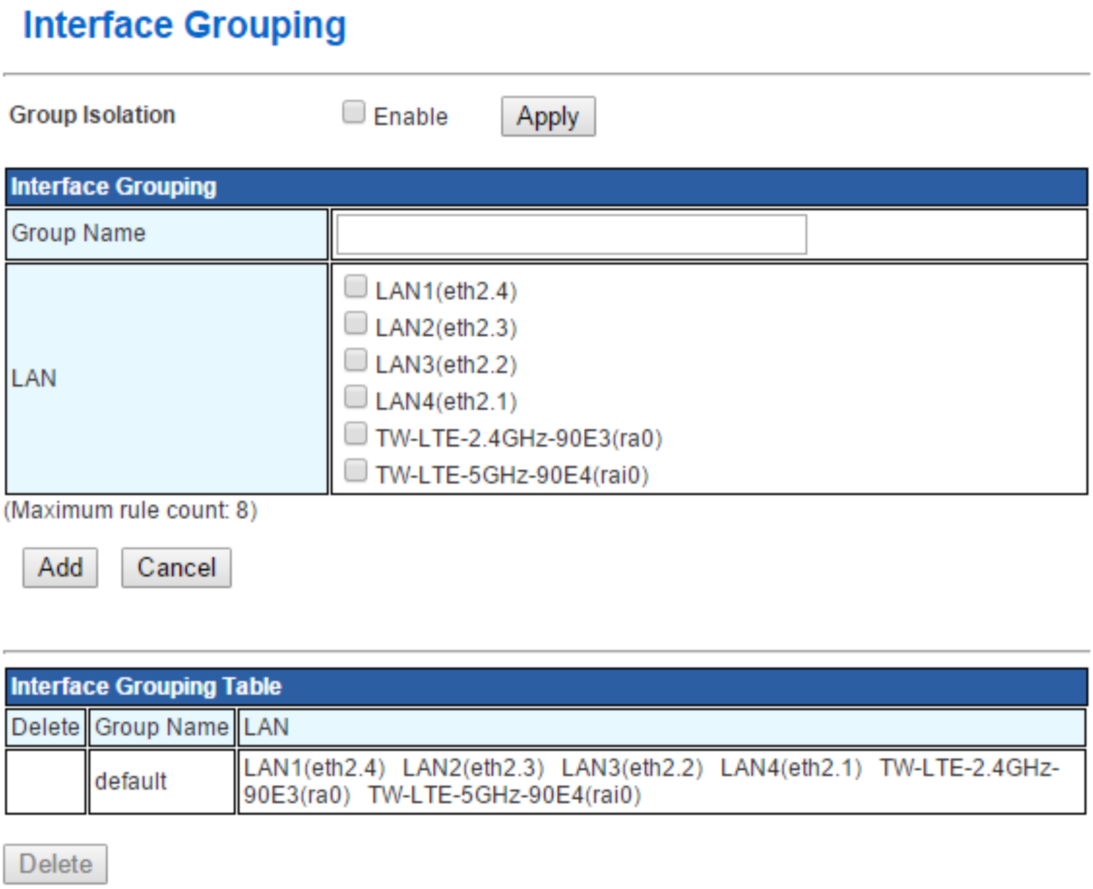
Name: Enter the name for specify PC.

MAC Address: Enter the MAC address of specify PC.

IP Address: Enter the fixed IP address that should be assigned to specify PC. The IP address here should be out of DHCP Server Pool range.

Interface Grouping

Interface grouping is a function to group interfaces, known as VLAN. A Virtual LAN, is a group of hosts with the common set of requirements that communicate as if they were attached to the same broadcast domain, regardless of the physical location. Each group will perform as an independent network.



Interface Grouping

Group Isolation ☐ Enable Apply

Interface Grouping	
Group Name	
LAN	☐ LAN1(eth2.4) ☐ LAN2(eth2.3) ☐ LAN3(eth2.2) ☐ LAN4(eth2.1) ☐ TW-LTE-2.4GHz-90E3(ra0) ☐ TW-LTE-5GHz-90E4(rai0)

(Maximum rule count: 8)

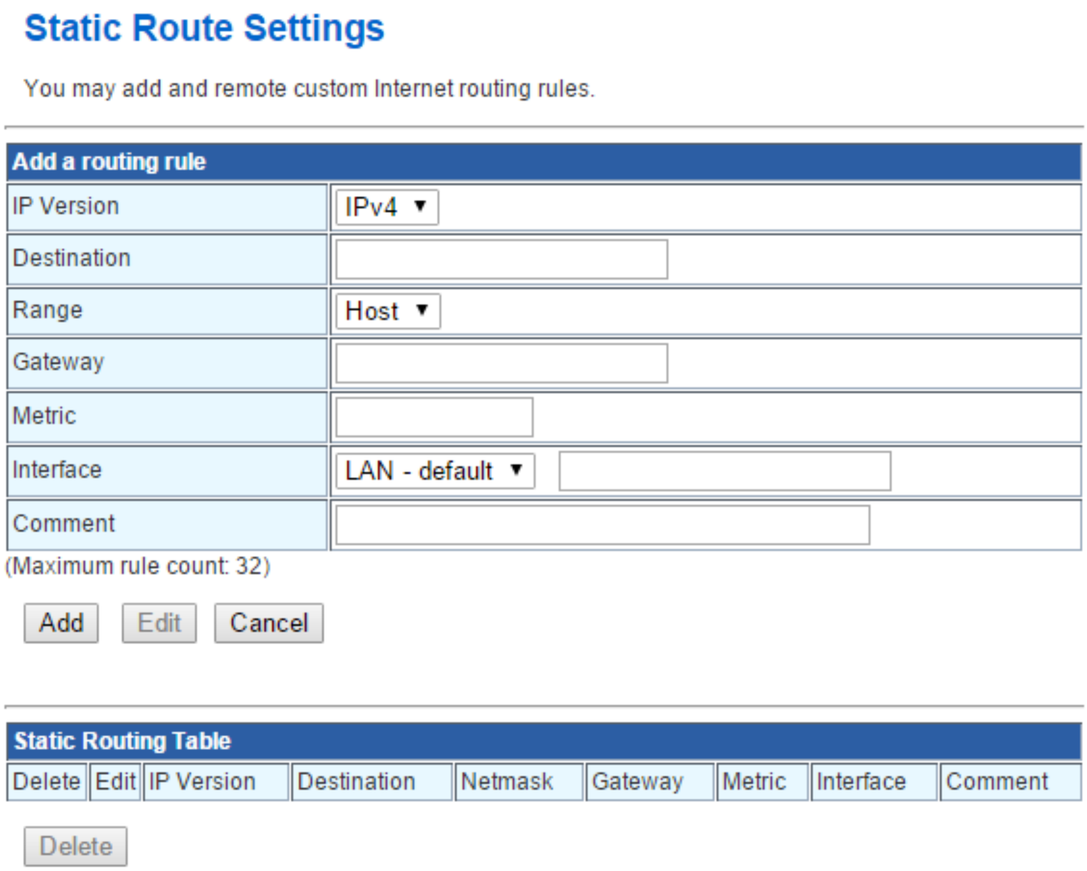
Interface Grouping Table

Delete	Group Name	LAN
	default	LAN1(eth2.4) LAN2(eth2.3) LAN3(eth2.2) LAN4(eth2.1) TW-LTE-2.4GHz-90E3(ra0) TW-LTE-5GHz-90E4(rai0)

Route

Static Route

Enter the static routing information for an entry to the routing table. Click **Add** button when you are finished.



Static Route Settings

You may add and remote custom Internet routing rules.

Add a routing rule	
IP Version	IPv4 ▼
Destination	
Range	Host ▼
Gateway	
Metric	
Interface	LAN - default ▼
Comment	

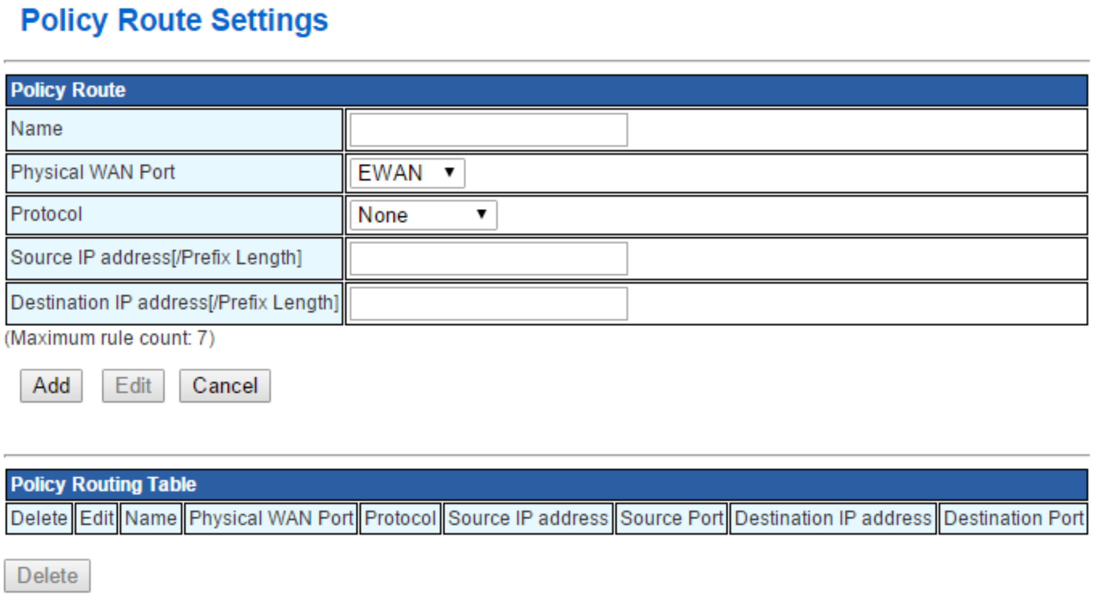
(Maximum rule count: 32)

Static Routing Table

Delete	Edit	IP Version	Destination	Netmask	Gateway	Metric	Interface	Comment

Policy Route

Enter the Policy Routing information. The different with Static Router is the rule here will force and send out the packet by using specify WAN interface. Click **Add** button when you are finished.



Policy Route Settings

Policy Route	
Name	
Physical WAN Port	EWAN ▼
Protocol	None ▼
Source IP address[/Prefix Length]	
Destination IP address[/Prefix Length]	

(Maximum rule count: 7)

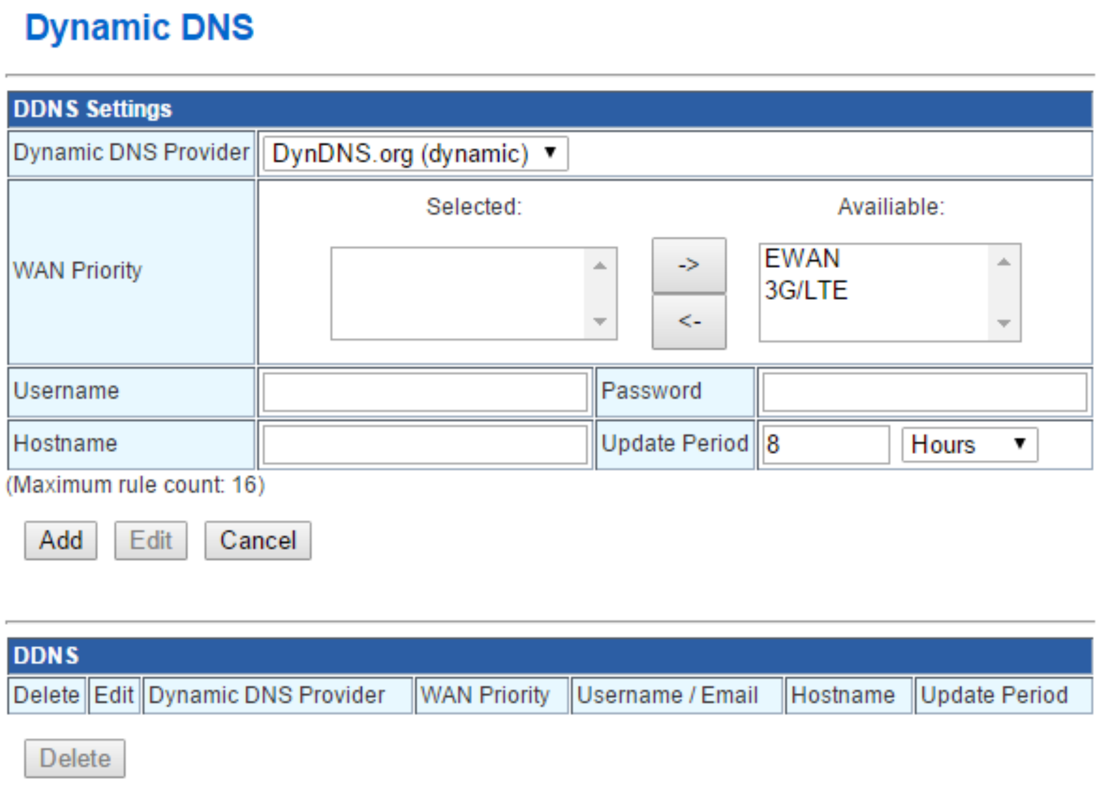
Policy Routing Table

Delete	Edit	Name	Physical WAN Port	Protocol	Source IP address	Source Port	Destination IP address	Destination Port

Dynamic DNS

The Dynamic DNS function allows you to alias a dynamic IP address to a static hostname, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your ADSL connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.

You will first need to register and establish an account with the Dynamic DNS provider using their website, for example http://www.dyndns.org/



Dynamic DNS

DDNS Settings

Dynamic DNS Provider	DynDNS.org (dynamic) ▼		
WAN Priority	Selected:	-> <-	Availiable: EWAN 3G/LTE
Username		Password	
Hostname		Update Period	8 Hours ▼

(Maximum rule count: 16)

DDNS

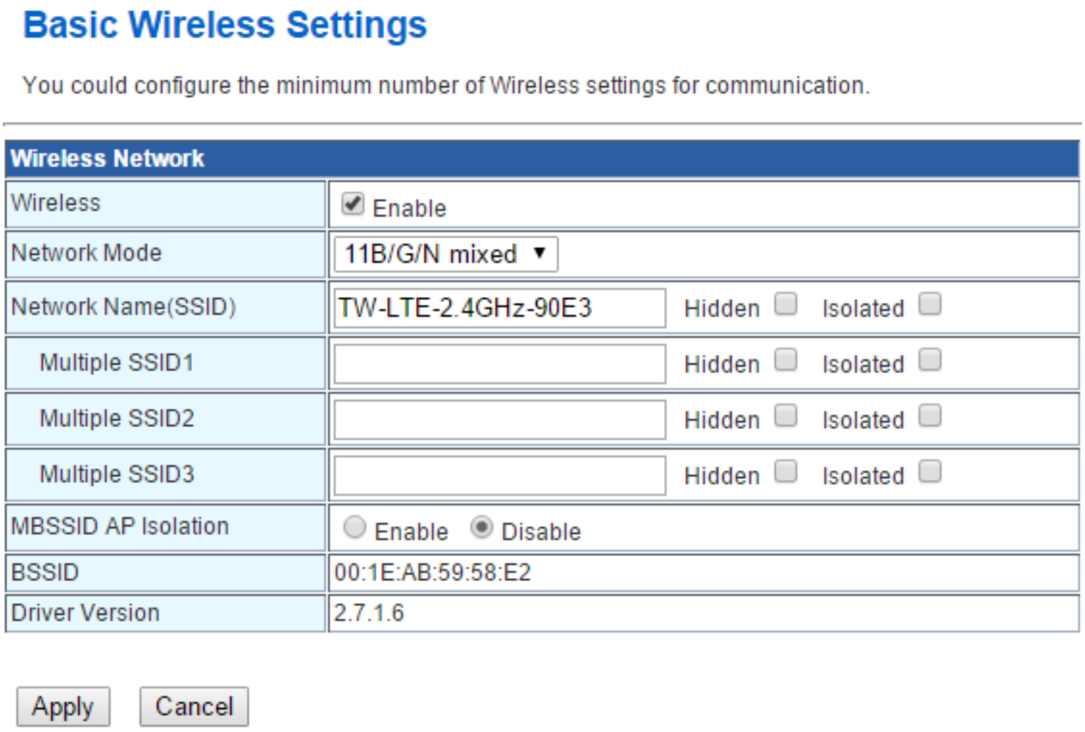
Delete	Edit	Dynamic DNS Provider	WAN Priority	Username / Email	Hostname	Update Period

Wireless Settings

WLAN 2.4GHz

Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication.

Wireless Network	
Wireless	☑ Enable
Network Mode	11B/G/N mixed ▼
Network Name(SSID)	TW-LTE-2.4GHz-90E3 Hidden □ Isolated □
Multiple SSID1	Hidden □ Isolated □
Multiple SSID2	Hidden □ Isolated □
Multiple SSID3	Hidden □ Isolated □
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:1E:AB:59:58:E2
Driver Version	2.7.1.6

Wireless: Enable/Disable the Wireless module.

Network Mode: Specify the mode for Wireless standard support. Set to 11N only for better performance if there is no more 11B/11G client in your network.

Network Name (SSID): Network ID is used for identifying the Wireless LAN. User can also make this SSID hidden, so user can only enter the SSID manually for connecting if **Hidden** box checked. All wireless clients cannot communicate each other if **Isolated** box checked.

Multiple SSID1 / Multiple SSID2 / Multiple SSID3: The device support three more SSID for different connection service (optional).

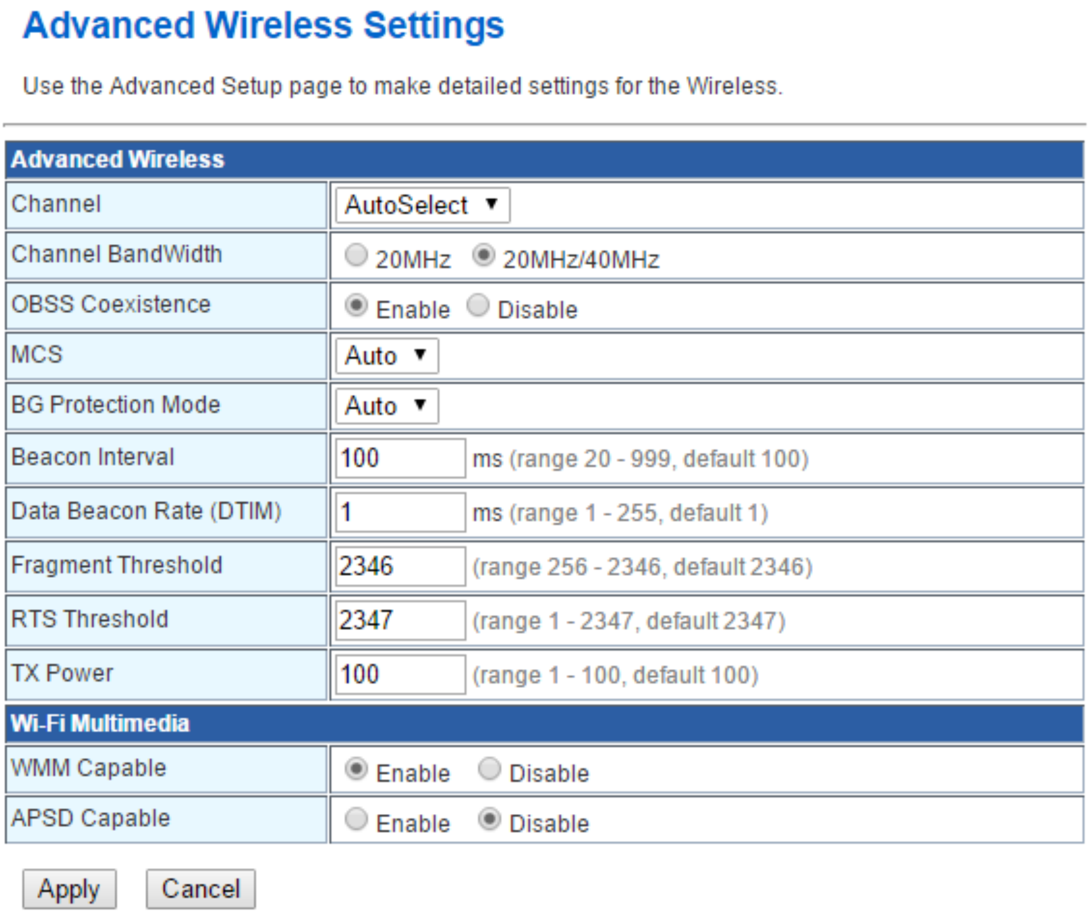
MBSSID AP Isolation: Enable/Disable the traffic between default SSID and SSID1/SSID2/SSID3.

BSSID: BSSID of this 2.4G wireless interface.

Driver Version: Driver version for this 2.4G wireless module.

Advanced

Here user can set some advanced parameters about wireless.



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless.

Advanced Wireless	
Channel	AutoSelect ▼
Channel BandWidth	○ 20MHz ● 20MHz/40MHz
OBSS Coexistence	● Enable ○ Disable
MCS	Auto ▼
BG Protection Mode	Auto ▼
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)
Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable

Channel: The radio channel n umber. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

Channel Bandwidth: Select channel bandwidth for wireless, bigger bandwidth can get higher link rate. But it also depends on interference of your environment.

OBSS Coexistence: Coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

MCS: Select the MCS index, default is set to Auto.

BG Protection Mode: Enabling "B/G" protection ensures that the AP waits long enough for these slower protocols.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 20- 999. The beacon transmissions identify the presence of an access point.

Data Beacon Rate (DTIM): Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Fragment Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

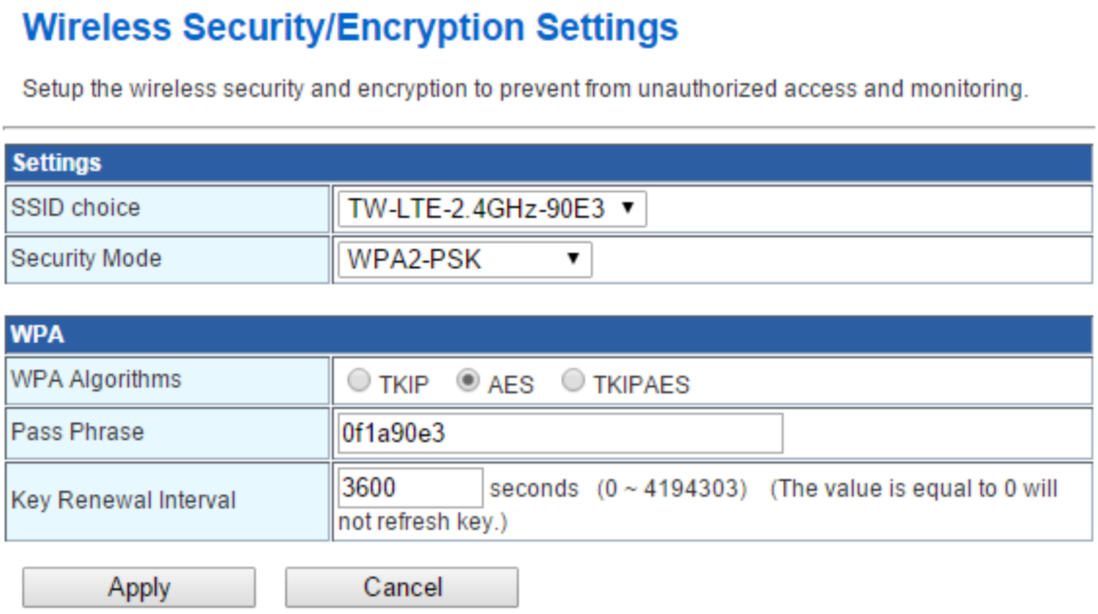
TX Power: Specify the transmitting power of your wireless signal.

WMM Capable: you can choose to enable or disable this function which allows for priority of certain data over wireless network.

APSD Capable: Automatic Power save Delivery. Enable this to save power.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Settings	
SSID choice	TW-LTE-2.4GHz-90E3 ▼
Security Mode	WPA2-PSK ▼

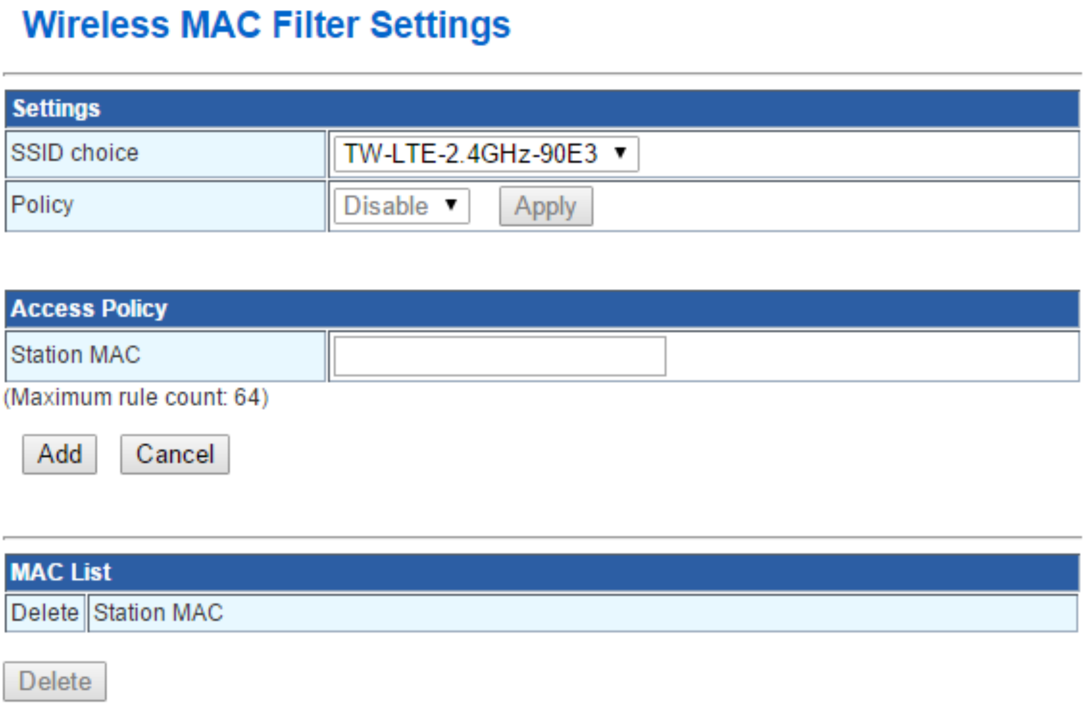
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	0f1a90e3
Key Renewal Interval	3600 seconds (0 ~ 4194303) (The value is equal to 0 will not refresh key.)

SSID choice: Select the SSID for security settings.

Security Mode: User can select one of the following authentications to secure your wireless network: Open, WPA2-PSK or WPA/WPA2-PSK.
WPA Algorithms: Select the algorithm for wireless security. If TKIP selected the maximum link rate is up to 54Mbps according to wireless standard.
Pass Phrase: Enter the key for your wireless security setting.
Key Renewal Interval: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

MAC Filter

The MAC Filter is only apply to specify SSID and help user to make better security for the wireless network. User must to add **Station MAC** first to get **Policy** selectable.



Wireless MAC Filter Settings

Settings	
SSID choice	TW-LTE-2.4GHz-90E3 ▼
Policy	Disable ▼ Apply

Access Policy	
Station MAC	

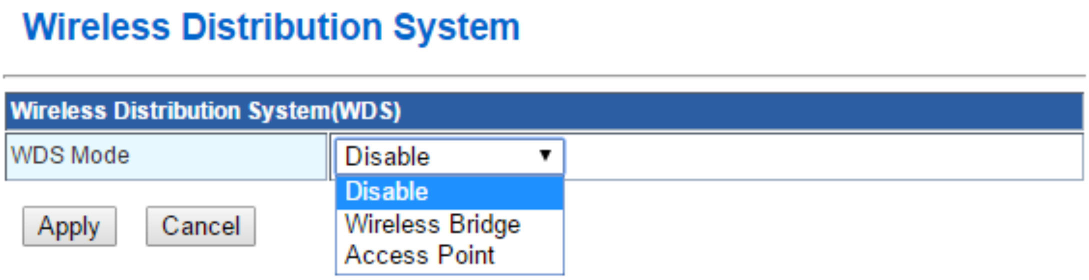
(Maximum rule count: 64)

MAC List	
Delete	Station MAC

SSID choice: Select the specify SSID for applying the MAC filter rule.
Policy: Define the policy rule: Disable, Allow or Reject. It will only be selectable when there is MAC in **MAC List**.
Station MAC: Enter or select specified wireless client MAC address.

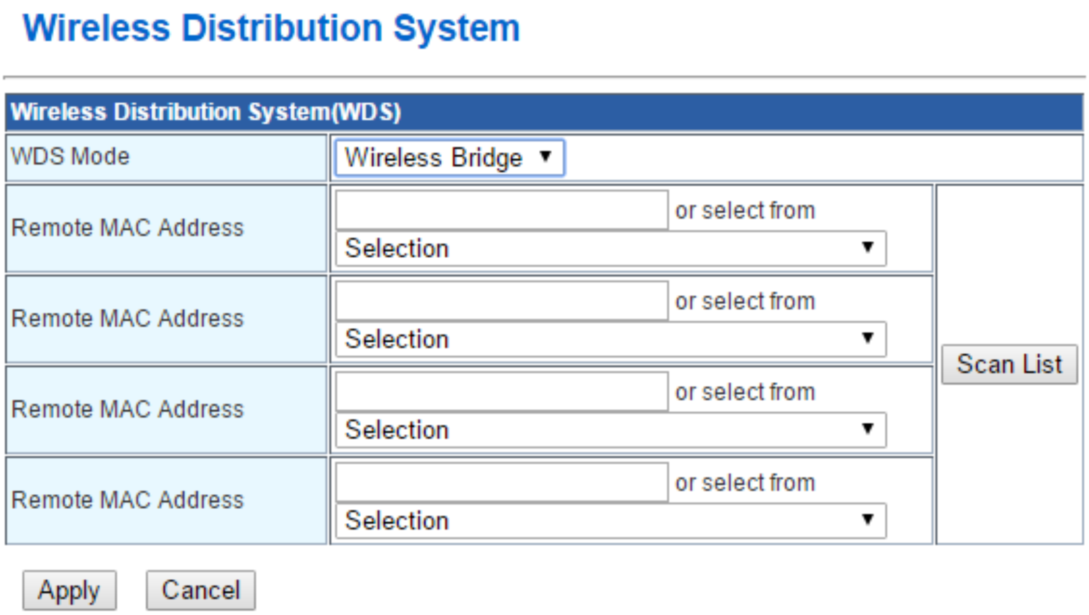
WDS

WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It's easy to install, simply define the peer's MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.



Wireless Distribution System

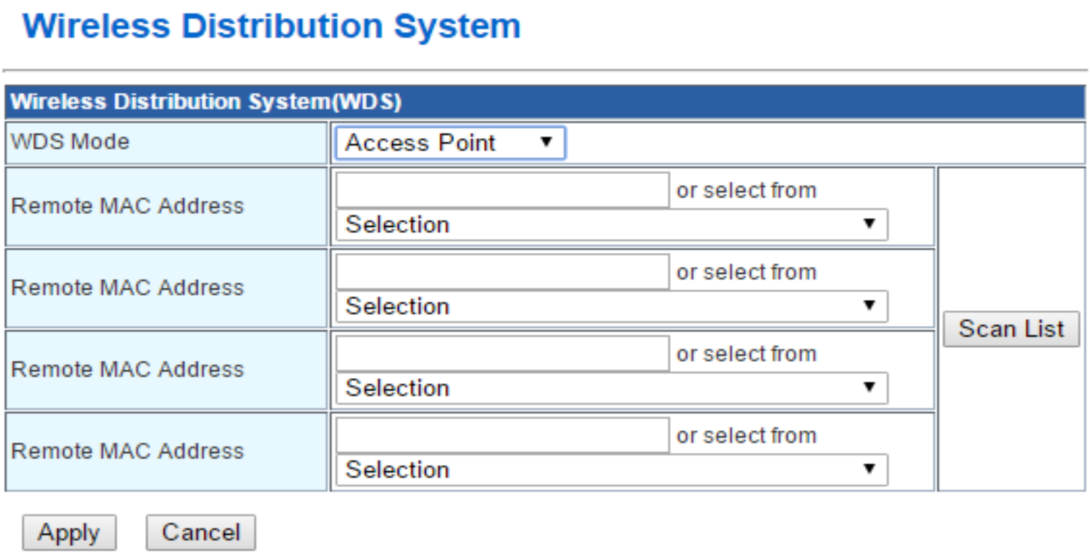
Wireless Distribution System(WDS)	
WDS Mode	Disable ▼



Wireless Distribution System

Wireless Distribution System(WDS)		
WDS Mode	Wireless Bridge ▼	
Remote MAC Address	or select from Selection ▼	Scan List
Remote MAC Address	or select from Selection ▼	
Remote MAC Address	or select from Selection ▼	
Remote MAC Address	or select from Selection ▼	

Enable WDS and work like a bridge. The MAC address of peer WDS Aps should be configured in the **Remote MAC Address** field. In this mode, AP is just a bridge and will not send any beacon and will not respond to any probe request packet. Therefore STA will not be able to connect with it.



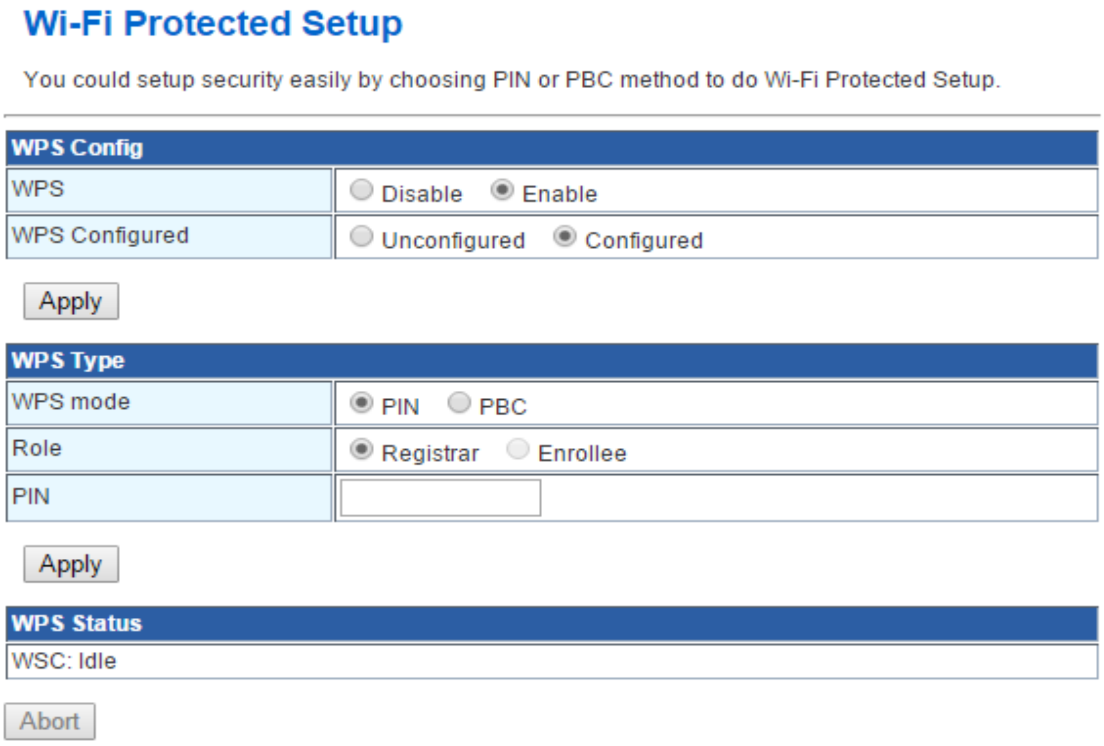
Wireless Distribution System

Wireless Distribution System(WDS)		
WDS Mode	Access Point ▾	
Remote MAC Address	or select from Selection ▾	Scan List
Remote MAC Address	or select from Selection ▾	
Remote MAC Address	or select from Selection ▾	
Remote MAC Address	or select from Selection ▾	

Enable WDS and work like a repeater. The MAC address of peer WDS Aps should be configured in the **Remote MAC Address** field.

WPS

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure AP settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known PIN method is supported to configure WPS.



Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

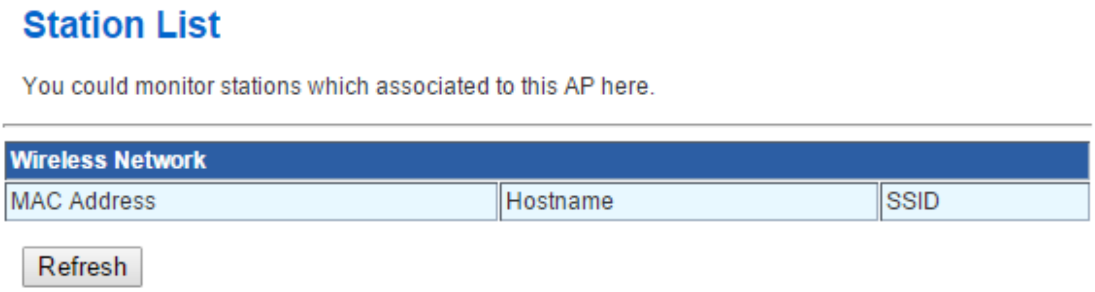
WPS Config	
WPS	○ Disable ● Enable
WPS Configured	○ Unconfigured ● Configured

WPS Type	
WPS mode	● PIN ○ PBC
Role	● Registrar ○ Enrollee
PIN	

WPS Status
WSC: Idle

Station List

Here you can view information about the wireless clients.



Station List

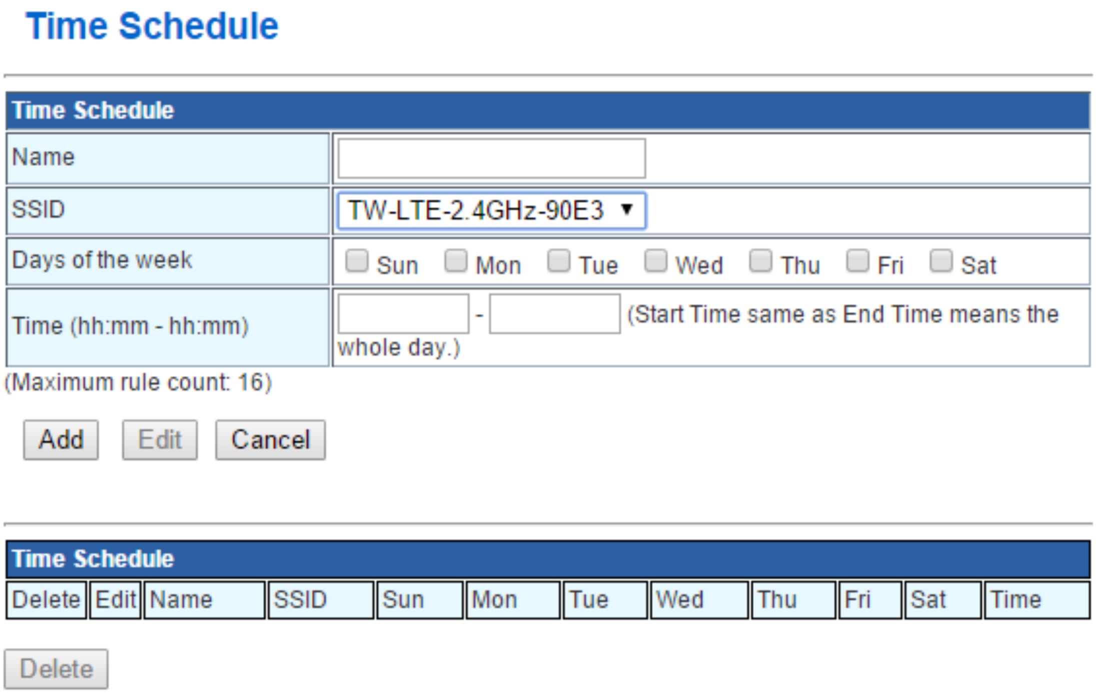
You could monitor stations which associated to this AP here.

Wireless Network		
MAC Address	Hostname	SSID

Refresh

Time Schedule

Time Schedule is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access. The Wireless schedule only functions whilst Wireless is enabled. The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.



Time Schedule

Time Schedule	
Name	
SSID	TW-LTE-2.4GHz-90E3 ▼
Days of the week	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Time (hh:mm - hh:mm)	- (Start Time same as End Time means the whole day.)

(Maximum rule count: 16)

Add Edit Cancel

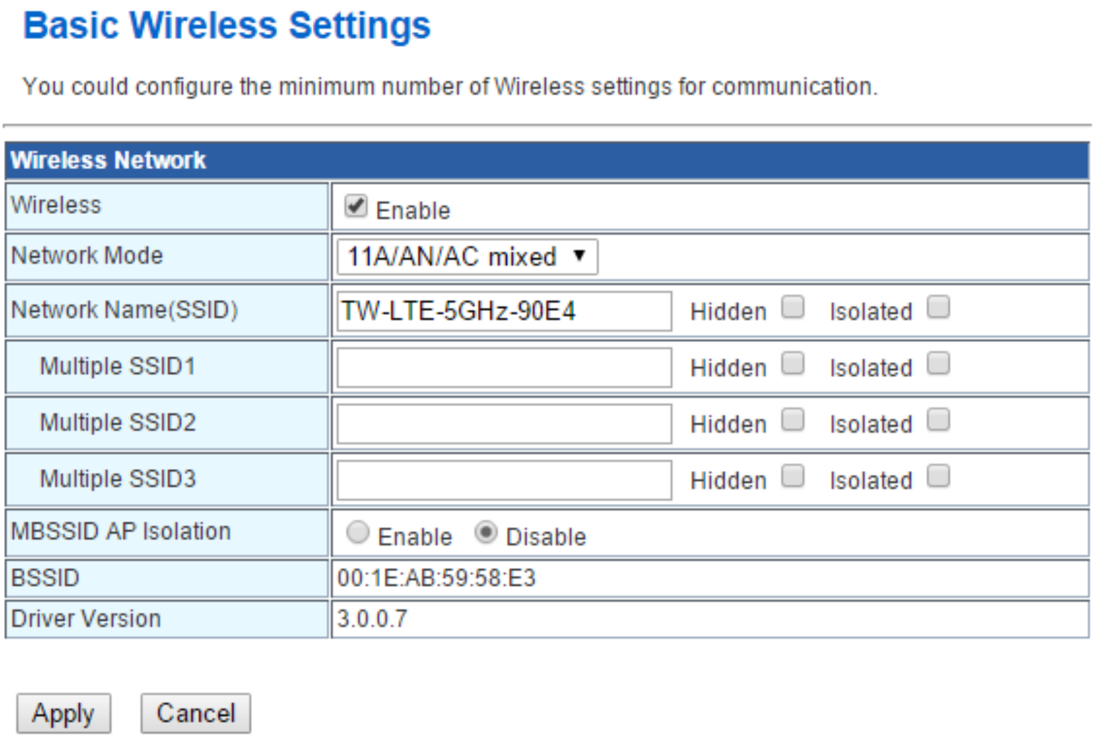
Time Schedule											
Delete	Edit	Name	SSID	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time

Delete

WLAN 5GHz

Basic

It let you determine whether to enable Wireless function and set the basic parameters of an AP and the Virtual APs



Basic Wireless Settings

You could configure the minimum number of Wireless settings for communication.

Wireless Network			
Wireless	☑ Enable		
Network Mode	11A/AN/AC mixed ▼		
Network Name(SSID)	TW-LTE-5GHz-90E4	Hidden □	Isolated □
Multiple SSID1		Hidden □	Isolated □
Multiple SSID2		Hidden □	Isolated □
Multiple SSID3		Hidden □	Isolated □
MBSSID AP Isolation	○ Enable ● Disable		
BSSID	00:1E:AB:59:58:E3		
Driver Version	3.0.0.7		

Wireless: Enable/Disable the Wireless module.

Network Mode: Specify the mode for Wireless standard support.

Network Name (SSID): Network ID is used for identifying the Wireless LAN. User can also make this SSID hidden, so user can only enter the SSID manually for connecting if **Hidden** box checked. All wireless clients cannot communicate each other if **Isolated** box checked.

Multiple SSID1 / Multiple SSID2 / Multiple SSID3: The device support three more SSID for different connection service (optional).

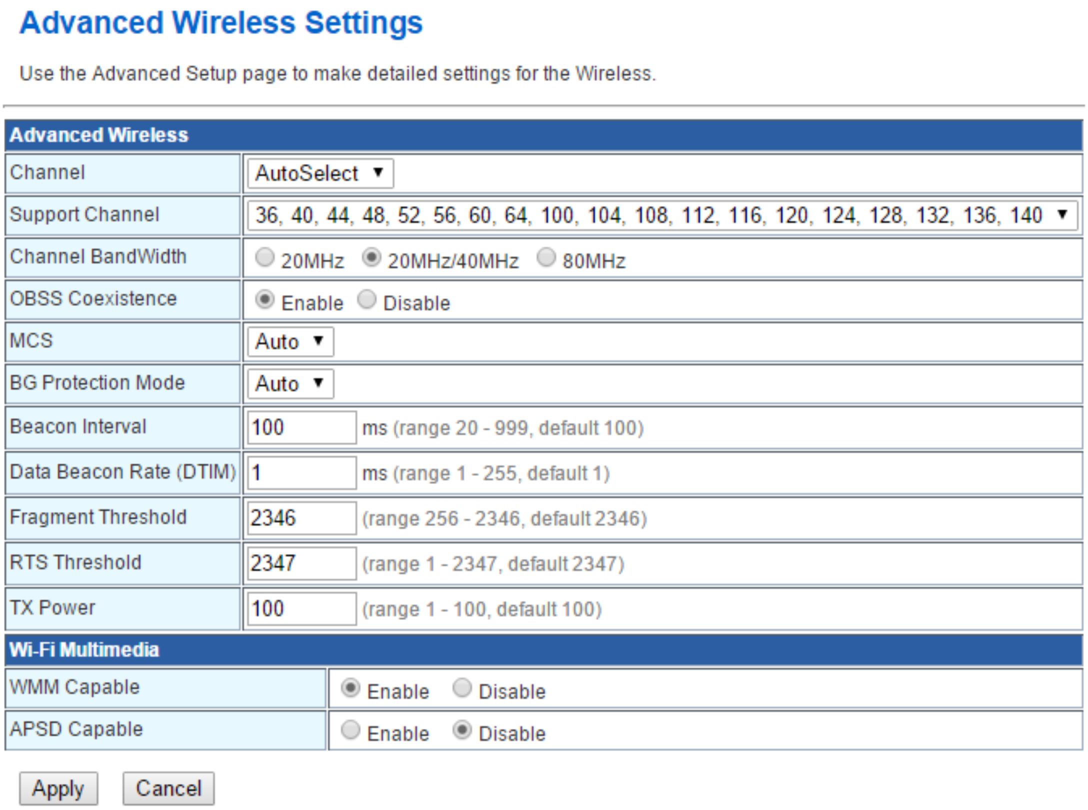
MBSSID AP Isolation: Enable/Disable the traffic between default SSID and SSID1/SSID2/SSID3.

BSSID: BSSID of this 5G wireless interface.

Driver Version: Driver version for this 5G wireless module.

Advanced

Here user can set some advanced parameters about wireless.



Advanced Wireless Settings

Use the Advanced Setup page to make detailed settings for the Wireless.

Advanced Wireless	
Channel	AutoSelect ▼
Support Channel	36, 40, 44, 48, 52, 56, 60, 64, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140 ▼
Channel BandWidth	○ 20MHz ● 20MHz/40MHz ○ 80MHz
OBSS Coexistence	● Enable ○ Disable
MCS	Auto ▼
BG Protection Mode	Auto ▼
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	1 ms (range 1 - 255, default 1)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 (range 1 - 100, default 100)

Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable

Channel: The radio channel n umber. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.

Support Channel: Select supported channel range.

Channel Bandwidth: Select channel bandwidth for wireless, bigger bandwidth can get higher link rate. But it also depends on interference of your environment.

OBSS Coexistence: Coexistence (or not) between 20 MHZ and 40 MHZ overlapping basic service sets (OBSS) in wireless local area networks.

MCS: Select the MCS index, default is set to Auto.

BG Protection Mode: Enabling "B/G" protection ensures that the AP waits long enough for these slower protocols.

Beacon Interval: The amount of time between beacon transmissions in is milliseconds. The default is 100ms and the acceptable is 20- 999. The beacon transmissions identify the presence of an access point.

Data Beacon Rate (DTIM): Delivery Traffic Indication Message (DTIM). The entry range is a value between 1 and 255. A DTIM is countdown variable that informs clients of the next window for listening to broadcast and multicast messages. When the AP has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM interval value. AP clients hear the beacons and awaken to receive the broadcast and multicast messages. The default is 1.

Fragment Threshold: A threshold (in bytes) whether the packets will be fragmented and at what size. Packets succeeding the fragmentation threshold of 802.11n WLAN will be split into smaller units suitable for circuit size. While the packets smaller than fragmentation threshold will not be fragmented. Default is 2346, setting the fragmentation too low may result in poor performance.

RTS Threshold: Request to Send (RTS) threshold specifies the packet size, when exceeds the size, the RTS/CTS will be triggered. The default setting of 2347(max length) will disable the RTS.

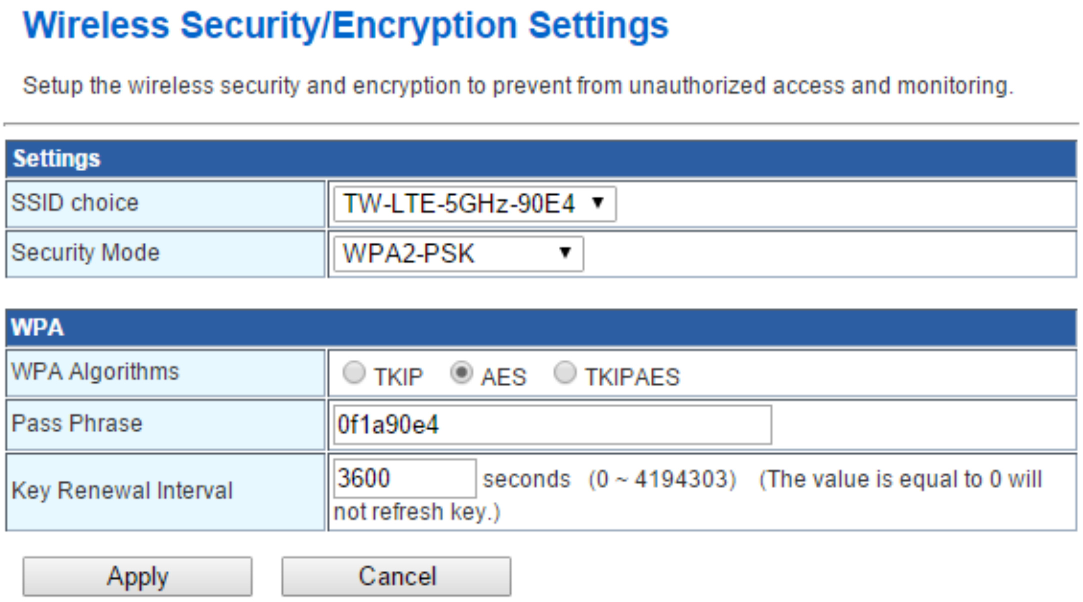
TX Power: Specify the transmitting power of your wireless signal.

WMM Capable: you can choose to enable or disable this function which allows for priority of certain data over wireless network.

APSD Capable: Automatic Power save Delivery. Enable this to save power.

Security

Wireless security prevents unauthorized access or damage to computers using wireless network.



Wireless Security/Encryption Settings

Setup the wireless security and encryption to prevent from unauthorized access and monitoring.

Settings	
SSID choice	TW-LTE-5GHz-90E4 ▼
Security Mode	WPA2-PSK ▼

WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	0f1a90e4
Key Renewal Interval	3600 seconds (0 ~ 4194303) (The value is equal to 0 will not refresh key.)

SSID choice: Select the SSID for security settings.

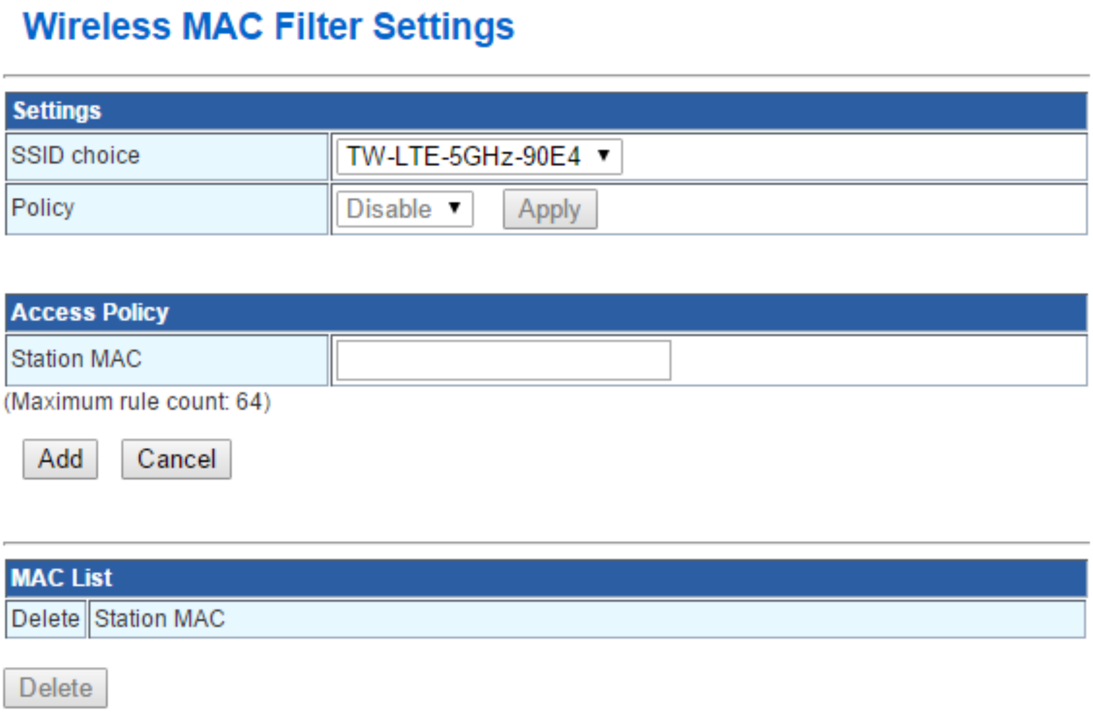
Security Mode: User can select one of the following authentications to secure your wireless network: Open, WPA2-PSK or WPA/WPA2-PSK.

WPA Algorithms: Select the algorithm for wireless security. If TKIP selected the maximum link rate is up to 54Mbps according to wireless standard.

Pass Phrase: Enter the key for your wireless security setting.
Key Renewal Interval: The period of renewal time for changing the security key automatically between wireless client and Access Point (AP). This is in seconds.

MAC Filter

The MAC Filter is only apply to specify SSID and help user to make better security for the wireless network. User must to add **Station MAC** first to get **Policy** selectable.



Wireless MAC Filter Settings

Settings	
SSID choice	TW-LTE-5GHz-90E4 ▼
Policy	Disable ▼ Apply

Access Policy	
Station MAC	

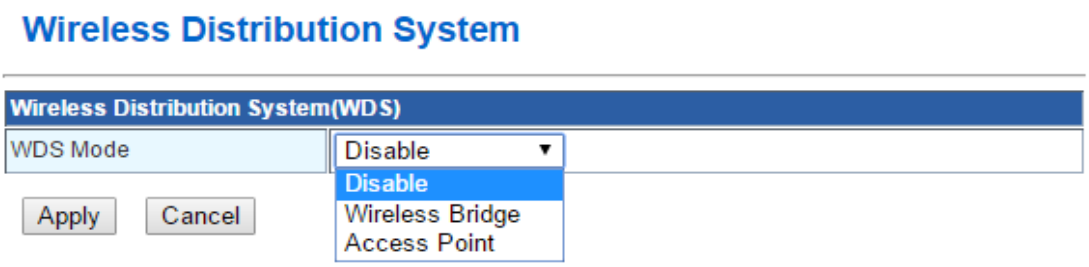
(Maximum rule count: 64)

MAC List	
Delete	Station MAC

SSID choice: Select the specify SSID for applying the MAC filter rule.
Policy: Define the policy rule: Disable, Allow or Reject. It will only be selectable when there is MAC in **MAC List**.
Station MAC: Enter or select specified wireless client MAC address.

WDS

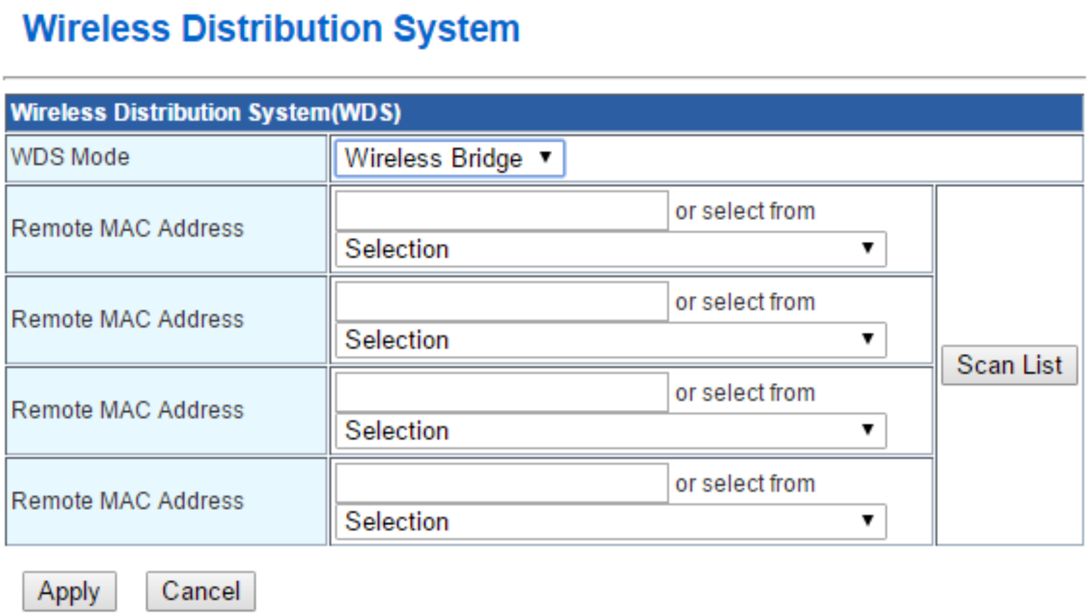
WDS (wireless distributed system) is a wireless access point mode that enables wireless link and communication with other access points. It’s easy to install, simply define the peer’s MAC address of the connected AP. WDS takes advantage of cost saving and flexibility with no extra wireless client device required to bridge between two access points and extending an existing wired or wireless infrastructure network to create a larger network.



Wireless Distribution System

Wireless Distribution System(WDS)

WDS Mode: Disable

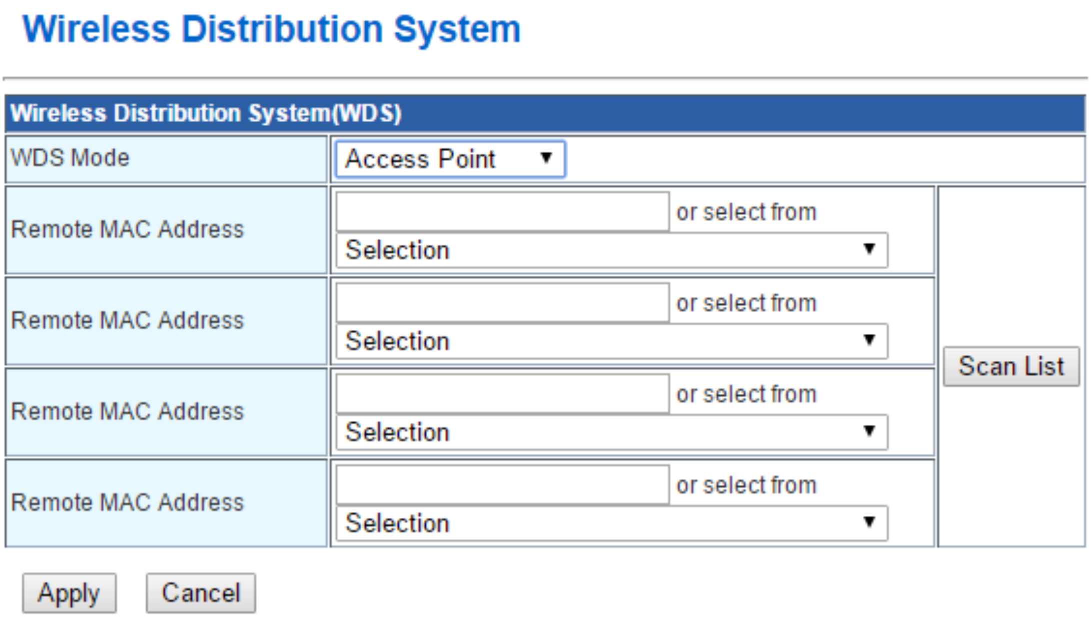


Wireless Distribution System

Wireless Distribution System(WDS)

WDS Mode	Wireless Bridge	
Remote MAC Address	or select from Selection	Scan List
Remote MAC Address	or select from Selection	
Remote MAC Address	or select from Selection	
Remote MAC Address	or select from Selection	

Enable WDS and work like a bridge. The MAC address of peer WDS Aps should be configured in the **Remote MAC Address** field. In this mode, AP is just a bridge and will not send any beacon and will not respond to any probe request packet. Therefore STA will not be able to connect with it.



Wireless Distribution System

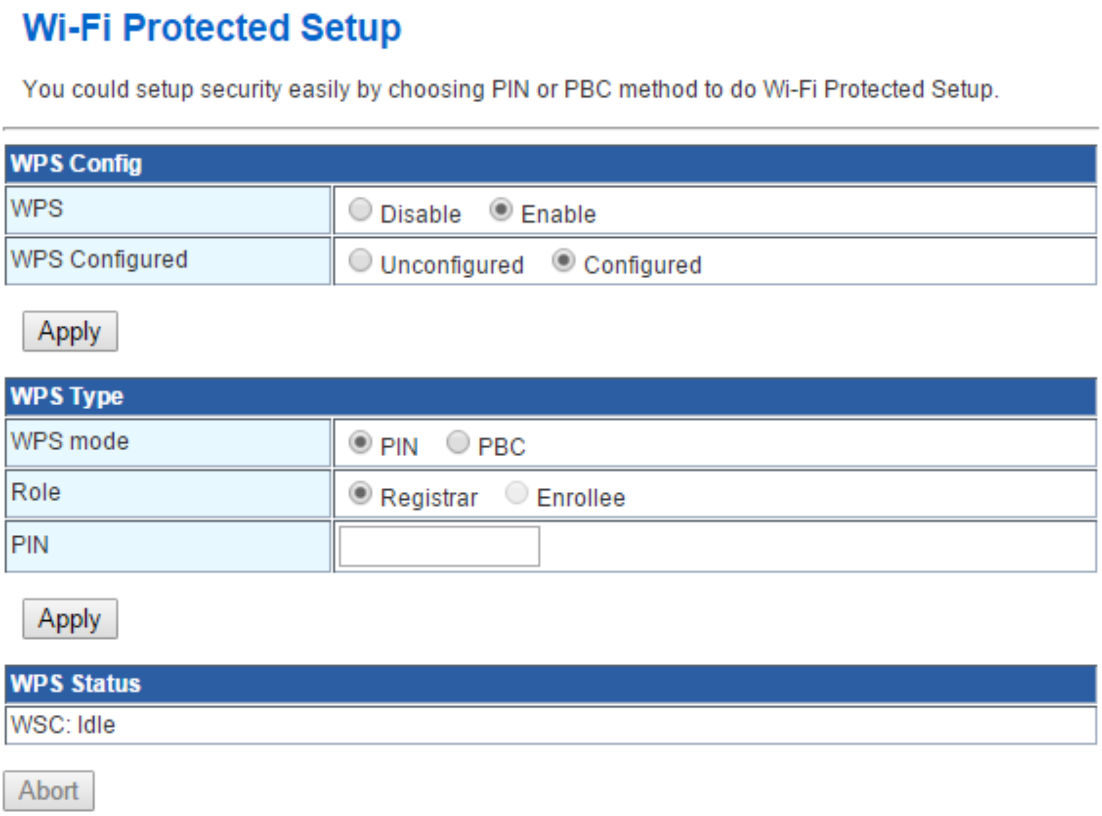
Wireless Distribution System(WDS)

WDS Mode	Access Point	
Remote MAC Address	or select from Selection	Scan List
Remote MAC Address	or select from Selection	
Remote MAC Address	or select from Selection	
Remote MAC Address	or select from Selection	

Enable WDS and work like a repeater. The MAC address of peer WDS Aps should be configured in the **Remote MAC Address** field.

WPS

WPS (Wi-Fi Protected Setup) feature is a standard protocol created by Wi-Fi Alliance. WPS is used to exchange the AP setting with Station and configure AP settings. This feature greatly simplifies the steps needed to create a Wi-Fi network for a residential or an office setting. The commonly known PIN method is supported to configure WPS.



Wi-Fi Protected Setup

You could setup security easily by choosing PIN or PBC method to do Wi-Fi Protected Setup.

WPS Config	
WPS	○ Disable ● Enable
WPS Configured	○ Unconfigured ● Configured

Apply

WPS Type	
WPS mode	● PIN ○ PBC
Role	● Registrar ○ Enrollee
PIN	

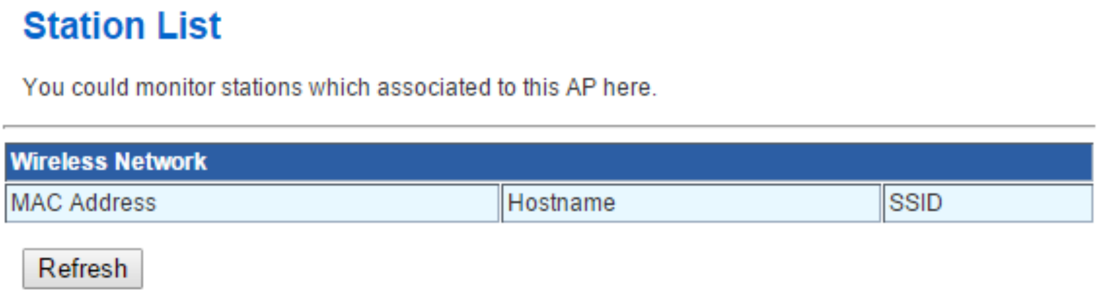
Apply

WPS Status
WSC: Idle

Abort

Station List

Here you can view information about the wireless clients.



Station List

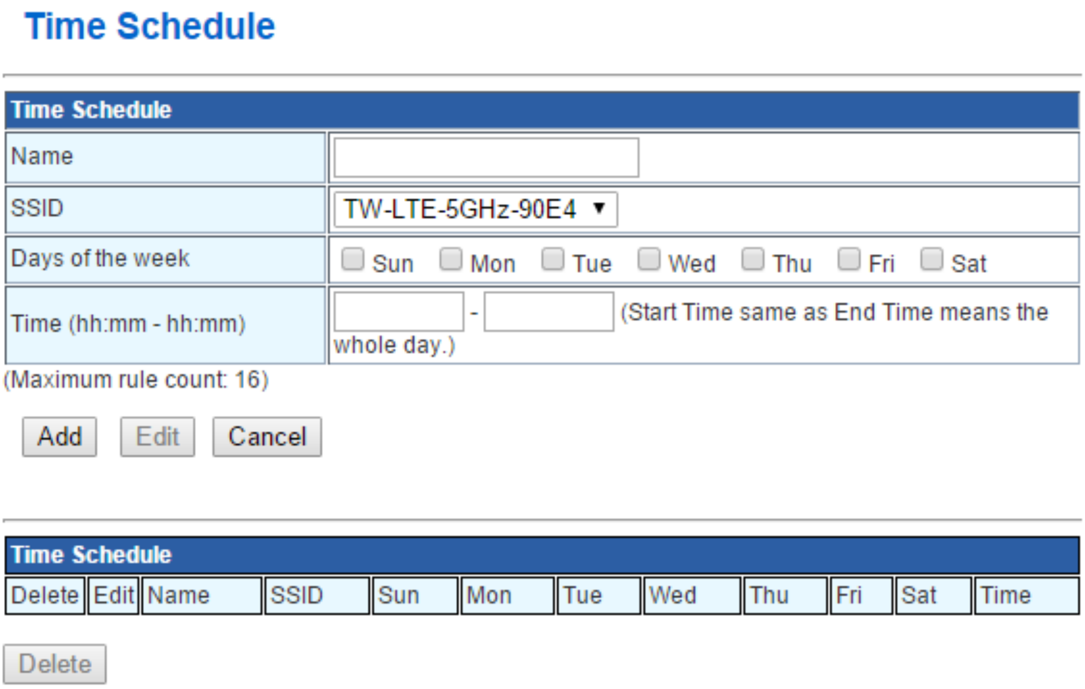
You could monitor stations which associated to this AP here.

Wireless Network		
MAC Address	Hostname	SSID

Refresh

Time Schedule

Time Schedule is aimed to offer methods to flexibly control when the wireless network (SSID) is allowed for access. The Wireless schedule only functions whilst Wireless is enabled. The Guest/Virtual AP schedule control only operates whilst the associated AP is enabled.



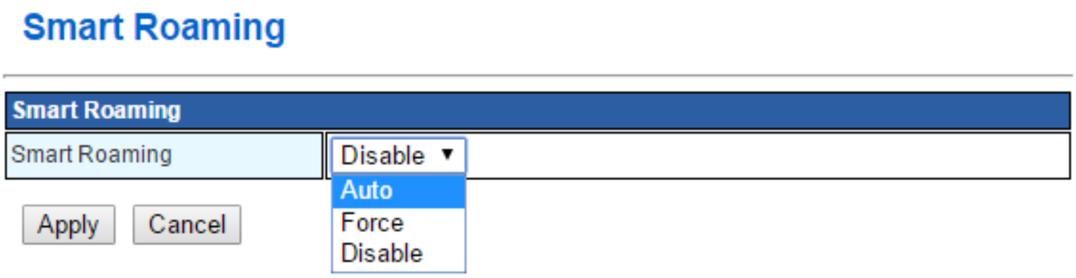
Time Schedule

Time Schedule	
Name	
SSID	TW-LTE-5GHz-90E4 ▼
Days of the week	□ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat
Time (hh:mm - hh:mm)	- (Start Time same as End Time means the whole day.)

(Maximum rule count: 16)

Time Schedule											
Delete	Edit	Name	SSID	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time

Smart Roaming



Smart Roaming

Smart Roaming	
Smart Roaming	Disable ▼

NAT Settings

Virtual Server

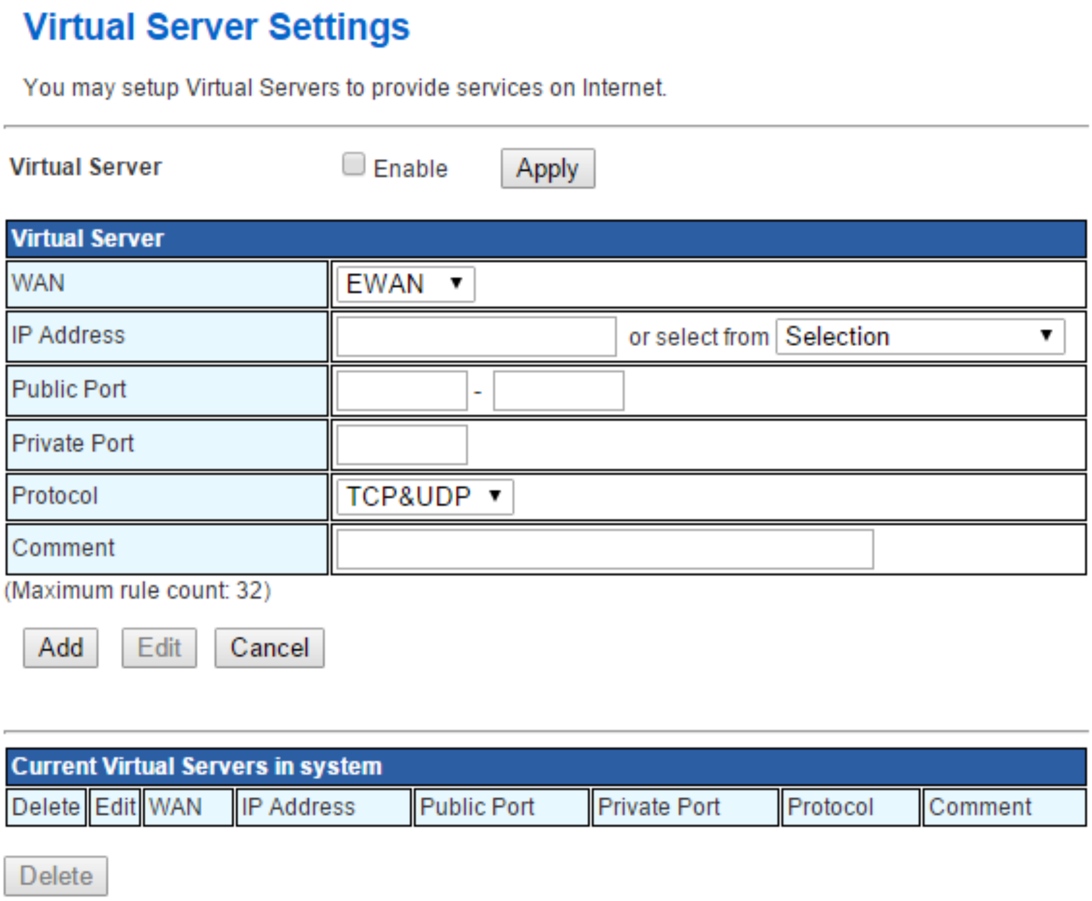
In TCP/IP and UDP networks a port is a 16-bit number used to identify which application program (usually a server) incoming connections should be delivered to. Some ports have numbers that are pre-assigned to them by the IANA (the Internet Assigned Numbers Authority), and these are referred to as “well-known ports”. Servers follow the well-known port assignments so clients can locate them.

If you wish to run a server on your network that can be accessed from the WAN (i.e. from other machines on the Internet that are outside your local network), or any application that can accept incoming connections (e.g. Peer-to-peer/P2P software such as instant messaging applications and P2P file-sharing applications) and are using NAT (Network Address Translation), then you will usually need to configure your router to forward these incoming connection attempts using specific ports to the PC on your network running the application. You will also need to use port forwarding if you want to host an online game server. The reason for this is that when using NAT, your publicly accessible IP address will be used by and point to your router, which then needs to deliver all traffic to the private IP addresses used by your

PCs. Please see the WAN configuration section of this manual for more information on NAT.

The device can be configured as a virtual server so that remote users accessing services such as Web or FTP services via the public (WAN) IP address can be automatically redirected to local servers in the LAN network. Depending on the requested service (TCP/UDP port number), the device redirects the external service request to the appropriate server within the LAN network.

This part is only available when NAT is enabled.



Virtual Server Settings

You may setup Virtual Servers to provide services on Internet.

Virtual Server ☐ Enable [Apply]

Virtual Server	
WAN	EWAN ▾
IP Address	or select from Selection ▾
Public Port	-
Private Port	
Protocol	TCP&UDP ▾
Comment	

(Maximum rule count: 32)

[Add] [Edit] [Cancel]

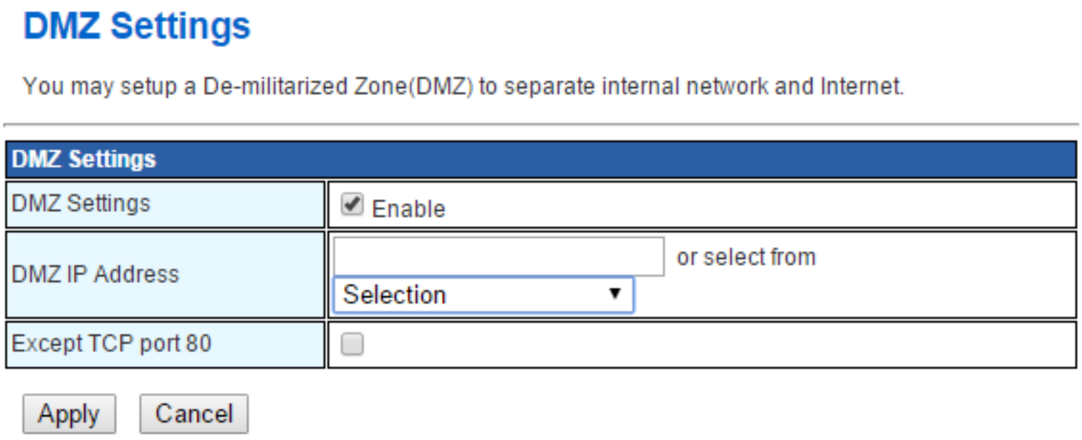
Current Virtual Servers in system

Delete	Edit	WAN	IP Address	Public Port	Private Port	Protocol	Comment

[Delete]

DMZ

The DMZ Host is a local computer exposed to the Internet. When setting a particular internal IP address as the DMZ Host, all incoming packets will be checked by Firewall and NAT algorithms before being passed to the DMZ host, when a packet received does not use a port number used by any other Virtual Server entries.



DMZ Settings

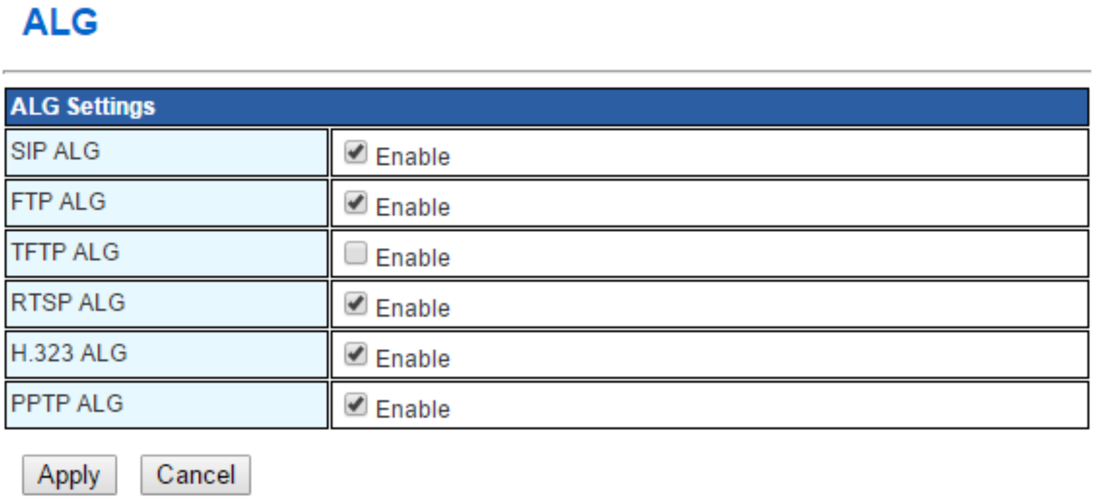
You may setup a De-militarized Zone(DMZ) to separate internal network and Internet.

DMZ Settings	
DMZ Settings	☑ Enable
DMZ IP Address	or select from Selection ▾
Except TCP port 80	☐

[Apply] [Cancel]

ALG

The ALG Controls enable or disable protocols over application layer.



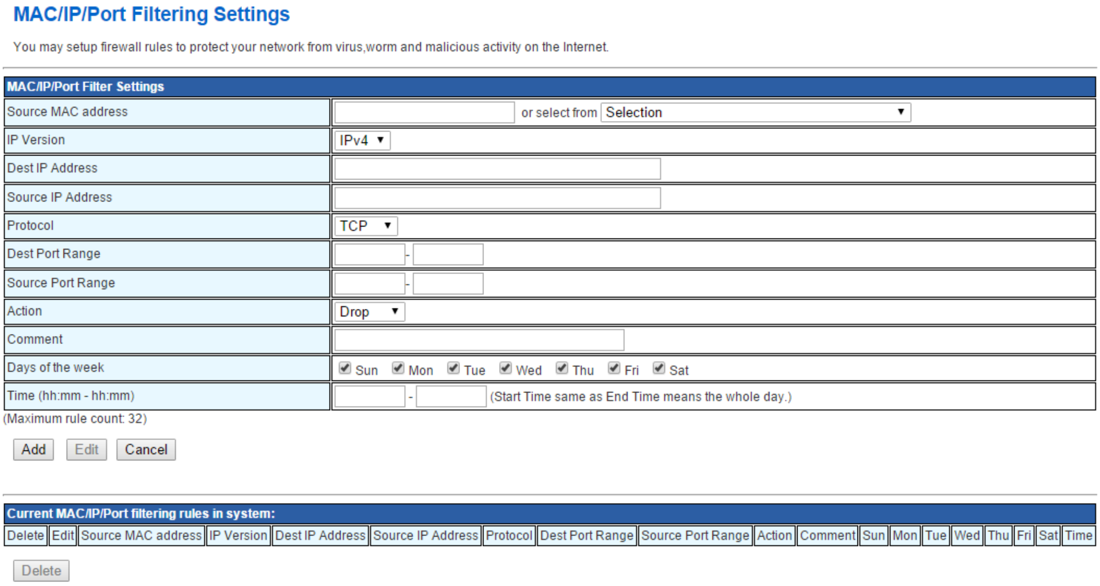
ALG

ALG Settings	
SIP ALG	☑ Enable
FTP ALG	☑ Enable
TFTP ALG	□ Enable
RTSP ALG	☑ Enable
H.323 ALG	☑ Enable
PPTP ALG	☑ Enable

Firewall

MAC/IP/Port Filtering

IP filtering enables you to configure your router to block specified internal/external users (IP address) from Internet access, or you can disable specific service requests (Port number) to /from Internet.



MAC/IP/Port Filtering Settings

You may setup firewall rules to protect your network from virus,worm and malicious activity on the Internet.

MAC/IP/Port Filter Settings	
Source MAC address	or select from Selection
IP Version	IPv4
Dest IP Address	
Source IP Address	
Protocol	TCP
Dest Port Range	-
Source Port Range	-
Action	Drop
Comment	
Days of the week	☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat
Time (hh:mm - hh:mm)	- (Start Time same as End Time means the whole day.)

(Maximum rule count: 32)

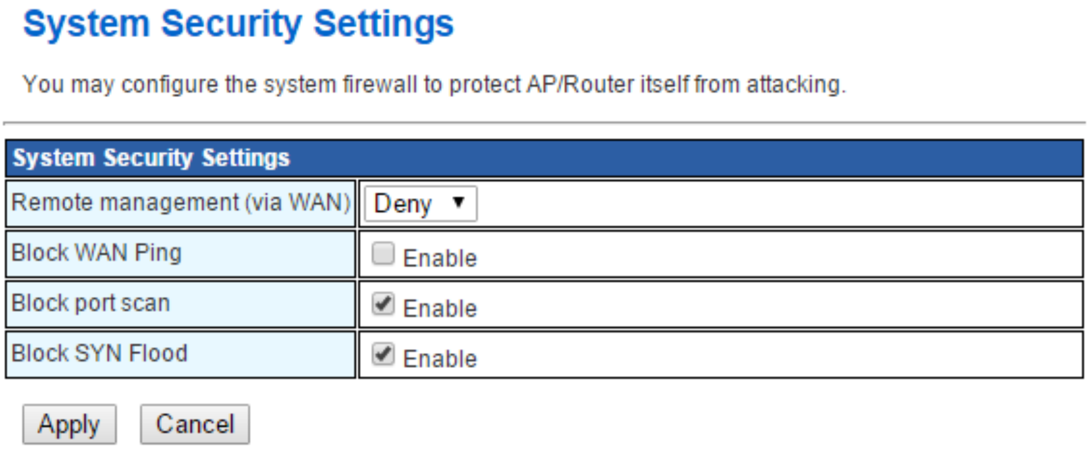
Current MAC/IP/Port filtering rules in system:

Delete	Edit	Source MAC address	IP Version	Dest IP Address	Source IP Address	Protocol	Dest Port Range	Source Port Range	Action	Comment	Sun	Mon	Tue	Wed	Thu	Fri	Sat	Time

Source MAC address: Specify the MAC address that will be applied to this rule.
IP Version: Select IP version IPv4 or IPv6.
Dest IP Address: Specify the destination IP address that will be applied to this rule.
Source IP Address: Specify the source IP address that will be applied to this rule.
Protocol: Specify the protocol (None/TCP/UDP/ICMP) that will be applied to this rule.
Dest Port Range: Enter the destination port range if protocol sets to TCP or UDP.
Source Port Range: Enter the source port range if protocol sets to TCP or UDP.
Action: Specify the action when the traffic is match to this rule.
Comment: Comment for this rule.
Days of the week: The rule will only be activated on specified days.
Time: The rule will only be activated on specified time.

System Security

This page allows to setup the security protection for device self.



System Security Settings

You may configure the system firewall to protect AP/Router itself from attacking.

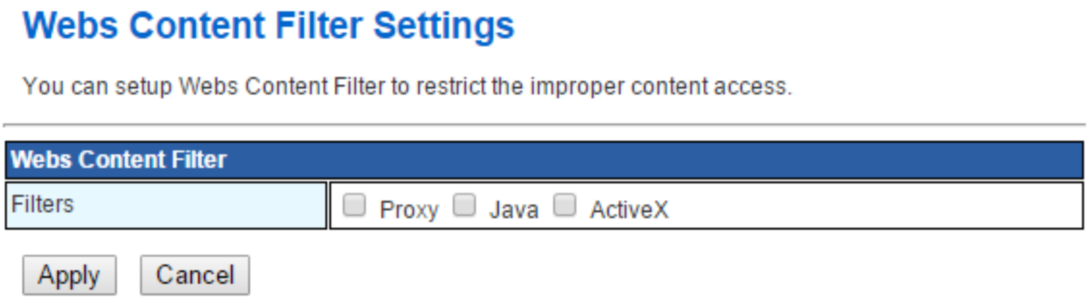
System Security Settings	
Remote management (via WAN)	Deny ▼
Block WAN Ping	□ Enable
Block port scan	☑ Enable
Block SYN Flood	☑ Enable

Content Filtering

The Content Filtering includes Web Content, Web URL and Web Host filtering.

Web Content Filtering

User can block the Proxy, Java or Active X that embedded in Web page content.



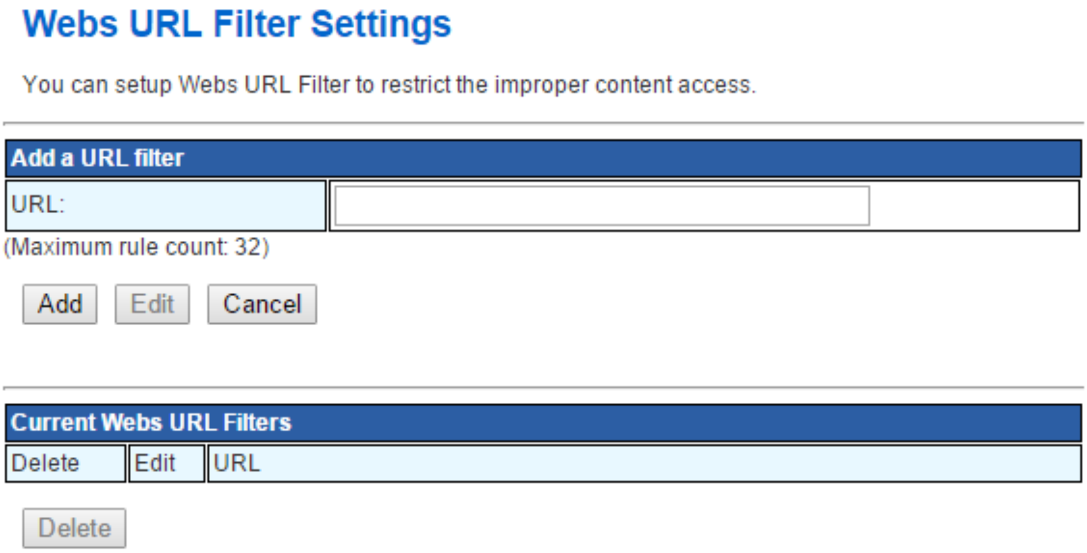
Webs Content Filter Settings

You can setup Webs Content Filter to restrict the improper content access.

Webs Content Filter	
Filters	□ Proxy □ Java □ ActiveX

Web URL Filtering

If website's URL matches the pre-defined URL here, the connection will be blocked.



Webs URL Filter Settings

You can setup Webs URL Filter to restrict the improper content access.

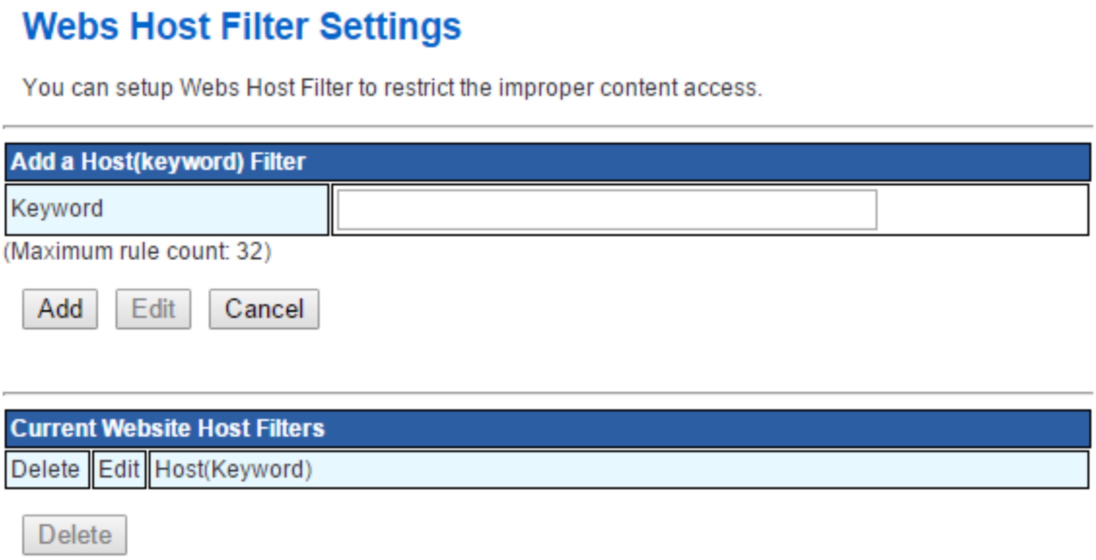
Add a URL filter	
URL:	

(Maximum rule count: 32)

Current Webs URL Filters		
Delete	Edit	URL

Web Host Filtering

If any part of the website's URL matches the pre-defined word, the connection will be blocked.



Webs Host Filter Settings

You can setup Webs Host Filter to restrict the improper content access.

Add a Host(keyword) Filter	
Keyword	

(Maximum rule count: 32)

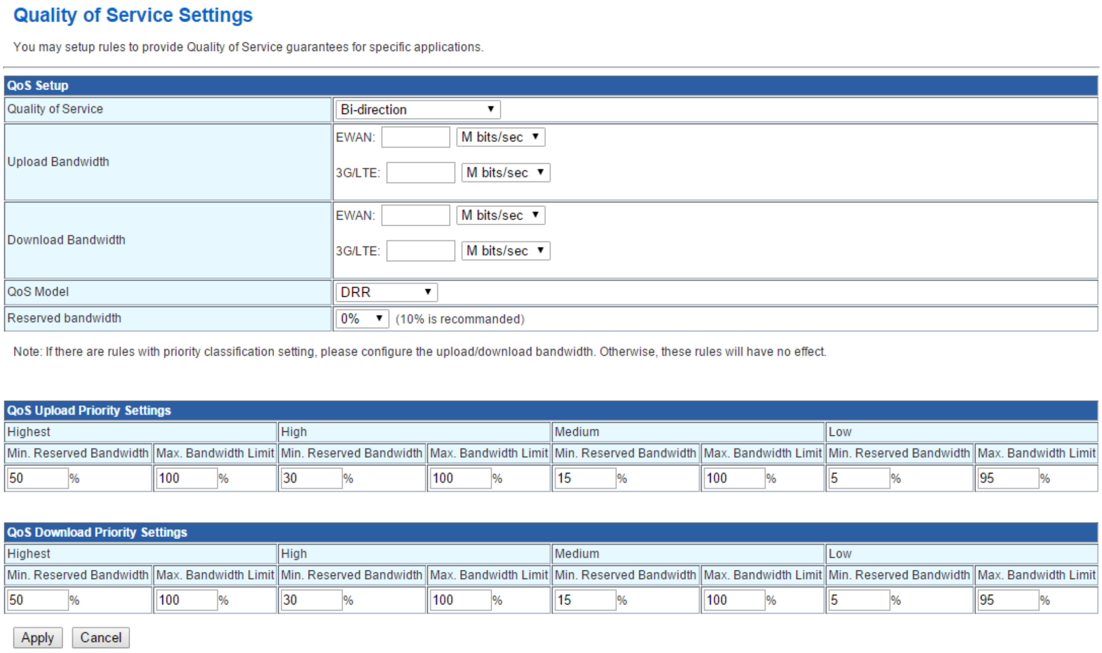
Current Website Host Filters		
Delete	Edit	Host(Keyword)

QoS

QoS or Quality of Service allows your Router to help prioritize the data packet flow in your Router and network. This is very important for time sensitive applications such as VoIP where it may help prevent dropped calls. Large amounts of non-critical data can be scaled so as not to affect these prioritized sensitive real-time programs.

QoS

This page allows to setup QoS for Bi-direction or Upload only or Download only. There are four levels (Highest/High/Medium/Low) and user can define the weight for each level here.



Quality of Service Settings

You may setup rules to provide Quality of Service guarantees for specific applications.

QoS Setup	
Quality of Service	Bi-direction ▼
Upload Bandwidth	EWAN: ＿ M bits/sec ▼ 3G/LTE: ＿ M bits/sec ▼
Download Bandwidth	EWAN: ＿ M bits/sec ▼ 3G/LTE: ＿ M bits/sec ▼
QoS Model	DRR ▼
Reserved bandwidth	0% ▼ (10% is recommanded)

Note: If there are rules with priority classification setting, please configure the upload/download bandwidth. Otherwise, these rules will have no effect.

QoS Upload Priority Settings

Highest		High		Medium		Low	
Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit
50 %	100 %	30 %	100 %	15 %	100 %	5 %	95 %

QoS Download Priority Settings

Highest		High		Medium		Low	
Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit	Min. Reserved Bandwidth	Max. Bandwidth Limit
50 %	100 %	30 %	100 %	15 %	100 %	5 %	95 %

Quality of Service: Specify the QoS for the traffic direction.

Upload Bandwidth: Specify the upload bandwidth for EWAN or 3G/LTE connection.

Download Bandwidth: Specify the download bandwidth for EWAN or 3G/LTE connection.

QoS Model: Select the QoS model (DRR/SPQ/SPQ+DRR/Remark only).

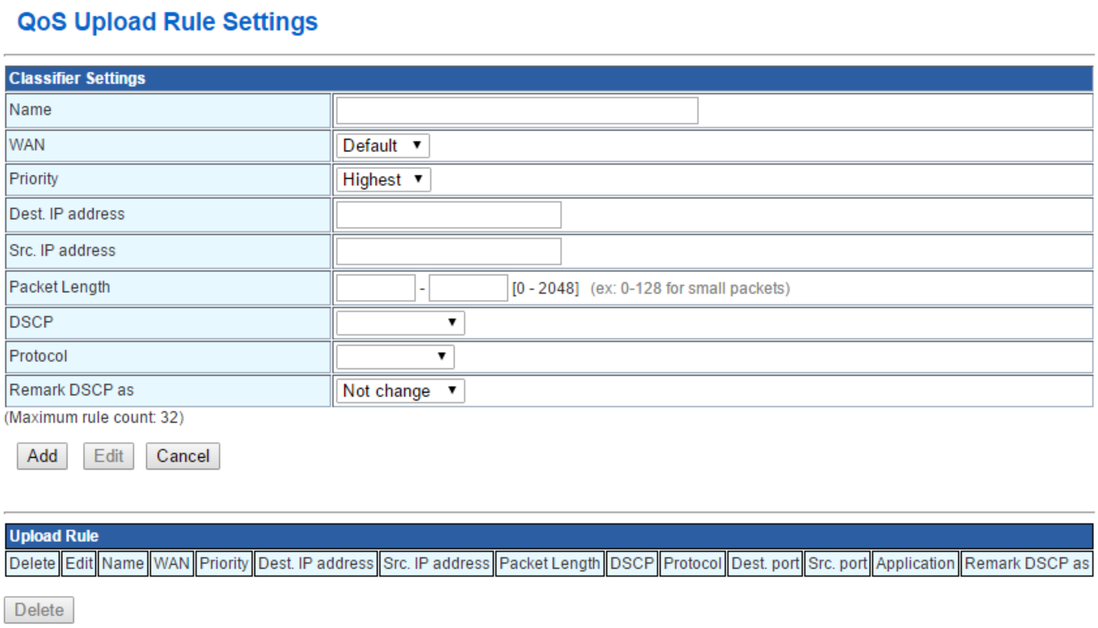
Reserved bandwidth: The percentage of reserved bandwidth here is for none IP traffic and apply to both upload and download direction.

QoS Upload Priority Settings: Specify the percentage for each level. Medium level is default level for all none match IP traffic.

QoS Download Priority Settings: Specify the percentage for each level. Medium level is default level for all none match IP traffic.

Upload Rule (LAN to WAN)

This page allows to create the rule for upload IP traffic. (LAN to WAN)



QoS Upload Rule Settings

Classifier Settings	
Name	
WAN	Default ▾
Priority	Highest ▾
Dest. IP address	
Src. IP address	
Packet Length	- [0 - 2048] (ex: 0-128 for small packets)
DSCP	▾
Protocol	▾
Remark DSCP as	Not change ▾

(Maximum rule count: 32)

Upload Rule

Delete	Edit	Name	WAN	Priority	Dest. IP address	Src. IP address	Packet Length	DSCP	Protocol	Dest. port	Src. port	Application	Remark DSCP as

Name: Specify the name for this rule.

WAN: Select the WAN interface that should be used for this rule.

Priority: Specify the priority when the upload IP traffic match this rule.

Dest. IP address: Specify the destination IP address.

Src. IP address: Specify the source IP address.

Packet Length: Specify the packet length range to hook upload IP traffic.

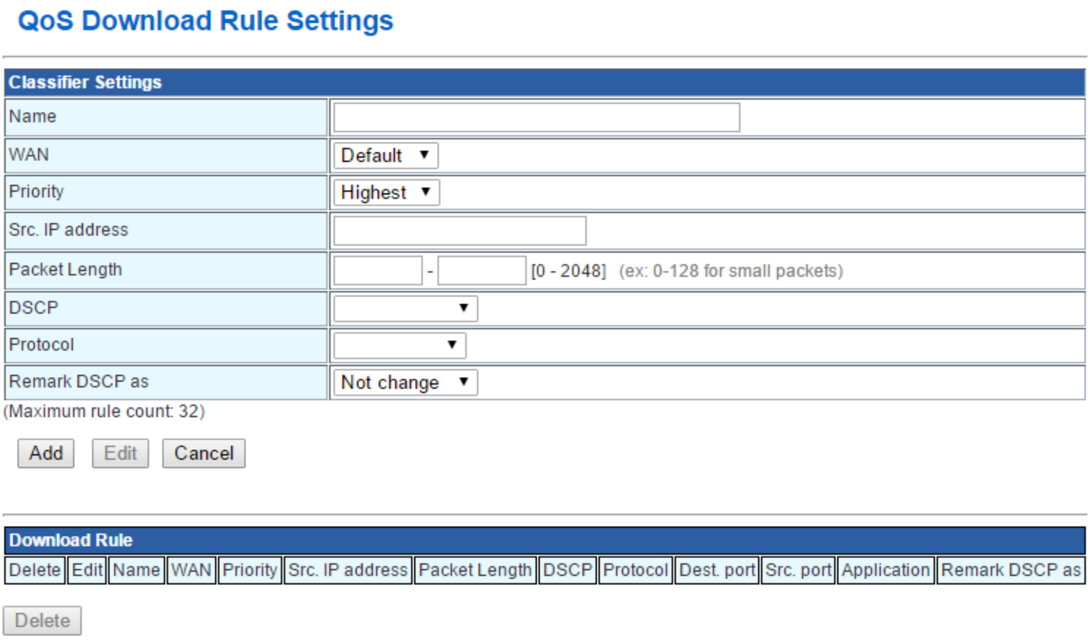
DSCP: Select the DSCP mark that should be hooked in upload IP traffic.

Protocol: Select the protocol that should be hooked upload IP traffic. If TCP or UDP selected, need to specify the port range as well.

Remark DSCP as: Change the original DSCP mark in upload IP traffic if this option set.

Download Rule

This page allows to create the rule for download IP traffic. (WAN to LAN)



QoS Download Rule Settings

Classifier Settings	
Name	
WAN	Default ▼
Priority	Highest ▼
Src. IP address	
Packet Length	- [0 - 2048] (ex: 0-128 for small packets)
DSCP	▼
Protocol	▼
Remark DSCP as	Not change ▼

(Maximum rule count: 32)

Download Rule

Delete	Edit	Name	WAN	Priority	Src. IP address	Packet Length	DSCP	Protocol	Dest. port	Src. port	Application	Remark DSCP as

Name: Specify the name for this rule.

WAN: Select the WAN interface that should be used for this rule.

Priority: Specify the priority when the download IP traffic match this rule.

Dest. IP address: Specify the destination IP address.

Src. IP address: Specify the source IP address.

Packet Length: Specify the packet length range to hook download IP traffic.

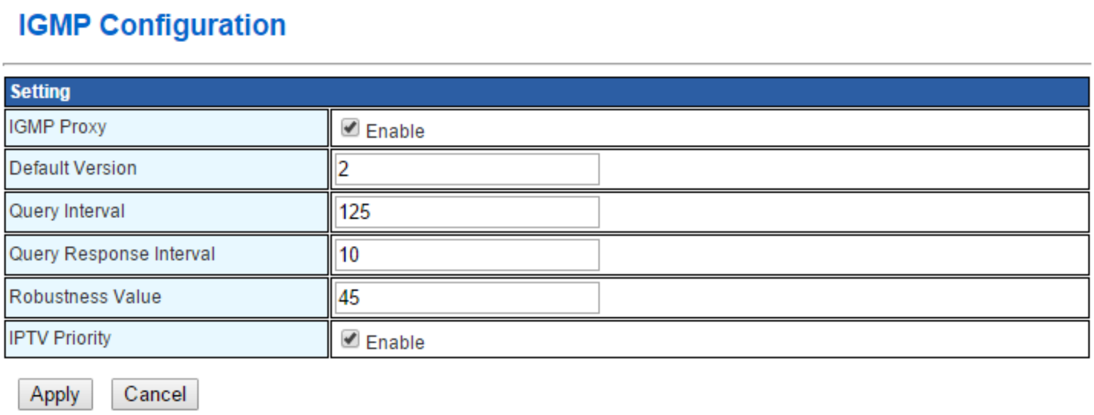
DSCP: Select the DSCP mark that should be hooked in download IP traffic.

Protocol: Select the protocol that should be hooked download IP traffic. If TCP or UDP selected, need to specify the port range as well.

Remark DSCP as: Change the original DSCP mark in download IP traffic if this option set.

Multicast

Multicast is one of the three network transmission modes, Unicast, Multicast, and Broadcast. It is a transmission mode that supports point-to-multipoint connections between the sender and the recipient. IGMP protocol is used to establish and maintain the relationship between IP host and the host directly connected multicast router. IGMP stands for Internet Group Management Protocol, it is a communications protocols used to manage the membership of Internet Protocol multicast groups. IGMP is used by IP hosts and the adjacent multicast routers to establish multicast group members. There are three versions for IGMP that is IGMPv1, IGMPv2 and IGMPv3.



IGMP Configuration

Setting	
IGMP Proxy	☑ Enable
Default Version	2
Query Interval	125
Query Response Interval	10
Robustness Value	45
IPTV Priority	☑ Enable

IGMP Proxy: Enable/Disable the IGMP Proxy. If disabled, the IPTV will not work with NAT enabled mode.

Default Version: Enter the supported IGMP version, 1-3, default is IGMP v2.

Query Interval: Enter the periodic query interval time (sec) the multicast router sending the query message to hosts to understand the group membership information.

Query Response Interval: Enter the response interval time (sec).

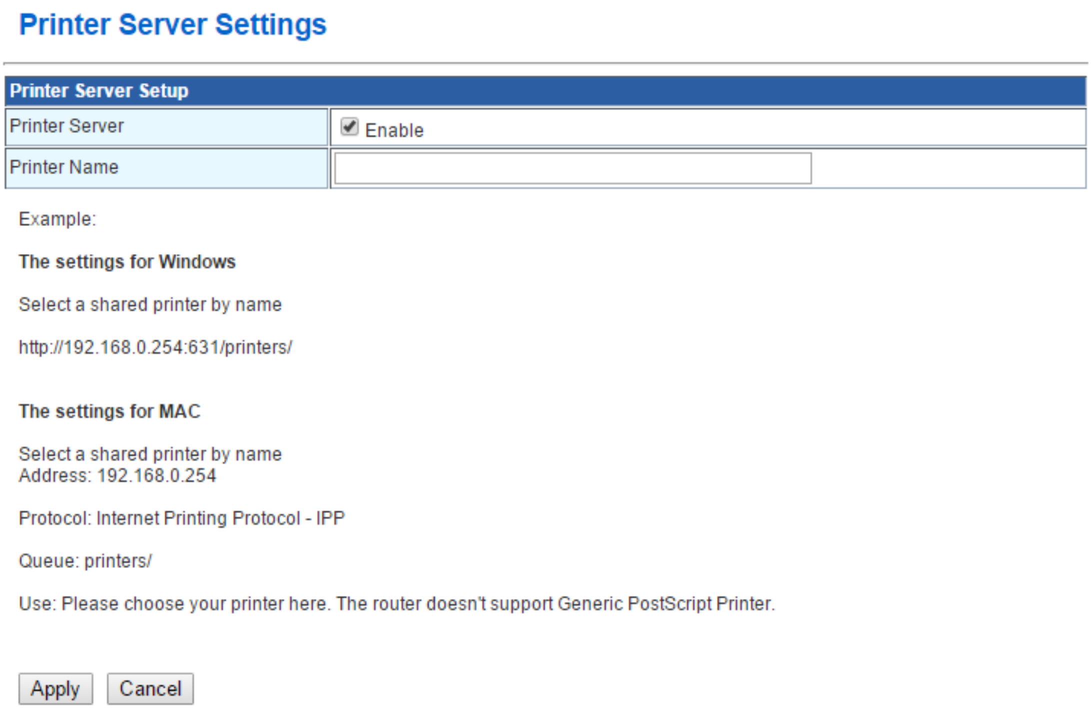
Robustness Value: Enter the router robustness parameter, the greater the robustness value, the more robust the Querier is.

IPTV Priority: Enable to reserve the bandwidth for IPTV traffic and always highest priority than any rule in QoS setting page.

USB

Printer Server

This page allows you to enable / disable printer support. Click the Apply / Save button when you are finished.



Printer Server Settings

Printer Server Setup	
Printer Server	☑ Enable
Printer Name	

Example:

The settings for Windows

Select a shared printer by name

http://192.168.0.254:631/printers/

The settings for MAC

Select a shared printer by name
Address: 192.168.0.254

Protocol: Internet Printing Protocol - IPP

Queue: printers/

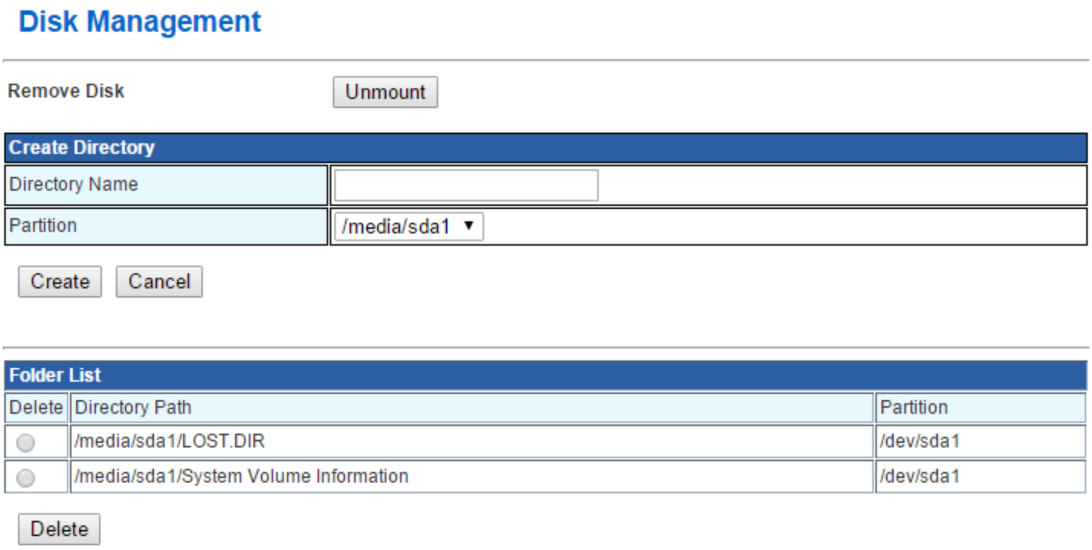
Use: Please choose your printer here. The router doesn't support Generic PostScript Printer.

Storage

This part provides FTP and SAMBA service for attached storage and do folder management.

Disk

Once the storage attached, user can create or delete the folder from this page.



Disk Management

Remove Disk [Unmount]

Create Directory	
Directory Name	
Partition	/media/sda1 ▼

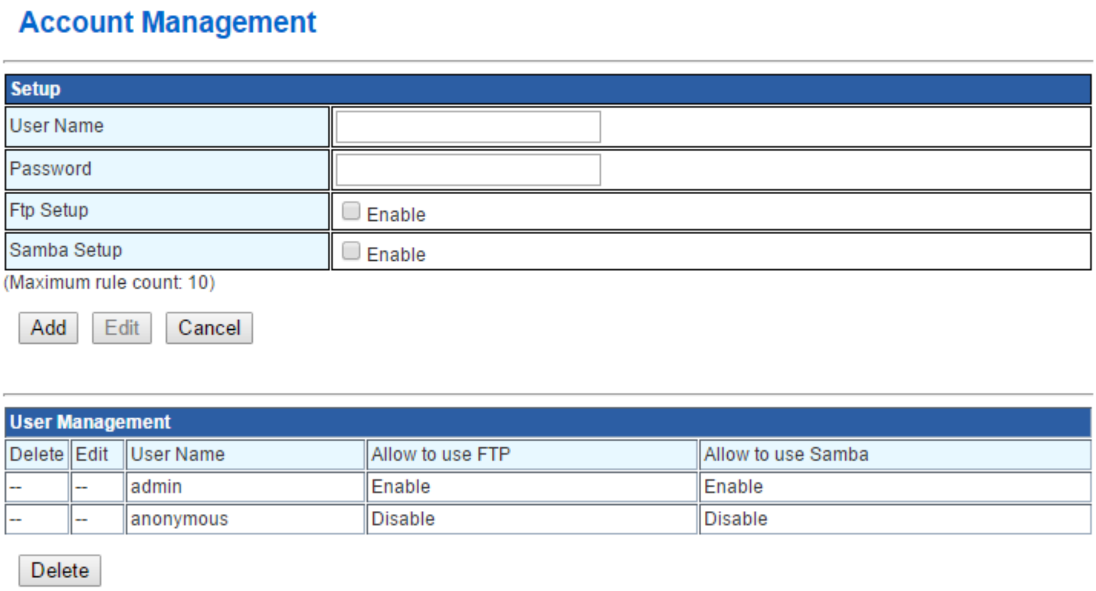
[Create] [Cancel]

Folder List		
Delete	Directory Path	Partition
○	/media/sda1/LOST.DIR	/dev/sda1
○	/media/sda1/System Volume Information	/dev/sda1

[Delete]

Account Management

Create the user account for FTP or Samba service.



Account Management

Setup	
User Name	
Password	
Ftp Setup	□ Enable
Samba Setup	□ Enable

(Maximum rule count: 10)

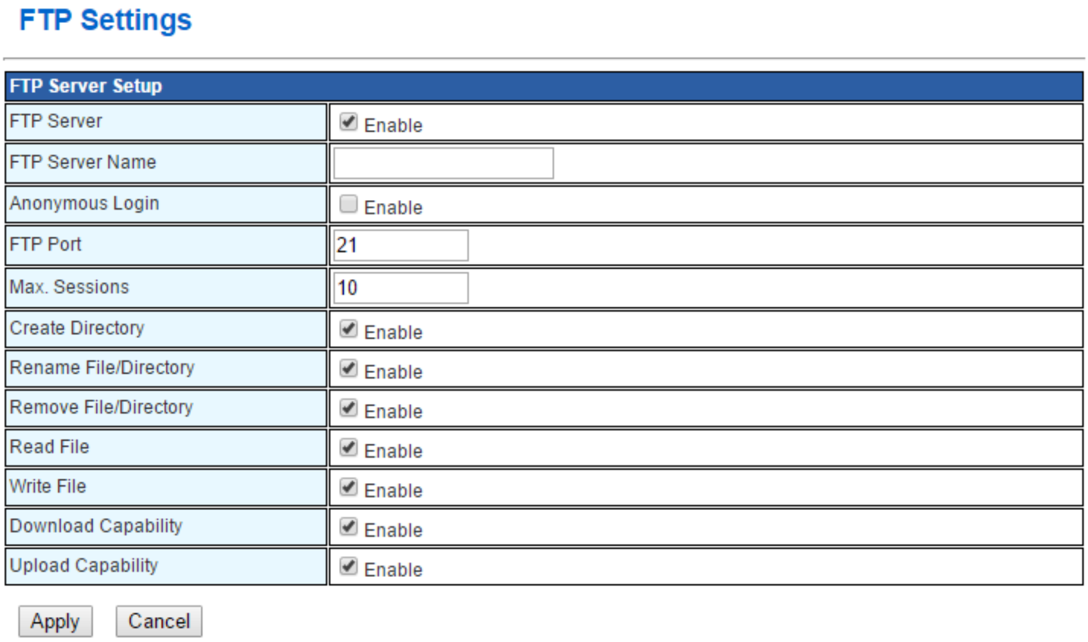
[Add] [Edit] [Cancel]

User Management				
Delete	Edit	User Name	Allow to use FTP	Allow to use Samba
--	--	admin	Enable	Enable
--	--	anonymous	Disable	Disable

[Delete]

FTP Server

This page allows to Enable/Disable FTP server service on device and also can setup the access right for all login users.



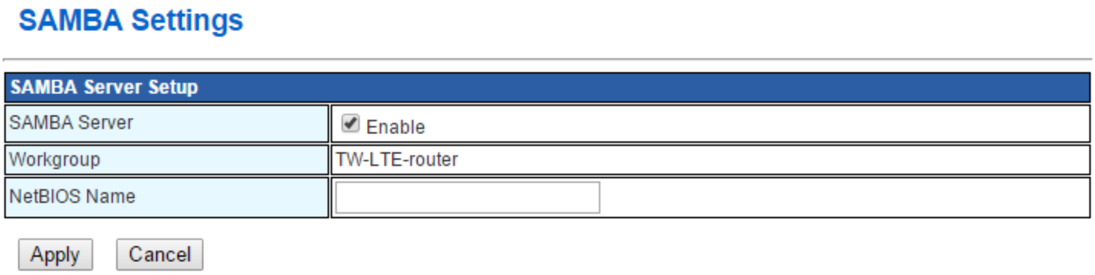
FTP Settings

FTP Server Setup

FTP Server	☑ Enable
FTP Server Name	
Anonymous Login	□ Enable
FTP Port	21
Max. Sessions	10
Create Directory	☑ Enable
Rename File/Directory	☑ Enable
Remove File/Directory	☑ Enable
Read File	☑ Enable
Write File	☑ Enable
Download Capability	☑ Enable
Upload Capability	☑ Enable

SAMBA Server

This page allows to Enable/Disable Samba server service on device.



SAMBA Settings

SAMBA Server Setup

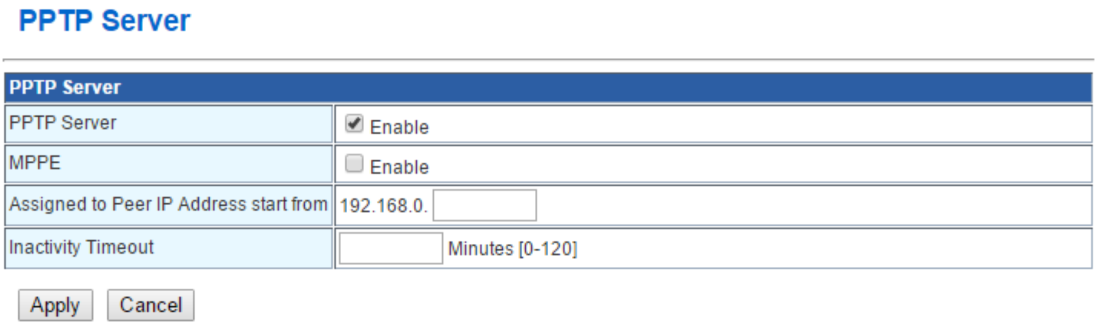
SAMBA Server	☑ Enable
Workgroup	TW-LTE-router
NetBIOS Name	

VPN

This device supports three different kind of VPN service, PPTP Server/Client, L2TP Server/Client and GRE tunnel.

PPTP Server

This page allows user to enable the PPTP server for remote PPTP client login.



PPTP Server

PPTP Server	
PPTP Server	☑ Enable
MPPE	□ Enable
Assigned to Peer IP Address start from	192.168.0.
Inactivity Timeout	Minutes [0-120]

PPTP Server: Enable/Disable PPTP Server function.

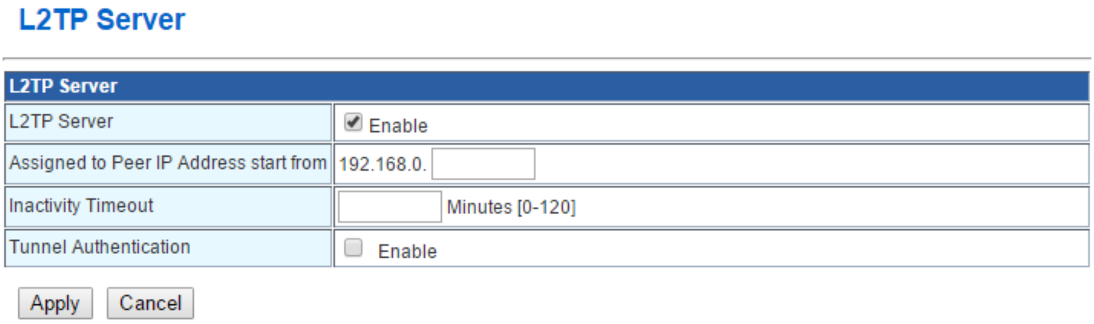
MPPE: Enable/Disable data encryption for PPTP connection.

Assigned to Peer IP Address start from: The IP address that will be assigned to client side. This IP address should not be in DHCP Server Pool range.

Inactivity Timeout: Setup the period of time that PPTP connection should be disconnected if no traffic on it. Blank or 0 means always on.

L2TP Server

This page allows user to enable the L2TP server for remote L2TP client login.



L2TP Server

L2TP Server	
L2TP Server	☑ Enable
Assigned to Peer IP Address start from	192.168.0.
Inactivity Timeout	Minutes [0-120]
Tunnel Authentication	□ Enable

L2TP Server: Enable/Disable L2TP Server function.

Assigned to Peer IP Address start from: The IP address that will be assigned to client side. This IP address should not be in DHCP Server Pool range.

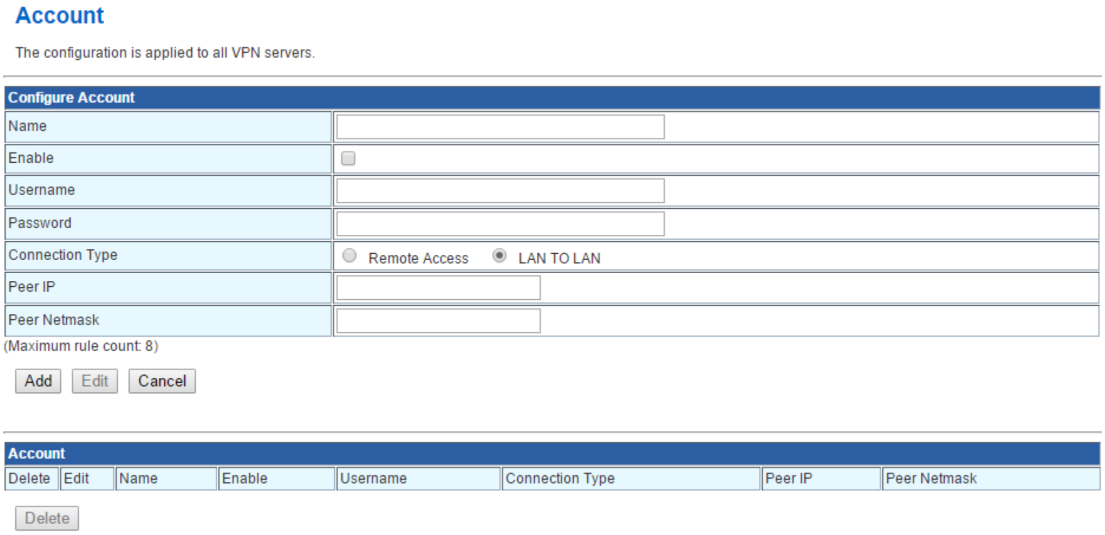
Inactivity Timeout: Setup the period of time that PPTP connection should be disconnected if no traffic on it. Blank or 0 means always on.

Tunnel Authentication: Enable/Disable the tunnel authentication.

Secret: Enter the secret key for tunnel authentication.

Account

This page allows to create the account for both PPTP and L2TP server login. Maximum user account is up to 8 and only two accounts can work at the same time.



Account

The configuration is applied to all VPN servers.

Configure Account	
Name	
Enable	□
Username	
Password	
Connection Type	○ Remote Access ● LAN TO LAN
Peer IP	
Peer Netmask	

(Maximum rule count: 8)

Account

Delete	Edit	Name	Enable	Username	Connection Type	Peer IP	Peer Netmask

Name: Enter the name for this account setting.

Enable: Enable/Disable this account.

Username: Enter the username for login authentication.

Password: Enter the password for login authentication.

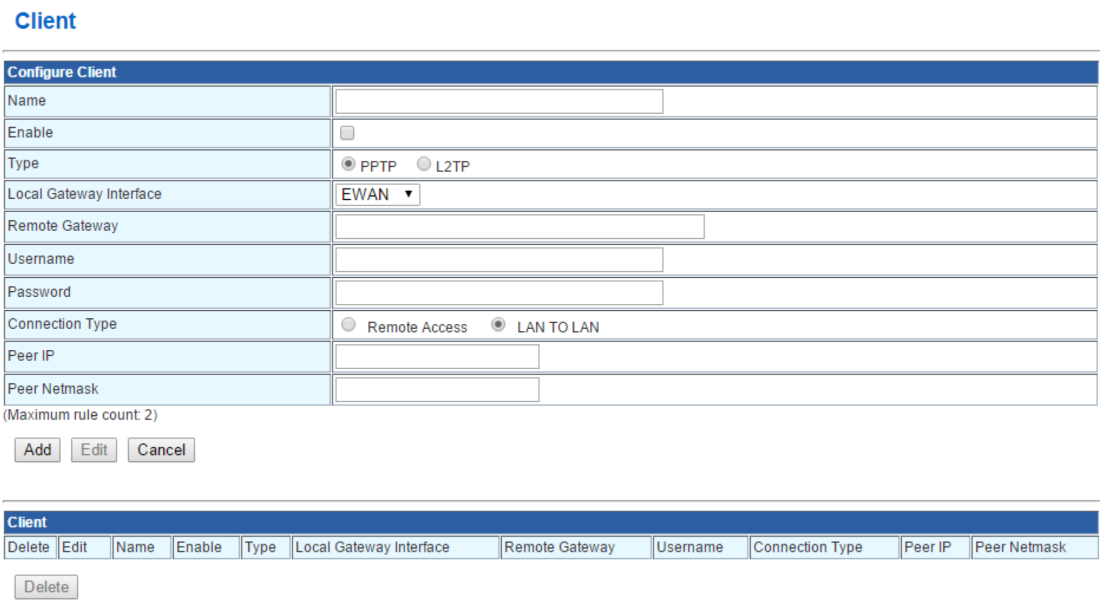
Connection Type: Define the connection type **Remote Access** or **LAN to LAN**.

Peer IP: Enter the peer side LAN IP address for **LAN to LAN** type.

Peer Netmask: Enter the peer side LAN subnet mask for **LAN to LAN** type.

Client

This page allows to setup a PPTP/L2TP client to login to remote PPTP/L2TP server.



Client

Configure Client	
Name	
Enable	□
Type	● PPTP ○ L2TP
Local Gateway Interface	EWAN ▾
Remote Gateway	
Username	
Password	
Connection Type	○ Remote Access ● LAN TO LAN
Peer IP	
Peer Netmask	

(Maximum rule count: 2)

Client

Delete	Edit	Name	Enable	Type	Local Gateway Interface	Remote Gateway	Username	Connection Type	Peer IP	Peer Netmask

Name: Enter the name for this client rule.

Enable: Enable/Disable this client rule.

Type: Specify the type for this client connection.

Local Gateway Interface: Specify the WAN interface for this client connection.

Remote Gateway: Specify the remote PPTP/L2TP server IP address or domain name.

Username: Enter the username for PPTP/L2TP login authentication.

Password: Enter the password for PPTP/L2TP login authentication.

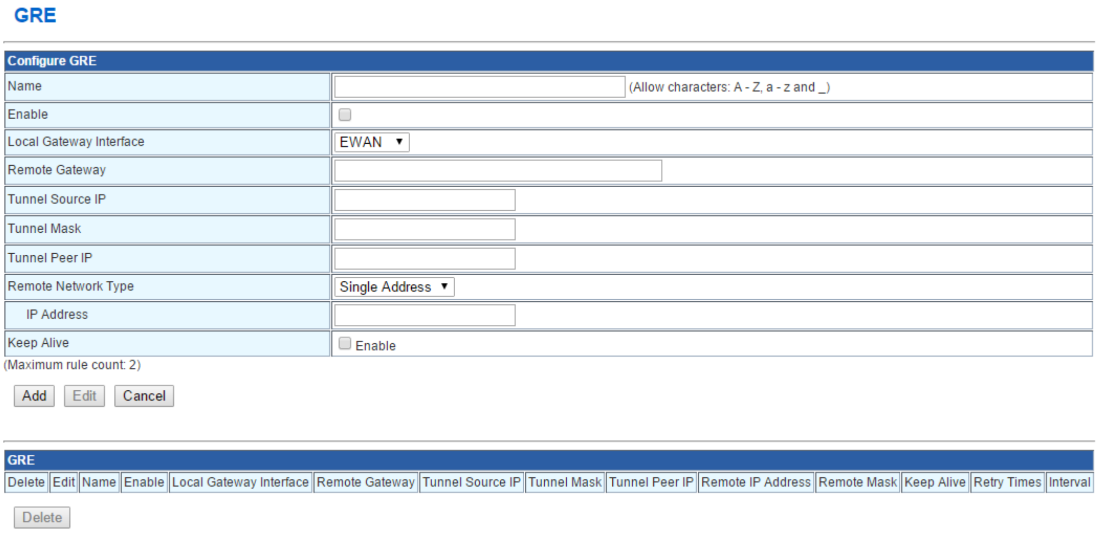
Connection Type: Specify the connection type is **Remote Access** or **LAN to LAN**.

Peer IP: Enter the peer side LAN IP address for **LAN to LAN** type.

Peer Netmask: Enter the peer side LAN subnet mask for **LAN to LAN** type.

GRE

Generic Routing Encapsulation (GRE) is a tunneling protocol that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol network.



GRE

Configure GRE	
Name	(Allow characters: A - Z, a - z and _)
Enable	□
Local Gateway Interface	EWAN ▼
Remote Gateway	
Tunnel Source IP	
Tunnel Mask	
Tunnel Peer IP	
Remote Network Type	Single Address ▼
IP Address	
Keep Alive	□ Enable

(Maximum rule count: 2)

GRE

Delete	Edit	Name	Enable	Local Gateway Interface	Remote Gateway	Tunnel Source IP	Tunnel Mask	Tunnel Peer IP	Remote IP Address	Remote Mask	Keep Alive	Retry Times	Interval

Name: Enter the name for this GRE Tunnel connection.

Enable: Enable the tunnel connection immediately after clicking Apply/Save button.

Local Gateway Interface: Select the correct WAN interface that will be used for establishing a GRE Tunnel.

Remote Gateway: Enter the remote WAN IP/Domain that will be used for establishing a GRE Tunnel.

Tunnel Source IP: Enter the IP address for local tunnel interface.

Tunnel Mask: Enter the net mask for local tunnel interface.

Tunnel Peer IP: Enter the IP address of remote tunnel interface.

Remote Network Type: Select the remote side is a client or subnet.

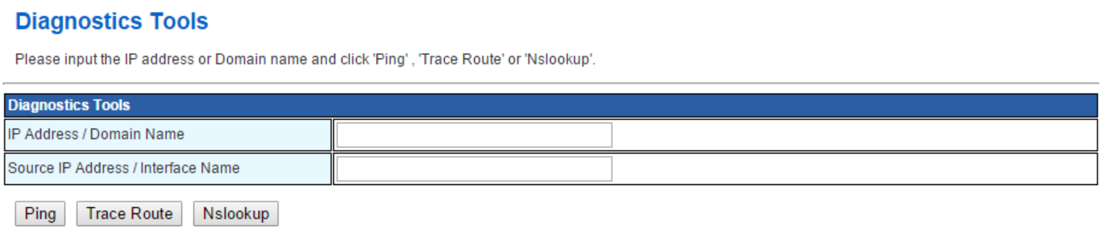
IP Address: Enter the IP address of remote client.

Mask: Enter the net mask of remote subnet when Remote Network Type sets to Subnet.

Keep Alive: Enable Keep Alive function for GRE Tunnel and can define the Retry Times and Interval once checked. This is follow Cisco's GRE Tunnel Keep Alive mechanism.

Diagnostics Tools

This page will help you to diagnostic the status of your Network. You can use "Ping", "Trace Route" and "Nslookup" methods in this page. After you input the IP address or Domain name, click **Ping**, **Trace Route** or **Nslookup** button.



Diagnostics Tools

Please input the IP address or Domain name and click 'Ping' , 'Trace Route' or 'Nslookup'.

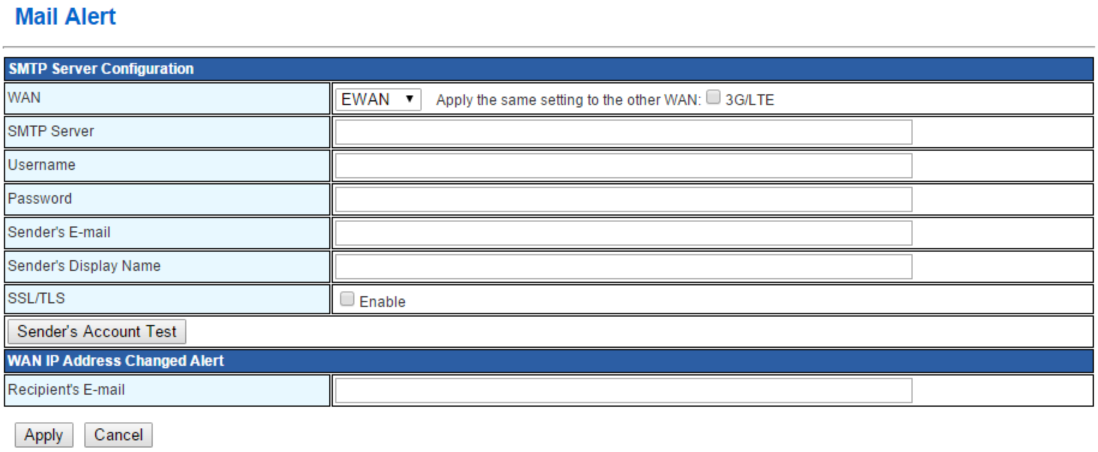
Diagnostics Tools	
IP Address / Domain Name	
Source IP Address / Interface Name	

Management

The Management directory features an array of options designed to help you get the most out of your Router.

Mail Alert

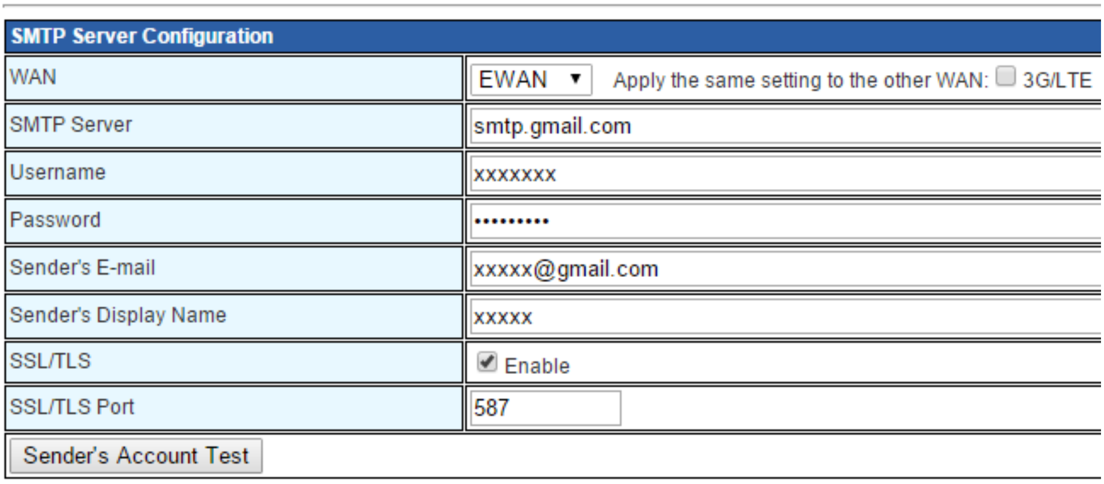
Mail Alert allows the router to send notification mail when WAN IP changed. User can fill in the SMTP server information from ISP and click **Sender's Account Test** button to check the SMTP setting is correct or not. Then enter the mail address who will receive the notification mail in the field of "Recipient's E-Mail".



Mail Alert

SMTP Server Configuration	
WAN	EWAN ▾ Apply the same setting to the other WAN: □ 3G/LTE
SMTP Server	
Username	
Password	
Sender's E-mail	
Sender's Display Name	
SSL/TLS	□ Enable
Sender's Account Test	
WAN IP Address Changed Alert	
Recipient's E-mail	

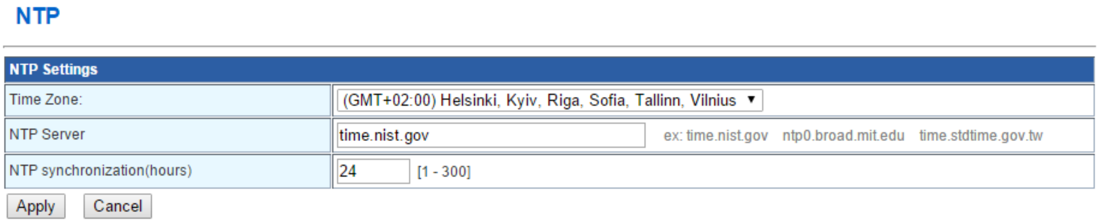
Below is an example with Gmail account.



SMTP Server Configuration	
WAN	EWAN ▼ Apply the same setting to the other WAN: □ 3G/LTE
SMTP Server	smtp.gmail.com
Username	xxxxxxx
Password	•••••••••
Sender's E-mail	xxxxx@gmail.com
Sender's Display Name	xxxxx
SSL/TLS	☑ Enable
SSL/TLS Port	587

NTP

Setup the Time Zone and NTP server here to correct and sync the time on the router.

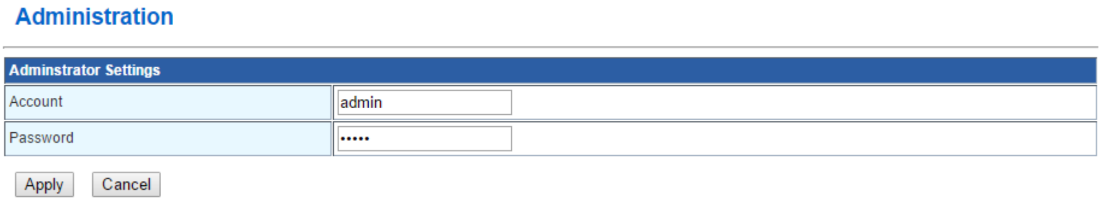


NTP

NTP Settings	
Time Zone:	(GMT+02:00) Helsinki, Kyiv, Riga, Sofia, Tallinn, Vilnius ▼
NTP Server	time.nist.gov ex: time.nist.gov ntp0.broad.mit.edu time.stdtime.gov.tw
NTP synchronization(hours)	24 [1 - 300]

Administration

The administrator username and password can be changed by this page.

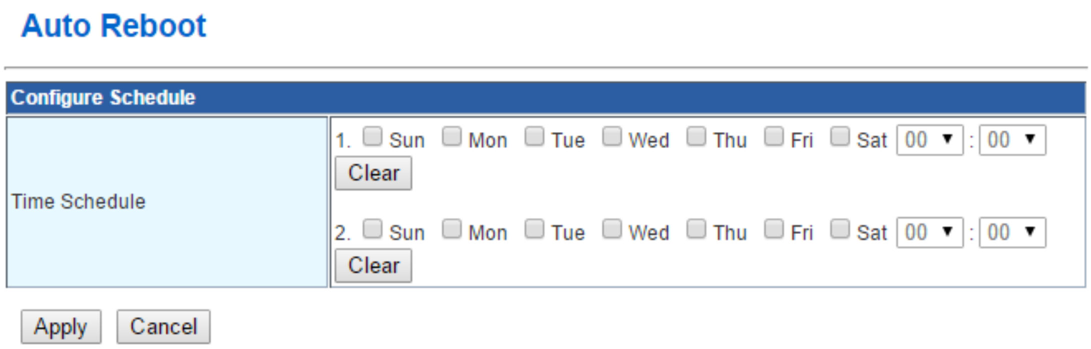


Administration

Adminstrator Settings	
Account	admin
Password	•••••

Auto Reboot

User can specify two time schedules to force device to reboot automatically.

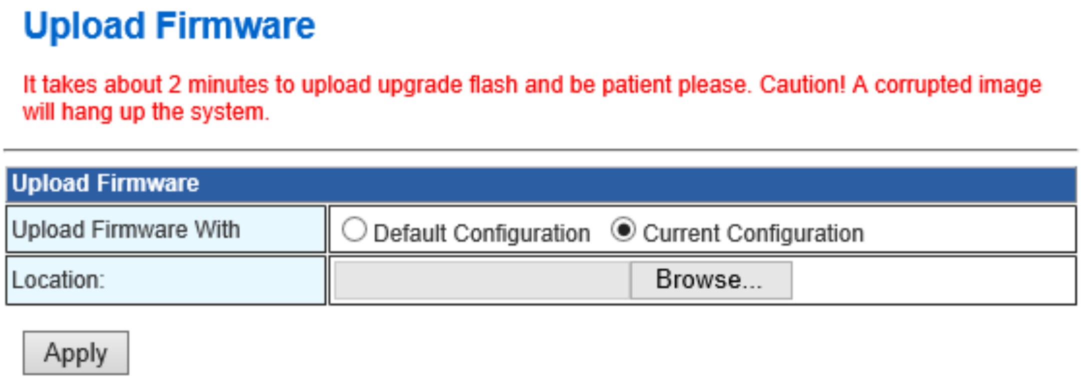


Auto Reboot

Configure Schedule	
Time Schedule	1. □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat 00 ▼ : 00 ▼ Clear 2. □ Sun □ Mon □ Tue □ Wed □ Thu □ Fri □ Sat 00 ▼ : 00 ▼ Clear

Upload Firmware

The firmware keeps enhancement and improvement. This page allows user to upgrade to a new firmware once it is available.



Upload Firmware

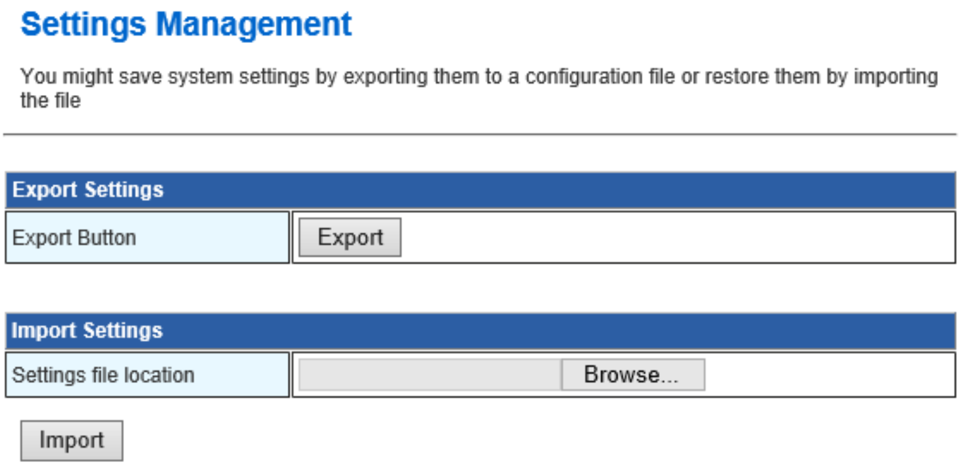
It takes about 2 minutes to upload upgrade flash and be patient please. Caution! A corrupted image will hang up the system.

Upload Firmware	
Upload Firmware With	○ Default Configuration ● Current Configuration
Location:	Browse...

Important: Please don't power off the router during upgrade, otherwise it may damage your router.

Settings Management

This page allows user to backup or restore the router settings to/from file.



Settings Management

You might save system settings by exporting them to a configuration file or restore them by importing the file

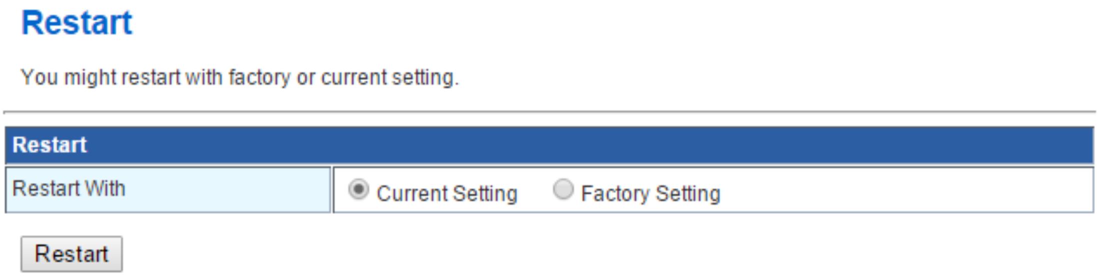
Export Settings	
Export Button	Export

Import Settings	
Settings file location	Browse...

Import

Restart

You can restart the router manually with current setting or factory setting.



Restart

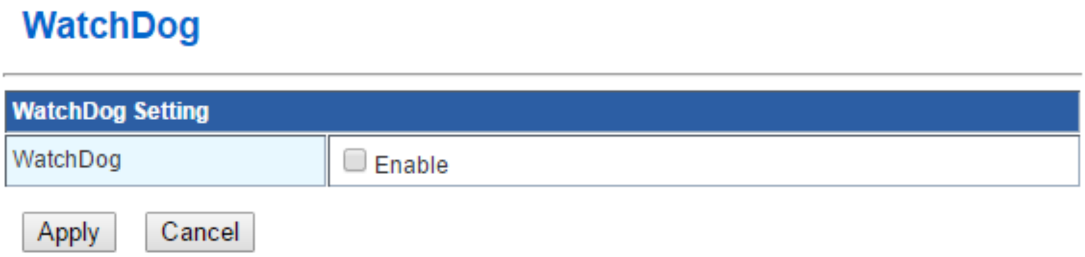
You might restart with factory or current setting.

Restart	
Restart With	● Current Setting ○ Factory Setting

Restart

WatchDog

WatchDog is a smart recovering function and helps router to back to normal state by restarting device automatically if any process locks the system.



WatchDog

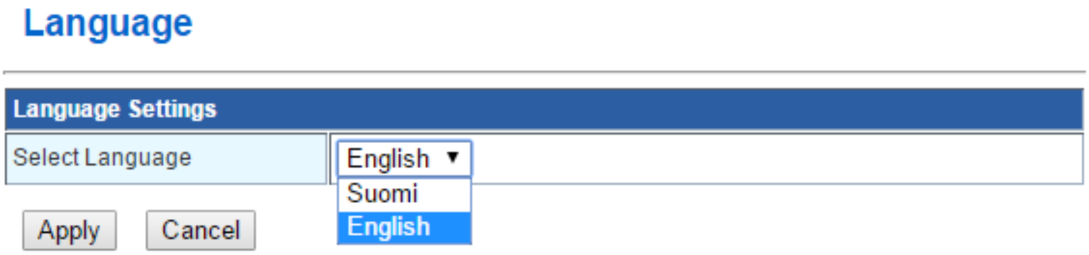
WatchDog Setting	
WatchDog	□ Enable

Apply Cancel

Note: Once WatchDog triggered, all the traffic through router will be terminated until system back to normal.

Language

You can select the language for the WEB GUI here. Just select the language you want and click **Apply** button and it can switch to new language immediately.


Language

Language Settings

Select Language: English