ISTRON

IWS SERIES
Industrial Dual Radio 2.4G+5GHz Concurrent Wireless Mesh AP/Client

User Manual

Copyright Notice

About This Manual

This user manual is intended to guide a professional installer to install and to configure the ISTRON Industrial Secured and Rugged LTE Serial Router. It includes procedures to assist you in avoiding unforeseen problems.

NOTE:

Only qualified and trained personnel should be involved with installation, inspection, and repairs of this router.

TABLE OF CONTENTS

1. Introduction

1.1 Overview

IWS SERIES series is designed for IIoT application by dual band concurrent Wireless LAN Radio. IWS SERIES is equipped with high performance Quad core ARM processor with 5GHz IEEE 802.11ac Wave 2 and 2.4G 802.11n WLAN radio, up to 866M+300Mbps high throughput, 2 Gigabit Ethernet port are able to support Bridge/Router mode and powered by 802.3af PoE switch. It supports MESH self-healing wireless network, DHCP Server, NAT and secure VPN connectivity can reach 150Mbps IPsec performance in 256-bit encryption.

1.2 Major Features

Below are the major features of IWS SERIES Series:

- Quad-Core ARM Processor
- IEEE 802.11ac Wave 2, compatible with 802.11a/b/g/n
- Concurrent dual-band 2.4 G+5GHz radio, up to 866Mbps + 300Mbps Bandwidth
- 2x SMA/N-type Antenna socket for 2.4GHz + 5GHz DBDC (Dual Band Dual Concurrent)
- Dual Gigabit Ethernet ports in Router mode for WLAN/LAN to Eth-WAN routing
- Support IEEE 802.3af PoE P.D. Input
- **Qualcomm® Wi-Fi SON MESH Technology** (IWS SERIESM Series)
  - ■ Self-Healing auto rerouting through multi-hop (up to 4 hops and 10 nodes)
  - ■ Self-Configuring Plug-and-play via Wireless network with ViewMaster utility
- **Enhanced Cyber Security & Redundancy**
  - ■ Support Firewall for inbound/outbound traffic
  - ■ OpenVPN (server/client), IPsec for secure remote connection
  - ■ IPSec Performance >150Mbps @256-bit encryption
  - ■ Support L2TP with PPP, PAP, CHAP(LCP, IPCP)
  - ■ HTTPs/SSH secure login
  - ■ Support TACACS+ multi-user authentication for privileged user management
- Support Industrial IoT Cloud Server, AWS, Azure, Private IoT and communication protocol
- Slim size 110x106x40mm Din-Rail mounting design (IWS SERIESM/IWS SERIES)
- Support 24V(9-50V) DC Input (IWS SERIES)
- Wide range operating temperature -40~70˚C

2. Installation

This chapter introduces mechanical and contains information on installation and configuration procedures.

1.1.1 Product Package

Standard package includes:

roduct Unit
uick Installation Guide
oE Injector with AC Plug
able Gland
ounting kit

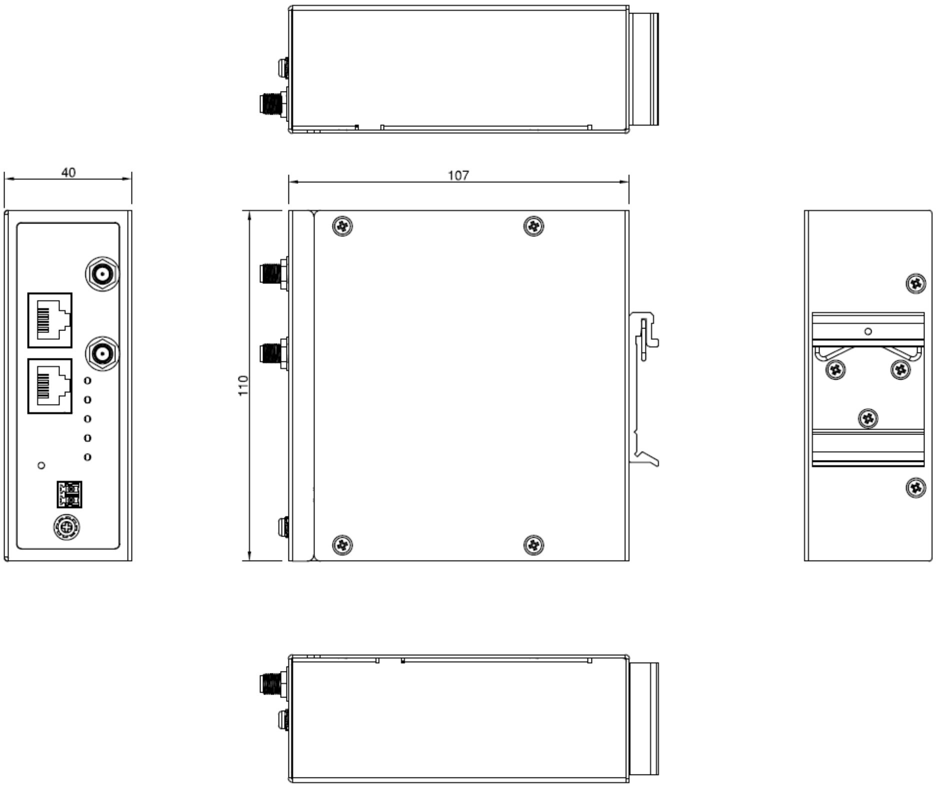
*Note: Antenna not included

1.1.2 Interface Installation

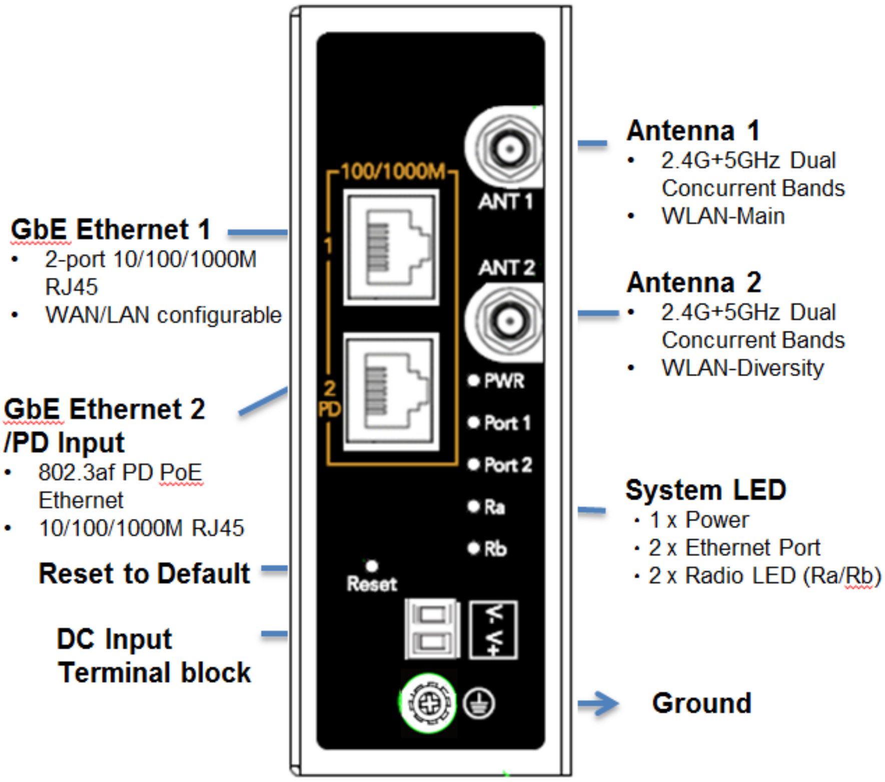
After unpacking the box, follow the steps below in order to properly connect the device.

2.2 IWS SERIES (DIN-Rail)

1.2.1 Dimension



1.2.2 Product Appearance



GbE Ethernet 1
- 2-port 10/100/1000M RJ45
- WAN/LAN configurable

GbE Ethernet 2 /PD Input
- 802.3af PD PoE Ethernet
- 10/100/1000M RJ45

Reset to Default

DC Input Terminal block

Antenna 1
- 2.4G+5GHz Dual Concurrent Bands
- WLAN-Main

Antenna 2
- 2.4G+5GHz Dual Concurrent Bands
- WLAN-Diversity

System LED
- 1 x Power
- 2 x Ethernet Port
- 2 x Radio LED (Ra/Rb)

Ground

1.2.3 Product Package (IWS SERIES)

Standard package includes:

roduct Unit
uick Installation Guide
WLAN Antenna, White
Attached Din Clip

Note: The model doesn’t offer PoE injector. If you need additional PoE injector or PoE switch, check with our sales contact window.

1.2.4 Interface Installation

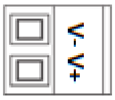
After unpacking the box, follow the steps below in order to properly connect the device.

1.2.4.1 Wiring Power Input

IWS SERIES supports standard IEEE 802.3af PoE Power Device (PD), it can be powered by PoE switch (P.S.E) or PoE injector. IWS SERIES equips with gigabit Ethernet ports and dual WLAN radio, it’s MUST to choose full gigabit PoE Switch with higher Ethernet bandwidth, for example the DP208, DP412, DP612.

The standard package in IWS SERIES-IP67 includes a PoE injector to power on IWS SERIES. It’s passive 48V (not standard 802.3af/at PoE) and available for AC 110V/220V Input. You can also choose standard IEEE 802.3af/af PoE Injector for powering.

The IWS SERIES supports DC terminal block with 24V(9~50V) DC input. The typical power input voltage is 24VDC. Wire the power positive(+) and native(-) correctly before turn on the power supply.



Wiring the Power Input through DC Terminal Block

1) Insert the positive and negative wires into the V+ and V- contact on the terminal block connector.

2) Tighten the wire-clamp screws.

3) Connect the power wires to suitable DC Switching type power supply. The input DC voltage should be in the range of the spec.

Wiring the Power Input through PoE Injector

1) Install PoE injector power cord.

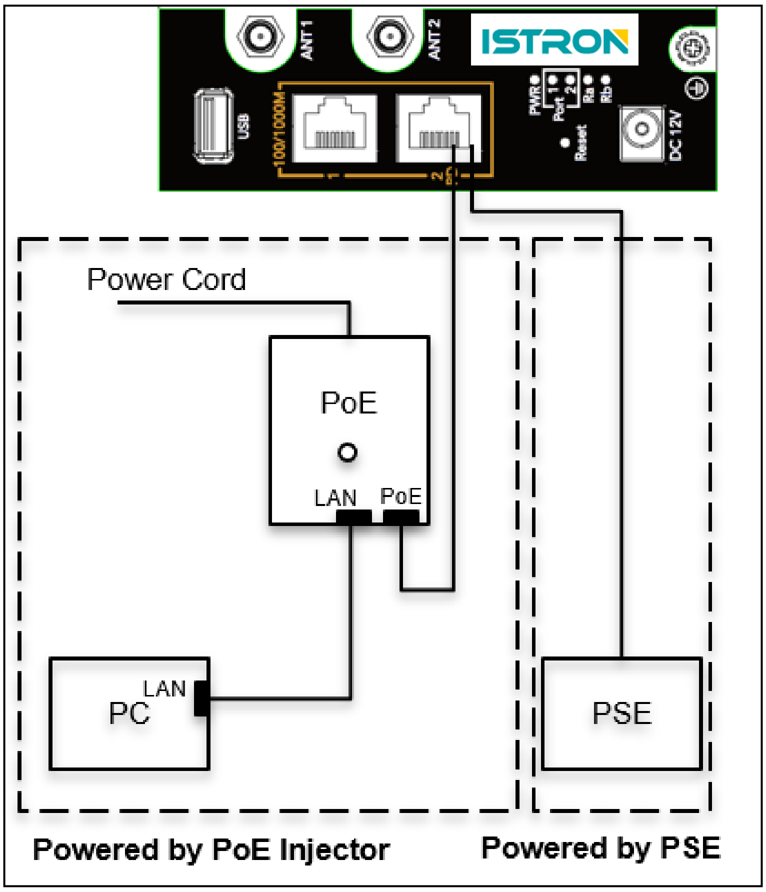
2) Install Ethernet cable between PoE ports of IWS SERIES and PoE injector.

3) Install Ethernet cable between LAN ports of IWS SERIES and PC/NB whenever proceeding WebGUI configuration.

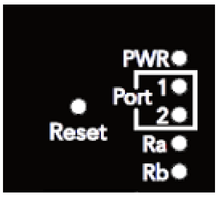
Wiring the Power Input through PSE switch

1) Install Ethernet cable between PoE ports of IWS SERIES and PSE switch

2) Install Ethernet cable between LAN ports of IWS SERIES and PSE switch whenever proceeding WebGUI configuration.



1.2.5 LED

	LED	Status	Description
	er	en On	er On
			Receiving Power
	t 1/2	en On	
		en Blinking	vity
	2.4GHz) 5GHz)	en On	node
		en Blinking	ion mode client connected
			ion mode/radio disabled

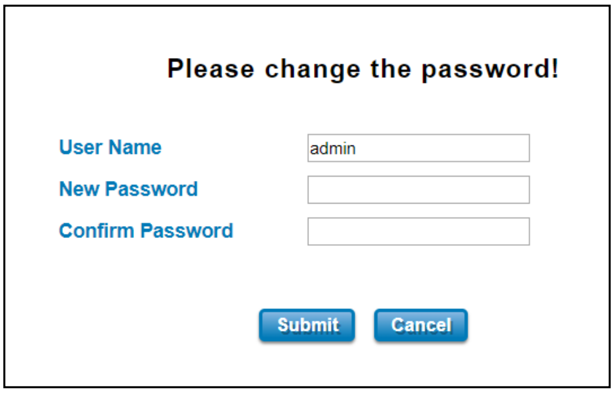
3. Web Management Configuration

To access the management interface, ISTRON router has two ways access mode through a network; they are web management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a router interface offering status information and a subset of device commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using telnet management which is offer configuration way through CLI Interface. This manual describes the procedures for Web Interface and how to configure and monitor the managed router only.

PREPARATION FOR WEB INTERFACE MANAGEMENT

ISTRON provides Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the router management on the network.

1. Plug the DC power to the router and connect router to computer.
2. Make sure that the router default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the router. For example, the PC and the router are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2)**. The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the router is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type **http://192.168.10.1** (or the IP address of the router). And then press **Enter** and the login page will appear.
7. Key in the **NEW User name and Password** in login screen while first Login. (There is no default user name and password for Security concern)
8. After you click OK, the Welcome page of the web-based management interface will appear.
9. On the left side you can see the list of software features, on the right side – available settings.



Please change the password!

User Name: admin

New Password:

Confirm Password:

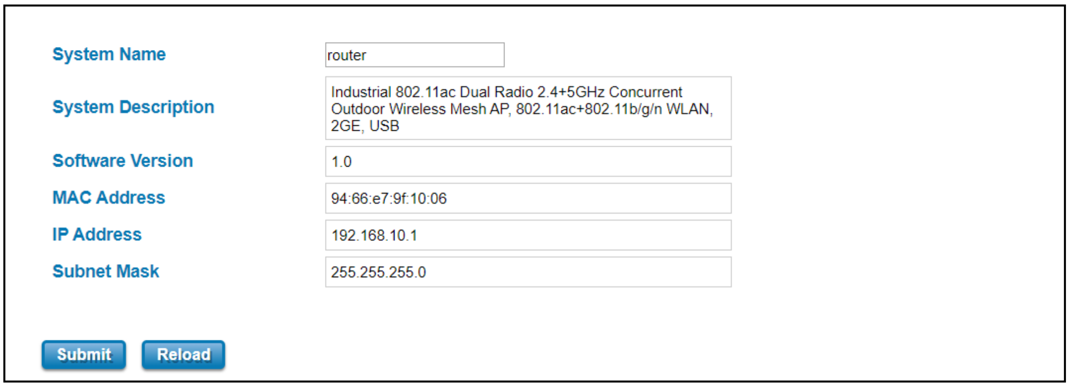
In this Web management for Featured Configuration, user will see all of ISTRON Router’s various configuration menus at the left side from the interface. Through this web management interface, user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the router on the network.

3.1 System

When the user login to the router, user will see the system section appear. This section provides all the basic setting and information or common setting from the router that can be configured by the administrator.
Following topics are included:

3.1.1 Information

Information section, this section shows the basic information from the router to make it easier to identify different router that is connected to User network and also it shows LAN Settings information. The figure below shows the interface of the Information section.



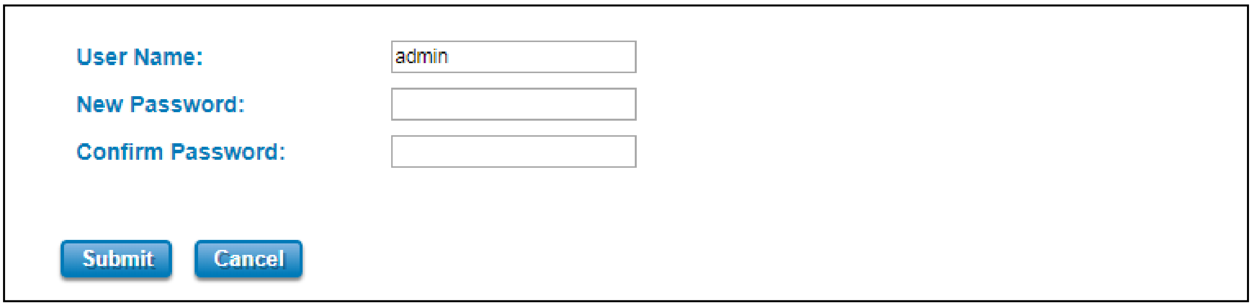
System Name	router
System Description	Industrial 802.11ac Dual Radio 2.4+5GHz Concurrent Outdoor Wireless Mesh AP, 802.11ac+802.11b/g/n WLAN, 2GE, USB
Software Version	1.0
MAC Address	94:66:e7:9f:10:06
IP Address	192.168.10.1
Subnet Mask	255.255.255.0

The description of the Information's interface is as below:

TERMS	DESCRIPTION
System Name	**Default: router** Set up a name to the device.
System Description	Display the name of the product.
Software Version	Display the firmware latest version that installed in the device.
MAC Address	Display the hardware's MAC address that assigned by the manufacturer.
IP Address	Display the IP Address of the device
Subnet Mask	Display the subnet mask of the device

3.1.2 Login Settings

ISTRON' router supports Login Setting that has several authentication methods. It is supported with TACACS+, Radius, and Multi-User Authentication. This Login Setting consists of two level, admin and guest. Where the admin level, it has the privilege to read and write and for the guest level the privilege is read only. Below is the **Login Setting** section for **admin level**.

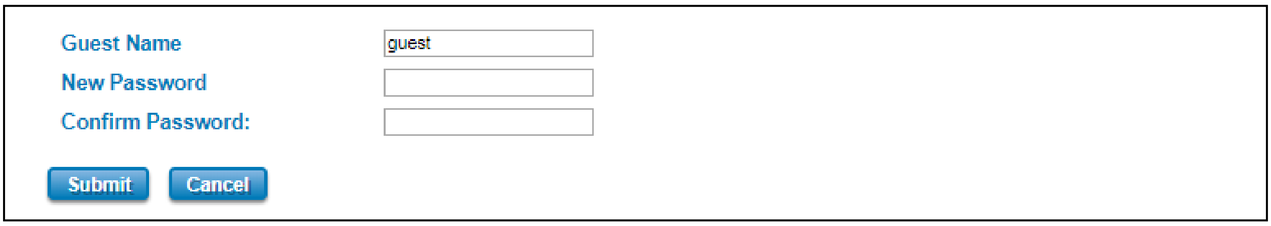


User Name:	admin
New Password:	
Confirm Password:	

With the Name first login setting is administrator user name level and the authority allow user to configure all of configuration parameters.

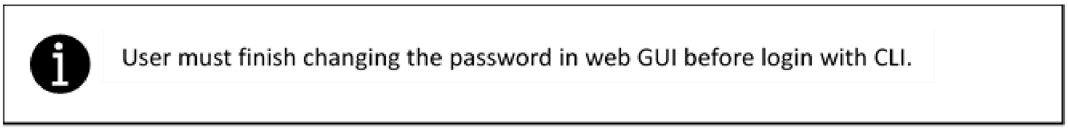
The Login Setting interface describes how to configure the system username and password for the web management login. To change the Name and Password, user just needs to input a new Name and New Password then confirm the new password in this section. Try to re-login with the new username and password.

Below is the interface for **guest level**.



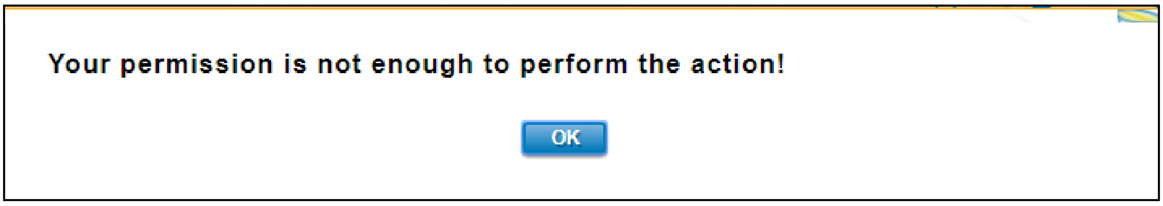
Guest Name	guest
New Password	
Confirm Password:	

With the Name default setting is **guest** and the authority allow user to read only all of configuration parameters.



User must finish changing the password in web GUI before login with CLI.

When user try to change the configuration, message will appear if user is not permitted to configure the configuration. Below is the interface.



Your permission is not enough to perform the action!

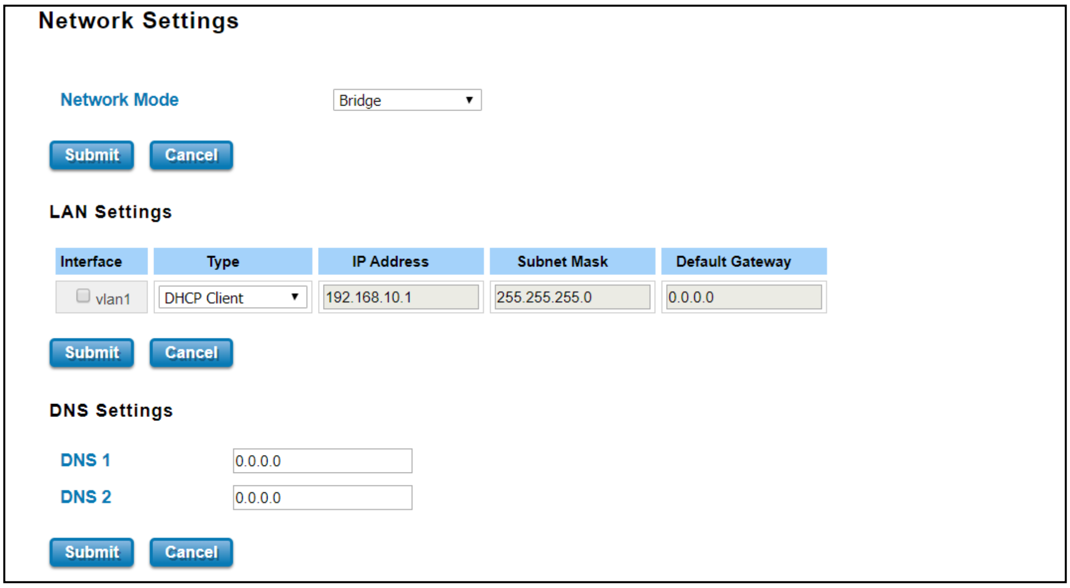
The description of the Login Setting interface is as below:

TERMS	DESCRIPTION
User Name/ Guest Name	**Default: admin/guest** Key in new username here.
New Password	Key in new password here.
Confirm Password	Re-type the new password again to confirm it.

After finishing configure the Username and Password, click on **Submit** to apply the configuration. Don’t forget to **Save** the configuration.

3.1.3 Network Settings

The Network Setting section allows users to configure both IPv4 values for management access over the network. ISTRON' router supports IPv4 and can be managed through either of these address types. Below is the IP Setting interface for **Bridge Mode**.



Network Settings

Network Mode: Bridge

LAN Settings

Interface	Type	IP Address	Subnet Mask	Default Gateway
□ vlan1	DHCP Client	192.168.10.1	255.255.255.0	0.0.0.0

DNS Settings

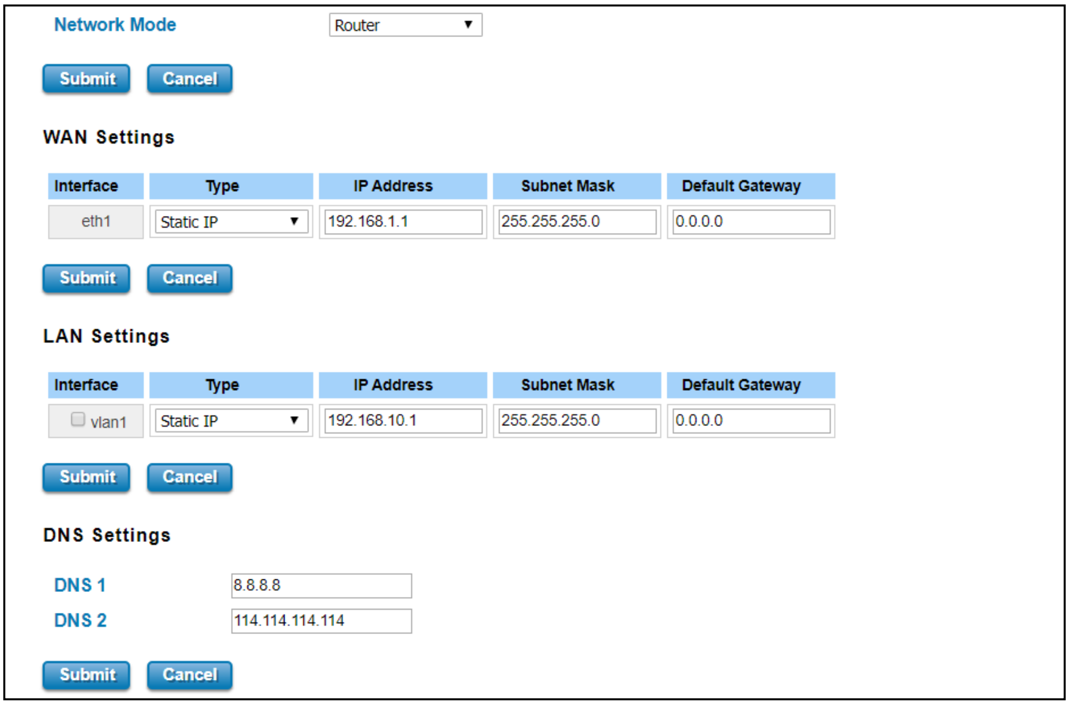
DNS 1: 0.0.0.0

DNS 2: 0.0.0.0

The description of the columns is as below:

TERMS	DESCRIPTION
Type	User can select to DHCP or Static IP to activate the function. **DHCP:** Select DHCP to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.10.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

And below is the IP Setting interface for the **Router Mode w**here it supports with the WAN port on port 2. User can configure the WAN Settings.



Network Mode: Router

WAN Settings

Interface	Type	IP Address	Subnet Mask	Default Gateway
eth1	Static IP	192.168.1.1	255.255.255.0	0.0.0.0

LAN Settings

Interface	Type	IP Address	Subnet Mask	Default Gateway
□ vlan1	Static IP	192.168.10.1	255.255.255.0	0.0.0.0

DNS Settings

DNS 1: 8.8.8.8

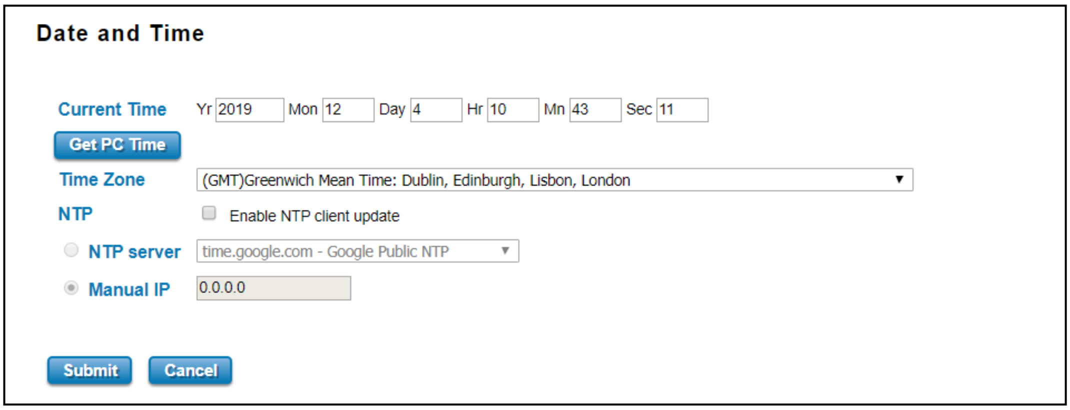
DNS 2: 114.114.114.114

The description of the columns is as below:

TERMS	DESCRIPTION
Type	User can select to DHCP Client or Static IP to activate the function. **DHCP Client:** Select DCHP Client to activate DHCP Client Function, no need to assign IP Address and received IP Address from DHCP Server. **Static IP:** Select Static IP to configure the IP configuration manually
IP Address	**Default: 192.168.1.1** Set up the IP address reserved by User network for User device. If DHCP Client function is enabled, no need to assign an IP address to device as it will be overwritten by DHCP server and shown here.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.
Gateway IP Address	**Default: 0.0.0.0.** Assign the gateway for the device here.
DNS 1	Specifies the IP address of the DNS server 1 that used in user network.
DNS 2	Specifies the IP address of the DNS server 2 that used in user network.

3.1.4 Date and Time

The ISTRON router has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.



Date and Time

Current Time	Yr 2019 Mon 12 Day 4 Hr 10 Mn 43 Sec 11
Time Zone	(GMT)Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London
NTP	□ Enable NTP client update
○ NTP server	time.google.com - Google Public NTP
● Manual IP	0.0.0.0

The description of the columns is as below:

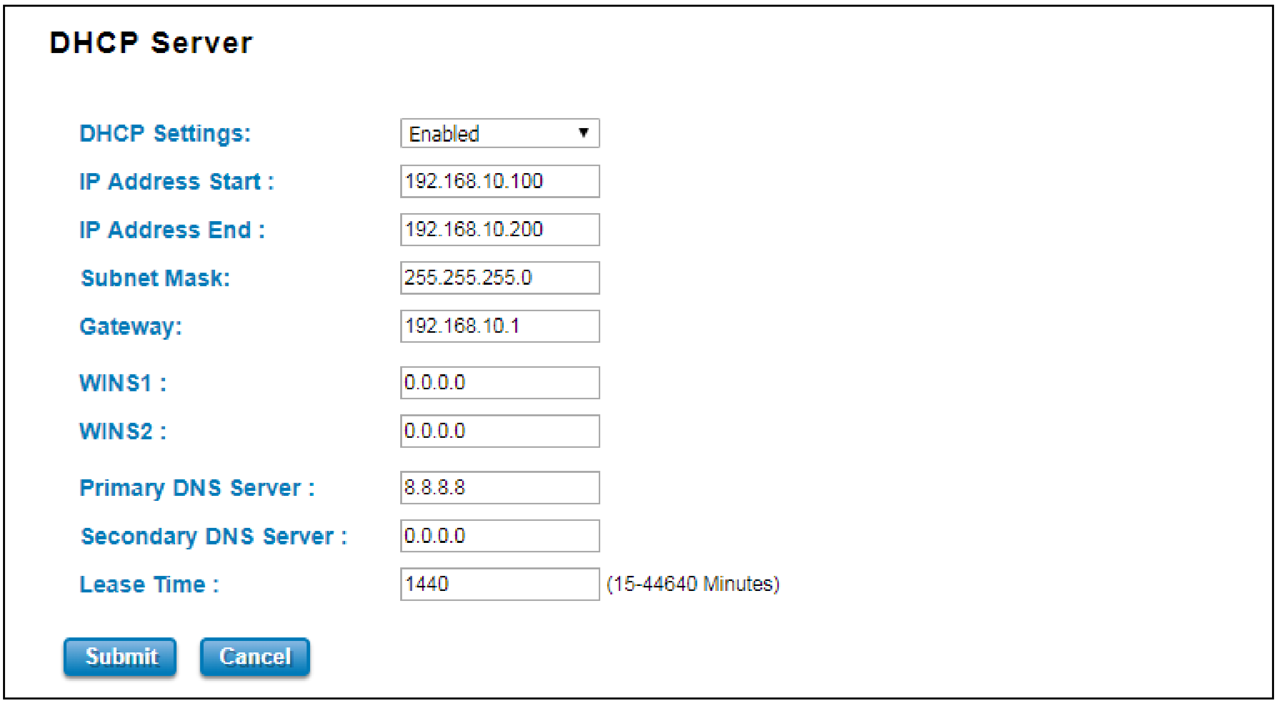
TERMS	DESCRIPTION
Current Time	User can configure time by input it manually. Get PC Time: get the time the PC
Time Zone	Choose the Time Zone section to adjust the time zone based on the user area.
NTP	**Enable NTP Client update** by checking this box. Select the time server from the **NTP Serve**r dropdown list or select **Manual IP** to manually input the IP address of available time server. ***Make sure that the device also has the internet connection.**

After finished configuring, click on **Submit** to activate the configuration.

3.1.5 DHCP Server

DHCP Server Setting

ISTRON router has DHCP Server Function that will provide a new IP address to DHCP Client. After enabling DHCP Server function, set up the Network IP address for the DHCP server IP address, Subnet Mask, Default Gateway address and Lease Time for client. Below is the DHCP Server Setting interface



DHCP Server

DHCP Settings:	Enabled
IP Address Start :	192.168.10.100
IP Address End :	192.168.10.200
Subnet Mask:	255.255.255.0
Gateway:	192.168.10.1
WINS1 :	0.0.0.0
WINS2 :	0.0.0.0
Primary DNS Server :	8.8.8.8
Secondary DNS Server :	0.0.0.0
Lease Time :	1440 (15-44640 Minutes)

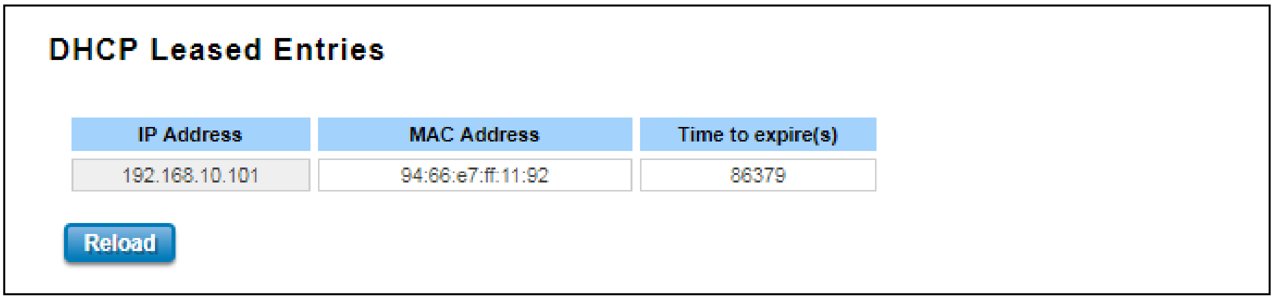
The description of the columns is as below:

TERMS	DESCRIPTION
DHCP Setting	Select to **Enable** or **Disable** to activate and deactivate DHCP Server function.
IP Address Start	Assign the IP Address Start range.
IP Address End	Assign the IP Address End range.
Subnet Mask	**Default: 255.255.255.0** Assign the subnet mask for the IP address here for DHCP Server.
Gateway	Assign the gateway for the router here for DHCP Server.
WIN S1	Enter WINS Server 1 IP address
WIN S2	Enter WINS Server 2 IP address
Primary DNS Server	Enter Primary DNS Server that used in user network.
Secondary DNS Server	Enter Secondary DNS Server that used in user network.
Lease Time	**Default: 1440** The maximum length of time for the IP address lease. Enter the Lease time in minutes. (Lease Time range: 15-44640 minutes)

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When user turns the computers on, they will automatically load the proper TCP/IP settings provided by the router. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

DHCP Leased Entries

The figure below shows the **DHCP Leased Entries.** It will show the MAC and IP address that was assigned by router. Click the **Reload** button to refresh the list.



DHCP Leased Entries

IP Address	MAC Address	Time to expire(s)
192.168.10.101	94:66:e7:ff:11:92	86379

The description of the columns is as below:

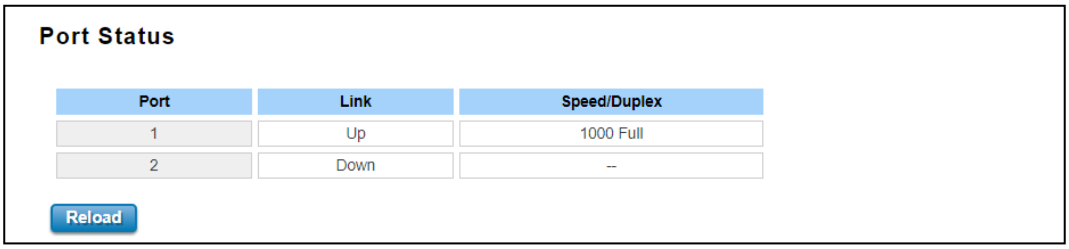
TERMS	DESCRIPTION
IP Address	IP address that was assigned by router.
MAC Address	The MAC Address of the network interface that was used to acquire the lease.
Time to expire(s)	Remains time for the IP address from DHCP Server leased.

3.2 Ethernet Port

Ethernet Port section is used to access the port configuration and rate limit control. It also allows User to view port status and port trunk information.

3.2.1 Port Status

Port Status section allows users to see the current status from the Ethernet.



Port Status

Port	Link	Speed/Duplex
1	Up	1000 Full
2	Down	--

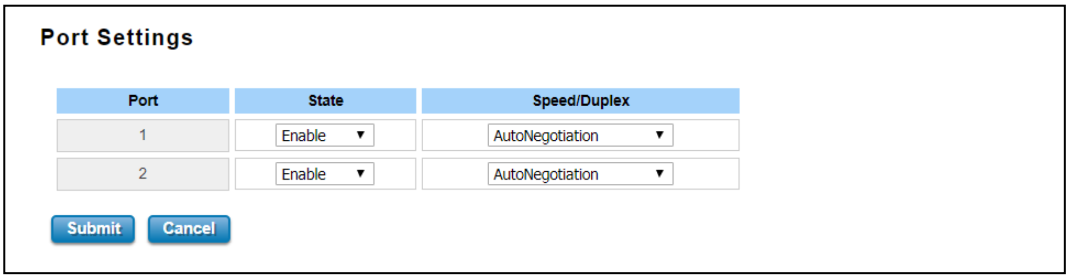
The description of the columns is as below:

TERMS	DESCRIPTION
Link	Display the Ethernet status, whether it is Link Up or Link Down.
Speed/Duplex	**Default: N/A** Show the Speed/Duplex for each port, such as 10 full,10 half,100 full,100 half mode for **Giga Ethernet Port 1~2**

Click on **Reload** to update the information.

3.2.2 Ethernet Setting

Use this page to configure the Ethernet setting.



Port Settings

Port	State	Speed/Duplex
1	Enable	AutoNegotiation
2	Enable	AutoNegotiation

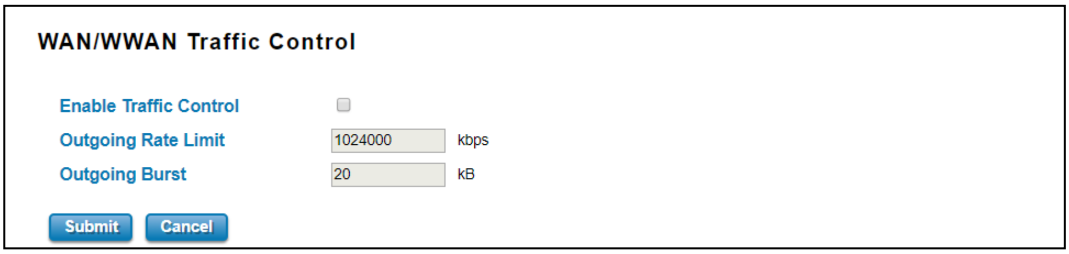
The description of the Ethernet Setting page is as below:

TERMS	DESCRIPTION
State	Enable or disable the port.
Speed/Duplex	**Default: Auto / Auto-Negotiation** Configure the Speed/Duplex of the port Ethernet 1. Users can set the bandwidth of each port as Auto-negotiation, 100 full, 100 half, 10 full, 10 half mode.

Click **Submit** to apply the configuration that just made.

3.2.3 Traffic Control

Traffic control is a form of flow control used to enforce a strict bandwidth limit at a port. User can configure separate Incoming Outgoing rate limits and burst



WAN/WWAN Traffic Control

Enable Traffic Control □

Outgoing Rate Limit 1024000 kbps

Outgoing Burst 20 kB

The description of the columns is as below:

TERMS	DESCRIPTION
Enable Traffic Control	Check the box to activate the function
Outgoing Rate Limit	**Default: 1024000 kbit/s** Set the maximum outgoing rate.
Outgoing Burst	**Default: 20 kBytes** Set the maximum outgoing burst.

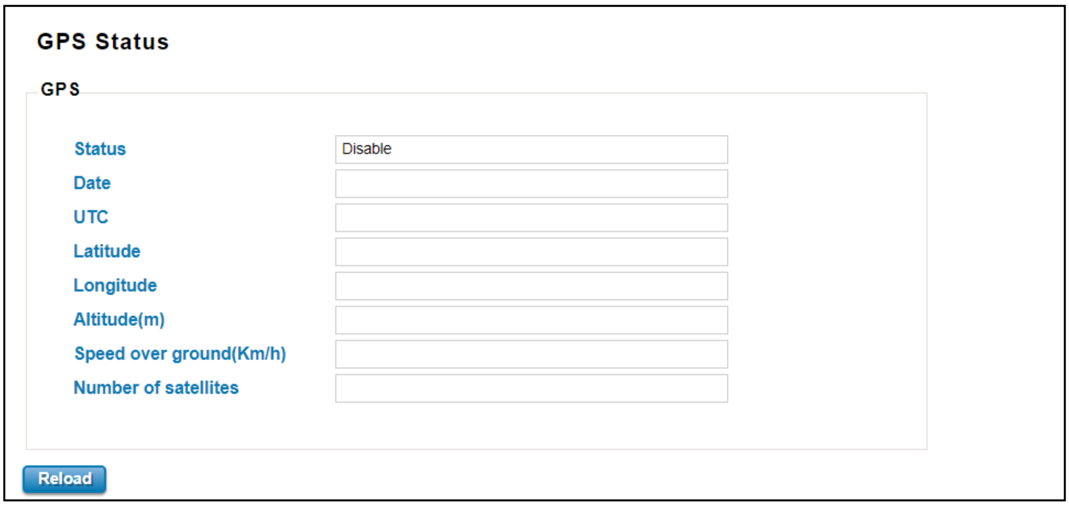
Click on **Submit** to apply the configuration.

3.3 GPS

This GPS section has the function to show the current position of the device. It could help the technician to track the device location.

3.3.1 GPS Status

GPS status is always disable since user need to manually input GPS coordinates in GPS settings page.



GPS Status

GPS

Status Disable

Date

UTC

Latitude

Longitude

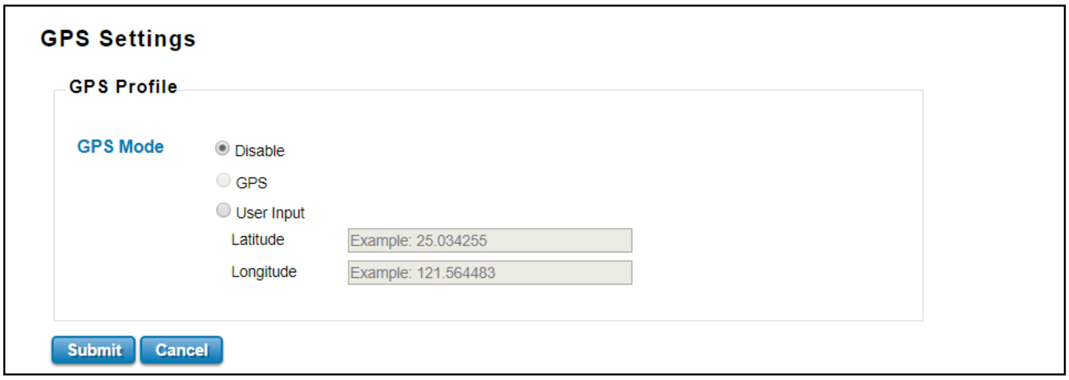
Altitude(m)

Speed over ground(Km/h)

Number of satellites

3.3.2 GPS Settings

In this GPS Setting section, user can manually input GPS coordinates. The coordinates can be used to report to cloud or specific server.



GPS Settings

GPS Profile

GPS Mode
● Disable
○ GPS
○ User Input
Latitude: Example: 25.034255
Longitude: Example: 121.564483

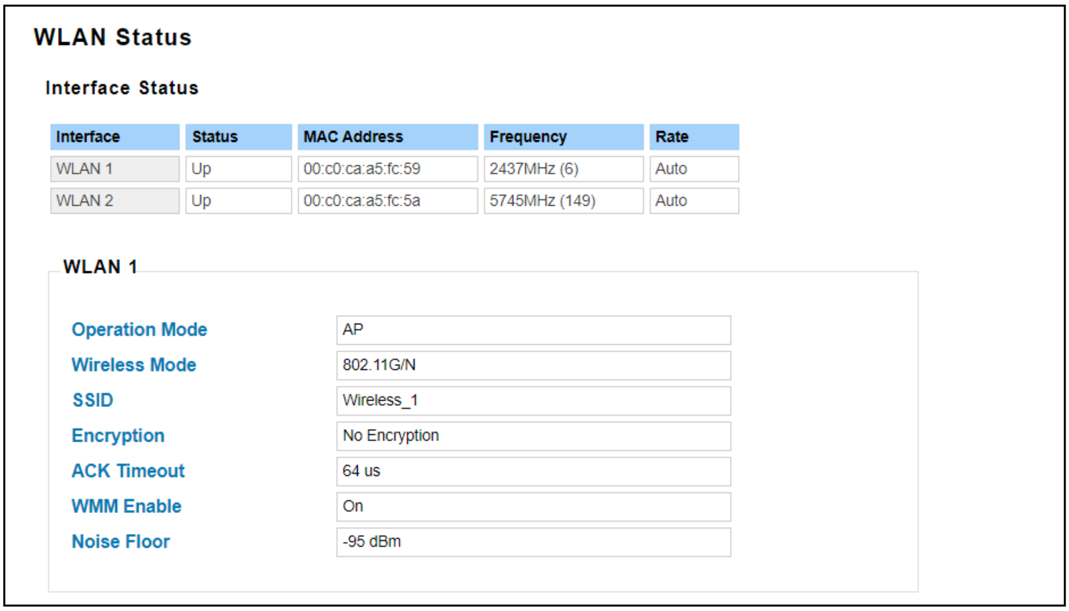
TERMS	DESCRIPTION
GPS mode	**Default: Disable** **Disable**: Disable GPS function. **GPS**: Enable GPS function. IWS SERIES series does not support active GPS. Contact ISTRON salesperson for GPS support. **User Input**: Input Latitude and Longitude. The coordinates can be used to report to cloud or specific server.

3.4 Wireless LAN

This Wireless LAN configuration pages only support the device that supported with Wi-Fi feature. This configuration page allows users to configure the Wireless LAN configuration.

3.4.1 WLAN Status

The figure below shows the WLAN status.



WLAN Status

Interface Status

Interface	Status	MAC Address	Frequency	Rate
WLAN 1	Up	00:c0:ca:a5:fc:59	2437MHz (6)	Auto
WLAN 2	Up	00:c0:ca:a5:fc:5a	5745MHz (149)	Auto

WLAN 1

Operation Mode: AP
Wireless Mode: 802.11G/N
SSID: Wireless_1
Encryption: No Encryption
ACK Timeout: 64 us
WMM Enable: On
Noise Floor: -95 dBm

The description of the columns is as below:

TERMS	**DESCRIPTION**
Operation Mode	Display the current operating modes on the device
Wireless Mode	Display the current wireless mode
SSID	Display the primary name of the SSID
Encryption	Display the encryption mode.
ACK Timeout	The ACK time of wireless beacon packet
WMM Enable	Display the status of the WMM support.
Noise Floor	Display the background noise level.
Description when MESH AP Enabled	
TERMS	**DESCRIPTION**
Mode	MESH AP or RE (Range Extender) mode
SSID	The current SSID of MESH network
WLAN 1 Signal Strength	WLAN 1 Signal in dBm unit
WLAN 1 Status	Connected or Disconnected Status
WLAN 1 Signal Strength	WLAN 2 Signal in dBm unit
WLAN 1 Status	Connected or Disconnected Status

3.4.2 WLAN Settings

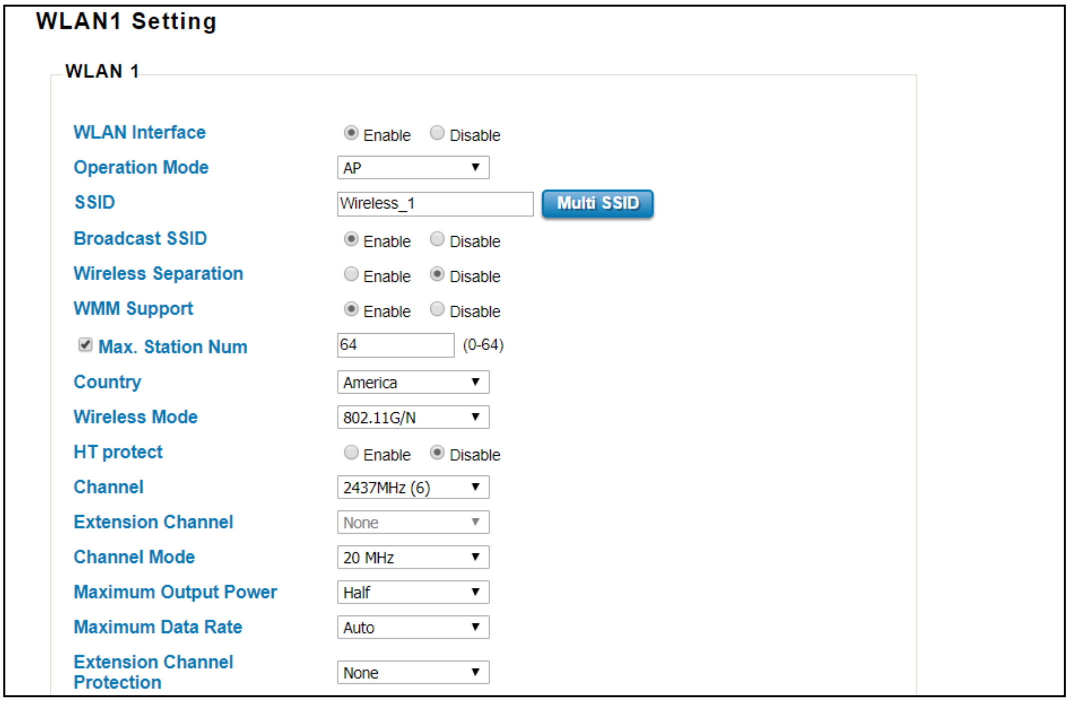
WLAN Setting page, on this page user may configure the parameters for Wireless LAN Interface includes change wireless interface modes and all of the related parameters for each operation mode.

There are 2 WLAN interfaces supported in IWS SERIES series. WLAN1 for 2.4GHz and WLAN2 for 5GHz in AP mode can be configured in the same time. Only one radio can be configured to client mode in the same time.

Pop up window will be displayed to indicate only one radio can be configured in client mode

3.4.2.1 AP mode

The Access Point mode, it establishes a wireless connection, receive from wireless clients and provide connection for wireless client devices, the client can search and connect to several the access points.



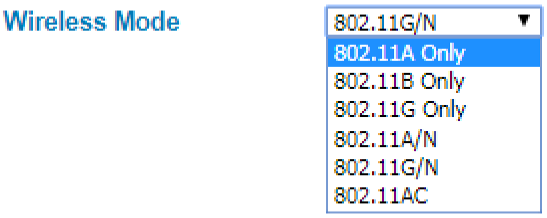
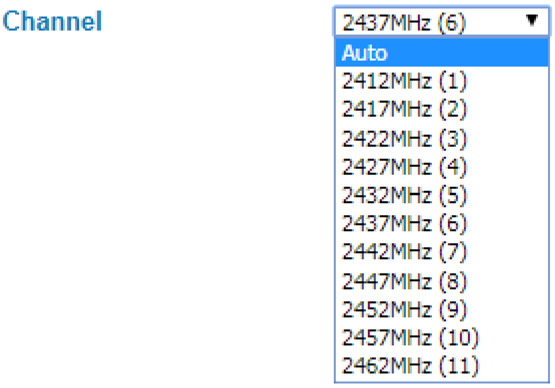
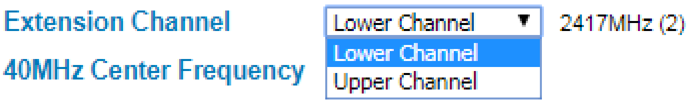
WLAN1 Setting

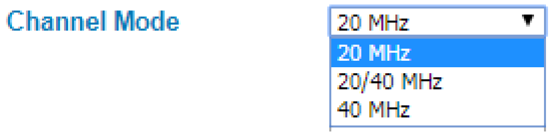
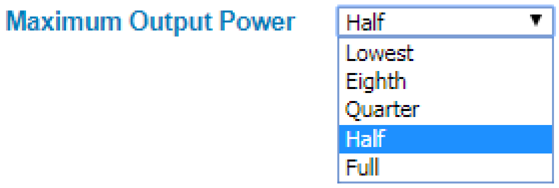
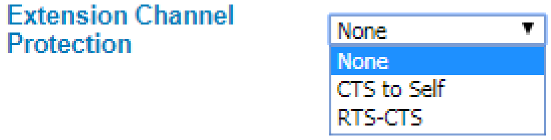
WLAN 1

WLAN Interface	● Enable ○ Disable
Operation Mode	AP ▼
SSID	Wireless_1
Broadcast SSID	● Enable ○ Disable
Wireless Separation	○ Enable ● Disable
WMM Support	● Enable ○ Disable
☑ Max. Station Num	64 (0-64)
Country	America ▼
Wireless Mode	802.11G/N ▼
HT protect	○ Enable ● Disable
Channel	2437MHz (6) ▼
Extension Channel	None ▼
Channel Mode	20 MHz ▼
Maximum Output Power	Half ▼
Maximum Data Rate	Auto ▼
Extension Channel Protection	None ▼

The description of the columns is as below:

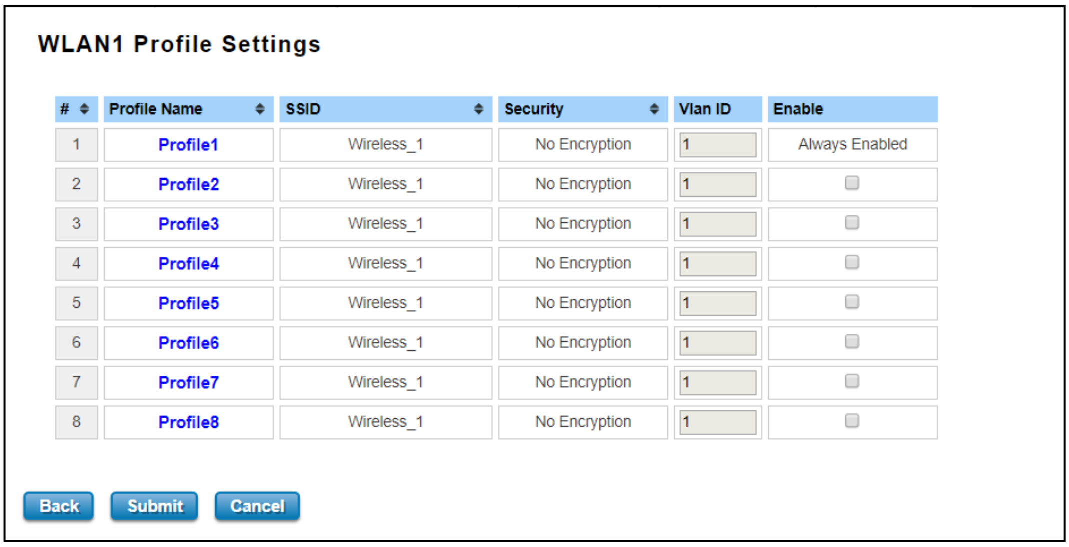
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	**Default: AP** Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.

Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcast SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Separation	**Default: Disable** By enabling the function, connected clients will be separated and can reach each other (ex: can't ping each other)
WMM support	**Default: Enable** To enable or disable WIFI multi-media QoS.
Max. Station Num	**Default: 64** Specify the maximum number of connected clients
Country	Select your country code for band regulation.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has the specific frequency and it has different basic settings.  Wireless Mode 802.11G/N 802.11A Only 802.11B Only 802.11G Only 802.11A/N 802.11G/N 802.11AC
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel.  Channel 2437MHz (6) Auto 2412MHz (1) 2417MHz (2) 2422MHz (3) 2427MHz (4) 2432MHz (5) 2437MHz (6) 2442MHz (7) 2447MHz (8) 2452MHz (9) 2457MHz (10) 2462MHz (11)
Extension Channel	**Default: Lower Channel 2417MHz (2)**  Extension Channel Lower Channel 40MHz Center Frequency 2417MHz (2) This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**

	 There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half Lowest Eighth Quarter Half Full
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection None None CTS to Self RTS-CTS Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

At the SSID section, there is a **Multi SSID** button appeared. This AP mode supports the multiple SSID or multiple access point connections. So user may separate the connection into several access points and it is supported with 8 profiles for multiple SSID. Click the button then another form will appear, see the figure below.



WLAN1 Profile Settings

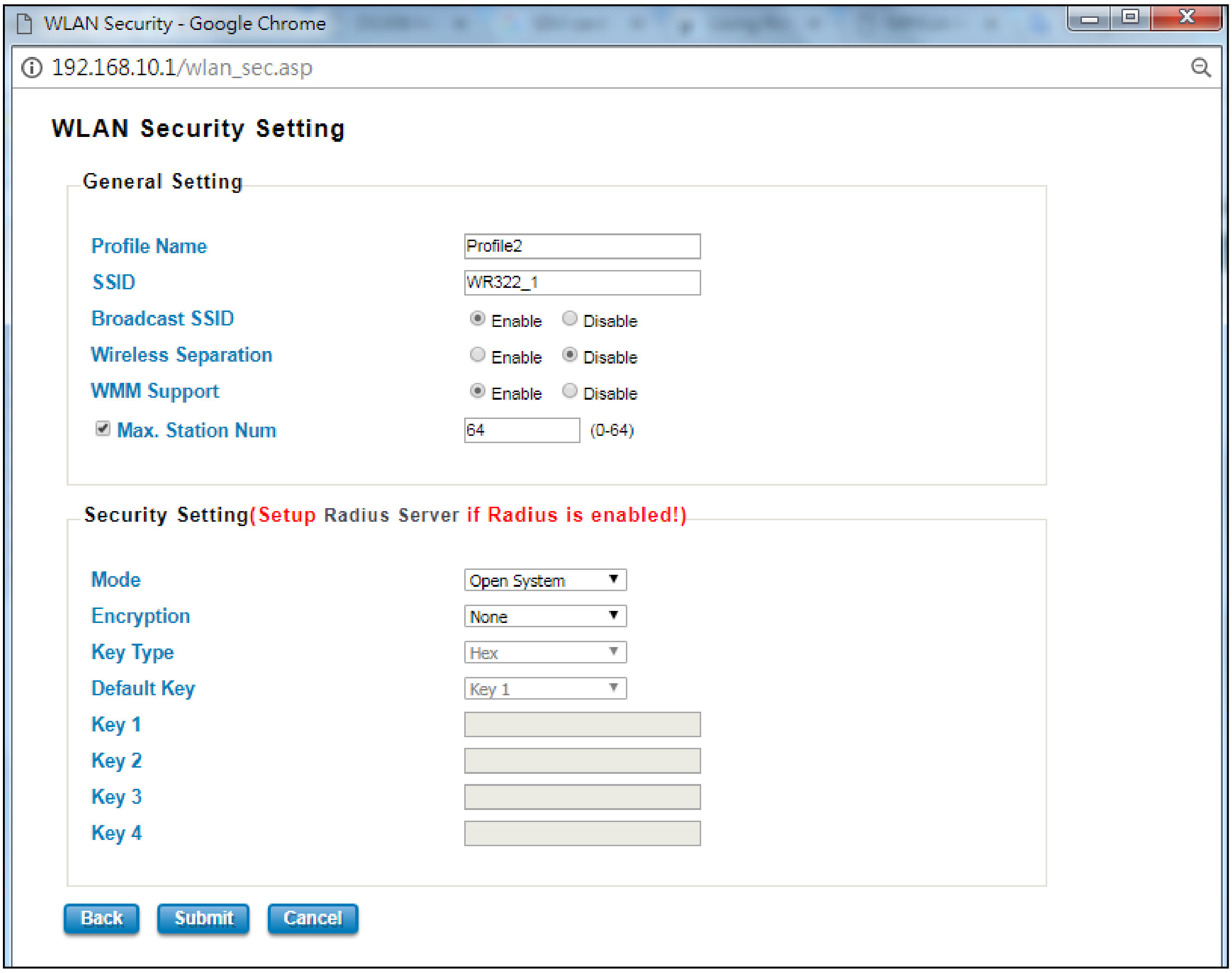
#	Profile Name	SSID	Security	Vlan ID	Enable
1	Profile1	Wireless_1	No Encryption	1	Always Enabled
2	Profile2	Wireless_1	No Encryption	1	☐
3	Profile3	Wireless_1	No Encryption	1	☐
4	Profile4	Wireless_1	No Encryption	1	☐
5	Profile5	Wireless_1	No Encryption	1	☐
6	Profile6	Wireless_1	No Encryption	1	☐
7	Profile7	Wireless_1	No Encryption	1	☐
8	Profile8	Wireless_1	No Encryption	1	☐

The description of the column is as below:

TERMS	DESCRIPTION
Profile Name	Display the available WLAN Profile name
SSID	Display the SSID Name.
Security	Display the current security mode for the Wireless network
VLAN ID	Display the VLAN ID
Enable	Check the box to enable the WLAN Profile. When user enabled the Profile, user may configure the WLAN Setting by click the Profile name.

Click **Submit** to apply the configuration

The Multi SSID section shows the configuration page where the Profile1 always enabled. In this section, user may configure each Profile by check the box to enable the Profile and then click the profile name to open the configuration page for specific Profile. The figure below is the pop-up WLAN Security configuration page for each Profile. In this configuration page, user can configure the AP profile, divide the AP connection and set the security setting by put the encryption mode and set the key or password to access the AP. Refers to the WLAN Security Section for more description (3.7.3).


WLAN Security - Google Chrome

192.168.10.1/wlan_sec.asp

WLAN Security Setting

General Setting

Profile Name	Profile2
SSID	WR322_1
Broadcast SSID	● Enable ○ Disable
Wireless Separation	○ Enable ● Disable
WMM Support	● Enable ○ Disable
☑ Max. Station Num	64 (0-64)

Security Setting(Setup Radius Server if Radius is enabled!)

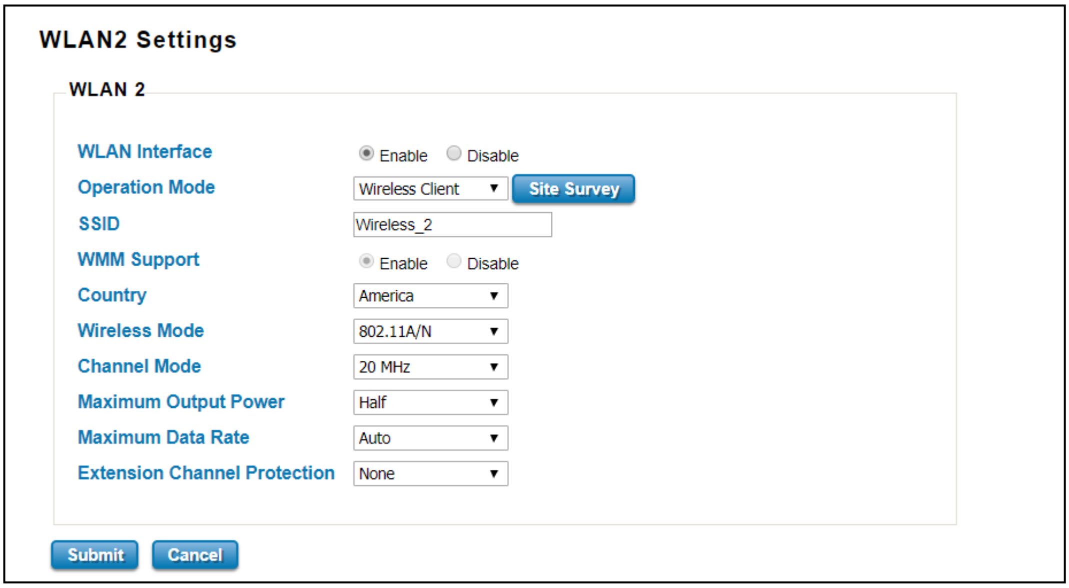
Mode	Open System
Encryption	None
Key Type	Hex
Default Key	Key 1
Key 1	
Key 2	
Key 3	
Key 4	

Click **Submit** to apply the configuration

Pop up window may be blocked by browser. Change browser settings to allow pop-up window to configure multi-SSID.

3.4.2.2 Client mode

Wireless Client mode, in this mode the device is able to connect to the Access Point and join the wireless network around the device that opens the connection. User can find the best connection for the AP by click the **Site Survey** and the AP list will appear.



WLAN2 Settings

WLAN 2

WLAN Interface ● Enable ○ Disable

Operation Mode Wireless Client ▼

SSID Wireless_2

WMM Support ● Enable ○ Disable

Country America ▼

Wireless Mode 802.11A/N ▼

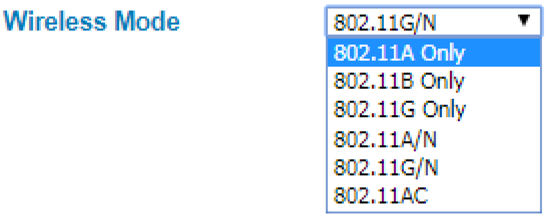
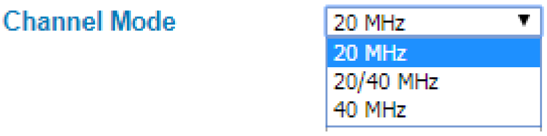
Channel Mode 20 MHz ▼

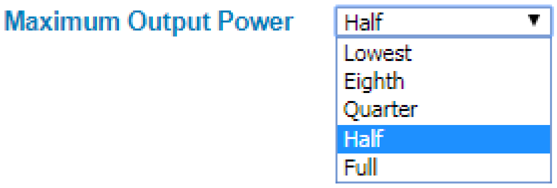
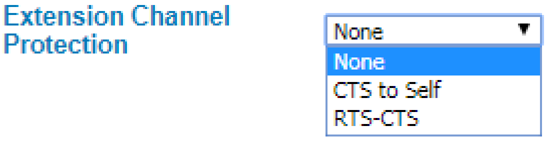
Maximum Output Power Half ▼

Maximum Data Rate Auto ▼

Extension Channel Protection None ▼

The description of the columns is as below:

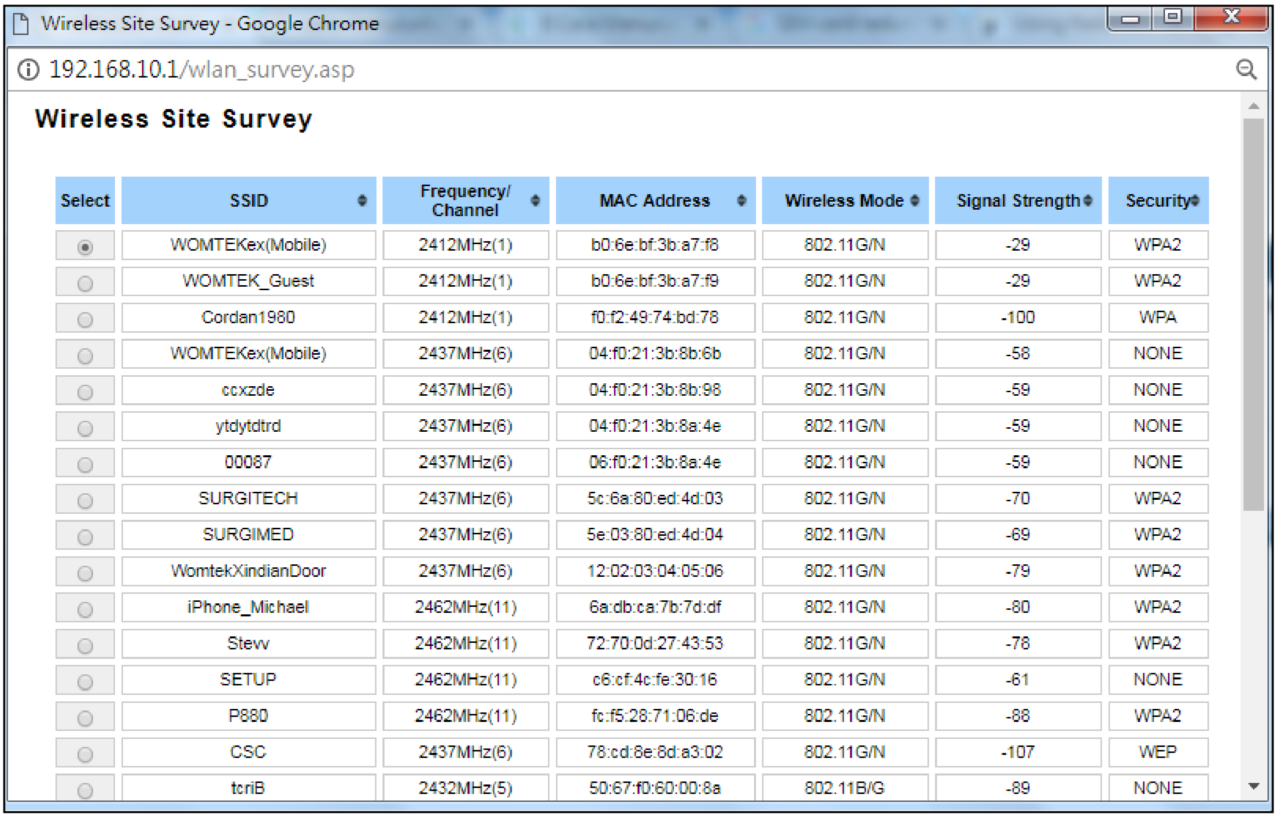
TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	Input the primary name of the access point.
WMM support	**Default: Enable** To enable or disable WIFI multi-media QoS.
Country	Select your country code for band regulation.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting.  Wireless Mode 802.11G/N ▼ 802.11A Only 802.11B Only 802.11G Only 802.11A/N 802.11G/N 802.11AC
Channel Mode	**Default: 20MHz**  Channel Mode 20 MHz ▼ There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequency, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the

	transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half Lowest Eighth Quarter Half Full
Maximum Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select lower rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection None None CTS to Self RTS-CTS Select from the drop down list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function, it may decrease wireless network performance.

Click **Submit** to apply the configuration

Wireless Site Survey (Wireless Client & WDS-Client)

Click the Site Survey button to open the Wireless Site Survey page. On this page user may choose the Access Point that appeared on the list. After selects the specific AP, then click **Selected** to apply the choice. Click **Scan** to refresh the list.



192.168.10.1/wlan_survey.asp

Wireless Site Survey

Select	SSID	Frequency/ Channel	MAC Address	Wireless Mode	Signal Strength	Security
●	WOMTEKex(Mobile)	2412MHz(1)	b0:6e:bf:3b:a7:f8	802.11G/N	-29	WPA2
○	WOMTEK_Guest	2412MHz(1)	b0:6e:bf:3b:a7:f9	802.11G/N	-29	WPA2
○	Cordan1980	2412MHz(1)	f0:f2:49:74:bd:78	802.11G/N	-100	WPA
○	WOMTEKex(Mobile)	2437MHz(6)	04:f0:21:3b:8b:6b	802.11G/N	-58	NONE
○	ccxzde	2437MHz(6)	04:f0:21:3b:8b:98	802.11G/N	-59	NONE
○	ytdytdtrd	2437MHz(6)	04:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	00087	2437MHz(6)	06:f0:21:3b:8a:4e	802.11G/N	-59	NONE
○	SURGITECH	2437MHz(6)	5c:6a:80:ed:4d:03	802.11G/N	-70	WPA2
○	SURGIMED	2437MHz(6)	5e:03:80:ed:4d:04	802.11G/N	-69	WPA2
○	WomtekXindianDoor	2437MHz(6)	12:02:03:04:05:06	802.11G/N	-79	WPA2
○	iPhone_Michael	2462MHz(11)	6a:db:ca:7b:7d:df	802.11G/N	-80	WPA2
○	Stevv	2462MHz(11)	72:70:0d:27:43:53	802.11G/N	-78	WPA2
○	SETUP	2462MHz(11)	c6:cf:4c:fe:30:16	802.11G/N	-61	NONE
○	P880	2462MHz(11)	fc:f5:28:71:06:de	802.11G/N	-88	WPA2
○	CSC	2437MHz(6)	78:cd:8e:8d:a3:02	802.11G/N	-107	WEP
○	tcriB	2432MHz(5)	50:67:f0:60:00:8a	802.11B/G	-89	NONE

The description of the columns is as below:

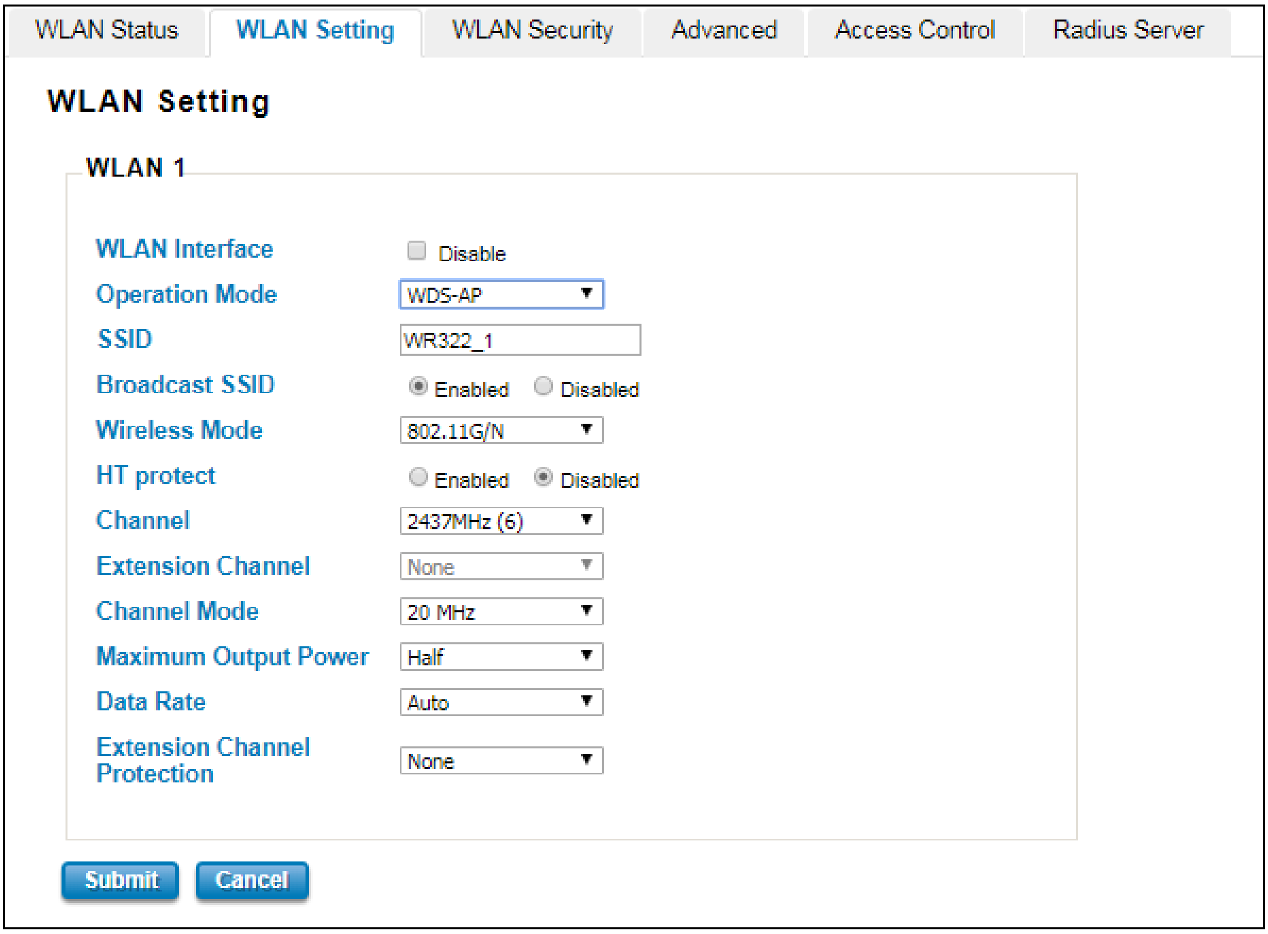
TERMS	DESCRIPTION
Select	Select the SSID.
SSID	Display the detected SSID's name
Frequency/Channel	Display the current frequency of the AP.
MAC Address	Display the listed AP MAC Address.
Wireless Mode	Display the Wireless mode.
Signal Strength	Display the signal strength
Security	The security mode of the Access Point.

Click **Selected** to connect to the specific SSID.

Pop up window may be blocked by browser. Change browser settings to allow pop-up window to configure multi-SSID.

3.4.2.3 WDS AP Mode

The WDS-AP mode usually implements the Point to Point (P2P) connection, so the access point should be WDS-AP and the wireless client should be WDS-Client. In this case, the AP just can share the connection to the specific wireless client that has its MAC Address. But WDS-AP can be a repeater to provide network access to general clients.



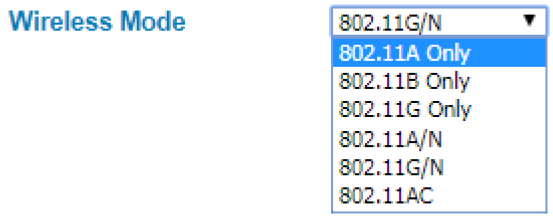
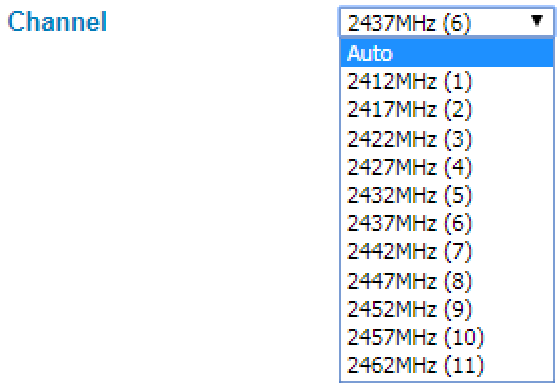
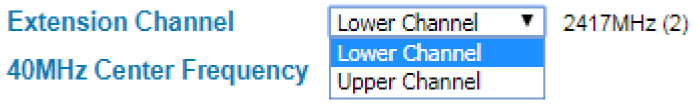
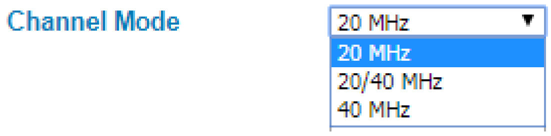
WLAN Setting

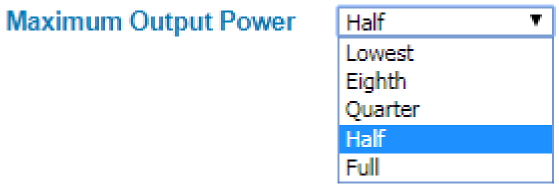
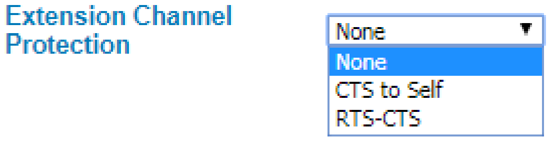
WLAN 1

WLAN Interface	□ Disable
Operation Mode	WDS-AP
SSID	WR322_1
Broadcast SSID	● Enabled ○ Disabled
Wireless Mode	802.11G/N
HT protect	○ Enabled ● Disabled
Channel	2437MHz (6)
Extension Channel	None
Channel Mode	20 MHz
Maximum Output Power	Half
Data Rate	Auto
Extension Channel Protection	None

The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless function.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
Broadcast SSID	**Default: Enabled.** By enabling the broadcast SSID, it makes the AP can be accessed and searched by the clients, and for the security concern by disabling this broadcaset SSID, the network will be hidden in order to prevent any malicious attack.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has different configuration. For each wireless mode, it has specific frequency and it has different basic setting.

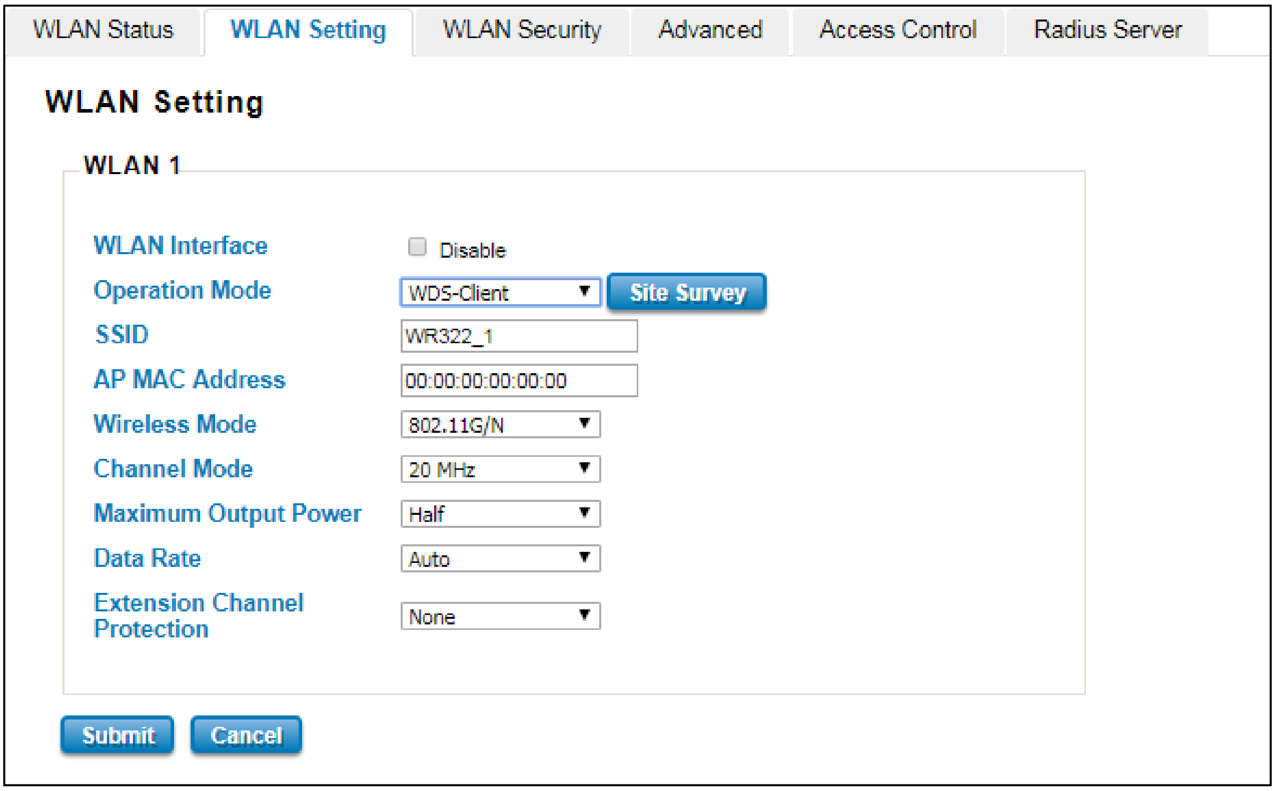
	 Wireless Mode 802.11G/N 802.11A Only 802.11B Only 802.11G Only 802.11A/N 802.11G/N 802.11AC
HT Protect	**Default: Disabled** Select Enabled to activate the High Throughput protect to ensure HT transmission with MAC mechanism.
Channel	**Default: 2437MHz (6)** Select the proper channel, each country has different band user may select the channel based on the situation. Or select auto to automatically set the channel.  Channel 2437MHz (6) Auto 2412MHz (1) 2417MHz (2) 2422MHz (3) 2427MHz (4) 2432MHz (5) 2437MHz (6) 2442MHz (7) 2447MHz (8) 2452MHz (9) 2457MHz (10) 2462MHz (11)
Extension Channel	**Default: Lower Channel 2417MHz (2)**  Extension Channel Lower Channel 2417MHz (2) 40MHz Center Frequency This option would be appeared when user select the Channel Mode to 20/40MHz or 40MHz. To put range for the frequency, it provides the Lower Channel (2417MHz (2)) with the 40MHz center frequency is 2427MHz (4) and Upper Channel (2457MHz (10)) with the 40MHz center frequency is 2447MHz (8).
Channel Mode	**Default: 20MHz**  Channel Mode 20 MHz There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.

	 Maximum Output Power: Half
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate; the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection: None Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activating this function it may decrease wireless network performance.

Click **Submit** to apply the configuration

3.4.2.4 WDS Client Mode

In WDS-Client mode, user must specify the specific WDS-AP's SSID and MAC address. So WDS-Client just do the transmission to the WDS-AP only. In this mode, please make sure that the configuration should be the same as the WDS-AP as well.



WLAN Setting

WLAN 1

WLAN Interface □ Disable

Operation Mode: WDS-Client

SSID: WR322_1

AP MAC Address: 00:00:00:00:00:00

Wireless Mode: 802.11G/N

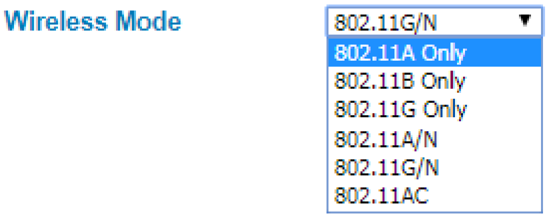
Channel Mode: 20 MHz

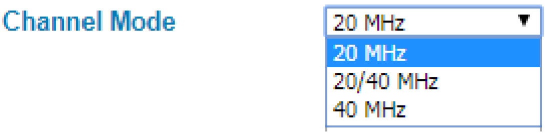
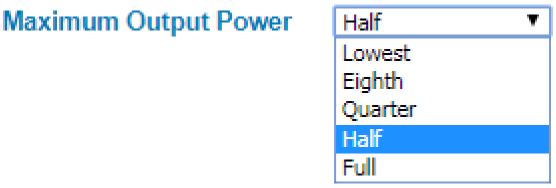
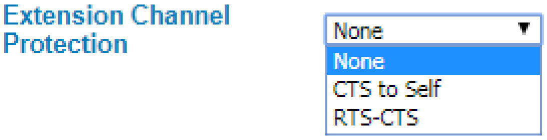
Maximum Output Power: Half

Data Rate: Auto

Extension Channel Protection: None

The description of the columns is as below:

TERMS	DESCRIPTION
WLAN Interface	Check the box to disable the WLAN interface and stop all of the wireless functions.
Operation Mode	Select the Operation Mode for the router. (AP, Wireless Client, WDS-AP and WDS-Client)
SSID	**Default: WR322_1** Input the primary name of the access point.
AP MAC Address	**Default: 00:00:00:00:00:00** Set the specific AP MAC Address of the WDS-AP.
Wireless Mode	**Default: 802.11G/N** Select the specific wireless mode, different wireless mode has a different configuration. For each wireless mode, it has a specific frequency and it has different basic setting.  Wireless Mode: 802.11G/N 802.11A Only 802.11B Only 802.11G Only 802.11A/N 802.11G/N 802.11AC
Channel Mode	**Default: 20MHz**

	 There are three channel modes, 20MHz, 20/40MHz and 40MHz. If user select 20MHz, the frequency that can be received maximum is 20MHz. For 20/40MHz it can receive both frequencies, and for the 40MHz, it provides bigger data rate and received the 40MHz frequency. But basically, if the transmission happened between the AP and the client, both AP and client can have the negotiation phase about the frequency.
Maximum Output Power	**Default: Half** Specify the transmission power. For the higher output power, it can cover the signal widely and of course may need big power consumption. The Full output power may need the antenna.  Maximum Output Power Half Lowest Eighth Quarter Half Full
Data Rate	**Default: Auto** Select the specific data rate in order to control the transmission rate. **Auto** is preferred rate, the access point will automatically select the highest available rate to transmit. User may select the low rate when there is no great demand for transmission speed, for long distance transmission.
Extension Channel Protection	 Extension Channel Protection None None CTS to Self RTS-CTS Select from the dropdown list option between **CTS-Self or RTS-CTS** to avoid conflict with other wireless network and to improve the ability of the device to catch all the wireless transmissions. By activate this function it may decrease wireless network performance.

3.4.2.5 Mesh Settings

IWS SERIESM series support mesh network. Click checkbox and submit button to enable mesh network. SSID will be used as connections for both mesh links and wireless clients. Mesh link will be connected automatically to form adaptive mesh network. There are 2 roles in mesh network:

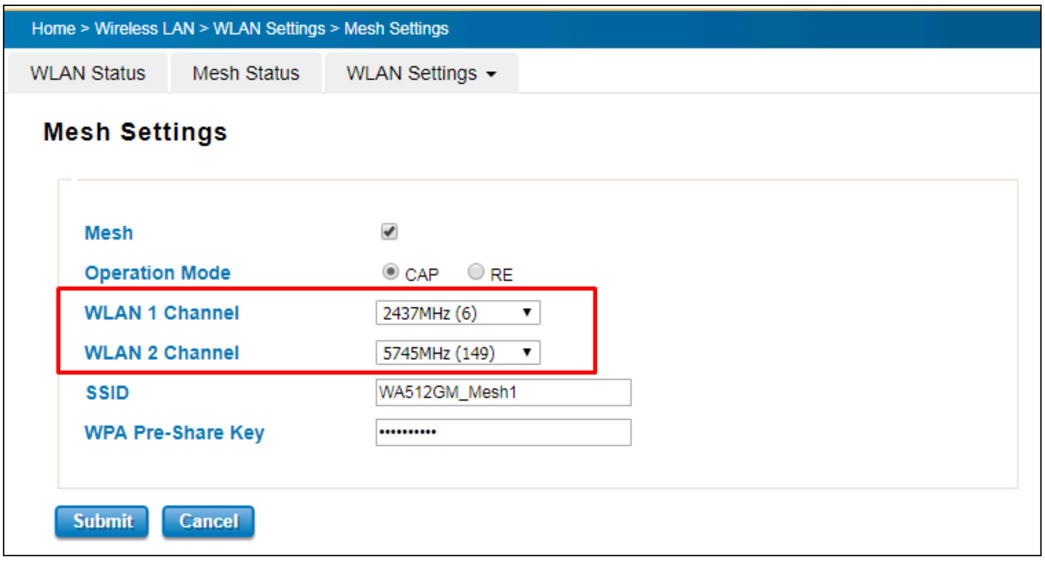
CAP: Central AP, also known as root AP, with a wired data connection that can be configured to relay data to and from mesh APs. In CAP, you can enable MESH in 2.4GHz or 5GHz frequency, define SSID and Key for the MESH network. The DHCP server feature is enabled automatically in CAP, it can assign IP address to MESH RE devices and connected clients.

RE: Range Extender, to form a mesh network by uplink to other RE or CAP. In MESH RE device, the MESH SSID and Key setting must follow CAP settings.

Note that other wireless modes including AP/client/WDS AP/WDS client modes will be dismissed and can't be configured. Disable mesh to go back to AP/client/WDS AP/WDS client mode.

AP/client/WDS AP/WDS client modes will be dismissed when mesh enabled. Disable mesh to enable AP/client/WDS AP/WDS client modes again.

MESH Settings



Mesh Settings

Mesh ☑

Operation Mode ● CAP ○ RE

WLAN 1 Channel 2437MHz (6)

WLAN 2 Channel 5745MHz (149)

SSID WA512GM_Mesh1

WPA Pre-Share Key ••••••••••

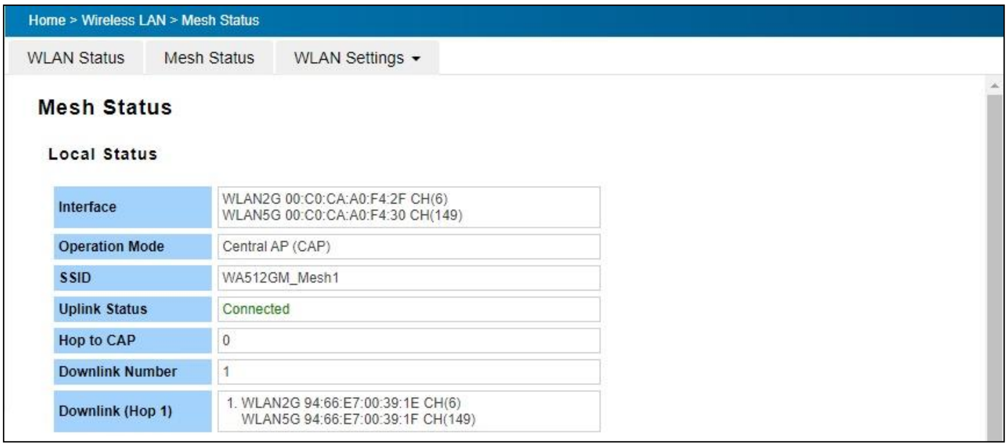
TERMS	DESCRIPTION
Mesh	Check the box to enable mesh network
Operation Mode	Select the Operation Mode in mesh network. CAP: Central AP, node with WAN uplink for outside network. RE: Node has only uplink to other RE nodes or CAP nodes, functions as range extender.
WLAN 1 Channel	Select the channel of WLAN 1 (CAP only)
WLAN 2 Channel	Select the channel of WLAN 2 (CAP only)
SSID	The SSID will be used for both mesh links and wireless clients. The setting within the MESH network must be the same.
WPA Pre-Share Key	Passphrase used to connect to SSID. The setting within the MESH network must be the same.

MESH Status

Click MESH Status, you can find the MESH status of the connected AP in this page.

The MESH Status in CAP:

In **Local Status,** you can find the information of the WLAN interface, Operation mode, MESH SSID, Uplink Status, Hop to CAP(0 in CAP), Downlink number and Hops.

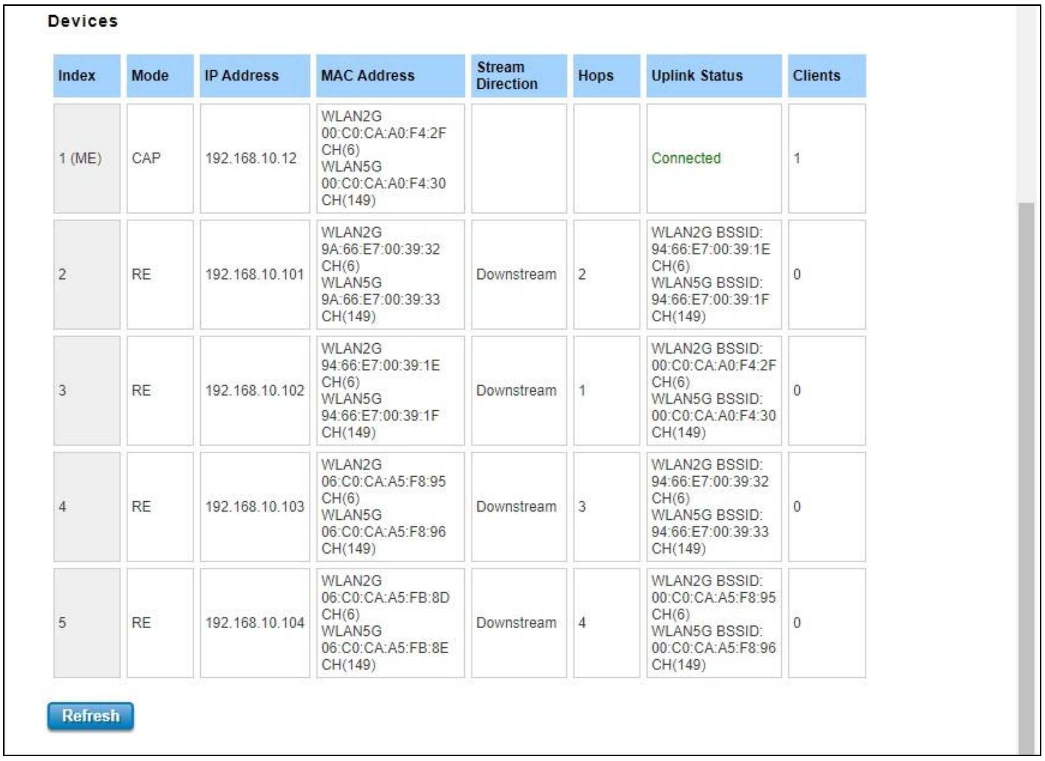


Mesh Status

Local Status

Interface	WLAN2G 00:C0:CA:A0:F4:2F CH(6) WLAN5G 00:C0:CA:A0:F4:30 CH(149)
Operation Mode	Central AP (CAP)
SSID	WA512GM_Mesh1
Uplink Status	Connected
Hop to CAP	0
Downlink Number	1
Downlink (Hop 1)	1. WLAN2G 94:66:E7:00:39:1E CH(6) WLAN5G 94:66:E7:00:39:1F CH(149)

In **Device,** you can find all the APs' role and information. It helps you to monitor the MESH network. You can draw your MESH network architecture according to the information. The first column you see is "ME", the role of your connected AP. While check RE, the first column will be 1(ME): RE mode.



Devices

Index	Mode	IP Address	MAC Address	Stream Direction	Hops	Uplink Status	Clients
1 (ME)	CAP	192.168.10.12	WLAN2G 00:C0:CA:A0:F4:2F CH(6) WLAN5G 00:C0:CA:A0:F4:30 CH(149)			Connected	1
2	RE	192.168.10.101	WLAN2G 9A:66:E7:00:39:32 CH(6) WLAN5G 9A:66:E7:00:39:33 CH(149)	Downstream	2	WLAN2G BSSID: 94:66:E7:00:39:1E CH(6) WLAN5G BSSID: 94:66:E7:00:39:1F CH(149)	0
3	RE	192.168.10.102	WLAN2G 94:66:E7:00:39:1E CH(6) WLAN5G 94:66:E7:00:39:1F CH(149)	Downstream	1	WLAN2G BSSID: 00:C0:CA:A0:F4:2F CH(6) WLAN5G BSSID: 00:C0:CA:A0:F4:30 CH(149)	0
4	RE	192.168.10.103	WLAN2G 06:C0:CA:A5:F8:95 CH(6) WLAN5G 06:C0:CA:A5:F8:96 CH(149)	Downstream	3	WLAN2G BSSID: 94:66:E7:00:39:32 CH(6) WLAN5G BSSID: 94:66:E7:00:39:33 CH(149)	0
5	RE	192.168.10.104	WLAN2G 06:C0:CA:A5:FB:8D CH(6) WLAN5G 06:C0:CA:A5:FB:8E CH(149)	Downstream	4	WLAN2G BSSID: 00:C0:CA:A5:F8:95 CH(6) WLAN5G BSSID: 00:C0:CA:A5:F8:96 CH(149)	0

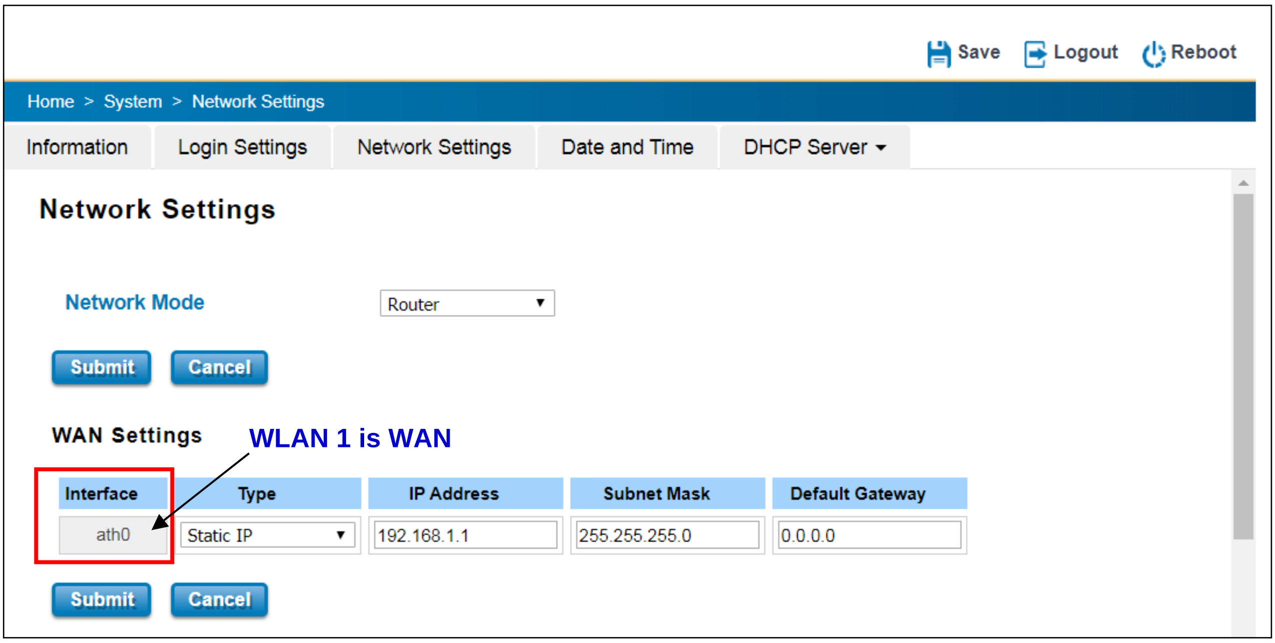
3.4.2.6 Client Router (Wireless WAN NAT) Mode

Some of the specific firmware supports the “Client Router” operation mode, also known as WLAN NAT or Wireless WAN mode. The configured WLAN 1 or WLAN 2 interface acts as WAN interface instead of other Ethernet or WLAN interfaces. Refer to the below comparison table of WALN/Ethernet interface to Router operation mode.

	RJ45 Interface		WLAN Interface		
Interface\ Operation Mode	**Eth 1**	**Eth 2/PD**	**WLAN 1**	**WLAN 2**	**Note**
WLAN 1- Clinet Router	LAN	LAN	**WAN (ath0)**	LAN	LAN to Wireless WAN NAT Routing.
WLAN 2- Clinet Router	LAN	LAN	LAN	**WAN (ath16)**	LAN to Wireless WAN NAT Routing.
Ethernet - Router	LAN	**WAN (Eth1)**	LAN	LAN	
Ethernet - Bridge (Default Setting)	LAN	LAN	LAN	LAN	Default: All interfaces work as LAN segment

Note: Only one Radio can be enabled as Client/Client Router mode.

After enabled the WLAN Client Router mode, the interface of WLAN 1 in WAN Settings of Network settings is “ath0”. The interface of WLAN 2 in WAN Settings of Network settings is “ath16”. You can select Static IP or DHCP Client, and assign the IP address for your Wireless WAN interface. The system will run the LAN to Wireless WAN NAT Routing.



Network Settings

Network Mode: Router

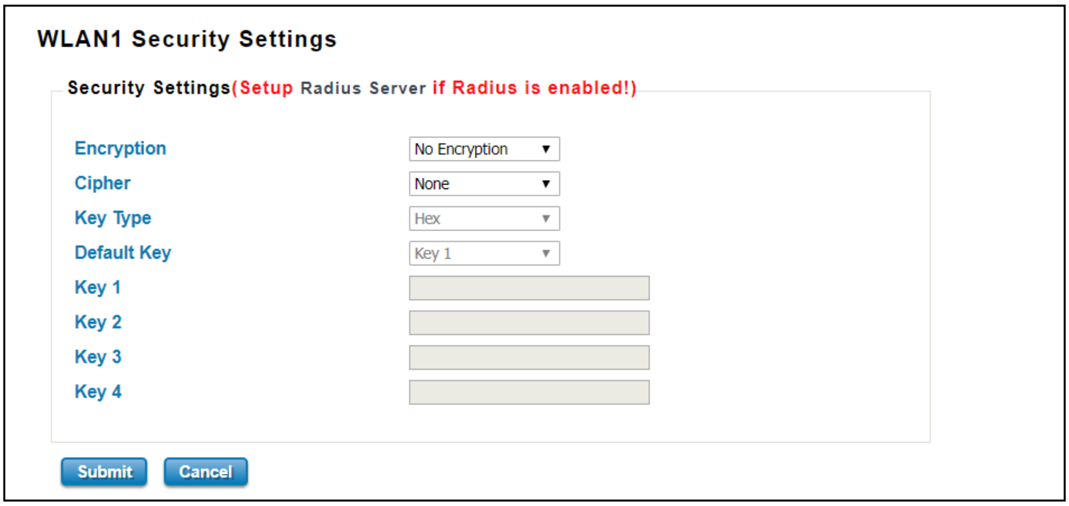
WAN Settings

WLAN 1 is WAN

Interface	Type	IP Address	Subnet Mask	Default Gateway
ath0	Static IP	192.168.1.1	255.255.255.0	0.0.0.0

3.4.3 WLAN Security

On this configuration page, user can configure the WLAN Security feature.



WLAN1 Security Settings

Security Settings(Setup Radius Server if Radius is enabled!)

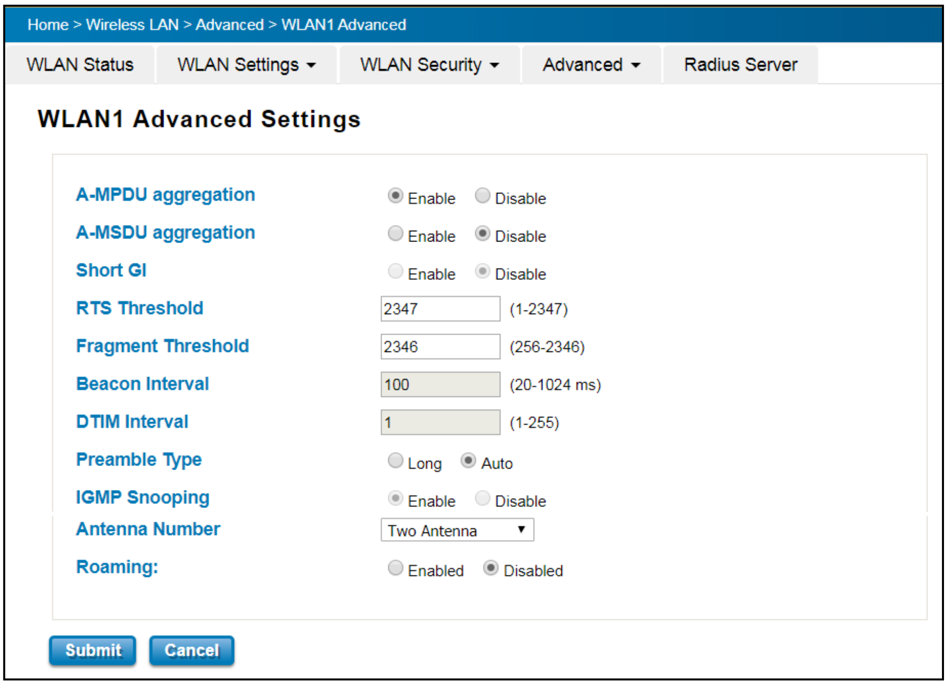
Encryption	No Encryption
Cipher	None
Key Type	Hex
Default Key	Key 1
Key 1	
Key 2	
Key 3	
Key 4	

The description of the columns is as below:

TERMS	DESCRIPTION
Encryption	Configure the data encryption mode. ● **None**: Available only when the authentication type is an open system. ● **64 bits WEP**: It is made up of 10 hexadecimal numbers. ● **128 bits WEP**: It is made up of 26 hexadecimal numbers. ● **TKIP**: Temporal Key Integrity Protocol, which is a kind of dynamic encryption, is co-used with WPA-PSK. ● **AES**: Advanced Encryption Standard, it is usually co-used with WPA2-PSK.
Key Type	**Default: Hex** WEP can be configured with a 64-bit or 128-bit Shared Key (hexadecimal or ASCII). As defined, hexadecimal number is represented by 0-9, A-F or a-f; ASCII is represented by 0-9, A-F, a-f or punctuation. Each one consists of two-digit hexadecimal.
Default Key	**Default: Key 1** Set the specific default key.
Key 1~4	Enter the specific encryption key.

3.4.4 Advanced

The page allows the advanced user to configure advanced wireless setting with more experience about the WLAN. If user doesn’t have any qualified knowledge about WLAN, we suggest not to change the default setting except user know the effects when the setting is changed. The wrong configuration may impact the performance of wireless network.



WLAN1 Advanced Settings

A-MPDU aggregation ● Enable ○ Disable

A-MSDU aggregation ○ Enable ● Disable

Short GI ○ Enable ● Disable

RTS Threshold 2347 (1-2347)

Fragment Threshold 2346 (256-2346)

Beacon Interval 100 (20-1024 ms)

DTIM Interval 1 (1-255)

Preamble Type ○ Long ● Auto

IGMP Snooping ● Enable ○ Disable

Antenna Number Two Antenna ▾

Roaming: ○ Enabled ● Disabled

The description of the columns is as below:

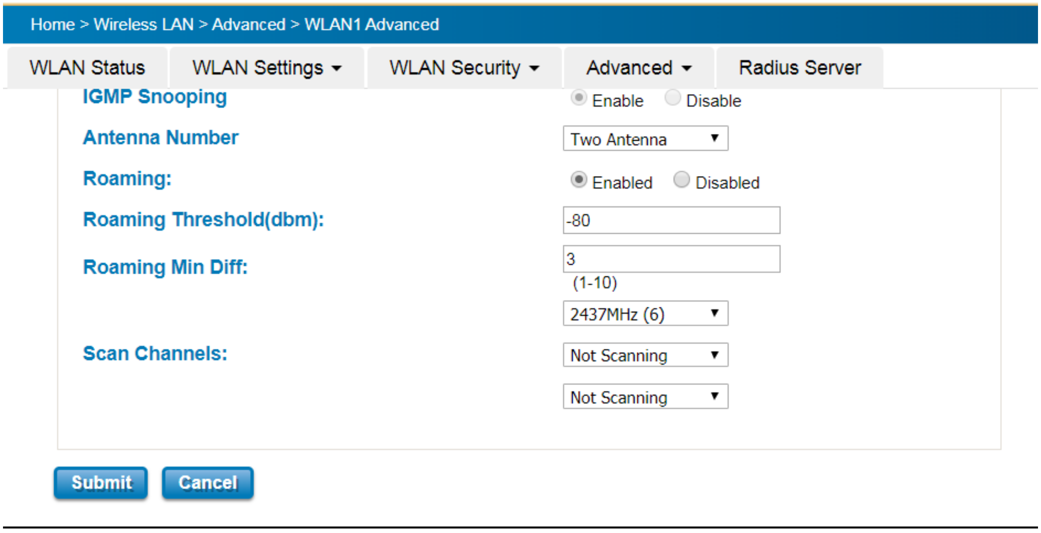
TERMS	DESCRIPTION
A-MPDU/A-MSDU aggregation	For the AP mode, the data rate of the AP could be enhanced greatly. Do not enable this function if the wireless clients don’t support A-MPDU/A-MSDU aggregation.
Short GI	Enable this function to obtain better data rate. (careful with compatibility issue)
RTS Threshold	**Default: 2347 (1-2347)** Basically, it is about the transmission process between the AP and the end station. When the AP sends Request to Send frames to station and it will do the negotiation process about sending the data frame. When the station receives an RTS frame, the station will respond with send back Clear to Send frame to confirm the right to start transmission.
Fragment Threshold	**Default: 2346 (256-2436)** Specify the maximum size in byte for a packet before data is fragmented into multiple packets. Setting it too low may result in poor network performance.
Beacon Interval	**Default: 100ms (20-1024 ms)** Specify the interval to broadcast packets.
DTIM Interval	**Default: 1 (1-255)** Delivery Traffic Indication Message interval is an additional message added after the beacon interval broadcast by access point. It is for enhancing the wireless transmission efficiency. The more intervals we added, the more power that we need. By setting a low value of DTIM, user can effectively keep the devices awake indefinitely so they

	never go into sleep mode when idling.
Preamble Type	**Default: Long** Preamble Type setting means that it adds some additional data header strings to help check the Wi-Fi data transmission errors. Basically, preamble type divided into two, long and short. Short is for shorter data strings that adds less data to transmit the error redundancy check which means that it is much faster. Long Preamble Type uses longer data strings which allow for better error checking capability. Auto Preamble Type the device can set the Preamble Type Automatically according to the need, which is can be long or can be short.
IGMP Snooping	**Default: Enable** By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the AP. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic.
Antenna Number	**Default: Two Antenna** The Antenna Number setting allows user to choose the antenna that used in the wireless connection. Basically, the default setting is set to Two antennas, because the device itself provide two antenna sockets. User can configure One Antenna or Two Antenna. Please refer to the Antenna Placement table to connect the antenna correctly.
Roaming	**Client Based Fast Roaming** The feature is available in WLAN Client mode. The client can check better AP by itself and start the Fast Roaming mechanism without AP controller. Select “Enable” to configure the Fast Roaming feature, you will find more advanced settings. Check the Fast Roaming description in below.

3.4.4.1 Roaming (Client based Fast Roaming)

The description of the columns after Enabled Fast Roaming is as below:

TERMS	DESCRIPTION
Roaming	Select "Enable" to configure the Fast Roaming feature, you will find more advanced settings as below.
Roaming Threshold(dbm)	Type the Threshold of when to roaming to new AP. While there are some APs, the client checks the signal strength, listens the available APs, and start to connect new AP while reaching the Roaming Threshold. You can check and measure the performance in the site, then type the suitable value for your environment.
Roaming Min Diff (1~10)	Default: 3 (Range: 1-10) It is practical to install multiple APs with overlapping coverage, this is gray or red zone area. In this area, the client with Fast Roaming can find other available APs, check better signal connectivity and then quickly switch to new AP. However, to avoid frequently switch the connected AP among the available APs, it is better to reserve a minimum gray area before switching from the connected AP to new AP. For example, the "Roaming Threshold" is configured as -55dbm and the Roaming Min Diff" is 3. The client starts Fast Roaming mechanism while the signal strength of other available AP is -55dbm. The Client continuously check the signal strength of the available APs, however, it still connects to original AP until the signal strength of the new available AP is less than -52dbm (Min Diff =3).
Scan Channel	Fixed the target scan channel can reach quick roaming performance. The system allows 3 channels, select the specific channel here.

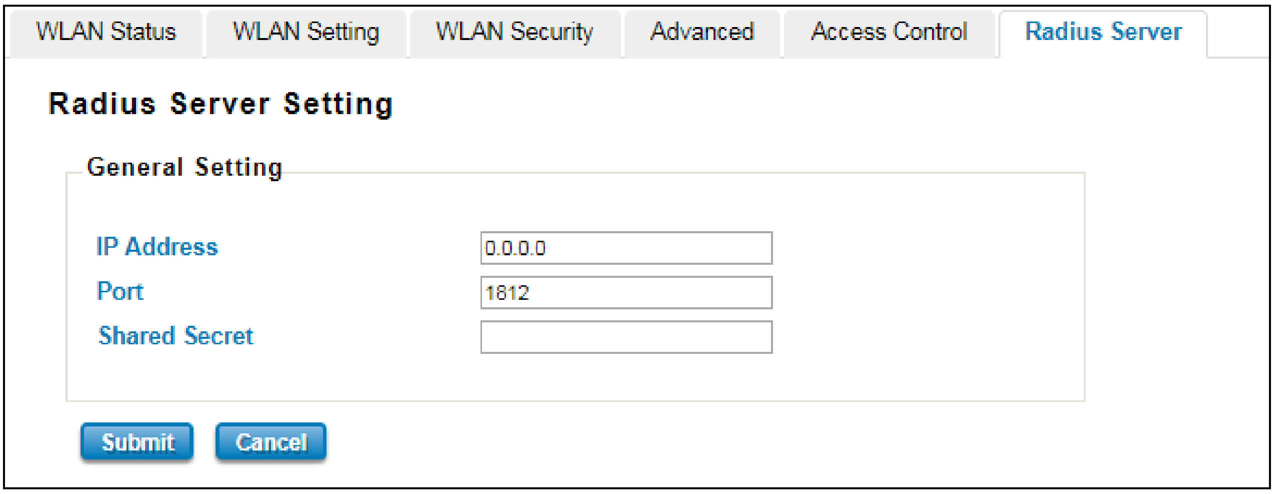


Home > Wireless LAN > Advanced > WLAN1 Advanced

IGMP Snooping	● Enable ○ Disable
Antenna Number	Two Antenna ▾
Roaming:	● Enabled ○ Disabled
Roaming Threshold(dbm):	-80
Roaming Min Diff:	3 (1-10)
Scan Channels:	2437MHz (6) ▾ Not Scanning ▾ Not Scanning ▾

3.4.5 RADIUS Server (AP Mode)

The Remote Authentication Dial In User Service (RADIUS) mechanism is a centralized “AAA” (Authentication, Authorization, and Accounting) system for connecting to network services. The fundamental purpose of RADIUS is to provide an efficient and secure mechanism for user account management. The RADIUS server system allows you to access the router through secure networks against unauthorized access.



Radius Server Setting

General Setting

IP Address 0.0.0.0

Port 1812

Shared Secret

How to set up a RADIUS server:

a. Enter the IP address of the RADIUS server in **Server IP Address**

b. Enter the **Shared Secret** of the RADIUS server

c. Enter the **Server port** if necessary, by default RADIUS server listens to port 1812

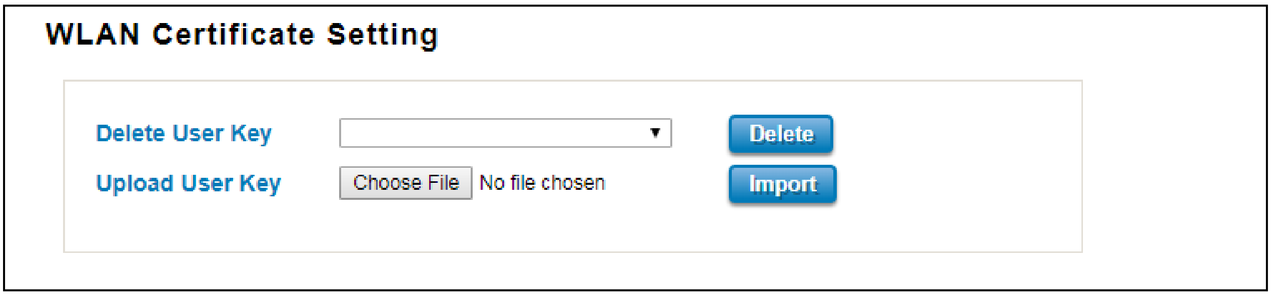
d. Click **Submit**

The description of the RADIUS Authentication interface is as below:

TERMS	**DESCRIPTION**
IP Address	Radius Server IP Address
Server Port	Set communication port on an external RADIUS server as the authentication database. The default value is 1812
Shared Key	Shared key is used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared key. Shared key also verifies that the RADIUS message has not been modified in transit (message integrity).

3.4.6 Certificate File (Client Mode)

Using digital certificates for authentication method through the RADIUS that provided by the AP. User needs to upload the specific certificate file, so then the client can access the Wi-Fi connection.



WLAN Certificate Setting

Delete User Key ▾ Delete

Upload User Key Choose File No file chosen Import

The description of the columns is as below:

TERMS	DESCRIPTION
Delete User Key	Delete the selected certificate
Upload User Key	Upload a certificate file from a specified file location

3.5 Security

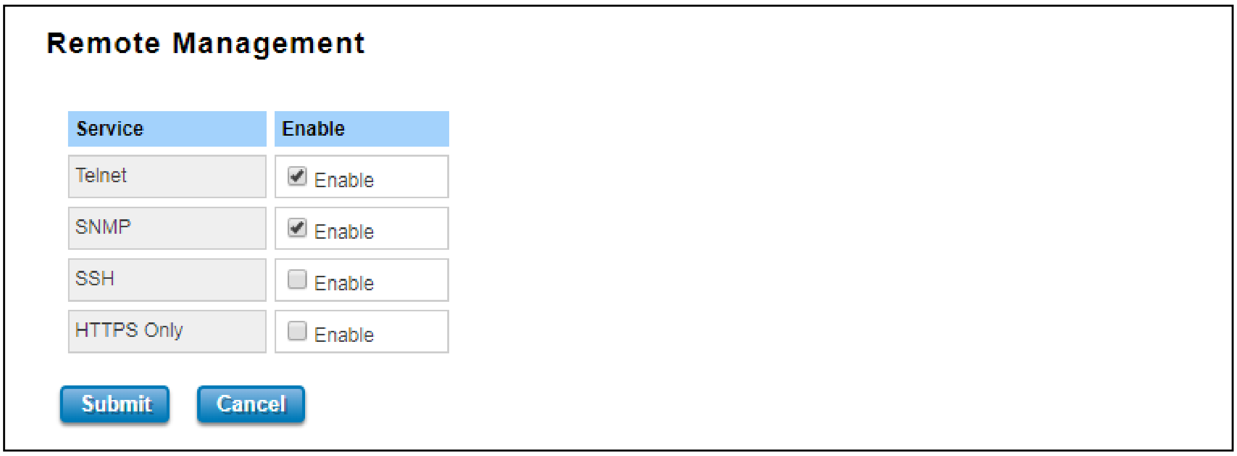
ISTRON Router provides several security features for User to secure access to its management functions and it can be remotely managed (monitored and configured).

3.5.1 Access Control

ISTRON router provides access control mode in several ways, such as Remote Management, WAN Service Access Control and Custom Exception. By configuring this configuration, user can enhance the security access to the device.

Remote Management

Remote management function: open the Remote Management, that would allow the user via the local access (WAN Port) Remote Management the router.



Remote Management

Service	Enable
Telnet	☑ Enable
SNMP	☑ Enable
SSH	□ Enable
HTTPS Only	□ Enable

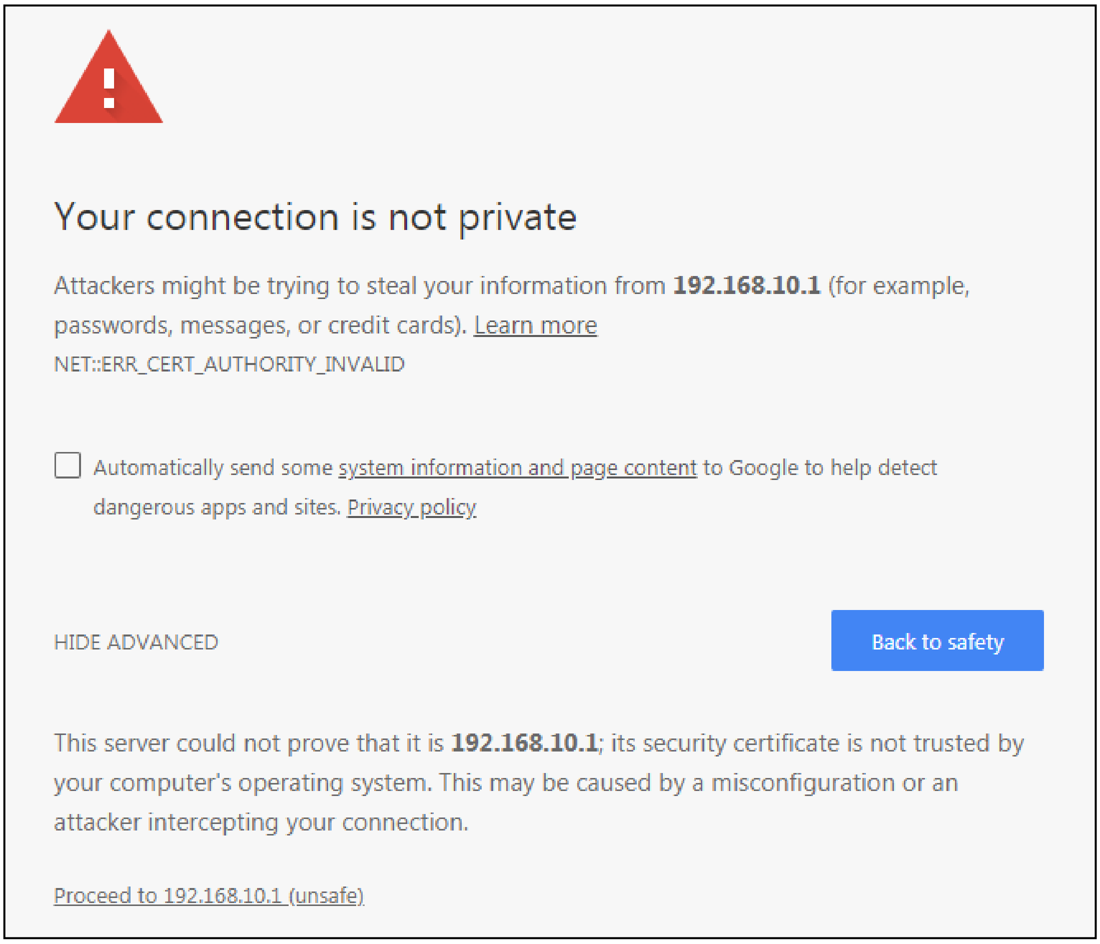
The description of the columns is as below:

TERMS	DESCRIPTION
Telnet	Allows the user to remotely login and manage the device by Telnet. When user doesn't enable it, the connection through telnet will not allow.
SNMP	Allows the user to remotely login and manage the device by SNMP. When user doesn't enable it, the connection through SNMP will not allow.
SSH	Allows the user to remotely login and manage the device by SSH/ When user doesn't enable it, the connection through SSH will not allow.
HTTPS Only	Allows the user to remotely login and manage the device by HTTPS access for secure connection, and it would disable the HTTP access.

Once User finishes configuring the settings, click on **Submit** to apply configuration.

HTTPS Only

HTTP Secure is the use of the HTTP protocol over an SSL/TLS protocol. It is used primarily to protect against eavesdropping of communication between a web browser and the web site to which it is connected. This is especially important when you wish to have a secure connection over a public network such as the internet. HTTPS connections are secured through the use of certificates issued by trusted certificate authorities. When a web browser makes a connection attempt to a secured web site, a digital certificate is sent to the browser so that it can verify the authenticity of the site using a built-in list of trusted certificate authorities.



Your connection is not private

Attackers might be trying to steal your information from **192.168.10.1** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_AUTHORITY_INVALID

□ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

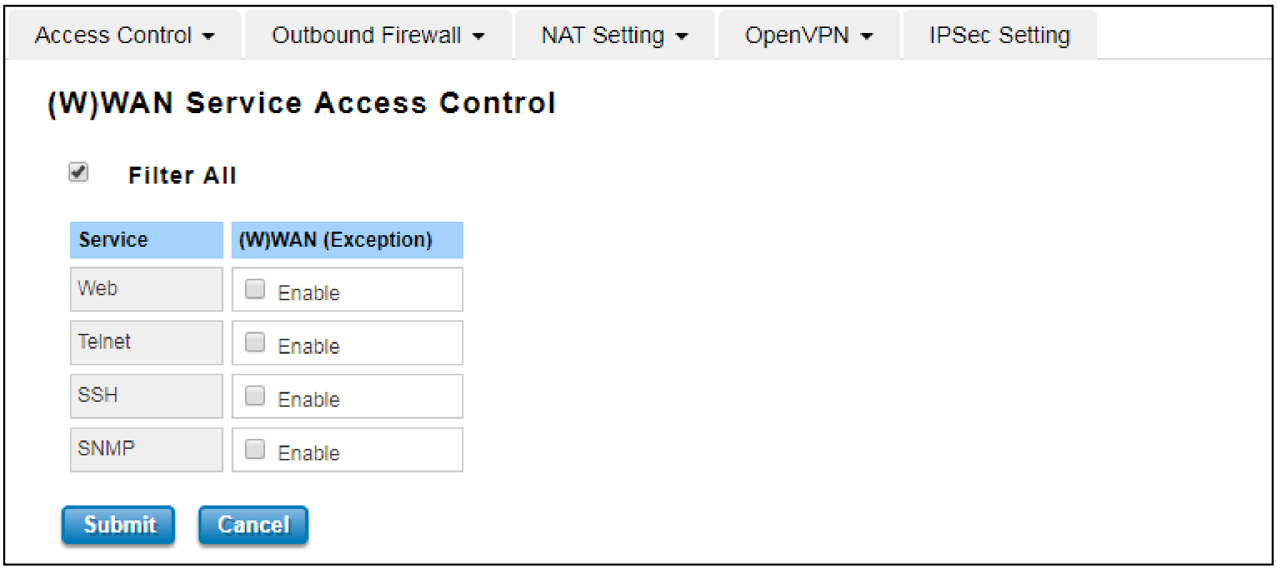
This server could not prove that it is **192.168.10.1**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

Proceed to 192.168.10.1 (unsafe)

If user uses the HTTPS Only, a warning page would appear when user access the device in order to provide a secure access. The picture above is the warning message about the digital certificate and user just need to accept this warning by click **"Proceed to 192.168.10.1 (unsafe)"**.

WAN Access

When user changes the device mode to **router mode (Port 1 – WAN interface)** the WAN Access feature can be activated. This feature is about the exception to access the device through the WAN interface for security concern. So that the access or the traffic that coming through the WAN interface can be limited as required. The user may choose the **Filter All** functions to block all access from the WAN interface or enable the exception options, then the router allows user to remotely access to the router from WAN interface.



(W)WAN Service Access Control

☑ Filter All

Service	(W)WAN (Exception)
Web	□ Enable
Telnet	□ Enable
SSH	□ Enable
SNMP	□ Enable

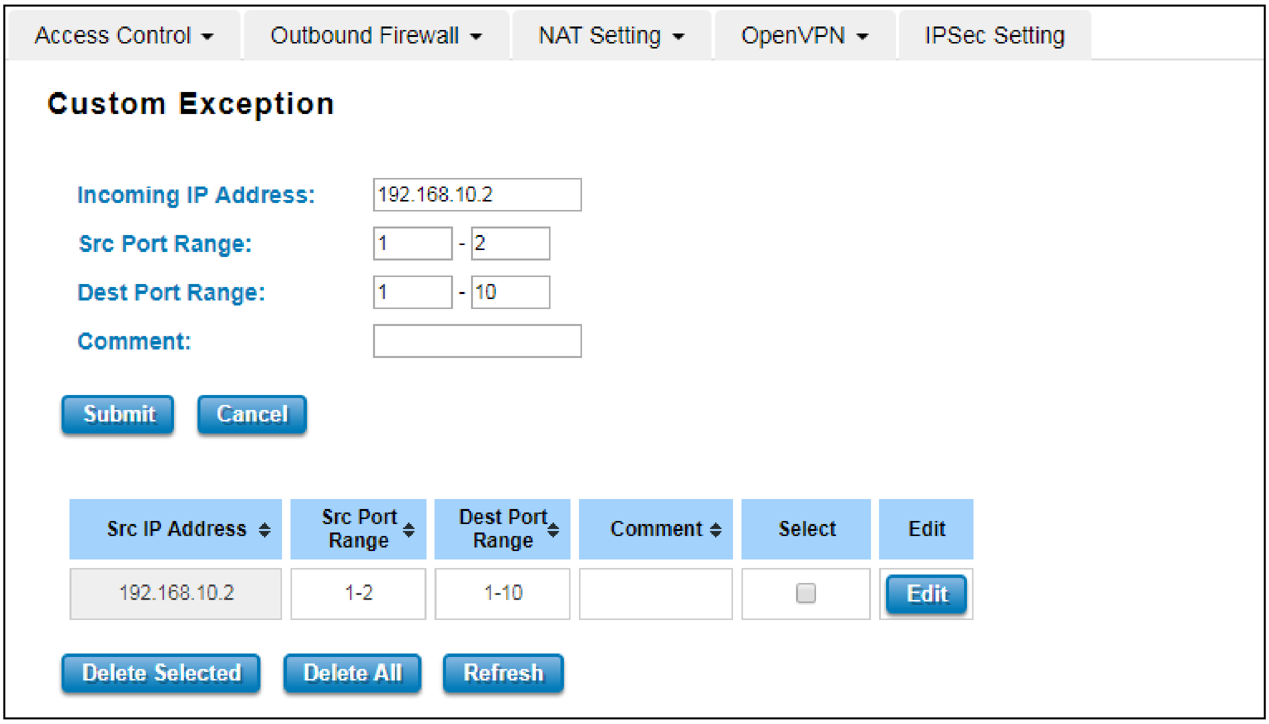
The description of the columns is as below:

TERMS	DESCRIPTION
Filter All	By select Filter All, it will block all external access from WAN interface to the device (such as SSH, SNMP, Web and Telnet) and unblock the exception options.
Web	Select this option to allow access to the router using Web (HTTP or HTTPS) from the WAN Interface
Telnet	Select this option to allow access to the router using Telnet from the WAN Interface
SSH	Select this option to allow access to the router using SSH from the WAN Interface
SNMP	Select this option to allow access to the router using SNMP from the WAN Interface

Once User finishes configuring the settings, click on **Submit** to apply configuration.

Custom Exception

Another choice for the access control is also provided by ISTRON, it is called custom exception feature. Through this feature, it can help to allow the incoming access through the firewall to local devices. If the condition does not meet the requirement from the table, then the access would be denied.



Custom Exception

Incoming IP Address: 192.168.10.2

Src Port Range: 1 - 2

Dest Port Range: 1 - 10

Comment:

Src IP Address ⇕	Src Port Range ⇕	Dest Port Range ⇕	Comment ⇕	Select	Edit
192.168.10.2	1-2	1-10		□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Src IP Address	Set up the source IP Address that may access the device.
Src Port Range	Set up the source port range where the access came from.
Dest Port Range	Set up the destination port range where the access is going to.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

Once User finishes configuring the settings, click on **Submit** to apply configuration and a new line will directly appear on the table.

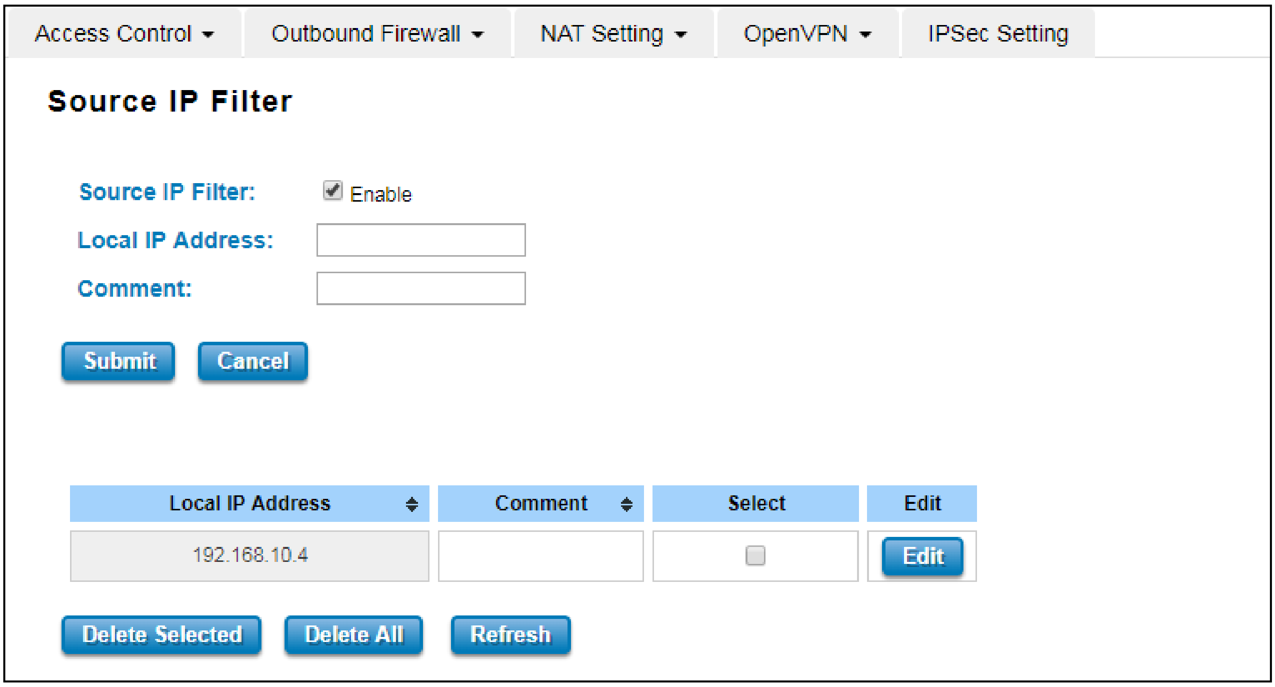
3.5.2 Outbound Firewall

ISTRON' router has different types firewall settings, user can enable the setting, configure the rules. The following section is Outbound Firewall Settings pages where user can configure the Outbound Firewall setting.

TERMS	DESCRIPTION
Source IP Filter	Source IP addresses Filtering from LAN to Internet through the router.
Destination IP Filter	Destination IP addresses Filtering from the LAN to Internet through the router.
Source Port Filtering	Source Ports Filtering from the LAN to Internet through the router.
Destination Port Filtering	Destination Ports Filtering from the LAN to Internet through the router

Src IP Filter

By entries parameter in this table, it can restrict certain types of data packets from the local network to the internet through the Router. The Source IP Filter will help to filter all of the packets that coming into the router. If the source IP is on the list, then the packets would be dropped. But if the source IP is not on the list, then the packets can be received. Select **Enable** to activate **Source IP Filtering**, type the **Local IP Address** and **Comment** to write notes for the entry. Click Submit to activate the settings. After applied, then user can see the new entry shown in the below table.



Source IP Filter

Source IP Filter: ☑ Enable

Local IP Address:

Comment:

Local IP Address	Comment	Select	Edit
192.168.10.4		□	Edit

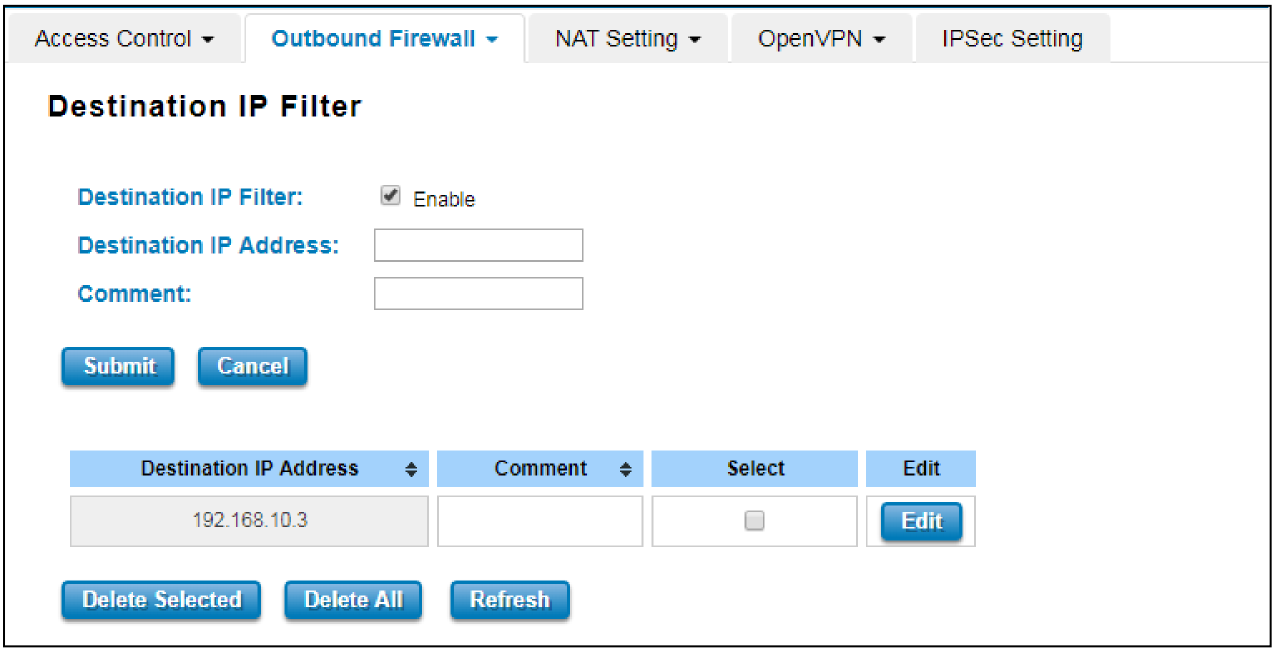
The description of the columns is as below:

TERMS	DESCRIPTION
Local IP Address	Display the Source IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

Click **Refresh** to refresh the table

Dest IP Filter

By entries parameters in this table are used to restrict the computers in LAN from accessing certain websites in WAN according to IP address. The concept is the same as the source IP Filter. The packet would not send to the specific IP Address that showed on the list. Only the IP Address that shows on the list that cannot receive the packets. Select **Enable** to activate **Destination IP Filtering**, type the **Destination IP Address** and **Comment** to write a note for the entry and then click Submit to apply the settings. After applied, then user can see the new entry shown in the below table.



Destination IP Filter

Destination IP Filter: ☑ Enable

Destination IP Address:

Comment:

Destination IP Address	Comment	Select	Edit
192.168.10.3		□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Destination IP Address	Display the Destination IP address.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

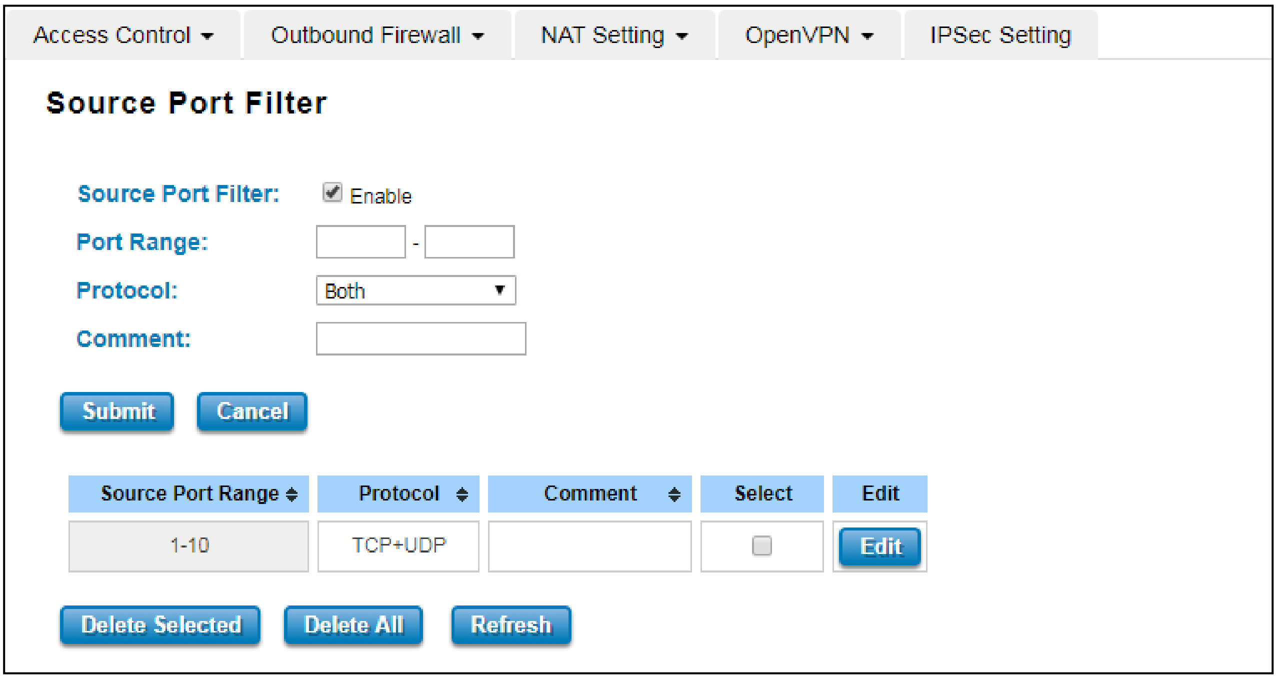
Click **Refresh** to refresh the table

Src Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to the Internet through the Router. Use of such filters can be helpful in securing or restricting local network. The device just cannot receive any packets from the source port that showed on the list, the other packet that sent from any source port that not on the list would be received.

Select **Enable Source Port filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or Both**. Type the **Comment** to write a note for the entry and then click **Submit** to activate the settings.

After applied, user can see the new entry shown in the below table.



Source Port Filter

Source Port Filter: ☑ Enable

Port Range: [ ] - [ ]

Protocol: Both ▾

Comment: [ ]

Source Port Range ⬍	Protocol ⬍	Comment ⬍	Select	Edit
1-10	TCP+UDP		□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Source Port Range	Display the Source Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

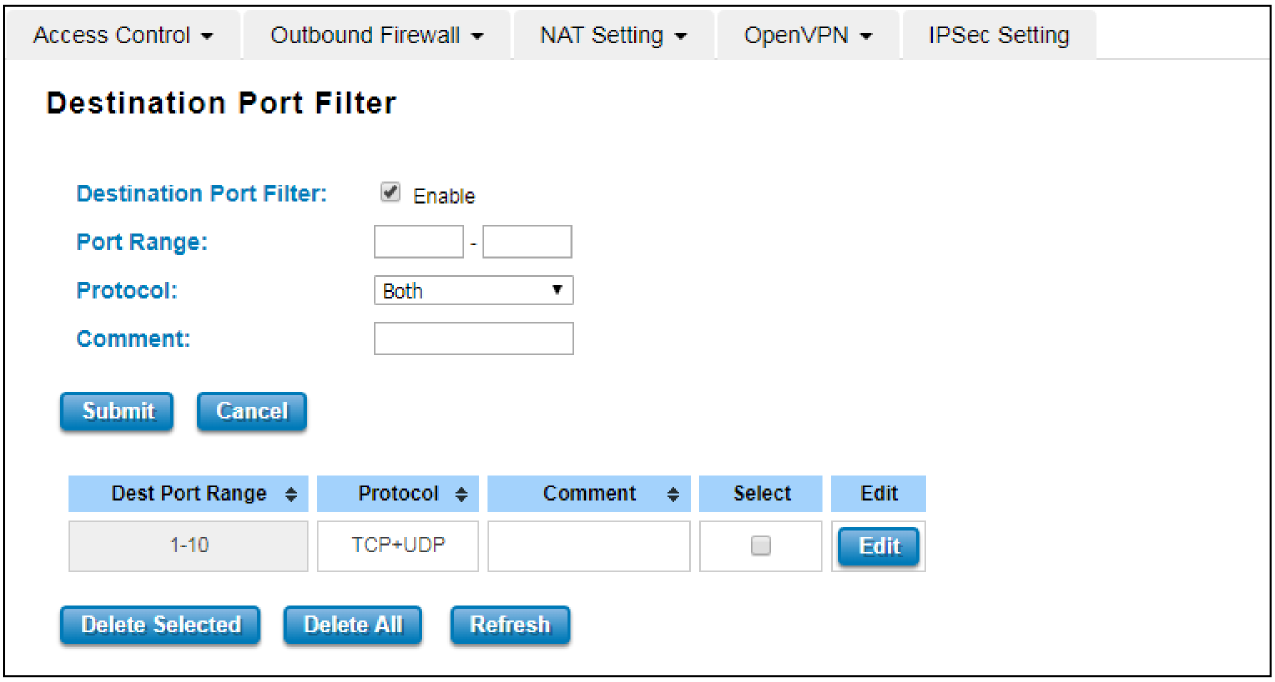
Click **Refresh** to refresh the table

Dest Port Filter

Entries in this table are used to restrict certain ports of data packets from user's local network to Internet through the router. Use of such filters can be helpful in securing or restricting local network. And the device cannot send any packets to the destination port that showed on the list.

Select **Enable Destination Port Filtering**, type the **Port Range** of below **Protocol** type, the protocol type can be **UDP, TCP or Both**. Type the **Comment** to write note for the entry and then press **Submit** to apply the settings.

After applied, then user can see the new entry shown in the below table.



Destination Port Filter

Destination Port Filter: ☑ Enable

Port Range: [ ] - [ ]

Protocol: Both

Comment: [ ]

Dest Port Range	Protocol	Comment	Select	Edit
1-10	TCP+UDP		□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
Dest Port Range	Display the Destination Port Range (Range is from 1 to 65535)
Protocol	Display the protocol that has been chosen by the user.
Comment	Put any notes for the entry.
Select	Select the table, so user can press **Delete Selected** to delete,
Edit	Click edit to modify the parameters

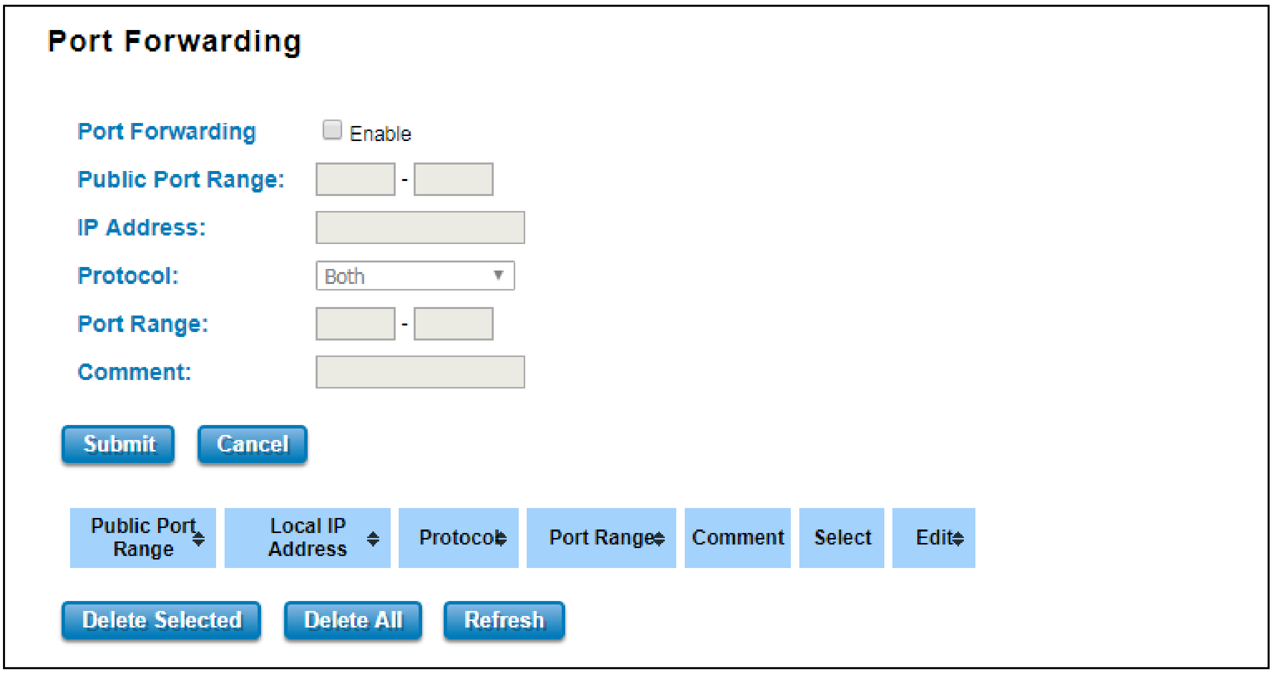
Click **Refresh** to refresh the table

3.5.3 NAT Setting

Network Address Translation is the process where a network device, usually a firewall, assigns a public address to a device or group of devices inside a private network. The main use of NAT is to limit the number of public IP addresses an organization or company must use, for both economic and security purposes. The simple type of NAT provides one to one translation of IP address. It can be used to interconnect two IP networks, normally one network is for Local Area Network and the other network is for Wide Area Network/Internet. To support this function, there are two ways to do it, by using Source Network Address Translation (SNAT), Destination Network Address Translation (DNAT). Basically, Network Address Translation (NAT) occurs when one of the IP addresses in an IP packet header is changed. In a SNAT, the destination IP address is maintained and the source IP address is changed. Most commonly, a SNAT allows a host on the "inside" of the NAT, in an RFC 1918 IP address space, to initiate a connection to a host on the "outside" of the NAT. It supports the Port Forwarding, DMZ and 1 to 1 NAT configuration. A DNAT, by way of contrast, occurs when the destination address is changed and the source IP address is maintained. A DNAT allows a host on the "outside" to connect to a host on the "inside". In both cases, the NAT has to maintain a connection table which tells the NAT where to route returning packets. An important difference between a SNAT and a DNAT is that a SNAT allows multiple hosts on the "inside" to get to any host on the "outside". By way of contrast, a DNAT allows any host on the "outside" to get to a single host on the "inside". It is supported in NAPT and 1 to 1 NAT features.

To configure the NAT Setting, the **Port Forwarding, DMZ, Port Mapping Policy and 1 to 1 NAT** configuration page are provided in this section.

Port Forwarding



Port Forwarding

Port Forwarding: □ Enable

Public Port Range: -

IP Address:

Protocol: Both

Port Range: -

Comment:

By configuring this table, it allows user to automatically redirect common network services to a specific machine behind the NAT firewall. Select **Enable** to activate **Port Forwarding** function and then input all of the parameters to configure the port forwarding.

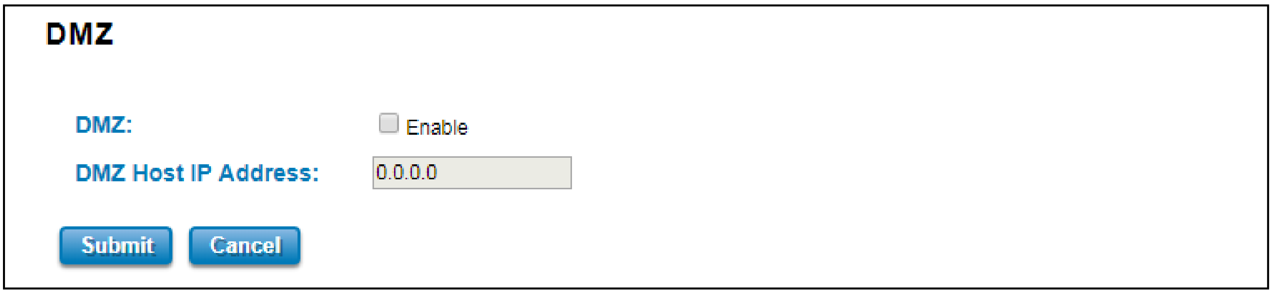
The description of the columns is as below:

TERMS	DESCRIPTION
Port Forwarding	Select Enable to activate Port Forwarding function.
Public Port Range	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.
IP Address	Configure the IP Address of the LAN PC. The traffic from the public port range will be redirected to this IP address.
Protocol	Configure TCP, UDP or Both (TCP + UDP) protocol type.
Port Range	Configure the port range of the LAN; the traffic from the public port will be redirected to these ports.
Comment	Add information to the entry.

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

DMZ

A **Demilitarized Zone** is used to provide Internet services without sacrificing unauthorized access to its local private network. Typically, the DMZ host contains device accessible to Internet traffic, such as Web (HTTP) servers, FTP servers, SMTP (e-mail) servers and DNS servers.



DMZ

DMZ: □ Enable

DMZ Host IP Address: 0.0.0.0

Click **Enable** to activate the function and assign the IP address of **DMZ Host IP Address**. This is the DMZ computer’s IP address. Click Submit to activate the function.

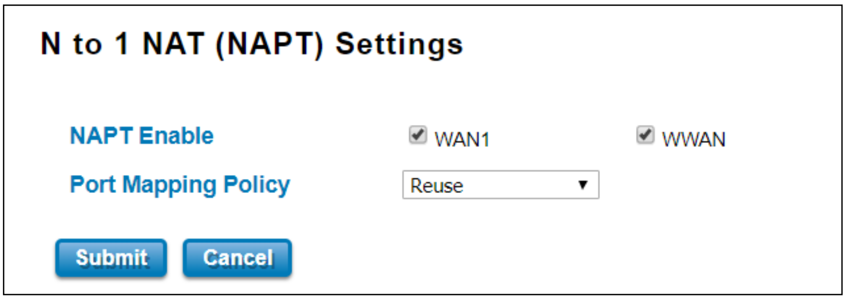
The description of the columns is as below:

TERMS	DESCRIPTION
DMZ	Select Enable to activate DMZ function.
DMZ Host IP Address	Configure the port range, which will be public to a WAN / Internet. User can configure one or a range of TCP/UDP port number.

Click **Submit** to apply the configuration.

N to 1 NAT (NAPT) /Port Mapping Policy

This page allows user to Enable NAPT interface and configure the Port Mapping policy from NAT Setting.



N to 1 NAT (NAPT) Settings

NAPT Enable ☑ WAN1 ☑ WWAN

Port Mapping Policy: Reuse

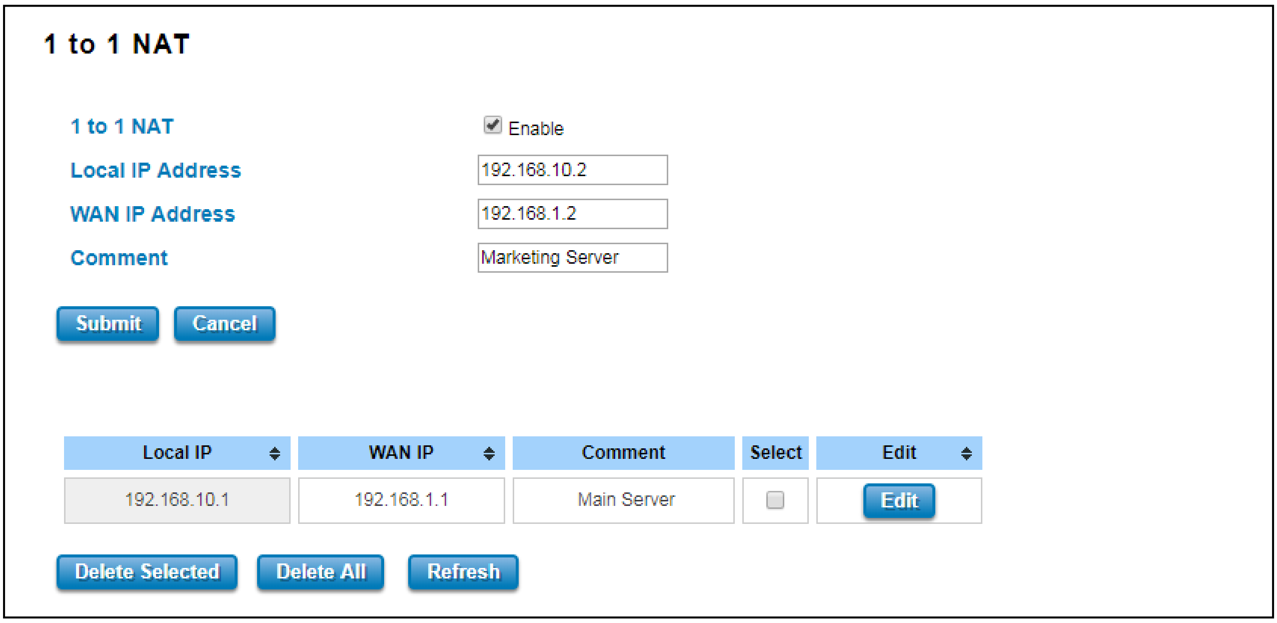
The description of the columns is as below:

TERMS	DESCRIPTION
NAPT Enable	Select the Interface while the router supports multiple WAN ports. There is only one activate WAN interfaces in this AP, select either Ethernet WAN or Wireless WAN. While you select Router/Client Router mode for both Ethernet and Wireless LAN interfaces, Client Router of Wireless WAN has higher priority and only it works.
Port Mapping Policy	**Default: Reuse** Reuse: Use the same port number that has been used to access the same remote device. Randomize: Change the port number every time access the remote device.

Click **Submit** to apply the configuration.

1 to 1 NAT

One-to-one NAT is a way to make systems behind a firewall and configured with private IP addresses (those reserved for private use in RFC 1918) appear to have public IP addresses. With one-to-one NAT, you assign local systems RFC 1918 addresses then establish a one-to-one mapping between those addresses and public IP addresses. For outgoing connections SNAT (Source Network Address Translation) occurs and on incoming connections DNAT (Destination Network Address Translation) occurs. Below is the 1 to 1 NAT section interface.



1 to 1 NAT

1 to 1 NAT: ☑ Enable

Local IP Address: 192.168.10.2

WAN IP Address: 192.168.1.2

Comment: Marketing Server

Local IP	WAN IP	Comment	Select	Edit
192.168.10.1	192.168.1.1	Main Server	□	Edit

The description of the columns is as below:

TERMS	DESCRIPTION
1 to 1 NAT	Check the box to enable the function
Local IP Address	The target local IP Address
WAN IP Address	The incoming IP Address that coming through the WAN
Comment	Enter a comment

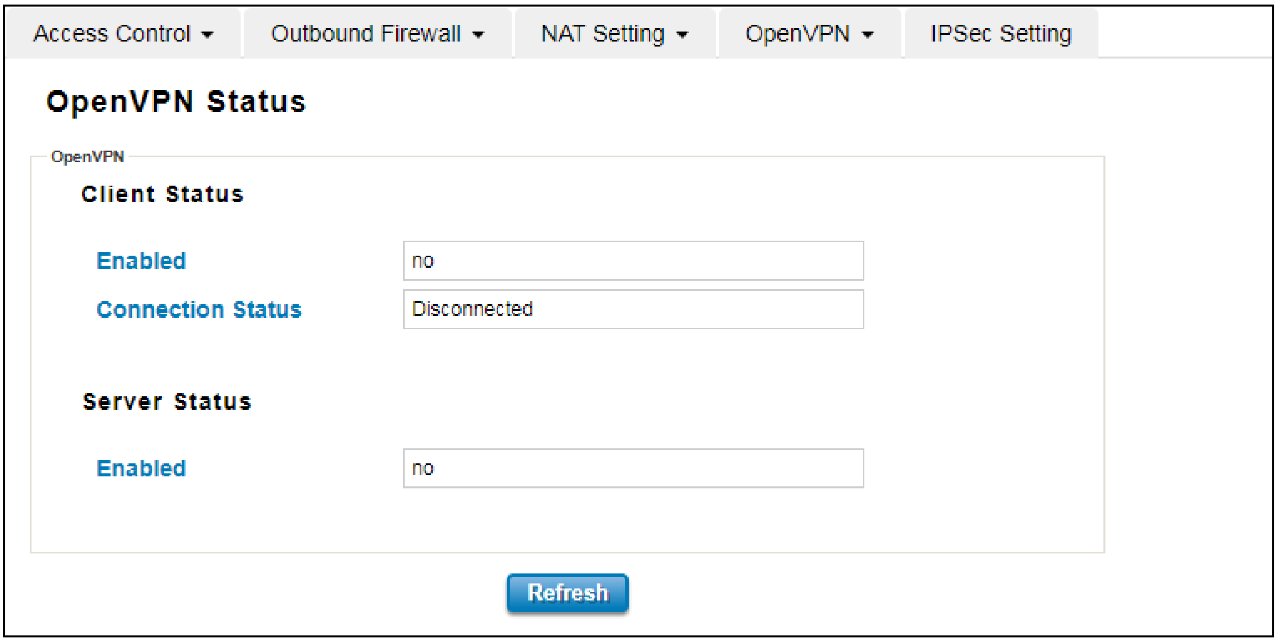
Click **Submit** to apply the configuration.

3.5.4 OpenVPN

ISTRON router supports OpenVPN. It implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections. It is possible to create one-to-many tunnel for the VPN Server. OpenVPN implementation offers a cost-effective, simply configurable alternative to other VPN technologies. OpenVPN allows peers to authenticate each other using a pre-shared secret key, certificates, or username/password. The server and client have almost the same configuration. The difference in the client configuration is the remote endpoint IP or hostname field. Also, the client can set up the keepalive settings.

OpenVPN Status

This section shows the VPN Client and Server current status.



OpenVPN Status

OpenVPN

Client Status

Enabled: no

Connection Status: Disconnected

Server Status

Enabled: no

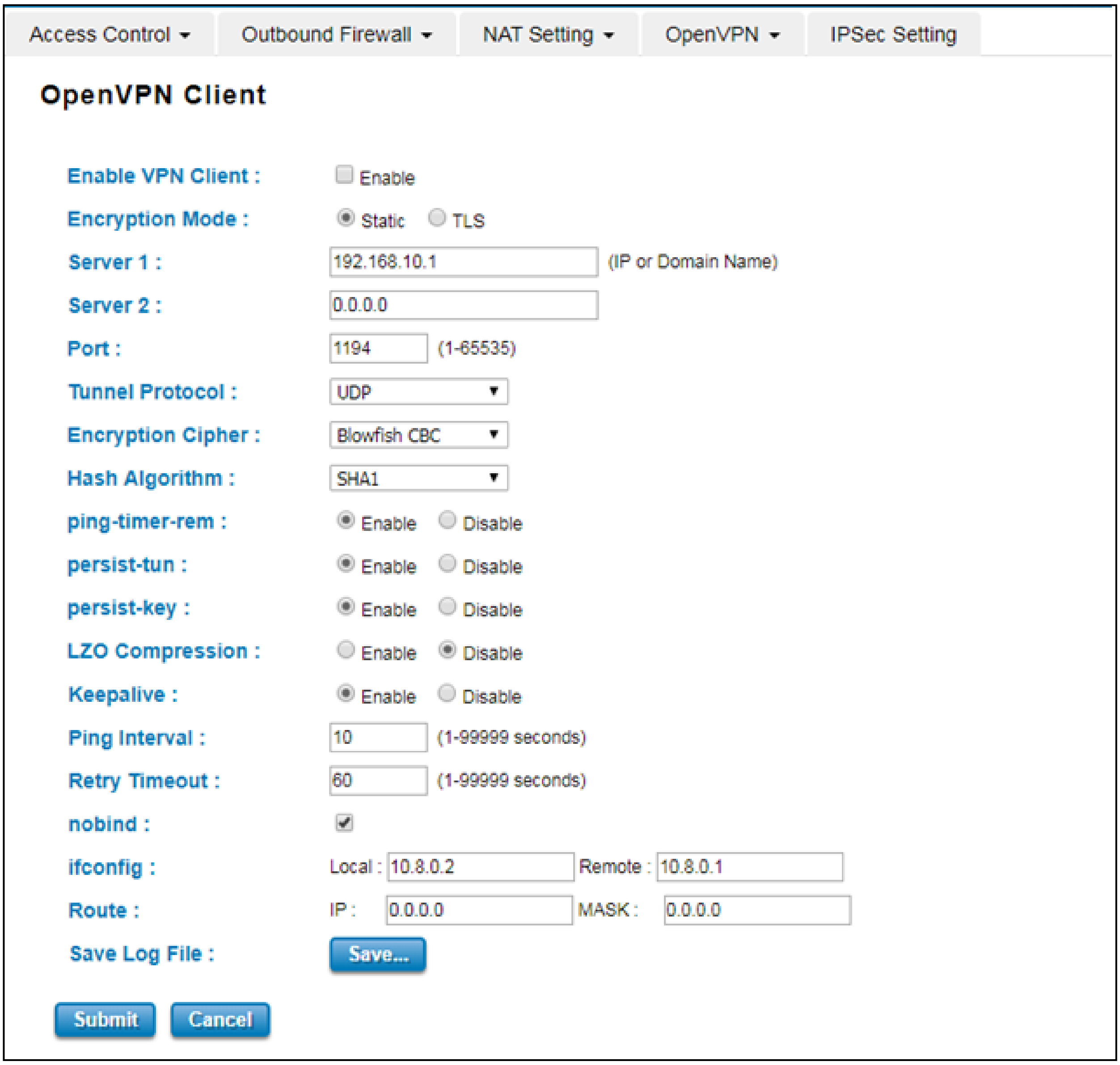
The description of the columns is as below:

TERMS	DESCRIPTION
Enabled	**Default: no** **yes:** The VPN function is enabled. **no:** The VPN function is not enabled
Connection Status	**Default: Disconnected** **Connected:** The VPN connection is established **Disconnected:** The VPN connection is not established

Click **Refresh** to update the information.

OpenVPN Client

This page is about the OpenVPN Client configuration page. While the device set as the VPN client, the parameters must follow the VPN Server settings. User should adjust the parameters with the administrator of the VPN server to entry the correct parameters. Two VPN servers IP are also provided in order to have the backup connection for VPN Server.



OpenVPN Client

Enable VPN Client : □ Enable

Encryption Mode : ● Static ○ TLS

Server 1 : 192.168.10.1 (IP or Domain Name)

Server 2 : 0.0.0.0

Port : 1194 (1-65535)

Tunnel Protocol : UDP

Encryption Cipher : Blowfish CBC

Hash Algorithm : SHA1

ping-timer-rem : ● Enable ○ Disable

persist-tun : ● Enable ○ Disable

persist-key : ● Enable ○ Disable

LZO Compression : ○ Enable ● Disable

Keepalive : ● Enable ○ Disable

Ping Interval : 10 (1-99999 seconds)

Retry Timeout : 60 (1-99999 seconds)

nobind : ☑

ifconfig : Local : 10.8.0.2 Remote : 10.8.0.1

Route : IP : 0.0.0.0 MASK : 0.0.0.0

Save Log File :

The description of the columns is as below:

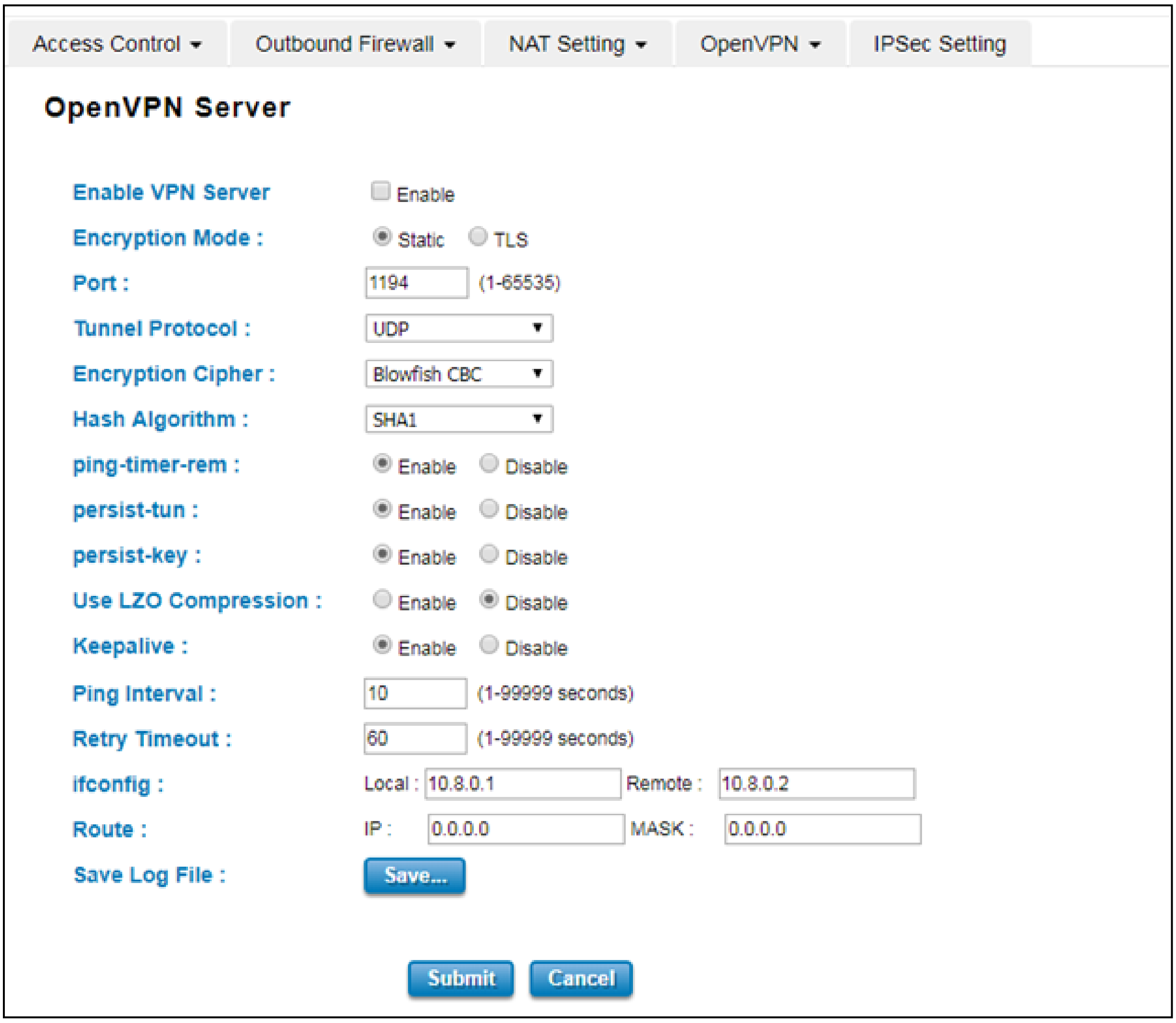
TERMS	DESCRIPTION
Enable VPN Client	Select Enable to activate the VPN Client function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.

Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1，SHA256，SHA512，MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, this function prevent unnecessary restart at server/client when network fail.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is use to detect the status of connection.
Ping Interval	**Default: 10** Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	**Default: 60** Input the retry timeout, the range can from 1~99999 seconds.
nobind	Check the box to activate nobind function. With nobind function, the source ports are random.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Client Log.

Click **Submit** to apply the configuration.

OpenVPN Server

To help user create the One to One Secure connection for the remote devices, ISTRON device supports both OpenVPN Server and OpenVPN Client. This Server setting allows user to configure the Secure M2M connection for one remote Client. But ISTRON router also supports one to multiple for VPN Client.



OpenVPN Server

Enable VPN Server	□ Enable
Encryption Mode :	● Static ○ TLS
Port :	1194 (1-65535)
Tunnel Protocol :	UDP
Encryption Cipher :	Blowfish CBC
Hash Algorithm :	SHA1
ping-timer-rem :	● Enable ○ Disable
persist-tun :	● Enable ○ Disable
persist-key :	● Enable ○ Disable
Use LZO Compression :	○ Enable ● Disable
Keepalive :	● Enable ○ Disable
Ping Interval :	10 (1-99999 seconds)
Retry Timeout :	60 (1-99999 seconds)
ifconfig :	Local : 10.8.0.1 Remote : 10.8.0.2
Route :	IP : 0.0.0.0 MASK : 0.0.0.0
Save Log File :	Save...

The description of the columns is as below:

TERMS	DESCRIPTION
Enable VPN Server	Select Enable to activate the VPN Server function
Encryption Mode	Choose the Encryption Mode Static Key: Use a pre-shared static key. TLS: Use SSL/TLS + certificates for authentication and key exchange.
Server 1	Type the IP Address of the VPN Server
Server 2	Type the second IP Address of the VPN Server if needed.
Port	**Default: 1194** Input the port number that VPN service used. Please check the VPN Server port setting. The range from 1-65535.
Tunnel Protocol	Choose use TCP or UDP to establish the VPN connection.
Encryption Cipher	Select the encryption cipher from Blowfish to AES in Pull-down menus.
Hash Algorithm	Hash algorithm provides a method of quick access to data, including SHA1, SHA256, SHA512, and MD5
ping-timer-rem	**Default: Enable** Select enable or disable the ping-timer-rem, this function is to prevent

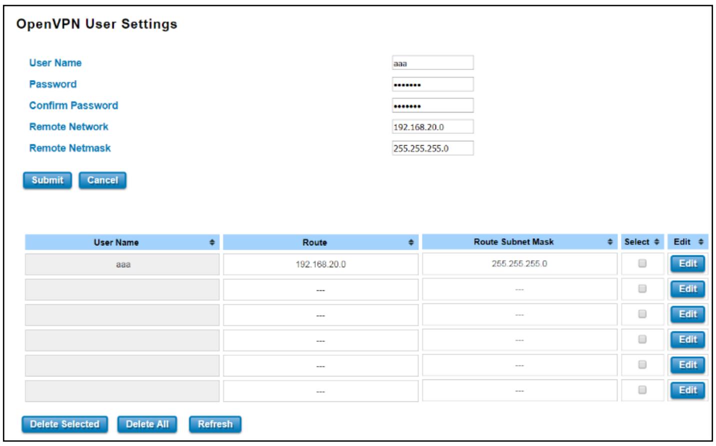
	unnecessary restart at server/client when the network fails.
persist-tun	**Default: Enable** Select enable or disable the persist-tun, enable this function will keep tun(layer 3) device linkup after Keepalive timeout.
persist-key	**Default: Enable** Select enable or disable the persist-key, enable this function will keep the key first use if VPN restart after Keepalive timeout.
LZO Compression	**Default: Disable** Select use LZO Compression or not, this function compresses data to decrease the traffic, but also need more CPU effort.
Keepalive	**Default: Enable** Select enable or disable Keepalive function, this function is used to detect the status of the connection.
Ping Interval	Input the ping interval, the range can from 1~99999 seconds.
Retry Timeout	Input the retry timeout, the range can from 1~99999 seconds.
ifconfig	Input the tunnel IP addresses that VPN use.
Route	Input the route IP and MASK. This is the target IP domain that user can access through the VPN tunnel.
Save Log File	Click Save to keep the VPN Server Log.

Click **Submit** to apply the configuration.

OpenVPN User Settings

This is extended setting of OpenVPN Server and applied in 1 Server to N Clients OpenVPN connectivity.

You can add User Name settings in this page. Add User Name, Password and Confirm Password, Remote Network and Netmask and click “Submit”. Then you can see the User Name database in below column.

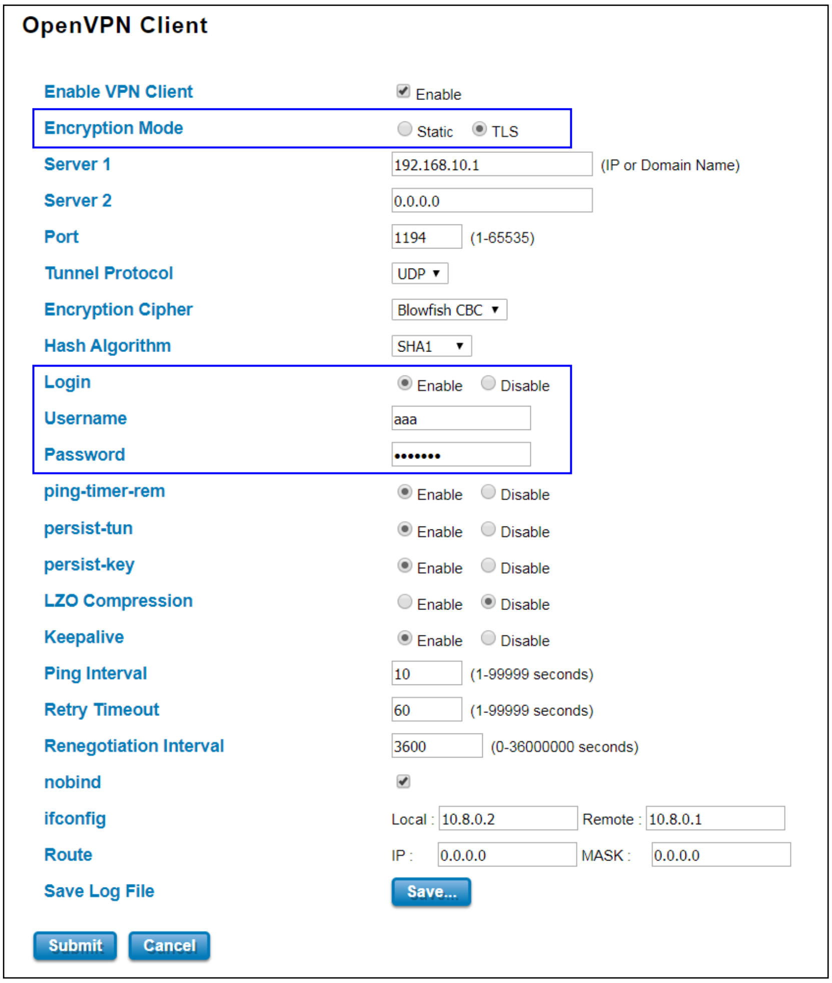


OpenVPN User Settings

User Name	aaa
Password	•••••••
Confirm Password	•••••••
Remote Network	192.168.20.0
Remote Netmask	255.255.255.0

User Name	Route	Route Subnet Mask	Select	Edit
aaa	192.168.20.0	255.255.255.0	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit
	---	---	□	Edit

In OpenVPN client, you must type correct user name and password for authentication. Below is our OpenVPN client setting page, select the “**TLS**” Encryption Mode and Enable ”**Login**” checkbox, then the Username/Password columns are displayed. Type correct Username and password added in OpenVPN User Settings.

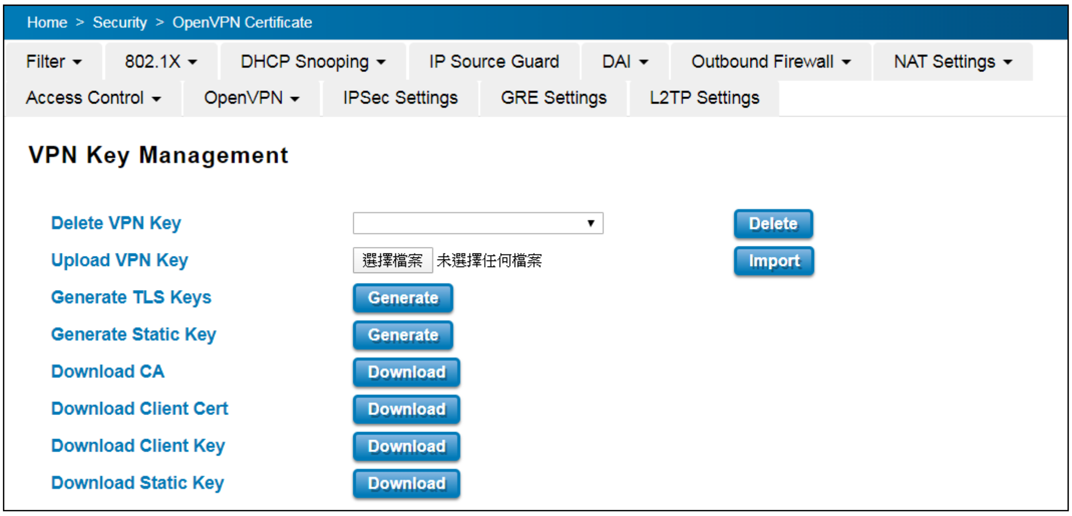


OpenVPN Client

Enable VPN Client	☑ Enable
Encryption Mode	○ Static ● TLS
Server 1	192.168.10.1 (IP or Domain Name)
Server 2	0.0.0.0
Port	1194 (1-65535)
Tunnel Protocol	UDP ▾
Encryption Cipher	Blowfish CBC ▾
Hash Algorithm	SHA1 ▾
Login	● Enable ○ Disable
Username	aaa
Password	•••••••
ping-timer-rem	● Enable ○ Disable
persist-tun	● Enable ○ Disable
persist-key	● Enable ○ Disable
LZO Compression	○ Enable ● Disable
Keepalive	● Enable ○ Disable
Ping Interval	10 (1-99999 seconds)
Retry Timeout	60 (1-99999 seconds)
Renegotiation Interval	3600 (0-36000000 seconds)
nobind	☑
ifconfig	Local : 10.8.0.2 Remote : 10.8.0.1
Route	IP : 0.0.0.0 MASK : 0.0.0.0
Save Log File	Save...

OpenVPN Certificate

Using digital certificates for authentication instead of preshared keys in VPNs is considered more secure. In ISTRON’ devices, digital certificates are one way of authenticating two peer devices to establish a VPN tunnel.



Key Generation in the device

For OpenVPN connectivity, the OpenVPN Client must have the client Key/CA file generated by the OpenVPN Server. Normally, you can generate the key in your VPN server and upload to the router switch which is Open VPN client. However, while you just want to establish site to site VPN connectivity, install another Open VPN server may consume lots of cost and engineer effort.

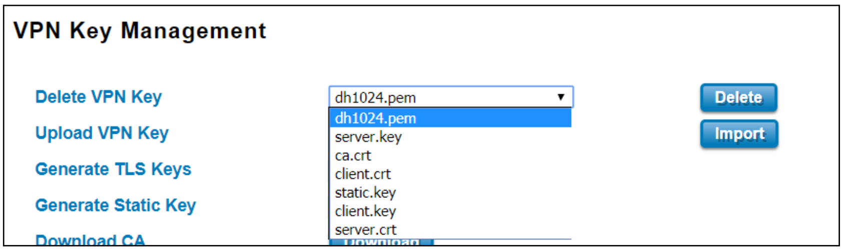
In the latest firmware, the ISTRON Secure Router Switch supports Key generation feature. Click **“Generate”** in **“Generate TLS Keys”** and **“Generate Static Key” in the Open VPN Router**, the system prompts you to wait 30 seconds to generate the key. Click “Yes” to start and wait 30 seconds. After generated, there are some VPN key/CA files generated and stored within the system. The files include both OpenVPN Server and Client key/ca files.

The two key/ca files, **dh1024.pem and server.crt** are applied to Open VPN Server only. The two files must be stored within the Open VPN server. **For security concern, the files are not allowed to download. You just need to generate the keys while configured the Router as an Open VPN Server.**

The rest of key/ca files include **CA, Client Cert and Client Key**. The three files must be stored within both the Open VPN server and client. You can download the keys to your PC and upload the files to OpenVPN client. Then the client has the same key. This is usefully tool for you to build you OpenVPN connectivity.

If you prefer to use Static Key, you can generate the **static.key** in OpenVPN Server and put the key in both OpenVPN Server and Clients.

You can see the files’ name by select the drop-down menu of “Delete VPN Key”, download/import OpenVPN client key/ca files in below columns.

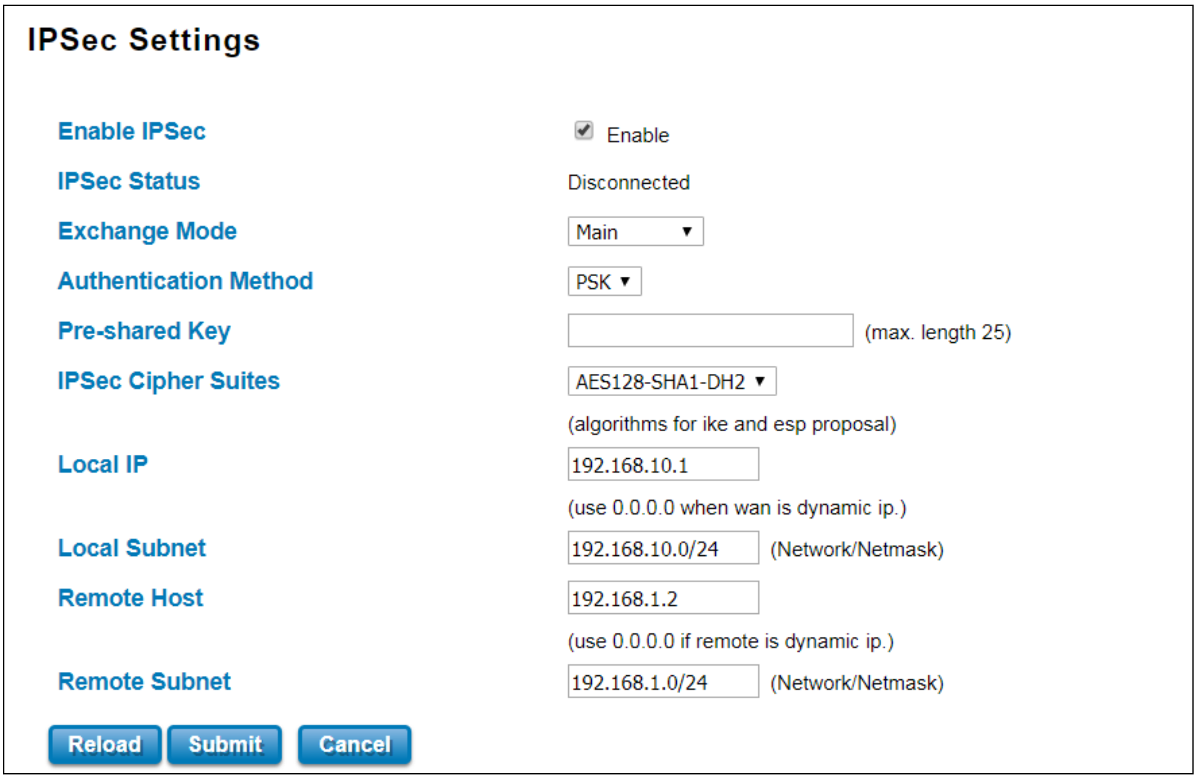


The description of the columns is as below:

TERMS	DESCRIPTION
Delete VPN Key	Display the ca/key files after generated TLS/Static Key. You can select and Delete the ca/key file here.
Upload VPN Key	Upload a certificate file from a specified file location.
Generate TLS Keys	The setting allows you to generate TLS key/ca files by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start…then you will have multiple key/ca files.
Generate Static Key	The setting allows you to generate Static key by the router switch. After click Generate, the system prompts you to wait 30 seconds to generate the key. Click Yes to start… then you will have static.key file in the system.
Download CA	Download the generated ca.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Cert	Download the generated client.crt file here. Copy and Upload the key to the OpenVPN client Router.
Download Client Key	Download the generated client.key file here. Copy and Upload the key to the OpenVPN client Router.
Download Static Key	Download the generated static.key file here. Copy and Upload the key to the OpenVPN client Router while you prefer to establish OpenVPN connectivity by using Static Key.

3.5.5 IPSEC Settings

Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. By configure this configuration page, user allows IPsec tunnels to pass through the router.



IPSec Settings

Enable IPSec ☑ Enable

IPSec Status Disconnected

Exchange Mode Main ▾

Authentication Method PSK ▾

Pre-shared Key (max. length 25)

IPSec Cipher Suites AES128-SHA1-DH2 ▾ (algorithms for ike and esp proposal)

Local IP 192.168.10.1 (use 0.0.0.0 when wan is dynamic ip.)

Local Subnet 192.168.10.0/24 (Network/Netmask)

Remote Host 192.168.1.2 (use 0.0.0.0 if remote is dynamic ip.)

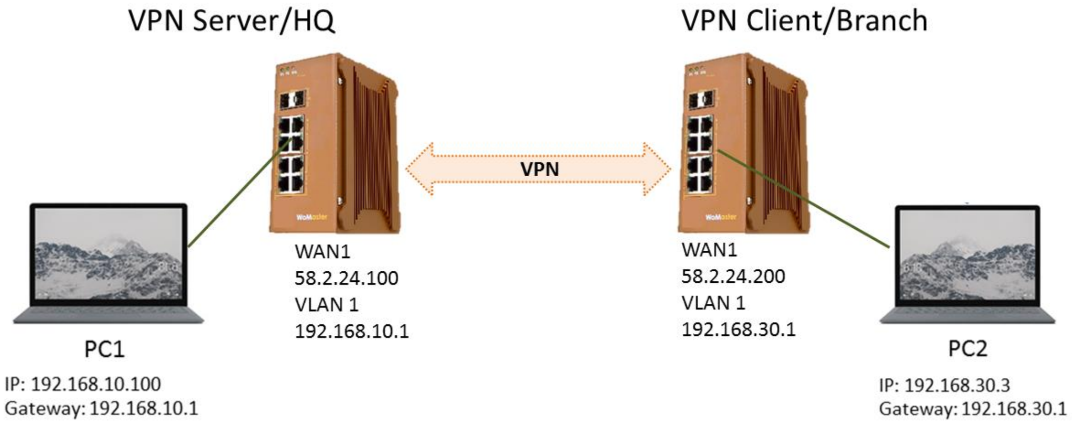
Remote Subnet 192.168.1.0/24 (Network/Netmask)

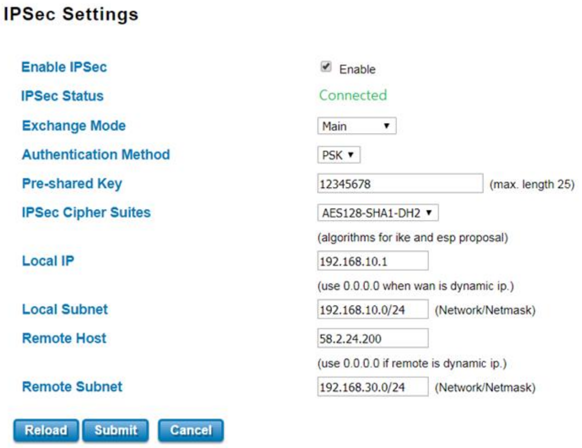
The description of the columns is as below:

TERMS	DESCRIPTION
Enable IPsec	Select Enable to activate the IPsec function
IPsec Status	Display the IPsec status, whether it is connected or disconnected When the VPN is connected, the IPsec status will display “Connected”. IPsec Status Connected
Exchange Mode	Main or Aggressive mode selection
Authentication Method	Default: PSK Optional: Pre Shared Key or Certificate
Pre-shared key	**Default: none** Type the Pre-shared key. The Pre-share key must be the same in both ends.
IPsec Cipher Suites	**Default: AES128-SHA1-DH2** Set algorithms for IKE and ESP proposal, choose AES128-SHA1-DH2, DES-SHA1-DH2, 3DES-SHA1-DH2 and AES256-SHA1-DH2. The cipher must be the same in both ends.
Local IP	IP Address of the local side of the tunnel. (Use 0.0.0.0 when WAN is dynamic IP.)
Local Subnet	Set IPSec local protected subnet and subnet mask, i.e. 192.168.1.0/24
Remote Host	**Default: 0.0.0.0** Set IPsec Remote Host, use the default setting if remote is dynamic IP
Remote Subnet	Set IPsec Remote Protected Subnet/Subnet Netmask

Click **Submit** to apply the configuration.

An Example of IPSec VPN:

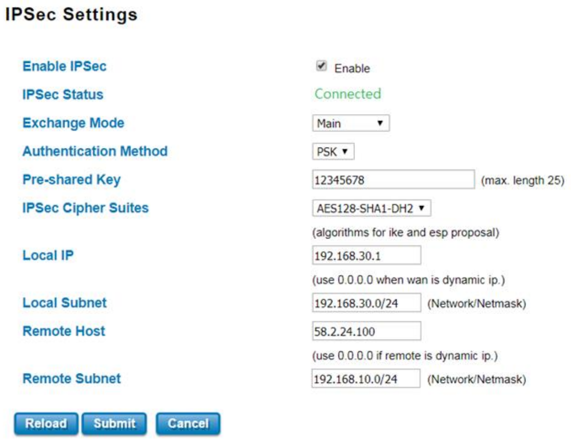




IPSec Settings

Enable IPSec	☑ Enable
IPSec Status	Connected
Exchange Mode	Main ▼
Authentication Method	PSK ▼
Pre-shared Key	12345678 (max. length 25)
IPSec Cipher Suites	AES128-SHA1-DH2 ▼ (algorithms for ike and esp proposal)
Local IP	192.168.10.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet	192.168.10.0/24 (Network/Netmask)
Remote Host	58.2.24.200 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet	192.168.30.0/24 (Network/Netmask)

Reload Submit Cancel



IPSec Settings

Enable IPSec	☑ Enable
IPSec Status	Connected
Exchange Mode	Main ▼
Authentication Method	PSK ▼
Pre-shared Key	12345678 (max. length 25)
IPSec Cipher Suites	AES128-SHA1-DH2 ▼ (algorithms for ike and esp proposal)
Local IP	192.168.30.1 (use 0.0.0.0 when wan is dynamic ip.)
Local Subnet	192.168.30.0/24 (Network/Netmask)
Remote Host	58.2.24.100 (use 0.0.0.0 if remote is dynamic ip.)
Remote Subnet	192.168.10.0/24 (Network/Netmask)

Reload Submit Cancel

The reference topology above is how the branch office can get the access to the headquarter. The two laptops are connected to the secure router switch through the Ethernet cable.

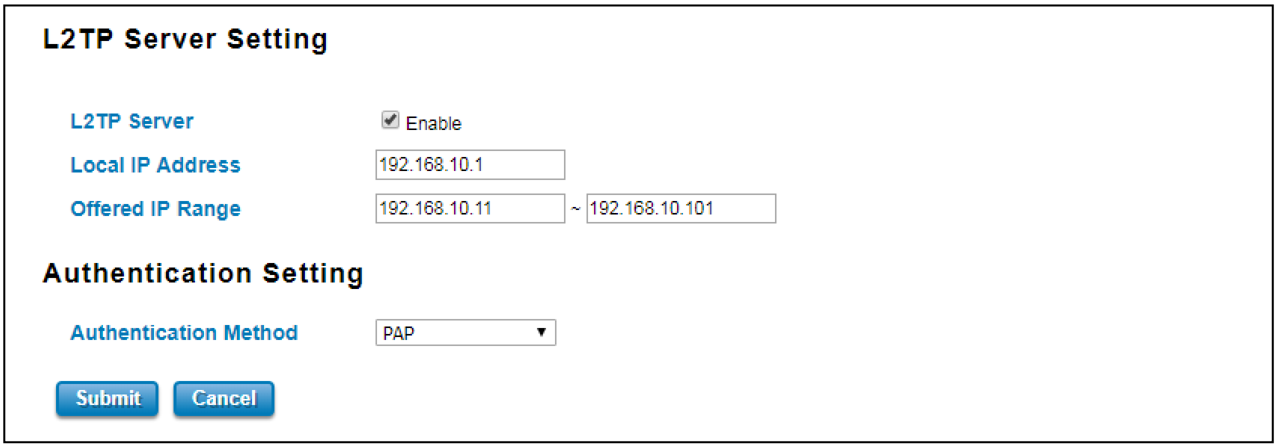
Enable the IPSec, type the same pre-share key and select the same cipher for both ends.

Configure the IP address for both ends. The Router at the branch office normally acts as the VPN Client role (not really client mode in IPSec), the Router at head quarter normally acts as the VPN Server role. The HQ normally has public IP, that's the Remote IP of the router in branch office. The local subnet in HQ is the remote subnet of the router in branch office. If you have public IP in branch, it's better to use public IP address for the WAN interface. If you just have dynamic IP address for branch office, then use 0.0.0.0 as local IP.

To check the connection status, you can use Ping tool in Router's Web GUI to check the WAN connection. You must ping remote WAN IP address successfully first. Then you can try ping from PC2 to its connected interface, WAN IP of two routers and then remote PC1. This is also the typical debugging rule to check WAN and VPN connectivity.

3.5.6 L2TP SETTING

L2TP is a popular choice for remote roaming users for VPN applications since an L2TP client is built in to the Microsoft Windows operating system. In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy. Below is the L2TP Server Setting interface.



L2TP Server Setting

L2TP Server ☑ Enable

Local IP Address 192.168.10.1

Offered IP Range 192.168.10.11 ~ 192.168.10.101

Authentication Setting

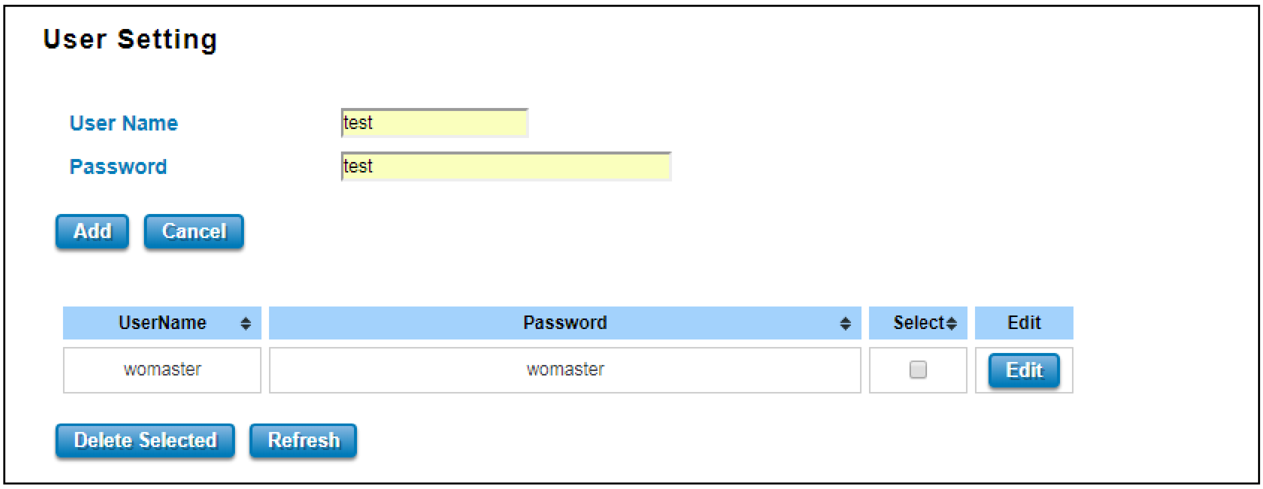
Authentication Method PAP ▼

The description of the column is as below:

TERMS	DESCRIPTION
L2TP Server	Check the box to enable the function.
Local IP Address	The IP Address of the L2TP Server.
Offered IP Range	Offered IP Address range for the L2TP Clients (Maximum 10 clients)
Authentication Method	This section belongs to User Setting section. User can choose authentication using the password authentication protocol (PAP) and challenge handshake authentication protocol (CHAP).

Click the **Submit** button to apply the configuration.

Below is the User Setting for the L2TP Authentication connection.



User Setting

User Name test

Password test

UserName	Password	Select	Edit
womaster	womaster	☐	Edit

The description of the column is as below:

TERMS	DESCRIPTION
User Name	Username for L2TP connection
Password	Password for L2TP connection
Select	Select the list on the table, so user can press **Edit** or **Delete Selected** to delete.

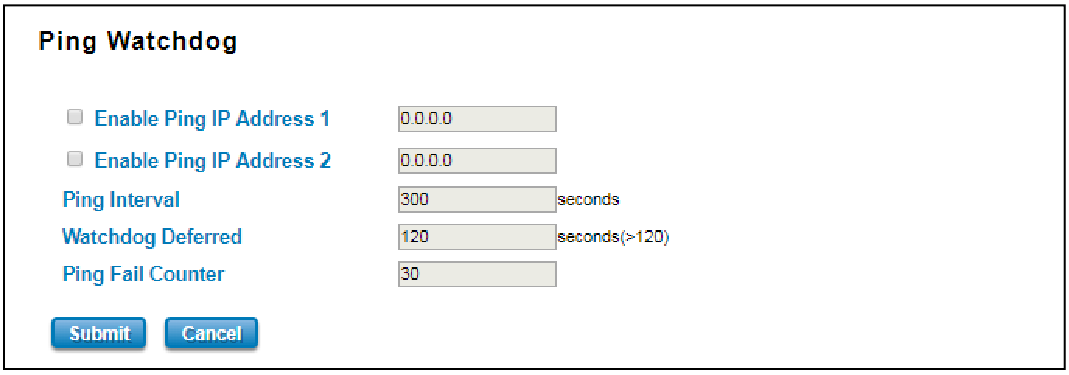
Click the **Refresh** button to refresh the list.

3.6 Warning

ISTRON' router provides several types of Warning feature for remote monitoring of end devices status or network changes.

3.6.1 Ping Watchdog

Ping Watchdog is a feature that helps ISTRON' router to allow user continuously ping a specific remote host for connection status using a user-defined IP address (or an Internet gateway). In this section, ISTRON provides two target IP Addresses, in order if the other IP Address cannot be reached, so there is another backup IP address. There are two conditions in this Ping Watchdog section, the first one is when the device continuously ping the target IP and in the end, it can reach one of the target IPs the device would not reboot. But if both targets IPs cannot be reached, the device will start counting the Ping Fail Counter time till it can be reached. If it is unable to ping the target IP address, this device will automatically reboot. After User finishes configuring the settings, click on **Submit** to apply User configuration.



Ping Watchdog

□ Enable Ping IP Address 1	0.0.0.0	
□ Enable Ping IP Address 2	0.0.0.0	
Ping Interval	300	seconds
Watchdog Deferred	120	seconds(>120)
Ping Fail Counter	30	

The description of the columns is as below:

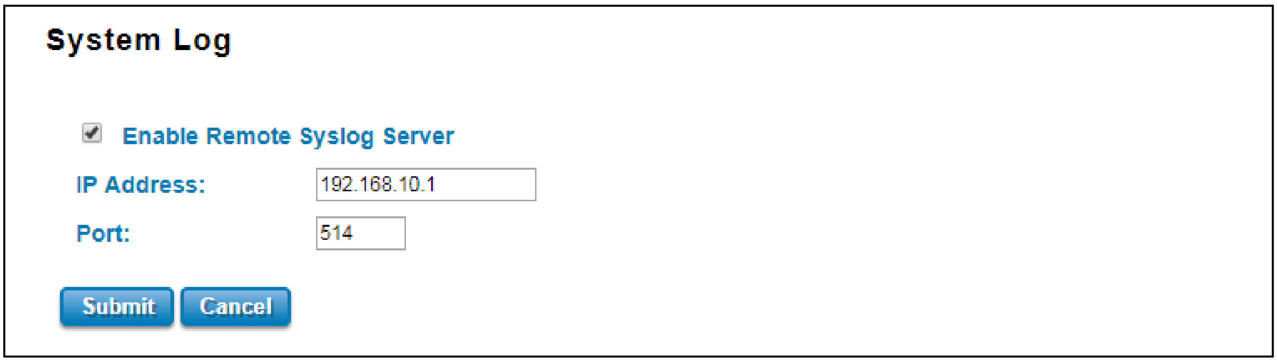
TERMS	DESCRIPTION
Enable Ping IP Address 1	Clicks enable to activate the feature. Set the first IP Address to check if the device is alive or not
Enable Ping IP Address 2	Clicks enable to activate the feature. Set the second IP Address to check if the device is alive or not
Ping Interval	**Default: 300 (seconds)** Set the interval timer to Ping the remote device. Every 300 seconds the device will try to ping the target IP.
Watchdog Deferred	**Default: 120 (seconds) >120** The device needs time to boot, the startup delay use to buffer to prevent the device continue to reboot itself.
Ping Fail Counter	**Default: 30** When the remaining Ping Fail Counter reach to 0 or reach the failure count, the device will reboot.

Click **Submit** to apply the configuration.

3.6.2 SYSLOG Settings

System Log is useful to provide system administrator locally or remotely monitor router events history.

Once User finishes configuring the settings, click on **Submit** to apply User configuration. User can monitor the system



System Log

☑ Enable Remote Syslog Server

IP Address: 192.168.10.1

Port: 514

logs in [Diagnostics] / [Event Log] page

The condition or term described as following table.

TERMS	DESCRIPTION
Enable Remote Syslog Server	Select Enable to enable system log
IP Address	Specify the IP address of the server.
Port	**Default: 514** Specify the port number of the server

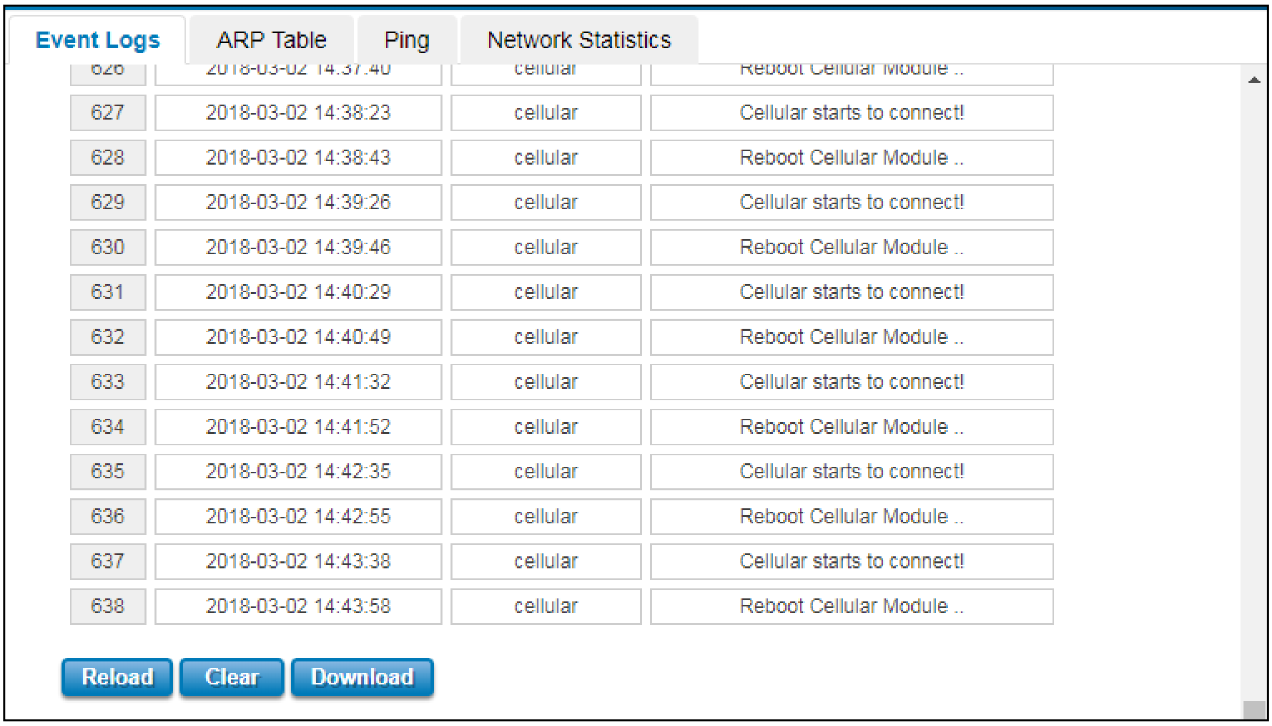
After finish with the configuration, clicks **Submit** to activate the function.

3.7 Diagnostics

ISTRON Router provides several types of features for User to monitor the status of the router or diagnostic for User to check the problem when encountering problems related to the router.

3.7.1 Event Logs

When remote System Log server mode is activated, the router will record occurred events in local log table. This page shows this log table. The entry includes the index, occurred data, time and content of the events.



626	2018-03-02 14:37:40	cellular	Reboot Cellular Module ..
627	2018-03-02 14:38:23	cellular	Cellular starts to connect!
628	2018-03-02 14:38:43	cellular	Reboot Cellular Module ..
629	2018-03-02 14:39:26	cellular	Cellular starts to connect!
630	2018-03-02 14:39:46	cellular	Reboot Cellular Module ..
631	2018-03-02 14:40:29	cellular	Cellular starts to connect!
632	2018-03-02 14:40:49	cellular	Reboot Cellular Module ..
633	2018-03-02 14:41:32	cellular	Cellular starts to connect!
634	2018-03-02 14:41:52	cellular	Reboot Cellular Module ..
635	2018-03-02 14:42:35	cellular	Cellular starts to connect!
636	2018-03-02 14:42:55	cellular	Reboot Cellular Module ..
637	2018-03-02 14:43:38	cellular	Cellular starts to connect!
638	2018-03-02 14:43:58	cellular	Reboot Cellular Module ..

TERMS	DESCRIPTION
#	Event index assigned to identify the event sequence.
Time	The time is updated based on how the current date and time is set in the Basic Setting page.
Source	Show the log's source.
Message	Show the record status.

Click **Reload** to refresh the table. Click **Clear** to remove the entire event logs list. User may download the event logs file by click **Download**.

3.7.2 ARP Table

Basically, ISTRON device is supported with two types of ARP which is the standard ARP and ARP with 802.2 LLC Type 2. Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address that is recognized in the local network. A table, usually called the ARP cache, is used to maintain a correlation between each MAC address and its corresponding IP address. ARP provides the protocol rules for making this correlation and providing address conversion in both directions. The other ARP feature is ARP with 802.2 LLC Type 2 is the new level of ARP where the device will response the request of 802.2 snap ARP on the Ethernet port and not support sending the request of 802.2 snap ARP. Below is the Data format.

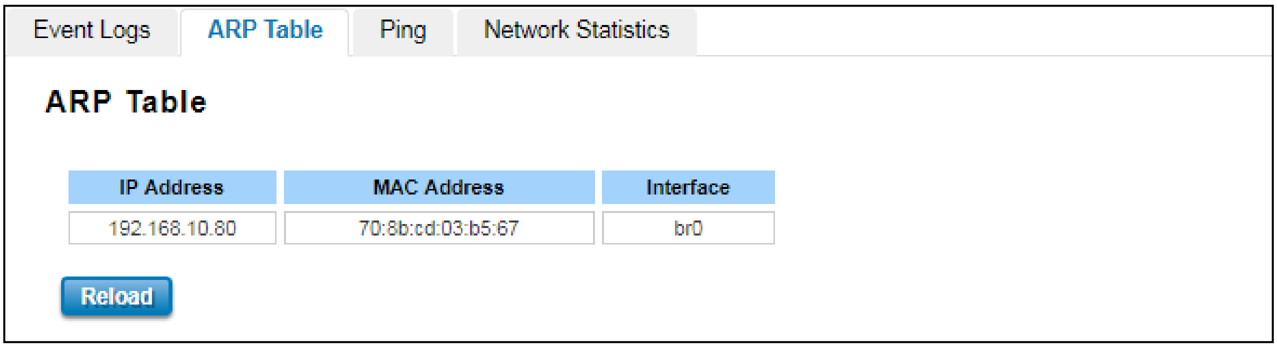
Data Format

Protocol Header:

802.3 + 802.2 LLC + 802.2 snap

|- (DS + SA + Len) -|- DSAP + SSAP + CTRL -|- Org + type

This page shows the routers active ARP table. An ARP table contains recently cached MAC addresses of every immediate device that was communicating with the router.



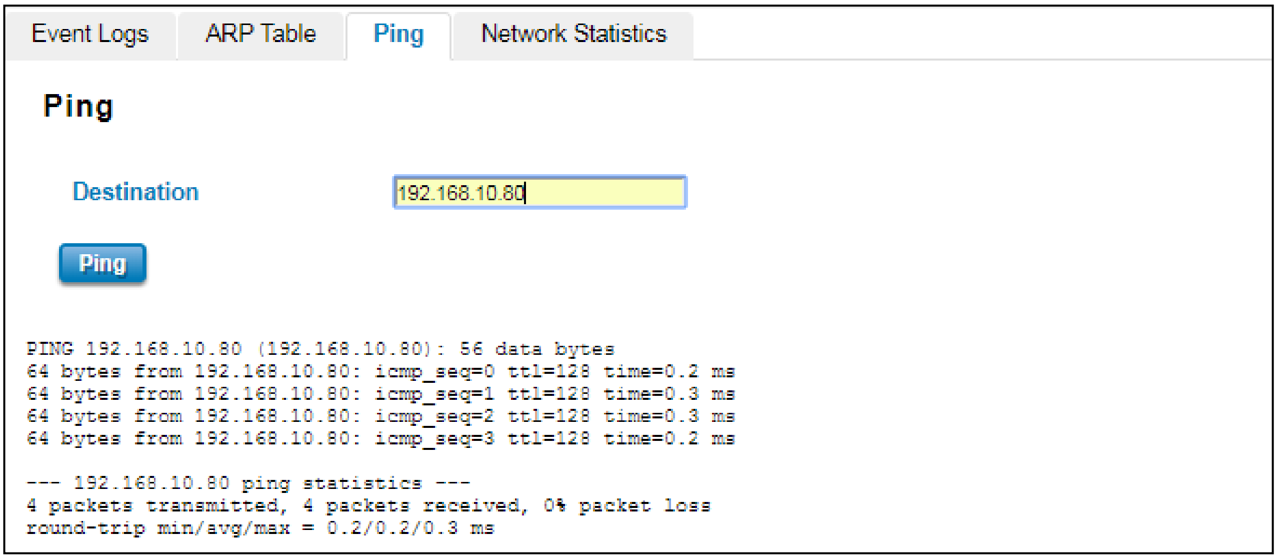
ARP Table

IP Address	MAC Address	Interface
192.168.10.80	70:8b:cd:03:b5:67	br0

Click on **Reload** to change the value.

3.7.3 Ping

ISTRON’ provides **Ping** utility in the management interface, the function is to give users a simple but powerful tool for troubleshooting network problems and check that the remote device is still alive or not. Type **Destination** IP address of the target device and click on **Ping** to start the ping.



Ping

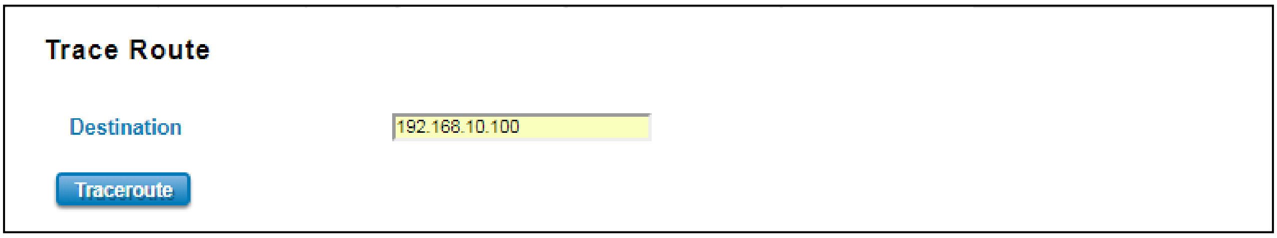
Destination: 192.168.10.80

```
PING 192.168.10.80 (192.168.10.80): 56 data bytes
64 bytes from 192.168.10.80: icmp_seq=0 ttl=128 time=0.2 ms
64 bytes from 192.168.10.80: icmp_seq=1 ttl=128 time=0.3 ms
64 bytes from 192.168.10.80: icmp_seq=2 ttl=128 time=0.3 ms
64 bytes from 192.168.10.80: icmp_seq=3 ttl=128 time=0.2 ms

--- 192.168.10.80 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.3 ms
```

3.7.4 Traceroute

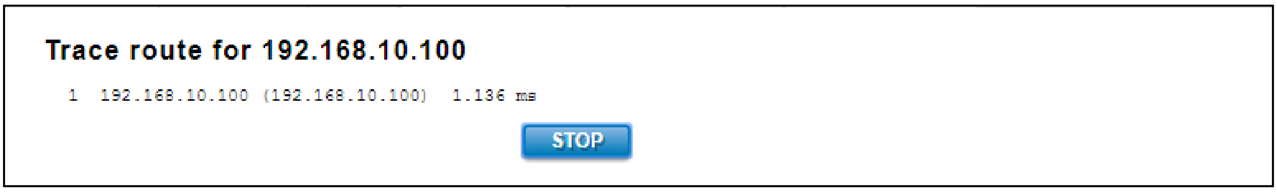
Traceroute is a diagnostics tool for displaying the route (path) and measuring transit delays of packets across an Internet IP network. Log containing route information will be shown after few seconds. Enter the destination IP Address then click traceroute to start the process.



Trace Route

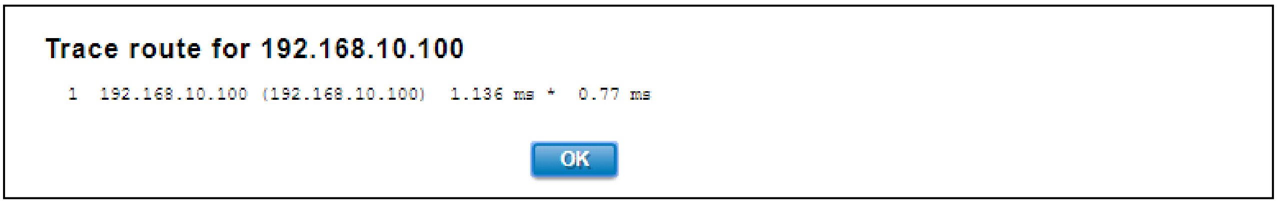
Destination: 192.168.10.100

It will start search the route and measuring the transit delays of the packet.



Trace route for 192.168.10.100

```
1  192.168.10.100 (192.168.10.100)  1.136 ms
```

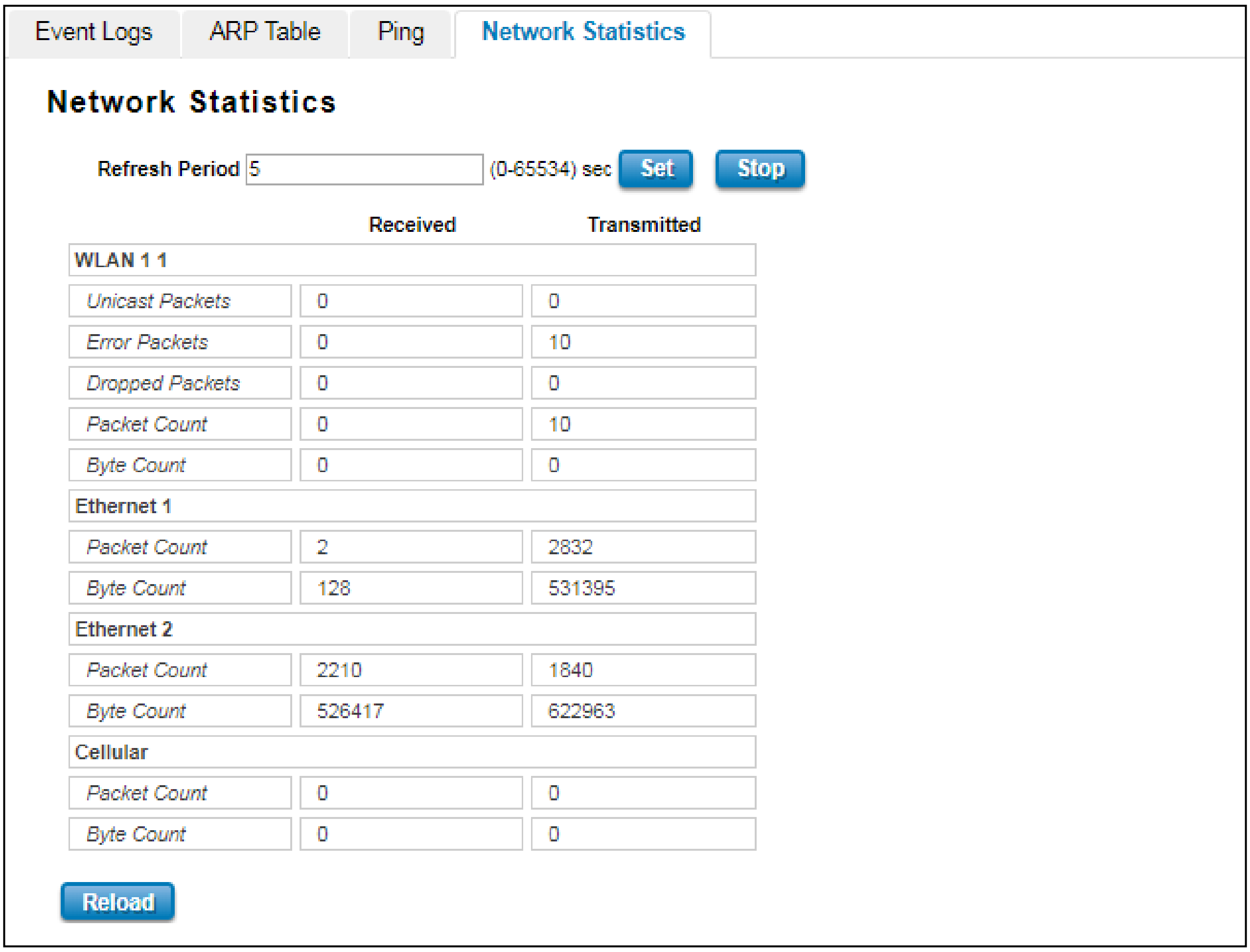


Trace route for 192.168.10.100

```
1  192.168.10.100 (192.168.10.100)  1.136 ms *  0.77 ms
```

3.7.5 Network Statistics

This section shows about the packet data that transmitted or received regarding the Ethernet and Cellular activity. The Cellular packets include Wi-Fi and 2G/3G/LTE transmission.



Network Statistics

Refresh Period 5 (0-65534) sec

	Received	Transmitted
WLAN 1 1		
Unicast Packets	0	0
Error Packets	0	10
Dropped Packets	0	0
Packet Count	0	10
Byte Count	0	0
Ethernet 1		
Packet Count	2	2832
Byte Count	128	531395
Ethernet 2		
Packet Count	2210	1840
Byte Count	526417	622963
Cellular		
Packet Count	0	0
Byte Count	0	0

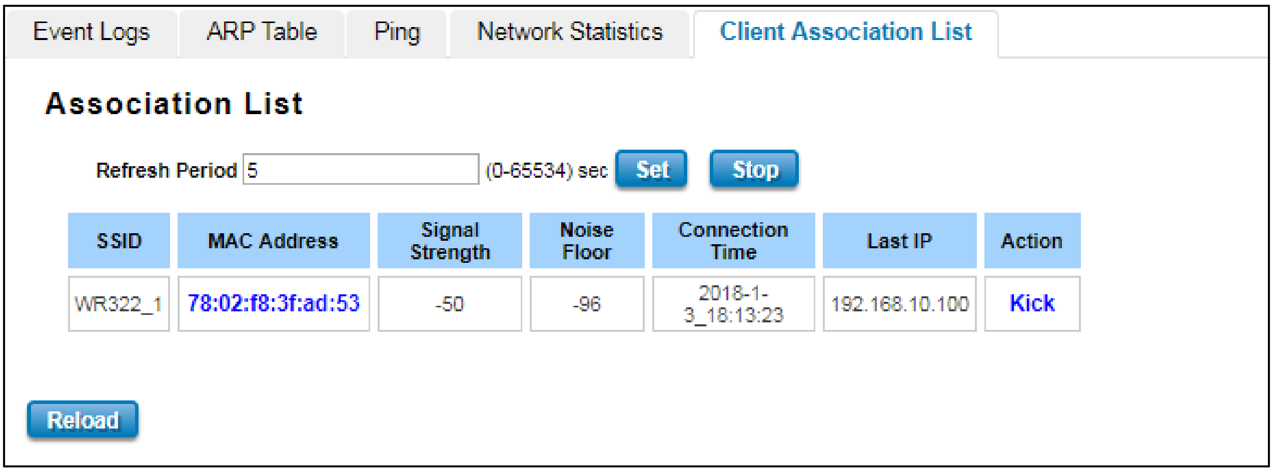
Click on **Reload** to refresh the table.

The description of the columns is as below:

TERMS	DESCRIPTION
Poll Interval	**Default: 5** To set the Poll Interval time setting with range from 0 to 65534. (second)
Set	To set new Interval time. Stop the old Poll Interval first before set the new interval.
Stop	To stop Polling Interval, this action can be executed when user wants to change the poll interval time.

3.7.6 Client Association List

This Client Association List displays the current wireless connection status when there is a client that connected to the AP. It shows the SSID, MAC Address, Signal Strength, Noise Floor, Connection Time, Last IP and Action. For the security concern, in this page user can do the security action, such as **Kick** the unexpected user from the wireless networks. This page also provides the refresh function to refresh the list automatically, where user may set the refresh period for refresh the list. Click **Set** to apply the setting, click **Stop** to stop the refresh function.



Association List

Refresh Period 5 (0-65534) sec

SSID	MAC Address	Signal Strength	Noise Floor	Connection Time	Last IP	Action
WR322_1	78:02:f8:3f:ad:53	-50	-96	2018-1-3_18:13:23	192.168.10.100	Kick

Click **Reload** to refresh the list.

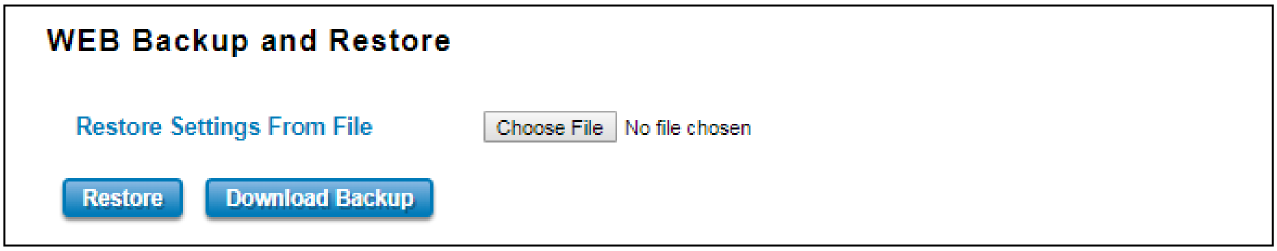
The description of the columns is as below:

TERMS	DESCRIPTION
SSID	Display the primary name of the SSID that available on the network.
MAC Address	Display the MAC Address that connected to the AP.
Signal Strength	Display the connection signal strength.
Noise Floor	Display the background noise level.
Connection Time	Display the time when the client connected to the AP.
Last IP	Show the IP Address of the wireless client.
Action	In this section user may do an action by **kick** the unexpected wireless client.

3.9 Backup and Restore

User can use ISTRON's Backup and Restore configuration to save and load configuration through the router.

Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the router. This mode is only provided by Web UI while CLI is not supported. Also, this feature provides the Download Backup button in order to download the backup configuration from the router.



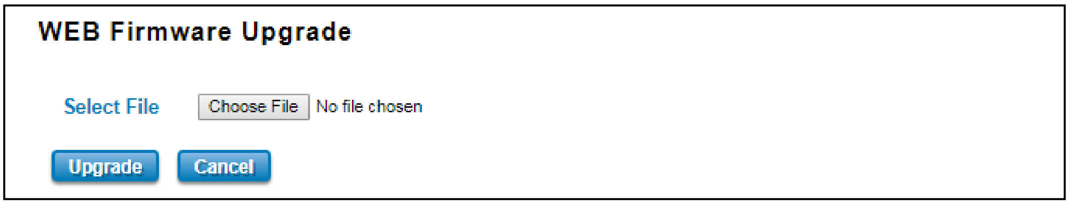
WEB Backup and Restore

Restore Settings From File

3.10 Firmware Upgrade

ISTRON provides the latest firmware online at www.ISTRON.eu. The new firmware may include new features, bug fixes or other software changes. ISTRON also provides the release notes for the update as well. For technical viewpoint, ISTRON suggests user uses the latest firmware before installing the router to the customer site.

Note that the system will be automatically rebooted after User finished upgrading the new firmware. Please remind the attached network users before User performs this function.



WEB Firmware Upgrade

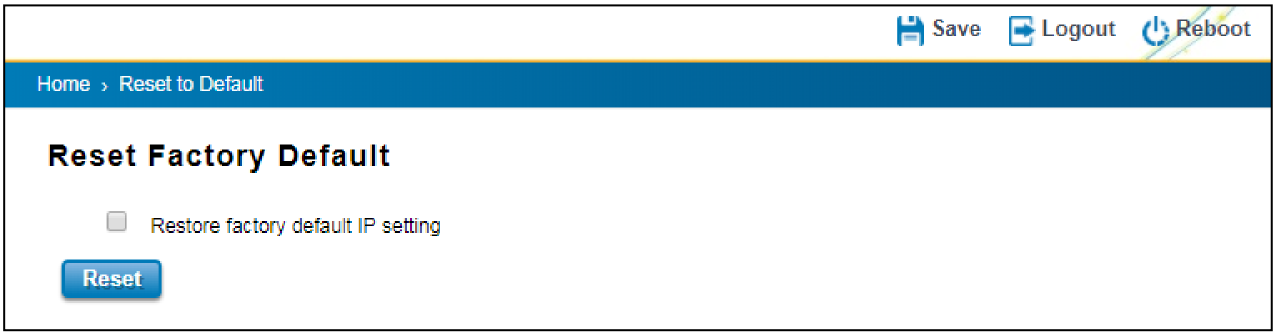
Select File Choose File No file chosen

Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.

3.11 Reset to Defaults

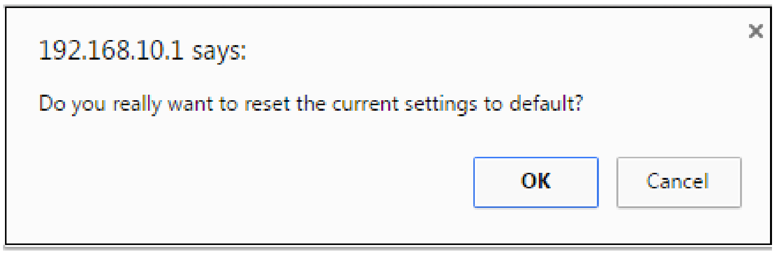
This function provides users with a quick way of restoring the ISTRON router’s configuration to factory defaults. By check the Restore Factory default IP setting, it means the IP of the device will directly change to the default IP (192.168.10.1).

Pop-up message screen to show User that have done the command. Click on **OK** to close the screen and reboot the device.



Reset Factory Default

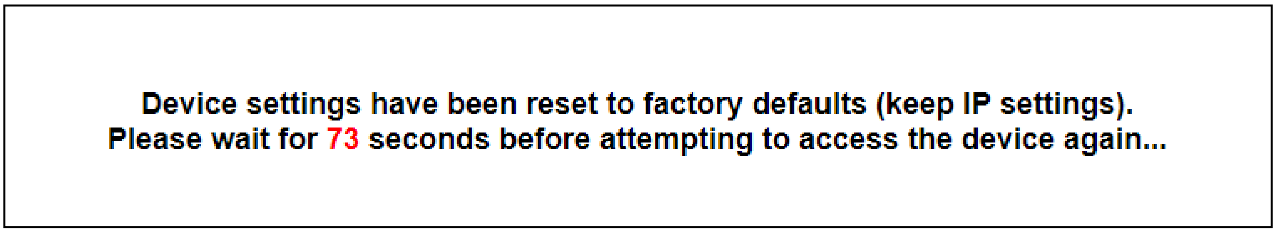
□ Restore factory default IP setting



192.168.10.1 says:

Do you really want to reset the current settings to default?

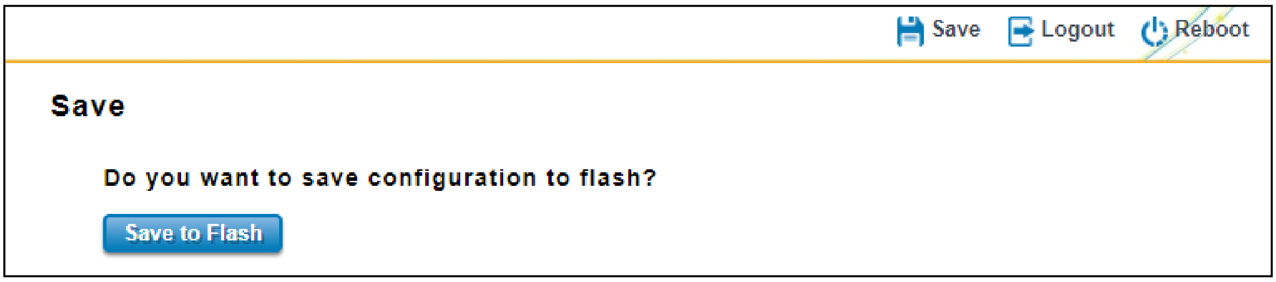
Below is the interface for resetting the device with keep the IP Settings.



Device settings have been reset to factory defaults (keep IP settings).
Please wait for 73 seconds before attempting to access the device again...

3.12 Save

Save option allows user to save any configuration. Powering off the router without clicking on **Save** will cause loss of new settings. After selecting **Save**, click on **Yes** to save new configuration.



Save

Do you want to save configuration to flash?

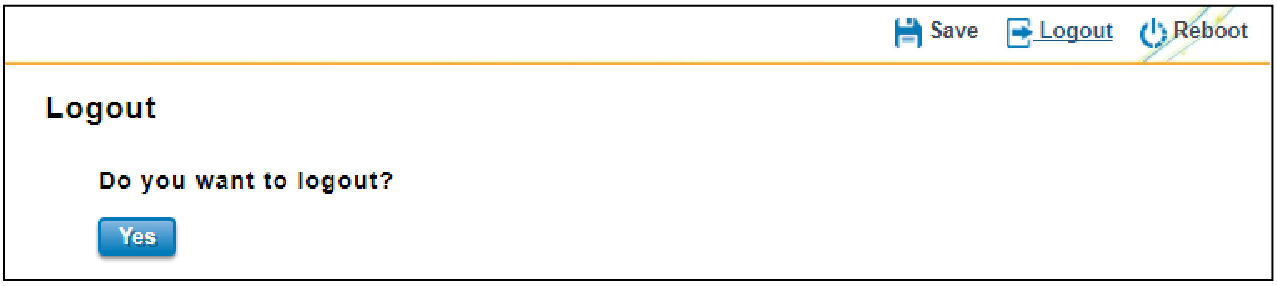
FCC Warning
This device complies with part 15 of the FCC rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any inte rference received, including interference that may cause undesired operation.

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interferenceto radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
•Increase the separation between the equipment and receiver.
•Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
•Consult the dealer or an experienced radio/TV technician for help.
Radiation Exposure Statement
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

3.13 Logout

There are 2 logout methods. If user doesn't input any command within 30 seconds, the web connection will be logged out. The Logout command allows user to manually logout the web connection. Click on **Yes** to logout.



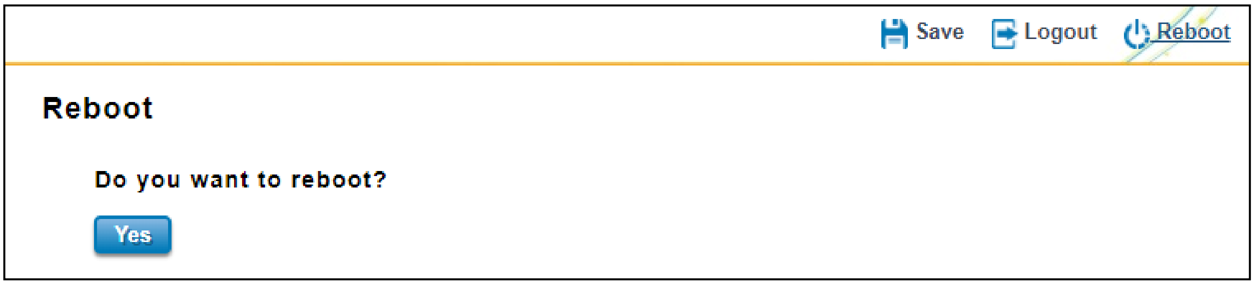
Logout

Do you want to logout?

3.14 Reboot

System Reboot allows user to reboot the device. Some of the feature changes require user to reboot the system. Click on **Reboot** to reboot device.

Reboot main screen, to do confirmation request. Click **Yes**, then the router will reboot immediately.



Reboot

Do you want to reboot?

Remember to click on Save button to save configuration settings. Otherwise, the settings user made will be gone when the router is powered off.