RICON MOBİLE

S9922M Series LTE Router

USER MANUAL

RICON MOBILE

S9922M Series LTE Router

© Ricon Mobile Inc.
Ahi Evran Cad. No:21, Polaris
Plaza Kat:8/40
Maslak / İstanbul / Türkiye
Website: http://www.riconmobile.com
Phone: (+90) 212 346 26 00

@Ricon Mobile Inc.(HQ)
460 Brant Street Unit 300 Burlington,
Ontario Canada
+1 (905) 336 24 50

@Ricon Mobile Inc. FZE
Ras Al Khaimah U.A.E.
Phone: (+97) 172 041 010 (U.A.E)

@Ricon Mobile Inc. Ltd.
F5-Building 3, FengMenao Industrial Park,
Bantian Streets, Longgang District
Shenzhen 518129, China

Trademarks and Permissions

RICON® is the trademarks and logos of Ricon Mobile Inc. Other trademarks and logos mentioned in this manual belong to other organizations related. Ricon Mobile Inc. does not own the rights of other trademarks and logos.

Caution

Due to product updates or functional upgrading, we may renew the content of this file.
All statement, information, suggestions etc. in this file do not compose any form of guarantee and we Ricon Mobile Inc. reserves the right of final explanation.

ABOUT THE DOCUMENT

PURPOSE

S9922M Router is designed and manufactured by Ricon Mobile Inc., it based on 3G/LTE cellular network technology with industrial class quality. With its embedded cellular module, it widely used in multiple case like ATM connection, remote office security connection, data collection. etc. This document introduced how to use S9922M and its powerful features.

RELATED VERSİONS

The following table lists the product versions related to this document.

Model	Version
S9922M:	V30
Firmware Version starting from:	S9922M_APP_V7.0.2_T1_ricon_1710161204
Date of issue:	24.10.2019

CONTENTS

1. PRODUCT

1.1 OVERVIEW

RICON S9922M Series Router by Ricon Mobile Inc. Industrial grade quality, designed and manufactured in accordance with 3G/LTE cellular network technology. With embedded cellular module, ATM connection, remote office security connection, data collection etc. It is widely used in many cases such as. Ricon Mobile S9922M series router provides maximum service to customers while Zero touch-SMS installation minimizes the need for field service with easy and automatic product installation service. The unique feature of the S9922M Series Router is that it is online and redundant over the network between WAN, WLAN, 3G/LTE network. This feature allows the S9922M series to provide maximum network availability and reduce the likelihood of network failure to prevent losses due to network failures. S9922M series routers are web-based and easily routed through CLI. In addition, the Ricon Management System (RMS) successfully accomplishes the goal of reducing the maintenance costs with the ability to access all the Ricon products in the network and to access instant and statistical data on the web environment and manage them 100%.

1.2 FUNCTIONS & FEATURES

- VPN support, GRE over IPSec, IPsec over PPTP/L2TP
- VPN Passthrough
- WAN port support PPPoE, static IP, DHCP client (Auto Link Backup)
- LCP/ICMP/flow/heartbeat check, ensure network usability
- SNMP network management, NTP support (Free MIBs)
- Local & remote firmware update
- Local & remote log check
- Supports DNS proxy and Dynamic DNS (DDNS)
- Supports timing operations
- Supports LED status indication
- VRRP (hardware resiliency)
- IPFix/Netflow Features (Traffic Monitor & Export) (Available with RMS)
- SMS Send/Receive
- Configuration vis SMS Commands with status replies
- Traffic Filtering (Domain, IP and Mac Address)
- Supports NAT/Routed traffic flow
- Tacacs+ compatible
- DHCP Relay (With Backup Server)
- DHCP Relay Option 43/60 Support for Wireless Management

2

2. PRODUCT STRUCTURE

2.1 APPEARANCE

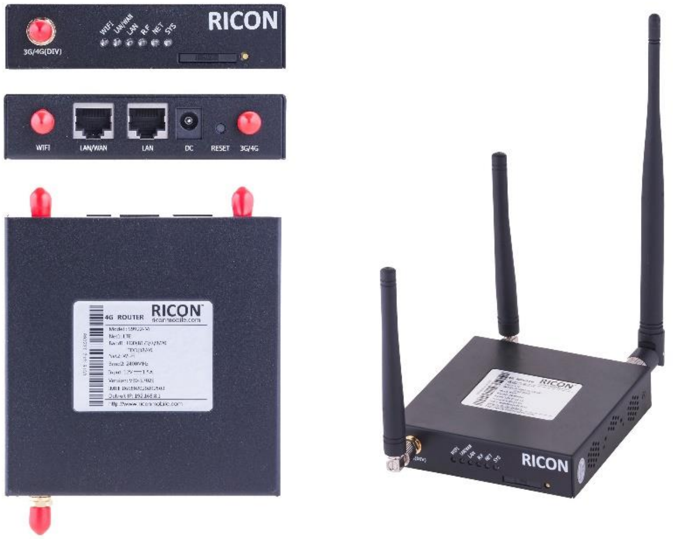


Figure.1-S9922M Router appearance

ACCESSORIES

Accessories name	Number	Note
S9922M Router	1 pcs	
3G/LTE antenna	1 pcs	According to GSM Technology (3G/LTE)
Wi-Fi antenna	1 pcs	Optional
RJ45 cable	1 pcs	
Mounting Kit	1 pair	Optional
Certificate and warranty card	1 pcs	
+12V power adapter	1 pcs	

3

3. GENERAL CONFIGURATION

3.1 PREPARATION

3.1.1 SIM CARD INSTALLATİON

Prepare the SIM card which is in standard size, not the scissored mini card. Put the SIM card into SIM card apparatus and push the SIM card to the SIM slot. Then attach the antennas.

Your router comes with two detachable antennas. These one external antenna is required for proper 4G LTE service.

Only use power adapters compatible with the router and provided by a designated manufacturer. Use of an incompatible power adapter or one from an unknown manufacturer may cause the router to malfunction, fail, or could even cause a fire. Such use voids all warranties, whether expressed or implied, on the product

3.1.2 LOGGING IN TO THE WEB MANAGEMENT PAGE

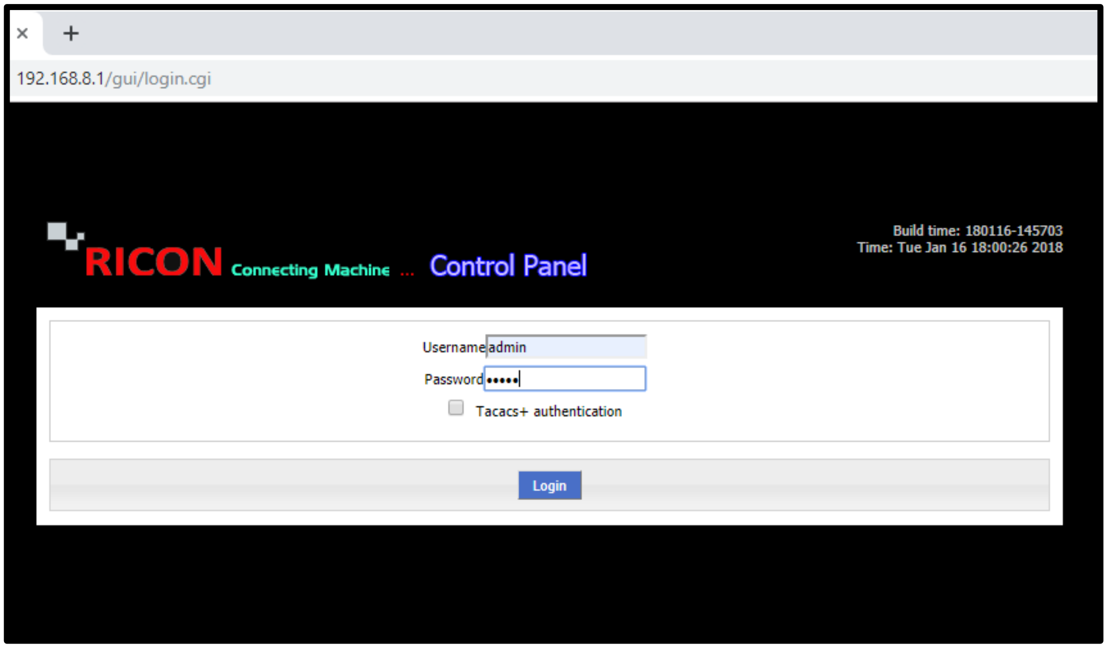
The web-based configuration utility can be used for initial device installation, parameter configuration, and function management through the browser.

Use ethernet port directly connected to S9922M router and computer, or transferred by a switch. This method will temporarily interrupt the communication between the computer under configuration and LAN, and the specific parameter configuration is shown as below:

IP address: 192.168.8.* (*indicates any integral between 2 to 254)

Subnet mask: 255.255.255.0

Default gateway: 192.168.8.1



192.168.8.1/gui/login.cgi

Build time: 180116-145703
Time: Tue Jan 16 18:00:26 2018

Username admin

Password •••••

□ Tacacs+ authentication

Figure.2- Website preparation

Launch the browser and enter http://192.168.8.1 in the address bar. The login page appears.

Input the username and password then click **Login**.

- *The default user name is admin.*
- *The default password is admin.*

<u>NOTE:</u>

- *The device's default IP address is 192.168.1.1 and subnet mask is 255.255.255.0*
- *It is recommended that you use the automatically obtained IP addresses for the computer and domain name system (DNS) server. If you manually configure the computer IP address, you must set the DNS server IP address to the device IP address. Otherwise, you will fail to log in to the web management page.*

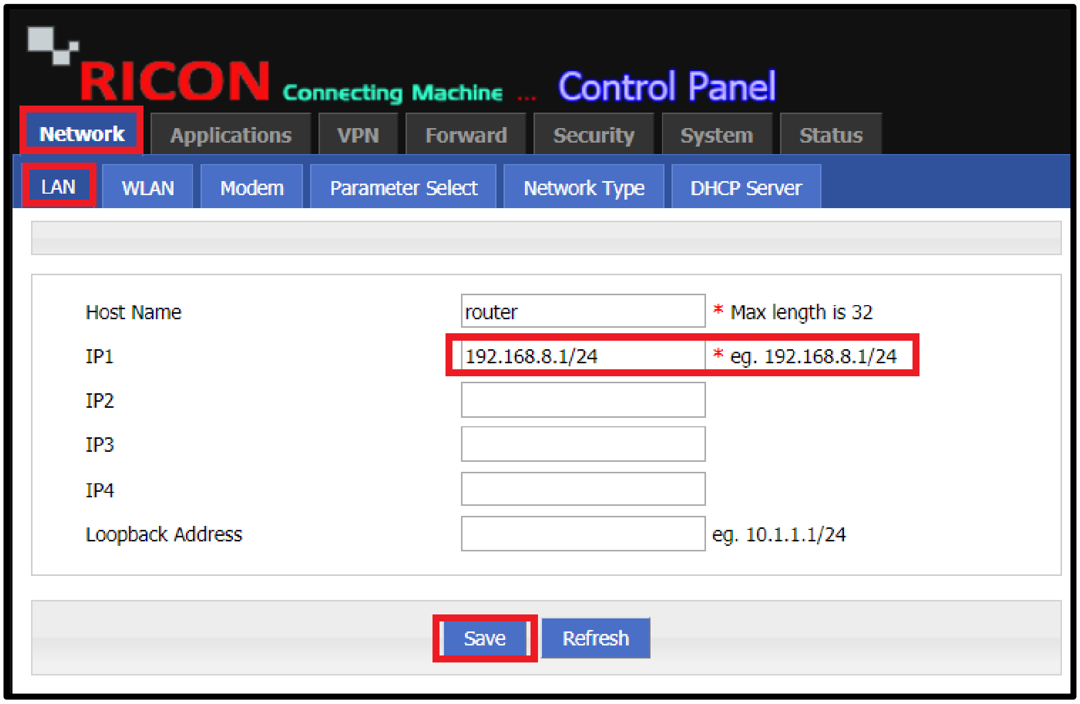
3 NETWORK CONFIGURATION

3.1 LAN SETTING

LAN settings are used to manage local area network units which are connected to a S9922M Router, make them reach to the desired network or internet regarding the network topology. Follow the steps below to change the existing LAN IP block or add another IP block. Enter the IP block you have specified and click **Save**.

Host Name is your router's name and IP1 is router's LAN IP address.

NETWORK>LAN



Host Name	router	* Max length is 32
IP1	192.168.8.1/24	* eg. 192.168.8.1/24
IP2		
IP3		
IP4		
Loopback Address		eg. 10.1.1.1/24

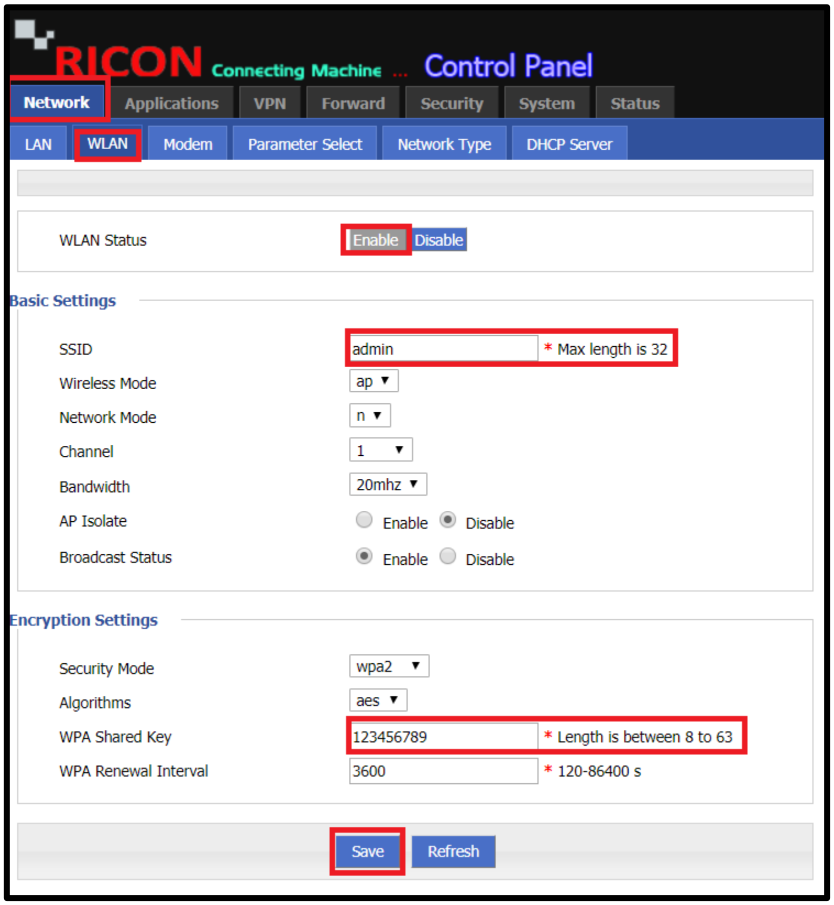
Figure.3- Network>LAN

3.2 Wi-Fi SETTING

For a wireless connection, your router and computer, smartphone or tablet will need to have the same Wi-Fi network name and security settings. Ricon recommends that you use wireless security.
The default Wi-Fi network name and password appear on the Figure 4. Follow the steps below to make Wi-Fi connection.

- ✓ **SSID;** Set SSID is your Wi-Fi connection name.
- ✓ **Network mode;** n, g, b.
  -N: Specifications providing for up to 300 Mbps of network bandwidth. N also offers somewhat better range over earlier Wi-Fi standards due to its increased signal intensity, and it is backward-compatible with B/G gear.
  -G: Support bandwidth up to 54 Mbps, and it uses the 2.4GHz frequency for greater range.
  -B: Supports bandwidth up to 11 Mbps and Uses radio signal frequency 2.4GHz.
- ✓ **Channel;** There are 11 different channel selection options.
- ✓ **Bandwidth;** 20mhz or 40mhz can be selected according to the specifications of the devices you want to use in wireless network.
- ✓ **AP Isolate;** Users connecting to your network can not access each other.
- ✓ **Broadcast Status;** If you want the SSID to be hidden, select disable.
- ✓ **Security Mode and Algorithms;** Disable, WPA, WPA2, TKIP, AES.
  -Disable; Wireless network is connected to the network without password.
  -WPA improved security, but is now also considered vulnerable to intrusion. WPA2, while not perfect, is currently the most secure choice. Temporal Key Integrity Protocol (TKIP) and Advanced Encryption Standard (AES) are the two different types of encryption you'll see used on networks secured with WPA2.
- ✓ **WPA Shared Key;** Set is your Wi-Fi connection password.
- ✓ **WPA Renewal Interval;** The number of seconds the wireless network needs to be refreshed is entered here.
- ✓ Single click **Save** icon to finish.

NETWORK>WLAN



WLAN Status	Enable Disable

Basic Settings

SSID	admin * Max length is 32
Wireless Mode	ap ▾
Network Mode	n ▾
Channel	1 ▾
Bandwidth	20mhz ▾
AP Isolate	○ Enable ● Disable
Broadcast Status	● Enable ○ Disable

Encryption Settings

Security Mode	wpa2 ▾
Algorithms	aes ▾
WPA Shared Key	123456789 * Length is between 8 to 63
WPA Renewal Interval	3600 * 120-86400 s

Figure.4- Network>Wlan

3.3 WAN SETTING

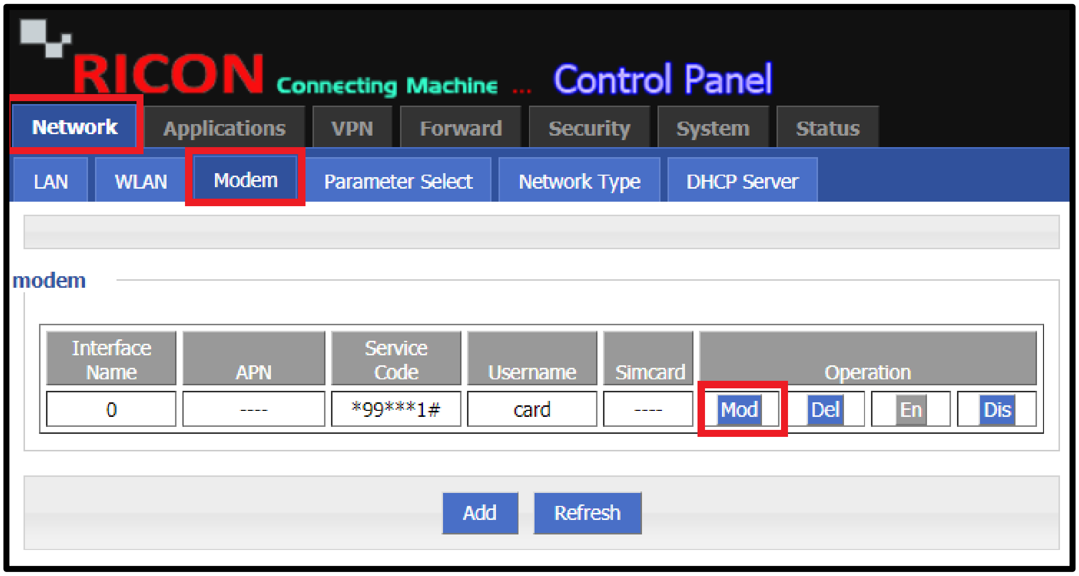
An APN profile is a group of dial-up parameters related to an access point name (APN). You can select an APN profile for the router to access the Internet via SIM card.

S9922M Router core function is connecting to a desired network (corporate or internet) by cellular connection. Usually 3G/LTE network bandwidth is (Depending on the operators' infrastructure) between 1～300Mbps

Single click **"Mod"** to access modem parameter settings section. After that you can set APN profile of your SIM card.

- ✓ Set **APN**, **Username** and **Password** (If you have PIN of SIM card you can set PIN disable)
- ✓ Set **Network Type** to **Edge**, **WCDMA**, **TDD-LTE, FDD-LTE** or **Auto**
- ✓ Click the **Save** icon to finish.

NETWORK>MODEM>MOD



Interface Name	APN	Service Code	Username	Simcard	Operation
0	----	*99***1#	card	----	Mod Del En Dis

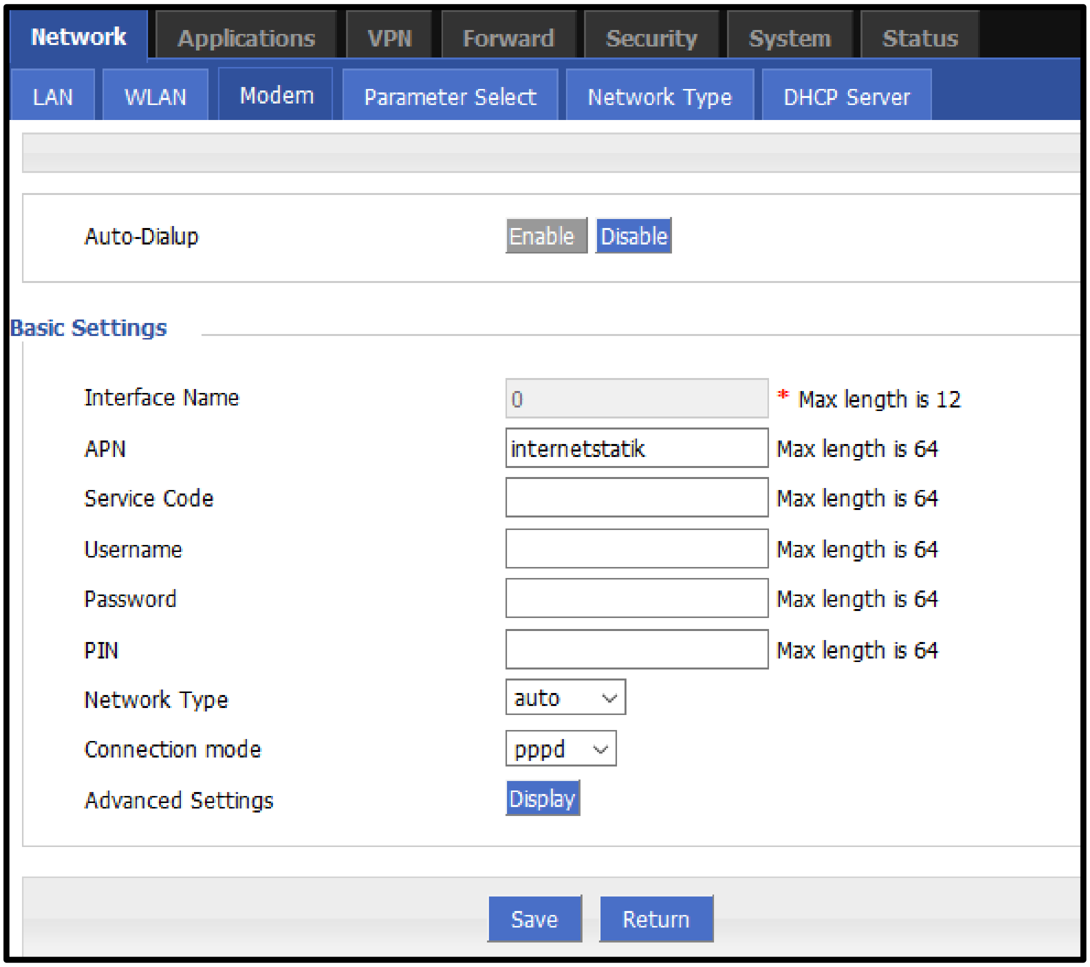
Figure.5- Network>Modem>Mod

In this screen you can see your Interface Name and APN list. You can **Modify** (Mod), **Delete** (Del), **Enable** (En) and **Disable** (Dis) your APN profile.

Single click **"Mod"** to access modem parameter settings section. After that you can set APN profile of your SIM card.

- ✓ Set **APN**, **Username** and **Password** (If you have PIN of SIM card you can set PIN disable)
- ✓ Set **Network Type** to **Edge**, **WCDMA**, **TDD-LTE, FDD-LTE** or **Auto**
- ✓ Click the **Save** icon to finish.

NETWORK>MODEM>MOD



Auto-Dialup: Enable Disable

Basic Settings

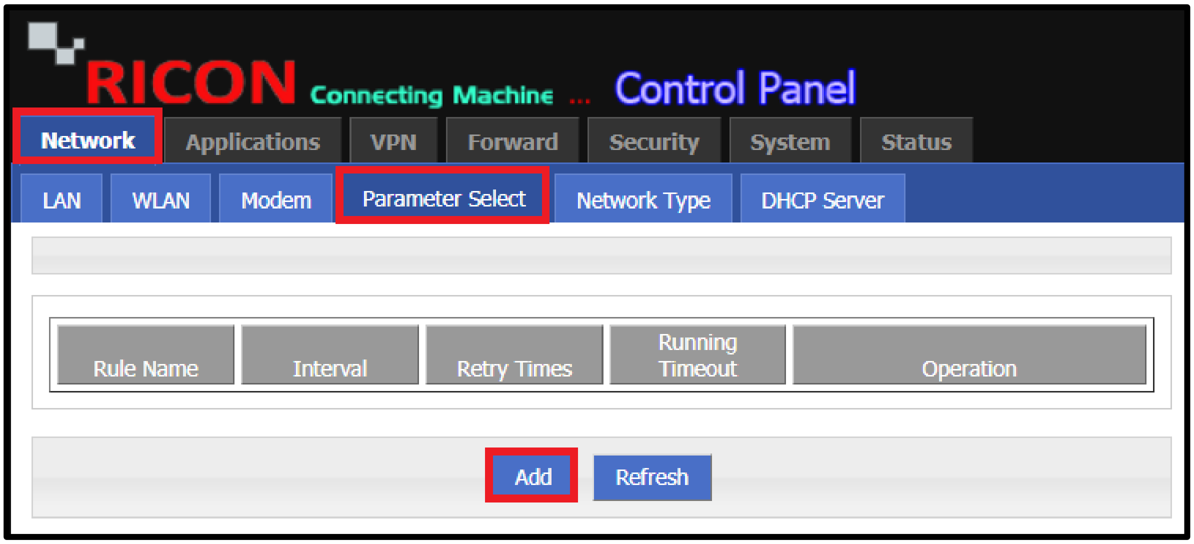
Interface Name	0	* Max length is 12
APN	internetstatik	Max length is 64
Service Code		Max length is 64
Username		Max length is 64
Password		Max length is 64
PIN		Max length is 64
Network Type	auto	
Connection mode	pppd	
Advanced Settings	Display	

Figure.6- Network>Modem>Mod

3.4 PARAMETER SETTING

The S9922M router can also log specific users or interfaces. To do follow the steps below.

NETWORK>PARAMETER SELECT



Rule Name	Interval	Retry Times	Running Timeout	Operation

Figure.7- Network>Parameter Select

- ✓ **Status;** Enable must be selected for the entered parameters to be active.

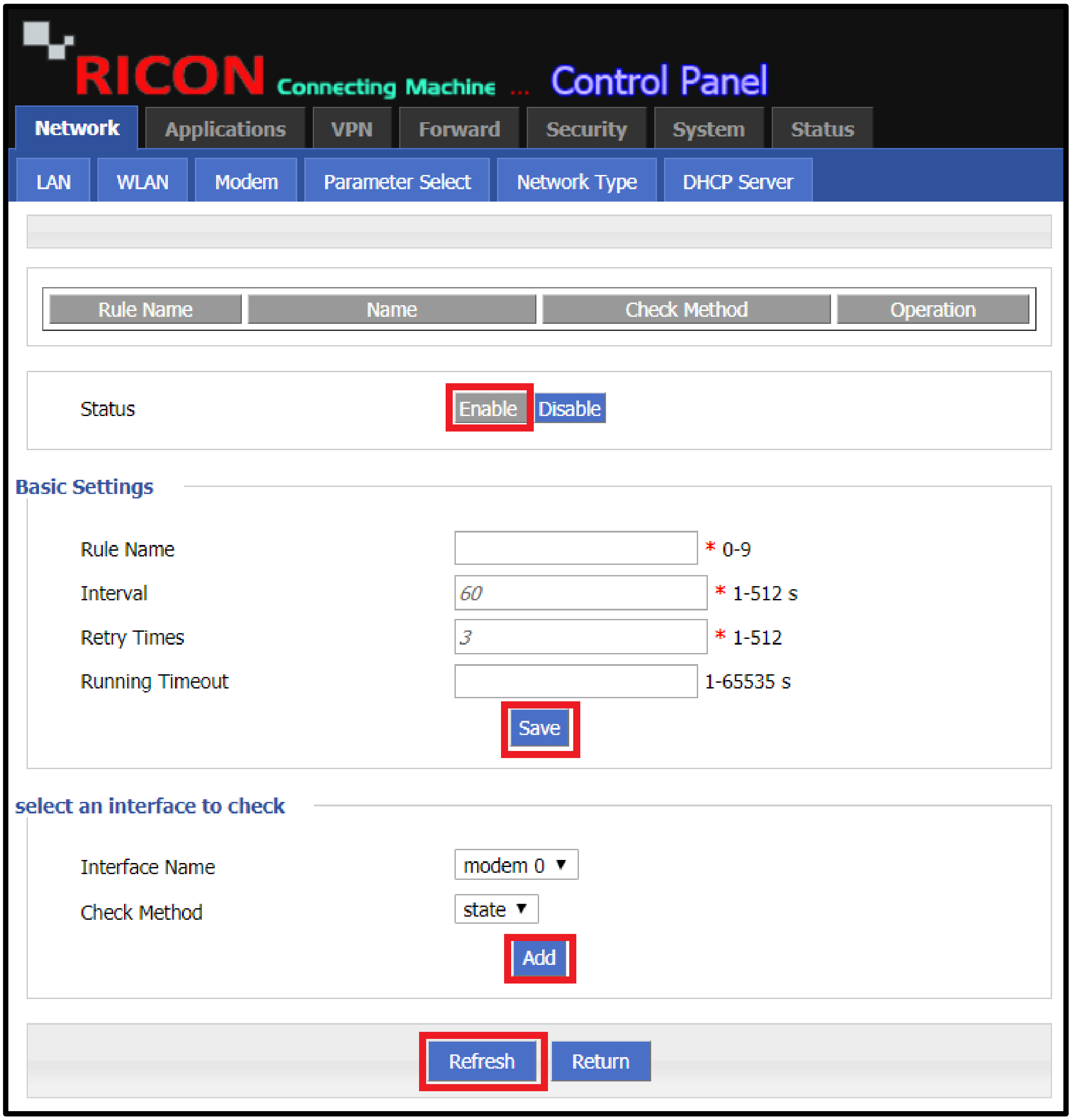
Basic Settings;

- ✓ **Rule Name;** Enter parameter name here.
- ✓ **Interval;** Enter the time you want to log.
- ✓ **Retry Times;** Enter retry times here.
- ✓ **Running Timeout;** Enter the period of inaccessibility to the user or interface here.
- ✓ Click the **Save** icon to finish.

Select an interface to check;

- ✓ **Interface Name;** modem 0 and br0**.** Select the user-accessed interface.
- ✓ **Check Method;** state or icmp.
  - **State**; If you select state, the interface of your choice is logged.
  - **Icmp**; If you select icmp, the logs of the specified user are kept.
- ✓ Click the **Add** and **Refresh** icon to finish.

NETWORK>PARAMETER SELECT>ADD



Rule Name	Name	Check Method	Operation

Status: Enable / Disable

Basic Settings

Rule Name		* 0-9
Interval	60	* 1-512 s
Retry Times	3	* 1-512
Running Timeout		1-65535 s

select an interface to check

Interface Name	modem 0 ▼
Check Method	state ▼

Figure.8- Network>Parameter Select> Add

3.5 NETWORK TYPE SETTING

✓ **Default Route;** modem, eth0, eth1.

- **Modem;** Select the modem if you want the device to access to internet via cellular.
- **Eth0;** Select the modem if you want the device to access the internet through the LAN port and enter your default gateway here.
- **Eth1;** Select the modem if you want the device to access the internet via the LAN / WAN port.

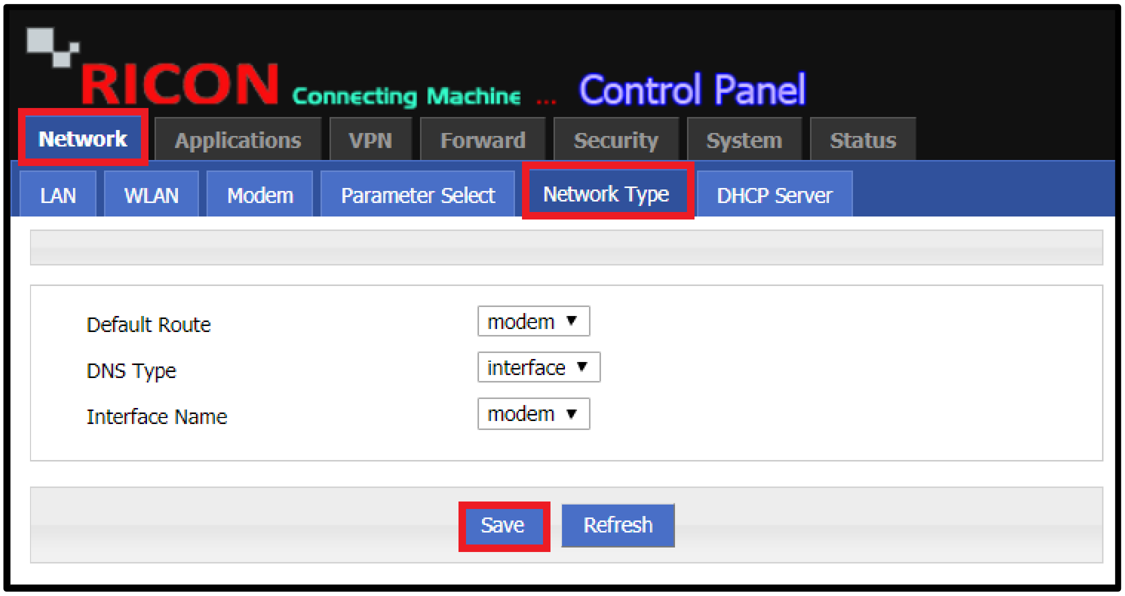
✓ **DNS Type;** interface and custom.

- **Interface**; The DNS settings of your internet provider service are assumed to be default.
- **Custom**; The DNS which you specify are considered valid.

✓ **Interface Name;** modem and eth1**.** You must select the WAN port of your device.

✓ Click the **Save** icon to finish.

NETWORK>NETWORK TYPE



Default Route: modem ▼

DNS Type: interface ▼

Interface Name: modem ▼

Figure.9- Network>Network Type

3.6 DHCP SETTING

S9922M series LTE router function is as a DHCP server, letting it assign the following to all computers connected to the router's LAN:
• IP address
• DNS server
• Default gateway address

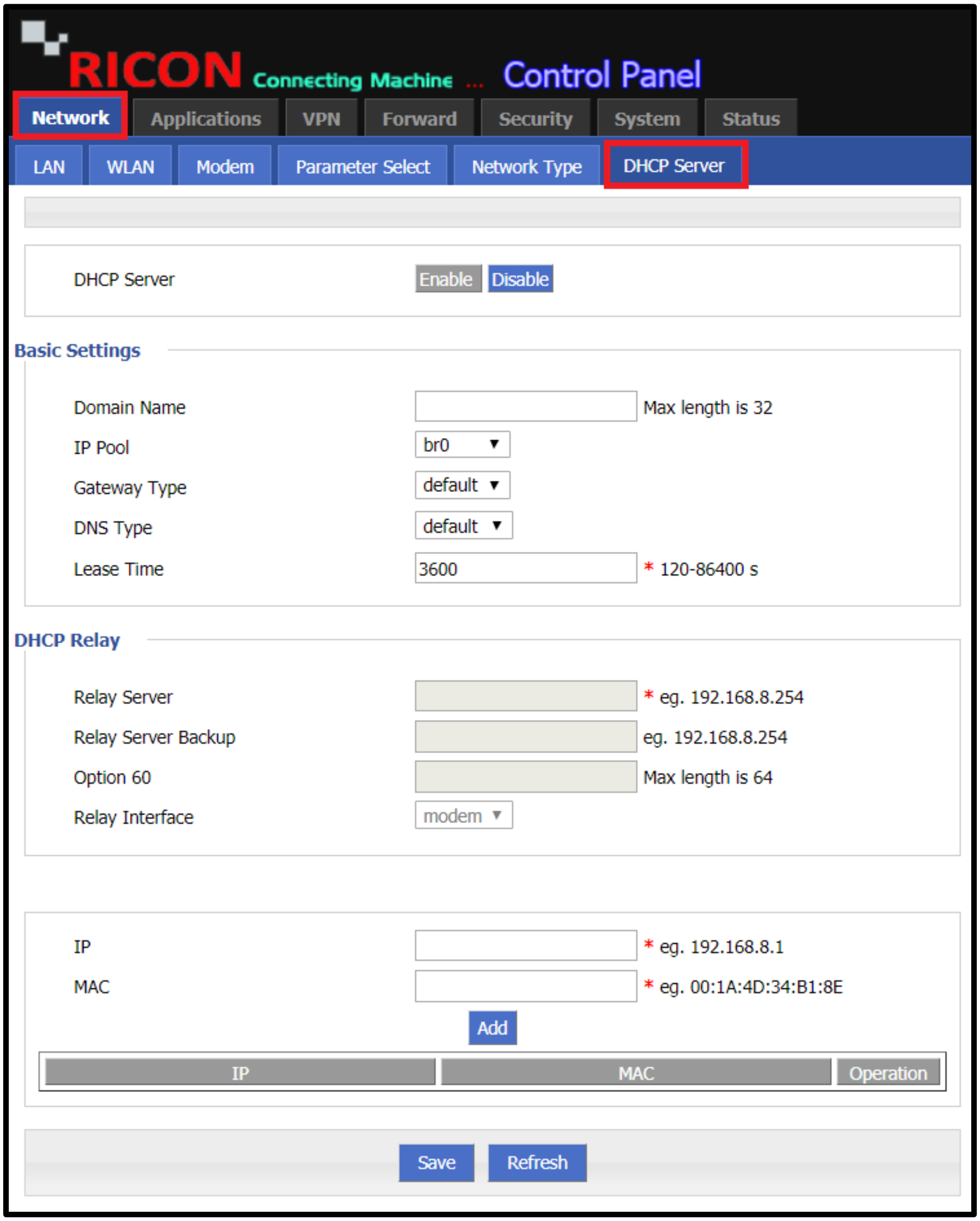
DHCP is disable in default S9922M series. So firstly, you have to enable DHCP Server. After that you can follow the steps below to configure the DHCP settings.

- ✓ **IP Pool;** br0 and custom
- ✓ **Gateway;** default, br0 or custom
- ✓ **DNS Type;** default, modem, br0 or custom

If DHCP Server disable is selected, DHCP relay is activated.

- ✓ **Relay Server;** Enter the DHCP relay server IP here.
- ✓ **IP;** Enter the DHCP relay IP here.
- ✓ **MAC;** Enter the DHCP relay MAC address here.
- ✓ Click the **Save** icon to finish.

NETWORK>DHCP SERVER



DHCP Server: Enable / Disable

Basic Settings

Domain Name		Max length is 32
IP Pool	br0	
Gateway Type	default	
DNS Type	default	
Lease Time	3600	* 120-86400 s

DHCP Relay

Relay Server		* eg. 192.168.8.254
Relay Server Backup		eg. 192.168.8.254
Option 60		Max length is 64
Relay Interface	modem	

IP		* eg. 192.168.8.1
MAC		* eg. 00:1A:4D:34:B1:8E

IP	MAC	Operation

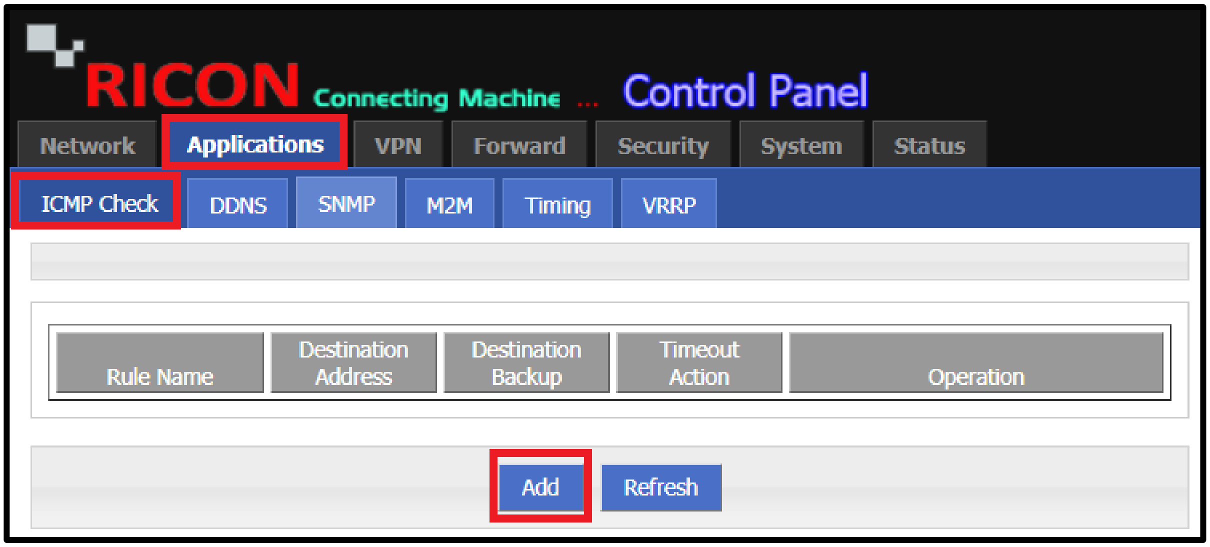
Figure.10- Network>DHCP Server

4 APPLICATIONS CONFIGURATION

4.1 ICMP CHECK SERVICE

The S9922M series LTE routers are can automatically take the actions which you want to the specific interface, IP or domain can't accessible. Follow steps below.

APPLICATIONS > ICMP CHECK

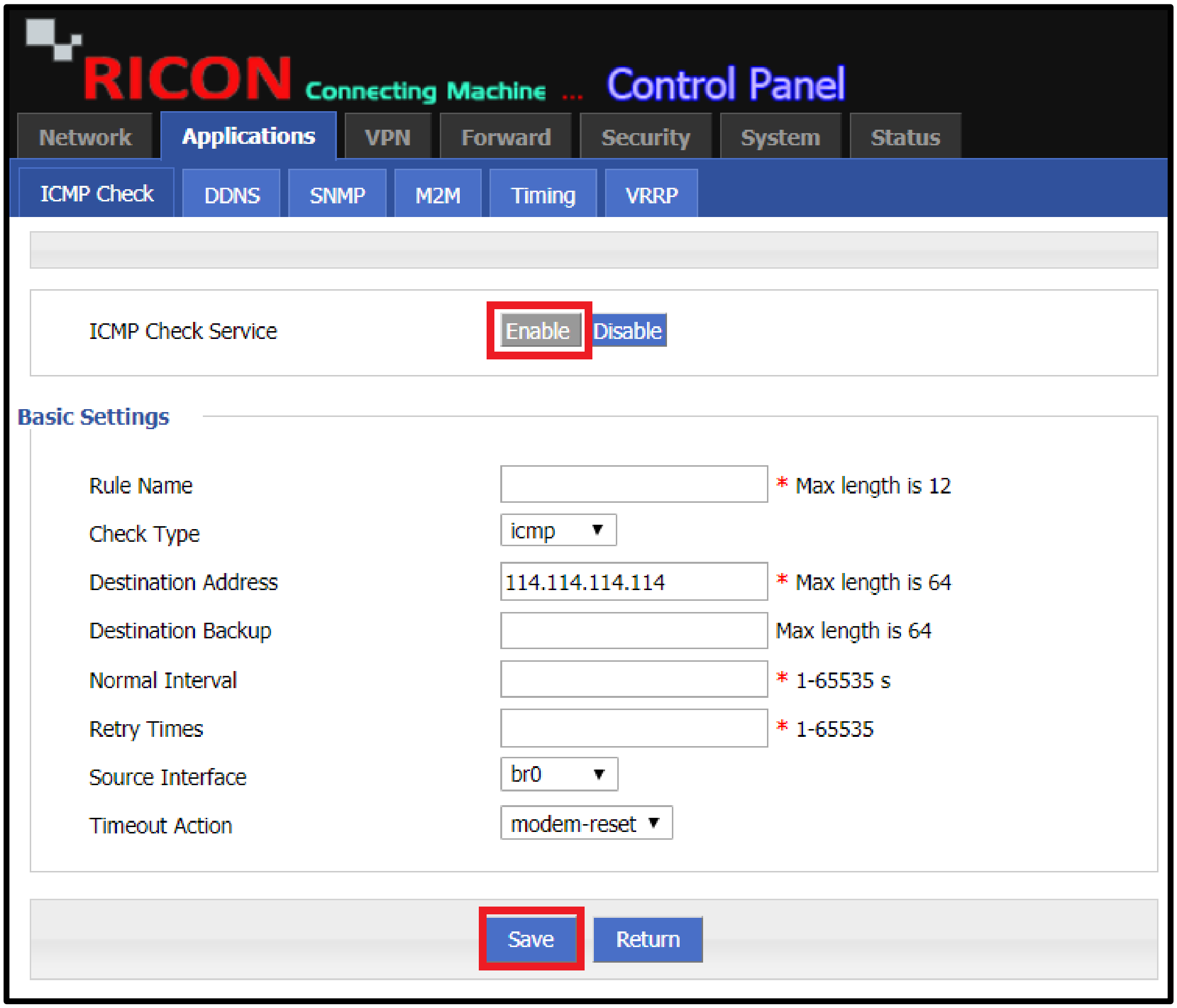


Rule Name	Destination Address	Destination Backup	Timeout Action	Operation

Figure.11- Applications>ICMP Check

- ✓ **ICMP Check Service;** Enable must be selected for ICMP Check feature
- ✓ **Rule Name;** Enter the name of ICMP Check Rule
- ✓ **Check type;** icmp or domain.
  - **Icmp;** If the specific user or interface IP is selected, must select Icmp.
  - **Domain;** If the domain IP is to be entered, must select Domain.
- ✓ **Destination Address;** Enter the destination IP.
- ✓ **Destination Backup;** The secondary destination IP, depending on your request.
- ✓ **Normal Interval;** Enter inaccessibility time before action is taken.
- ✓ **Retry Times;** Enter the number of repetitions.
- ✓ **Source Interface;** br0, modem. Select the interface you want to select as the source.
- ✓ **Timeout Action;** modem-reset, reboot, custom.
  - **Modem-reset;** Restarts the wan interface.
  - **Reboot;** Restart the device.
  - **Custom;** The “Run Commands” interface comes up, enter the action you want the device to take.
- ✓ Click the **Save** icon to finish.

APPLİCATİONS>ICMP CHECK>ADD



ICMP Check Service: Enable

Basic Settings

Rule Name		* Max length is 12
Check Type	icmp ▼	
Destination Address	114.114.114.114	* Max length is 64
Destination Backup		Max length is 64
Normal Interval		* 1-65535 s
Retry Times		* 1-65535
Source Interface	br0 ▼	
Timeout Action	modem-reset ▼	

Figure.12- Applications>ICMP Check>Add

4.2 DDNS CONFIGURATION

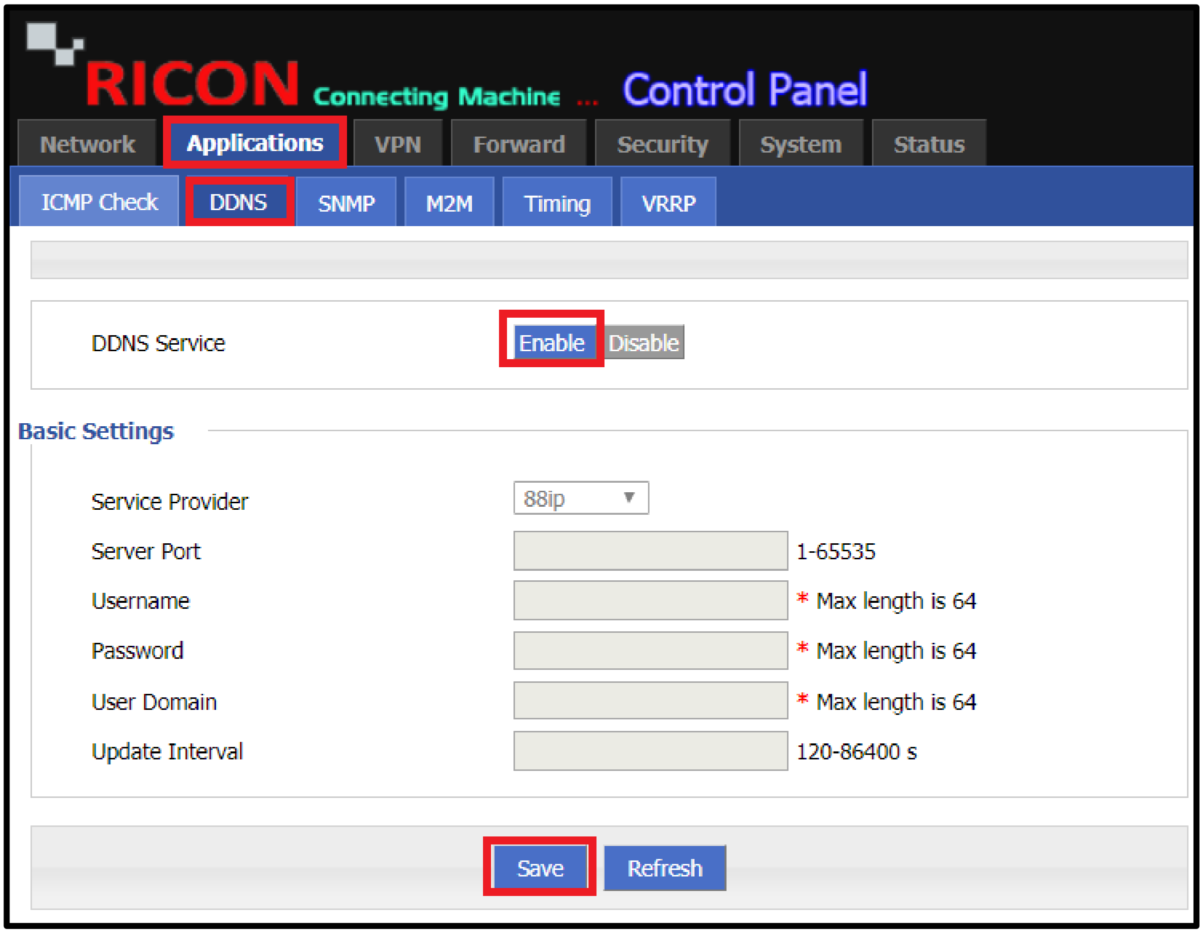
Dynamic domain name server (DDNS) associates a static domain name with the dynamic IP address of its host.

With DDNS, which associates a static domain name with the dynamic IP address of its host, users on the Internet can access the server only with domain names.

The S9922M series LTE routers are router is capable of Dynamic DNS. To do this, follow the steps. Click the Applications tab and choose DDNS from the navigation menu.

- ✓ **DDNS Service;** Enable must be selected for the entered DDNS to be active.
- ✓ **Server Port;** Enter the port you specified here.
- ✓ **Username;** Enter your username.
- ✓ **Password;** Enter your password.
- ✓ **User Domain;** Enter the domain of the device you are using.
- ✓ **Update Interval;** Enter the refresh interval of DDNS .
- ✓ Click the **Save** icon to finish.

APPLİCATİONS>DDNS



DDNS Service ● Enable ○ Disable

Basic Settings

Service Provider	88ip ▼	
Server Port		1-65535
Username		* Max length is 64
Password		* Max length is 64
User Domain		* Max length is 64
Update Interval		120-86400 s

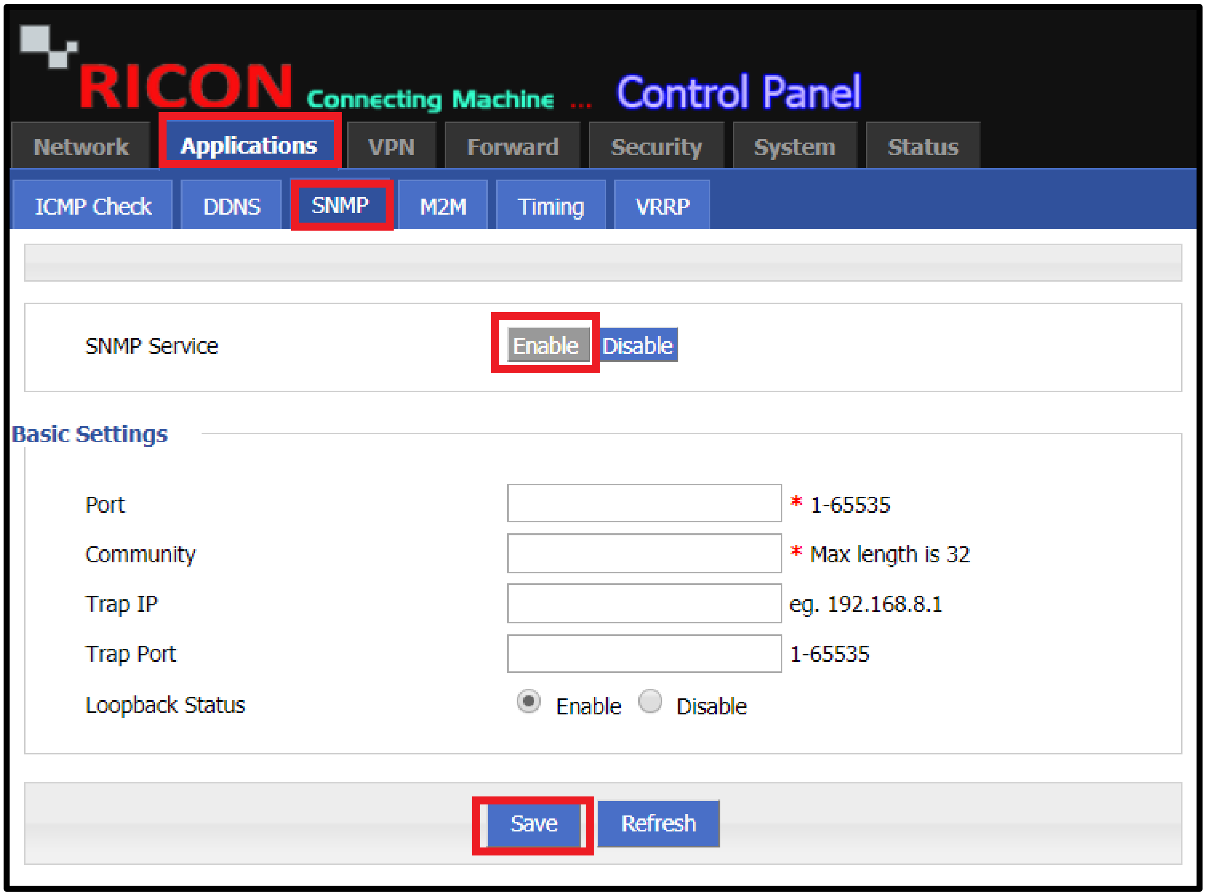
Figure.13- Applications>DDNS

4.3 SNMP CONFIGURATION

SNMP settings window allows you to remotely monitor and send GSM event information to the server. Follow the steps below to configure SNMP.

- ✓ **SNMP Service;** Enable must be selected for SNMP to be active.
- ✓ **Port;** Enter SNMP service's port. (ex: 161)
- ✓ **Community;** The SNMP Community is like a user id or password that allows access to a router's or other device's statistics
- ✓ **Trap IP;** Enter the IP of the device we want to send a message to.
- ✓ **Trap Port;** Enter the port number of the device we want to send a message to.
- ✓ **Loopback Status;** Optionally, you can enable or disable loopback.
- ✓ Click the **Save** icon to finish.

APPLİCATİONS>SNMP



SNMP Service: Enable | Disable

Basic Settings

Port: * 1-65535

Community: * Max length is 32

Trap IP: eg. 192.168.8.1

Trap Port: 1-65535

Loopback Status: ● Enable ○ Disable

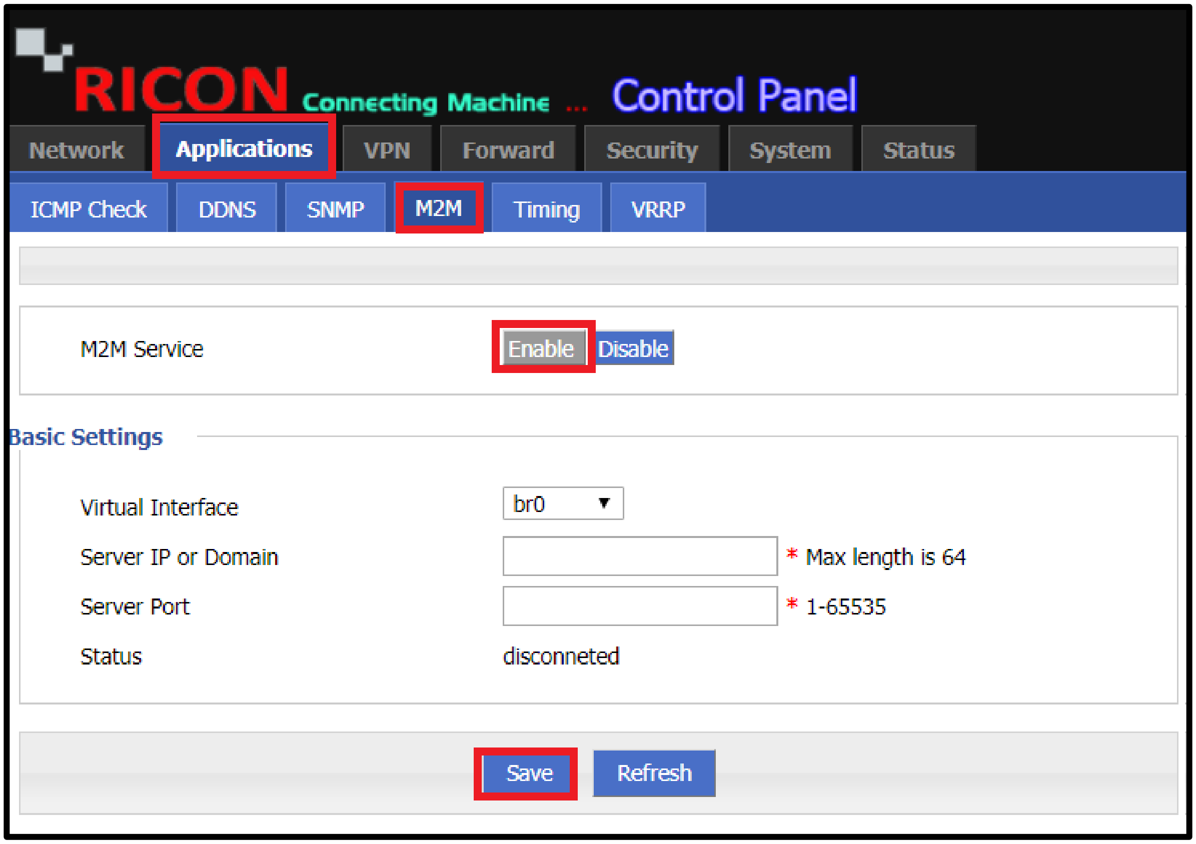
Figure.14- Applications>SNMP

5.4 M2M CONFIGURATION

Through S9922M series LTE routers, you can do machine to machine service. With the Ricon management system, you can view the current status information of all your Ricon S9922M series LTE router models through a single interface.

- ✓ **M2M Service;** Enable must be selected for the entered M2M to be active.
- ✓ **Virtual Interface;** br0 and modem. Select the device's WAN port.
- ✓ **Server IP or domain;** Enter the IP of the Ricon Management System (RMS) server IP
- ✓ **Server Port;** Enter the specific server port which router and RMS are communicate.
- ✓ Click the **Save** icon to finish.

APPLİCATİONS>M2M



M2M Service: Enable | Disable

Basic Settings

Virtual Interface: br0 ▼

Server IP or Domain: * Max length is 64

Server Port: * 1-65535

Status: disconneted

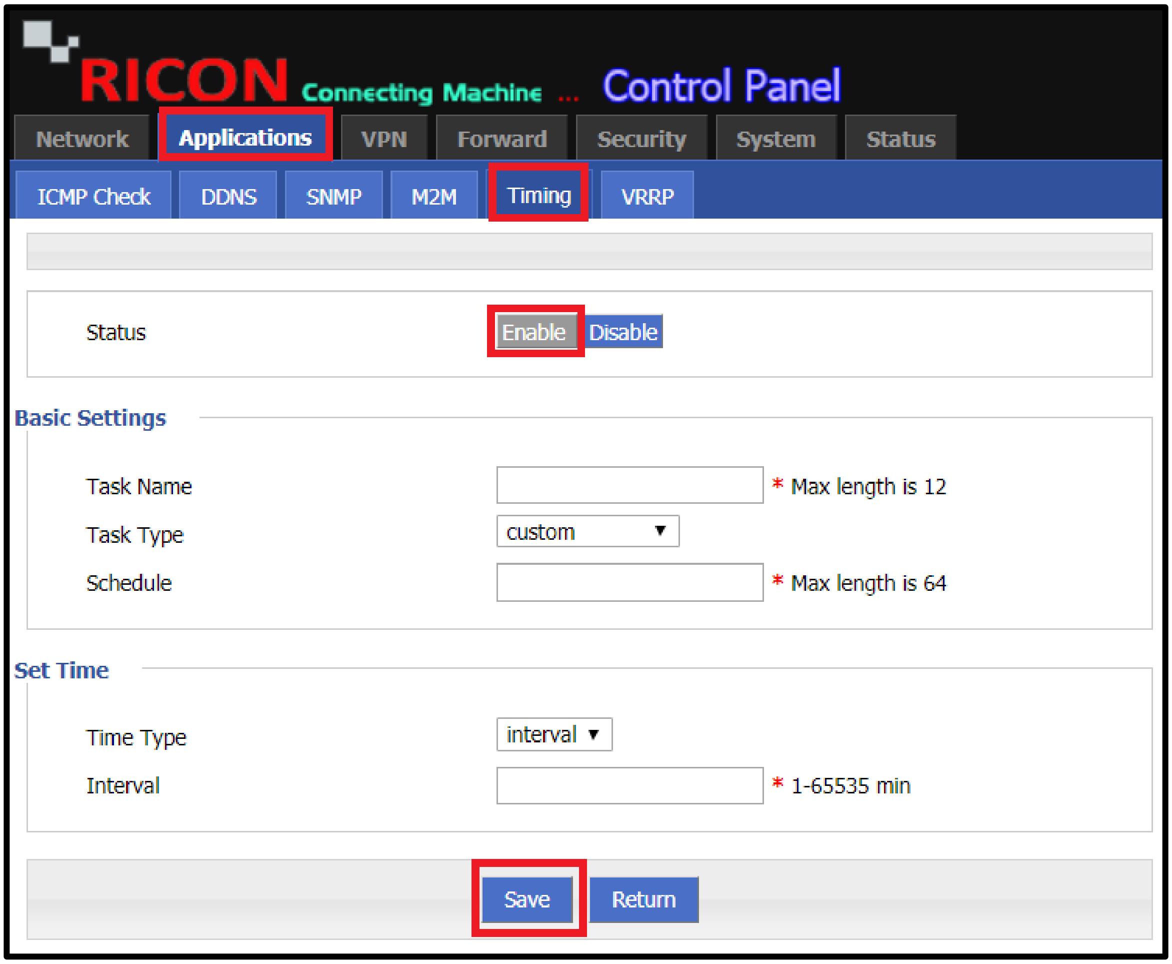
Figure.15- Applications>M2M

5.5 TIMING SETTING

After setting the clock of the S9922M series LTE router, the device can be automatically restarted at the specified time or intervals with Timing configuration, the LTE WAN port can be turned on and off, or the desired action can be taken.

- ✓ **Status;** Enable must be selected for the entered Timing settings to be active.
- ✓ **Task Name;** Enter timing name here.
- ✓ **Task Type;** modem-online, reboot and custom.
  - **Modem-online;** modem online control.
  - **Reboot;** restarts the device.
  - **Custom;** The Schedule interface comes up and the specified action must be entered here.
- ✓ **Time Type;** Range and interval.
  - **Range;** If range is selected, the desired action is taken on certain dates.
  - **Interval;** If interval is selected, the desired action is taken at specified time intervals.
- ✓ Click the **Save** icon to finish.

APPLİCATİONS>TİMİNG



Status: Enable

Basic Settings

Task Name * Max length is 12

Task Type: custom

Schedule * Max length is 64

Set Time

Time Type: interval

Interval * 1-65535 min

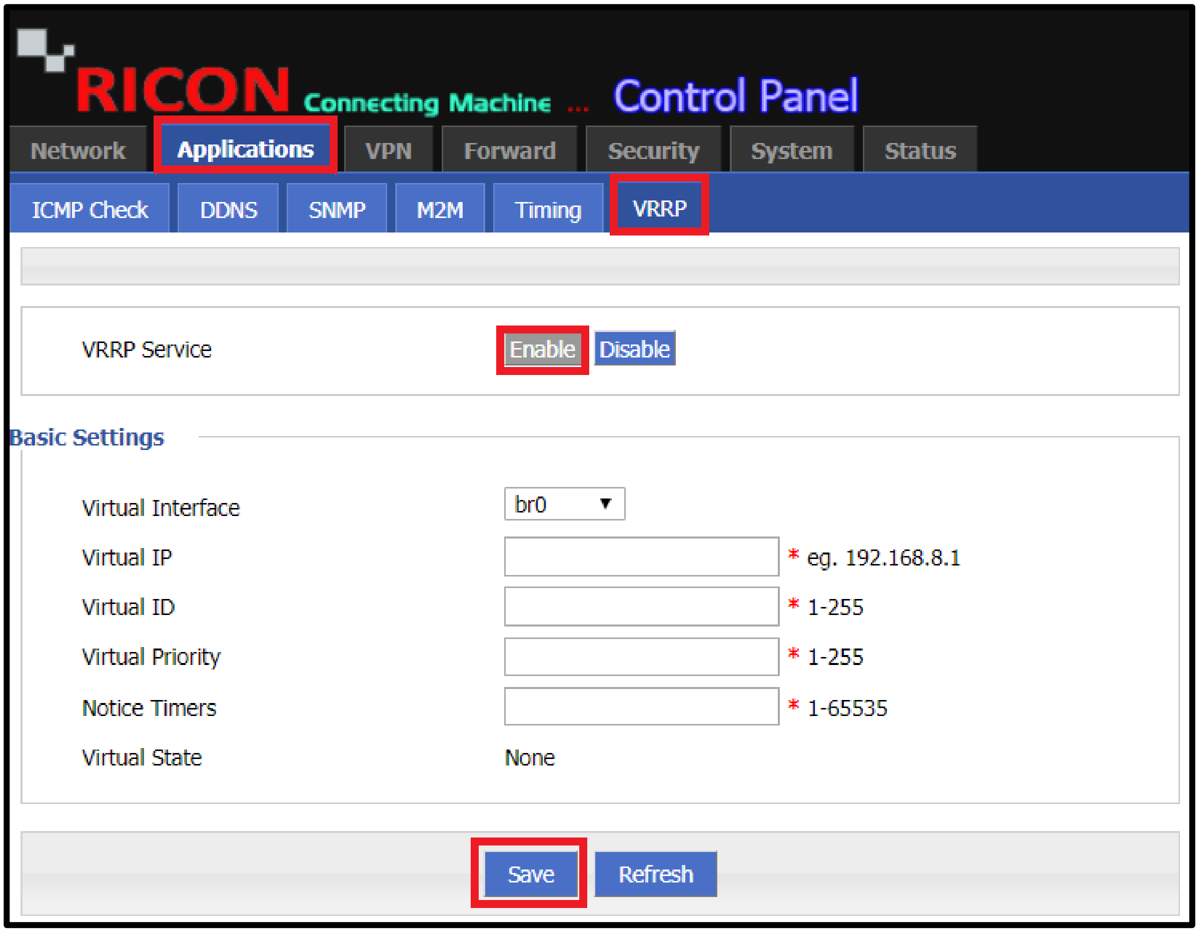
Figure.16- Applications>Timing

5.6 VRRP CONFIGURATION

Virtual Router Redundancy Protocol (VRRP) is the open standard version at Cisco proprietary protocol called HSRP, so it can support from different vendors including Ricon devices. The VRRP works exactly the same as HSRP in providing a gateway using one virtual IP address. To perform VRRP over the S9922M series LTE routers, follow the steps below.

- ✓ **VRRP Service;** Enable must be selected for the entered VRRP to be active.
- ✓ **Virtual Interface;** br0 and modem. Select the device's WAN port.
- ✓ **Virtual IP;** Enter your virtual IP here.
- ✓ **Virtual ID;** Enter your virtual ID here.
- ✓ **Virtual Priority;** Enter your virtual priority here.
- ✓ **Notice Timers;** Enter the desired time period here.
- ✓ Click the **Save** icon to finish.

APPLICATION>VRRP



VRRP Service

Basic Settings

Virtual Interface	br0 ▼	
Virtual IP		* eg. 192.168.8.1
Virtual ID		* 1-255
Virtual Priority		* 1-255
Notice Timers		* 1-65535
Virtual State	None	

Figure.17- Applications>VRRP

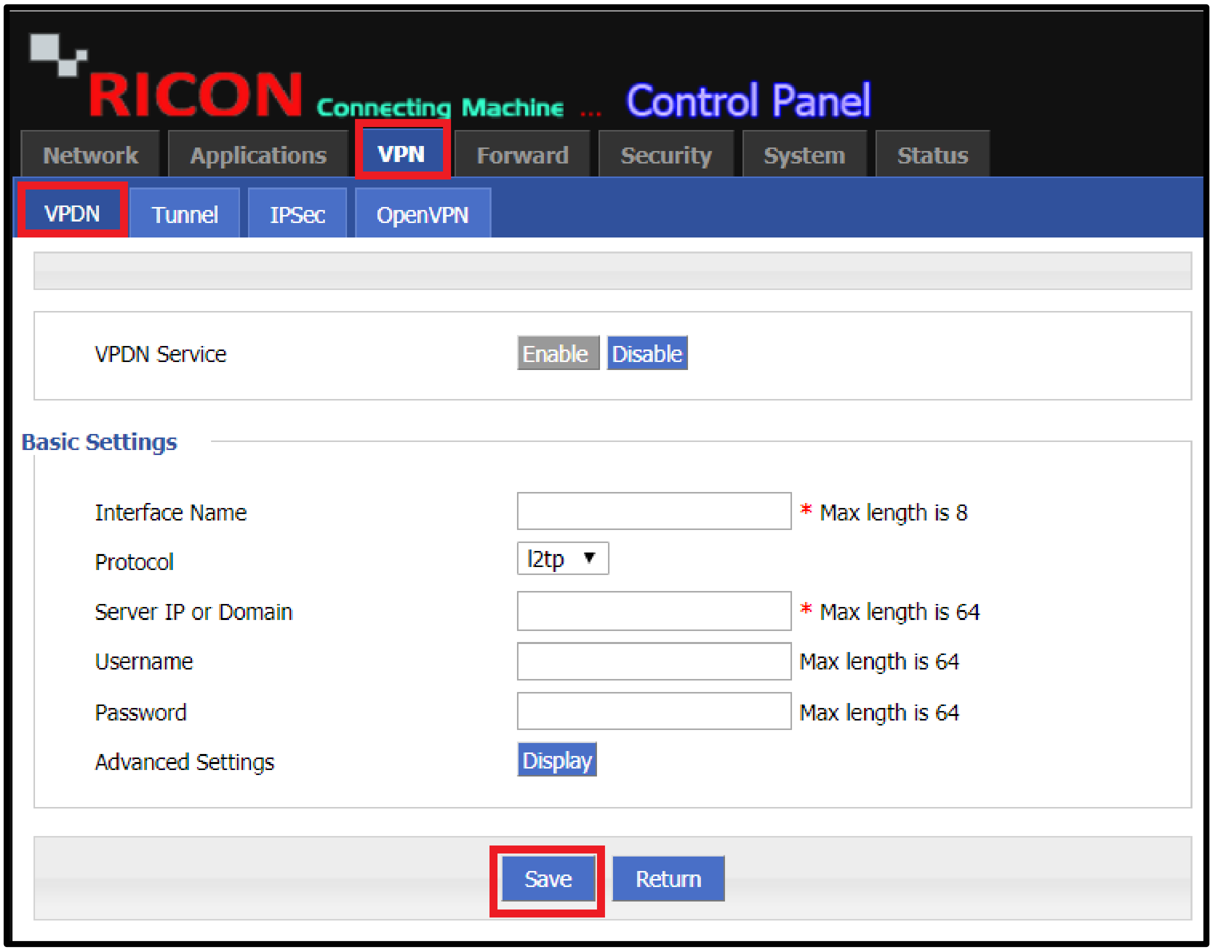
6 VPN CONFIGURATION

6.1 VPDN CONFIGURATION

Virtual Private Dial-up Network (VPDN) is a network that extends remote access to a private network using a shared infrastructure. VPDNs are a cost-effective method of establishing a long-distance, point-to-point connection between remote dial users and a private network. Follow the steps below to make Virtual Private Dialup Network over the router.

- **VPDN Service;** Enable must be selected for the entered VPDN service to be active.
- **Interface Name;** Enter VPDN name here.
- **Protocol;** l2tp and pptp. Select the protocol you specified.
- **Server IP or Domain;** Enter your server’s IP or domain name.
- **Username;** Enter the username of your tunnel.
- **Password;** Enter the password of your tunnel.
- Click the **Save** icon to finish.

VPN>VPDN



VPDN Service

Basic Settings

Interface Name * Max length is 8

Protocol l2tp ▼

Server IP or Domain * Max length is 64

Username Max length is 64

Password Max length is 64

Advanced Settings

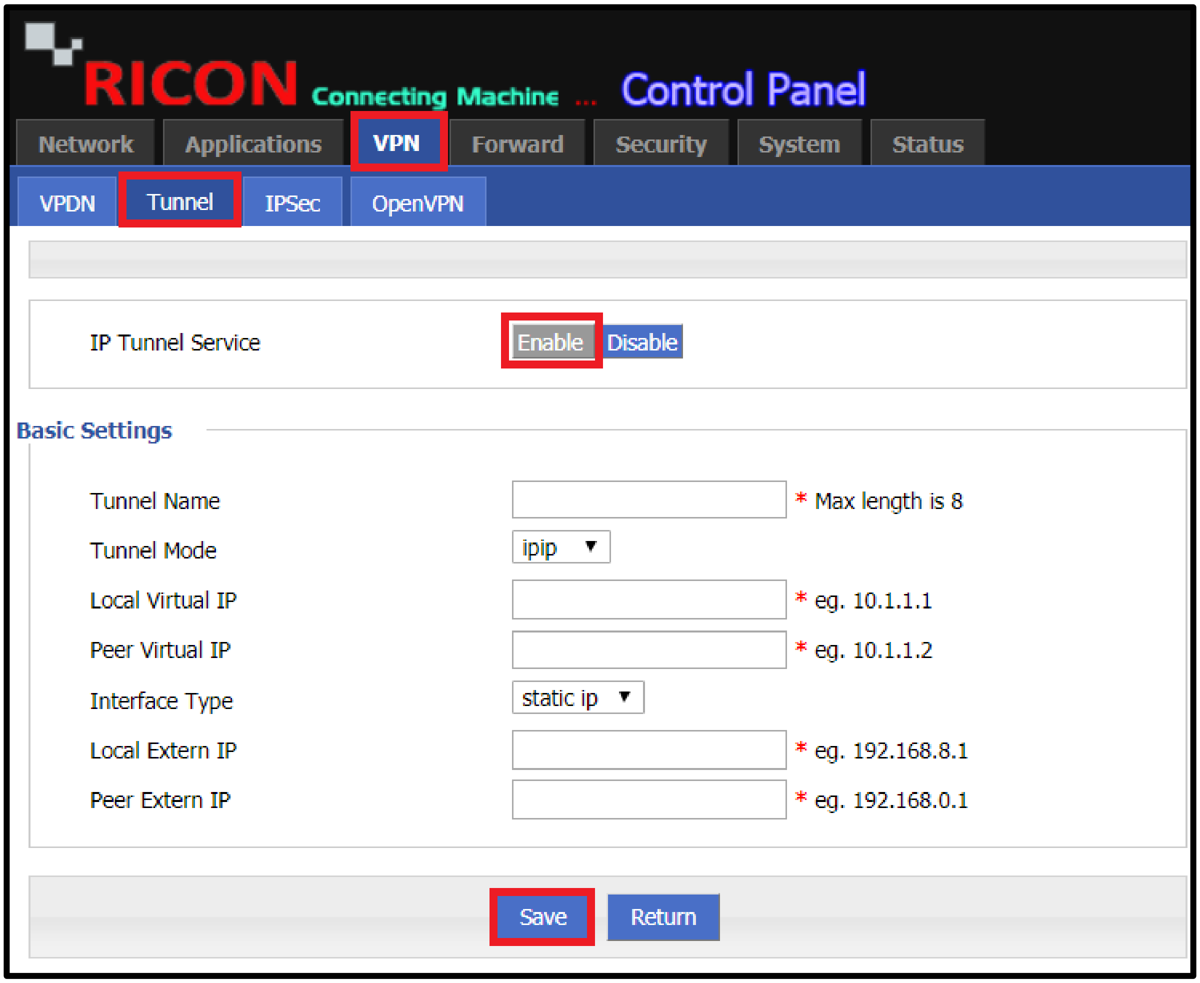
Figure.18- VPN>VPDN

6.2 TUNNEL CONFIGURATION

A VPN tunnel (often simply referred to as a VPN, or virtual private network) is an encrypted connection between your computer or mobile device and the wider internet. Since your connection is encrypted, nobody along the VPN tunnel is able to intercept, monitor, or alter your communications. Follow the steps below to tunnel with the S9922M series LTE routers.

- ✓ **IP Tunnel Service;** Enable must be selected for the entered Tunnel configuration to be active.
- ✓ **Tunnel Name;** Enter the name your specified here.
- ✓ **Tunnel Mode;** ipip, gre and mgre. Select according to the tunnel definitions to be made.
- ✓ **Local Virtual IP;** The local IP required to access the opposite end must be entered here.
- ✓ **Peer Virtual IP;** The external IP required to access the local terminal from the opposite end must be entered here.
- ✓ **Interface Type;** Static ip and interface. Select the wan port to be communicated with or your specified IP.
- ✓ **Local Extern IP;** Enter your local external IP.
- ✓ **Peer Extern IP;** Enter your peer external IP
- ✓ Click the **Save** icon to finish.

VPN>TUNNEL>ADD



IP Tunnel Service

Basic Settings

Tunnel Name		* Max length is 8
Tunnel Mode	ipip ▼	
Local Virtual IP		* eg. 10.1.1.1
Peer Virtual IP		* eg. 10.1.1.2
Interface Type	static ip ▼	
Local Extern IP		* eg. 192.168.8.1
Peer Extern IP		* eg. 192.168.0.1

Figure.19- VPN>Tunnel>Add

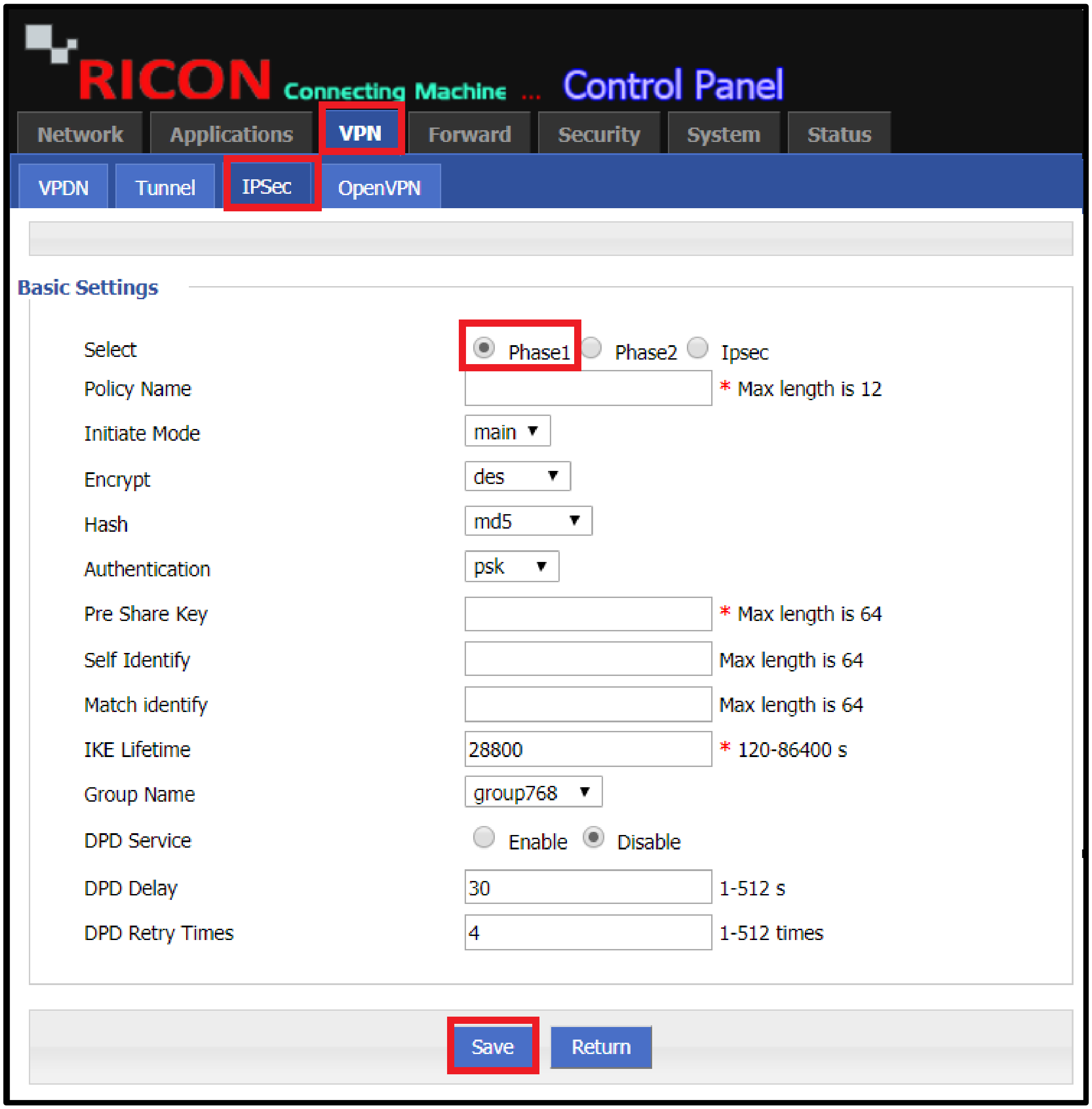
6.3 IPSEC CONFIGURATION

IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices. By following the steps below, S9922M series LTE routers can do IPsec.

6.3.1 PHASE1 CONFIGURATION

- ✓ **Policy Name;** Enter the policy name you specified here.
- ✓ **Initiate Mode;** main and aggr. Select your initiate mode.
- ✓ **Encrypt;** des, 3des, aes256, aes192, aes128. Select your specific encryption mode.
- ✓ **Hash;** md5, sha1, sha2_256. Select your specific encryption mode.
- ✓ **Authentication;** psk, rsasig, xauth. Select your specific authentication.
- ✓ **Pre share Key;** Enter the share key you specified.
- ✓ **Self identify;** Enter your self identify here.
- ✓ **Match identify;** Enter your match identify here.
- ✓ **IKE Lifetime;** Enter the IKE lifetime you specified here.
- ✓ **Group Name;** group768, group1024, group1536. Select the group name you specified.
- ✓ **DPD Service;** Select enable or disable according to your request.
- ✓ Click the **Save** icon to save phase1.

VPN>IPSEC>ADD>PHASE1



Basic Settings

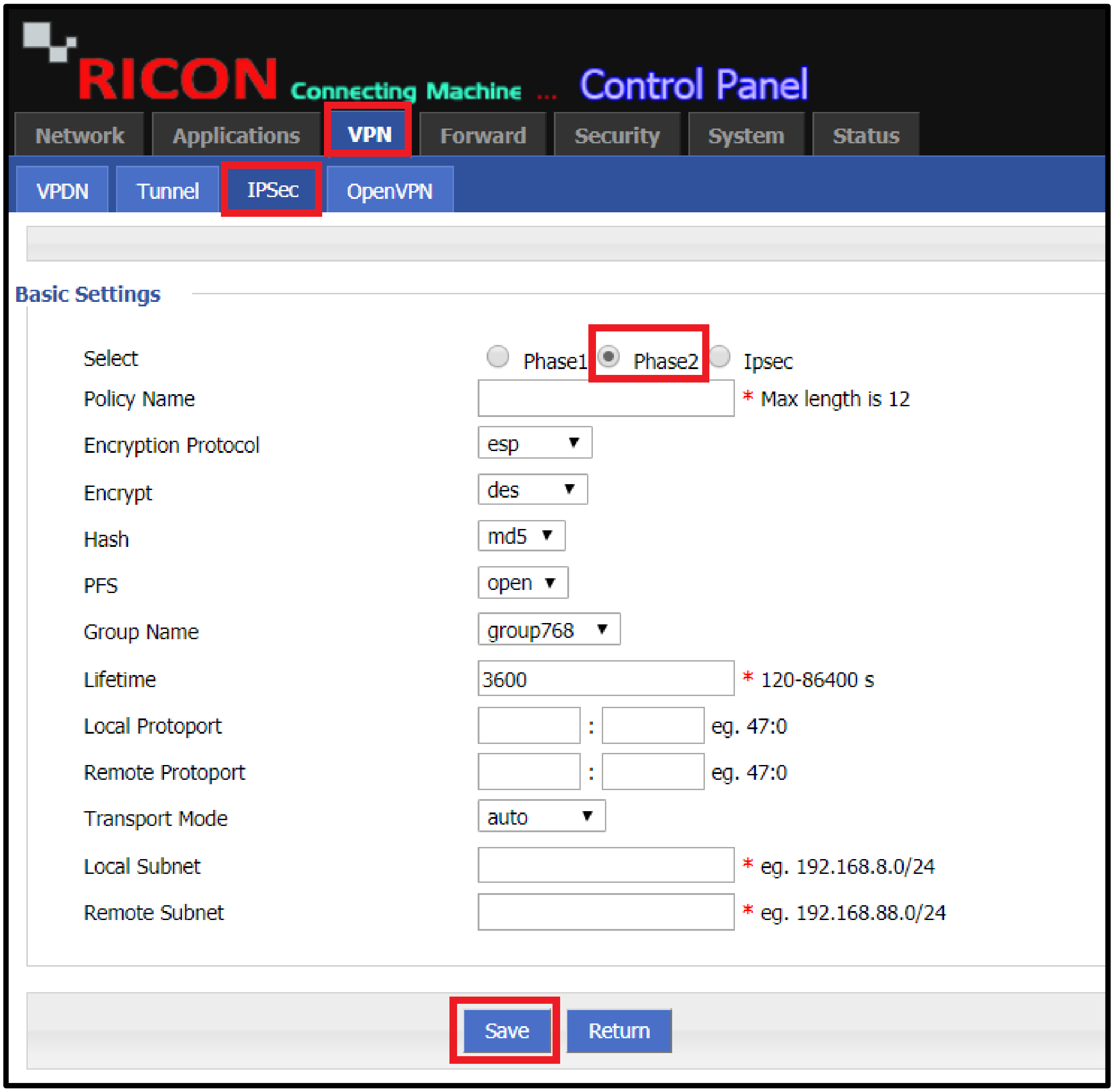
Select	● Phase1 ○ Phase2 ○ Ipsec	
Policy Name		* Max length is 12
Initiate Mode	main ▼	
Encrypt	des ▼	
Hash	md5 ▼	
Authentication	psk ▼	
Pre Share Key		* Max length is 64
Self Identify		Max length is 64
Match identify		Max length is 64
IKE Lifetime	28800	* 120-86400 s
Group Name	group768 ▼	
DPD Service	○ Enable ● Disable	
DPD Delay	30	1-512 s
DPD Retry Times	4	1-512 times

Figure.20- VPN>IPSec>Add>Phase1

6.3.2 PHASE2 CONFIGURATION

- ✓ **Policy Name;** Enter the policy name you specified here.
- ✓ **Encryption Protocol;** esp, ah, ah+esp.
- ✓ **Encrypt;** des, 3des, aes256, aes192, aes128. Select your specific encryption mode.
- ✓ **Hash;** md5, sha1. Select your specific encryption mode.
- ✓ **PFS;** open and close. Choose according to your request.
- ✓ **Group Name;** group768, group1024, group1536. Select the group name you specified.
- ✓ **Lifetime;** Enter the lifetime you specified here.
- ✓ **Local Subnet;** Enter the local block of S9922M here.
- ✓ **Remote Subnet;** Enter the local block of the end device here.
- ✓ Click the **Save** icon to save phase2.

VPN>IPSEC>ADD>PHASE2



Basic Settings

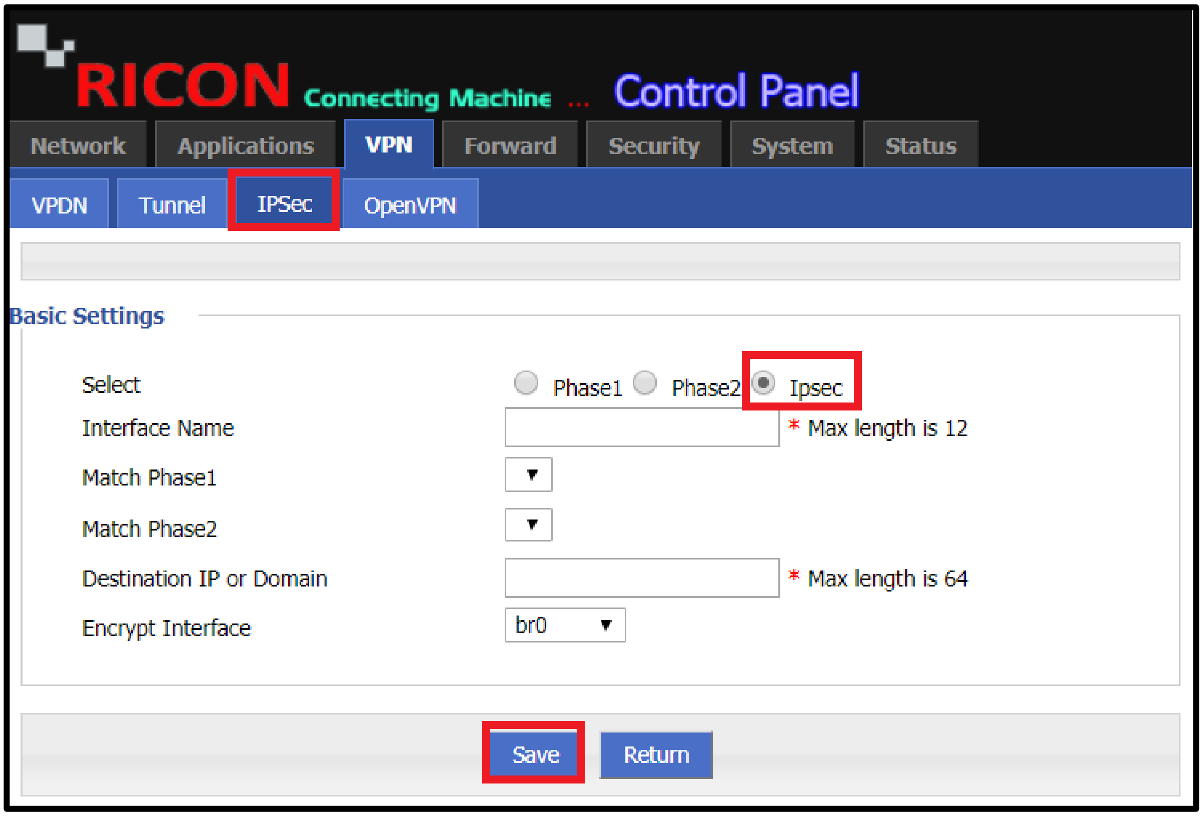
Select	○ Phase1 ● Phase2 ○ Ipsec
Policy Name	* Max length is 12
Encryption Protocol	esp
Encrypt	des
Hash	md5
PFS	open
Group Name	group768
Lifetime	3600 * 120-86400 s
Local Protoport	: eg. 47:0
Remote Protoport	: eg. 47:0
Transport Mode	auto
Local Subnet	* eg. 192.168.8.0/24
Remote Subnet	* eg. 192.168.88.0/24

Figure.21- VPN>IPSec>Add>Phase2

6.3.3 IPSec CONFIGURATION

- ✓ **Interface Name;** Enter the ipsec name you specified here.
- ✓ **Match Phase1;** Select the desired phase1.
- ✓ **Match Phase2;** Select the desired phase2.
- ✓ **Destination IP or Domain;** md5, sha1. Select your specific encryption mode.
- ✓ **Encrypt Interface;** Select the wan ip or domain where you want ipsec to work.
- ✓ Click the **Save** icon to save IPsec.

VPN>IPSEC>ADD>IPSEC



Basic Settings

Select	○ Phase1 ○ Phase2 ● Ipsec
Interface Name	* Max length is 12
Match Phase1	▼
Match Phase2	▼
Destination IP or Domain	* Max length is 64
Encrypt Interface	br0 ▼

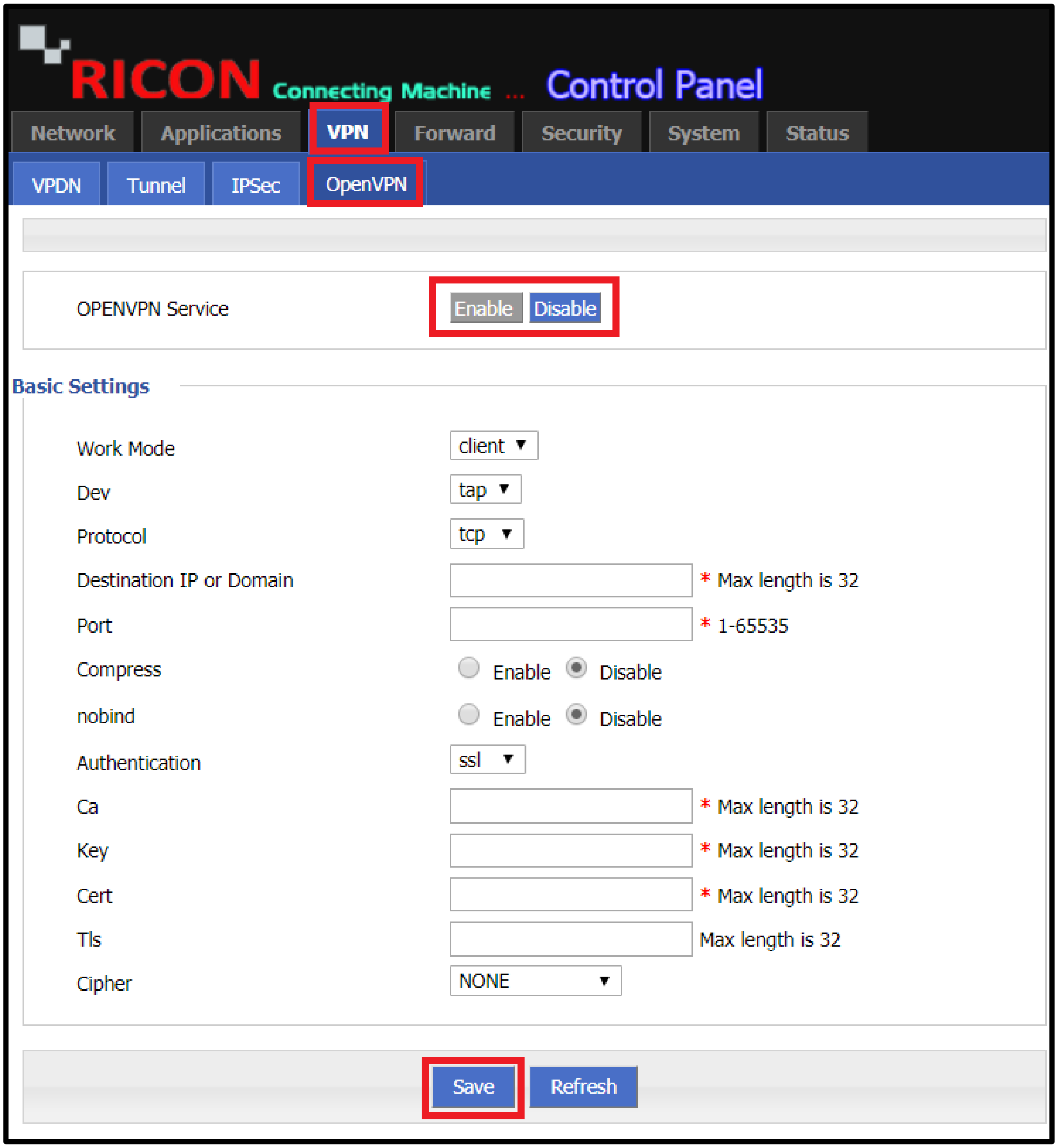
Figure.22- VPN>IPSec>Add>IPsec

6.4 OpenVPN CONFIGURATION

OpenVPN is an open-source commercial software that implements virtual private network (VPN) techniques to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Follow the steps to make OPENVPN with S9922M series LTE routers.

- ✓ **OPENVPN Service;** Enable must be selected for the entered Tunnel configuration to be active.
- ✓ **Dev;** tap and tun.
- ✓ **Protocol;** tcp and udp.
- ✓ **Destination IP or Domain;** Enter your destination IP or domain information.
- ✓ **Port;** Enter the port information here.
- ✓ **Ca;** Enter the Certificate Authority here.
- ✓ **Key;** Enter the Certificate Key here.
- ✓ **Cert;** Enter the Certificate here.
- ✓ Click the **Save** icon to finish.

VPN>OPENVPN



OPENVPN Service [Enable] [Disable]

Basic Settings

Work Mode	client ▼
Dev	tap ▼
Protocol	tcp ▼
Destination IP or Domain	* Max length is 32
Port	* 1-65535
Compress	○ Enable ● Disable
nobind	○ Enable ● Disable
Authentication	ssl ▼
Ca	* Max length is 32
Key	* Max length is 32
Cert	* Max length is 32
Tls	Max length is 32
Cipher	NONE ▼

[Save] [Refresh]

Figure.23- VPN>OpenVPN

7

7 FORWARD CONFIGURATION

7.1 NAT CONFIGURATION

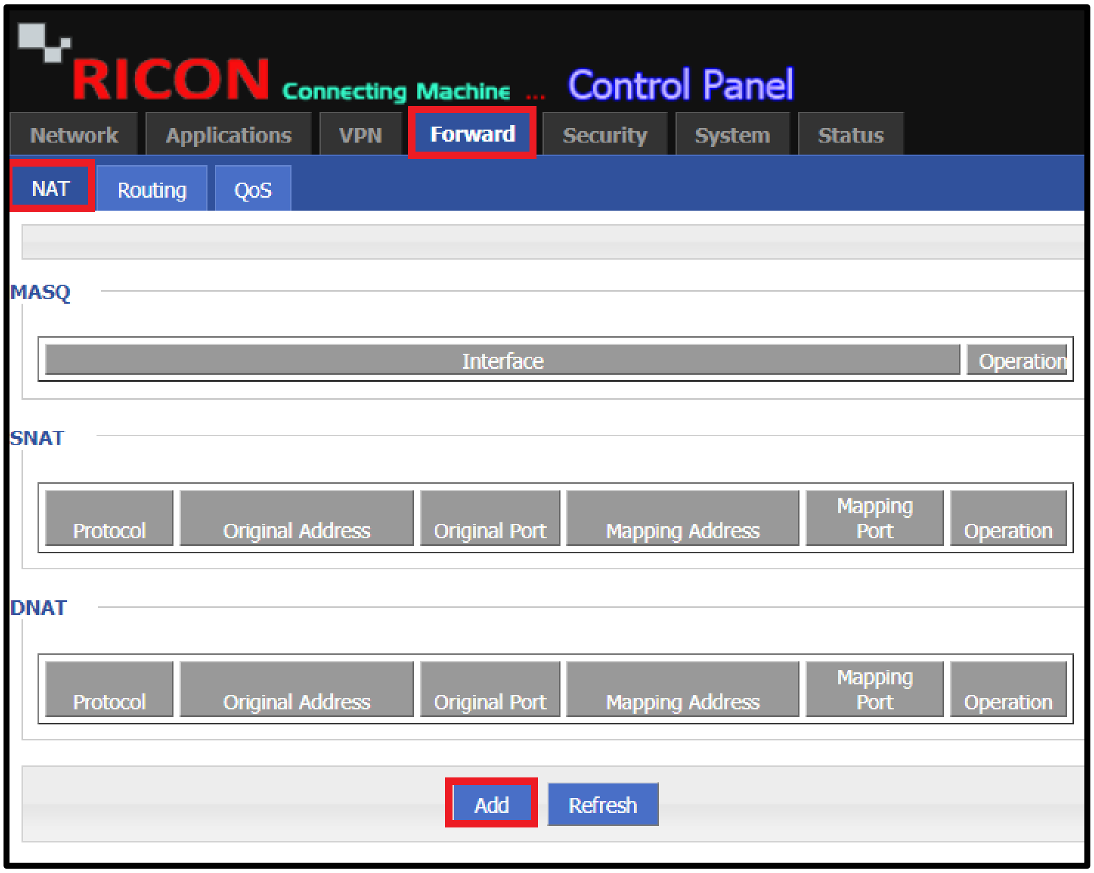
Network Address Translation (NAT) is a method used by routers to translate a public IP address (used on the Internet) into a private IP address (used on your local network). This is done for multiple purposes:

- to add security to the network by keeping the private IP addresses hidden from the Internet.

- to allow multiple devices to share a single IP address

To add NAT configuration to S9922M Series LTE router, proceed as follows.

FORWARD>NAT>ADD



MASQ

Interface	Operation

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

DNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation

Figure.24- Forward>NAT>Add

✓ **NAT Type;** DNAT, SNAT, MASQ.

- **DNAT;** Destination NAT changes the destination address of packets passing through the Router. It also offers the option to perform the port translation in the TCP/UDP headers. Destination NAT mainly used to redirect incoming packets with an external address or port destination to an internal IP address or port inside the network.

- **SNAT;** Source NAT is the translation of the source IP address of a packet leaving the Juniper Networks device. Source NAT is used to allow hosts with private IP addresses to access a public network.

- **MASQ;** The variant of NAT that most people use is known as IP masquerading. NAT type must be **MASQ** (Masquerade) if you want to allows a set of machines to invisibly access the internet.

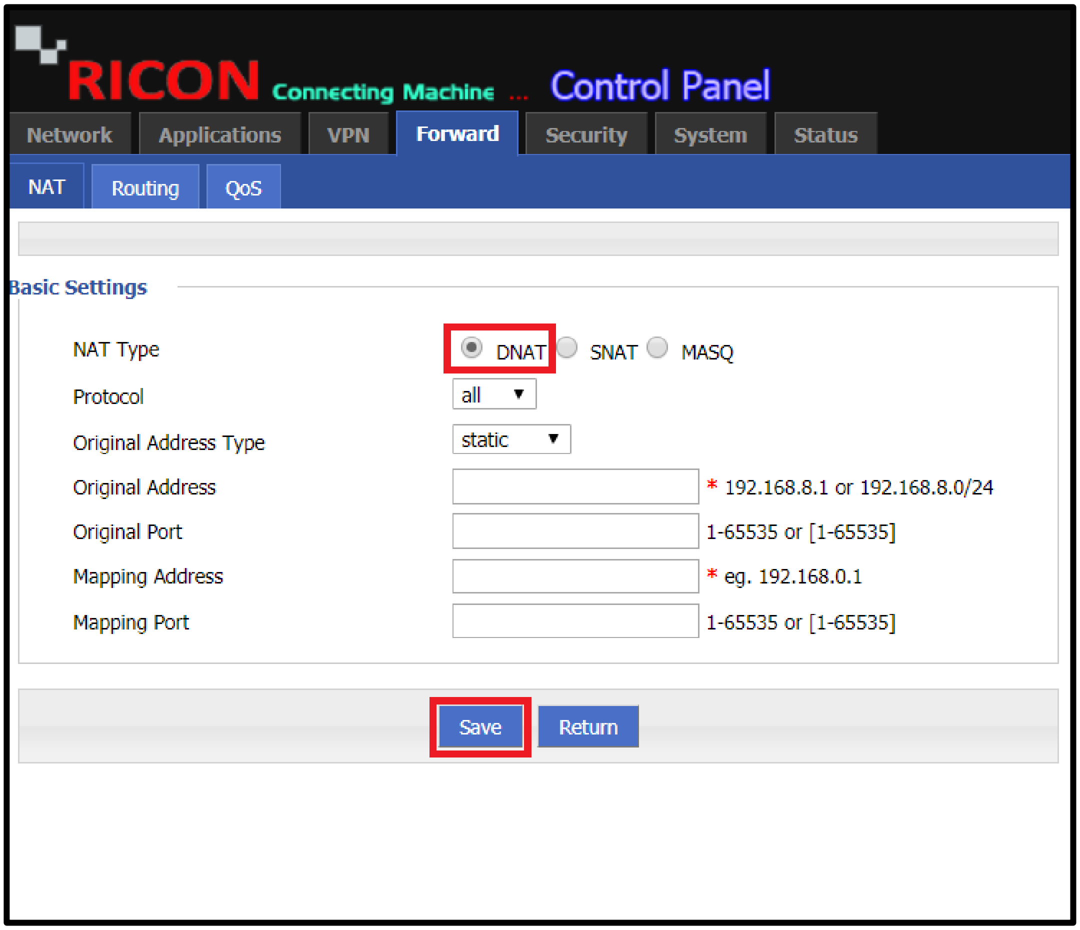
7.1.1 DNAT SETTING

DNAT is a technique in which multiple public Internet Protocol (IP) addresses are mapped and used with an internal or private IP address. If you want DNAT configuration;

- ✓ **Original Address Type;** Interface and Static.
  - If selected interface, there are interface line options in **br0, modem** and **eth1**. The desired WAN port must be selected in order for DNAT to go to the external network.

    Br0 is bridge mode, modem is cellular circuit, eth1 is means LAN/WAN port.
  - If you select static, the original address is displayed. The desired WAN IP must be entered here.
- ✓ **Mapping Address;** With DNAT, enter the IP block that we want to get out.
- ✓ Click the **Save** icon to finish.

FORWARD>NAT>DNAT



Basic Settings

NAT Type	● DNAT ○ SNAT ○ MASQ
Protocol	all ▼
Original Address Type	static ▼
Original Address	* 192.168.8.1 or 192.168.8.0/24
Original Port	1-65535 or [1-65535]
Mapping Address	* eg. 192.168.0.1
Mapping Port	1-65535 or [1-65535]

Figure.25- Forward>NAT>DNAT

7.1.2 SNAT SETTING

SNAT allows traffic from a private network to go out to the internet. Virtual machines launched on a private network can get to the internet by going through a gateway capable of performing SNAT.

✓ **Original Address;** The IP address or IP block that we want to connect to the external network with SNAT must be entered here.

✓ **Mapping Address Type;** Interface and Static.

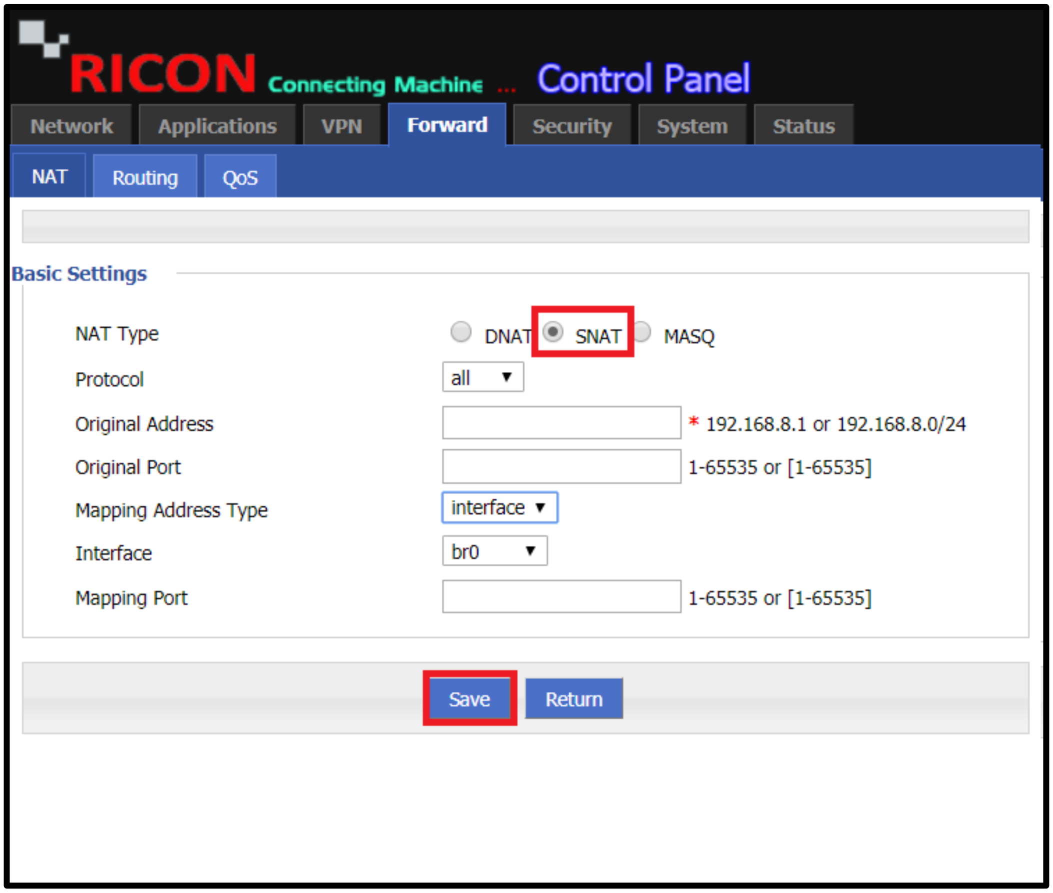
- If selected interface, there are interface line options in **br0, modem** and **eth1**. The desired WAN port must be selected in order for DNAT to go to the external network.

  Br0 is bridge mode, modem is cellular circuit, eth1 is means LAN/WAN port.

- If you select static, the original address is displayed. The desired WAN IP must be entered here.

✓ Click the **Save** icon to finish.

FORWARD>NAT>SNAT



NAT Type ○ DNAT ● SNAT ○ MASQ

Protocol: all

Original Address: * 192.168.8.1 or 192.168.8.0/24

Original Port: 1-65535 or [1-65535]

Mapping Address Type: interface

Interface: br0

Mapping Port: 1-65535 or [1-65535]

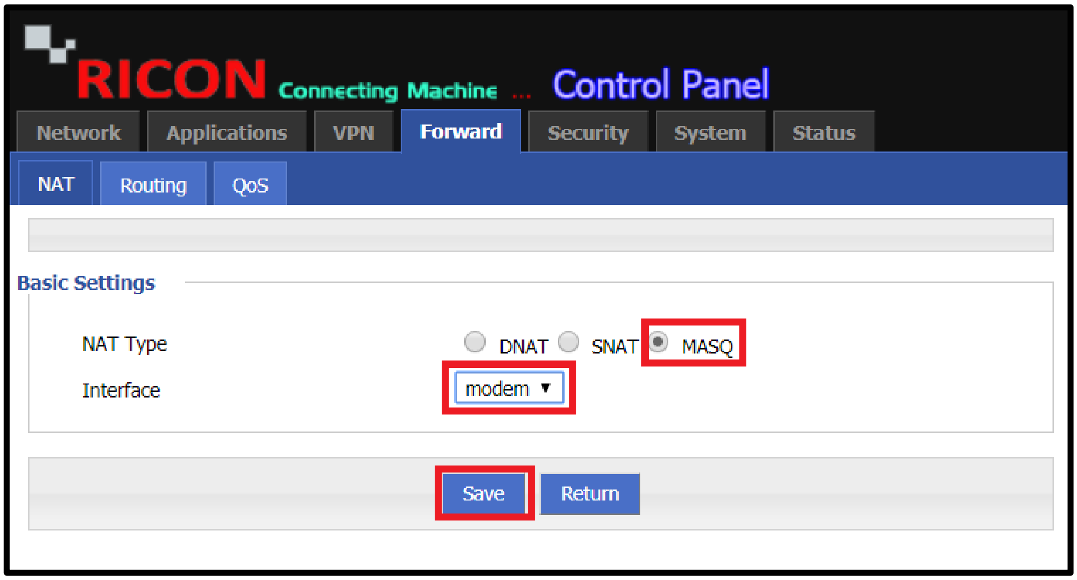
Figure.26- Forward>NAT>SNAT

7.3.3 MASQ SETTING

MASQ allows a set of machines to invisibly access the Internet via the MASQ gateway. To other machines on the Internet, the outgoing traffic will appear to be from the IP MASQ itself. In addition to the added functionality, IP Masquerade provides the foundation to create a heavily secured networking environment.

- ✓ **Interface;** There are 3 options **br0, modem** and **eth1**. The desired WAN port must be selected in order for MASQ to go to the external network.
- ✓ Click the **Save** icon to finish.

FORWARD>NAT>MASQ



NAT Type ○ DNAT ○ SNAT ● MASQ

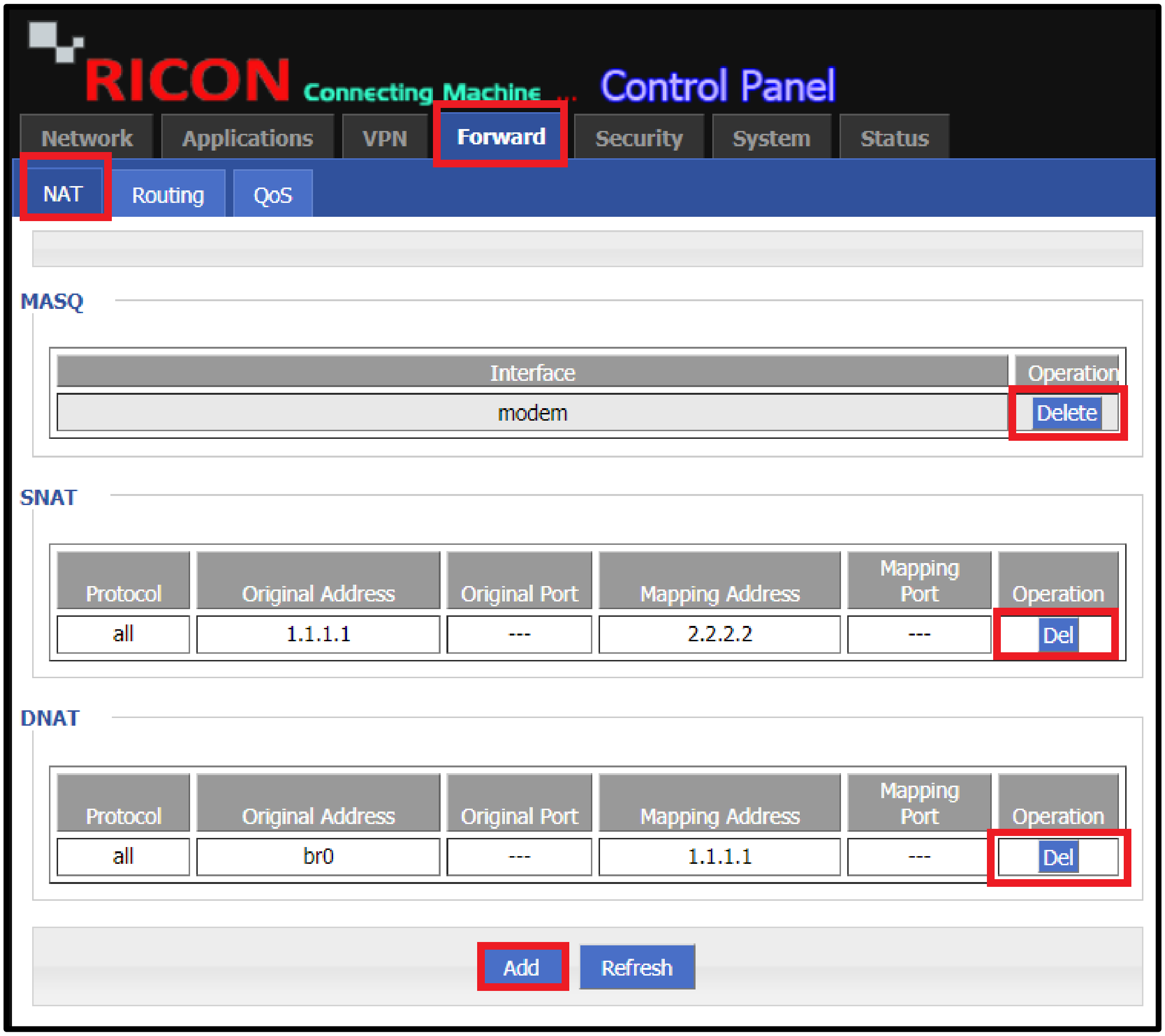
Interface modem ▼

Figure.27- Forward>NAT>MASQ

7.3.4 DELETE NAT SETTINGS

Follow the steps below to delete the current NAT configuration. Single click **Delete** icon corresponding to the NAT line you want to delete.

FORWARD>NAT>DELETE



MASQ

Interface	Operation
modem	Delete

SNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
all	1.1.1.1	---	2.2.2.2	---	Del

DNAT

Protocol	Original Address	Original Port	Mapping Address	Mapping Port	Operation
all	br0	---	1.1.1.1	---	Del

Figure.28- Forward>NAT>Delete

7.2 ROUTING CONFIGURATION

Router offers the option to change the default route and DNS.

✓ **Route Type;** Static Route, Policy Route.

- Static Route; Enter the LAN block of the device in the **Network** line.
- Policy Route;

✓ **Source Type;**

- If you select an interface as the source type, you must select the interface you want the gateway to access. These include the modem and eth1 (LAN /WAN port).
- If you select static IP as the source type, you must enter the IP block you want to enter into the gateway here.

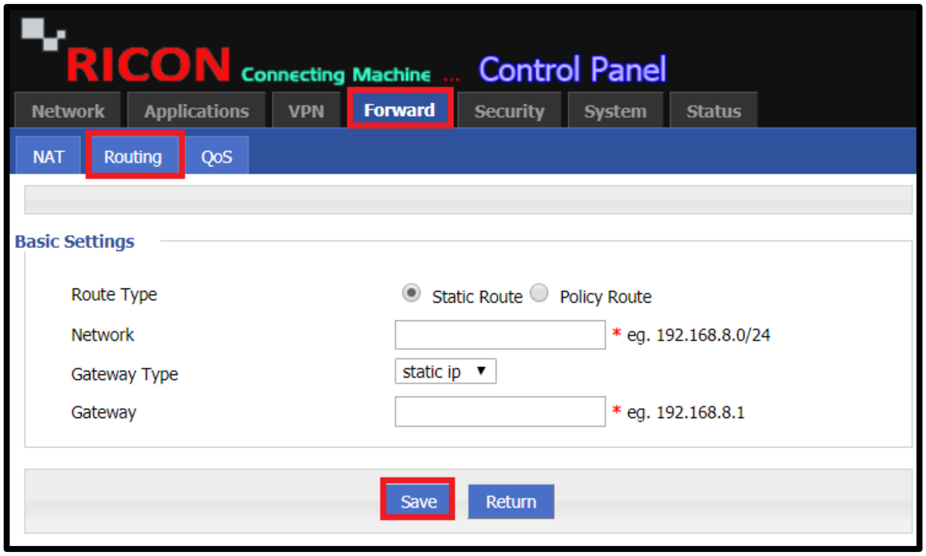
✓ **Gateway Type;**

- If you select Static IP as the gateway type, you must enter your gateway.
- If you select the interface, you must select the port of the device that accesses the external network. (br0, modem, eth1)

✓ **Priority;** Enter the priority of your route here.

✓ Click the **Save** icon to finish.

FORWARD>ROUTING



Basic Settings

Route Type	● Static Route ○ Policy Route
Network	* eg. 192.168.8.0/24
Gateway Type	static ip ▼
Gateway	* eg. 192.168.8.1

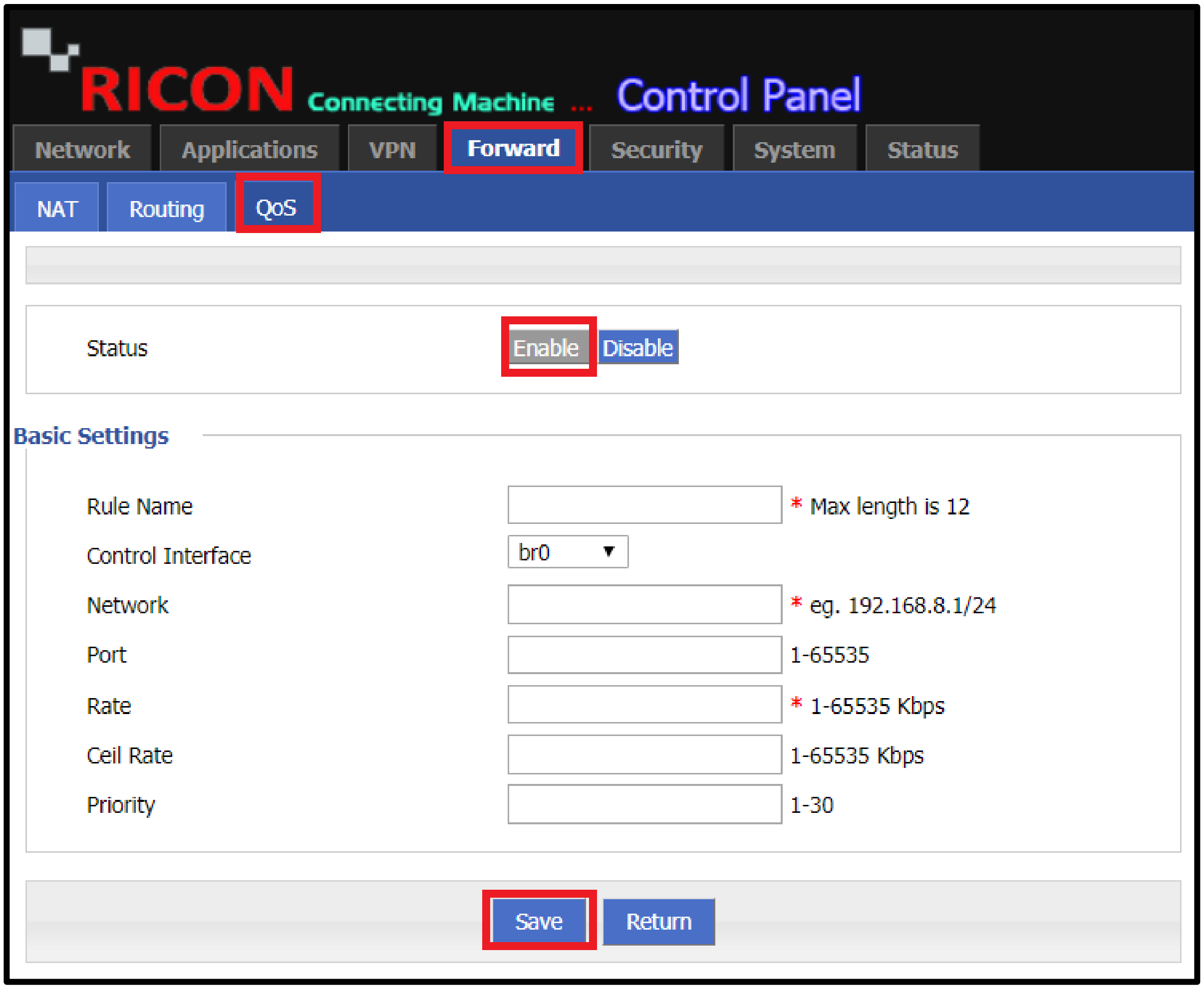
Figure.29- Forward>Routing

7.3 QOS CONFIGURATION

Quality of Service (QoS) is an advanced feature that prioritizes internet traffic for Ethernet LAN ports, specified MAC addresses or IP addresses to minimize the impact of busy bandwidth. Follow the steps below to reset the device and single click the icon.

- ✓ **Status;** Select enable for the Qos configuration to be active.
- ✓ **Rule Name;** Enter the rule name here.
- ✓ **Control Interface;** br0 and modem. Select the interface you want to limit.
- ✓ **Network;** Enter the IP you want to limit.
- ✓ **Port;** Enter the port information.
- ✓ **Rate;** Enter the limit you set.
- ✓ Click the **Save** icon to finish.

FORWARD>QOS>ADD



Status	Enable / Disable

Basic Settings

Rule Name		* Max length is 12
Control Interface	br0 ▼	
Network		* eg. 192.168.8.1/24
Port		1-65535
Rate		* 1-65535 Kbps
Ceil Rate		1-65535 Kbps
Priority		1-30

Figure.30- Forward>QOS>Add

8

8 SECURITY CONFIGURATION

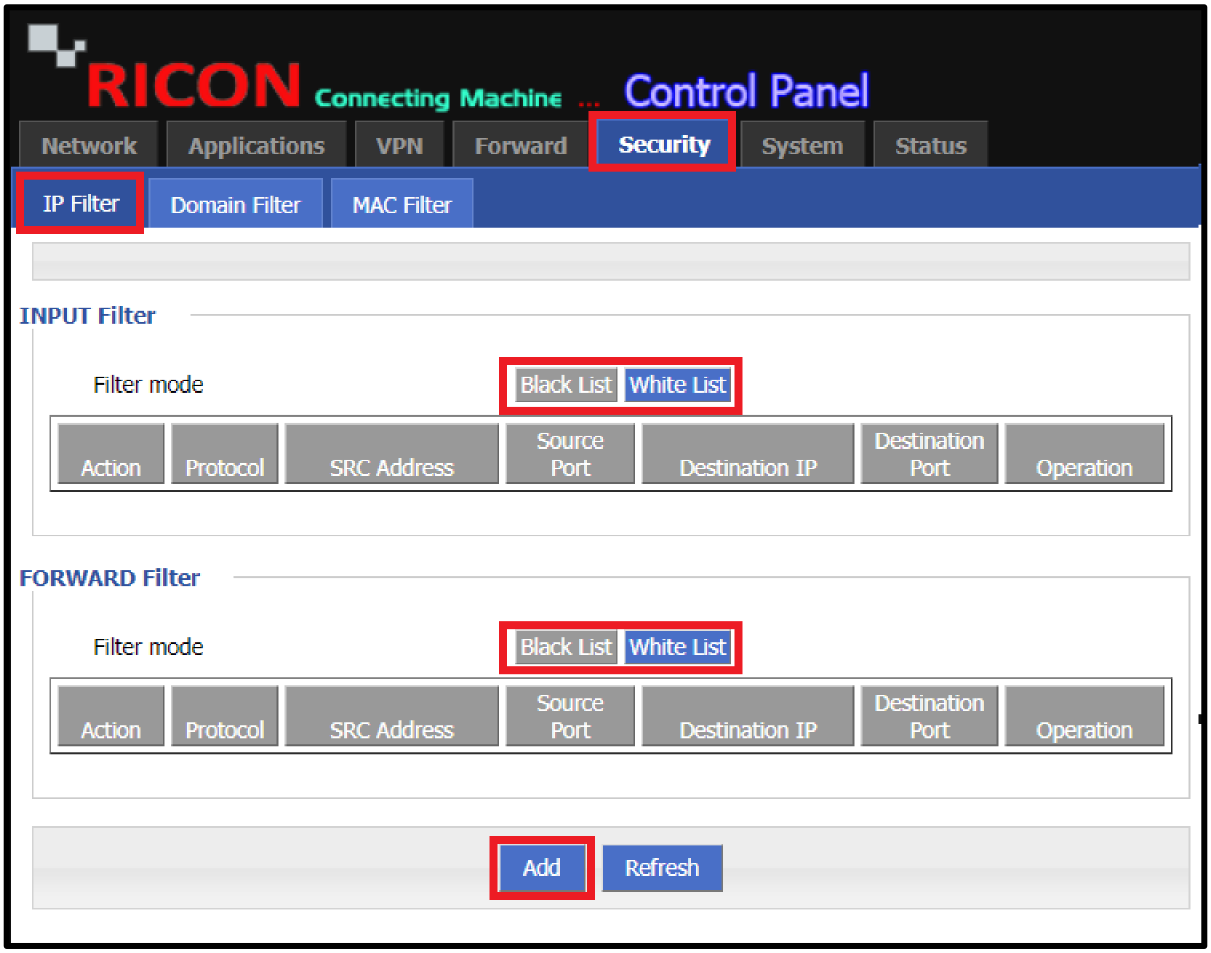
S9922M series LTE routers router can filter. Filtering allows you to block users that you don’t want to connect to the device or connect only the users you want. Blocking is done via IP address, domain name or MAC addresses. The S9922M series LTE routers router has 2 types of filtering lists. These are Black list and White list.

- ✓ **Black List;** the IP, domain or MAC addresses you entered can’t be connected to your device.
- ✓ **White List;** only the IP, domain or MAC addresses you entered can be connected to your device.

8.1 IP FILTER SETTİNGS

The advantage of IP filtering compared to other filtering is that it determines the IPs that a particular IP or block can or can’t reach. Follow the steps to IP filtering.

SECURİTY>IP FILTER>ADD



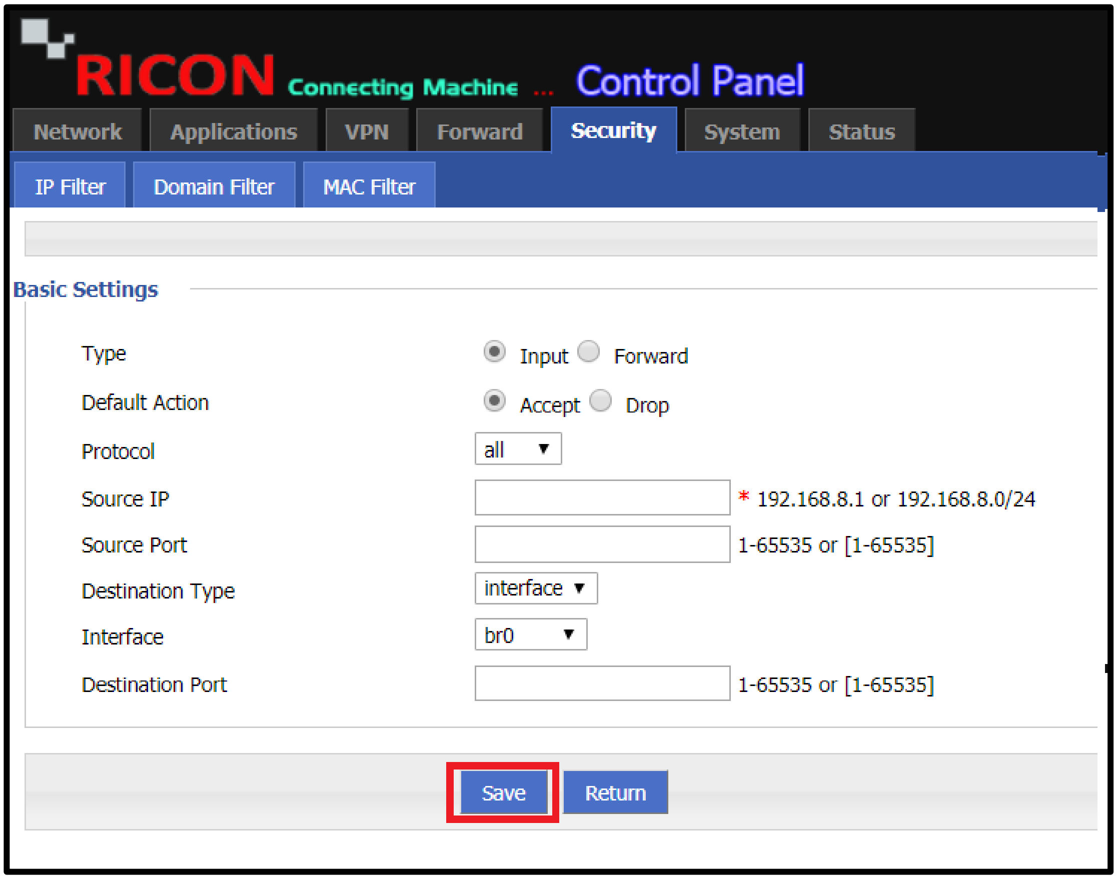
Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation

Figure.31- Security>IP Filter>Add

- ✓ **Type;**
    - **Input**; IP or blocks that are unwanted to access the router must be entered into INPUT
    - **Forward**; If static IP or blocks aren't required to access static IP or blocks, select FORWARD.
- ✓ **Default Action;**
    - **Accept**; If White List is used, Accept must be selected. With this method, only the IPs that you allow can connect to the router.
    - **Drop**; If Black List is used, Drop must be selected. So, filtered IPs can't access the router.
- ✓ **Mirror Rule;** If IP filtering is done with forward, the router offers the Mirror Rule option. This enable the entered filtering to be mutually valid if enable.
- ✓ **Source IP;** IP or block to be routed must be entered here.
- ✓ **Destination Type;** If filtering with INPUT, the router provides the destination type option. The target interface (br0, modem, eth1) should be selected or the IP can be blocked directly with ANY option.
- ✓ **Destination IP;** Router destinate IP if IP filtering with FORWARD options. You must enter the target IP to be accessed here.
- ✓ Click the **Save** icon to finish.

SECURİTY>IP FILTER>ADD

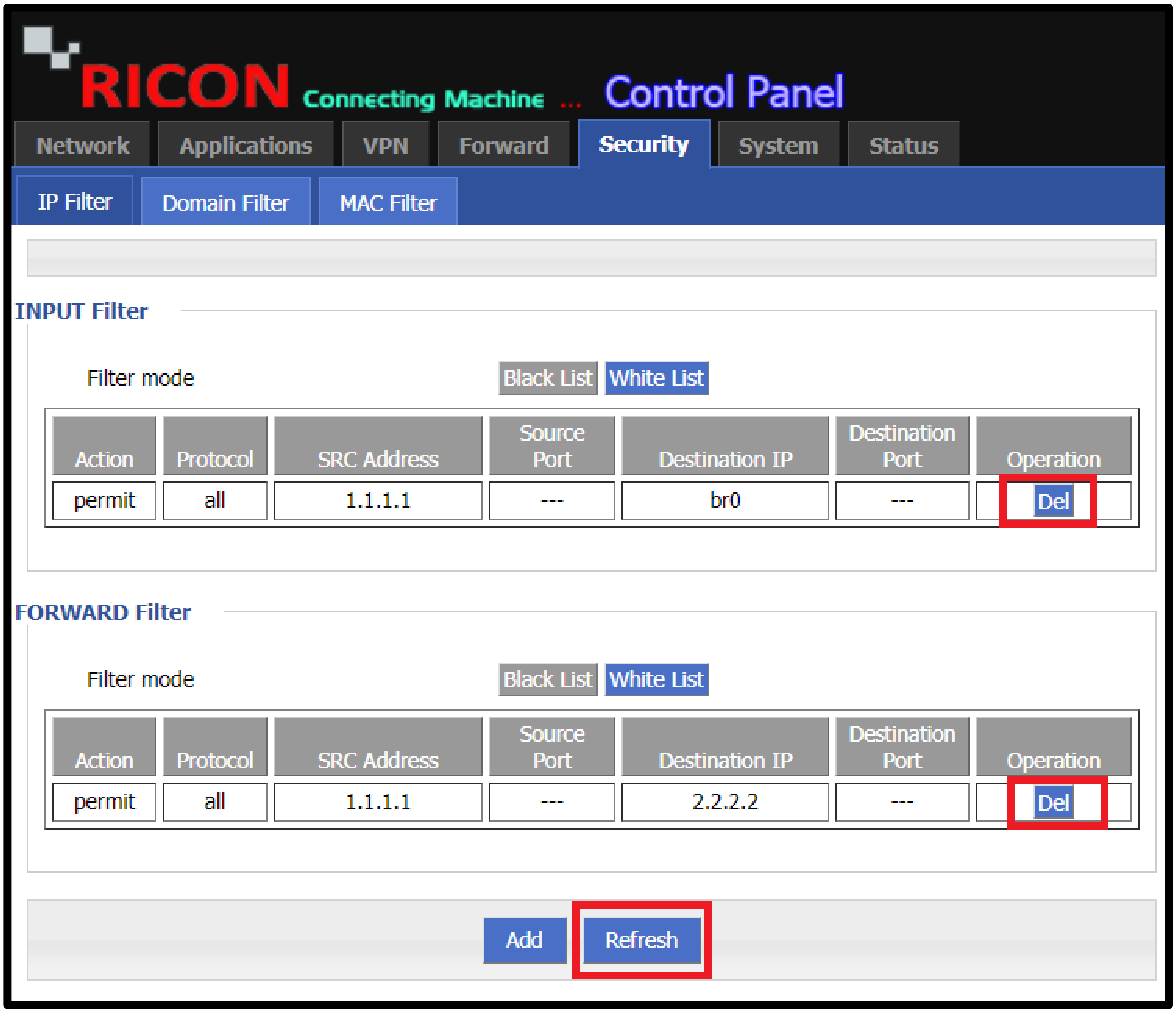


Basic Settings

Type	● Input ○ Forward
Default Action	● Accept ○ Drop
Protocol	all ▼
Source IP	* 192.168.8.1 or 192.168.8.0/24
Source Port	1-65535 or [1-65535]
Destination Type	interface ▼
Interface	br0 ▼
Destination Port	1-65535 or [1-65535]

Figure.32- Security>IP Filter>Add

If you want to delete IP filtering, you should come back to the IP filtering page and sing click **DEL** icon opposite to the desired filtering.



INPUT Filter

Filter mode: Black List | White List

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation
permit	all	1.1.1.1	---	br0	---	Del

FORWARD Filter

Filter mode: Black List | White List

Action	Protocol	SRC Address	Source Port	Destination IP	Destination Port	Operation
permit	all	1.1.1.1	---	2.2.2.2	---	Del

Figure.33- Security>IP Filter>Add

8.2 DOMAIN FILTER SETTİNGS

If you don’t want users or devices in a specific domain to access the S9922M series LTE routers, or if you only want devices the domain you specify. Follow the steps below.

SECURİTY>DOMAİN FILTER>ADD

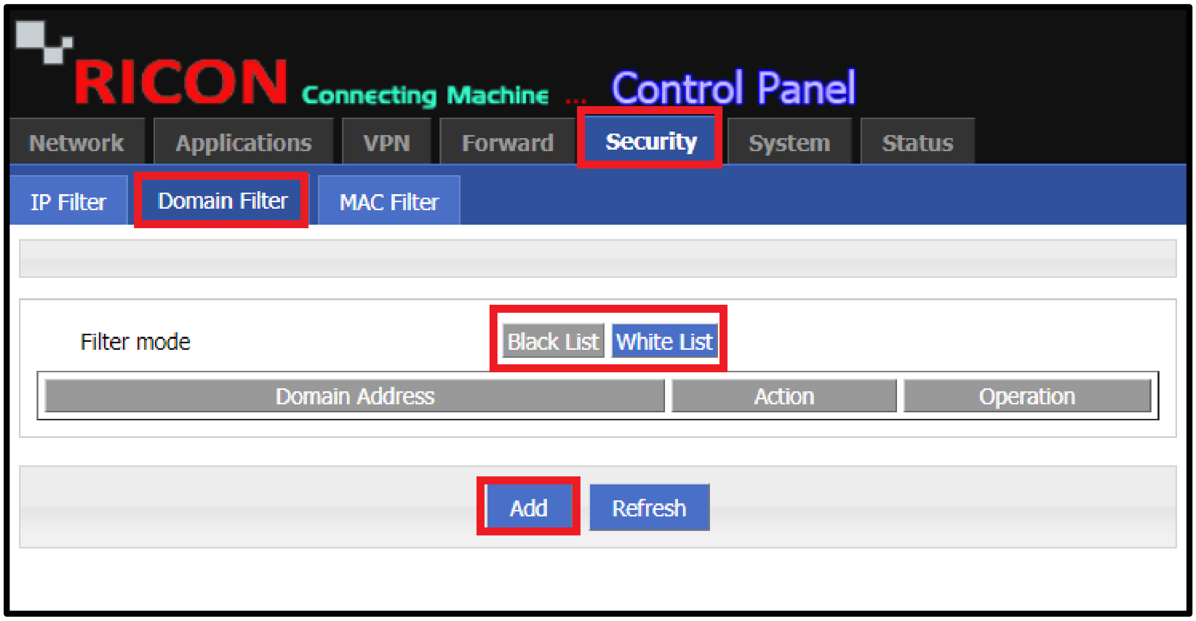
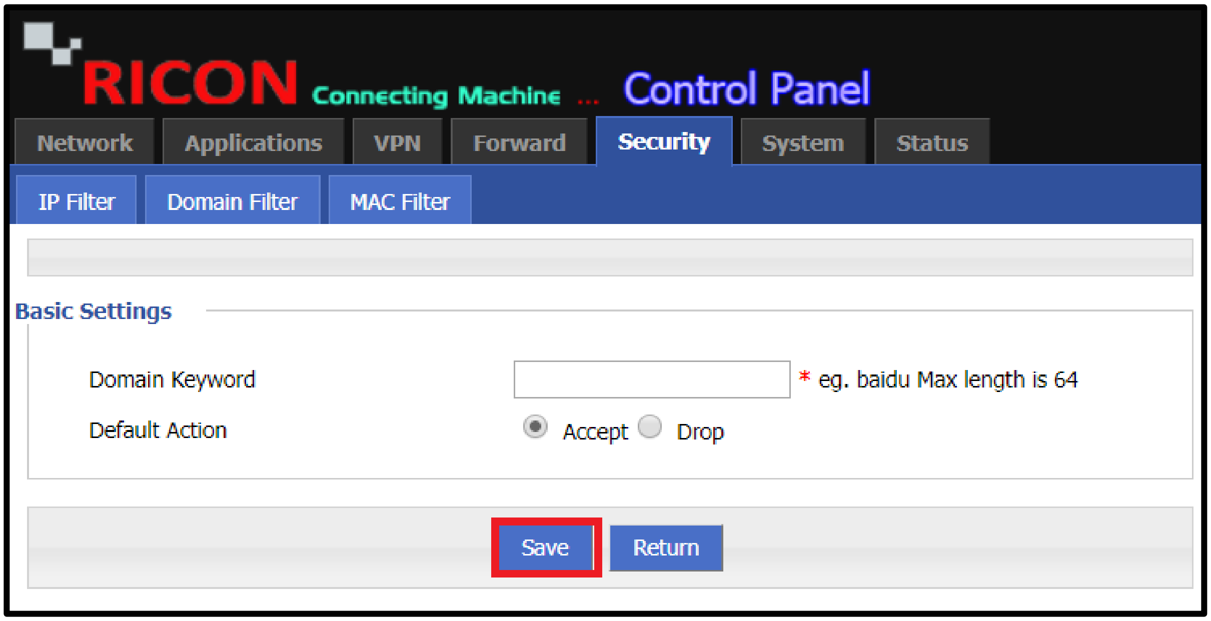


Figure.34- Security>Domain Filter>Add

- ✓ **Domain Keyword;** Domain name must be entered here.
- ✓ **Default Action;**
  - **Accept**; If White List is used, Accept must be selected. With this method, only the domains that you allow can connect to the router.
  - **Drop**; If Black List is used, Drop must be selected. So, filtered domain can’t access the router.
- ✓ Click the **Save** icon to finish.

SECURITY>DOMAIN FILTER>ADD



Basic Settings

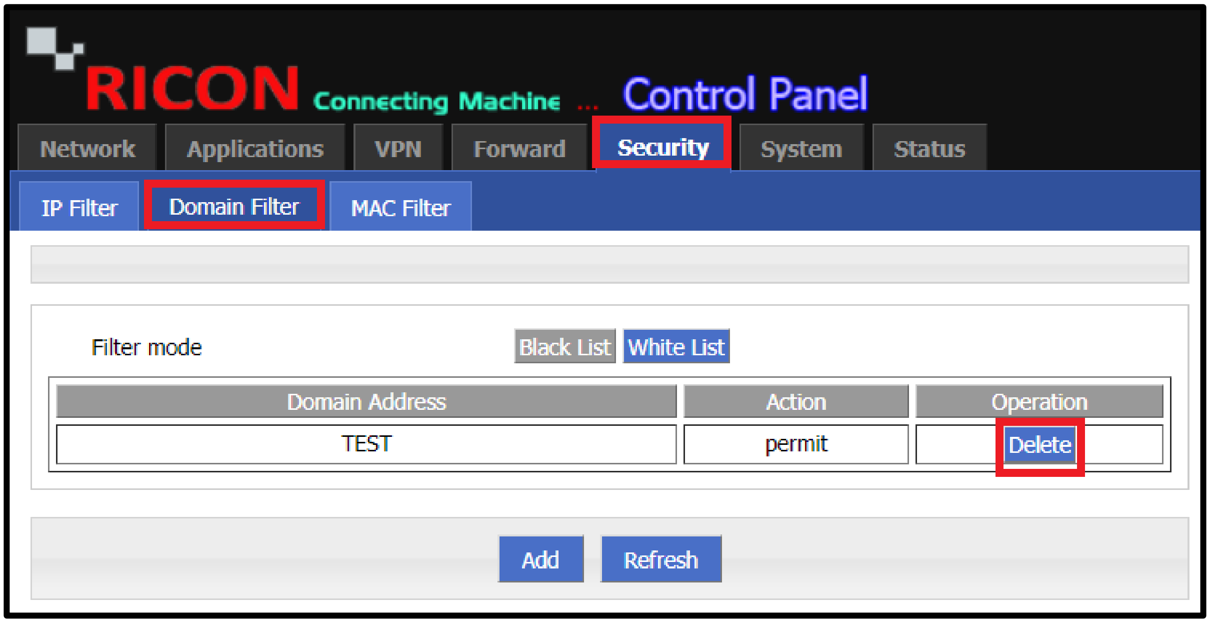
Domain Keyword * eg. baidu Max length is 64

Default Action ● Accept ○ Drop

Figure.35- Security>Domain Filter>Add

If you want to delete domain filtering, you should come back to the domain filtering page and sing click **Delete** icon opposite to the desired filtering.

SECURITY>DOMAIN FILTER>ADD



Filter mode Black List White List

Domain Address	Action	Operation
TEST	permit	Delete

Figure.36- Security>Domain Filter>Add

8.3 MAC FILTER SETTİNGS

Follow the steps for mac filtering.

SECURITY>MAC FILTER>ADD

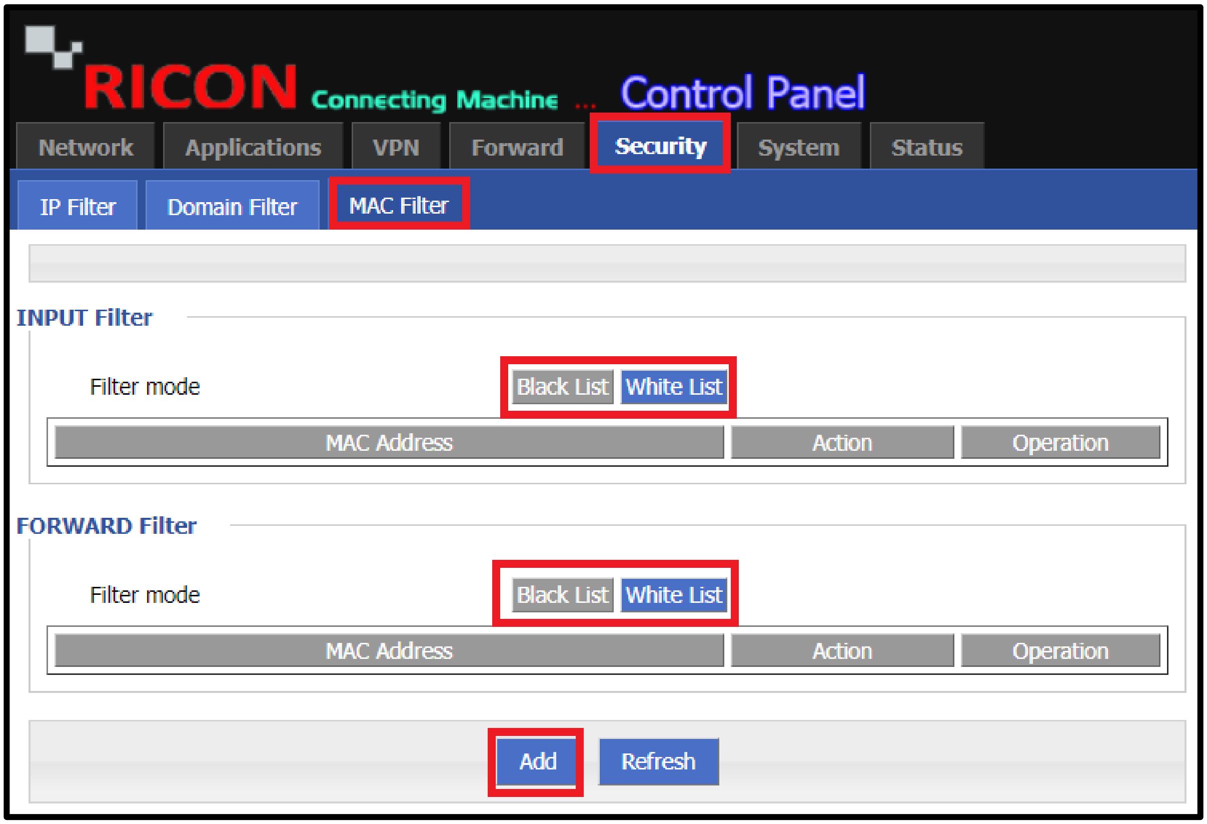
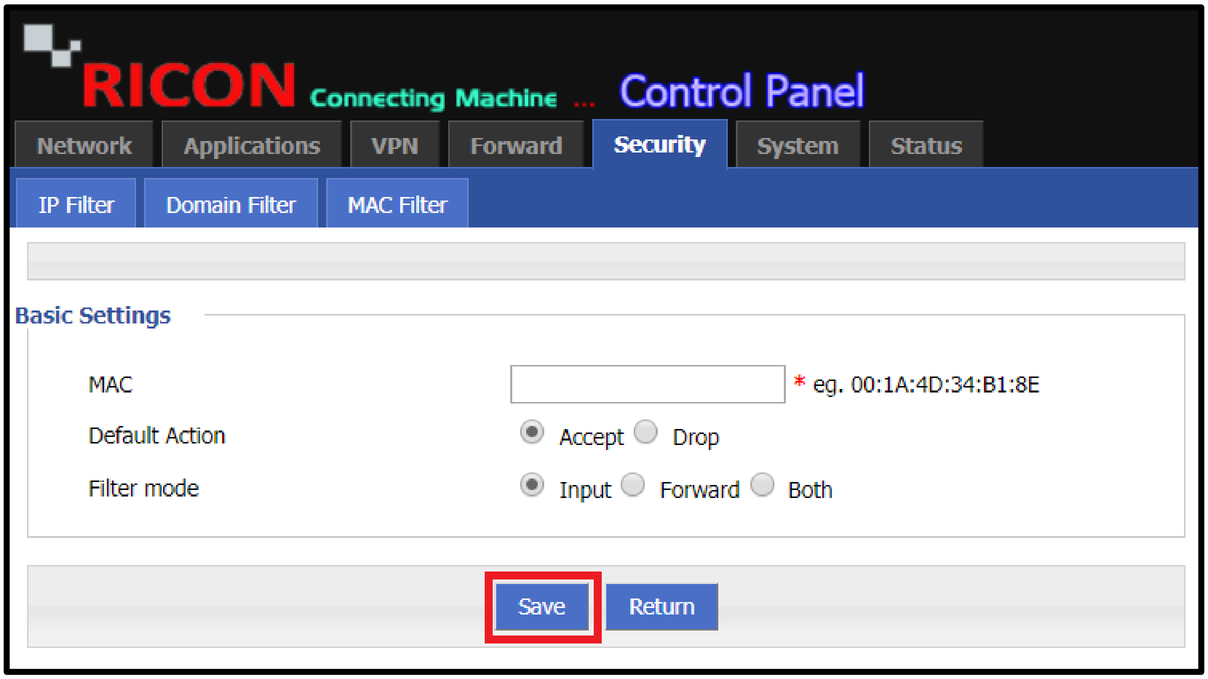


Figure.37- Security>MAC Filter>Add

- ✓ **MAC;** Enter the MAC address you specified here.
- ✓ **Default Action;**
  - **Accept**; If White List is used, Accept must be selected. With this method, only the MAC that you allow can connect to the router.
  - **Drop**; If Black List is used, Drop must be selected. So, filtered MAC can't access the router.
- ✓ **Filter mode;**
  - **Input**; MAC that are unwanted to access the router must be entered into INPUT
  - **Forward**; If you don't want the MAC address you have entered to access the external network but the internal network, FORWARD should be selected.
- ✓ Click the **Save** icon to finish.

SECURITY>MAC FILTER>ADD



MAC * eg. 00:1A:4D:34:B1:8E

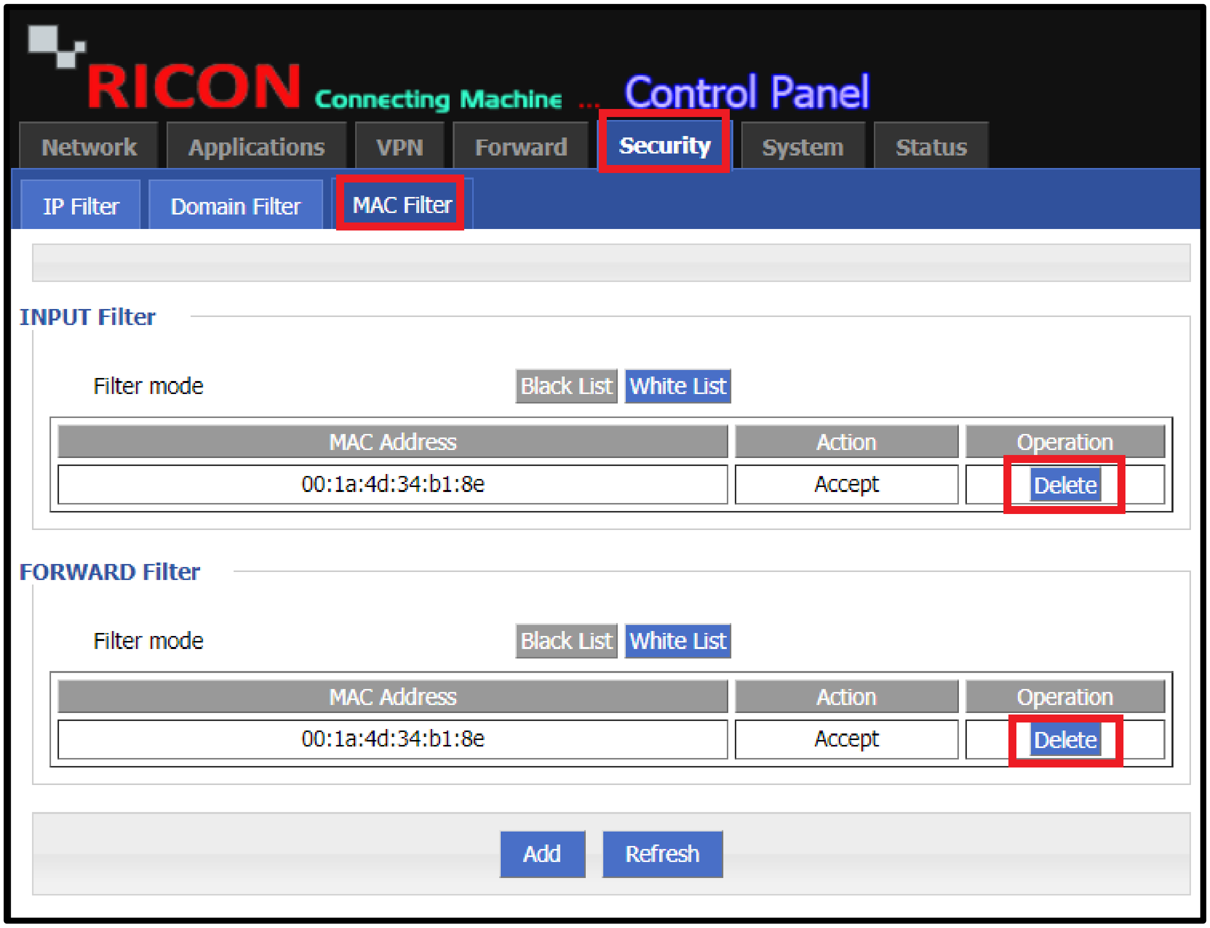
Default Action ● Accept ○ Drop

Filter mode ● Input ○ Forward ○ Both

Figure.38- Security>MAC Filter>Add

If you want to delete MAC filtering, you should come back to the MAC filtering page and sing click **Delete** icon opposite to the desired filtering.

SECURITY > MAC FILTER > ADD



INPUT Filter

Filter mode

MAC Address	Action	Operation
00:1a:4d:34:b1:8e	Accept	Delete

FORWARD Filter

Filter mode

MAC Address	Action	Operation
00:1a:4d:34:b1:8e	Accept	Delete

Figure.39- Security>MAC Filter>Add

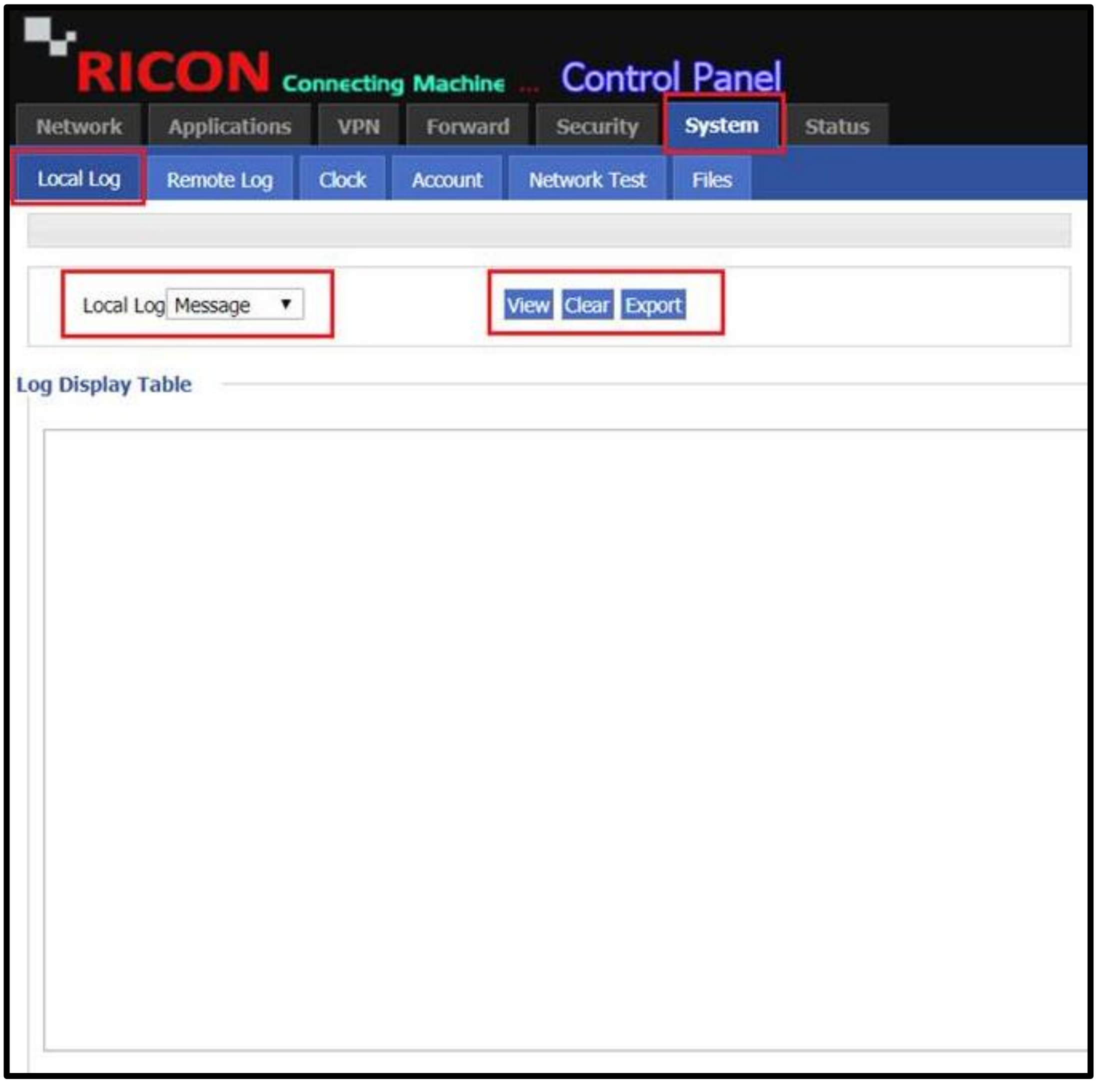
9 SYSTEM SETTINGS

9.1 LOCAL LOG SETTİNGS

You can monitor the current activities of the router through the log. When you set up a new system, you follow up by log tracking.

- ✓ Choose System> Local Log
- ✓ You can **View** instant Message Logs
- ✓ To clear the old log and see the current logs, select **Clear**.
- ✓ To export logs, select **Export** after viewing.

SYSTEM > LOCAL LOG



Local Log Message

Figure.40- System>Local Log

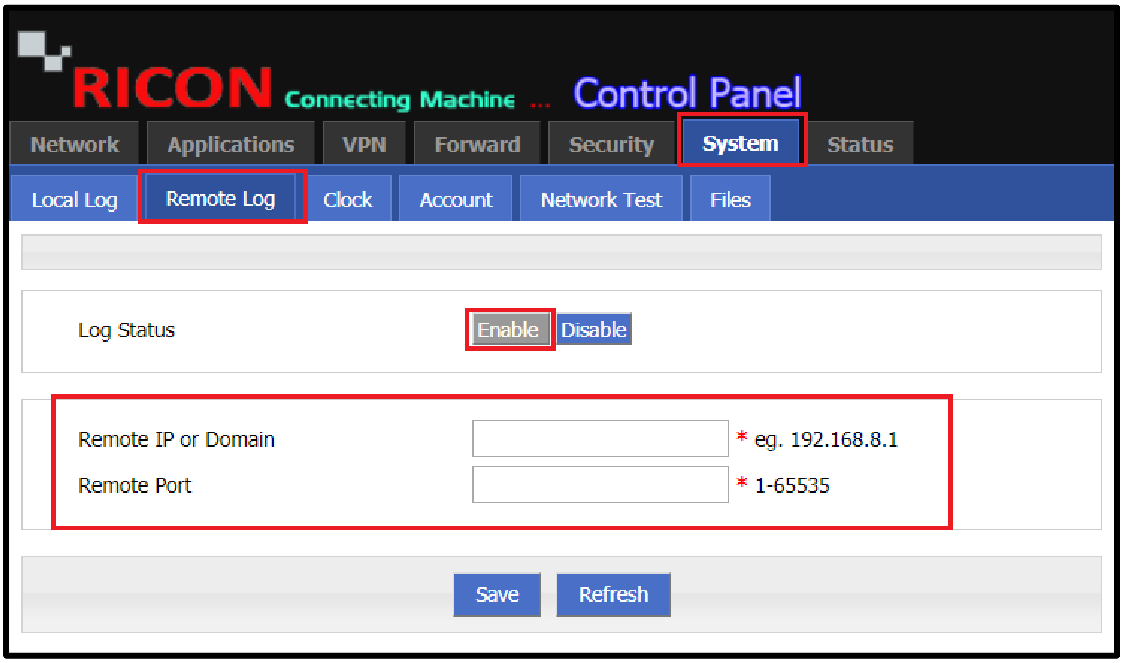
9.2 REMOTE LOG SETTING

The current status of the router can be monitored instantly from a remote device. The device you are monitoring must comply with this specification. Can be monitored directly by a domain.

To remotely monitor, follow these steps;

- ✓ Choose System>Remote Log
- ✓ **Log Status** must selected **Enable**
- ✓ Enter your **Remote IP or Domain**'s IP
- ✓ Enter your Device's **Remote Port**
- ✓ Click the **Save** icon to finish.

SYSTEM>REMOTE LOG



Log Status: Enable | Disable

Remote IP or Domain: * eg. 192.168.8.1

Remote Port: * 1-65535

Figure.41- System>Remote Log

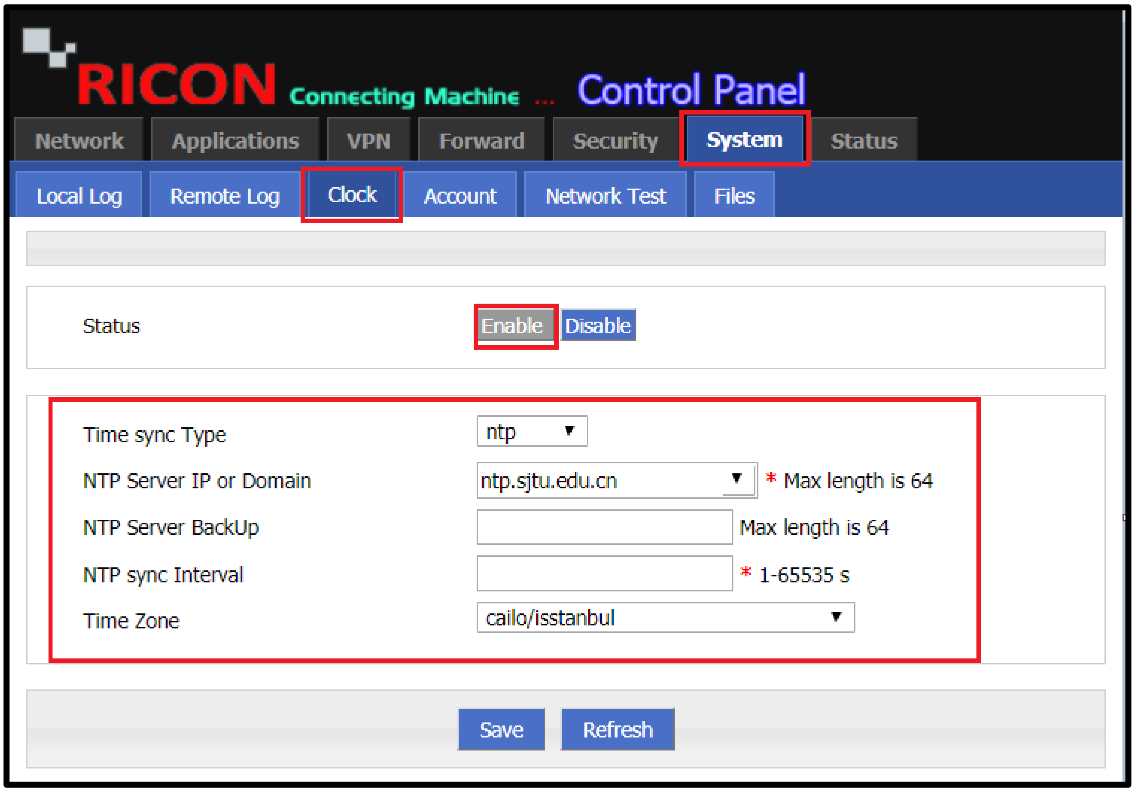
9.3 SYSTEM CLOCK SETTING

NTP is a sequential time distribution system with redundant capacity. Measures algorithms and delays on the network and on the target machine. Using these techniques, you can synchronize clocks in milliseconds.

You can use one of the generally accepted NTP servers, or if you own an NTP server, you can back up its information.

- ✓ Choose System>Clock
- ✓ **Status** must selected **Enable**
- ✓ Select the **Time synchronization Type** is **ntp**
- ✓ Select the **NTP Server IP or Domain**; navobs1.gatech.edu, clock.fmt.he.net, ntp.sjtu.edu.cn, clock.via.net, ntp.nasa.gov etc.
- ✓ Enter the **NTP Server BackUp** IP or Domain information
- ✓ Enter the **NTP sync Interval** value
- ✓ Choose your **Time Zone**
- ✓ Click the **Save** icon.

SYSTEM>CLOCK>NTP



Status: Enable

Time sync Type: ntp

NTP Server IP or Domain: ntp.sjtu.edu.cn * Max length is 64

NTP Server BackUp: Max length is 64

NTP sync Interval: * 1-65535 s

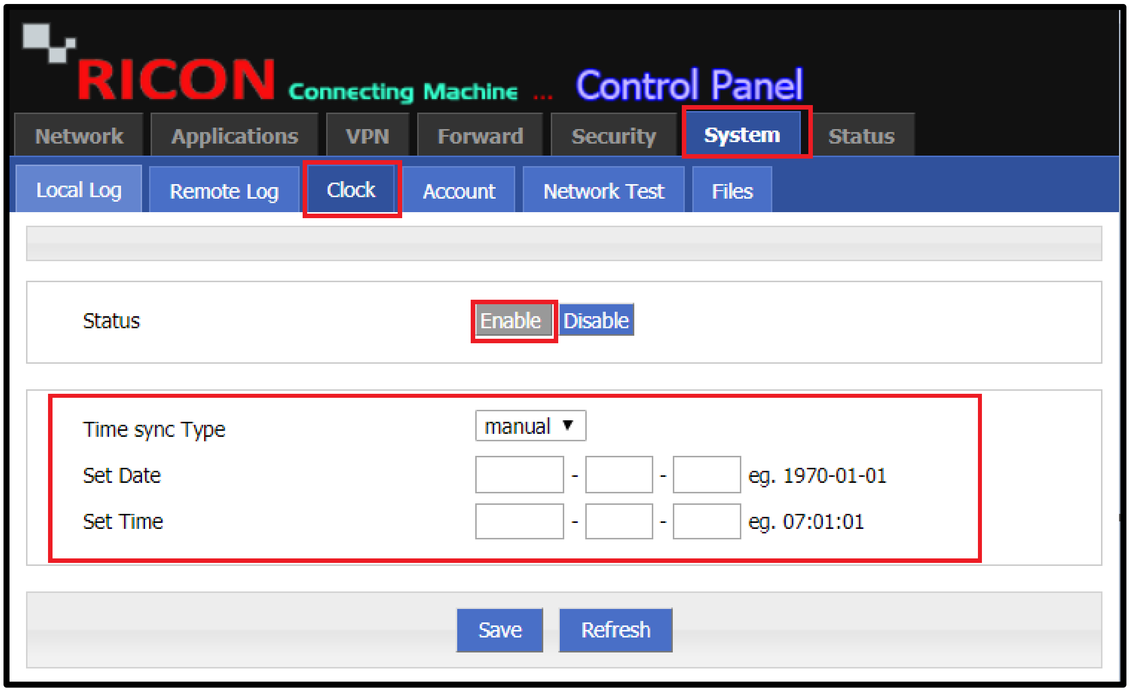
Time Zone: cailo/isstanbul

Figure.42- System>Clock>ntp

You can also do it yourself manually. It is important to enter the correct time to monitor the router.

- ✓ Choose System>Clock
- ✓ **Status** must selected **Enable**
- ✓ Select the **Time synchronization Type** is **manual**
- ✓ Enter the current date for your region in **Set Date**
- ✓ Enter the current time for your region in **Set Time**
- ✓ Click the **Save** icon.

SYSTEM>CLOCK>MANUAL



Status [✓ Enable] Disable

Time sync Type manual ▾

Set Date ___ - ___ - ___ eg. 1970-01-01

Set Time ___ - ___ - ___ eg. 07:01:01

Figure.43- System>Clock>Manual

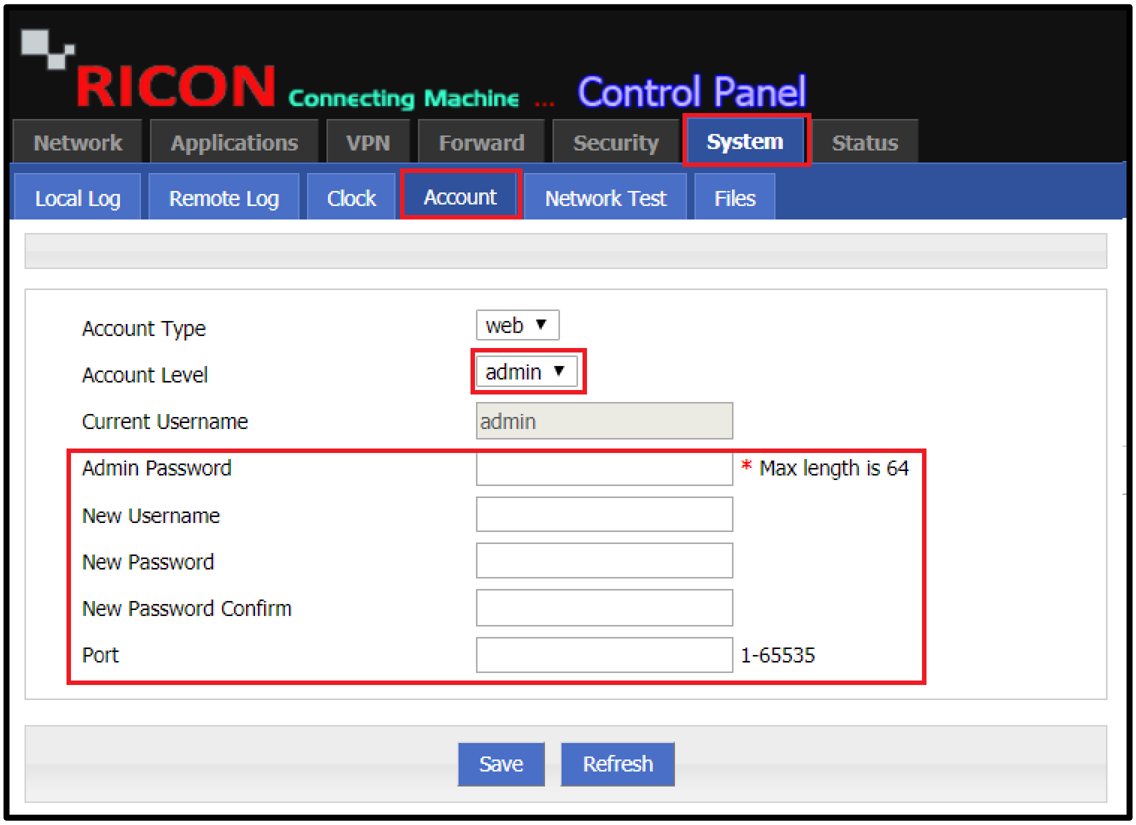
9.4 ACCOUNT SETTING

Router login password is important for security protocol. You can change your username and password for security when logging in to your router.

If you wish, you can define a guest user and restrict authorization with the help of port definition.

- ✓ Choose System>Account
- ✓ Select **Account Level** to define admin or guest
- ✓ Enter your current **Admin Password**
- ✓ Enter your new **New Username**
- ✓ Enter your new **New Password**
- ✓ Enter your reach **Port** (80, 8080 etc.)
- ✓ Click the **Save** icon to finish.

SYSTEM>ACCOUNT



Account Type	web ▼
Account Level	admin ▼
Current Username	admin
Admin Password	* Max length is 64
New Username	
New Password	
New Password Confirm	
Port	1-65535

Figure.44- System>Account

9.5 NETWORK TEST

You need to test the structure you configured you do it through ping. In case of problems, you can test the path of the package with trace to make troubleshooting easier. You can perform network tests from the router interface.

Follow the steps below to perform your network tests;

- ✓ Choose System>Network Test
- ✓ Enter the IP you want to ping in the **Destination box**
- ✓ Click the **Ping** and wait

SYSTEM>NETWORK TEST

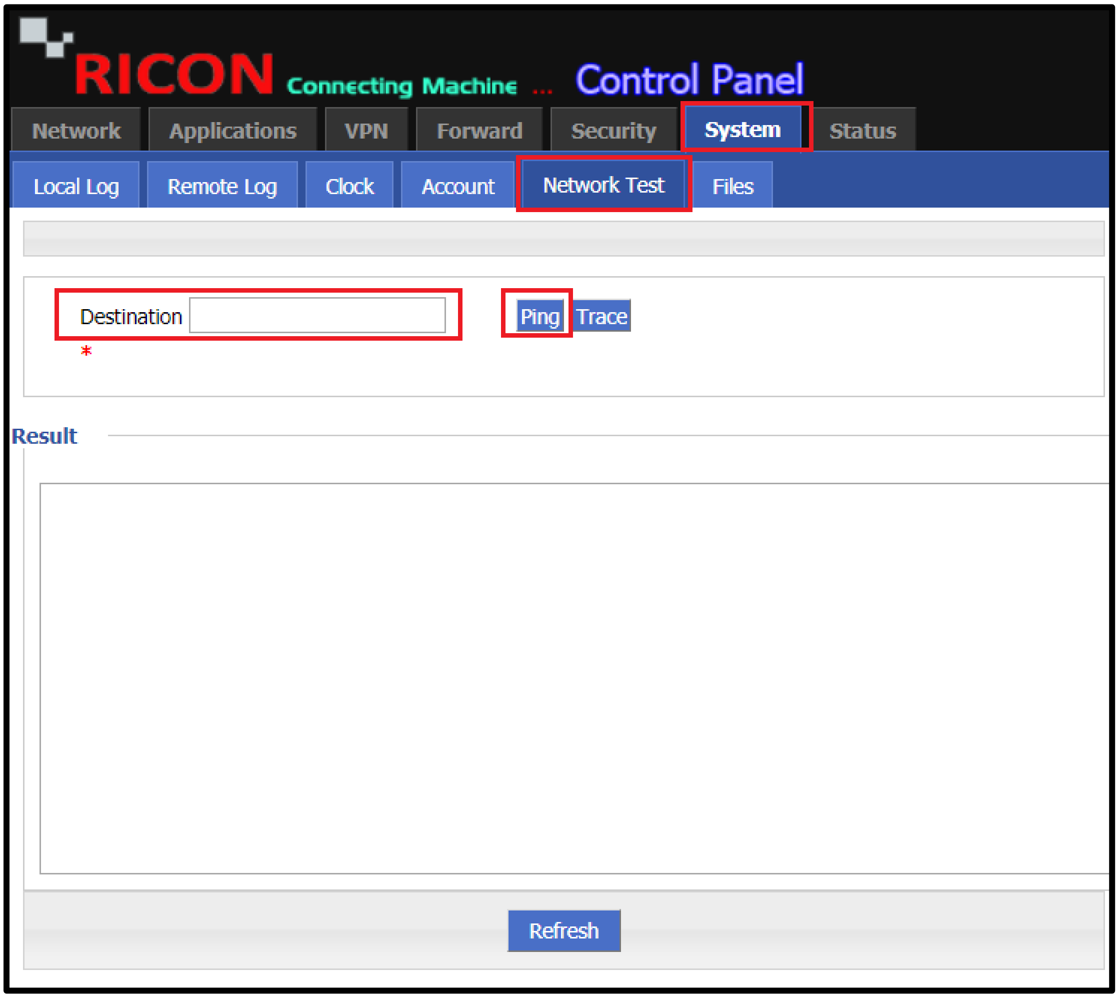


Figure.45- System>Network Test

- ✓ Choose System>Network Test
- ✓ Enter the IP you want to trace in the **Destination box**
- ✓ Click the **Trace** and wait

SYSTEM>NETWORK TEST

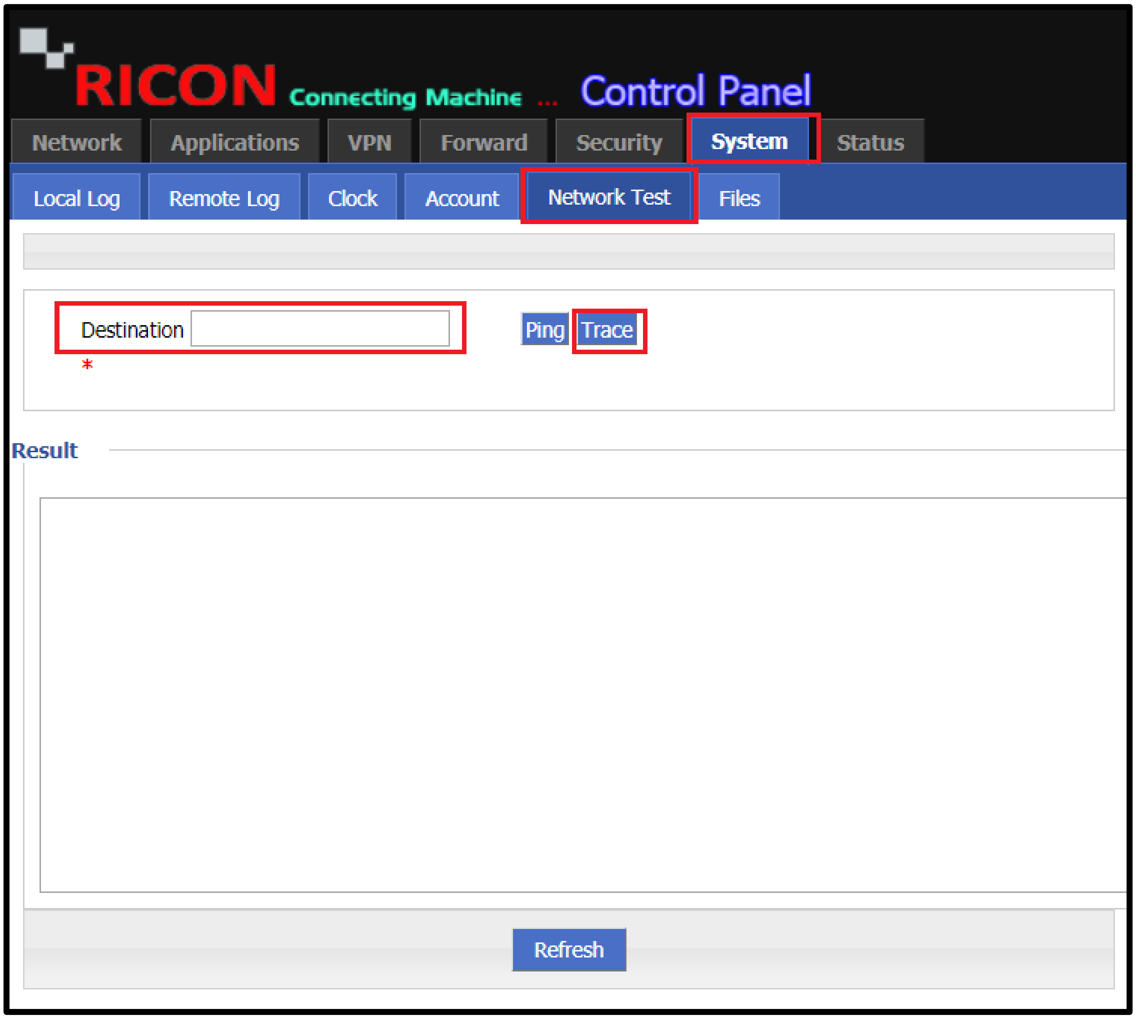


Figure.46- System>Network Test

NOTE: *If your test results log as follows, be sure to your configuration.*

5 packets transmitted, 0 packets received, 100% packet loss

9.6 FILES SETTINGS

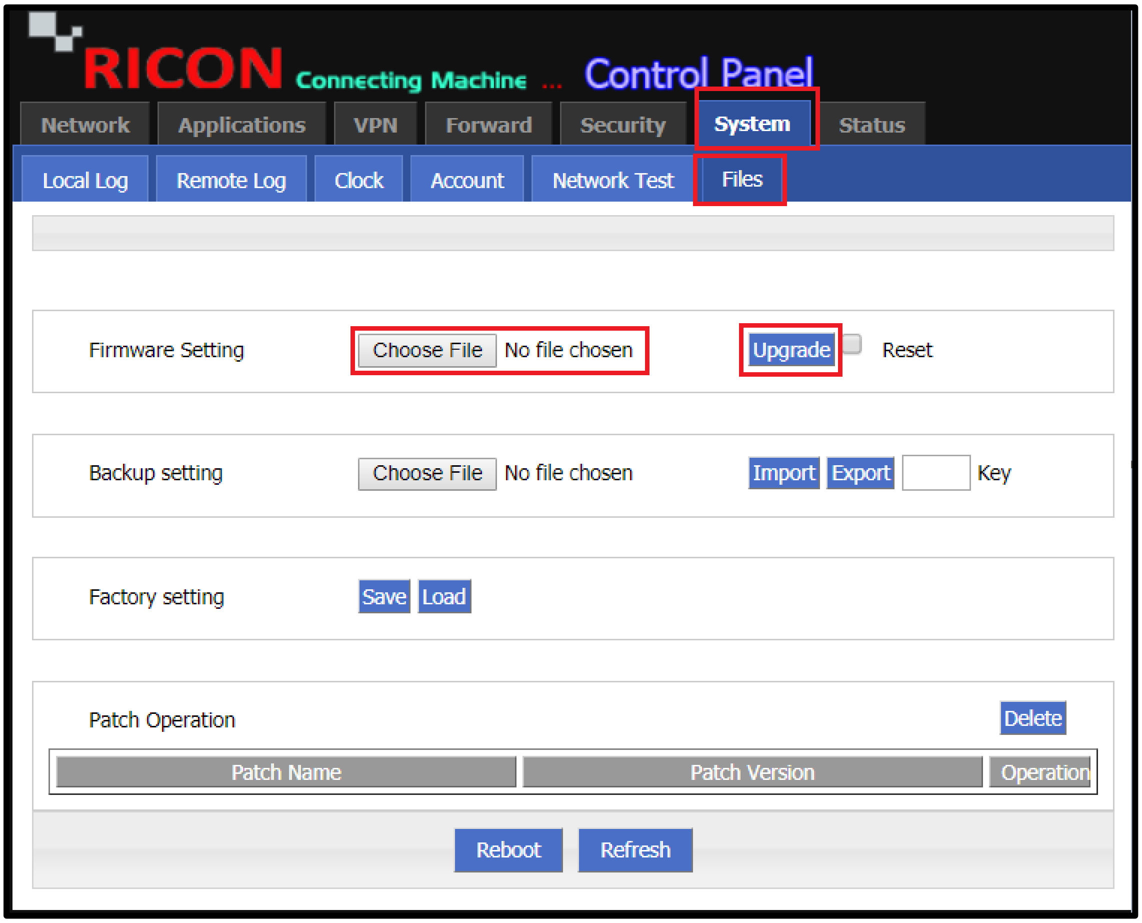
9.6.1 Firmware SETTINGS

The firmware is the program that controls the operation and functionality of the router. It is the combination of software and hardware that has program code and data stored in it in order for the device to function.

Follow these steps to install/upgrade the software that is current or appropriate for your configuration.

- ✓ Choose System>Files
- ✓ Select the firmware file you want to upgrade by clicking **Choose File**
- ✓ If you want the router to reset itself after the upgrade, click the **Reset box**
- ✓ To Upgrade the firmware file of your choice, click **Upgrade**

SYSTEM>FILES



Firmware Setting Choose File No file chosen Upgrade □ Reset

Backup setting Choose File No file chosen Import Export Key

Factory setting Save Load

Patch Operation

Figure.47- System>Files

9.6.2 BACKUP SETTINGS

To export an CLI file that contains a router and platform configuration, use the configuration export feature and export it to your local computer.

- ✓ Choose System>Files
- ✓ Select the field where you want to save the configuration file by clicking **Choose File**
- ✓ To export a configuration file to your local computer, click **Export**

SYSTEM>FILES

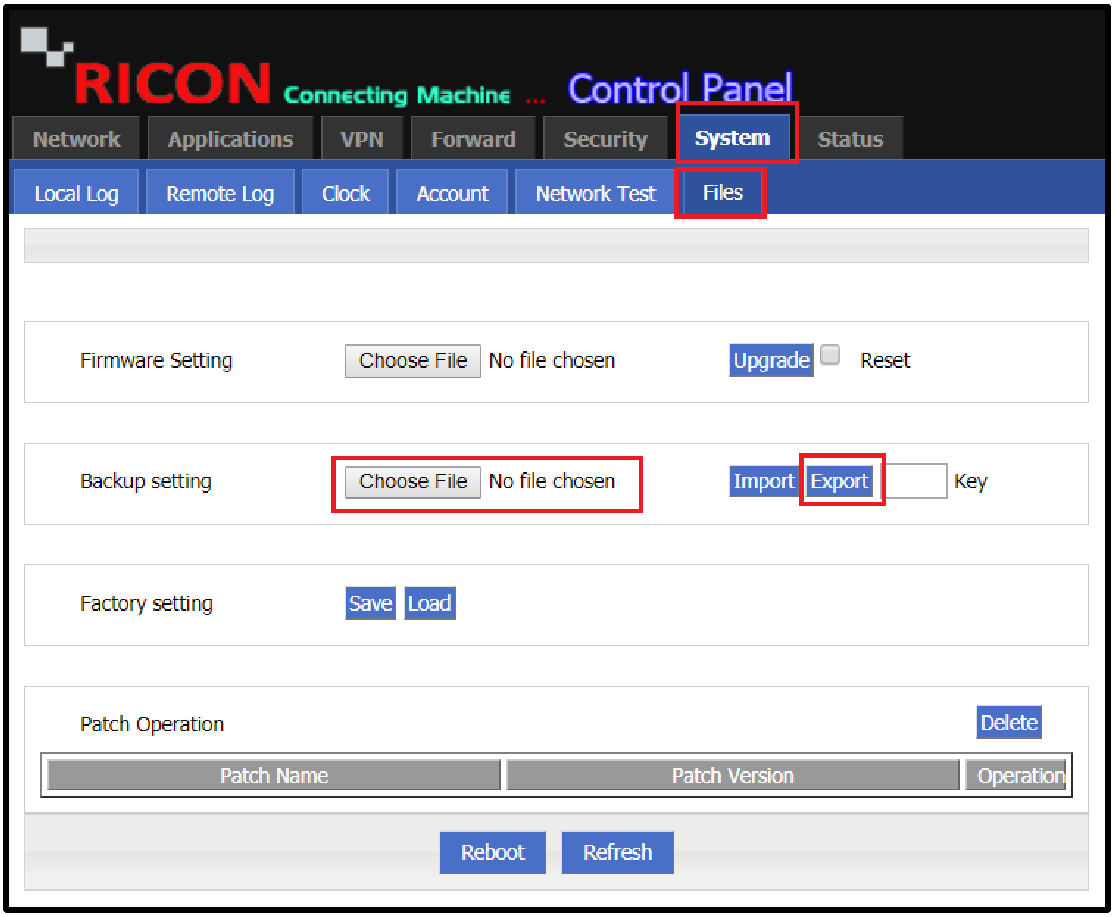


Figure.48- System>Files

To import a CLI file that contains a router and platform configuration to the router, use the configuration import feature and upload the file from your local computer to your router.

- ✓ Choose System>Files
- ✓ Select the configuration file you want to upload by clicking **Choose File**
- ✓ To import a configuration file on your local computer to the router, click **Import**

SYSTEM>FILES

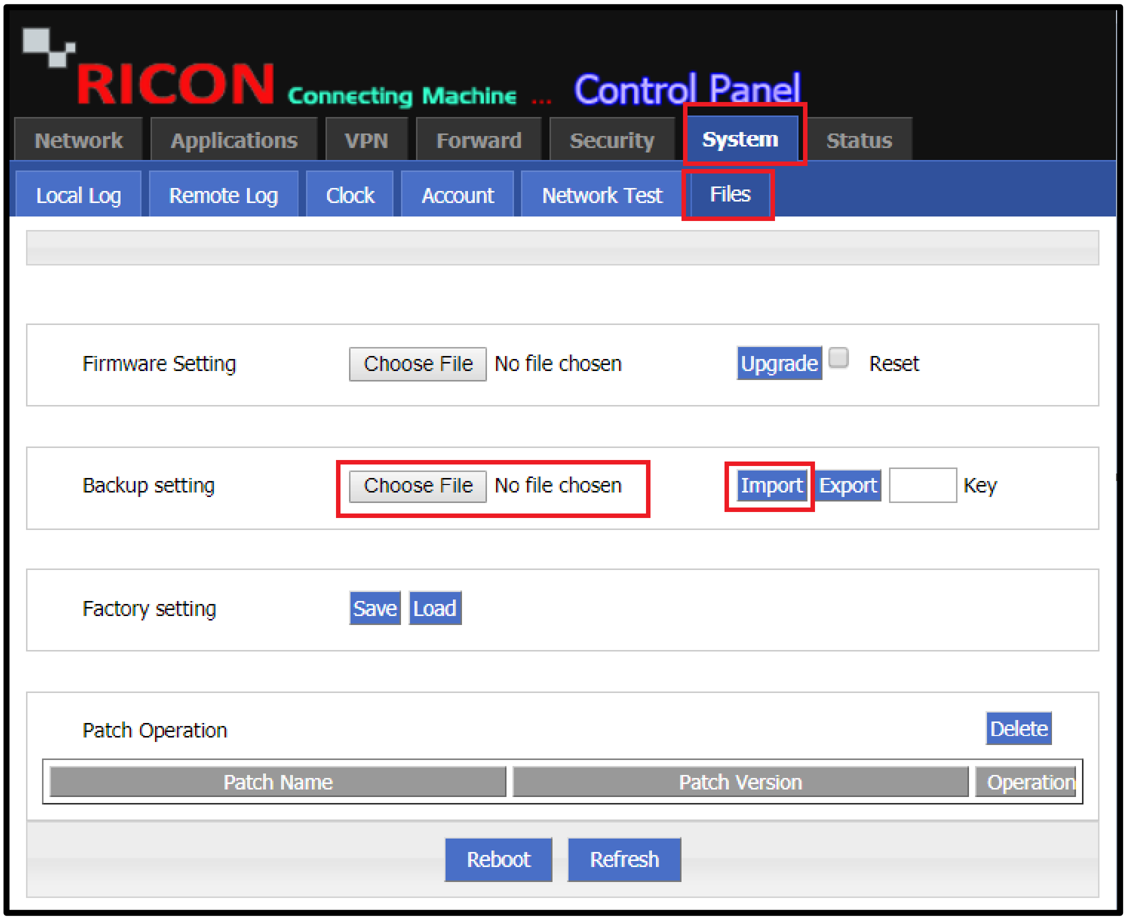


Figure.49- System>Files

9.6.3 FACTORY RESET SETTINGS

Follow the steps below to reset the device and single click the icon.

The router also has a “**Reset**” button to restore it to its original factory default settings at the back of the device. When user press the “Reset” button for up to 15s, the router will restore to its original factory default settings and restart automatically.

When you click the **Save** button, the config file you are using is saved as your factory default file. You can delete or modify this file at any time.

SYSTEM>FİLES>FACTORY SETTING

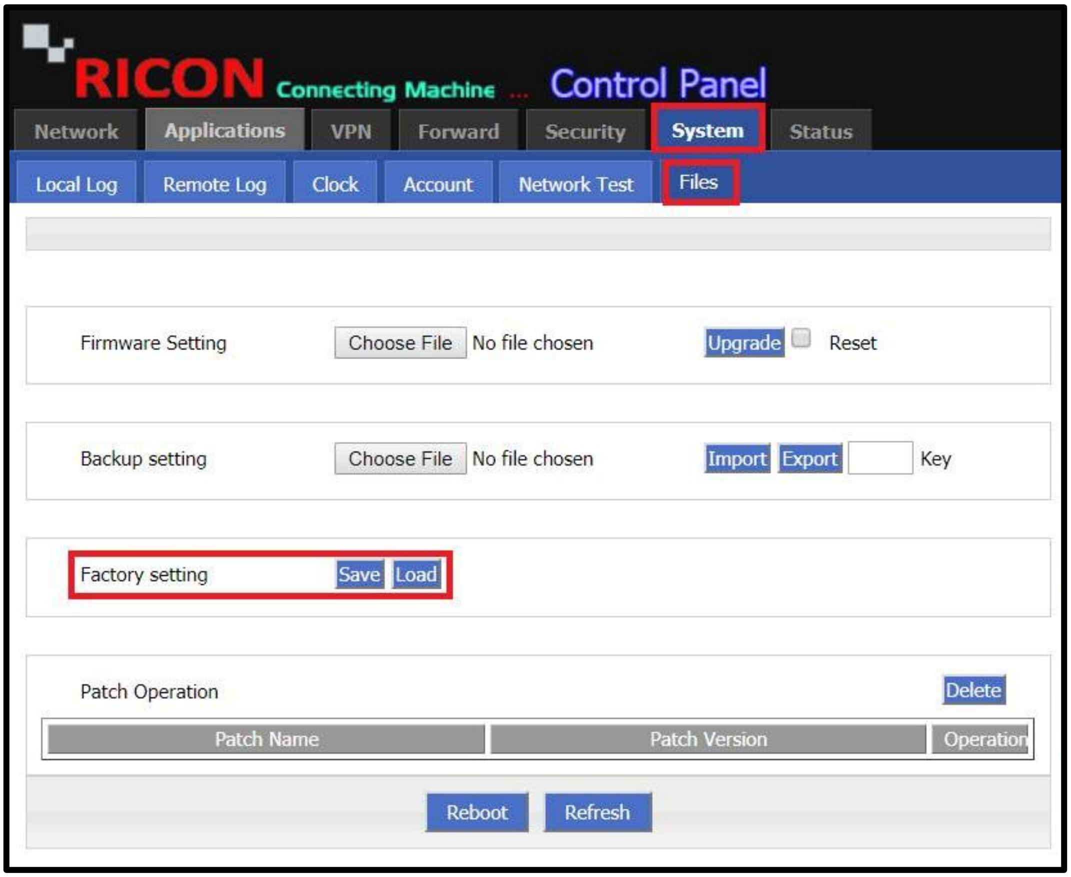


Figure.50-System>Files

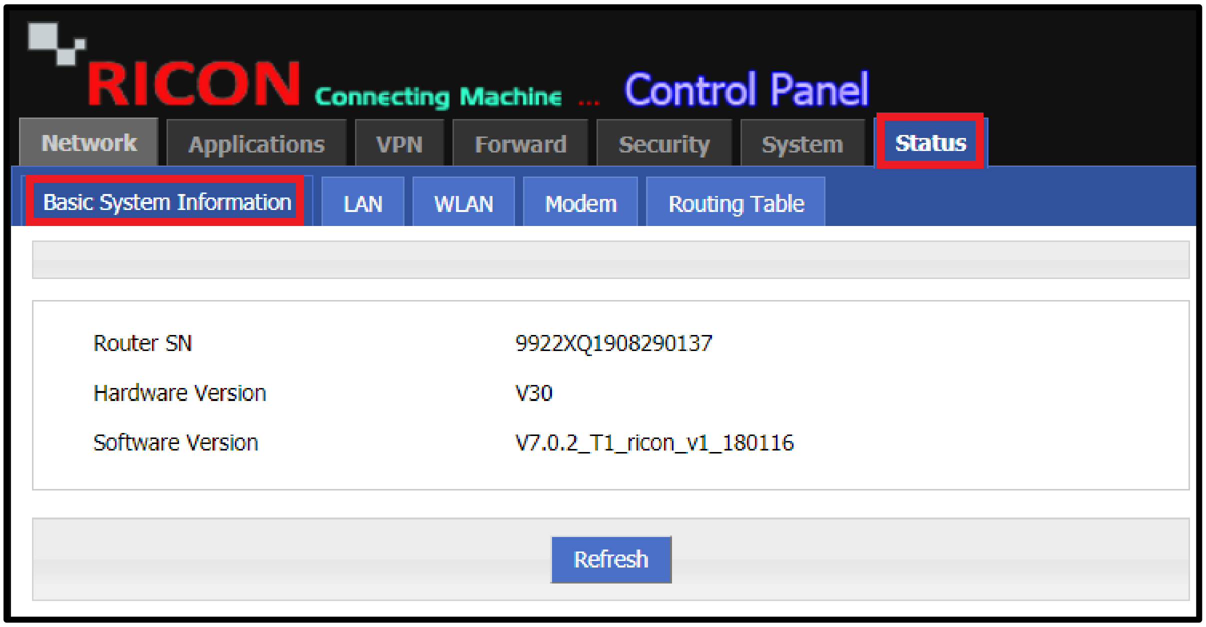
10 STATUS

The current status of the S9922M LTE series router can be viewed here.

10.1 BASIC SYSTEM INFORMATION

- ✓ Choose Status> Basic System Information
- ✓ You can see **Router's Serial Number**
- ✓ You can see **Router's Hardware Version**
- ✓ You can see **Router's Software Version** (Current Firmware)

STATUS>BASIC SYSTEM INFORMATION



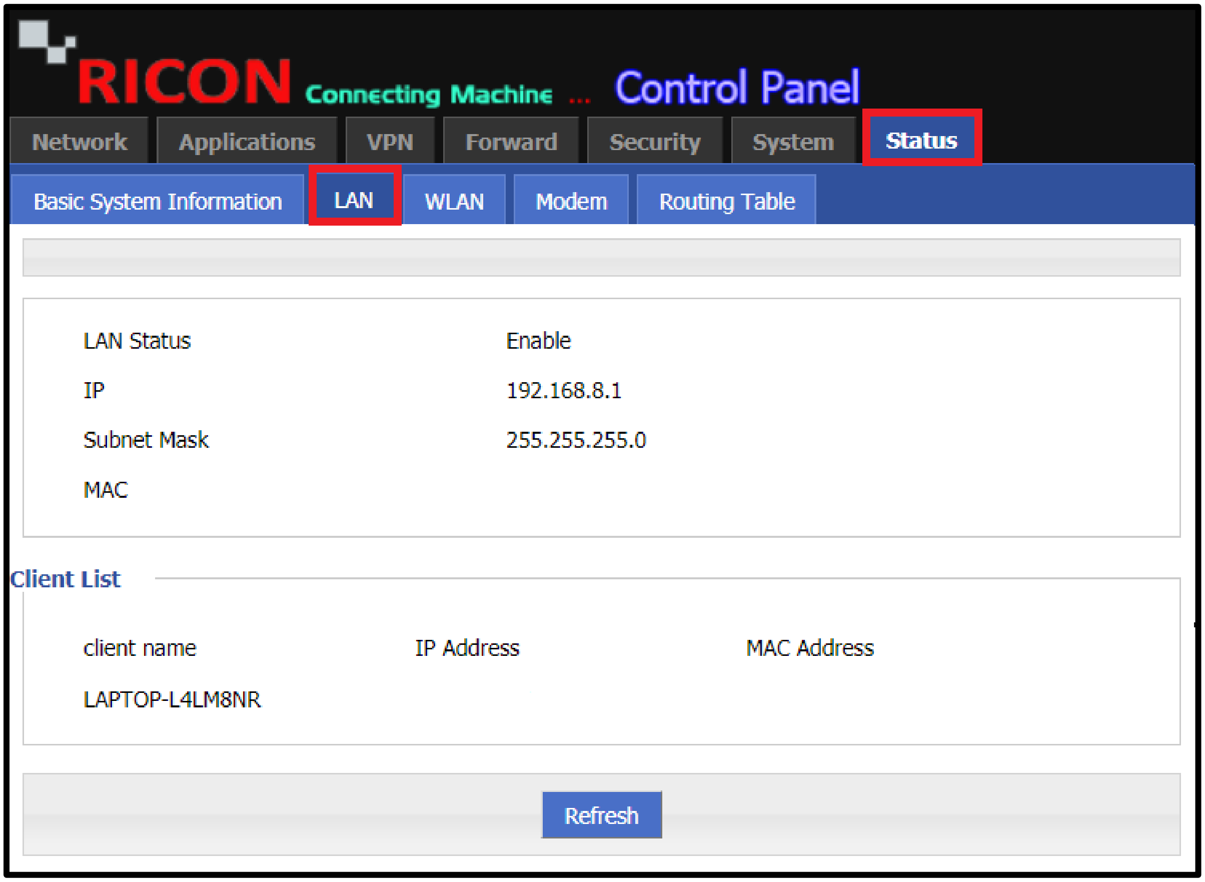
Router SN	9922XQ1908290137
Hardware Version	V30
Software Version	V7.0.2_T1_ricon_v1_180116

Figure.51- Status>Basic System Information

10.2 LAN INFORMATION

From the LAN tab, you can see whether the device's LAN (Local Area Network) port is active. In addition, if DHCP is enabled, you will see the devices that receive IP from DHCP with their MAC address and IP address here.

STATUS>LAN



LAN Status	Enable
IP	192.168.8.1
Subnet Mask	255.255.255.0
MAC	

Client List

client name	IP Address	MAC Address
LAPTOP-L4LM8NR		

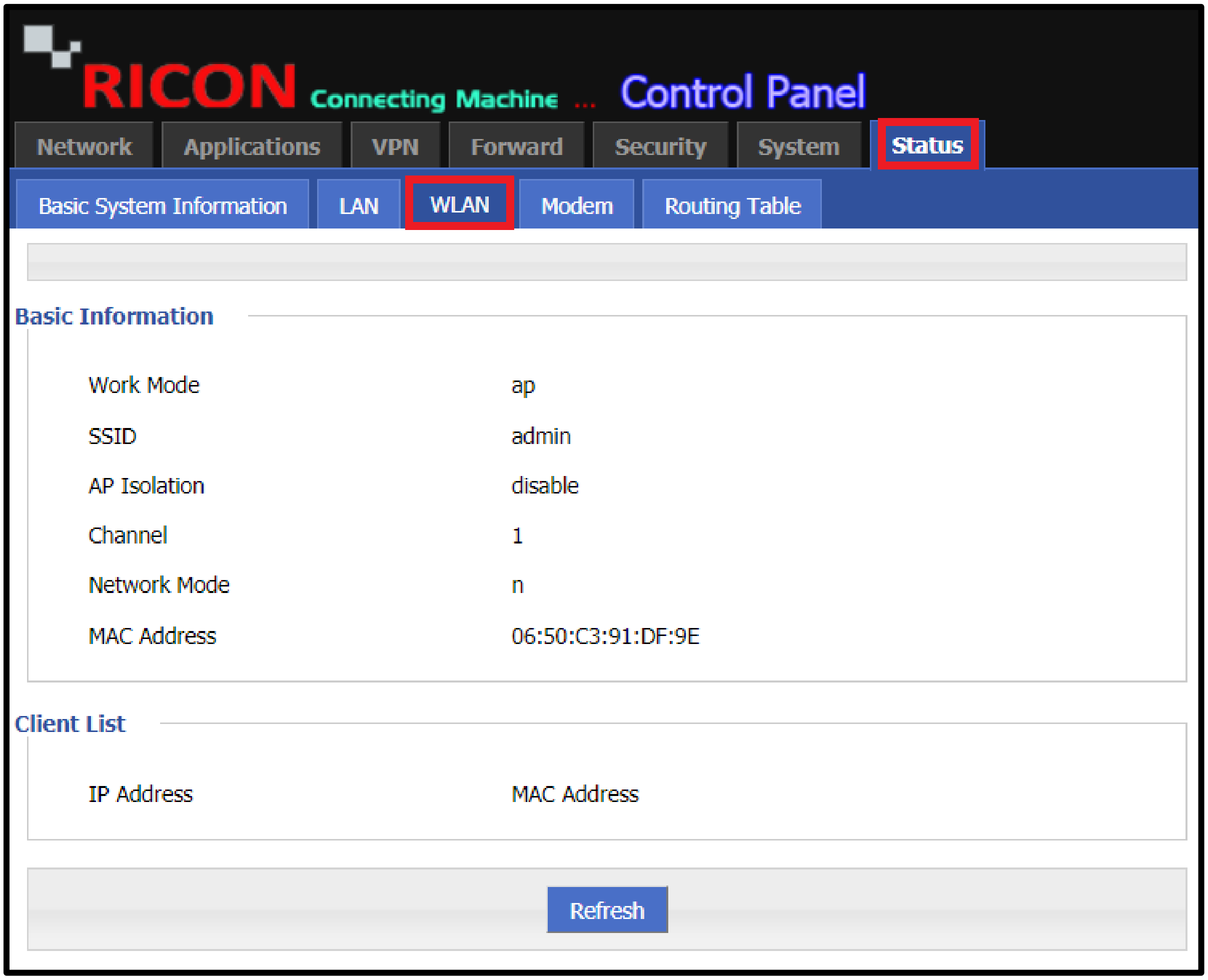
Figure.52- Status>LAN

10.3 WLAN INFORMATION

If WLAN (Wireless Local Area Network) is enabled on the Router, you can view its status here. Here you can see how many devices are connected via WLAN.

- ✓ In the example, if the WLAN is shown off but turned on, the Client List must be checked for testing.

STATUS>WLAN



Basic Information

Work Mode	ap
SSID	admin
AP Isolation	disable
Channel	1
Network Mode	n
MAC Address	06:50:C3:91:DF:9E

Client List

IP Address	MAC Address

Figure.53- Status>WLAN

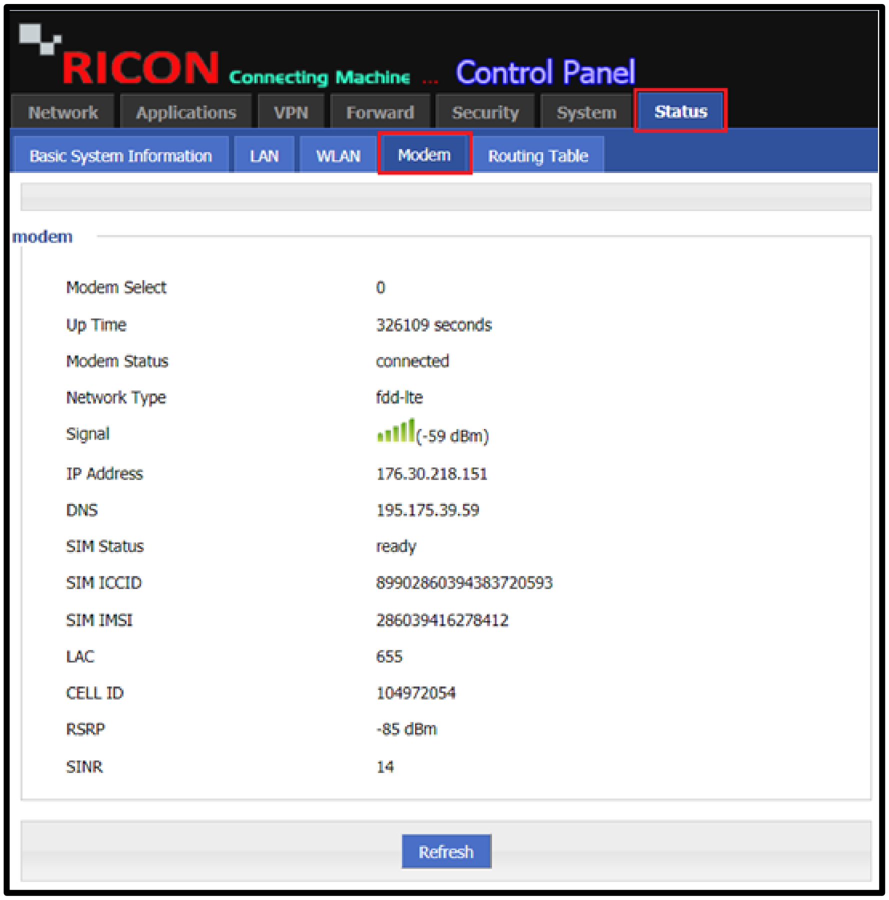
10.4 MODEM INFORMATION

You can view the status of your mobile circuit from this tab. Check whether the mobile circuit is working, how long it is connected, the signal level, the IP address it receives, the SIM information, and so on. you can check this information here.

Select **Status > Modem**, to check if the router is receiving IP over the SIM card. In this screen you can see **Up Time**, **Modem Status** (connected or disconnected), **Signal** (dBm), **IP Address** and **DNS**.

If you have some problem with your SIM card it will appears on SIM Status. In Figure 6 you can see SIM status "Sim Card Needs PIN Code"

STATUS>MODEM



modem

Modem Select	0
Up Time	326109 seconds
Modem Status	connected
Network Type	fdd-lte
Signal	(-59 dBm)
IP Address	176.30.218.151
DNS	195.175.39.59
SIM Status	ready
SIM ICCID	89902860394383720593
SIM IMSI	286039416278412
LAC	655
CELL ID	104972054
RSRP	-85 dBm
SINR	14

Figure.54- Status>Modem

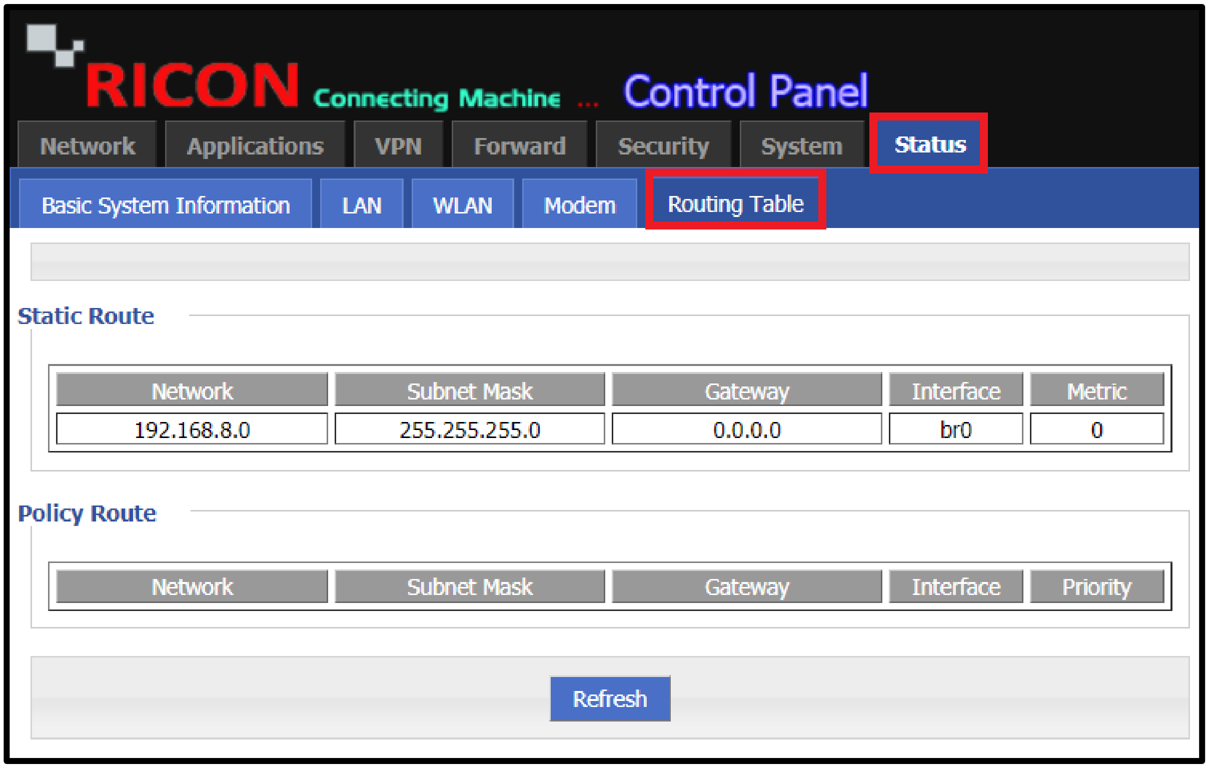
NOTE:

- *The LTE circuit runs stably at the lowest -95 dBm. Cuts at values less than -95 dBm may occur.*
- *If the mobile circuit receives a different WAN ip than you know, contact your ISP.*

10.5 ROUTING INFORMATION

You can follow the steps to check the current routes in the device.

STATUS>ROUTING TABLE



Static Route

Network	Subnet Mask	Gateway	Interface	Metric
192.168.8.0	255.255.255.0	0.0.0.0	br0	0

Policy Route

Network	Subnet Mask	Gateway	Interface	Priority

Figure.55- Status>Routing Table