RICON MOBILE

S9922L Series LTE Router

USER MANUAL

RICON MOBILE

S9922L 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

S9922L series LTE 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 VERSIONS

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

Model	Version
S9922L:	V30
Firmware Version starting from:	S9922L_APP_V7.0.2_T1_ricon_1710161204
Date of issue:	24.10.2019

Contents

1

1. PRODUCT

1.1 OVERVIEW

S9922L router series are mobile network router based on 2G/3G/4G/4.5G, WiFi and VPN technologies. Powerful 64-bit Processor and integrated real-time operating system specially developed by Ricon Mobile. Such as Ethernet and WiFi can easily connect any network device connected via interface connections, over the mobile network, transparently, to the internet or a central local network via a simple configuration. While the Ricon Mobile S9922L router series offers maximum service to customers, Zero touch-SMS installation minimizes the need for field service with easy and automatic product installation service. The best throughput of the S9922L router series is 100 Mbps. Its unique feature is that it is online and redundant across the network between WAN, WLAN, 3G/ LTE network. This feature allows the S9922L series to provide maximum network availability and reduce the possibility of network failure to prevent losses from network errors. In addition, the definable route table allows customers to assign bandwidth and reduce network delays by type of job. The Ricon Mobile S9922L router series is web-based and can be easily routed with CLI. In addition, with the Ricon Management System (RMS), it successfully achieves the goal of lowering maintenance costs with the ability to access all Ricon products on the network in bulk and with the possibility to access and manage 100% instant and statistical data related to these products.

1.2 FUNCTIONS & FEATURES

- VPN support, GRE over IPSec, IPsec over PPTP/L2TP
- RS232 or RS485 connection in series via the console port
- Maximum troughput value; 100mbps
- VPN Passthrough
- Configuration and maintenance with WEB, CLI and RMS
- 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-S9922L Series LTE Router Appearance

2.2 ACCESSORIES

Accessories name	Number	Note
S9922L Series Router	1 pcs	
3G/LTE antenna	2 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 Installation

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. This 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 S9922L series LTE 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: 192.168.1.* (*indicates any integral between 2 to 254)

Subnet mask: 255.255.255.0

Default gateway: 192.168.1.1

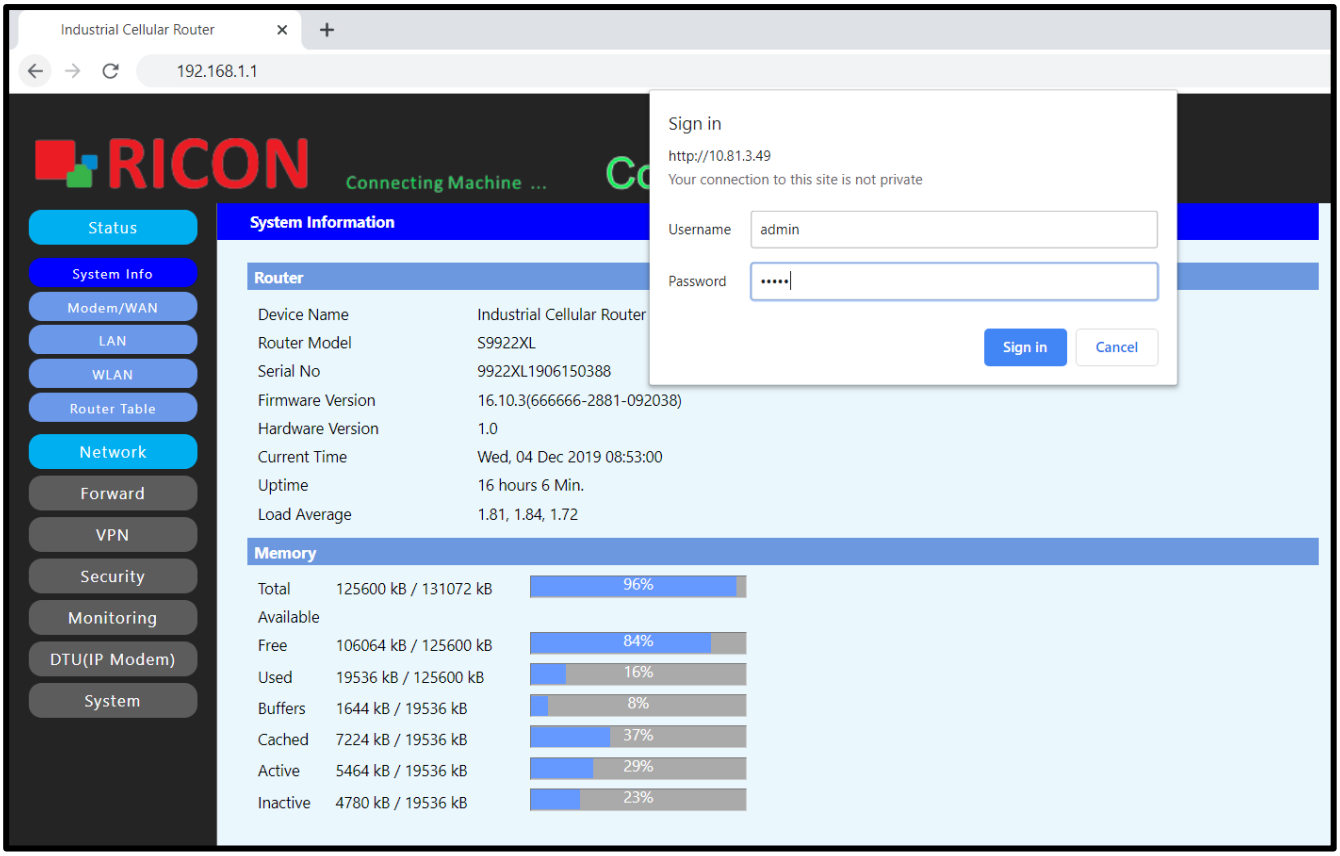

Figure.2- Website preparation

Launch the browser and enter http://192.168.1.1 in the address bar. The login page appears.

NOTE:

- *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.*

Input the username and password then click **Sign in**.

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

4

4. STATUS

All technical status of the S9922L series LTE router can be displayed under the status heading.

4.1 SYSTEM INFO

Device info, serial number, firmware version, date, up time and load average information are displayed under Router in System info heading.

Under the memory, the used and unused memory information of the router is displayed.

STATUS>SYSTEM INFO

Figure.4- Status>System Info

4.2 Modem/WAN INFORMATION

The current status of the LTE circuit or circuits active in the S9922L series LTE router, SIM card information, which SIM slot is active, signal level and WAN IP can be displayed on this page.

STATUS>MODEM/WAN

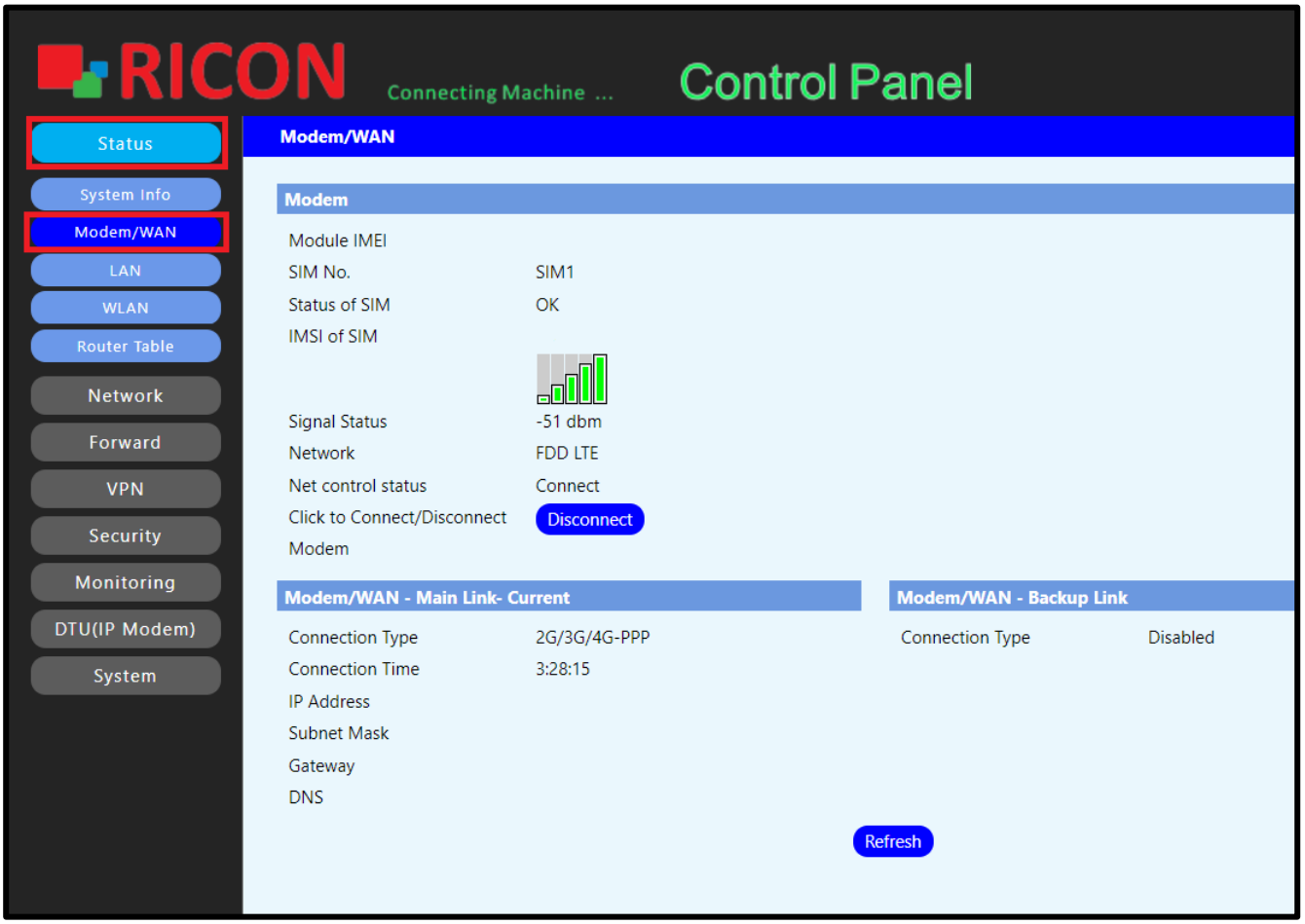

Figure.5- STATUS>Modem/Wan

4.3 LAN INFORMATION

From the LAN header, the device's MAC address, LAN IP information, and device information of users connected to the router can be displayed.

STATUS>LAN

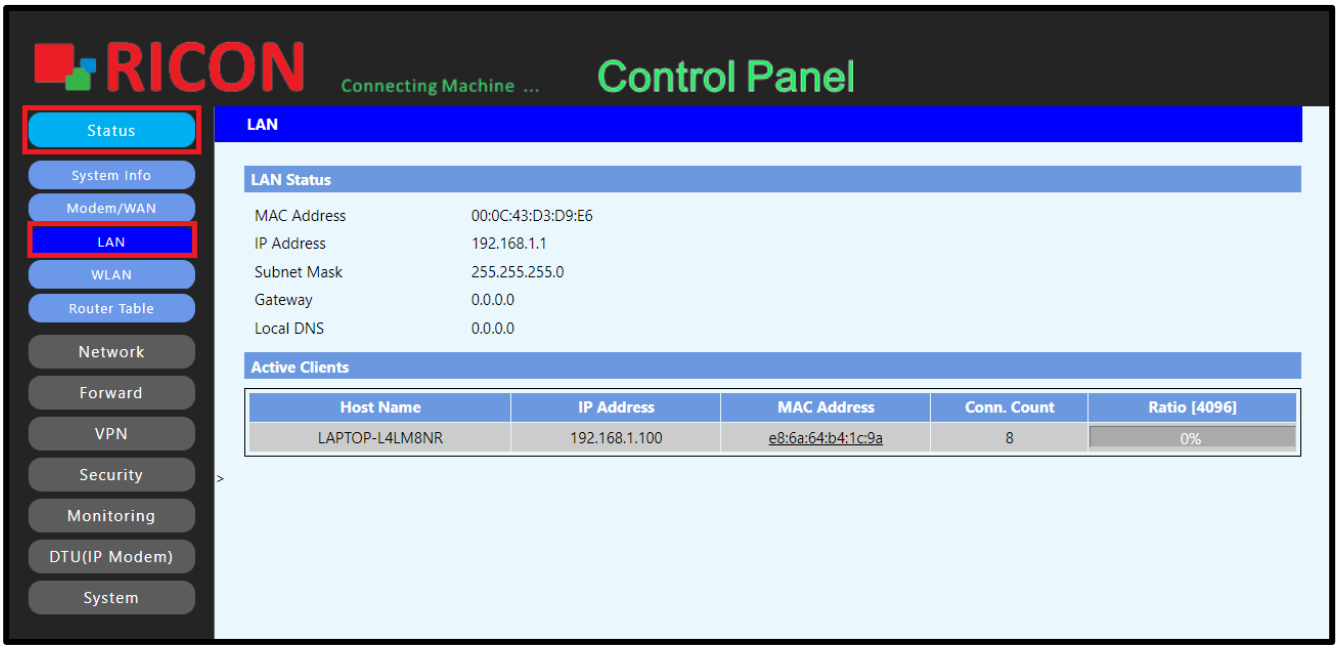

Figure.6- STATUS>LAN

4.4 WLAN INFORMATION

The S9922L series LTE router's wireless LAN configuration and users connected via the wireless network can be viewed on this page.

STATUS>WLAN

Figure.7- Status>WLAN

4.5 ROUTER TABLE

The gateways of the router are displayed here.

STATUS>ROUTER TABLE

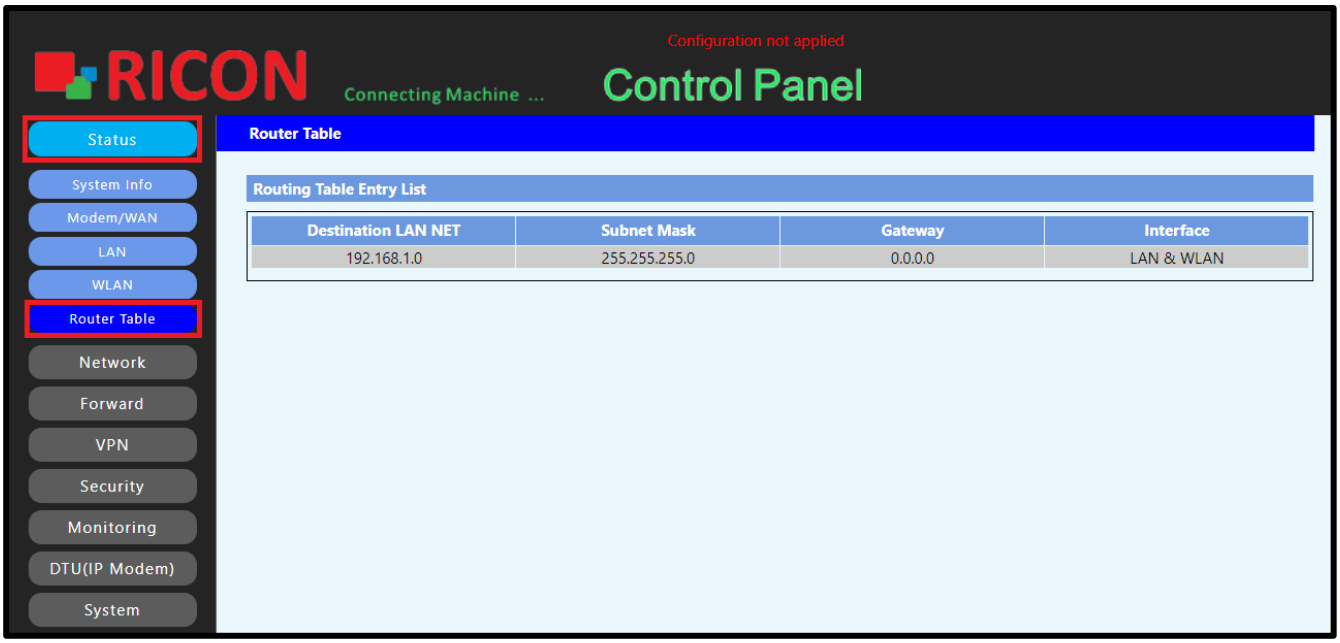

Figure.8- Status>Router Table

5

5. NETWORK CONFIGURATION

5.1 Modem/WAN CONFIGURATION

The configuration of LTE circuits is done from this page.

Under Link Backup

- ✓ **Backup Mode;**
  - **Main First;** The traffic is routed primarily through the LTE circuit, which is designated as the first sim.
  - **Mutual Preparation Mode;** The traffic is routed primarily via the active LTE circuit.
- ✓ **Link Fail to Restart;** The S9922L series LTE router can restart itself when LTE circuit is not up for a certain time. Enter the specified time here. If 0 is entered, this feature is assumed to be turned off.

Under Modem/AWN – Main Link

- ✓ **Connection Type;**
  - **Disable;** The cellular port is closed.
  - **2G/3G/4G-PPP;** If static IP is assigned to LTE circuit, PPP should be selected.
  - **2G/3G/4G-DHCP;** If LTE circuit will receive IP over DHCP, must be selected.
- ✓ **SIM Switch/Reset;** If the router is to run as a redundant, if the IP cannot be obtained for the entered time, the router automatically switches to the redundant SIM.
- ✓ **SIM Backup;** Enable is selected if the S9922L series LTE router is to be redundant.
- ✓ **Main SIM;** The SIM to be given priority is selected.

Under SIM 1; Enter the information of the card inserted in the SIM 1 slot.

- ✓ **User Name;** Enter the user name of your LTE circuit.
- ✓ **Password;** Enter the password of your LTE circuit.
- ✓ **Dial String;** The dialing string varies depending on the network standard. Enter the dialing string for the network you are using.
- ✓ **APN;** Enter the APN information obtained from the internet service provider.
- ✓ **PIN;** Enter the pin of the SIM card.
- ✓ **Network Mode;** Network mode is selected depending on the infrastructure.

Under SIM 2; Enter the information of the card inserted in the SIM 2 slot.

Others

- ✓ **Authentication;** Enter the authentication information received from the internet service provider.
- ✓ **Fixed WAN IP;** If the WAN IP is static, you can enter your IP here by selecting enable.
- ✓ **Fixed WAN Gateway;** If the WAN gateway is static, you can enter your IP here by selecting enable.
- ✓ **Force reconnect;** Select enable and enter the time for the device to try to retrieve IP again at a specified time during the period of inactivity.

- ✓ **Connect Fail;** Number of device restarts unless the circuit is up.
- ✓ **Dial Fail to Restart;** Unless the circuit is up, enter the time before the device restarts.
- ✓ **Keep Alive;** ICMP, PPP, Route, ICMP+.
    - **ICMP** and **ICMP+;** Internet Control Message Protocol and plus provide controls with the IP you specify.
    - **PPP;** Provides controls with your WAN IP.
    - **Route;** The controller is provided over the route you set.
- ✓ **Keep Alive Interval;** The period of inaccessibility to the specified IP must be entered here.
- ✓ **Keep Alive Fail;** Repeat switching to backup SIM card if the target IP cannot be reached for the specified time.
  Modem/WAN – Backup Link; If you want to configure the router as a backup, enter your backup SIM card information here.
- ✓ **MTU;** If the specified MTU value exists, enter it here. Auto is considered 1500.
- ✓ Click **Save** and **Apply** to save the configured settings.

NETWORK>MODEM/WAN

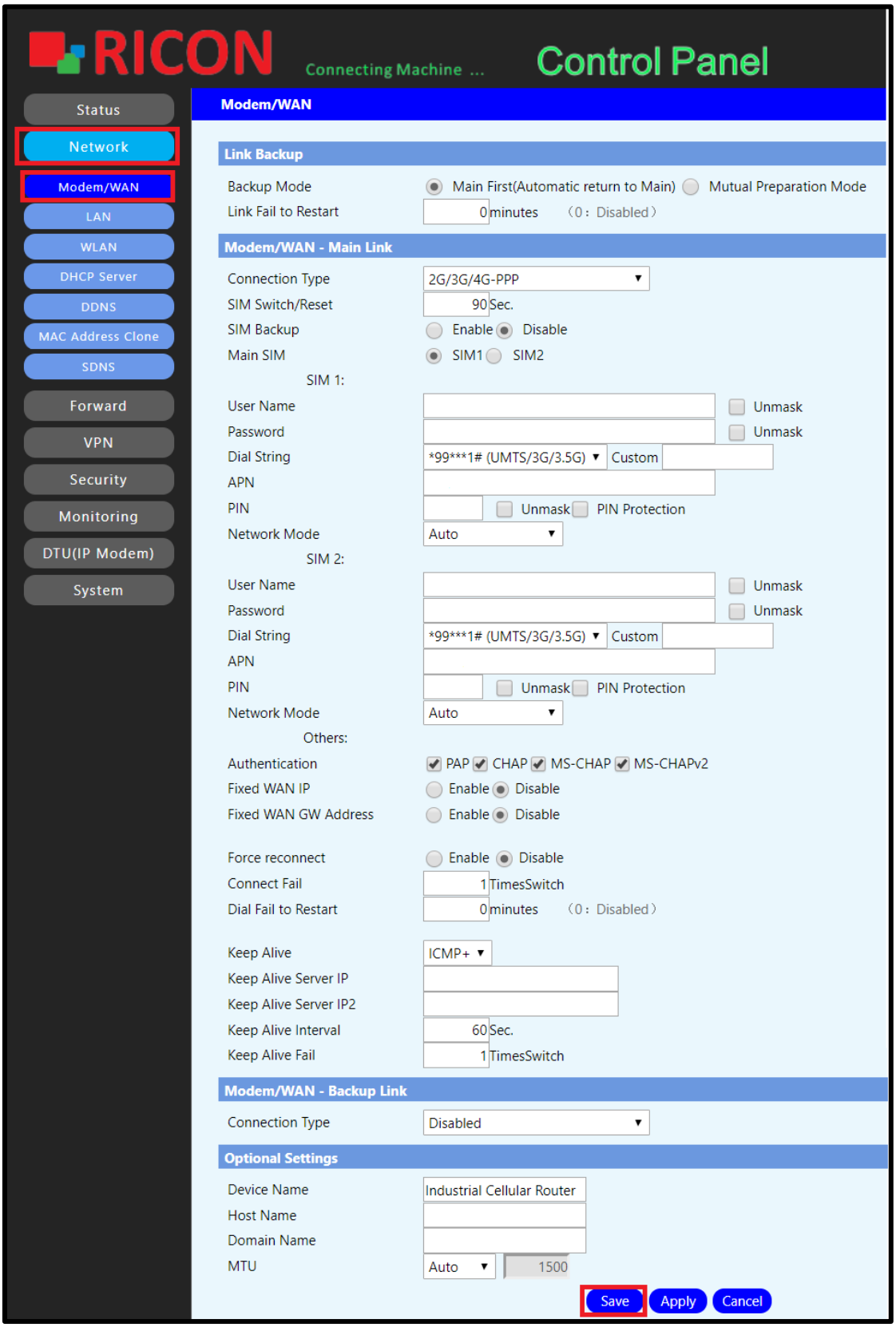

Figure.11- Network>Modem/WAN

5.2 LAN CONFIGURATION

LAN settings are used to manage local area network units which are connected to a S9922L series LTE 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**.

NETWORK>LAN

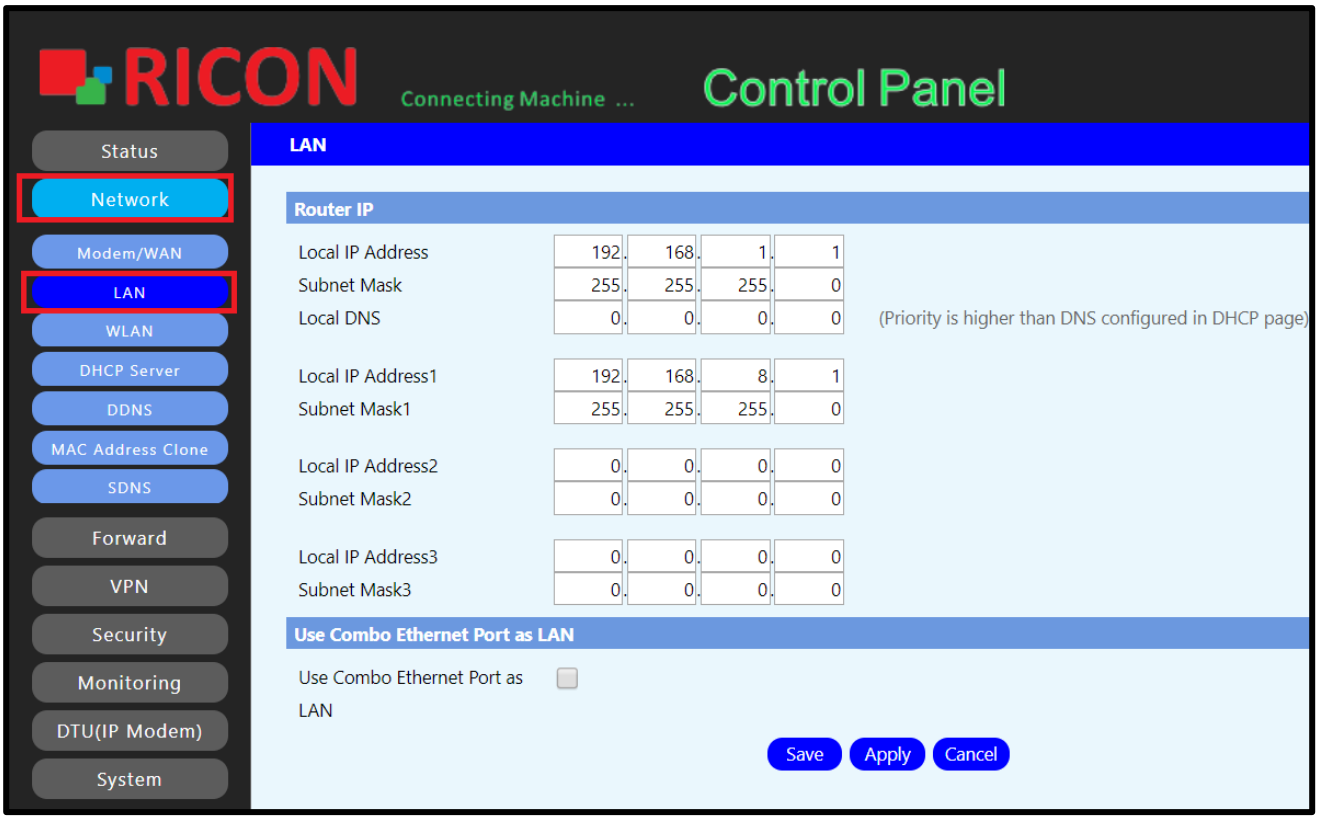

Figure.12- Network>LAN

5.3 WLAN CONFIGURATION

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. Follow the steps below to make Wi-Fi connection.

- ✓ **Wireless Network;** Enable must be selected for the WLAN to be active.
- ✓ **Wireless Mode;** AP, Client, Adhoc, Repeater, Repeater bridge.
    - **AP;** AP mode this is the default, most common mode for all wireless routers, also called Infrastructure mode. Your router acts as an central connection point, which wireless clients can connect to.
    - **Client;** AP Client or Wireless Client mode allows the Access Point to become a wireless client to another AP. In essence the AP has now become a wireless adapter card. You would use this mode to allow an AP to communicate with another AP.
    - **Adhoc;** Ad-hoc mode refers to a wireless network structure where devices can communicate directly with each other. This type of network is also used in small groups, where the main purpose of the connection is file-sharing.
    - **Repeater;** A wireless repeater is a protocol that takes an existing signal from a wireless router and rebroadcasts it to create a second network. When two or more hosts have to be connected with one another over the IEEE 802.11 protocol and the distance is too long for a direct connection to be established, a wireless repeater is used to bridge the gap.
    - **Repeater Bridge;** A wireless repeater bridge connects two LAN segments with a wireless link. The two segments are in the same subnet and look like two Ethernet switches connected by a cable to all computers on the subnet. Since the computers are on the same subnet, broadcasts reach all machines.
- ✓ **Network Mode;** Mixed, BG, B, G, NG, N.
    - **Mixed;**
    - **BG;** User can connect in B or N according to the capability of the device.
    - **B;** An improvement on previous standards that increased features, but shortened the range.
    - **G;** Combined the best of the previous modes and increased the maximum distance nodes could be from each other.
    - **NG;** User can connect in N or G according to the capability of the device.
    - **N;** Improvement to mode G, and the first to support multiple signals at the same time. Also increased the band to 5 GHz to reduce the effects of outside signals like microwaves.

Mode	Band	Data Range	Standard	Indoor Range (meters)	Created
Mixed	*2.4 and 5 GHz*	*Varies*	*N/A*	*N/A*	*N/A*
BG	*2.4 GHz*	*11 and 54 Mbps*	*N/A*	*38 m*	*N/A*
B	*2.4GHz*	*11 Mbps*	*802.11b*	*35 m*	*1999*
G	*2.4GHz*	*54 Mbps*	*802.11g*	*38 m*	*2003*
NG	*2.4 and 5 GHz*	*54 and 100 Mbps*	*N/A*	*70 m*	*N/A*
N	*2.4 and 5 GHz*	*100 Mbps*	*802.11n*	*70 m*	*2009*

- ✓ **SSID;** Set SSID is your Wi-Fi connection name.

- ✓ **Channel;** There are 14 different channel selection options.
- ✓ **Channel Width;** 20 MHz or 40 MHz can be selected according to the specifications of the devices you want to use in wireless network.
- ✓ **SSID Broadcast;** If you want the SSID to be hidden, select disable.
- ✓ **Security Mode;** Disable, WEP, WPA Personal, WPA Enterprise, WPA2 Personal, WPA2 Enterprise, WPA2 Personal Mixed, WPA2 Enterprise Mixed.
    - **Disable;** Wireless network is connected to the network without password.
    - **WEP;** Wired Equivalent Privacy (WEP) is a data encryption protocol for 802.11 wireless networks. All wireless stations and SSIDs on the network are configured with a static 64-bit or 128-bit Shared Key for data encryption.
    - **WPA Personal;** Supports TKIP (Temporal Key Integrity Protocol) or AES (Advanced Encryption System) encryption mechanisms for data encryption (default is TKIP). TKIP uses dynamic keys and incorporates Message Integrity Code (MIC) to provide protection against hackers. AES uses symmetric 128-bit block data encryption.
    - **WPA-Enterprise;** Uses WPA with RADIUS authentication. This mode supports TKIP and AES encryption mechanisms (default is TKIP) and requires the use of a RADIUS server to authenticate users.
    - **WPA2 Personal;** Always uses AES encryption mechanism for data encryption.
    - **WPA2 Enterprise;** Uses WPA2 with RADIUS authentication. This mode always uses AES encryption mechanism for data encryption and requires the use of a RADIUS server to authenticate users.
    - **WPA2-Personal mixed:** Supports the transition from WPA-Personal to WPA2-Personal. You can have client devices that use either WPA-Personal or WPA2-Personal.
    - **WPA2-Enterprise mixed:** Supports the transition from WPA-Enterprise to WPA2-Enterprise. You can have client devices that use either WPA-Enterprise or WPA2-Enterprise.
- ✓ **WPA Algorithms;** TKIP, AES TKIP+AES
    - TKIP (short for Temporal Key Integrity Protocol) is an encryption method. TKIP provides per-packet key mixing a message integrity and re-keying mechanism.
    - AES (short for Advanced Encryption Standard) is the Wi-Fi® authorized strong encryption standard.
    - WPA-PSK/ WPA2-PSK and TKIP or AES use a Pre-Shared Key (PSK) that is 8 or more characters in length, up to a maximum of 63 characters.
- ✓ **WPA Shared Key;** Set is your Wi-Fi connection password.
- ✓ **Key Renewal Interval;** The number of seconds the wireless network needs to be refreshed is entered here.
- ✓ Click the **Save** and **Apply** icons to finish the configuration.

NETWORK>WLAN

Figure.13- Network>WLAN

5.4 DHCP CONFIGURATION

DHCP stands for Dynamic Host Control Protocol. DHCP server letting it assign the following to all computers connected to the router's LAN:

- IP address
- DNS server
- Default gateway address

- ✓ **DHCP Type;** DHCP Server, DHCP Forwarder.
  - **DHCP Forwarder;** Activate by entering the DHCP relay IP.
- ✓ **DHCP Server;** If you want the router to automatically distribute IP, select enable.
- ✓ **Start IP Address;** Enter the starting IP.
- ✓ **Maximum DHCP Users;** Enter the maximum number of users here.
- ✓ **Client Lease Time;** Enter client lease time here.
- ✓ **Static DNS;** Enter the DNS that you want the router to automatically distribute here.
- ✓ **No DNS Rebind;** DNS rebinding is a method of manipulating resolution of domain names that is commonly used as a form of computer attack. Click Enable to activate.
  Static Assigned; Static IP can be assigned to specific users via the S9922L series LTE router.
- ✓ **Name;** Enter the rule name.
- ✓ **MAC Address;** Enter the user MAC address.
- ✓ **Host Name;** Enter the device user name.
- ✓ **IP Address;** Enter the IP address you specified.
- ✓ **Client Lease Time;** The user's time to stay connected can be specified. Enter the specified time here.
- ✓ Click the **Save** icon to save the configuration.

NETWORK>DHCP SERVER

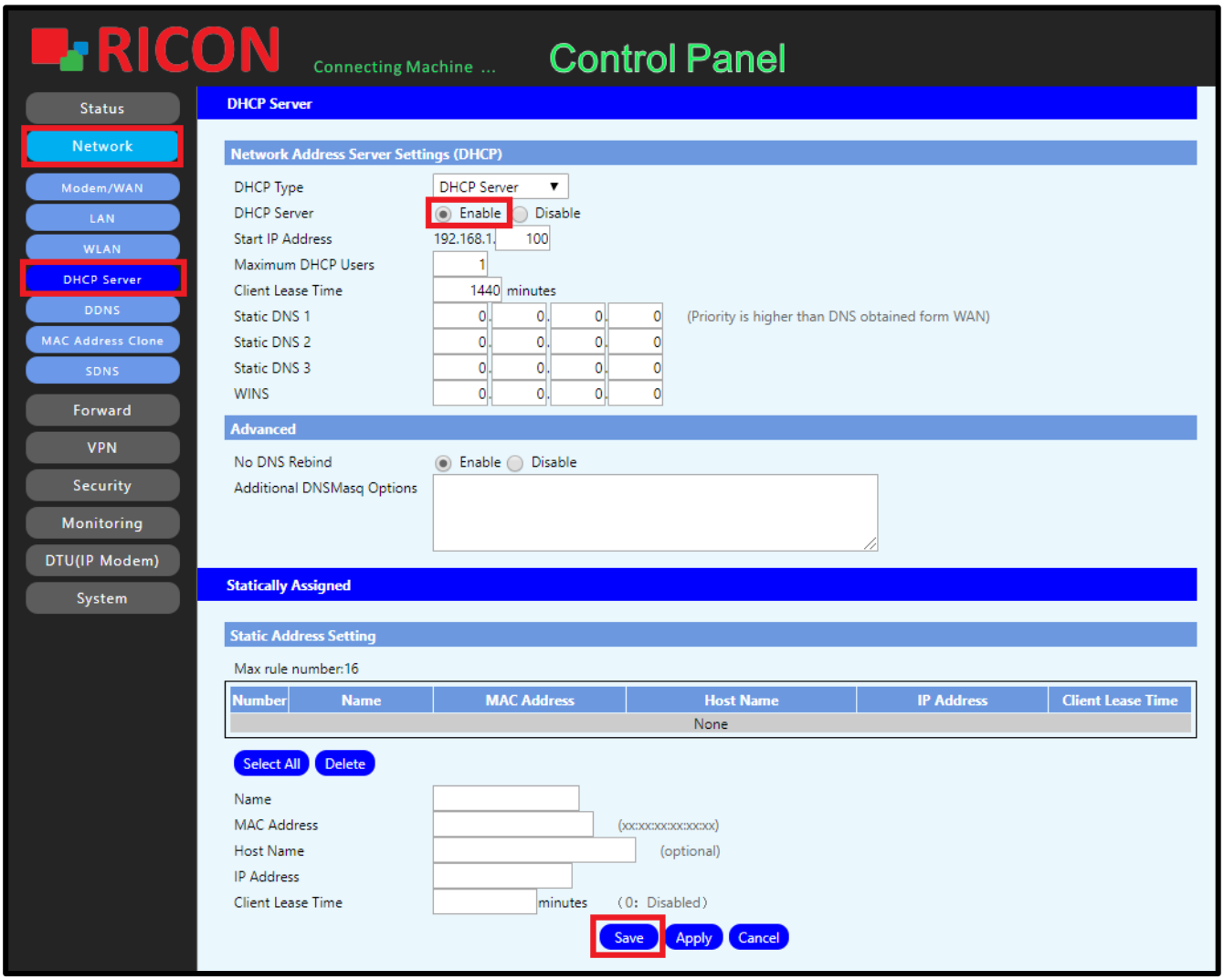

Figure.14- Network>DHCP Server

5.5 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 S9922L series LTE routers are router is capable of Dynamic DNS. To do this, follow the steps. Click the Network tab and choose DDNS from the navigation menu.

- ✓ **DDNS Service;** Custom
- ✓ **DYNDNS Server;** Enter the IP of the device from which you want access from the external network.
- ✓ **User Name;** Enter a specific user name.
- ✓ **Password;** Enter a specific password.
- ✓ **Host Name;** Enter the host name of the device you are using.
- ✓ **URL;** URL link can be entered according to usage request.
- ✓ **Do not use external ip check;** Click enable if access to external IP is desired.
- ✓ Click the **Save** button and save the configuration.

NETWORK>DDNS

Figure.15- Network>DDNS

5.6 MAC ADDRESS CLONE

You may need to set the MAC address of the interfaces of the S9922L LTE series router to the same MAC address or another MAC address as your PC. This is called MAC address cloning.

- ✓ **MAC Clone;** Click enable to clone.
- ✓ **Clone WAN MAC;** If it is necessary to change the mac address of the WAN port, enter the mac address you want to appear here. You can copy the current MAC address by clicking get current pc mac address.
- ✓ **Clone LAN(VLAN) MAC;** If it is necessary to change the mac address of the LAN ethernet port, enter the mac address you want to appear here.
- ✓ **Clone LAN(Wireless) MAC;** If it is necessary to change the mac address of the WLAN port, enter the mac address you want to appear here.
- ✓ Click **Save** icon to save cloned mac addresses.

NETWORK>MAC ADDRESS CLONE

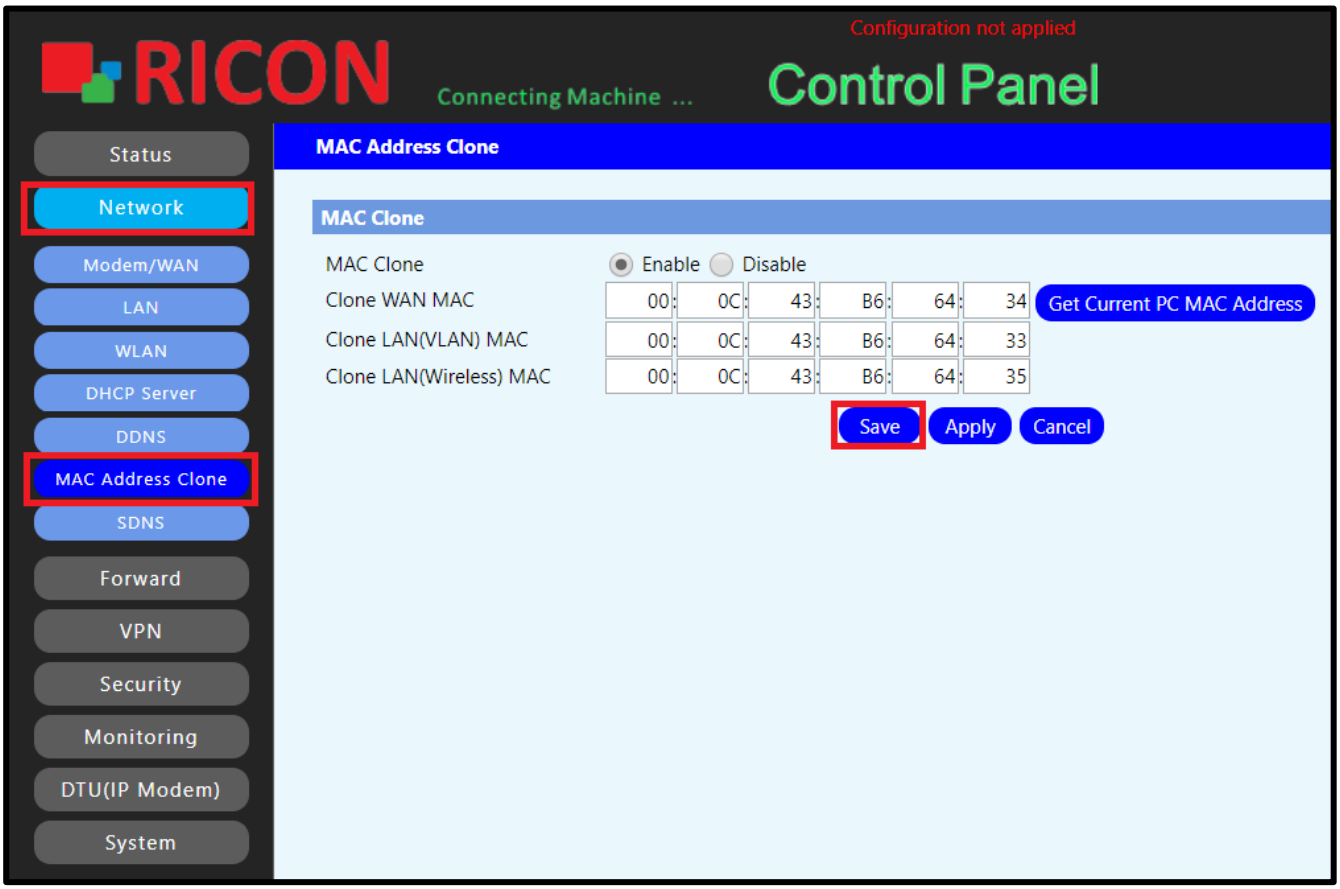

Figure.16- Network>MAC Address Clone

5.7 SDNS CONFIGURATION

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.

- ✓ **Name;** Enter the rule name here.
- ✓ **Domain Name;** Enter the domain name of the device with the private IP.
- ✓ **IP Address;** Enter the private IP here.
- ✓ Click the **Save** icon to finish.

NETWORK>SDNS

Figure.17- Network>SDNS

6

6. FORWARD CONFIGURATION

6.1 Static Routing

Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic.

- ✓ **Route Name;** Enter the rule name here.
- ✓ **Metric;** Metrics are calculated for multiple routes to determine the best route. The route having the best metrics is usually the easiest and fastest path for delivering the packet.
- ✓ **Destination LAN NET;** Enter the IP you want to forward here.
- ✓ **Subnet Mask;** Enter the subnet mask IP.
- ✓ **Gateway;** Enter the gateway IP here.
- ✓ **Interface;** Select the interface that the static route entered will use.
- ✓ Save static routing by clicking the **Save** icon.

FORWARD>STATIC ROUTING

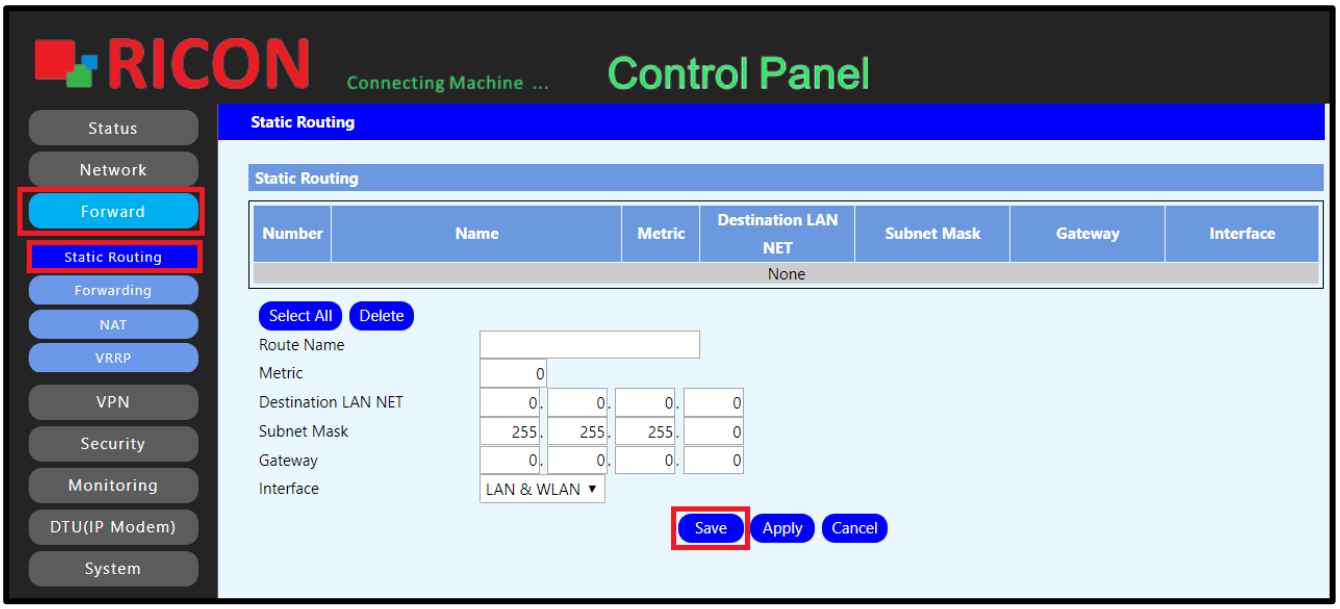

Figure.18- Forward>Static Routing

6.2 Forwarding CONFIGURATION

In computer networking, port forwarding or port mapping is an application of network address translation (NAT) that redirects a communication request from one address and port number combination to another while the packets are traversing a network gateway, such as a router or firewall.

- ✓ **Application;** Enter the name of the application (eg.test1)
- ✓ **Protocol;** Choose the protocol used by the application.
- ✓ **Source Net;** Enter the device IP for which you want access
- ✓ **Port from;** Enter the port information according to the type of device you want access to
- ✓ **IP address;** Enter the desired IP address of the host on the LAN side to which the specific IP traffic will be forwarded.
- ✓ **Start;** Enter the starting port range of the server or the Internet application.
- ✓ **End;** Enter the ending port range of the server or the Internet application.
- ✓ **DMZ;** In computer networks, a DMZ (demilitarized zone), also sometimes known as a perimeter network or a screened subnetwork, is a physical or logical subnet that separates an internal local area network (LAN) from other untrusted networks -- usually the internet. External-facing servers, resources and services are located in the DMZ. Therefore, they are accessible from the internet, but the rest of the internal LAN remains unreachable. Enter the DMZ IP and click **enable**.
- ✓ Click the **Save** icon to finish.

FORWARD>FORWARDING

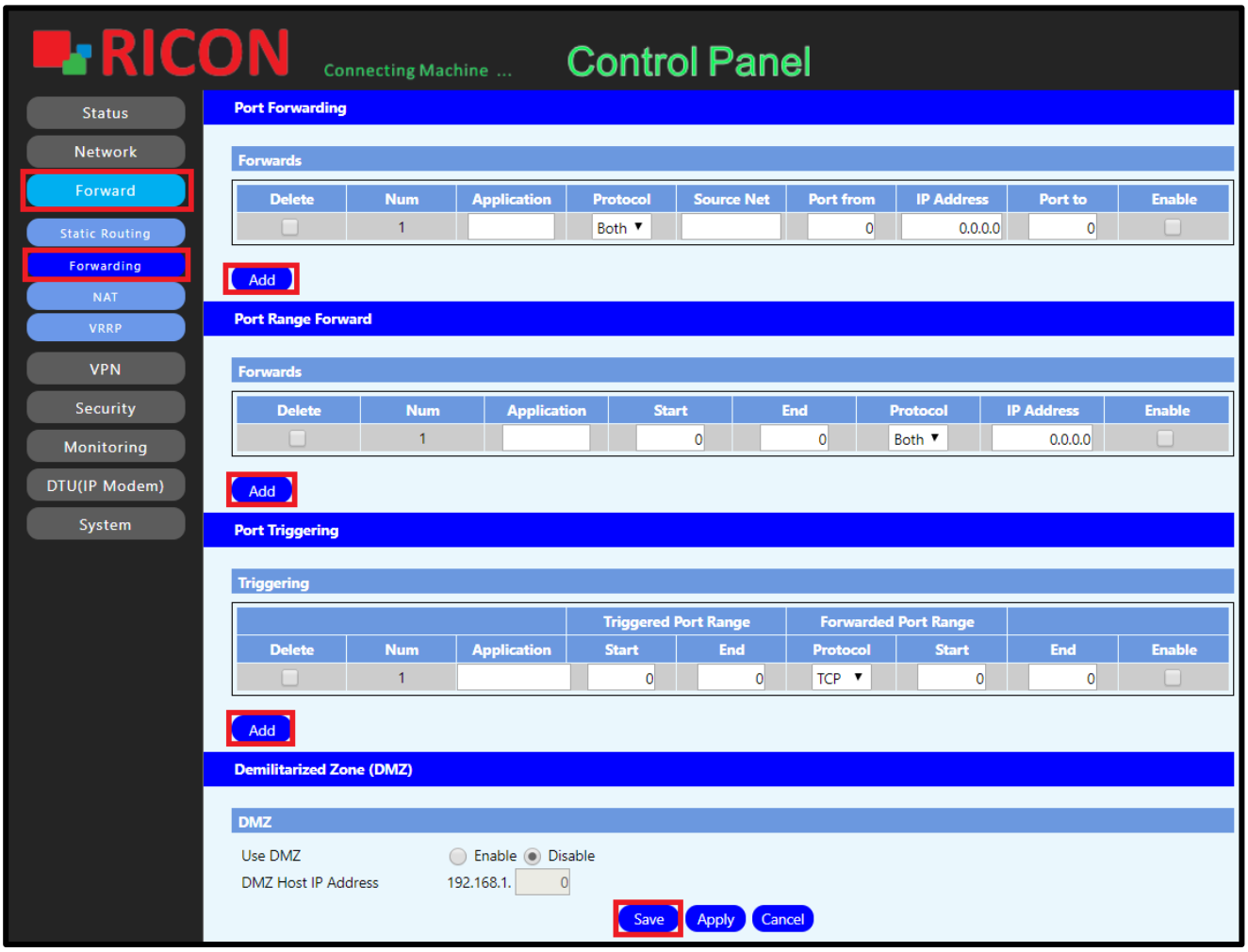

Figure.19- Forward>Forwarding

6.3 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 and to allow multiple devices to share a single IP address.

- ✓ **Wan Nat;** Click enable to activate.
- ✓ **Link;** Select NAT's external network interface.
- ✓ **STP;** Spanning Tree Protocol (STP) - Where two bridges are used to interconnect the same two computer network segments, spanning tree is a protocol that allows the bridges to exchange information so that only one of them will handle a given message that is being sent between two computers within the network. The spanning tree protocol prevents the condition known as a bridge loop.
- ✓ Click the **Save** and **Apply** icon to finish.

FORWARD>NAT

Figure.20- Forward>NAT

6.4 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 S9922L series LTE routers, follow the steps below.

- ✓ **VRRP Services;** Enable must be selected for the entered VRRP to be active.
- ✓ **Virtual Interface;** Select the interface.
- ✓ **Related to Wan;** Click enable if you need to go through the VRRP WAN port
- ✓ **Virtual Gateway;** Provide redundancy and enter the gateway to the creation of a single virtual router.
- ✓ **Serial Numbers;** Enter the total number of devices.
- ✓ **Priority;** Enter priority order.
- ✓ **Notice Timers;** Enter the notice timers.
- ✓ Click the **Save** icon to save the configuration.

FORWARD>VRRP

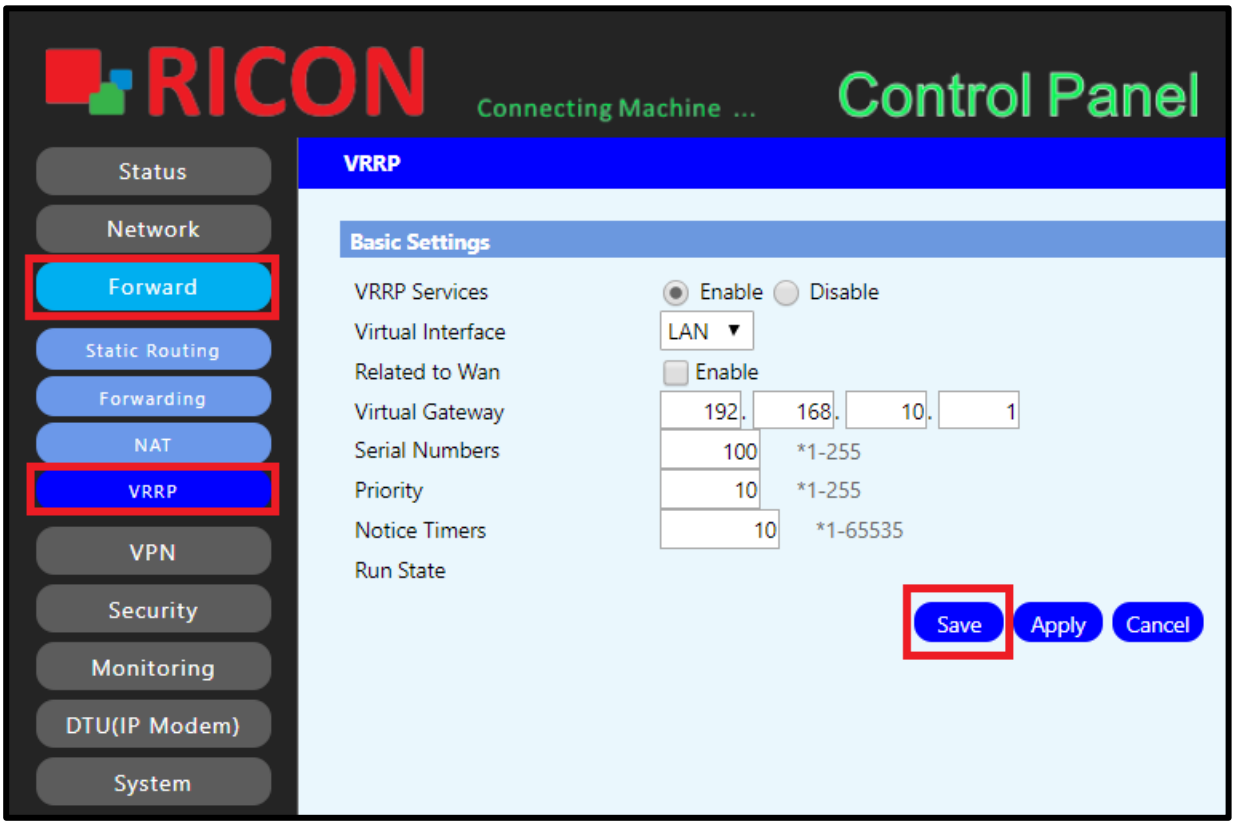

Figure.21- Forward>VRRP

7

7. VPN CONFIGURATION

7.1 PPTP CONFIGURATION

Stands for "Point-to-Point Tunneling Protocol." PPTP is a networking standard for connecting to virtual private networks, or VPNs. VPNs are secure networks that can be accessed over the Internet, allowing users to access a network from a remote location. This is useful for people who need to connect to an office network from home or access their home computer from another location.

- ✓ **PPTP Client Options;** Enable must be selected for the entered PPTP to be active.
- ✓ **Server IP or DNS Name;** VPN server enter the IP or domain name.
- ✓ **User Name;** Enter the specified username
- ✓ **Password;** Enter the specified password.
- ✓ **Remote Subnet;** Enter the IP address of users who will be.
- ✓ **Remote Subnet Mask;** Enter the IP subnet mask of users who will be.
- ✓ **Authentication;** Select your security protocol.
- ✓ **MPPE Encryption;** The client establishes a connection secured with MPPE. The router rejects the request for other protocols. The client uses as a minimum the key length specified in the router. Choose the one that's right for you.
- ✓ **MTU;** The Point-to-Point Tunneling Protocol (PPTP) uses the MTU to determine the maximum size of each packet in a transmission.
- ✓ **MRU;** Short for Maximum Receive Unit, MRU is data sent to inform remote systems of the local computer or network device's maximum packet size.
- ✓ Click the **Save** icon to save PPTP.

VPN>PPTP

Figure.22- VPN>PPTP

7.2 L2TP CONFIGURATION

The Layer 2 Tunneling Protocol (L2TP) allows the creation of a virtual private dialup network (VPDN) to connect a remote client to its corporate network by using a shared infrastructure, which could be the Internet or a service provider's network. Because of the lack of confidentiality inherent in the L2TP protocol, it is often implemented along with IPsec.

- ✓ **L2TP Client Options;** Enable must be selected for the entered L2TP to be active.
- ✓ **Tunnel Name;** Enter the tunnel name here.
- ✓ **User Name;** Enter the username you specified
- ✓ **Password;** Enter the password you specified.
- ✓ **Tunnel Authentication Pass;** Enter the tunnel password you specified.
- ✓ **Gateway (L2TP Server);** Enter the gateway of the L2TP server.
- ✓ **Remote Subnet;** Enter IP block of remote users that will allow access.
- ✓ **Remote Subnet Mask;** Enter subnet mask block of remote users that will allow access.
- ✓ **Authentication;** Select your security protocol.
- ✓ **MPPE Encryption;** The client establishes a connection secured with MPPE. The router rejects the request for other protocols. The client uses as a minimum the key length specified in the router. Choose the one that’s right for you.
- ✓ **MTU;** The Layer 2 Tunneling Protocol (L2TP) uses the MTU to determine the maximum size of each packet in a transmission.
- ✓ **MRU;** Short for Maximum Receive Unit, MRU is data sent to inform remote systems of the local computer or network device's maximum packet size.
- ✓ Click the **Save** and **Apply** icon to finish.

VPN>L2TP

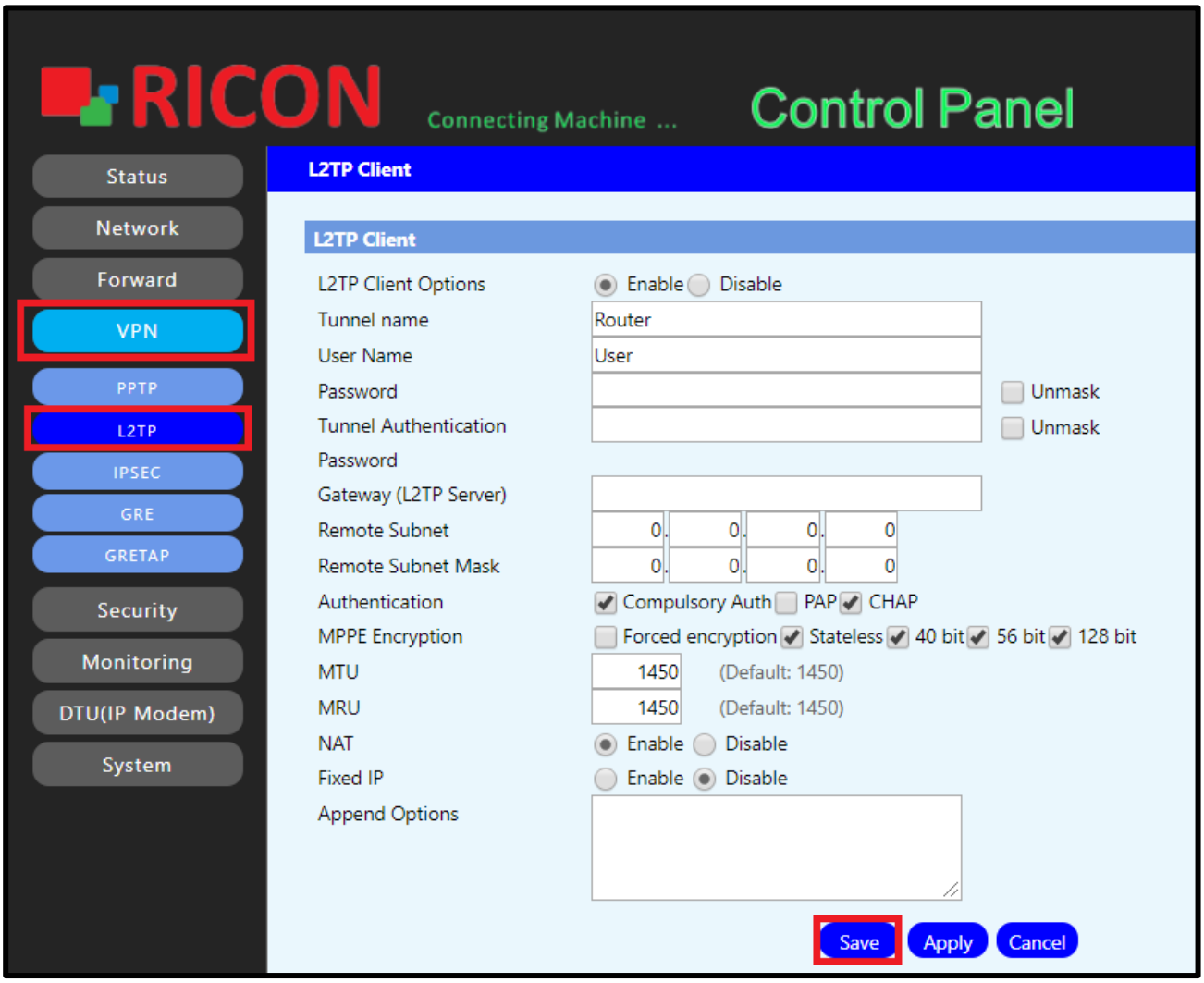

Figure.23- VPN>L2TP

7.3 IPSEC CONFIGURATION

IPsec acts at the network layer, protecting and authenticating IP packets between participating IPsec devices. By following the steps below, S9922L series LTE routers can do IPsec.

- ✓ **Name;** Enter the IPSEC name here.
- ✓ **Mode;**
  - **Tunnel;** Tunnel mode provides confidentiality (ESP) and/or authentication (AH) to the entire original packet, including the original IP headers.
  - **Transport;** Its secure communications between a client and a server. When using the transport mode, only the IP payload is encrypted.
- ✓ **Type;** If the end device to which IPSEC terminates is the server. Server should be chosen.
- ✓ **Local WAN Interface;** The external interface of the S9922L series LTE router must be selected.
- ✓ **Local Subnet;** Enter the local IP block that you want to be encrypted to access the opposite end.
- ✓ **Local Id;** You can enter the local ID as desired.
- ✓ **Use a Pre-Shared Key;** Enter the IPSEC password you specified. You must enter the same password on the end device where the IPSEC terminates.
- ✓ **Peer WAN address;** Enter the external IP of the end device to which IPSEC terminates.
- ✓ **Peer subnet;** Enter the local IP of the end device where IPSEC terminates.
- ✓ **Peer ID;** You can enter the peer ID as desired.
- ✓ **Enable advanced settings;** Enable must be selected.
- ✓ **Encryption;** Mutually the same encryption mode should be selected.
- ✓ **Integrity;** Mutually the same integrity mode should be selected.
- ✓ **DHGrouptype;** Mutually the same group type should be selected.
- ✓ **Lifetime&Keylife;** Mutually the same seconds should be selected.
- ✓ **Link;** Select the external interface priority where you want IPSEC to work.
- ✓ **Debug;** Open debug to see logs.
- ✓ **Remote** Ip; The remote IP of the remote device.
- ✓ Click the **Save** icon to save the configuration.

VPN>IPSEC

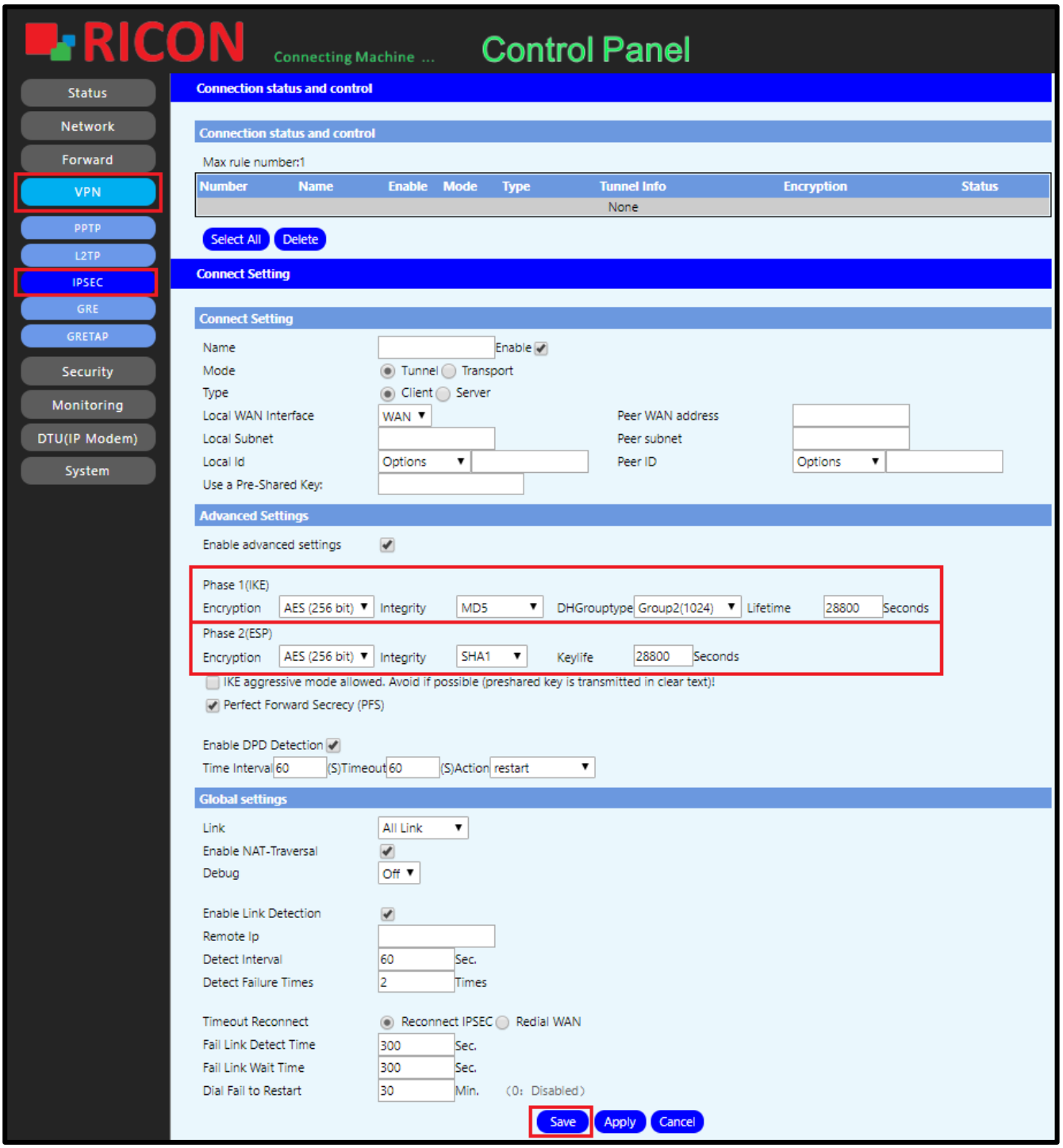

Figure.24- VPN>IPSEC

7.4 GRE CONFIGURATION

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. Follow the steps below to make GRE with the S9922L series LTE router.

- ✓ **Name;** Enter the GRE tunnel name.
- ✓ **Through;** Select the external interface where the GRE tunnel will be active. (WAN / LAN)
- ✓ **Local Tunnel IP;** Enter the IP to forward to the remote router.
- ✓ **Local Network;** Enter the subnet mask to forward to the remote router.
- ✓ **Peer Wan IP Address;** Enter the WAN IP of the remote router.
- ✓ **Peer Tunnel IP;** Enter the IP to which the remote device is tunneled.
- ✓ **Peer Subnet;** Enter the subnet mask to which the remote device is tunneled.
- ✓ Click the **Save** icon to save the configuration.

FORWARD>NAT>SNAT

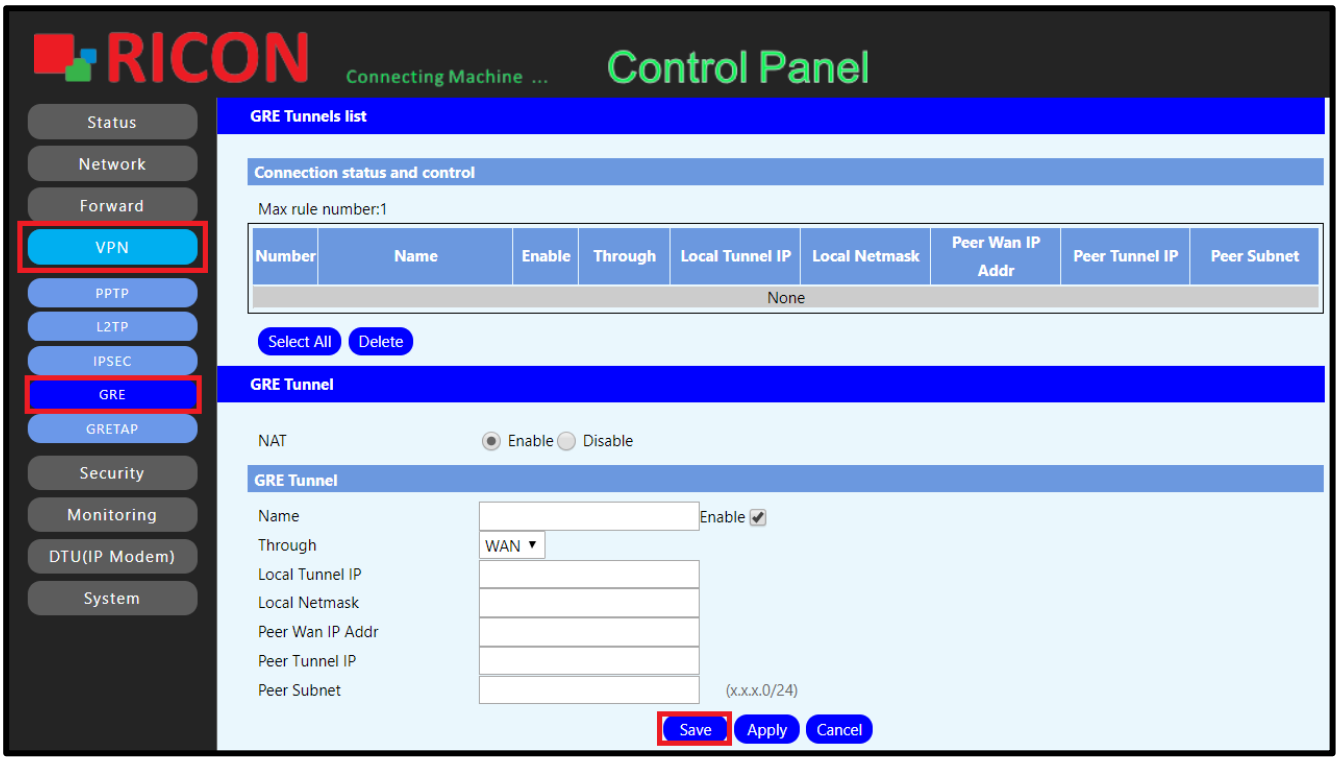

Figure.25- VPN>GRE

7.5 GRETAP CONFIGURATION

GRE is that doesn't dictate what can be encapsulated. When we encapsulate a payload and its ethernet header, it's called GRETAP.

- ✓ **GRETAP Tunnel;** Enable must be selected for the entered GRETAP to be active.
- ✓ **Local IP;** Enter the IP to forward to the remote router.
- ✓ **Remote IP;** Enter the IP to which the remote device is tunneled.
- ✓ Click the **Save** and **Apply** icon to finish.

FORWARD>NAT>SNAT

Figure.26- Forward>NAT>SNAT

8

8. SECURITY CONFIGURATION

8.1 Firewall Configuration

S9922L series LTE routers have their own firewall. Protects users and router against attacks.

- ✓ **SPI Firewall;** Stateful packet inspection is a technology that monitors active connections and checks whether incoming data packets correspond to these connections. It then decides whether to grant or deny permission for them to pass the firewall.
- ✓ **Block Anonymous WAN Requests;** Click the checkbox to ping your WAN IP.
- ✓ **Filtered IDENT;** Internet filter that keeps port 113 from being scanned by devices outside of your local network.
- ✓ **Block WAN SNMP Access;** Simple Network Management Protocol (SNMP) is a set of protocols for network management and monitoring. Click the checkbox to prevent this on the S9922L series LTE router.
- ✓ **Limit SSH Access;** Click the checkbox to turn off SSH access.
- ✓ **Limit Telnet Access;** Click the checkbox to turn off telnet access.
- ✓ **Additional Filters;** If you want filter, click on the checkbox Proxy, Cookies, Java Applets or ActiveX.
- ✓ Click the **Save** icon to save the firewall configuration.

SECURITY>FIREWALL

Figure.27- Security>Firewall

8.2 Access Restrictions

S9922L series LTE router can be made link or keyword access restriction. Time adjustments of restrictions can be made. To do so, follow the steps below.

- ✓ **Policy;** Select the number according to the rule priority.
- ✓ **Status;** Select enable to have the entered access restriction active.
- ✓ **Policy Name;** Enter the rule name.
- ✓ **PCs;** Access restriction can be applied to specific users. Click Edit List of clients to enter the MAC address of the users you want the restriction to apply to.
- ✓ **Days;** Select the days on which the restriction applies.
- ✓ **Times;** Select the times for which the restriction applies.
- ✓ **Website Blocking by URL Address;** Type the link to the page you want to restrict.
- ✓ **Website Blocking by Keyword;** Type the words you want to restrict.
- ✓ Click the **Save** icon to save the restriction configuration.

SECURITY>ACCESS RESTRICTIONS

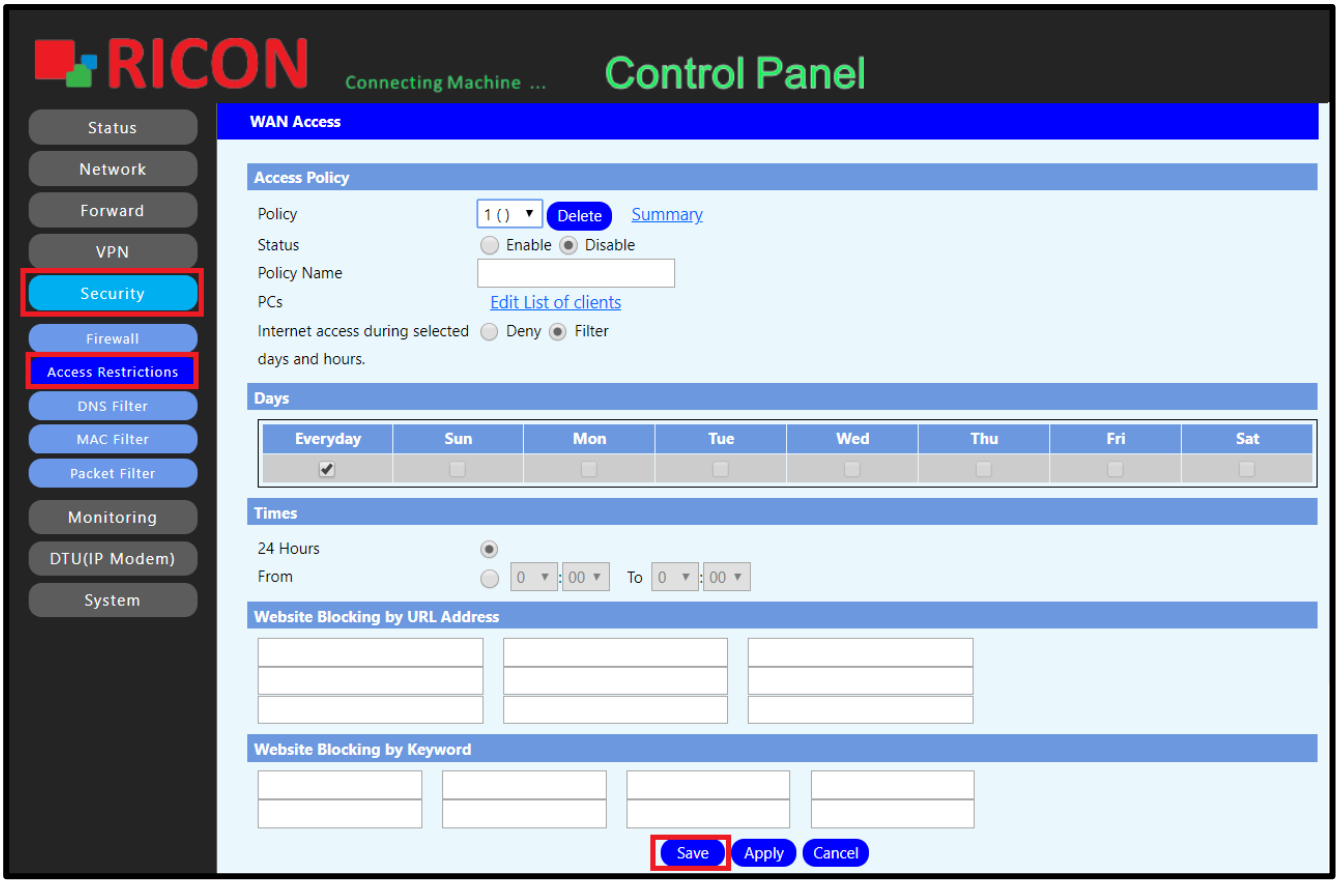

Figure.28- Security>Access Restrictions

8.3 DNS Filter

Domain Name System filter or DNS filtering is a strategy for making it difficult for users to locate specific domains or web sites on the Internet.

- ✓ **Enable DNS Filter;** Select the enable.
- ✓ **Policy for unlisted rules;** Discard the data packets or accept the data packets.
- ✓ **Name;** Enter the DNS that you want to filter.
- ✓ Click **Add** and **Save** icon to save the filtering.

SECURITY>DNS FILTER

Figure.29- Security>DNS Filter

8.4 MAC Filter

S9922L series LTE router can perform MAC filtering. For MAC filtering, follow these steps.

- ✓ **Enable MAC Filter;** Select the enable.
- ✓ **Policy;**
  - Accept only the data packets conform to the following rules; Only connects entered MAC addresses to the router.
  - Discard packets conform to the following rules; Select this to block entered MAC addresses.
- ✓ **Name;** Enter the name here.
- ✓ **MAC;** Enter the MAC address you want to filter.
- ✓ Click **Add** and **Save** icon to save the filtering.

SECURITY>DNS FILTER

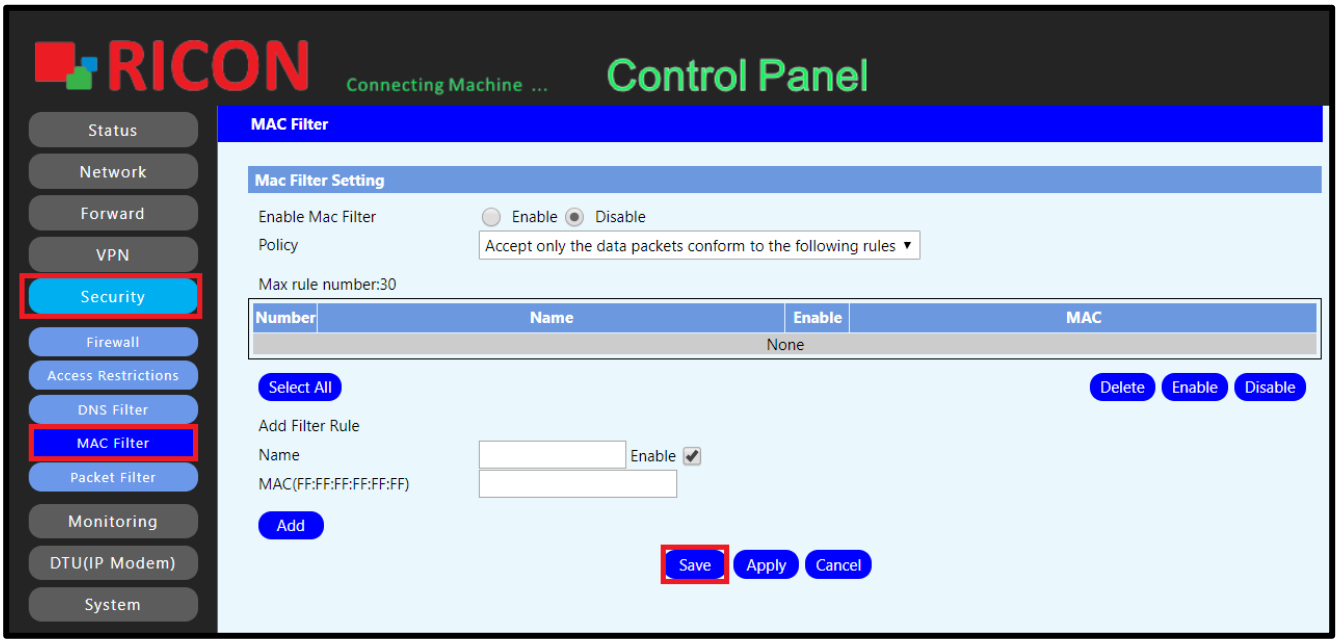

Figure.30- Security>DNS Filter

8.5 NetTest

Packet filtering is a firewall technique used to control network access by monitoring outgoing and incoming packets and allowing them to pass or halt based on the source and destination IP addresses, protocols and ports.

- ✓ **Enable Packet Filter;** Select the enable.
- ✓ **Policy;**
  - Accept only the data packets conform to the following rules; Only entered packet rules apply.
  - Discard packets conform to the following rules; IP addresses entered can not connect to the router.
- ✓ **Name;** Enter the name here.
- ✓ **Dir;** Select the direction you want to filter.
- ✓ **Pro;** Select the protocol.
- ✓ **Source IP;** Enter the IP block you want to forward or block.
- ✓ **Destination IP;** Enter the IP block that you want not to reach.
- ✓ Click **Add** and **Save** icon to save the filtering.

SECURITY>PACKET FILTER

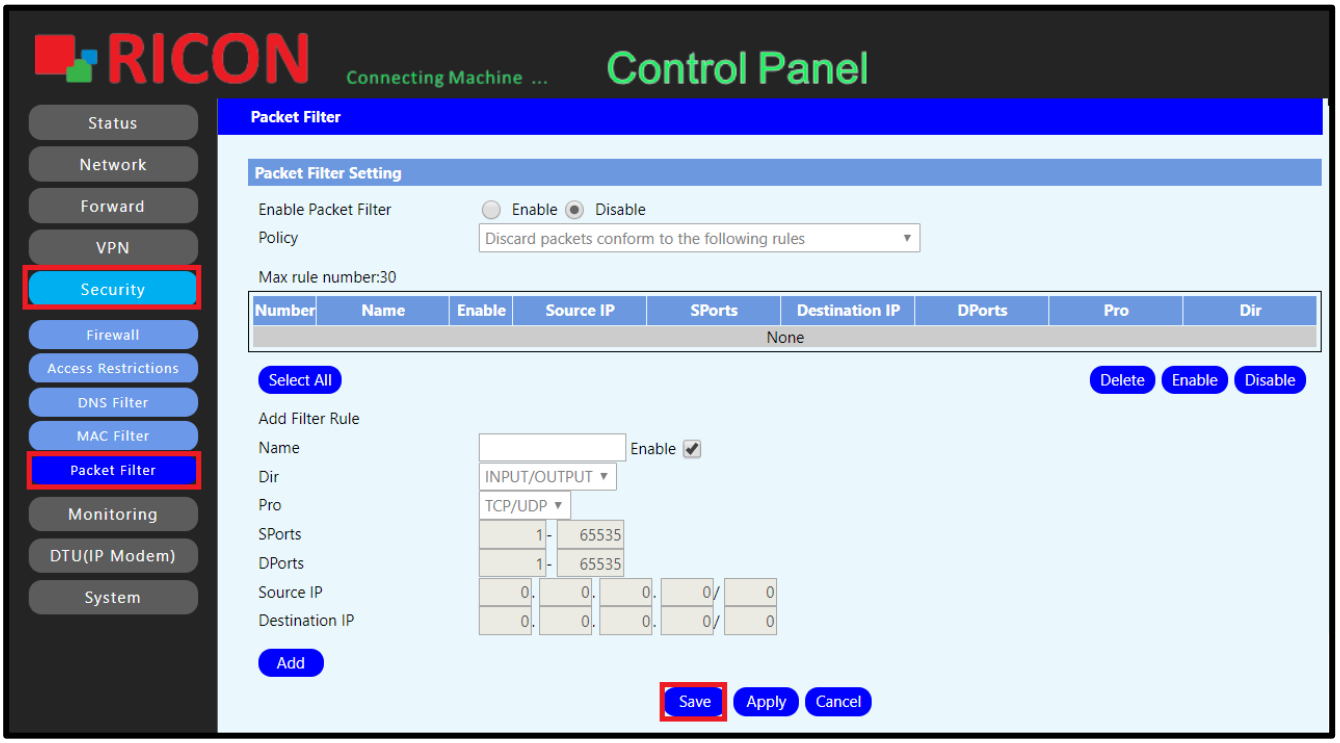

Figure.31- Security>Packet Filter

9

9. MONITORING

In the monitoring section, the traffic passing over the S9922L series LTE router can be displayed.

9.1 Traffic Monitor

Here you can graph the traffic passing through the interfaces and users of the router.

MONITORING>TRAFFIC MONITORING

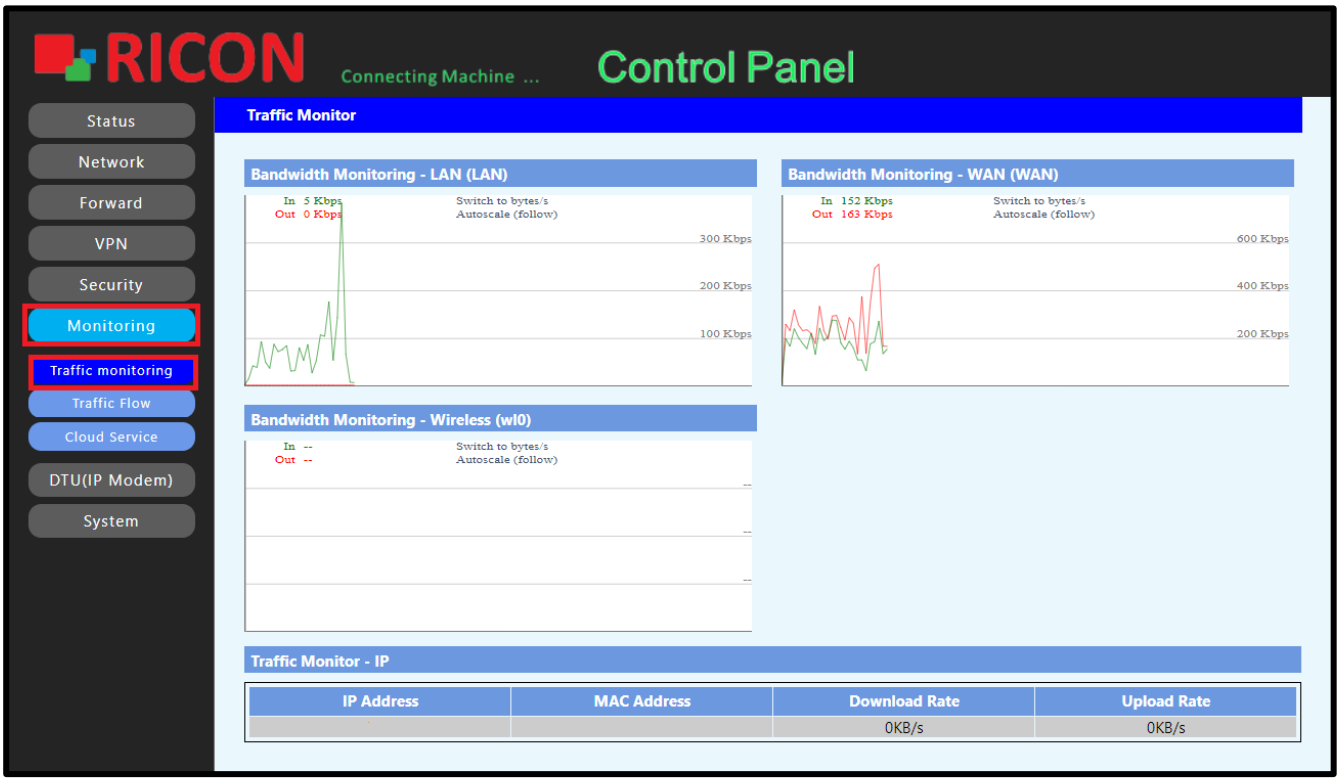

Figure.32- Monitoring>Traffic monitoring

9.2 Traffic Flow

From this interface, you can observe daily and total data passing through the router. You can turn off this feature by clicking Disable or you can clear the existing information by clicking Clear.

MONITORING>TRAFFIC FLOW

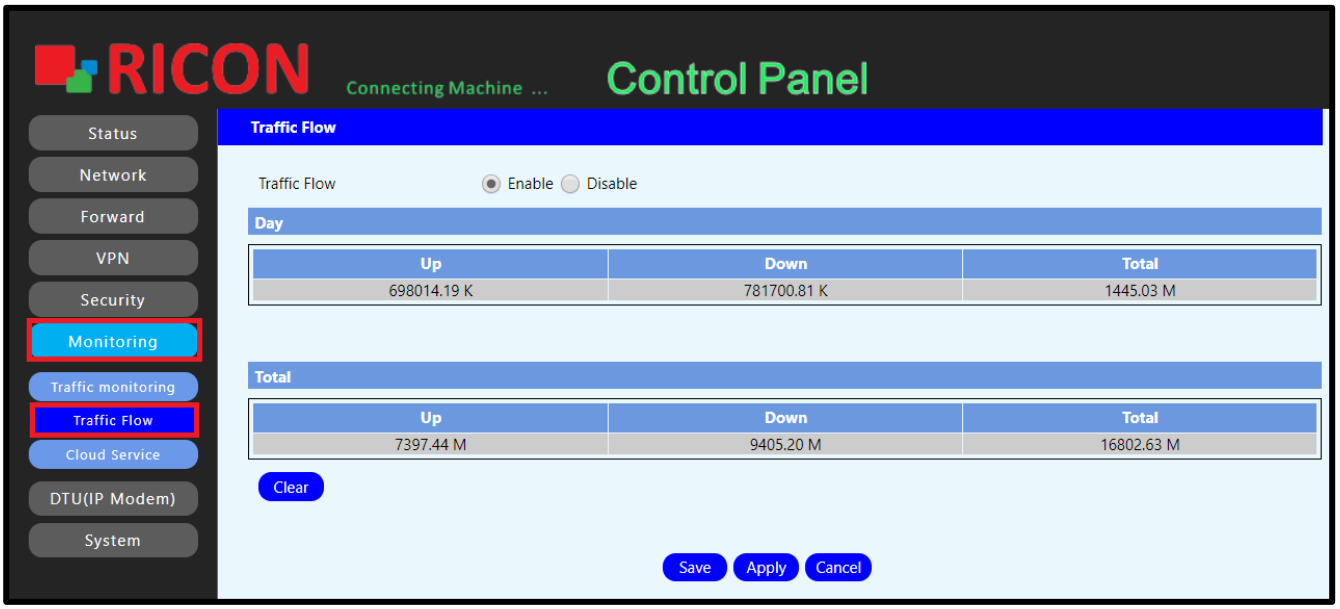

Figure.33- Monitoring>Traffic Flow

9.3 Cloud Service

The Ricon Management System (RMS) is activated from the Cloud Service interface. With RMS, you can monitor the current status of multiple Ricon S9922L series LTE routers from a single interface.

- ✓ **Cloud Service;** Select the enable.
- ✓ **Virtual Interface;** Select the port that accesses the RMS.
- ✓ **Server IP/Domain;** Enter the IP of the RMS.
- ✓ **Server Port;** Enter the RMS server port.
- ✓ **Report Status;** Select enable to report the current status
- ✓ **Report Interval;** Enter the reporting period.
- ✓ **Report Log;** Select enable if the S9922L series LTE router is required to report logs.
- ✓ **Report Interval;** Log reporting time duration.
- ✓ Click **Save** icon to finish.

MONITORING>CLOUD SERVICE

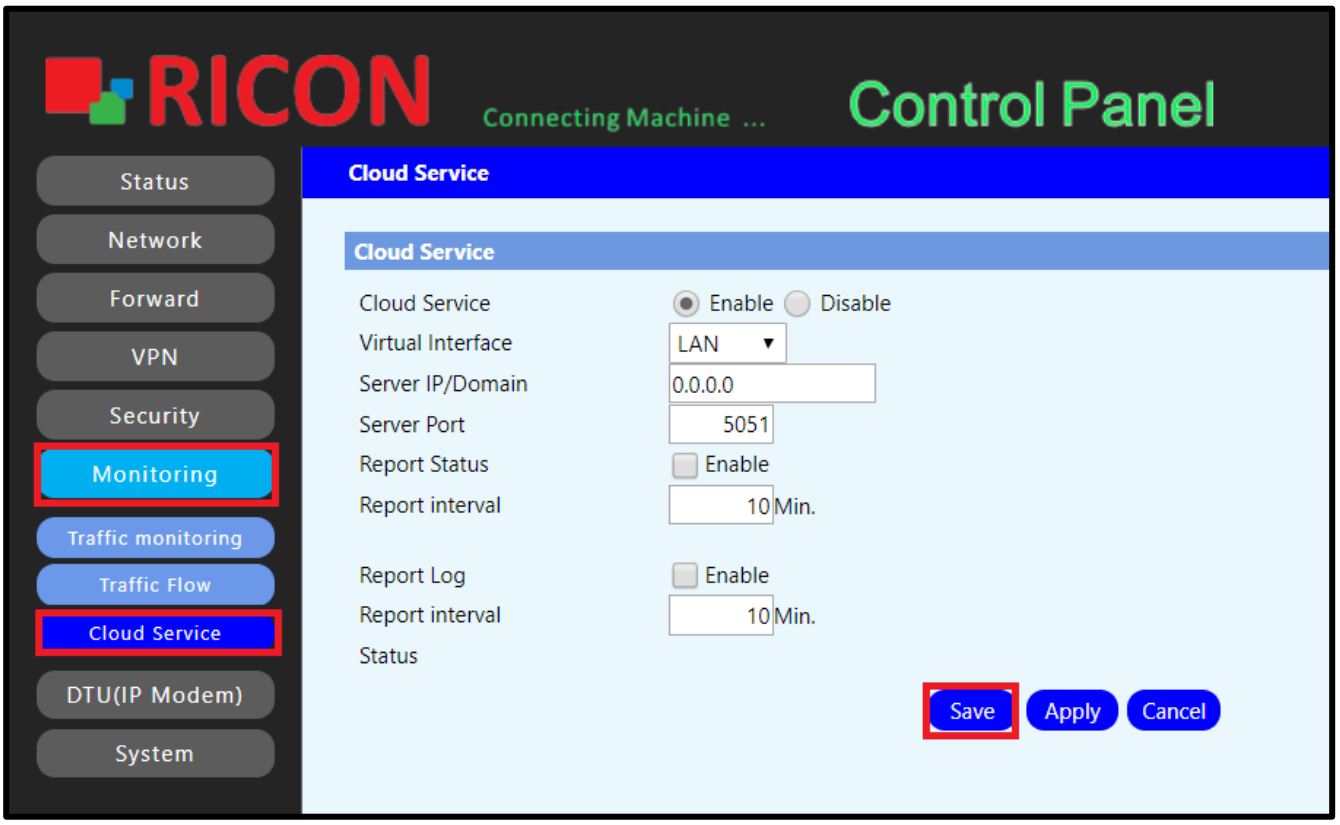

Figure.34- Monitoring>Cloud Service

11

10. SYSTEM

You can configure the system setting from this header.

11.1 Password

You can change username and password here. Then click **Save** icon.

SYSTEM>PASSWORD

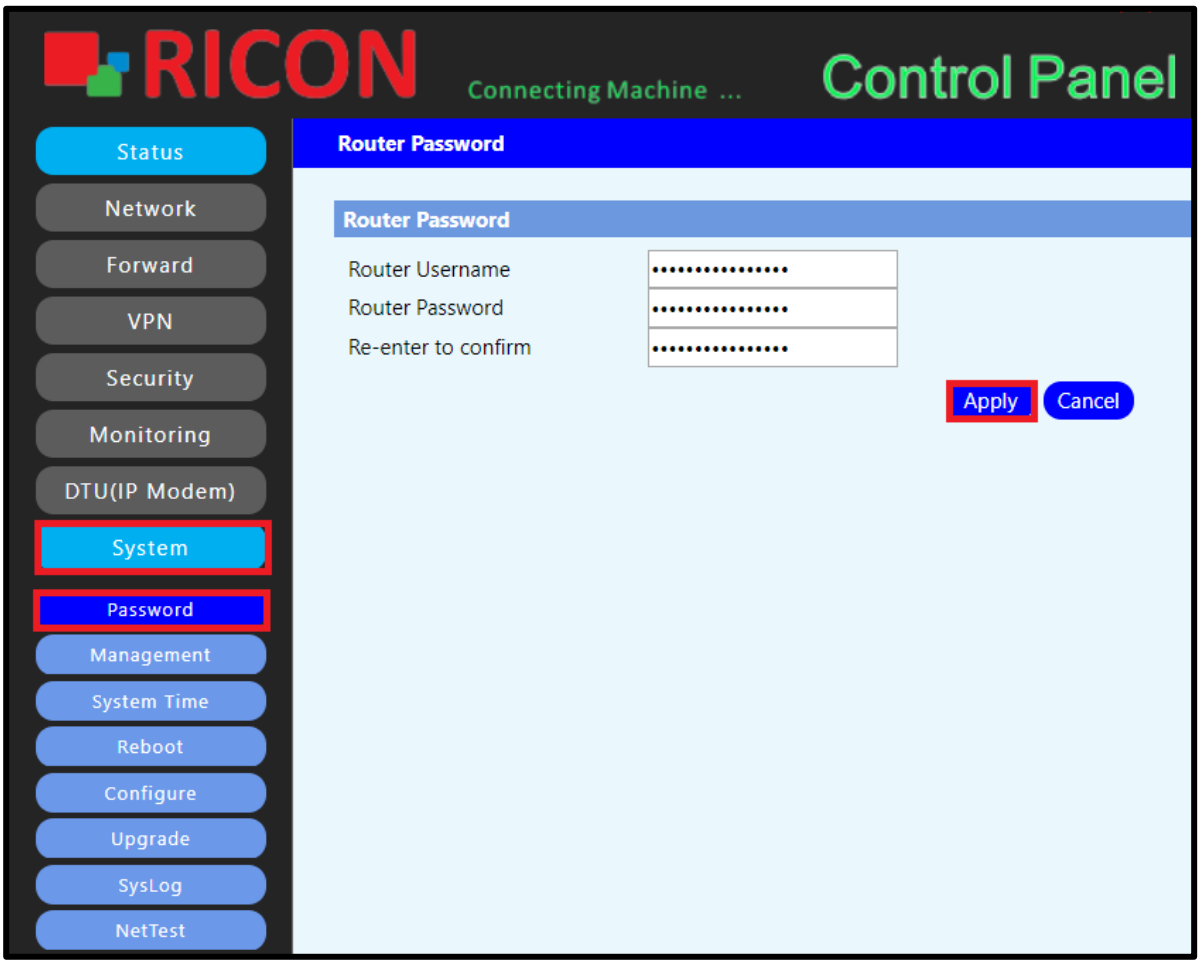

Figure.38- System>Password

11.2 Management

The access management configuration of the S9922L series LTE router can be done through this interface.

Web Access

- ✓ **Protocol;** HTTP, HTTPS. HTTP is unsecured while HTTPS is secured. HTTP sends data over port 80 while HTTPS uses port 443. HTTP
- ✓ **Local Web GUI Port;** The desired port for access to the router interface via the local web.
- ✓ **Telnet;** Enable should be selected if the router is to be open from local to telnet.

Remote Access

- ✓ **SSH;** Enable should be selected If the router is to be available for SSH access.
- ✓ **Web GUI Management;** Enable should be selected if the device is to be available for remote web access.
- ✓ **Web GUI Port;** The desired port for access to the router interface via the remote web.
- ✓ **SSH Management;** Enable should be selected if the device is to be enabled for remote SSH access.
- ✓ **SSH Remote Port;** Port required for remote access to the router via SSH.
- ✓ **Telnet Management;** Enable should be selected if the router is to be open to remote telnet access.
- ✓ **SNMP; Select enable to turn the router on to SNMP.**
- ✓ Click **Save** icon to finish.

SYSTEM>MANAGEMENT

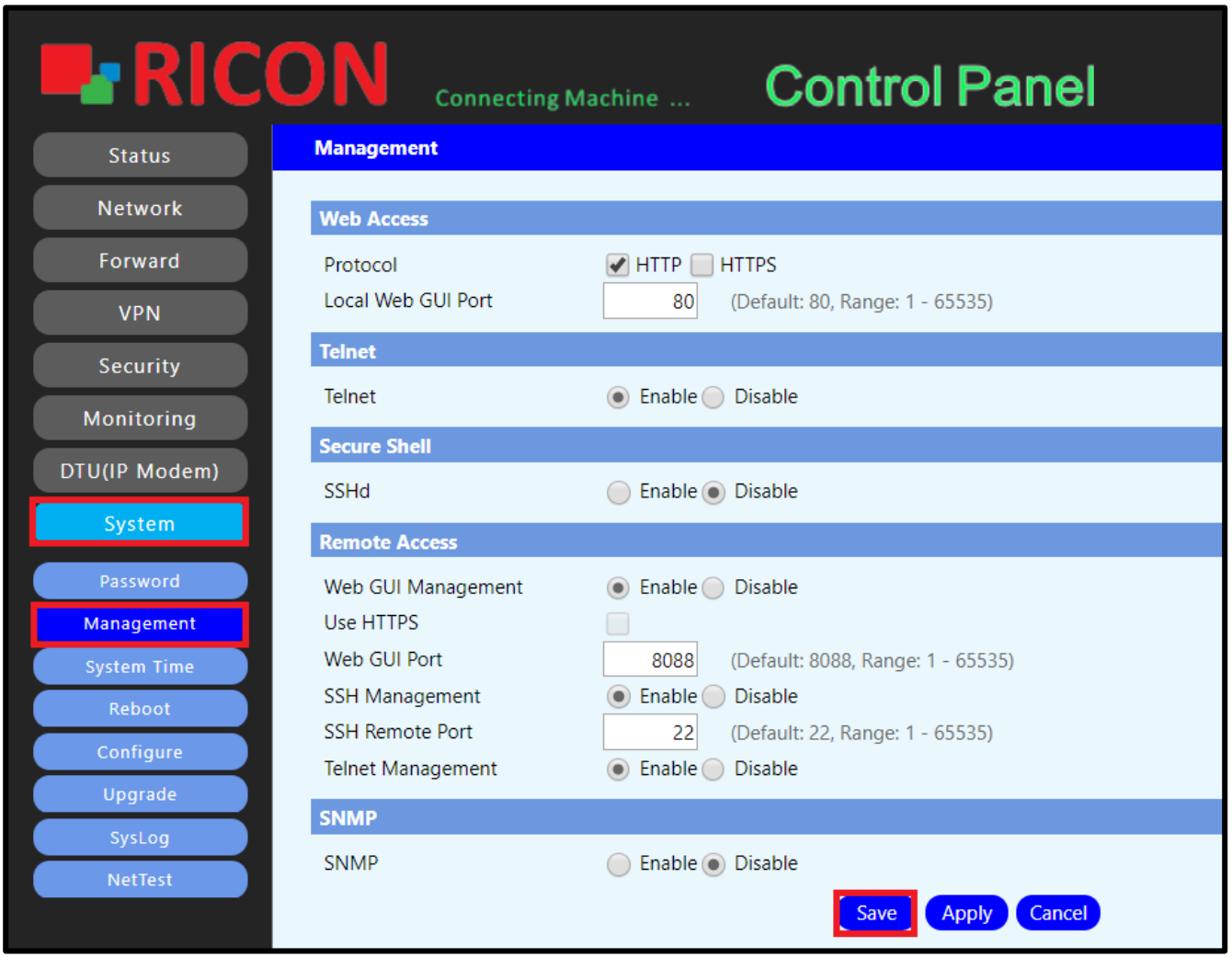

Figure.39- System>Management

11.3 System Time

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.

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

- ✓ **System Time;** Shows the current time of the device.
- ✓ **Time of PC;** If auto is clicked the computer clock used is automatically set to the device clock.
- ✓ **Manuel;** Enter the date manually and click on the manual.
- ✓ **NTP Client;** Select enable to set the date with the NTP client.
- ✓ **Time Zone;** Select the time zone of your area.
- ✓ **Server IP/Name;** Enter the IP or name of the NTP client server.
- ✓ **Interval;** Enter the update interval of the date with. NTP.
- ✓ Click **Save** icon to finish.

SYSTEM>SYSTEM TIME

Figure.40- System>System Time

11.4 Reboot

The S9922L series LTE router can automatically reboot at specified intervals or at specific times. The router can also be restarted from this interface. Follow these for configuration.

- ✓ **Schedule Reboot;** Click enable to make the configuration active.
- ✓ **Interval;** If you want to restart the device periodically, enter the time interval here.
- ✓ **Time;** If you want the device to restart on a specific date of the week, enter the date here.
- ✓ Click **Save** icon to finish.

- ✓ Click the **Reboot** icon to restart the device.

SYSTEM>REBOOT

Figure.41- System>Reboot

11.5 Configure

This interface is used to reset the configuration of the S9922L series LTE router, to make a backup and load the ready configuration.

- ✓ **Restore Factory Defaults;** Click **Yes** in the **Restore Factory Defaults** section to completely delete your config file and reset the device.
- ✓ **Backup;** Click the **Backup** tab in the **Backup Configuration** section to back up the currently configured config file to your computer.
- ✓ **Restore Settings;** To upload a config file that is already on your computer to the router, select your file from the **Choose File** section of the **Restore Configuration** tab. Then click the Restore button.

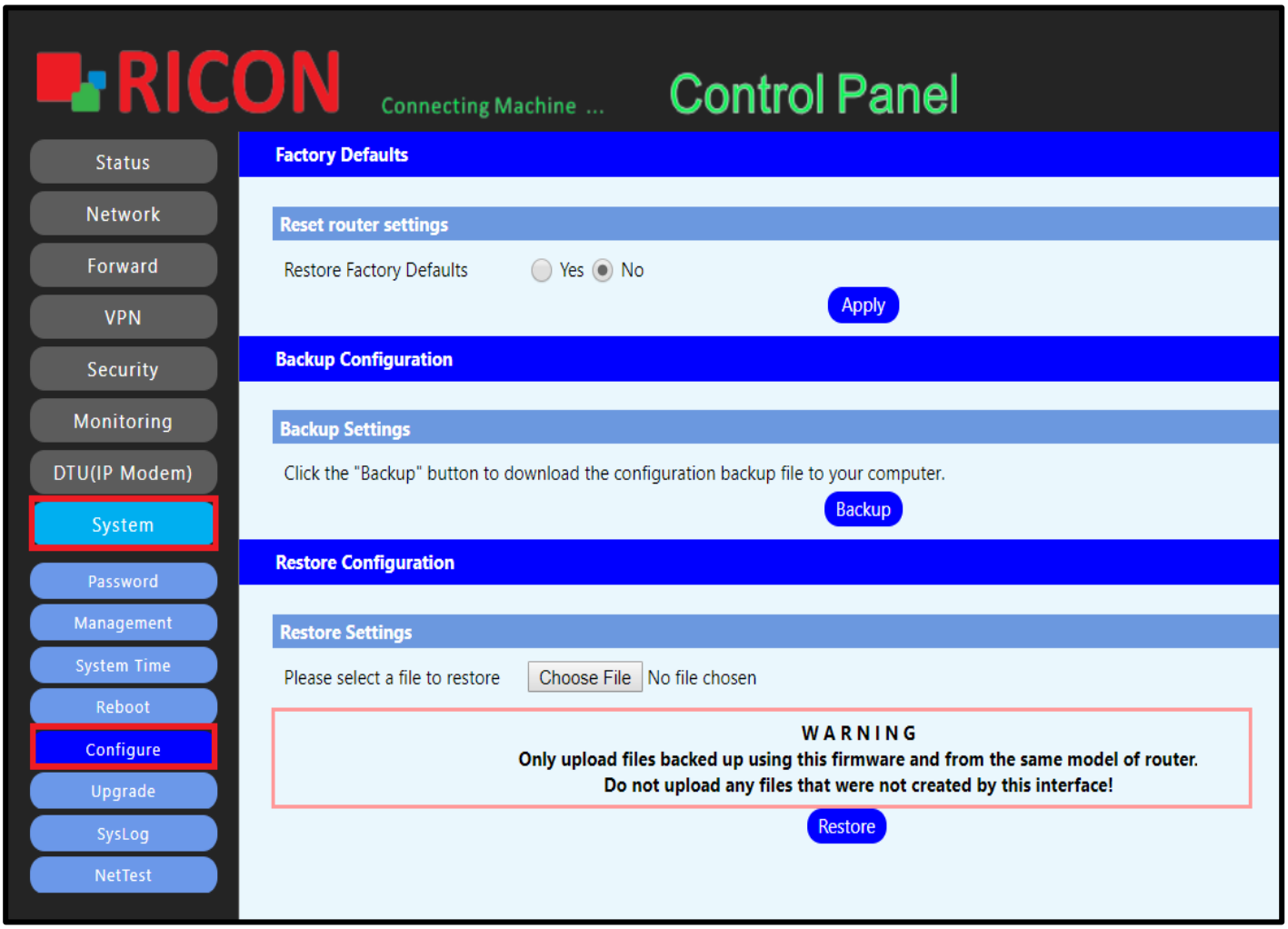

Figure.42- System>Configuration

NOTE:

- *Only upload files backed up using this firmware and from the same model of router. Do not upload any files that were not created by this interface.*

11.6 Upgrade

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.

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

SYSTEM>UPGRADE

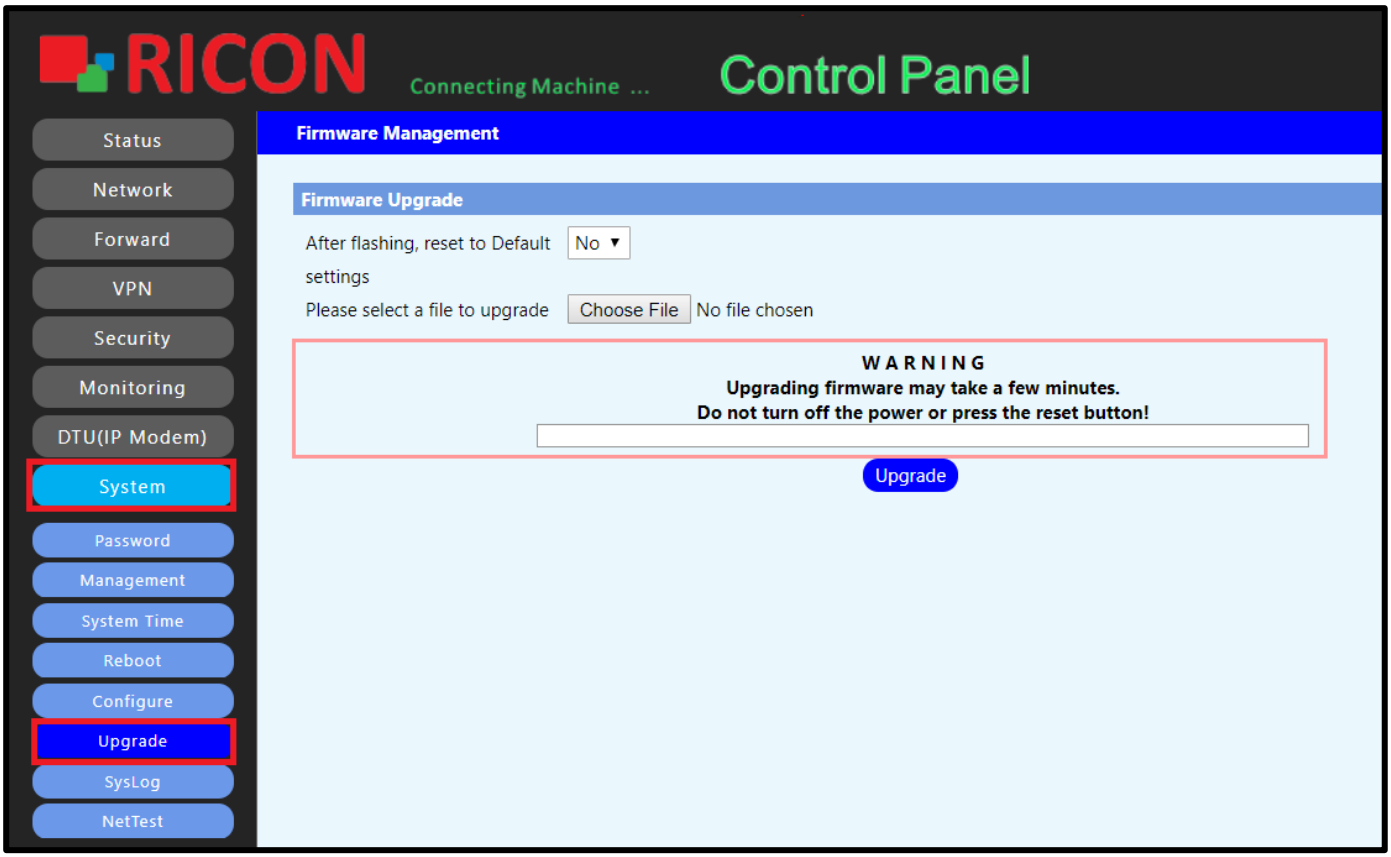

Figure.43- System>Upgrade

11.7 SysLog

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.

- ✓ You can View instant Message Logs
- ✓ To clear the old log and see the current logs, select **Delete**.
- ✓ To export logs, select **Backup** after viewing.

SYSTEM>SYSLOG

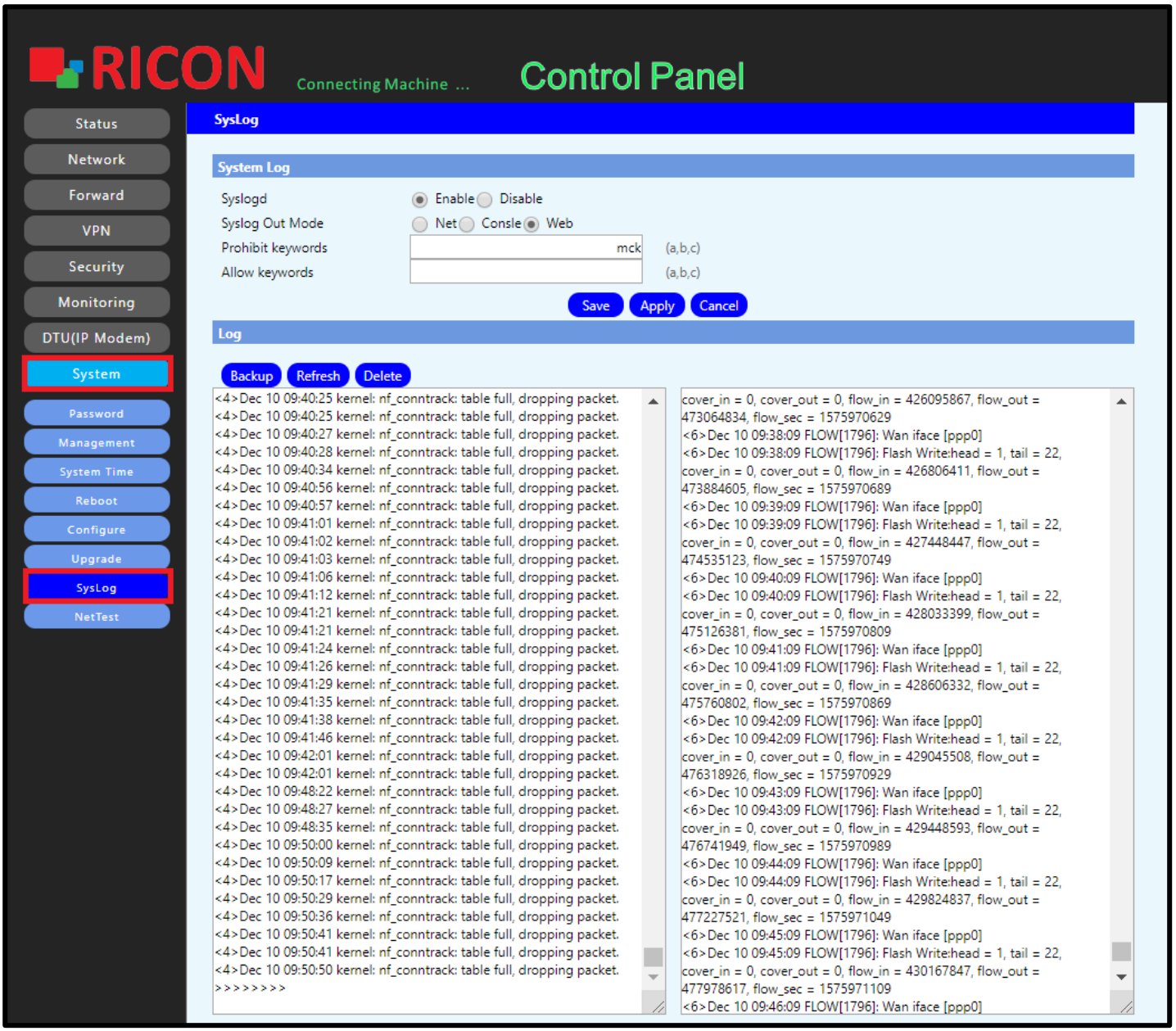

Figure.44- System>SysLog

11.8 NetTest

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;

- ✓ In the NetTest box, enter the IP you want to ping or trace.
- ✓ Click the **Ping** and Run Commands and wait.
- ✓ Click the **Trace** and Run Commands and wait.

SYSTEM>NETTEST

Figure.45- System>NetTest