Case Communications

6944 Industrial Router

Full Manual

With Configuration

Examples

Rev 2.8

This page left blank intentionally

REVISION HISTORY

Manual	Date	Firmware Version	Revision Details
V1.0.0.	May 2018		Initial release.
V1.1.0	Aug 2018		Add Schedule Reboot, OpenVPN, IPSec
V1.1.1	Oct 2018		Add SSH, GRE, VRRP, Wi-Fi Client
V1.2.0	Jun 2019	v1.1.0(278c6c6)	Add Data Roaming, IP Passthrough, SMS, GRE Layer2. AT Debug, APP structure
V.1.2.1	Jun 2019	v1.1.0 (ddcaac4)	Add SMS Gateway, SMS Notification
V.1.2.2	Sept 2019	V1.1.0 (addcaac4)	Added MODBUS Slave feature – Appendix 9
V.2.3	Sept 2019	V1.1.0 (addcaac4)	Added SMS Reboot missing from manual
V2.4	Feb 2020	V1.1.0 (addcaac4)	Added MODBUS Master Appendix F
V2.5	June 2020	V1.1.3(e335ec6)	Added Dynamic Routing and SNMP
V2.6	Sept 2020	V1.1.3(e335ec6)	Added section on testing Open VPN from PC
V2.7B	Jan 2021		Added Configuration examples
V2.8	Jan 2022	1.1.7 (cf8c6a1)	RADIUS (802.1X) Authentication added

Trademarks and copyright

Disclaimers

Information in this document is subject to change without notice and does not represent a commitment on the part of Case Communications.

Case Communications provides this document as is, without warranty of any kind, either expressed or implied, including, but not limited to, its particular purpose. Case Communications may make improvements and/or changes in this manual, or in the product(s) and/or the program(s) described in this manual at any time. Information provided in this manual is intended to be accurate and reliable. However, Case Communications assumes no responsibility for its use, or for any infringements on the rights of third parties that may result from its use.

Technical Support

E-mail: support@case.uk.com

Web: www.casecomms.com

Interference Issues

Avoid possible radio frequency (RF) interference by following these guidelines:

- The use of cellular telephones or devices in aircraft is illegal. Use in aircraft may endanger operation and disrupt the cellular network. Failure to observe this restriction may result in suspension or denial of cellular services to the offender, legal action, or both.
- Do not operate in the vicinity of gasoline or diesel fuel pumps unless use has been approved or authorized.
- Do not operate in locations where medical equipment that the device could interfere with may be in use.
- Do not operate in fuel depots, chemical plants, or blasting areas unless use has been approved and authorized.
- Use care if operating in the vicinity of protected personal medical devices, i.e., hearing aids and pacemakers.
- Operation in the presence of other electronic equipment may cause interference if equipment is incorrectly protected. Follow recommendations for installation from equipment manufacturers.

Declaration of Conformity

The 6944 Series products are in conformity with the essential requirements and other relevant provisions of the CE and RoHS.

TABLE OF CONTENTS

This page left blank intentionally

1. PRODUCT OVERVIEW

1.1. Overview

The Case Communications 6944 series industrial cellular VPN router offers a single, flexible platform to address a variety of wireless communications needs with over-the-air configuration and system monitoring for optimal connectivity. This router enables wireless data connectivity over public and private LTE cellular networks at 4G speeds.

The 6944 series router has dual SIM's for backup, 2 or 4 LAN ports, 1 port could be changed to Ethernet WAN connection (for fixed internet fail over to cellular). An optional 802.11 b/g/n Wi-Fi interface access point and client operations supports connectivity to IP applications in a variety of different connection scenarios. RS232 and RS485 interfaces are provided to support Serial to IP communication. The 6944 series router also support 2 x digital input and 2 x Digital output for alarm applications.

The 6944 series router supports 9 to 48 VDC wide range power inputs, designed with reverse-voltage protection mechanism for greater reliability. It is an advanced choice for universal wireless M2M applications with reliable features for data transmission.

1.2. Features and Benefits

Industrial internet access

- Wireless Mobile Broadband 2G / 3G / 4G Connection
- Remote access to SCADA System for Industrial Automation
- Reduce high costs for on-site maintenance

Designed for industrial usage

- Power Input Range 9 to 48 VDC
- Industrial designed for harsh environment
- Compact metal casing for easy mounting

Secure and reliable remote connection

- Connection manager ensure seamless communication
- Support Multiple VPN tunnels for data encryption
- Firewall prevents unsafe and unauthorized access

Easy to use and easy maintenance

- User-friendly web interface for human interaction
- Easy configuration for deployment
- Support 3rd Party remote management cloud

1.3. General Specifications

Cellular Interface

- Standards: FDD-LTE/TDD-LTE, WCDMA/UMTS/HSPA/HSPA+/EDGE/GPRS,
- 2× SMA female antenna connector
- 2 x SIM (3.0V & 1.8V)

Wi-Fi Interface (Optional)

- Standards: 802.11b/g/n, 300Mbps
- 2 x RP-SMA male antenna connector
- Support Wi-Fi AP and Client modes
- Security: WEP, WPA and WPA2 encryption
- Encryption: TKIP, CCMP

Ethernet Interface

- Standard: IEEE 802.3, IEEE 802.3u
- Number of Ports: 6944: 4 x 10/100 Mbps, RJ45 connector
- 1 x WAN interface (configurable on Web GUI)
- 1.5KV magnetic isolation protection

Serial Interface

- 1×RS232 (3 PIN): TX, RX, GND
- 1 x RS485 (2 PIN): Data+(A), Data-(B)
- Baud rate: 300 bps to 115200 bps
- Connector: terminal block
- 15KV ESD protection

DI/DO Interface

- Type: 2 x DI + 2 x DO
- Connector: terminal block
- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: 36VDC
- Absolute maximum ADC: 100mA

DI/DO Interface

- Type: 2 x DI + 2 x DO
- Connector: terminal block
- Isolation: 3KVDC or 2KVrms
- Absolute maximum VDC: 36VDC
- Absolute maximum ADC: 100mA

Other Interfaces

- 1× RST button
- LED instruction: 1 x SYS, 1 x NET, 1 x USR, 3 x RSSI

Software

- Network protocols: DHCP, ICMP, PPPoE, HTTP, HTTPS, DNS, VRRP, NTP…
- VPN: IPSec, GRE, OpenVPN, DMVPN
- Policy: RIPv1/RIPv2/OSPF/BGP dynamic route (optional)
- Firewall & Filter: Port forwarding, DMZ, anti-DoS, ACL
- Serial port: TCP server and client, UDP
- Management: Web, 3rd party platform

Power Supply and Consumption

- Connector: 3-pin 3.5 mm female socket with lock
- Input voltage range: 9~48VDC
- Power consumption:

  Idle: 100 mA@12V

  Data link: 400 mA (peak) @12V

Physical Specification

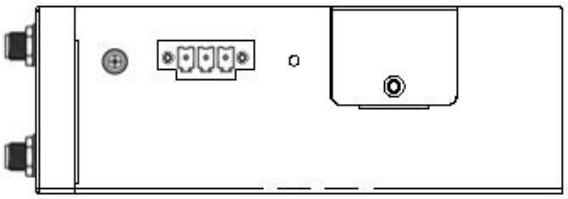
- Ingress Protection: IP30
- Housing & Weight: Metal, 300g
- Dimension: 104mm x 104mm x 38mm (excluding antenna)
- Installations: Din-rail mounting

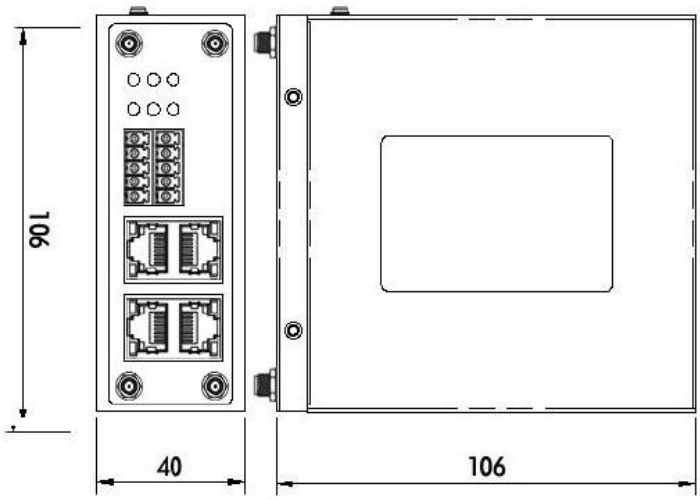
Environmental

- Operation temperature: -40~+75℃
- Store temperature: -40~+85℃
- Operation humidity: 5% to 95% non-condensing

1.4. Mechanical Specifications

Dimension: 104mm x 104mm x 38mm (excluding antenna)



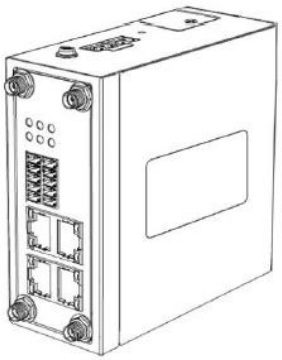


1.5. Packaging Checklist

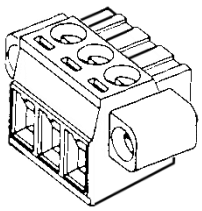
The 6944 series Router includes the parts shown in below, please verify your components.
NOTE: if any of the below items is missing or damaged, please contact your sales representative.

Equipment Included

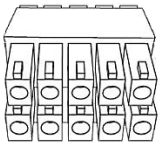
- 1 x Case Communications 6944 Series Industrial Cellular VPN router with Wi-Fi



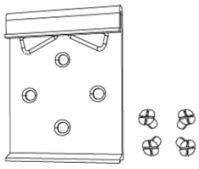
- 1 x 10-pin 3.5 mm male terminal block for RS232/RS485/DI/DO



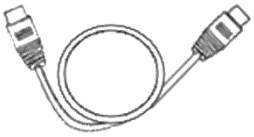
- 1 x 3-pin 3.5 mm male terminal block with lock for power supply



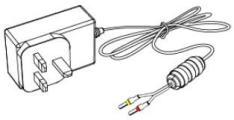
- 35mm Din-rail mounting kit



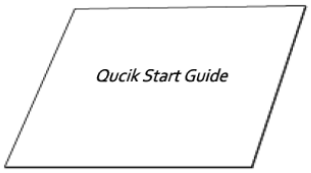
- 1 x Ethernet cable



- AC/DC power adapter (12VDC, 1.5A; EU/US/UK/AU plug optional)



- 1 x Quick Start Guide

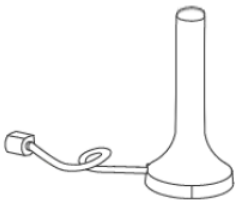


Optional Accessories (sold separately)

- 3G/4G cellular antenna

Stubby antenna

Magnet antenna

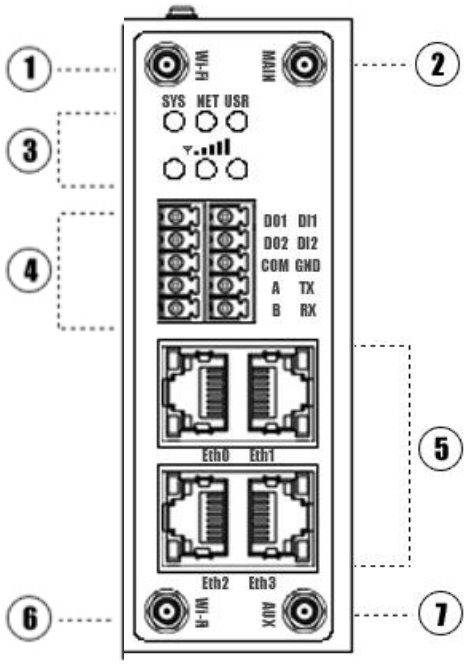


This page left blank intentionally

2 INSTALLATION

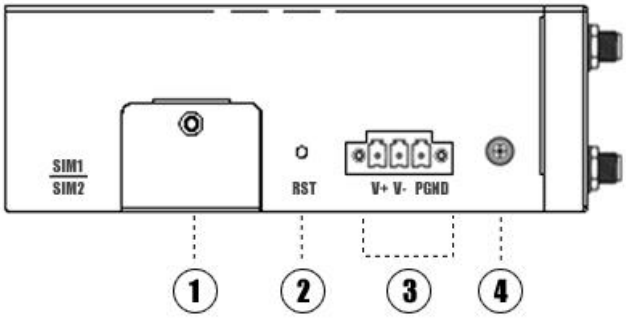
2.1. Product Overview

- **Front Panel**



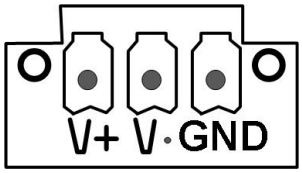
① Wi-Fi Antenna
② MAIN Cellular Antenna
③ LED Indicator
④ Serial port & DIDO
⑤ Ethernet port
⑥ Wi-Fi Antenna
⑦ AUX Cellular Antenna

- **Left Side Panel**



① SIM Card Slot
② Reset Button
③ Power Connector
④ Grounding Stud

- **Power Input**



PIN	Description
V+ (Red line)	Positive
V- (Yellow line)	Negative
PGND	GND

2.2. LED Indicators

Name	Color	Status	Description
SYS	Green	Slow Blinking (500ms duration)	Operating normally
		Fast Blinking	The 6944 is initialising
		Off	Power is off
NET	Green	On	Registering to Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network).
		Fast Blinking (500ms duration)	Registering to Non-Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network, then WCDMA and GPRS is non-highest priority network).
		Off	Registration has failed
USR: SIM	Green	On	The 6944 is trying cellular connection with SIM1
		Fast Blinking (250ms duration)	The 6944 is trying cellular connection with SIM2
		Off	No SIM detected
USR: Wi-Fi	Green	On	Wi-Fi is enabled but without data transmission
		Blinking	Wi-Fi is enabled and data transmission
		Off	Wi-Fi is disable or initialize failed
Signal Strength Indicator	Green	On, 3 LED light up	Signal strength (21-31) is high
		On, 2 LED light up	Signal strength (11-20) is medium
		On, 1 LED light up	Signal strength (1-10) is low
		Off	No signal

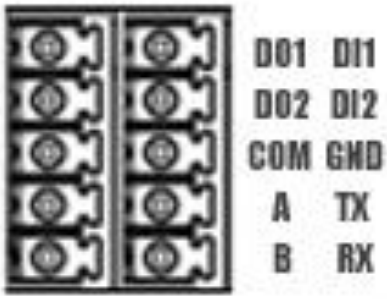
2.3. Ethernet Port Indicator

Name	Status	Description
Link indicator	On	Connection is established
	Blinking	Data is being transmitted
	Off	Connection is not established

NOTE：There are two LED indicators for each Ethernet port. Due to the chipset design the 6944 router will only light up the Green LED (Link indicator) on left side, if the right LED is Off it has no meaning

2.4. Ethernet Port Indicator

PIN	RS232	RS485	DI	DO	Direction
1	--	--	--	DO1	Router-->Device
2	--	--	--	DO2	Router-->Device
3	--	--	--	COM	--
4	--	A	--	--	Router<-->Device
5	--	B	--	--	Router<-->Device
6	--	--	DI1	--	Router<--Device
7	--	--	DI2	--	Router<--Device
8	GND	--	--	--	--
9	TX	--	--	--	Router-->Device
10	RX	--	--	--	Router<--Device



PIN	Description
V+ (Red line)	Positive
V- (Yellow line)	Negative
PGND	GND

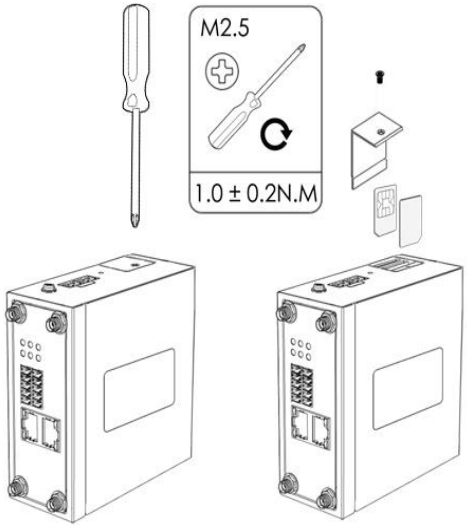
2.5. Reset Button

Function	Action
Reboot	Press the RST button within 3s under operation status
Factory Reset	Press the RST button between 3s to 10s, all LEDs blink few times then reboot the router manually.
Run Normally	Press the RST button more than 10s, router will run normally without reboot or factory reset.

2.6. Insert SIM card

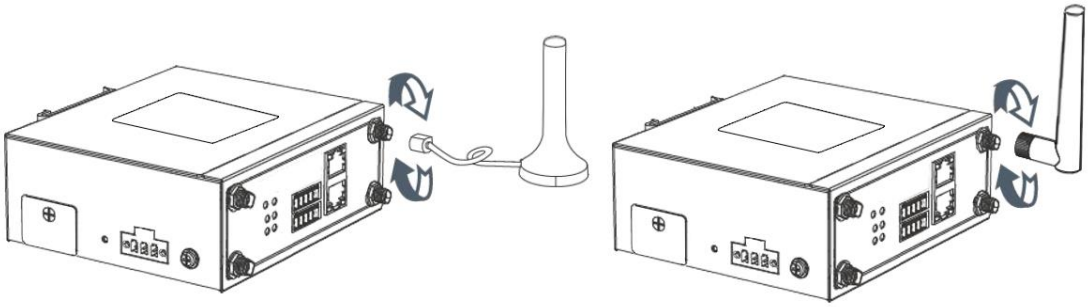
- **Insert / Remove SIM card**

1. Make sure the power is disconnected.
2. Use a Phillips-head screwdriver to remove SIM slot cover.
3. Insert the SIM card(s) into the SIM sockets.
4. Replace the SIM slot cover.



2.7. Installing the Antenna

- **Connect the cellular antenna to the MAIN and AUX connector on the unit.**

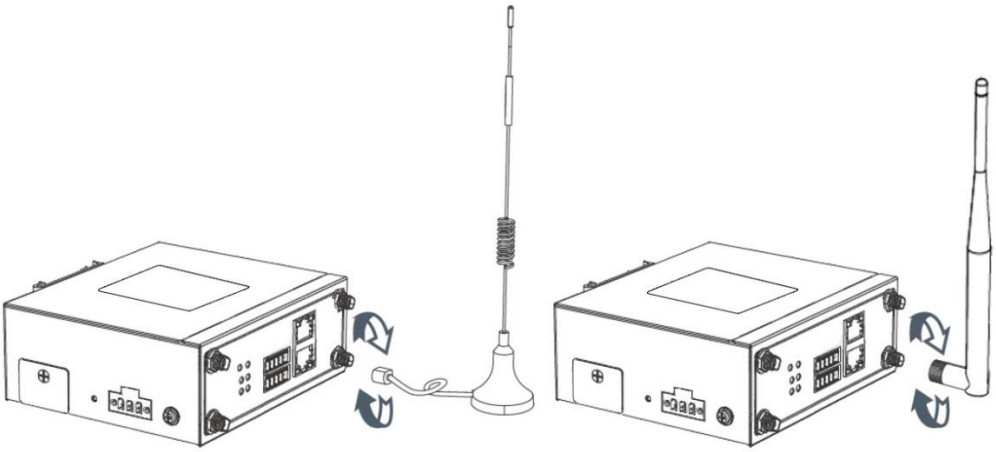


NOTE: The 6944 router supports dual antennas with MAIN and AUX connectors. The MAIN connector is for receiving and transmitting data. The AUX connector is for enhancing the signal strength, and should be used with the MAIN Antenna.

- **Connect the Wi-Fi antenna to the Wi-Fi connector on the unit.**

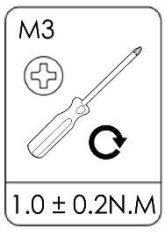
Please follow the picture below to install the Wi-Fi antenna in the right position before testing.

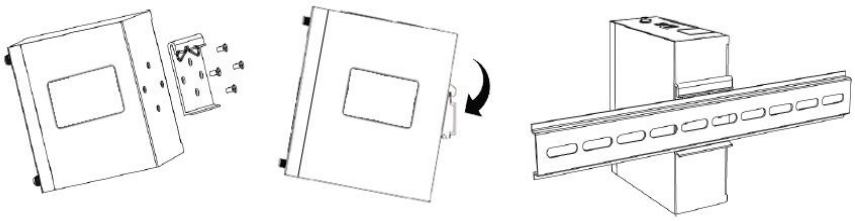
The Wi-Fi connectors are clearly marked on the 6944, both should be fitted to ensure the best quality Wi-Fi signal. The Wi-Fi antenna are, (depending on the model of antenna used), longer than the Cellular antenna and the Wi-Fi Antenna connectors are female, i.e. they don't have a pin.



2.8. DIN-Rail Mounting

1. Use 4 pcs of M3x6 flat head Phillips screws to fix the DIN-rail to the router.
2. Insert the upper lip of the DIN-rail into the DIN-rail mounting kit.
3. Press the router towards the DIN-rail until it snaps into place.

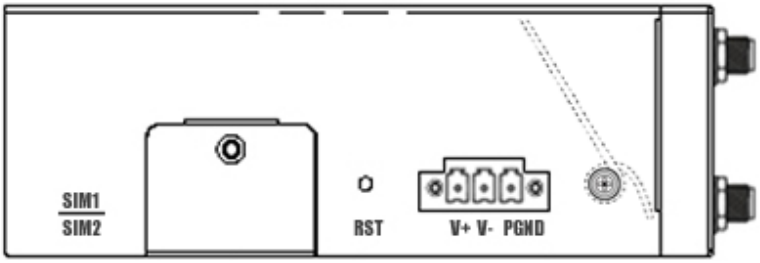




2.9. Protective Grounding Installation

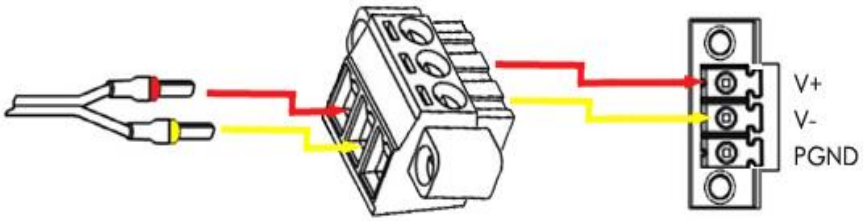
1. Remove the grounding nut.
2. Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.

   NOTE: Strongly recommended the router to be grounded when deployed



2.10. Power Supply Installation

1. Remove the pluggable connector from the unit, then loosen the screws for the locking flanges as needed.
2. Connect the wires of the power supply to the terminals.



COLOR	POLARITY
RED	V+
YELLOW	V-

2.11. Powering On The 6944 Router

1. Connect one end of the Ethernet cable to the LAN port on the unit and the other end to a LAN port on a PC.
2. Connect the AC power to a power source.
3. Router is ready when SYS LED is blinking.

This page left blank intentionally

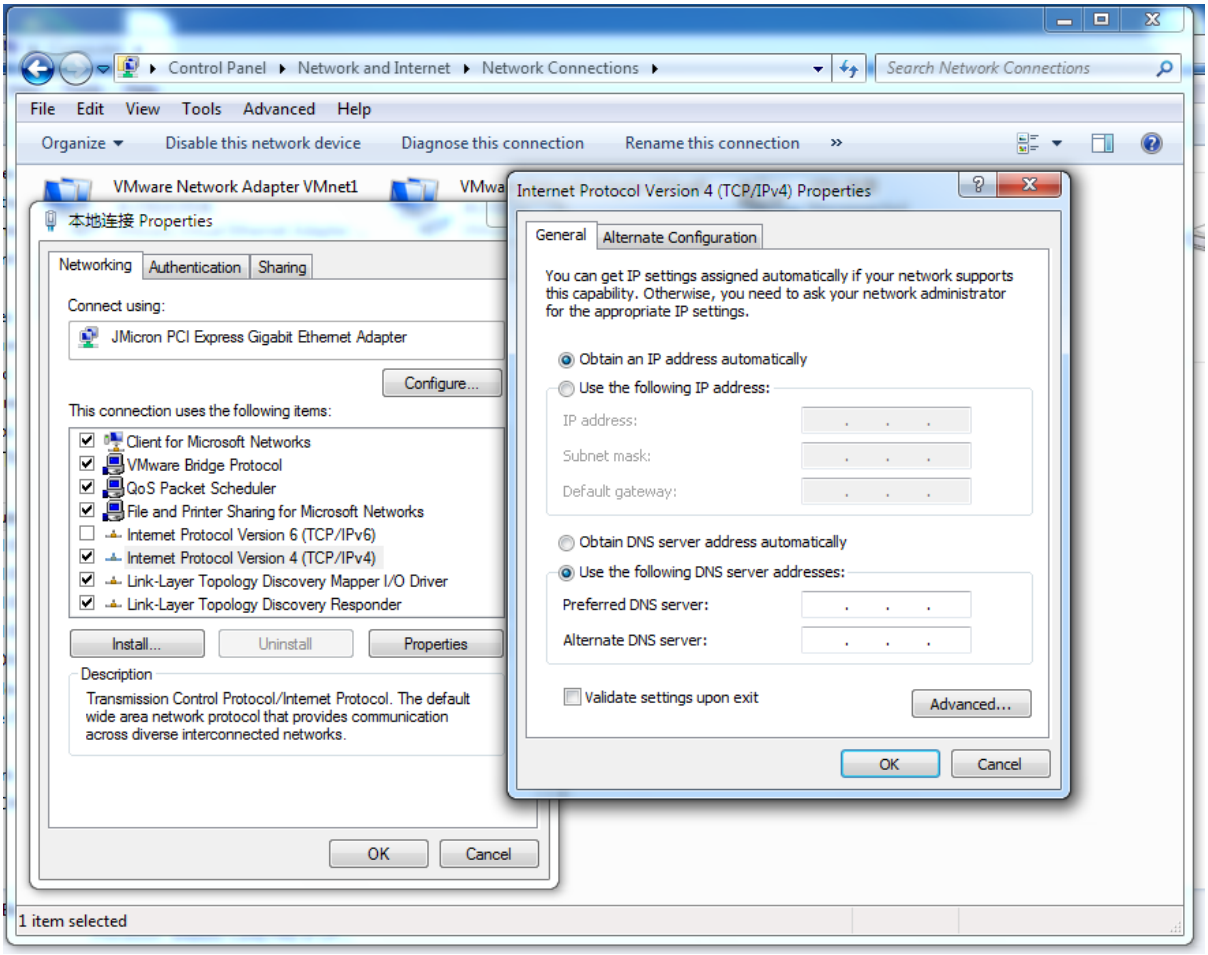
3. ACCESSING THE WEB CONFIGURATION

3.1. PC Configuration

The 6944 router contains a DHCP server which will automatically assign an IP address to your PC, however in some cases the user may need to change the network settings on their PC to accept the IP address from the 6944. or you can configure a static IP address manually.

- **Obtain an IP address automatically**

The process required to do this differs depending on the version of Windows you are using.
NOTE: The following steps are based on Windows 7.



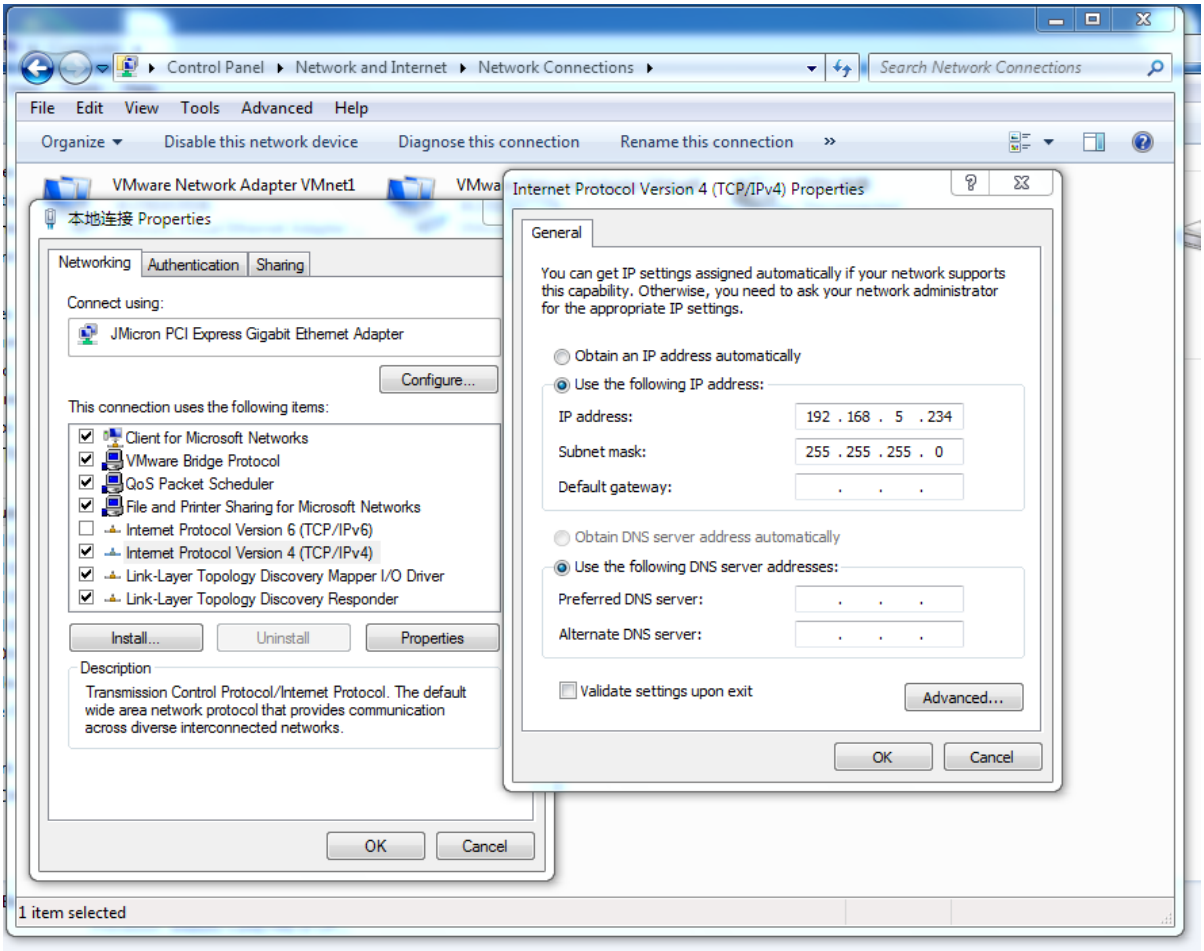
Select **Start » Control Panel » Network Connections**.

Right click **Local Area Connection** and select **Properties** to open the configuration dialog box for Local Area Connection. Select **Internet Protocol (TCP/IP)** and click **Properties** to open the TCP/IP configuration window.

On the General tab, select **Obtain an IP address automatically** and **Obtain DNS server address automatically**.

Click **OK** to complete TCP/IP configuration.

- **Set a static IP address**



click "**Use the IP Address shown in Factory Default Settings below**" to assign a static IP manually within the same subnet of the router but different so for example set 192.168.234.0.

NOTE：*Default gateway* and ***DNS server*** is not necessary if the PC not routing all traffic go through the 6944 router.

3.2. Factory Default Settings

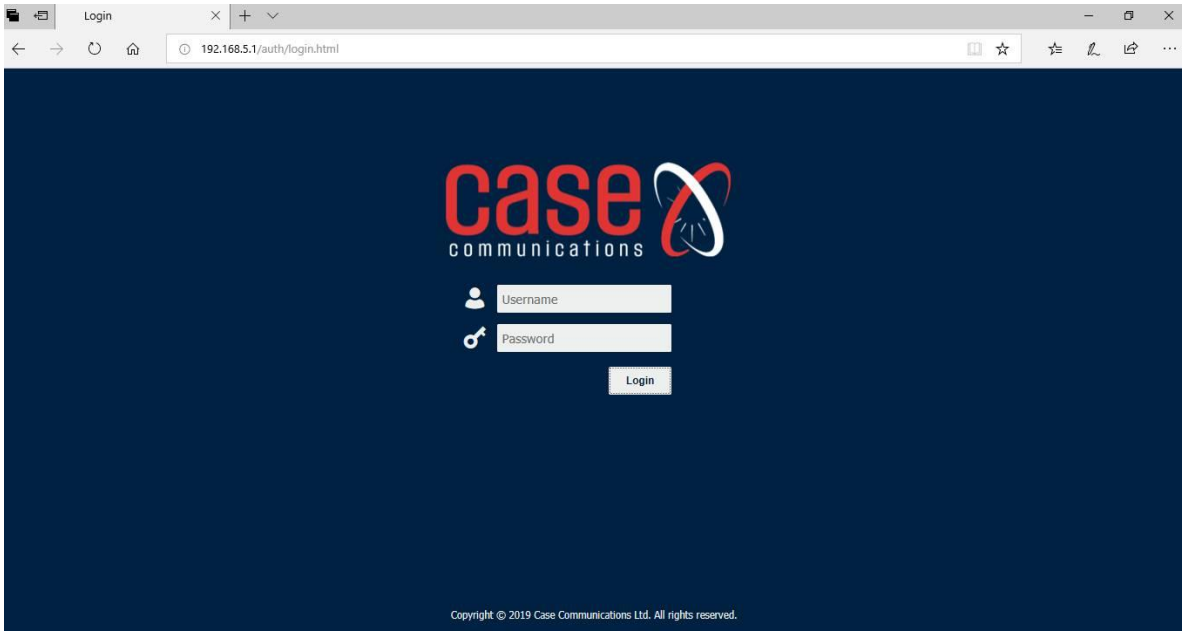
The 6944 router supports Web-based configuration interface for management. If this is the first time you have configured the router, please refer to below default settings.

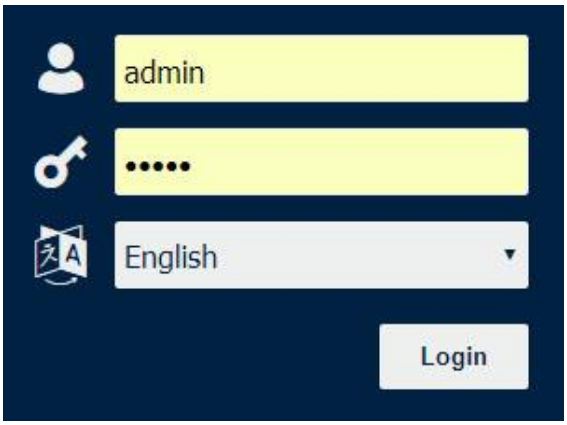
- Username: **admin**
- Password: **admin**
- LAN IP Address: **192.168.5.1** (Eth0~Eth1/Eth3 bridge as LAN mode)
- DHCP Server: **Enabled**

3.3. Logging in to the 6944 Web Page

Step 1: Start a Web browser on your PC (Chrome and IE are recommended), enter 192.168.5.1 into the address bar of the web browser.

Step 2: Then use the default username and password(admin/admin), to log in to the router.


Login
192.168.5.1/auth/login.html
Username
Password
Login
Copyright © 2019 Case Communications Ltd. All rights reserved.

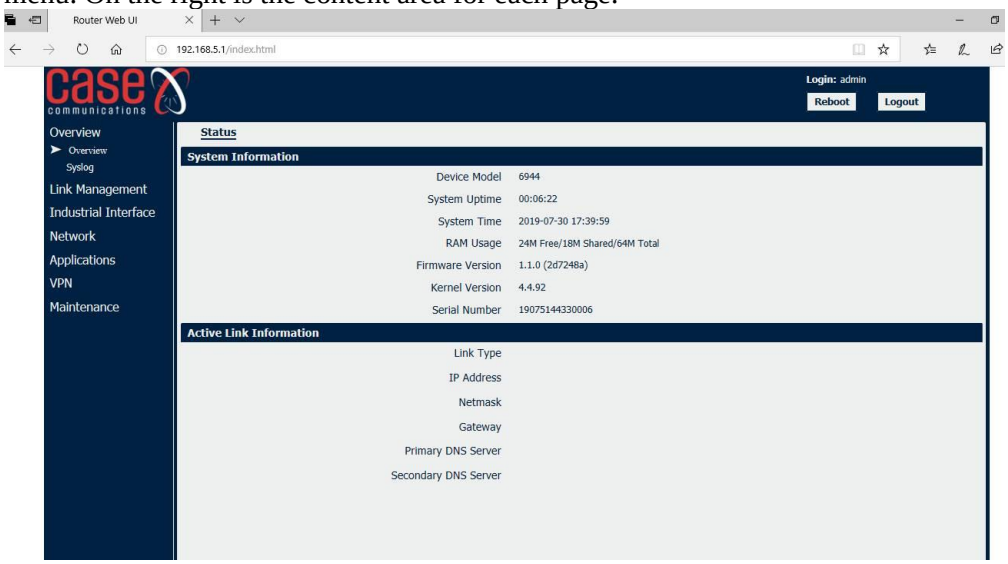

admin
English
Login

This page left blank intentionally

4. BASIC BROWSER CONFIGURATION

4.1 Web Interface Overview

The 6944 router Web interface is divided into two sections. In the left pane is the main navigation menu. On the right is the content area for each page.



NOTE: The navigation menu may contain fewer sections than shown here depending on which options are installed on your 6944.

4.1.1. System Settings

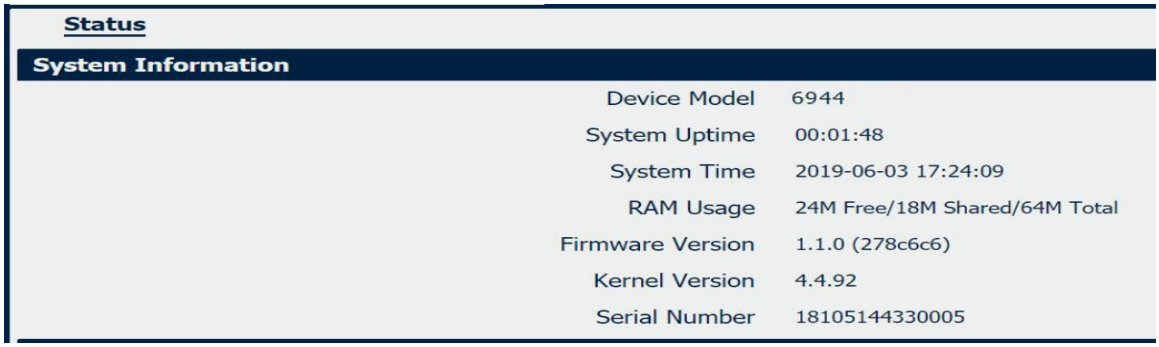
- **Reboot:** reset the router within power disconnect.
- **Logout:** logout to web authorization page.

- **Save:** save the configuration on current page.
- **Apply:** apply the changes on current page immediately.

- **Close:** exit without changing the configuration on current page.

4.1.2. Status

You can view the system information of the router on this page.



System Information

- **Device Module -** Displays the model name of router
- **System Uptime -** Displays the duration the system has been up in hours, minutes and seconds.
- **System Time -** Displays the current date and time.
- **RAM Usage -** Displays the RAM capacity and the available RAM memory.
- **Firmware Version -** Displays the current firmware version of router.
- **Kernel Version -** Displays the current kernel version of router.
- **Serial Number -** Display the serial number of router.

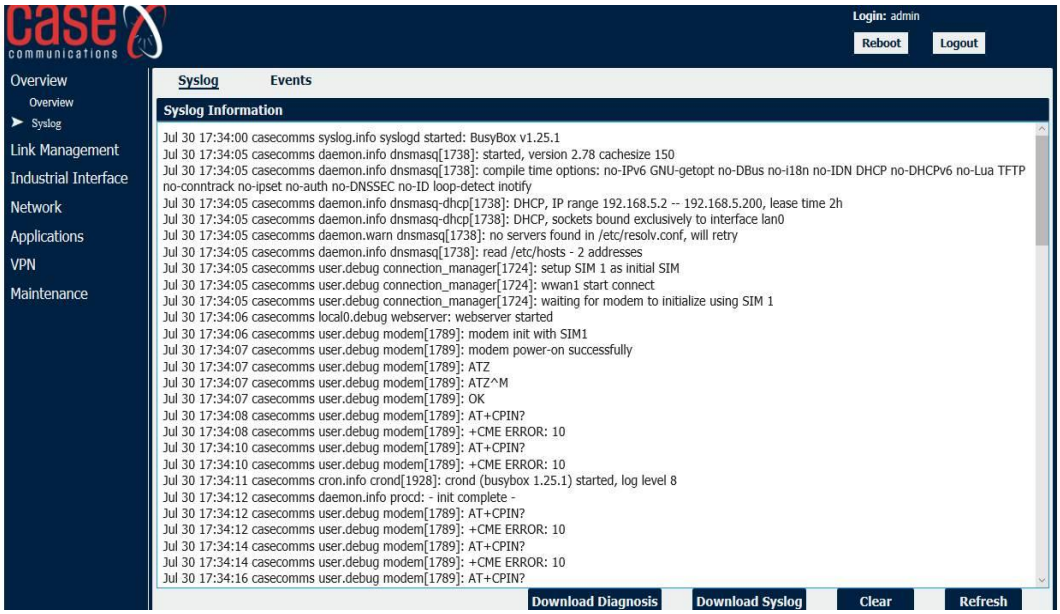
Active Link Information

- **Link Type -** Current interface for internet access.
- **IP Address -** Displays the IP address assigned to this interface.
- **Netmask -** Displays the subnet mask of this interface.
- **Gateway -** Displays the gateway of this interface. This is used for routing packets to remote networks.
- **Primary DNS Server -** Displays the primary DNS server of this interface.
- **Secondary DNS Server -** Displays the secondary DNS server of this interface.

4.1.3. Syslog

Syslog Information

- **Download Diagnosis -** Download the Diagnosis file for analysis.
- **Download Syslog -** Download the complete syslog since last reboot.
- **Clear -** Clear the current page syslog printing
- **Refresh -** Reload the current page with latest syslog printing.



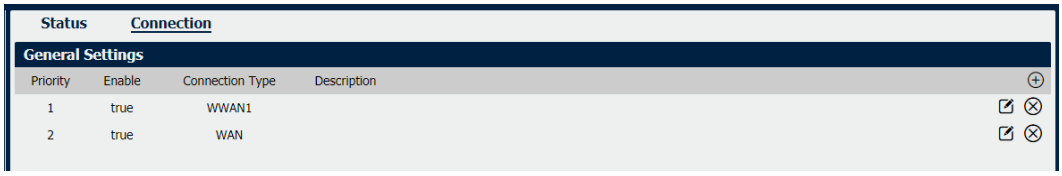
5 Link Management

This section shows you the setup of link management.

Connection Manager->Status

- **Type -** Displays the connection interface
- **Status -** Displays the connection status of this interface.
- **IP Address -** Displays the IP Address of this interface.
- **Netmask -** Displays the subnet mask of this interface.
- **Gateway -** Displays the gateway of this interface. This is used for routing packets to remote networks.

5.1 Connection Manager



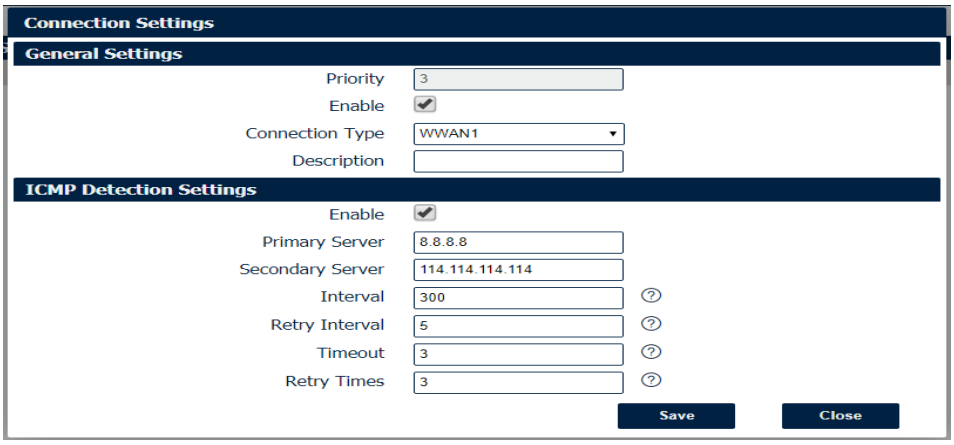
Click  to add a new priority interface.

Click  to edit current interface settings.

Click  to delete current interface

Connection Manager->Connection

- **Priority -** Displays the priority list of default routing selection.
- **Enable -** Displays the connection enable status.
- **Connection Type -** Displays the name of this interface.
- **Description -** Displays the description of this connection.



Connection Settings

- **Priority**

Displays current index on the priority list.

- **Connection Type**

Select the available interface as outbound link.
NOTE: specify SIM1 carrier link as WWAN1, SIM2 carrier link as WWAN2.

- **ICMP Detection Settings->Enable**

Check this box to detect link connection status based on pings to a specified IP address.

- **Primary Server**

Enter the primary IP address to send the pings to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8 (Google)).

- **Secondary Server**

Enter the secondary IP address to send the pings to, if the primary server ping fails, the 6944 will try to ping the secondary server.

- **Interval**

The duration of each ICMP detection in seconds.

- **Retry Interval**

The interval in seconds between each ping if no packets have been received.

- **Timeout**

Enter timeout for received ping reply to determine the ICMP detection failure.

- **Retry Times**

Specify the retry times for ICMP detection.

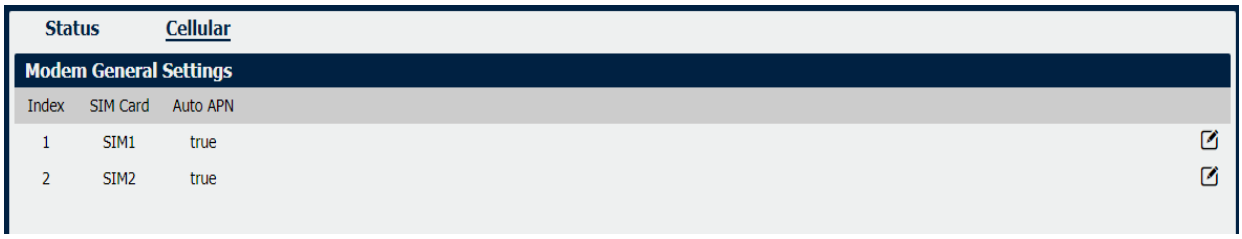
5.2 Cellular

5.2.1. Cellular Configuration

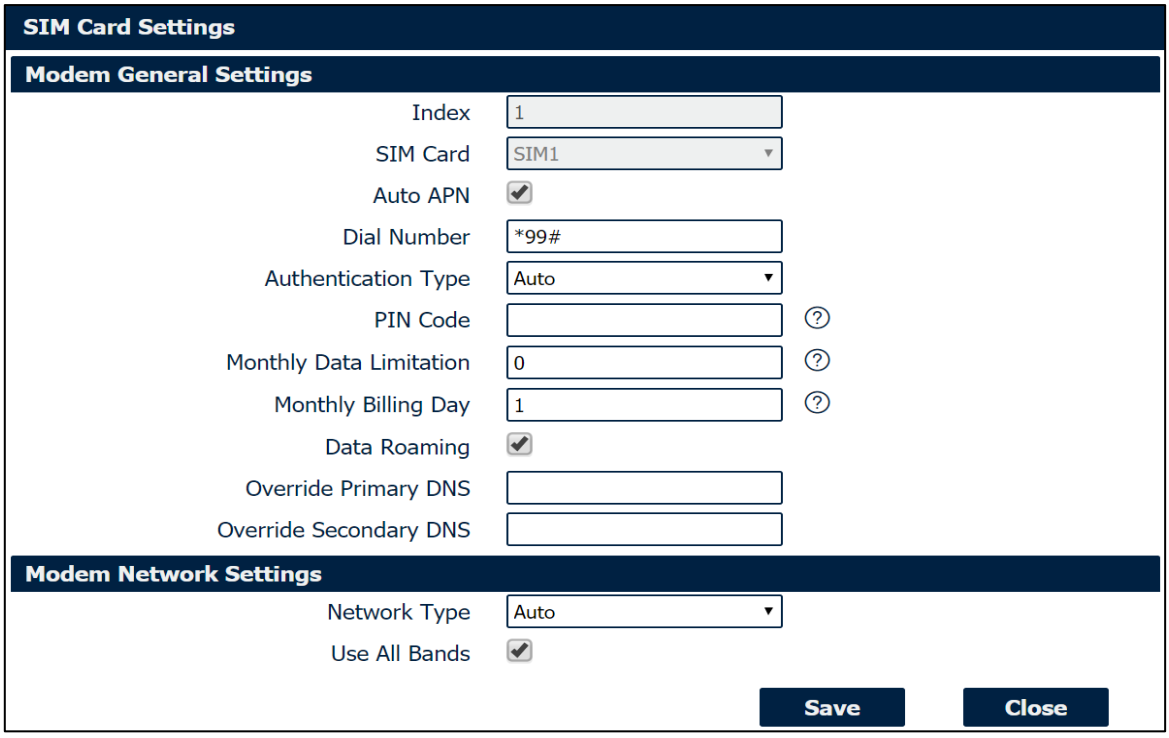
The 6944 Routers main function is connecting to Internet using its cellular modems.

Cellular->Status

- **Modem -** Displays the module of the modem used by this WWAN interface.
- **Registration -** Displays the registration status of SIM card.
- **CSQ -** Displays the signal strength of the carrier network.
- **Operator -** Displays the wireless network provider.
- **Network Type -** Displays the RF technology currently active. Example: LTE, UMTS, or CDMA.
- **IMEI -** International Mobile Electronic Identifier. Depending on the carrier and technology used, this may be required for the carrier when activating the data contract. In some cases this will be blank.
- **PLMN ID -** Displays the current PLMN ID, including MCC, MNC, LAC and Cell ID.
- **Local Area Code -** Displays the location area code of the SIM card.
- **Cell ID -** Displays the Cell ID of the SIM card location.
- **IMSI -** International Mobile Subscriber Identity, as read from the SIM. This is the user's network subscription.
- **TX Bytes -** Displays the total bytes transmitted since the time the unit was connected. The 6944 router would record this data with same SIM card, reboot would not erase this data.
- **RX Bytes -** Displays the total bytes received since the time the unit was connected. The 6944 router would record this data with same SIM card, reboot would not erase this data.
- **Modem Firmware -** Displays firmware version of the module used by the WWAN interface.

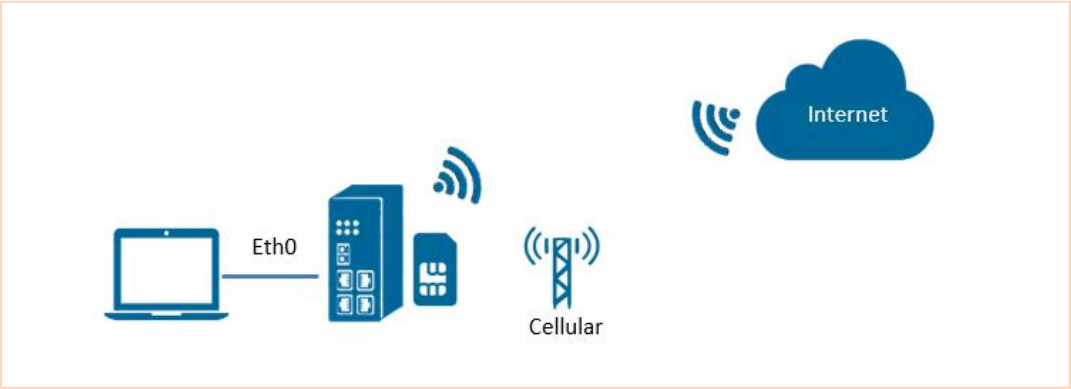


Cellular
• **SIM Card -** Displays the SIM card support on this unit.
• **Auto APN -** Displays the Enable status of auto APN function.
SIM Card Settings
• **SIM Card -** Displays the current SIM card settings
• **Auto APN -** Check this box enable auto checking the Access Point Name provided by the carrier.
• **Dial Number -** Enter the dial number of the carrier.
• **Authentication Type -** Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.
• **PIN Cod -** Enter a 4-8 characters PIN code to unlock the SIM.
• **Monthly Data Limitation -** Enter the data total amount for SIM card, SIM card switchover when data reach limitation.
• **Override Primary DNS -** Enter the primary DNS server will override the automatically obtained DNS.
• **Network Type -** Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.).
• **Use All Bands -** Check this box to enable all bands selection or choose specified bands.



5.2.2. Cellular Configuration Example

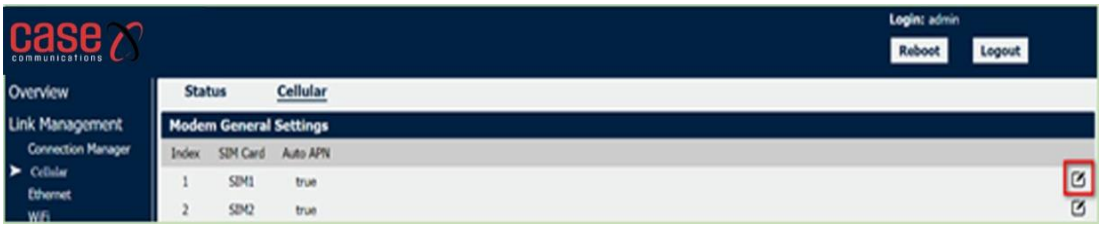
Topology for the cellular connection test



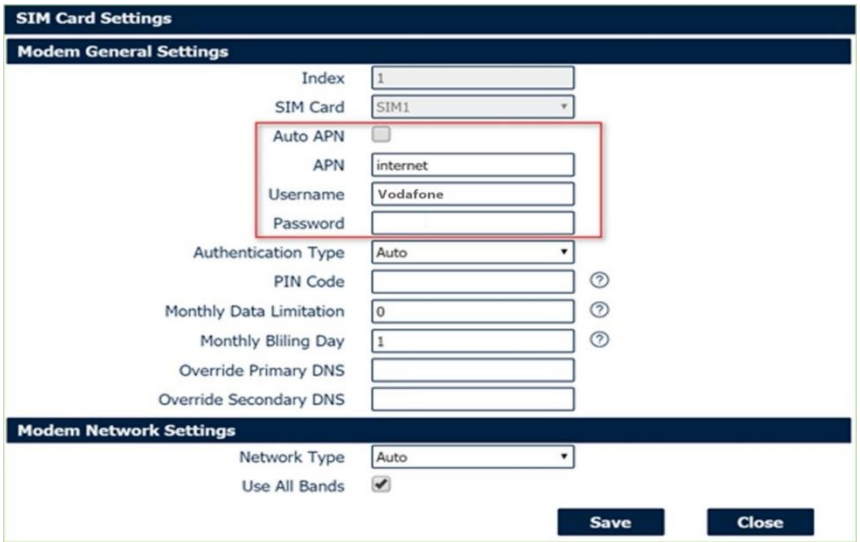
- Specify WWAN1 as primary link and the 6944 access cellular network via SIM card(wwan1).
- ETH0 works as a LAN interface and enable DHCP server, allocate IP to the end PC

<u>6944 Cellular Configuration</u>

Step 1: Go to **Link Management>Cellular>Cellular**, Click the **Edit button** of SIM1

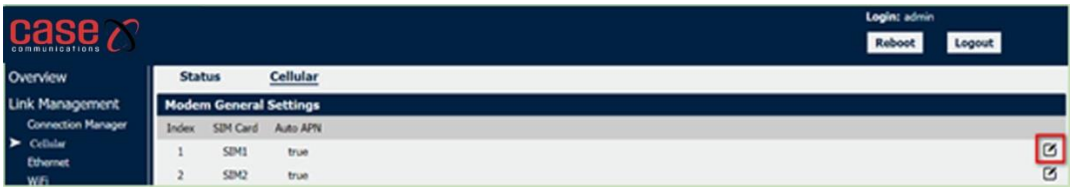


Step 2: Setup the APN, Username and Password of the SIM card, please also setup the PIN if the SIM work with the PIN code. And left the other parameters as default.

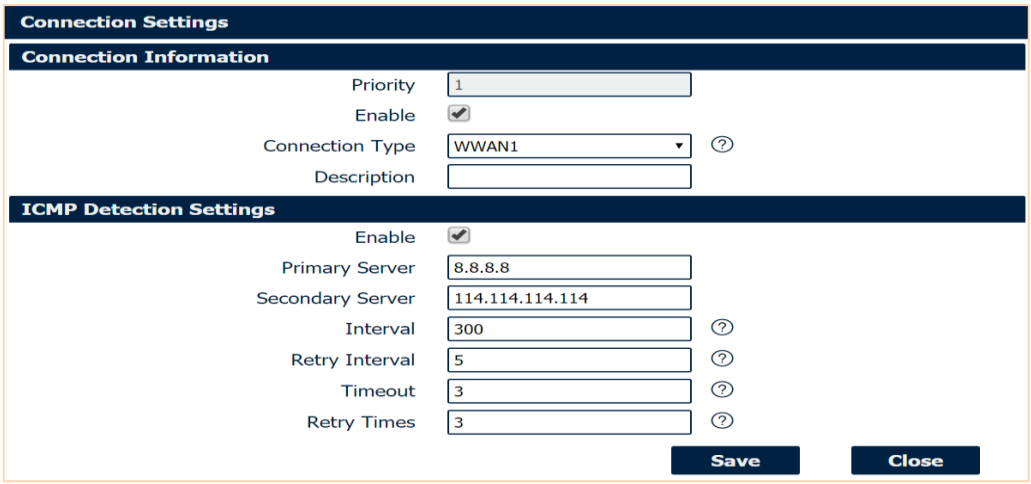


Step 3: Click Save>Apply.

Step 4: Go to Link **Management>Connection Manager>Connection**, Click the **Edit button** of WWAN1.



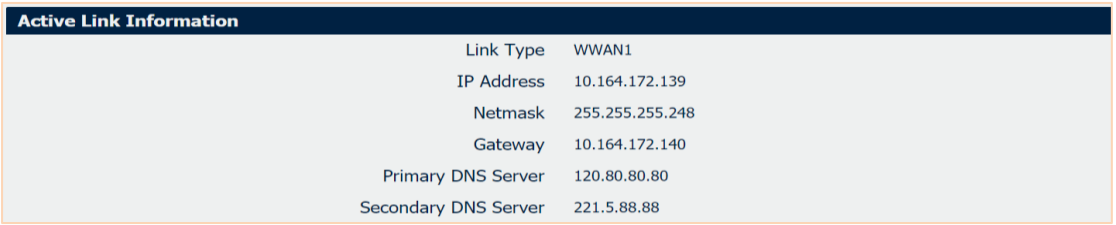
Step 5: Setup the parameters of WWAN1 as below:



Step 6: Click Save>Apply.

6944 Testing the Cellular Connection

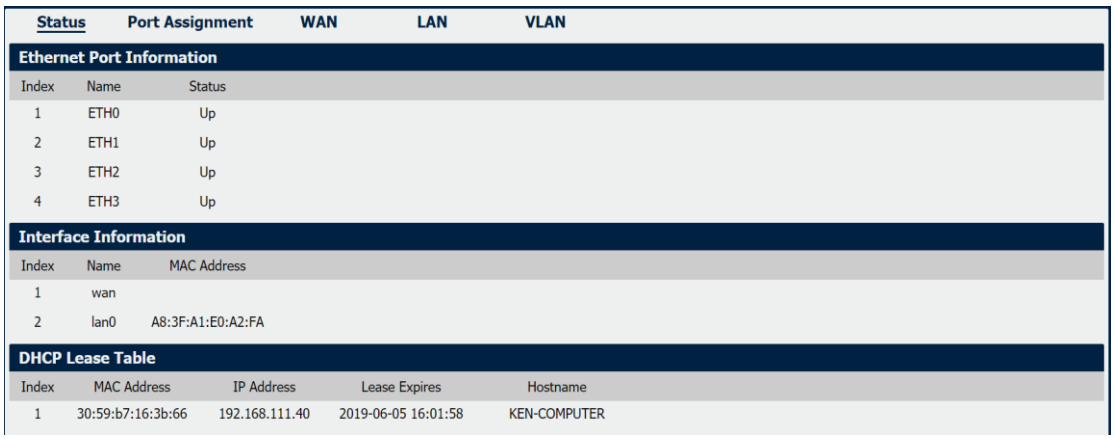
Step 1: Go to **Overview>Overview>Active Link Information**, the router had been got the IP information for ISP.



Step 2: Go to Link Management>Cellular>Status, to check the registration information.

5.3. Configuring Ethernet Ports

5.3.1. Ethernet port status

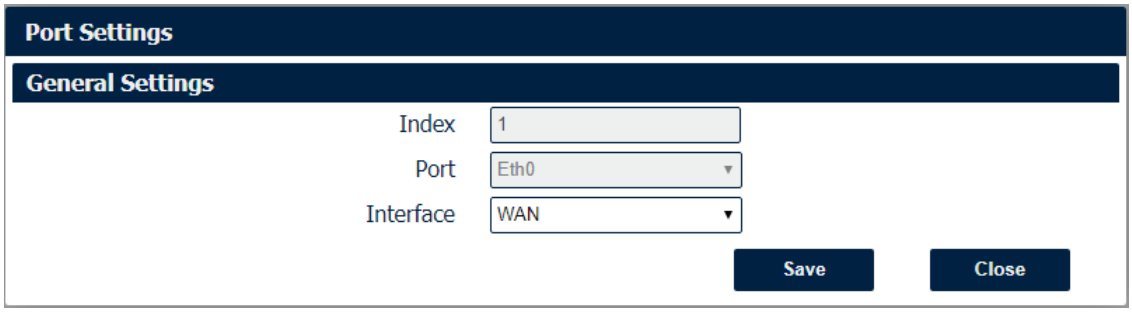


Ethernet->Status

- **Ethernet Port Information -** Displays the port physical connected states.
- **Interface Information -** Displays the name and MAC address of Ethernet interface.
- **DHCP Lease Table**

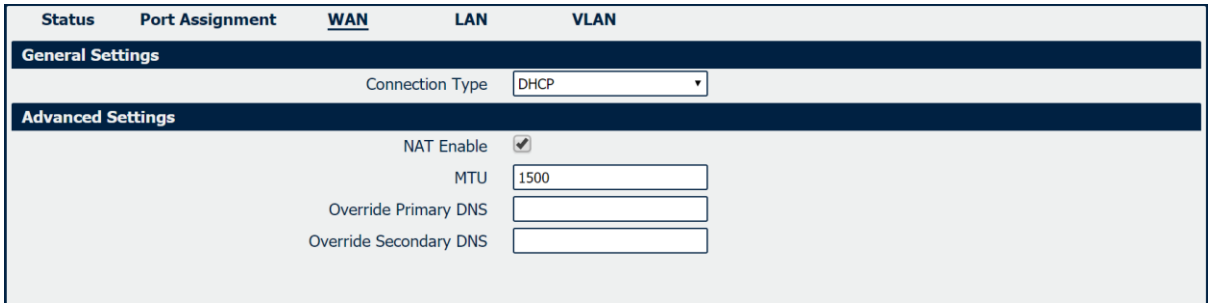
Ethernet->Port Assignment

- **Port -** Displays the port states and numbers of this unit
- **Interface -** Displays the port states of belong subnet



Ethernet->Port Settings

- **Port -** Indicates the current configuration of the port.
- **Interface -** Select this option to configure the port



5.3.2. Configuring an Ethernet LAN port

Ethernet->LAN

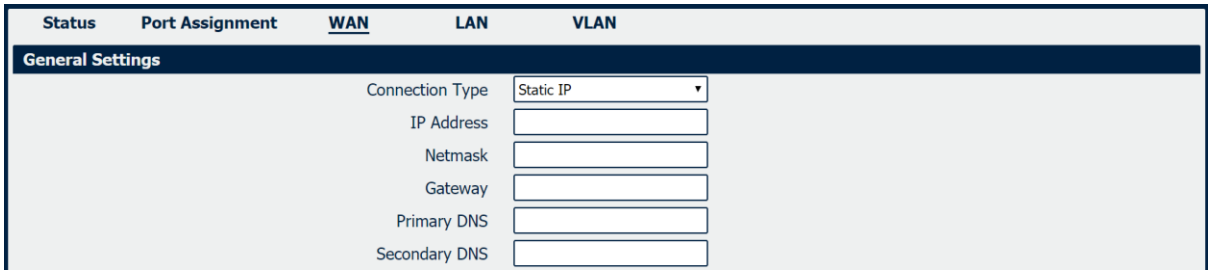
- **Interface -** Select the configurate LAN port of this subnet.
- **IP Address -** Enter LAN IP address for this interface.
- **Netmask -** Enter subnet mask for this subnet.
- **MTU**
  Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.
- **Enable -** Check this box to enable DHCP feature on current LAN port.
- **Mode -** Select the DHCP working mode from "Server" or "Relay".
- **Relay Server -** Enter the IP address of DHCP relay server.
- **IP Pool Start**
  External LAN devices connected to this unit will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.
- **IP Pool End -** This is the end of the pool of IP addresses.
- **Netmask**
  Subnet mask of the IP address obtained by DHCP clients from DHCP server.
- **Lease Time**
  The lease time of the IP address obtained by DHCP clients from DHCP server.
- **Gateway**
  The gateway address obtained by DHCP clients from DHCP server.
- **Primary DNS**
  Primary DNS server address obtained by DHCP clients from DHCP server.
- **Secondary DNS**
  Secondary DNS server address obtained by DHCP clients from DHCP server.
- **WINS Server**
  Windows Internet Naming Service obtained by DHCP clients from DHCP server.

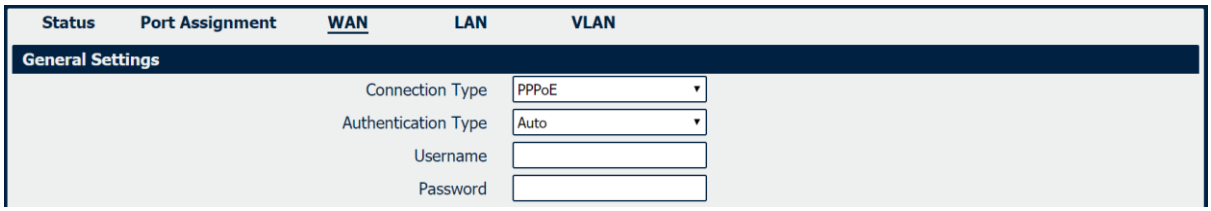
5.3.3. Configuring and Ethernet WAN Port

The 6944 also supports WAN connections for example set to Static IP and PPPoE mode.

Ethernet->WAN

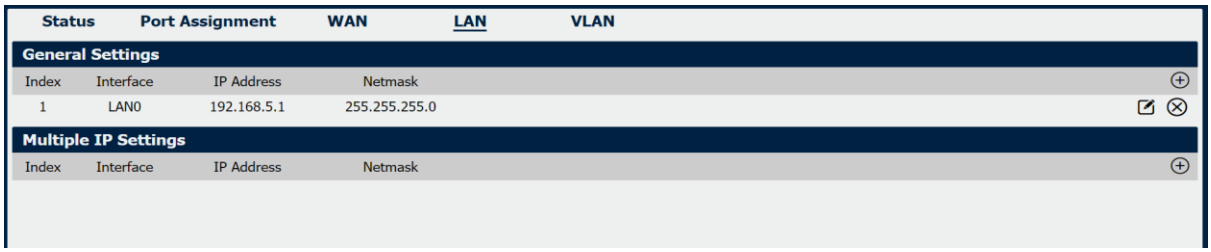
- **Connection Type -** If you select DHCP Client, external DHCP server will assign an IP address to this unit.
- **NAT Enable -** Enable or Disable NAT (Network Address Translation).
- **MTU -** Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.
- **Override Primary DNS -** Enter the primary DNS server will override the automatically obtained DNS.
- **Override Secondary DNS -** Enter the secondary DNS server will override the automatically obtained DNS.





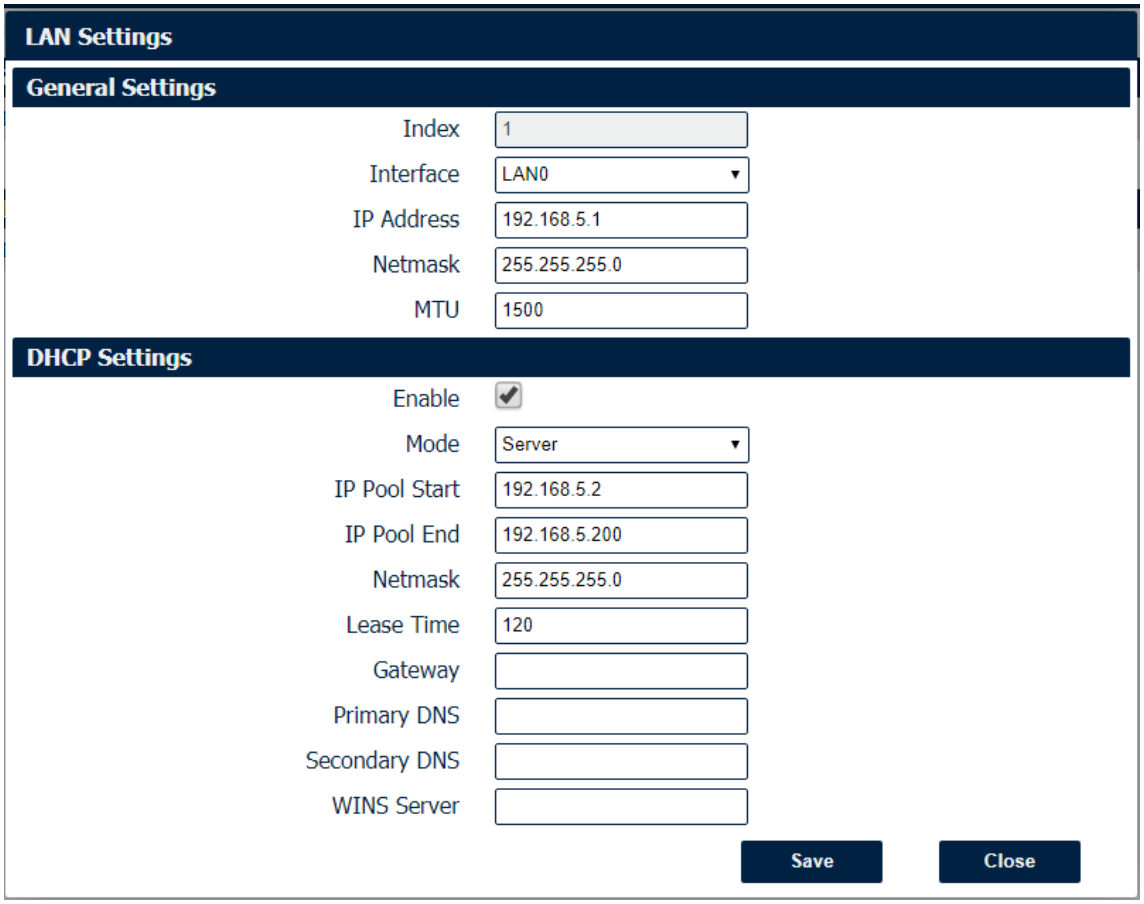
Ethernet->WAN->Static IP or PPPoE

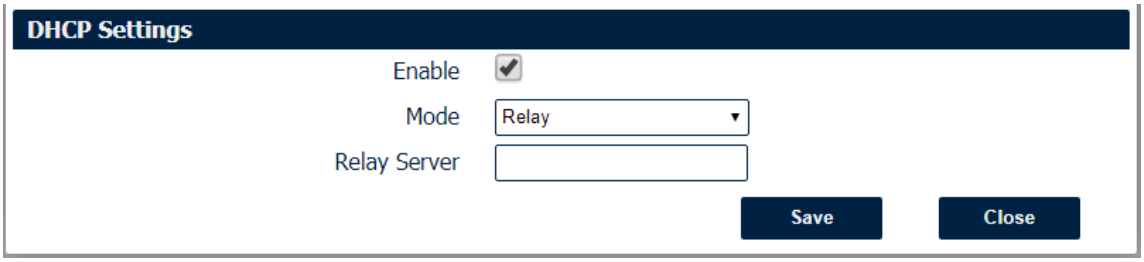
- **IP Address -** Static address for this interface. It must be on the same subnet as the gateway.
- **Netmask -** Will be assigned by the gateway.
- **Gateway -** IP address of the Gateway (DHCP Host). If not known this can be left as all zeros.
- **Primary DNS -** IP address of the primary DNS server.
- **Secondary DNS -** IP address of the secondary DNS server.
- **Authentication Type -** Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.
- **Username -** Username to provide when connecting.
- **Password -** Password to provide when connecting.



Ethernet->LAN

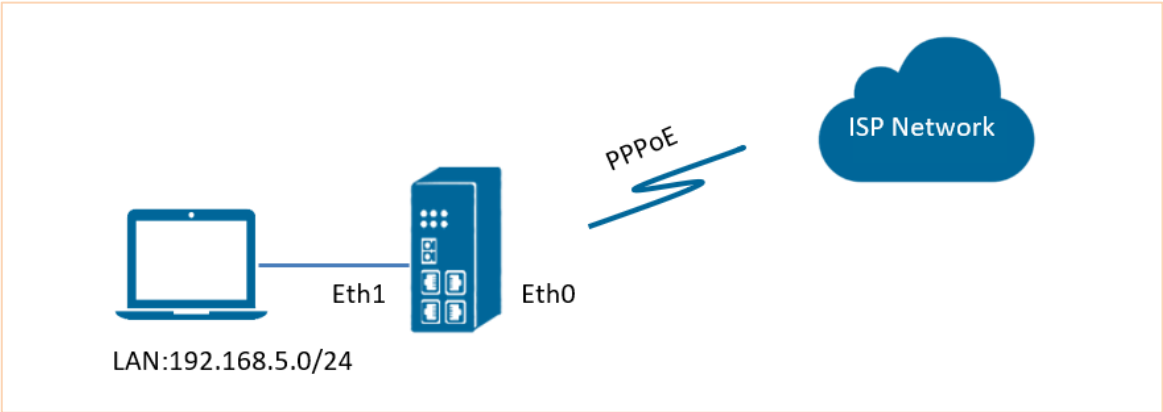
- **Interface -** Displays current name of LAN subnet.
- **IP Address -** Displays LAN IP address of this subnet.
- **Netmask -** Displays subnet mask for this subnet.





5.3.4. AN021 – Configuring PPPoE

Configuration Topology

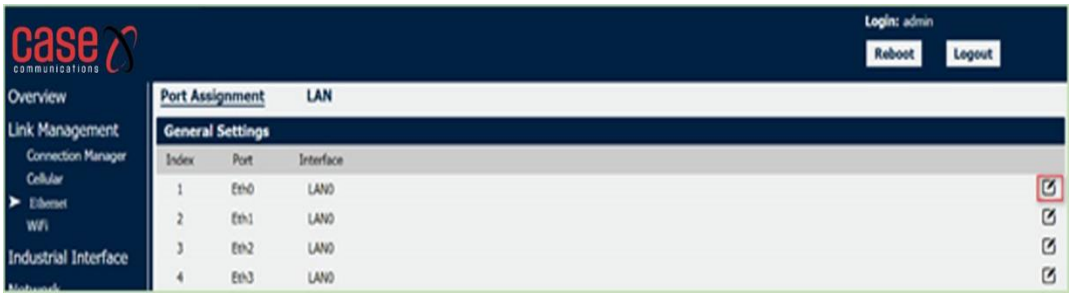


- Set Eth0 on the 6944 as a WAN Port and connect to the internet using PPPoE
- ETH1 works as a LAN Interface, enable the 6944 DHCP Server, and connect your PC allowing the 6944 to give it an IP Address.

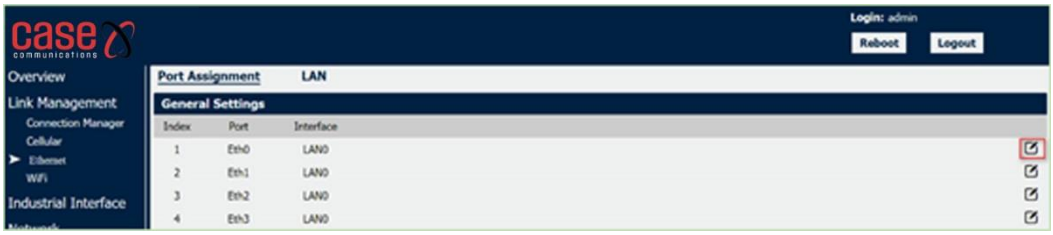
Configuration Steps

Ethernet Configuration

Step 1. Go to Link Management>Ethernet>Port Assignment, Click the Eth 0 Edit button.

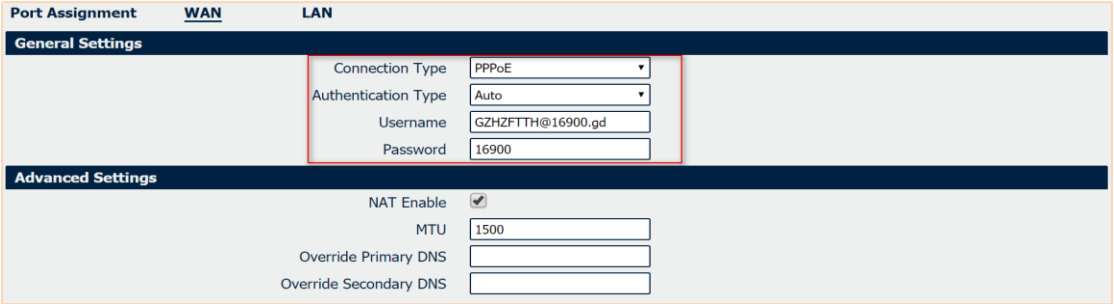


Step 2: Assigned the port ETH0 as WAN, as shown below:



Step 3: Click Save>Apply.

Step 4: Go to **Industrial Interface>Ethernet>Status>WAN**, specify the Connection Type as "PPPoE", enter "username" and "password" provided by ISP. Setting like below:



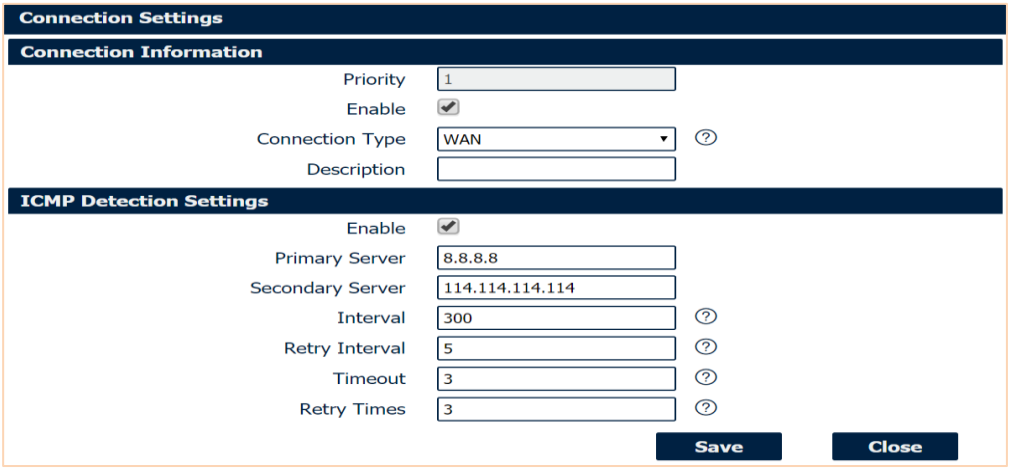
Note: *"Connection Type" also support "DHCP" and "Static IP", please configure accordingly. Here take "PPPoE" as an example.*

Step 5: Click Save>Apply.

Primary Link configuration

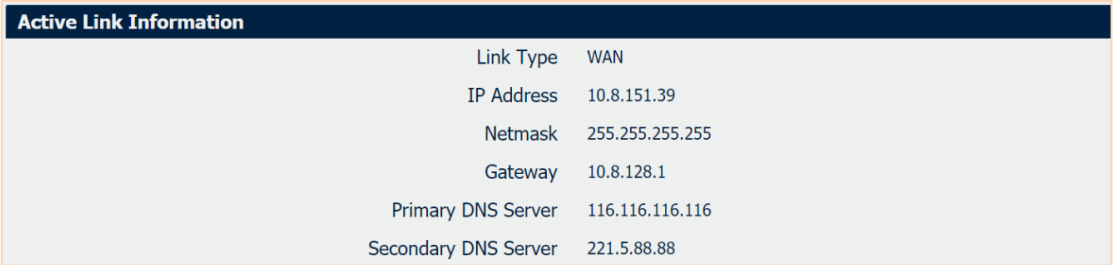
Step 1. Go to **Link Management>Connection Manager>Connection**, delete the WWAN1 and WWAN2 then click "Save>Apply". After that please add the "WAN" link follow below picture:

Step 2: Configure the WAN parameters as shown below:

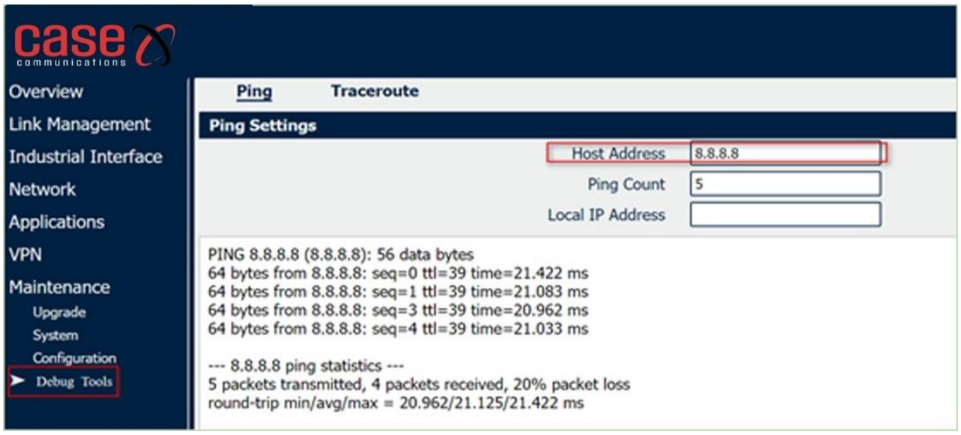


Testing

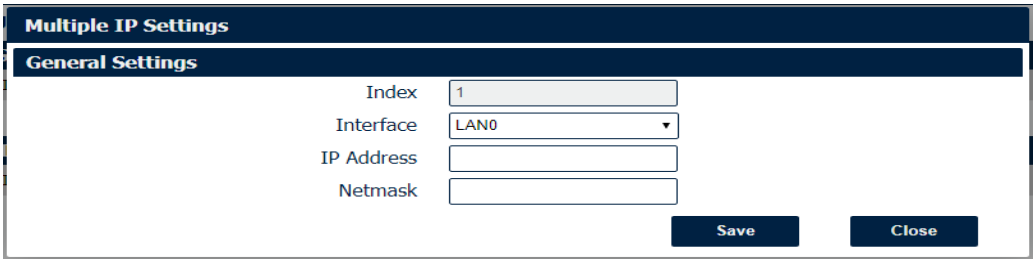
Step 1. Go to **Overview>Overview>Active Link Information**, to display the WAN (PPPoE) status as shown below:



Step 2. Make sure the Router can ping Google "8.8.8.8" successfully.



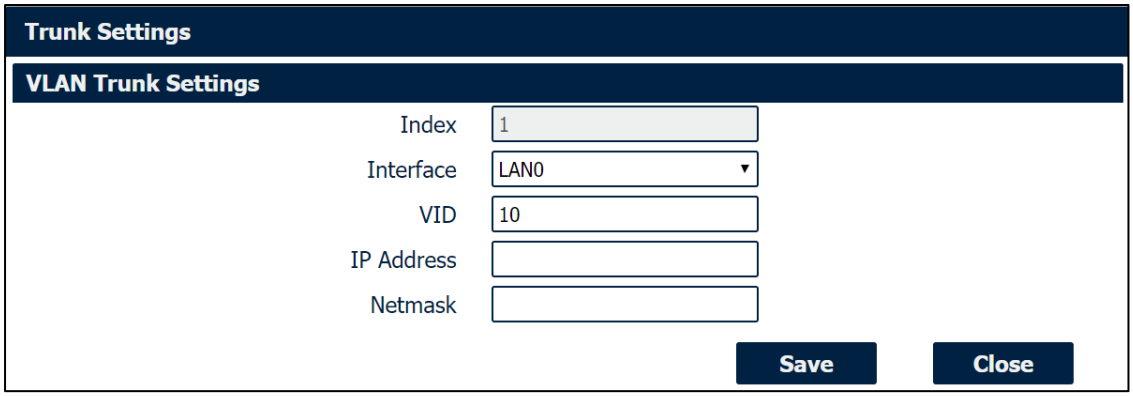
Step 3. Test successful.



Ethernet->LAN->Multiple IP Settings

- **Interface -** Select the configurate LAN port of this subnet.
- **IP Address -** Enter multiple IP address for this interface.

5.4 VLAN Trunk Settings

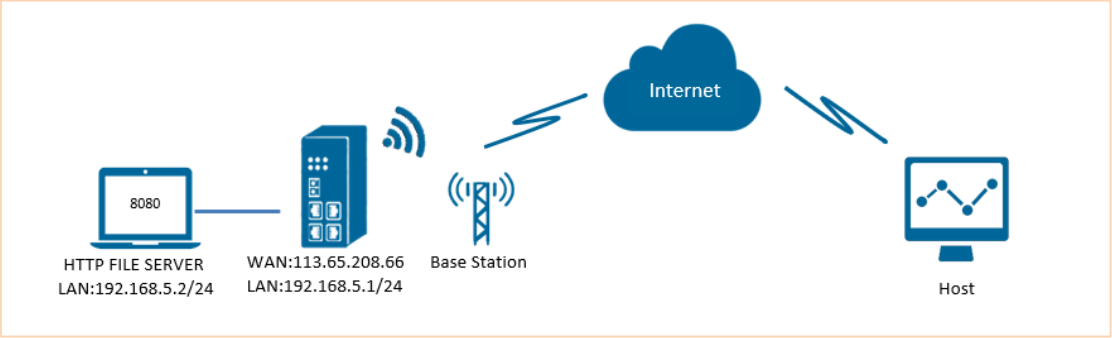


Ethernet->VLAN->VLAN Trunk Settings

- **Interface -** Select the LAN port for VLAN trunk.
- **VID -** Specify the VLAN ID for VLAN trunk.
- **IP Address -** Enter IP address for this VLAN trunk.
- **Netmask -** Enter subnet mask for this VLAN trunk.

5.5 Port Forwarding

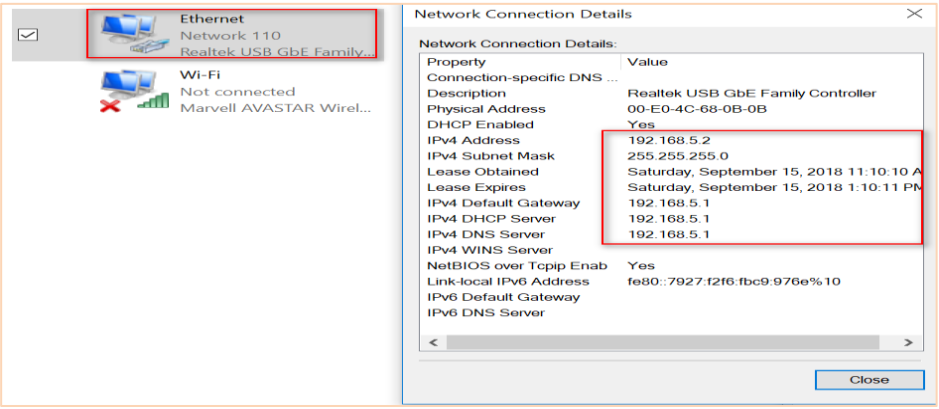
Testing Topology



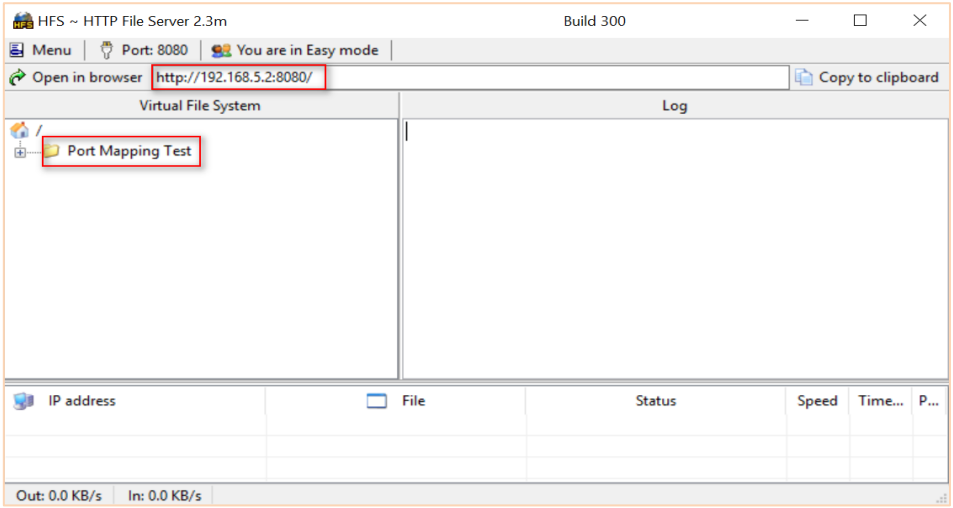
- The Case Communications 6944 works with a fixed public IP address.
- A remote host works with a PC, which can communicate with the Internet and reach the 6944
- The remote host access HTTP FILE SERVER behind 6944 via Port Mapping.

HTTP File Server Configuration

Step 1. Set up an IP address on a PC connected to the 6944 and make sure it can ping the 6944 successfully.

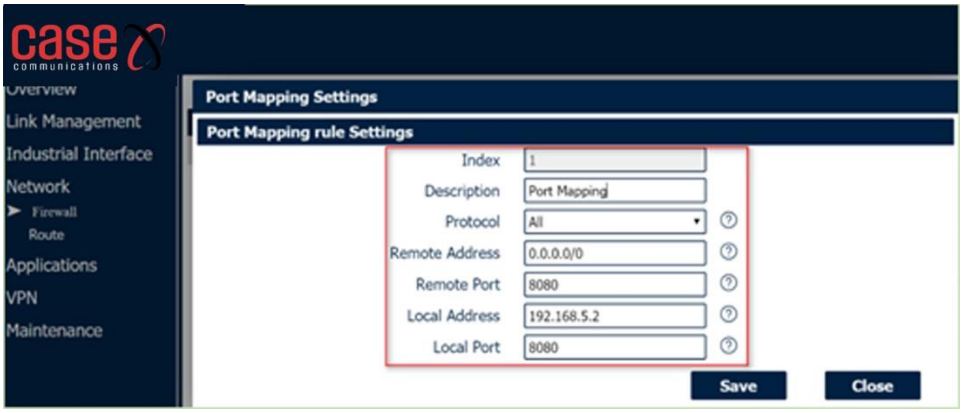


Step 2. Enable HTTP FILE SERVER on the PC.



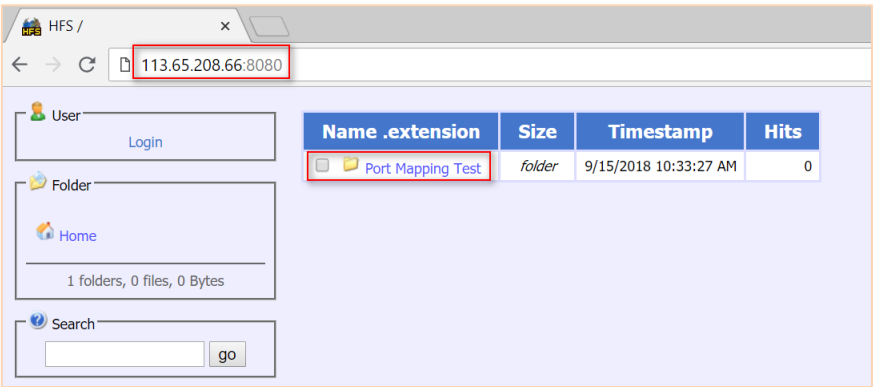
Port Mapping Configuration

Step1: Go to **Network>Firewall>Port Mapping,** and configure as shown below



Testing

Step1: Access the HTTP FILE SERVER from remote host with: **http:// 113.65.208.66:8080**



Step 2: Test successful

Note: Please turn off the Firewall on the PC behind 6944

5.6 RADIUS Authentication (IEEE 802.1x)

RADIUS - IEEE 802.1x

The 6944 can be configured to allow external authentication of management access using an external RADIUS server. This document will only cover configuration of the 6944, please see the documentation of the RADIUS server for configuration details of the server.

RADIUS (Remote Authentication Dial-In User Service)is a networking protocol that provides centralized authentication, authorization, and accounting (AAA) management for users who connect and use a network service. RADIUS is now a part of the IEEE 802 and IETF standards.

RADIUS is a client/server protocol that runs in the application layer and can use either TCP or UDP. The 6944 uses UDP for authentication requests to a RADIUS server.

RADIUS uses two types of packets to manage the full AAA process: Access-Request, which manages authentication and authorization; and Accounting-Request, which manages accounting. Authentication and authorization are defined in RFC 2865 while accounting is described by RFC 2866.

5.6.1 How RADIUS Works on the 6944

The 6944 acts as a facilitator for RADIUS authentication. Equipment connected to the Ethernet ports of the 6944 must be authenticated by the external RADIUS server before access to the 6944 network and WAN.

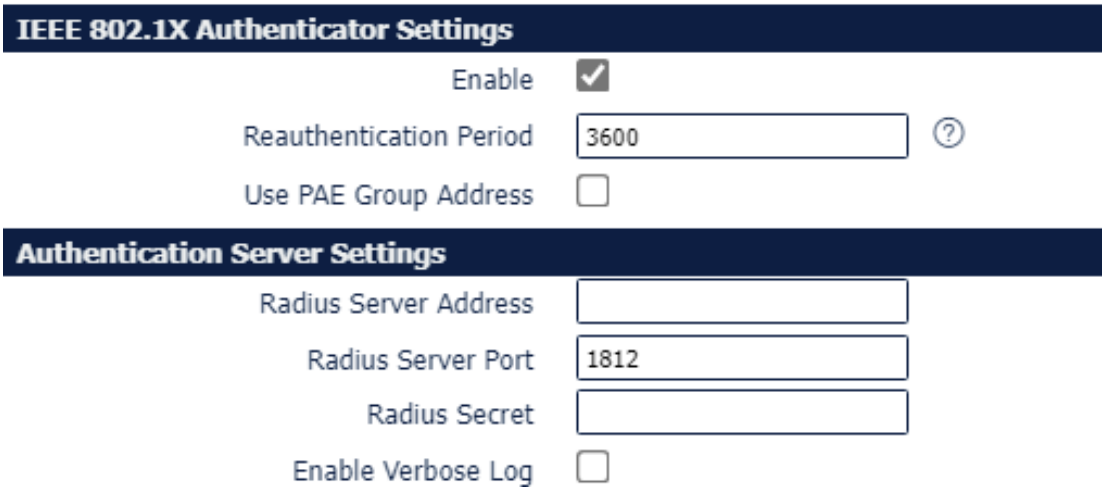
The equipment that is to be connected to the 6944 must be capable of being configured to request 802.1X/RADIUS authentication, without this the equipment will never be allowed access to the 6944's network or WAN.

The 6944 is configured with the RADIUS Server details. When equipment is connected to the 6944, they begin their authentication sequence. The 6944 receives this and sends the RADIUS credentials from the equipment to the RADIUS server. The RADIUS server will either authenticate the equipment or reject it. The 6944 receives the reply from the RADIUS server, if the credentials are authenticated then the equipment is allowed access to the 6944's LAN and WAN. If the credentials are rejected, then the 6944 will block access to it's LAN and WAN by the equipment.

Note: On the 6944 Eth0 is currently excluded from RADIUS authentication as it is often used as an ethernet WAN to an external device like DSL router. This means that if Eth0 is not configured as a WAN port then any equipment connected will gain access to the 6944's LAN and Wireless WAN without authentication.

5.6.2 RADIUS Configuration

Go to **Link Management>Ethernet>LAN**, to view the LAN General Settings. Select the required LAN interface and click the  icon to edit the interface. Under IEEE 802.1X Authenticator Settings select Enable with a tick to expand all RADIUS settings.



IEEE 802.1X Authenticator Settings

- **Enable**
  Enables or disables the RADIUS server settings
- **Reauthentication Period**
  Number of seconds to pass before equipment has to reauthenticate with the RADIUS server. Value 0 – 86400 and 0 disables reauthentication.
- **Use PAE Group Address**
  Port Access Entity (PAE) group address. This MAC address is set within 802.1X as 0180.c200.0003. When enabled the 6944 will use this MAC address as its own in communications with the RADIUS server.

Authentication Server Settings

- **RADIUS Server Address**
  IP address of the RADIUS server
- **RADIUS Server Port**
  UDP port that the RADIUS Server uses for authentication, default value is 1812
- **RADIUS Secret**
  Private/Client Shared Key. This is the alphanumeric string shared with the RADIUS Server and 6944.
- **Enable Verbose Log**
  When enabled the RADIUS application on the 6944 will provide more detailed logs in the 6944's Syslog, including authentication logs. When disabled only a general status of the RADIUS application will be shown.

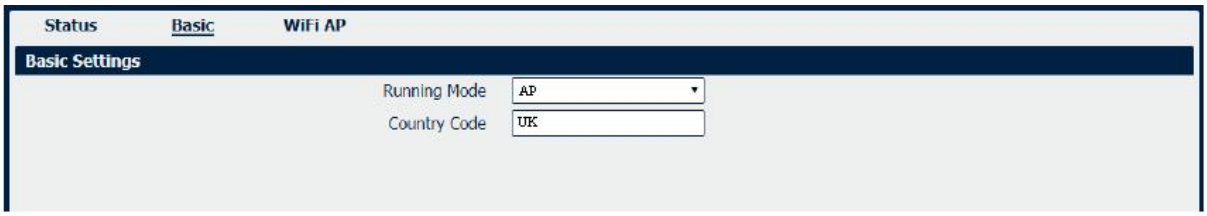
This page left blank intentionally

6 Wi-Fi

6.1 Wi-Fi Access Point

The 6944 Router can only be set to function as either a Wi-Fi Client or a Wi-Fi Access Point, but not both simultaneously. Select Wi-Fi (Access Point) from the main, menu and Wi-Fi (the default setting is the Access Point page) which contains the configuration for the Wi-Fi Access Point interface.

You can review the 6944 Wi-Fi connection status as shown below.

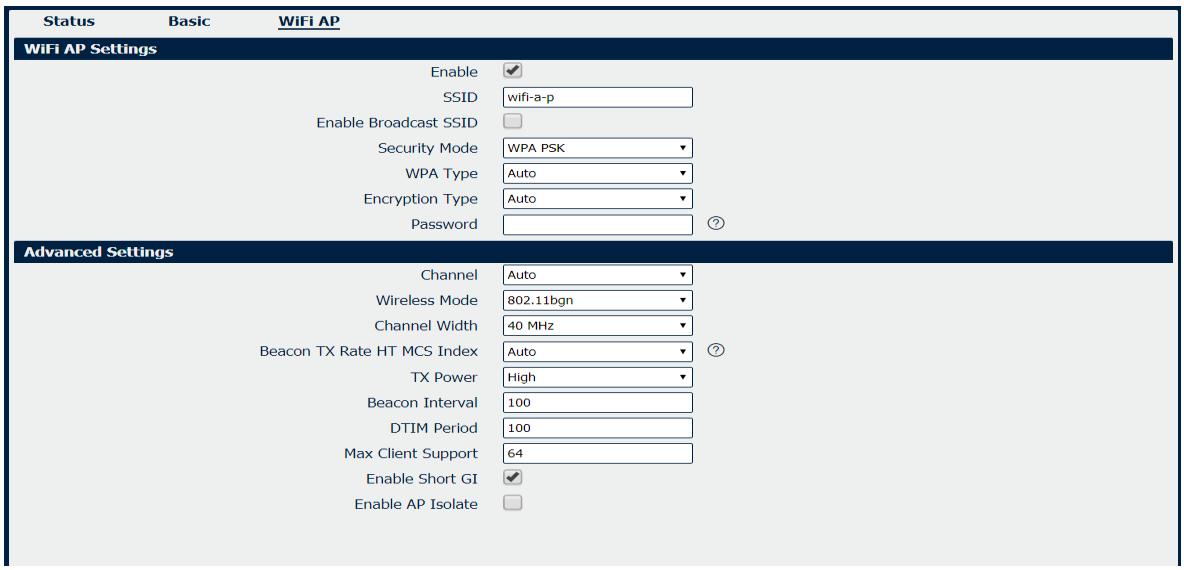


Wi-Fi->Basic

- **Running Mode -** Select the Wi-Fi configuration mode either AP or Client.
- **Country Code -** Enter the country where the AP is located.

5.7 Configuring the Wi-Fi Access Point

Follow the Wi-Fi Access Point settings using the menu page shown below

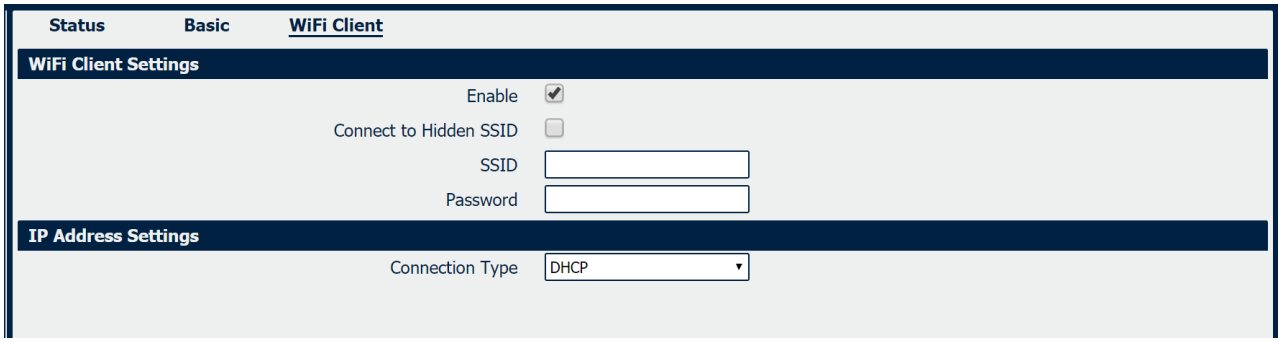


Wi-Fi->Wi-Fi AP

- **Enable -** Select this box to enable the Wireless interface.
- **SSID**
  The SSID is the name of the wireless local network. Devices connecting to the 6944 router WiFi access will identify the Access Point by this SSID.
- **Enable Broadcast SSID**
  When the checkbox is not checked, SSID broadcast is disabled, other wireless devices cannot find the SSID, and users have to enter the SSID manually to access to the wireless network.
- **Security Mode -** Select security mode from “None”, “WEP” or “WPA PSK”.
- **WPA Type -** Select WPA Type from “Auto”,“WPA” and “WPA2”.
- **Encryption Type**
  Select the encryption method. Options are “Auto”, “TKIP”, or “CCMP”. Because these options depend on the authentication method selected, some options will not be available.
- **Password -** Enter the pre-shared key of WEP/WPA encryption.
- **Channel**
  Select the Wi-Fi channel the module will transmit on. If there are other Wi-Fi devices in the area the 6944 router should be set to a different channel than the other access points. Channels available for selection depend on the selected Band.
- **Wireless Mode**
  Select the Wi-Fi 802.11 mode: B, G, or N. Available selections depend on the selected Band.
- **Channel Width**
  Select the width of the Wi-Fi channel. 20 MHz will limit the channel to 20 MHz wide; 20/40 MHz will enable the use of a 40 MHz wide channel when available.
- **Beacon TX Rate HT MCS Index**
  Modulation and Coding Scheme, The MCS modulation coding table is a representation proposed by 802.11n to characterize the communication rate of the WLAN. The MCS takes the factors affecting the communication rate as the columns of the table and uses the MCS index as a row to form a rate table.
- **TX power**
  Select the transmission power for the AP from “High”, “Medium” and “Low”.
- **Beacon Interval**
  Enter the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.
- **DTIM Period**
  Enter the delivery traffic indication message period and the router AP will multicast the data according to this period.
- **Max Client Support**
  Enter the maximum number of clients to access when the router is configured as AP.
- **Enable Short GI**
  Check this box to enable Short GI (guard interval), Short GI is a blank time between two symbols, providing a long buffer time for signal delay.
- **Enable AP Isolate**
  Check this box to enable AP isolate, the route will isolate all connected wireless devices.

5.8 Configuring the Wi-Fi Access Point

The 6944 Wi-Fi Client settings are configured using the menu options

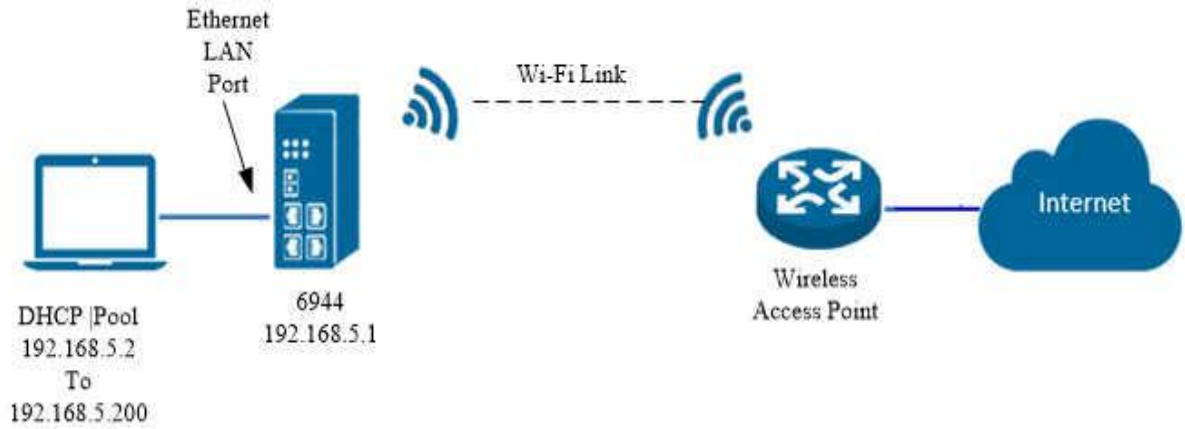


Wi-Fi->Wi-Fi Client

- **Enable -** Checking this box will enable the Wireless interface.
- **Connect to Hidden SSID -** Check this box will enable a connection toa hidden SSID.
- **SSID -** The SSID of the external access point.
- **Password -** Enter the password of the external access point.
- **Connection Type -** Select from DHCP Client or Static IP address.
- **IP Address -** Static address for this interface. It must be on the same subnet as the gateway.
- **Netmask -** Will be assigned by the gateway.
- **Gateway -** IP address of the Gateway.
- **Primary DNS -** Enter the primary DNS server to override the automatically obtained DNS.
- **Secondary DNS -** Enter the secondary DNS server to override the DNS being assigned automatically.

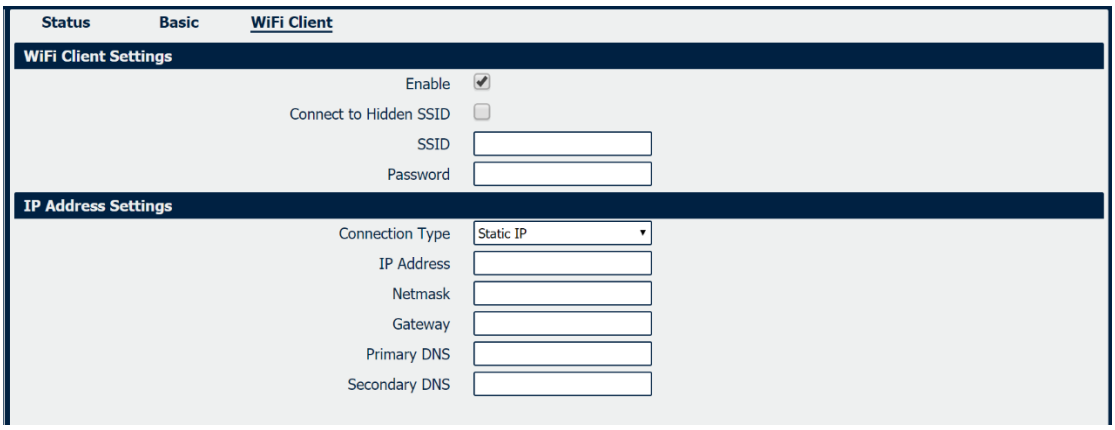
5.9 Wireless Access Configuration Example

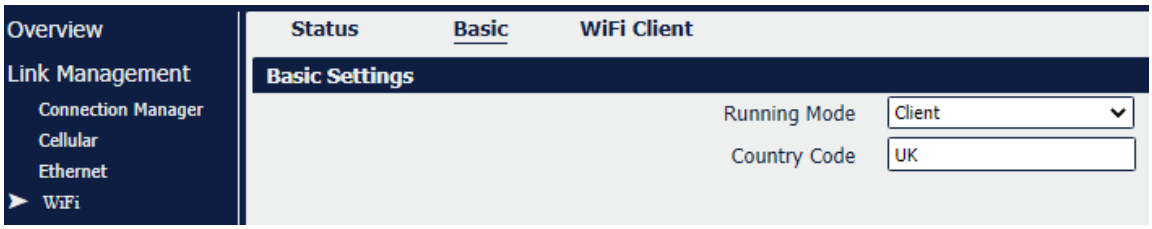
Testing Topology



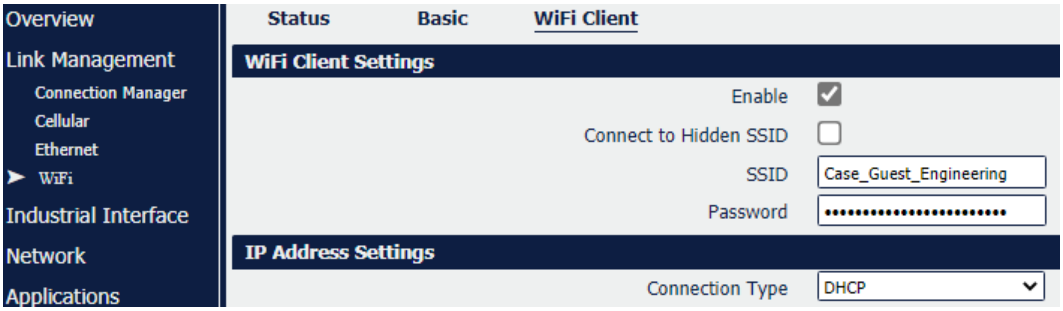
Configuring Wi-Fi

Step 1: Click on **Link Management >Wi-Fi > Basic**



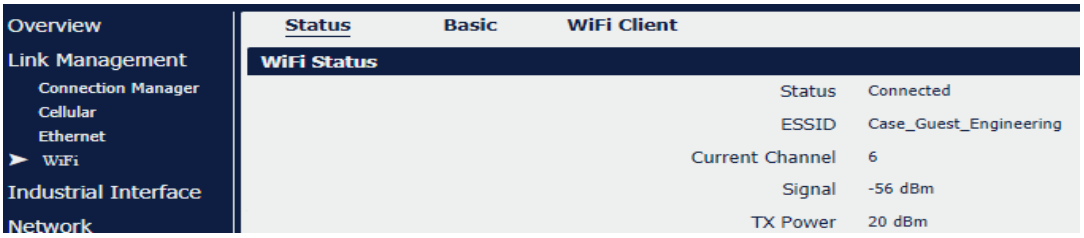


Step 2: Select Running Mode as Client and set the correct Country code.
Step 3: Click on Save and then Apply.
Step 4: Click on **Wi-Fi Client**



Step 5: Click 'Enable' and if required click 'Connect to Hidden SSID' if the router or access point hides the SSID.

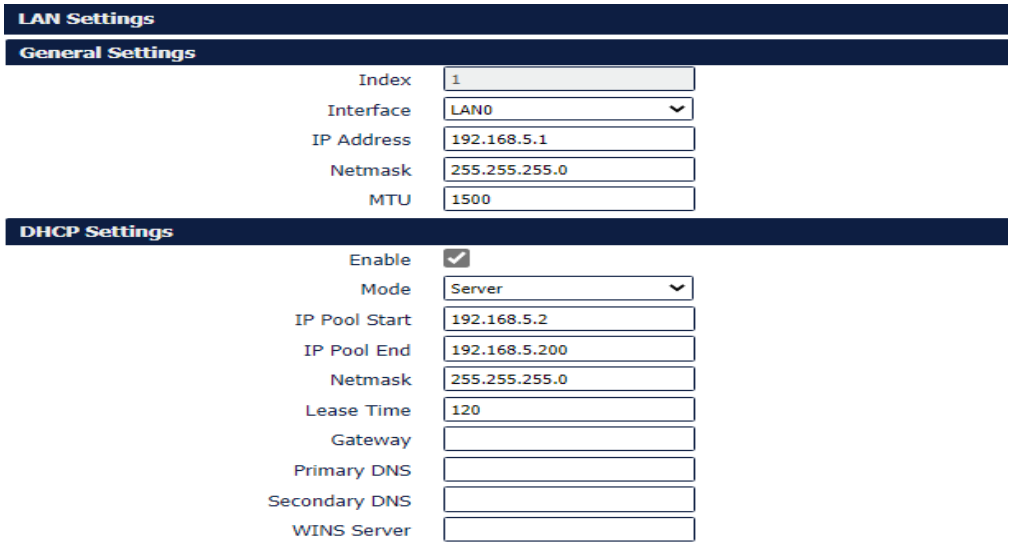
Step 6: Enter the SSID name and Password
Select the required Connection Type, Probably DHCP or a Static IP Address can be used, but only if a known, free IP address is available on the router or access point.
Step 7: Click on Save and then Apply.
Step 8: Click on **Status** and after a little time the 6944 should connect.



Configuring the Ethernet Ports

If the LAN Address needs to be different t the default of 192.168.5.1 use the following configuration. Please note that the 6944 LAN ports must be in a different IP range than the 3rd party Wireless router or access point.

Step 1: Click **Link Management – Ethernet – LAN -** Click to edit LAN0



Step 2: Edit the LAN settings as required.

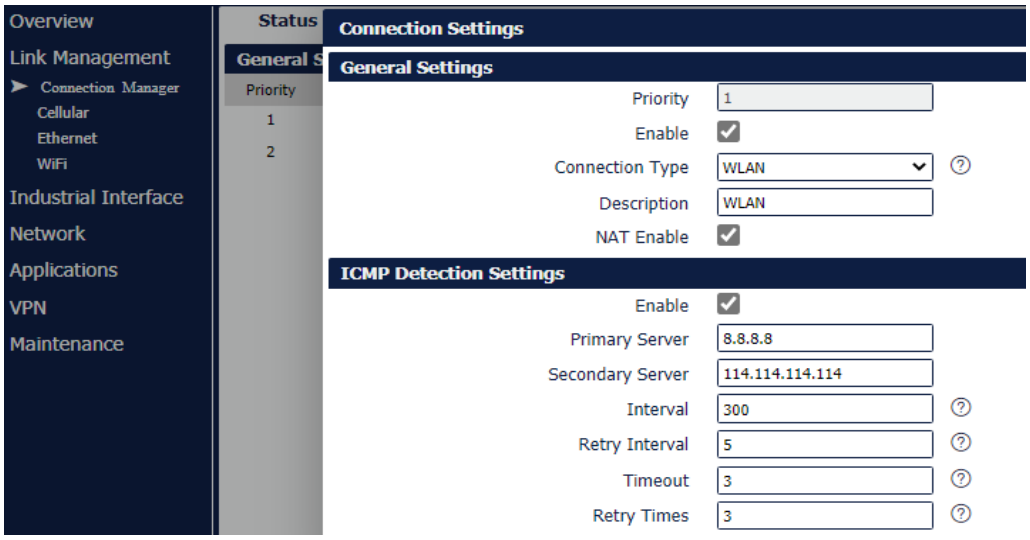
Step 3: Click Save and then Apply.

Please note that if the LAN is changed then you may need to reconnect.

Configuring the WAN Ports

Step 1: Click **Link Management – Connection Manager – Connection**

Step 2: Click to edit the Priority 1 entry.



Step 3: Set Connection Type to WLAN (Wi-Fi LAN)

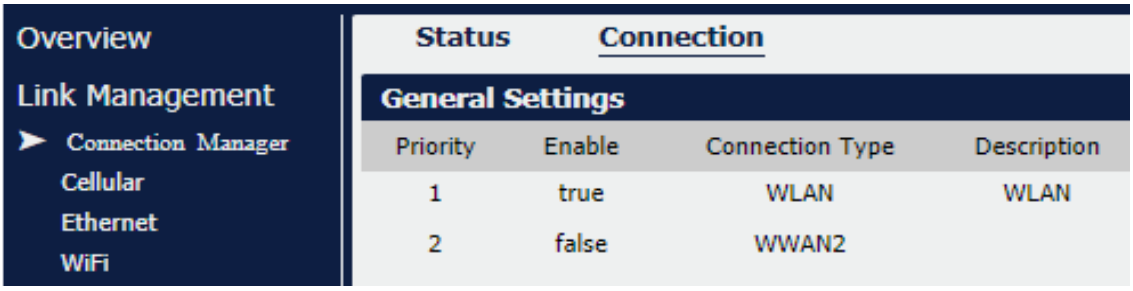
Step 4: Give it a description.

Step 5: Edit the ICMP Detection Settings as required.

Step 6: Click on Save and then Apply.

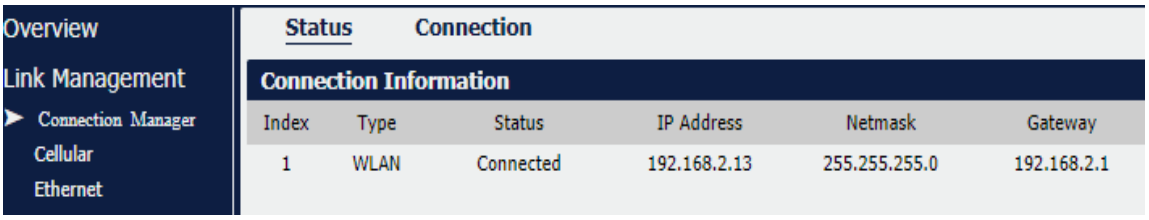
General Settings

Step 1: Either click to delete the Priority 2 entry or edit it to Disable.



Checking WAN Status

Click Status to view the WAN status.



As can be seen from above the 6944 Wireless LAN has connected to the external Wi-Fi router.

Testing Wi-Fi

Connect a PC to one of the 6944's Ethernet ports. Ensure that the PC is either a DHCP client or has been configured with a static IP address that is in the IP range of the 6944's LAN.

Open a command prompt and type **ping 8.8.8.8 (Google)**

```
Command Prompt

C:\>ping 8.8.8.8
Pinging 8.8.8.8. with 32 bytes of data
Reply from 8.8.8.8: bytes=32  time-16ms TTL=120
Reply from 8.8.8.8: bytes=32  time-16ms TTL=120
Reply from 8.8.8.8: bytes=32  time-16ms TTL=120

Ping statistics for 8.8.8.8:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 16ms, Maximum = 16ms, Average = 16ms
```

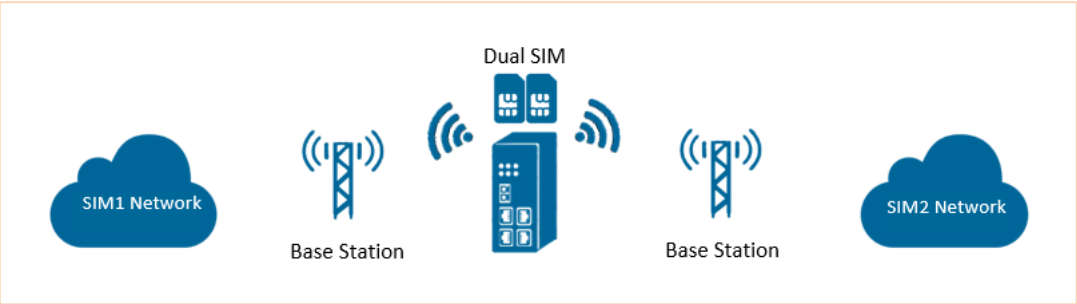
As can be seen a ping to one of Google's DNS servers is working.

7 Configuring Resilient Links

7.1 AN001 Dual SIM Configuration

Testing Topology

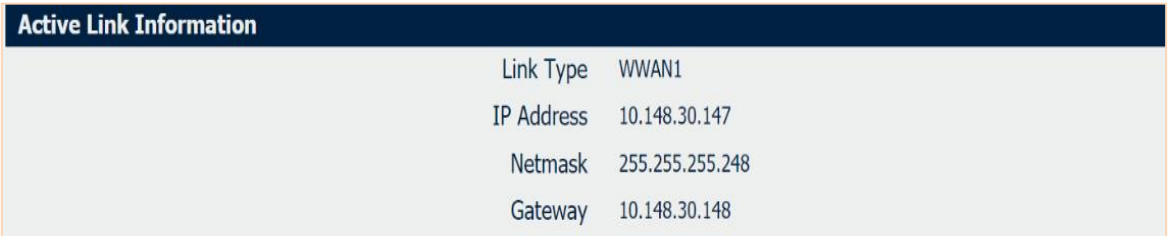
The 6944 Router has the ability to use one of two Cellular Connections, its Ethernet WAN or its Wi-Fi as possible routes out of the 6944, this part of the manual explains how to configure two SIMs for resilience.



- Two SIMs cards are inserted into Case Communications 6944 router, SIM1 as the main SIM and SIM2 as the backup SIM.
- If SIM1 fails to connect to Internet, then Case Communications 6944 will switch to SIM2 to provide continual network connection.

Internet Configuration

Step 1: Insert your SIM card to allow the 6944 to gain internet access.
Check the active link information

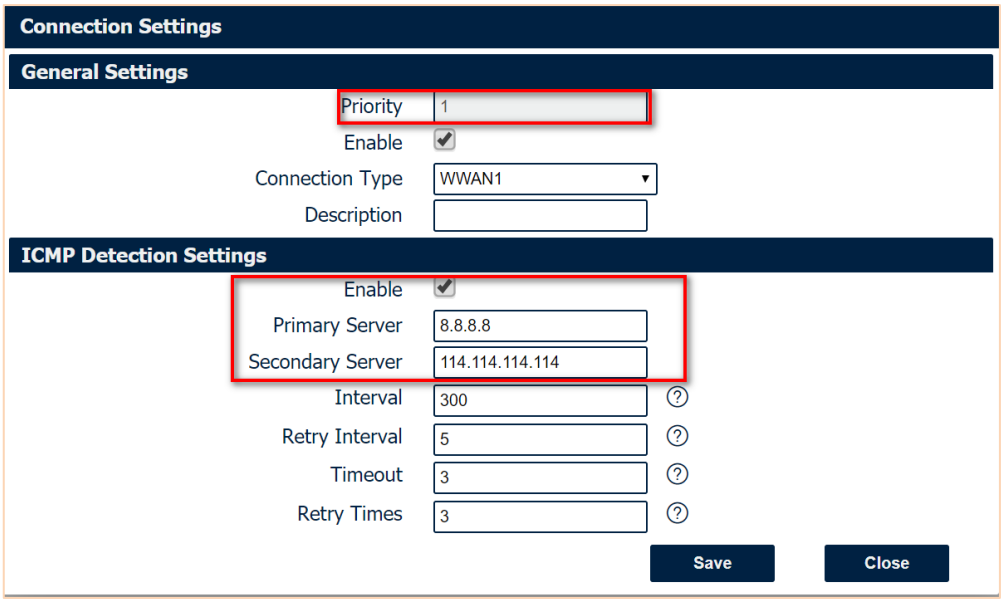


Dual SIMs Strategy Configuration

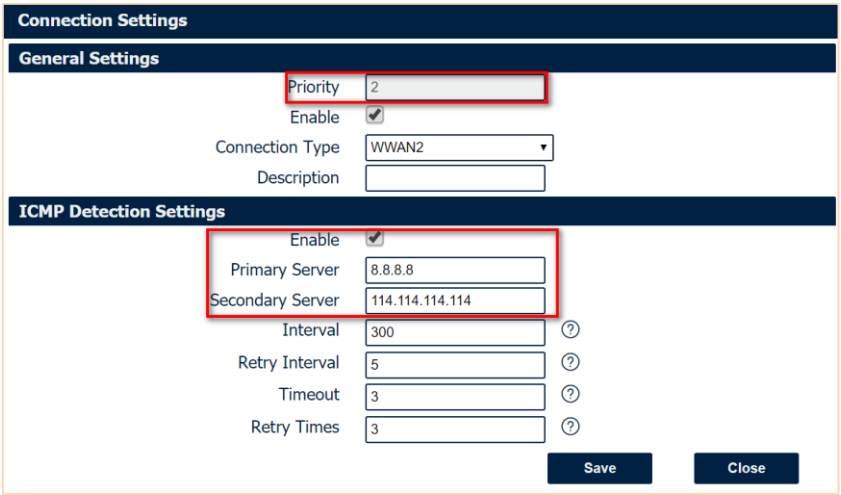
Step 1: Go to Link **Management>Connection Manager>Connection**, Click the **Edit button** of WWAN1 and WWAN2.

Step 2: Specify WWAN1 as Priority1, which means that the WWAN1 is primary link. Enable ICMP detection. Click **Save**

.



Step 3: Specify WWAN2 with a link Priority2, which means that the WWAN2 is the backup link. Enable ICMP detection. Click **Save**.

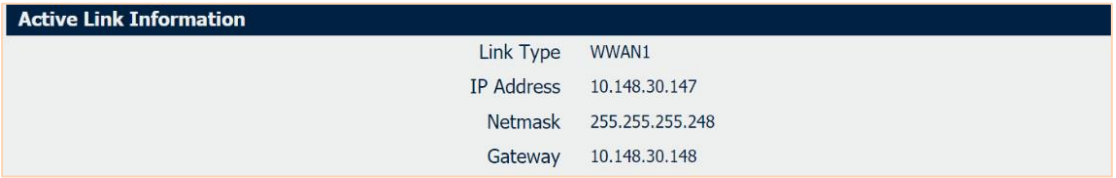


Step 4: Click **Save>Apply**.

<u>Testing</u>

Checking the Internet Connection Status

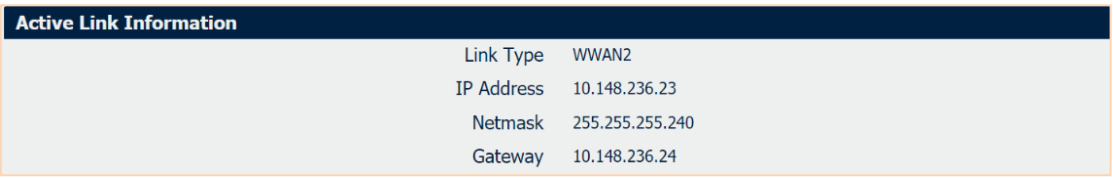
Go to **Overview>Overview>Active Link Information**, the current Link should be WWAN1.



Go to Link Management>Connection Manager>Status, only show the information of WWAN1.

Test Results

When WWAN1 fails to connect to the Internet (detected by an ICMP ping fail), WWAN2 will be active and connect to the Internet. Check the Internet status after switching the SIM card.



Checking the 6944 Syslog

Syslog shows the SIM card switch process, only the information relevant above configuration will be explain below:

==========

Jun 12 08:00:27 casecomms daemon.err udhcpc[1575]: lease of 10.44.201.229 obtained, lease time 7200

Jun 12 08:00:27 casecomms user.debug udhcpc: dhcpc get configuration of wwan1

Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: connection of wwan1 is connected

Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: setup active link wwan1

Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: start ICMP detecting(wwan1->8.8.8.8/114.114.114.114)

Jul 29 11:18:40 casecomms user.debug modem[1185]: +CGREG: 2,1,"2508","6016C02",7

Jul 29 11:18:40 casecomms user.debug modem[1185]: OK

Jul 29 11:18:40 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (1/3)

Jul 29 11:18:43 casecomms user.debug connection_manager[1115]: timer proc status = 2

Jul 29 11:18:43 casecomms user.debug connection_manager[1115]: start ICMP detecting(wwan1->8.8.8.8/114.114.114.114)

Jul 29 11:18:49 casecomms user.debug connection_manager[1115]: connection_manager proc_icmp_detection

Jul 29 11:18:49 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (2/3)

Jul 29 11:18:50 casecomms user.debug modem[1185]: OK

Jul 29 11:18:52 casecomms user.debug connection_manager[1115]: start ICMP detecting(wwan1->8.8.8.8/114.114.114.114)

Jul 29 11:18:55 casecomms user daemon.info urandom_seed[1338]: Seed saved (/etc/urandom.seed)

Jul 29 11:18:58 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (3/3)

Jul 29 11:18:59 casecomms user.debug modem[1185]: link wwan1 disconnected

Jul 29 11:18:59 casecomms user daemon.err udhcpc[1593]: entering released state

Jul 29 11:18:59 casecomms user.debug connection_manager[1115]: SIM switch from SIM1 to SIM2, reload modem with SIM2

Jul 29 11:18:59 casecomms user.debug connection_manager[1115]: II wwan2 modem[1185]: modemd exit

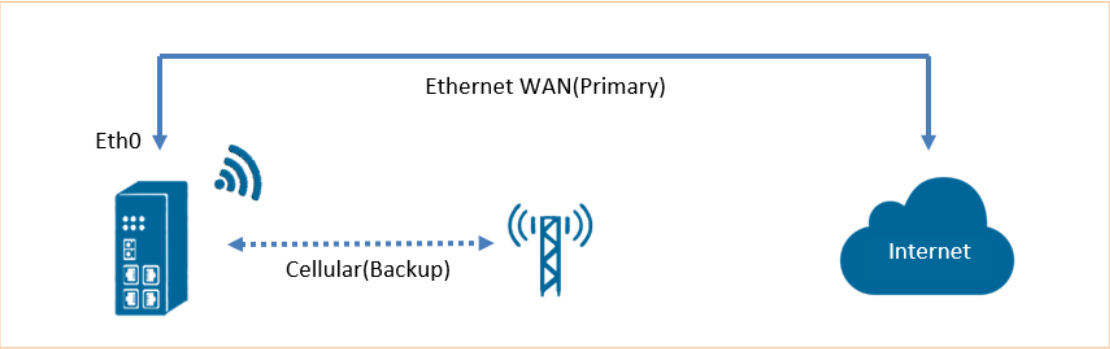
Jul 29 11:19:09 casecomms user.debug modem[2360]: modem init with SIM2

Jul 29 11:19:41 casecomms daemon.err udhcpc[3000]: lease of 10.148.236.23 obtained, lease time 7200

7.2 Link Back Up WAN to Cellular

This part of the manual explains how to back up an Ethernet WAN Port using the 6944's Cellular Links

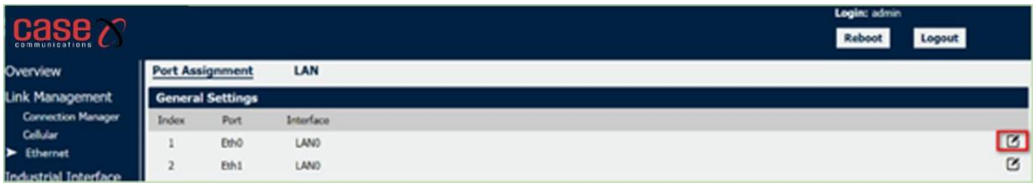
Testing Topology



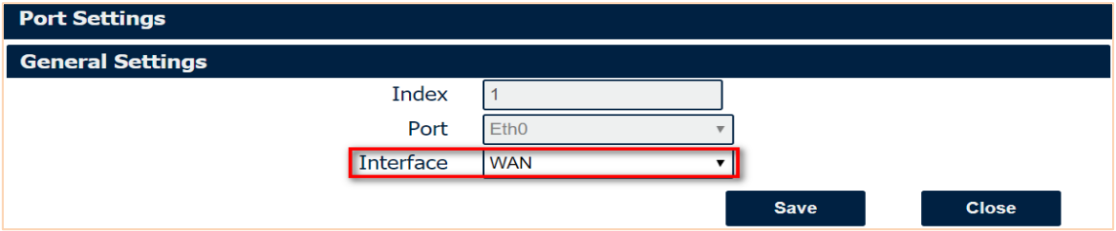
- Specify Eth0 as Primary WAN interface and cellular (wwan1) as the backup interface.
- If the 6944 detects the primary WAN is down, the 6944 will switch to the cellular network to provide continual network connection.
- The 6944 will keep using the WAN link to ping the ICMP address, if it succeeds in getting a reply then the 6944 will switch back from the backup link(cellular) to primary link(WAN)

Eth0 Configuration

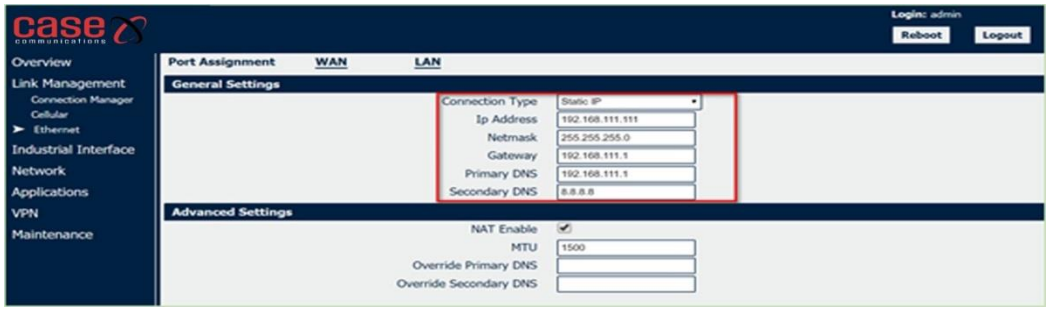
Step 1: Insert your SIM card to allow the 6944 to gain internet access. Check the active link information
Step 2: Go to **Link Management>Ethernet>Port Assignment**, click the **Edit Button** of Eth0.



Step 3: Specify the interface and set it as **WAN,** Click **Save.**



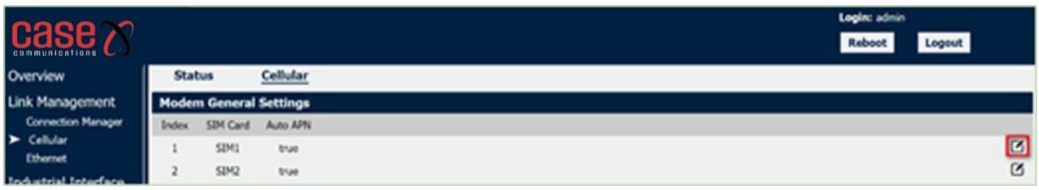
Step 4: Go to Link Management>Ethernet>WAN, enter the relevant information of the WAN port to make sure the 6944connects to Internet.



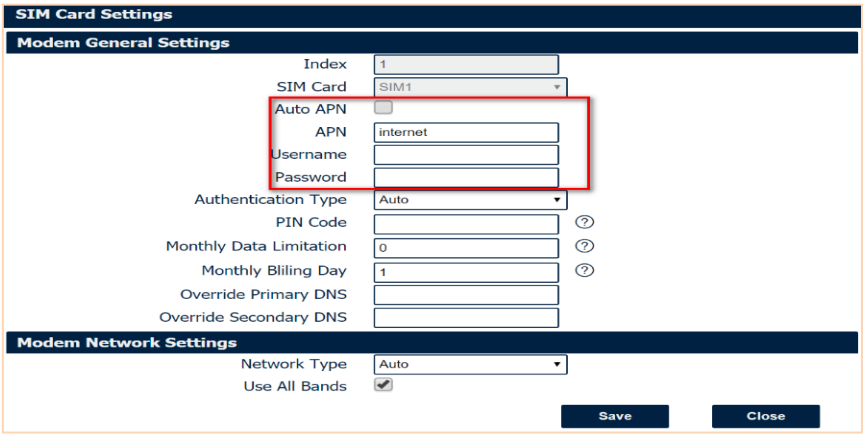
Step 5: Click **Save>Apply**.

Cellular Configuration

Step 1: Go to Link **Management>Cellular>Cellular**, click the **Edit button** for SIM1



Step 2: Enter the correct **APN, Username, Password** for SIM, to make sure the 6944connects to the Internet. Click **Save**.

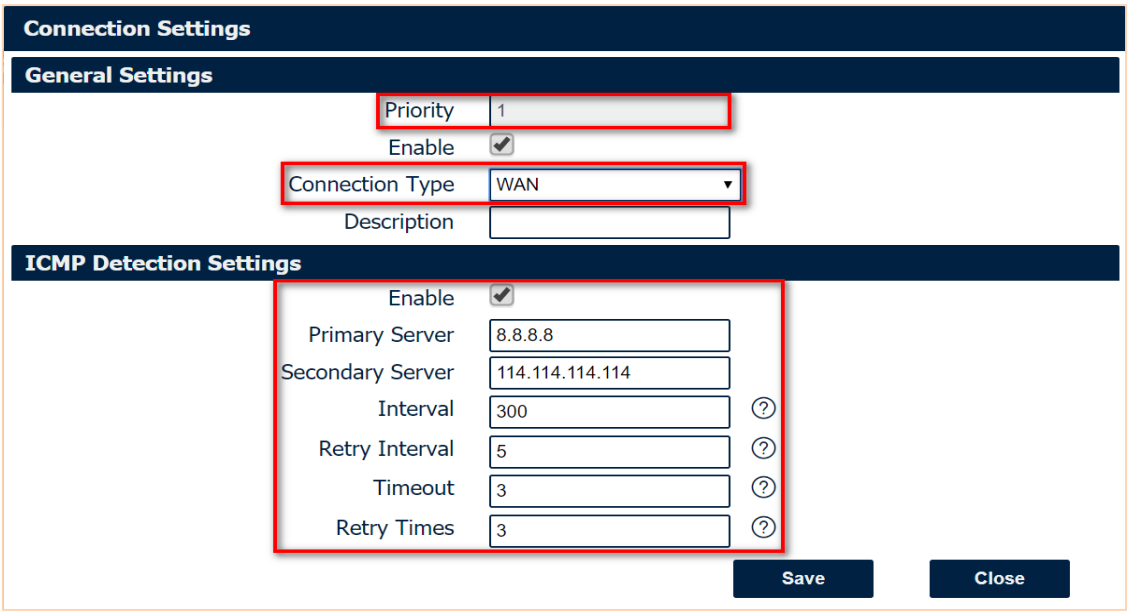


Step 3: Click **Save>Apply.**

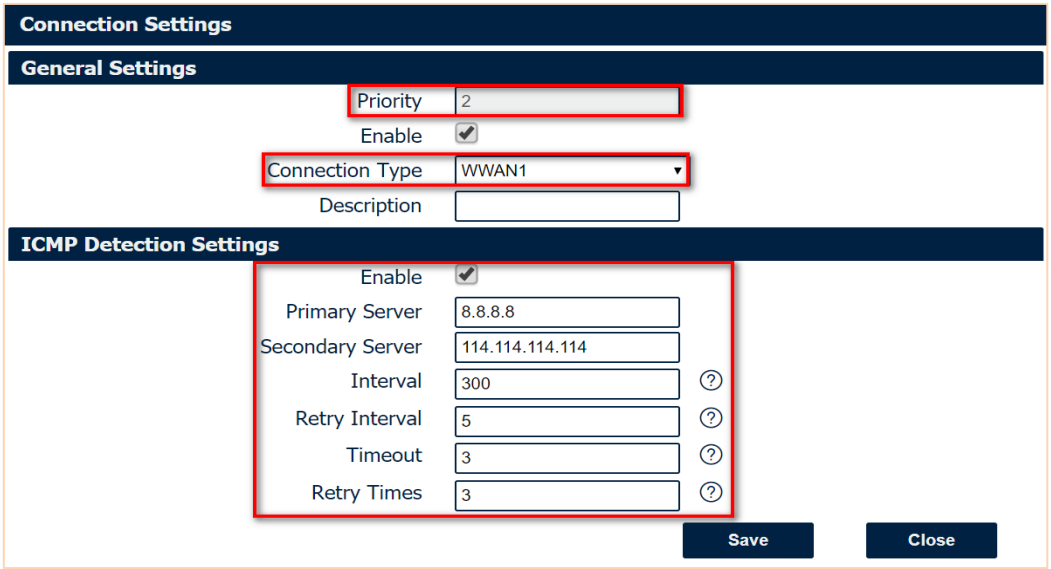
Link Backup Strategy Configuration

Step 1: Go to **Link Management>Connection Manager>Connection**, delete the WWAN1 and WWAN2 interface. Click **Save>Apply**.

Step 2: Add the WAN link and configure it as priority 1, enable ICMP detection for link detection. Click **Save**.



Step 3: Add WWAN1 link and configure it as priority 2, and enable ICMP detection used for link detection. Click **Save.**



Step 4: Click **Save>Apply**.

<u>Testing</u>

- Currently both the WAN and Cellular connections are online, the 6944 will connect to the Internet using primary link(WAN).
- If the 6944 detects the primary link (WAN) is down, then it will switch to the backup link(wwan1) for the Internet connection.
- If the Primary link (WAN) comes up again, then 6944 will switch back from backup link (WWAN1) to its primary WAN Link

Internet Status

Step 1: Go to **Overview>Overview>Active Link Information**, the 6944 is using the primary link(WAN) for Internet access.

Active Link Information	
Link Type	WAN
IP Address	192.168.111.111
Netmask	255.255.255.0
Gateway	192.168.111.1

Step 2: Remove the Ethernet Cable from the WAN port, to make the primary link go down. The 6944 will switch to WWAN1 to establish communications with Internet.

Step 3: Go to **Overview>Overview>Active Link Information** to check again**,** the 6944 is now using the backup link for Internet access.

Active Link Information	
Link Type	WWAN1
IP Address	10.162.9.151
Netmask	255.255.255.240
Gateway	10.162.9.152

Step 4: Insert the 6944 Ethernet Cable, and the 6944 will switch from the backup link to primary link.

Step 5: Go to **Overview>Overview>Active Link Information** to check the status**,** the 6944 is now using the primary link to gain Internet access.

Active Link Information	
Link Type	WAN
IP Address	192.168.111.111
Netmask	255.255.255.0
Gateway	192.168.111.1

Checking the 6944 Syslog

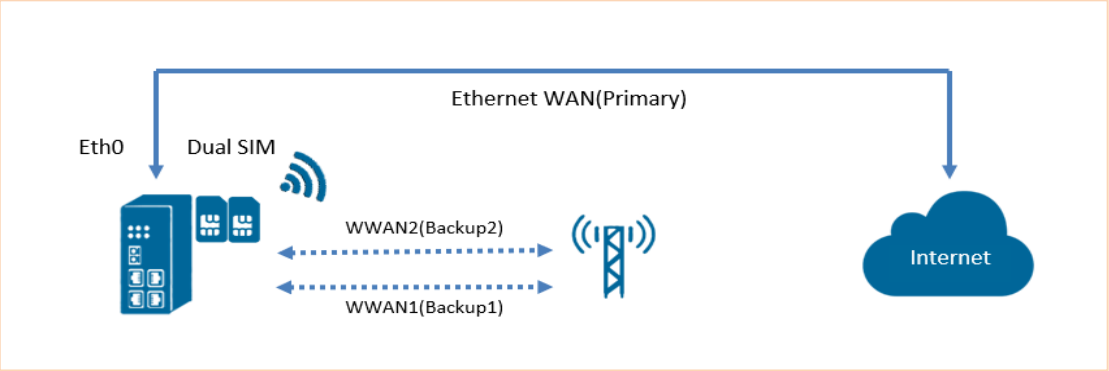
Syslog shows the switch process of link, please check below:

```
Jun 12 08:00:04 casecomms syslog.info syslogd started: BusyBox v1.25.1
Jun 12 08:00:07 casecomms user.debug connection_manager[1148]: setup active link wan
Jun 12 08:00:07 casecomms user.debug connection_manager[1148]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jun 12 08:00:08 casecomms user.debug connection_manager[1148]: connection_manager proc_icmp_detection
Jun 12 08:00:08 casecomms user.debug connection_manager[1148]: WAN ICMP detecting success
Jun 12 08:00:08 casecomms user.debug connection_manager: connection wan, active link 1, health state 0
Jul 29 16:08:20 casecomms user.debug connection_manager[1148]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jul 29 16:08:23 casecomms user.debug connection_manager[1148]: connection_manager proc_icmp_detection
Jul 29 16:08:23 casecomms user.debug connection_manager[1148]: WAN ICMP detecting failed (1/3)
Jul 29 16:08:29 casecomms user.debug connection_manager[1148]: connection_manager proc_icmp_detection
Jul 29 16:08:35 casecomms user.debug connection_manager[1148]: WAN ICMP detecting failed (3/3)
Jul 29 16:08:40 casecomms user.debug connection_manager[1148]: connection_manager proc_icmp_detection
Jul 29 16:08:40 casecomms user.debug connection_manager[1148]: WWAN1 ICMP detecting success
Jul 29 16:08:40 casecomms user.debug connection_manager[1148]: connection wwan1, active link 1, health state 0
Jul 29 16:08:46 casecomms user.debug connection_manager[1148]: start ICMP detecting(wan
Jul 29 16:08:46 casecomms user.debug connection_manager[1148]: connection_manager proc_icmp_detection
Jul 29 16:08:46 casecomms user.debug connection_manager[1148]: WAN ICMP detecting success
```

7.3 AN003 - 3 Link back up WAN, WWAN1 & WWAN 2

This part of the manual covers the 6944's triple alternate routes, Ethernet WAN, Wireless WAN 1 and Wireless WAN 2

Testing Topology

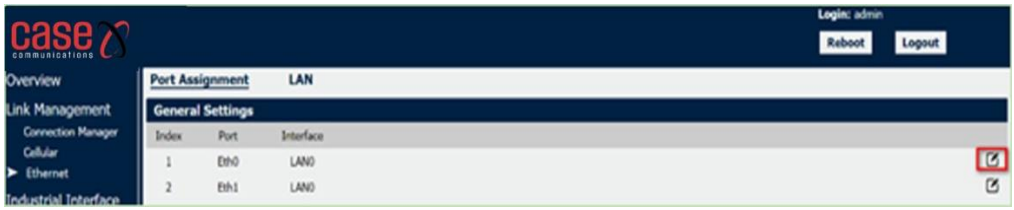


- Specify Eth0 as the Primary WAN interface and wwan1 as the secondary backup interface, and wwan2 as third backup interface.
- If the 6944 detects the primary WAN is down, it will switch to wwan1 (Wireless WAN 1) to provide an instant network connection.
- If the 6944 detects both WAN and wwan1 is down, it will switch to wwan2 to restore the network connection.
- The 6944 will keep trying an ICMP Ping on the WAN to ping the address, if it succeeds then it will switch back from backup link (wwan1 or wwan2) to primary link (WAN)

Configuring Ethernet 0

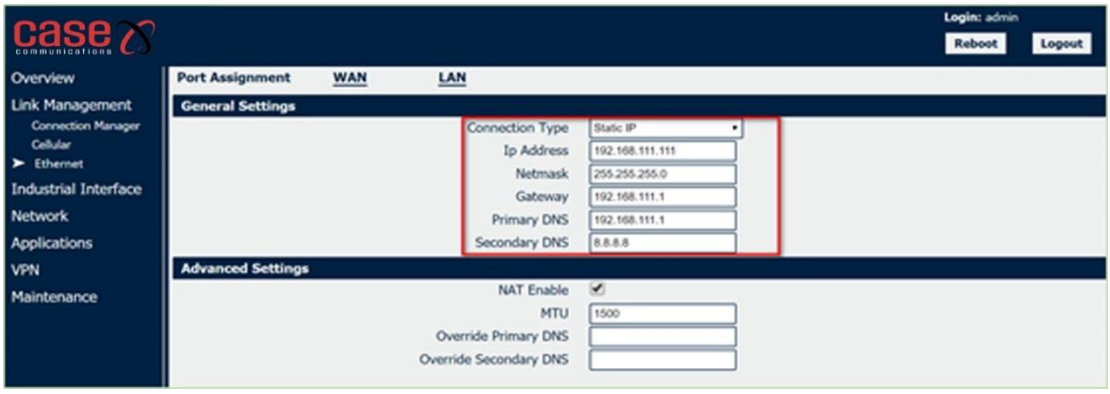
Step 1: Insert your SIM card to allow the 6944 to gain internet access. Check the active link information

Step 2: Go to **Link Management>Ethernet>Port Assignment**, click the **Edit Button** for Eth0.



Step 3: Specify the interface and set it as **WAN,** Click **Save.**

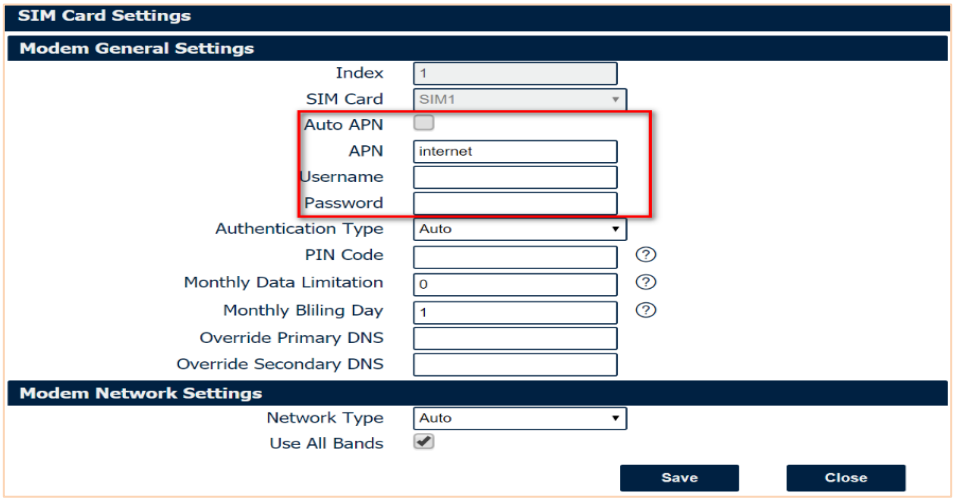
Step 4: Go to Link Management>Ethernet>WAN, enter the relevant information for the WAN port to make sure it can connect to the Internet.



Step 5: Click **Save>Apply**.

Cellular Configuration

Step 1: Go to Link **Management>Cellular>Cellular**, click the **Edit button** of **SIM 1 and SIM 2**.

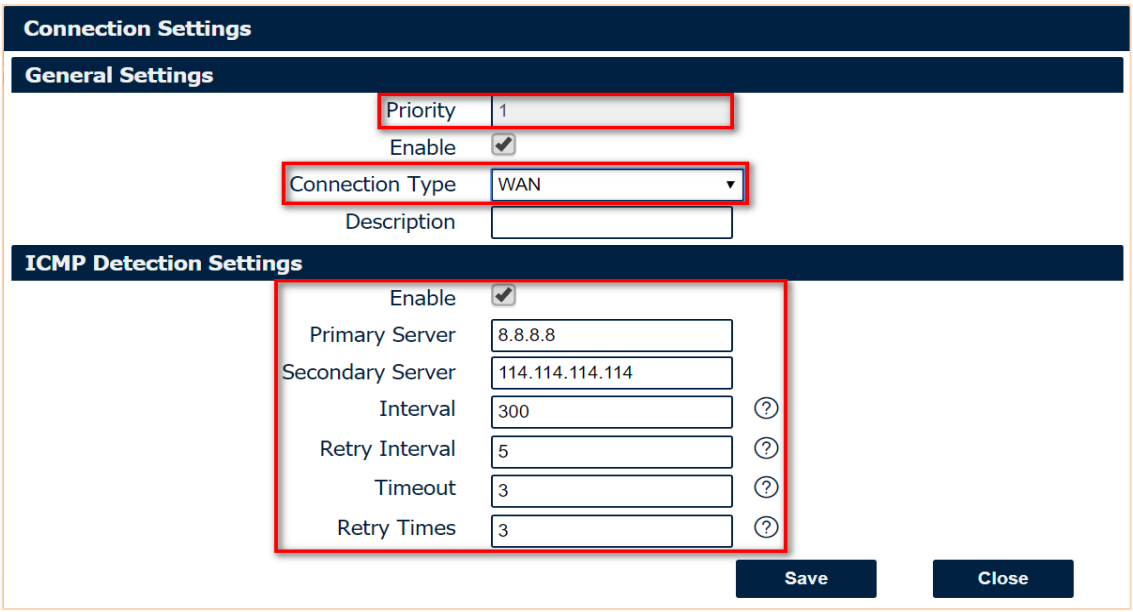


Step 2: Click **Save>Apply.**

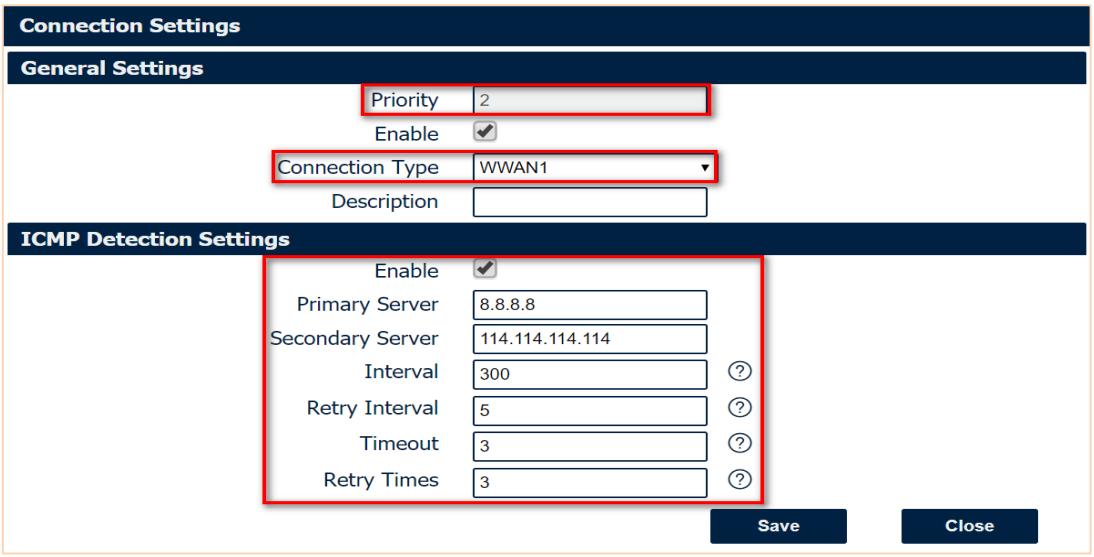
Link Backup Strategy Configuration

Step 1: Go to **Link Management>Connection Manager>Connection**, delete the WWAN1 and WWAN2 interfaces. Click **Save>Apply**.

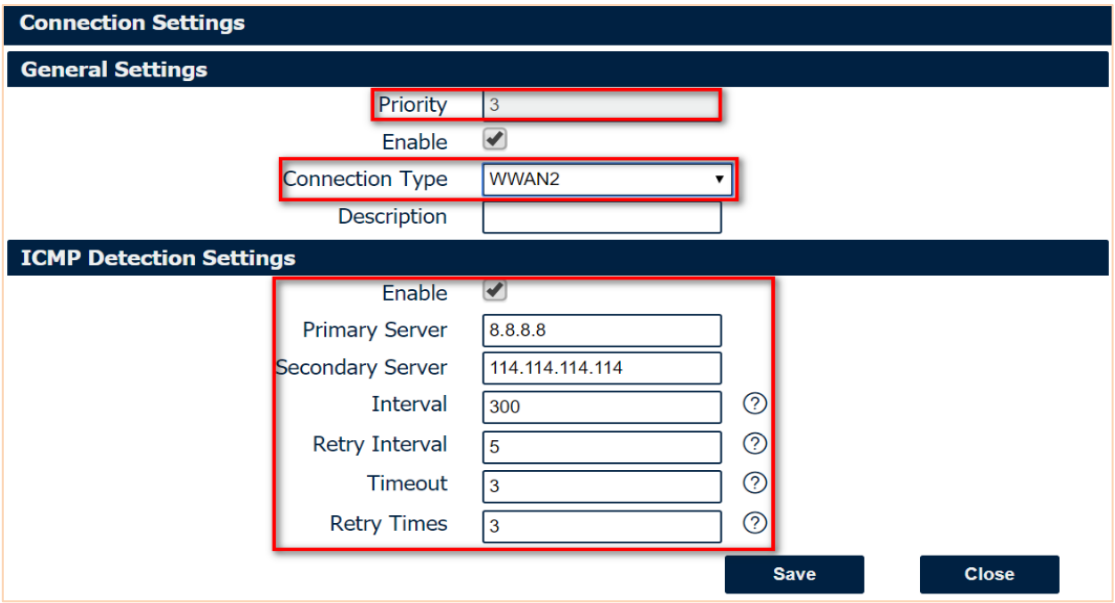
Step 2: Add the WAN link and make it's priority 1, and enable ICMP detection for link detection. Click **Save**.



Step 3: Add the WWAN1 link and set it to priority 2, enable ICMP detection used for link detection. Click **Save**



Step 4: Add the WWAN2 link and make it's priority 3, also enable ICMP detection for link detection. Click **Save**



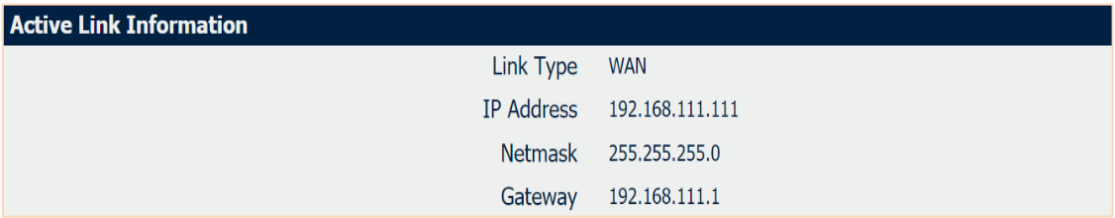
Step 5: Click **Save>Apply**.

Testing

- To Start make sure both WAN and WWAN1 are online, the 6944 will connect to Internet via the primary WAN.
- If the 6944 detects the primary WAN is down, then it will switch to the backup interface which is WWAN1 to access the Internet.
- If the 6944 detects both WAN and WWAN1 are down, then it will switch to WWAN2 to access the Internet
- If the Primary WAN link comes up again, then the 6944 will switch back to the primary WAN.

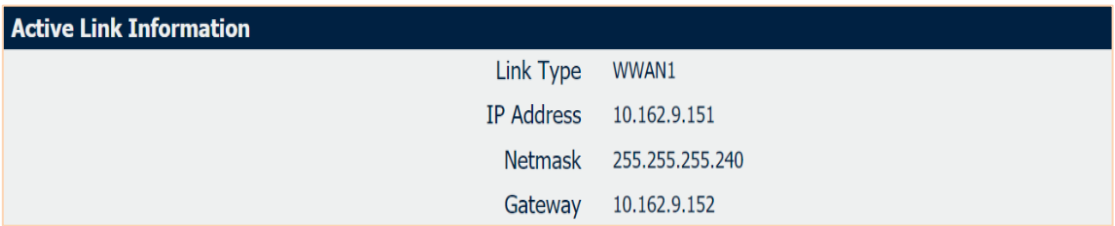
Internet Status

Step 1: Go to **Overview>Overview>Active Link Information**, 6944 is using primary WAN for Internet access.



Step 2: Remove the Ethernet Cable connected to the Ethernet WAN, to force the primary link down. The 6944 will switch to WWAN1 to connect to the Internet.

Step 3: Go to **Overview>Overview>Active Link Information** to check the 6944 is now using WWAN1 to access the Internet.



Step 4: When the 6944 detects WWAN1 is down, it will switch to WWAN2 for Internet access.

Active Link Information	
Link Type	WWAN2
IP Address	10.132.13.31
Netmask	255.255.255.192
Gateway	10.132.13.32

Step 5: Insert again the 6944 Ethernet Cable, and the 6944 will switch back from WWAN2 to the primary WAN again.

Step 6: Go to **Overview>Overview>Active Link Information** to check the status**,** 6944 is now using its primary link for Internet access again.

Active Link Information	
Link Type	WAN
IP Address	192.168.111.111
Netmask	255.255.255.0
Gateway	192.168.111.1

Checking the Syslog

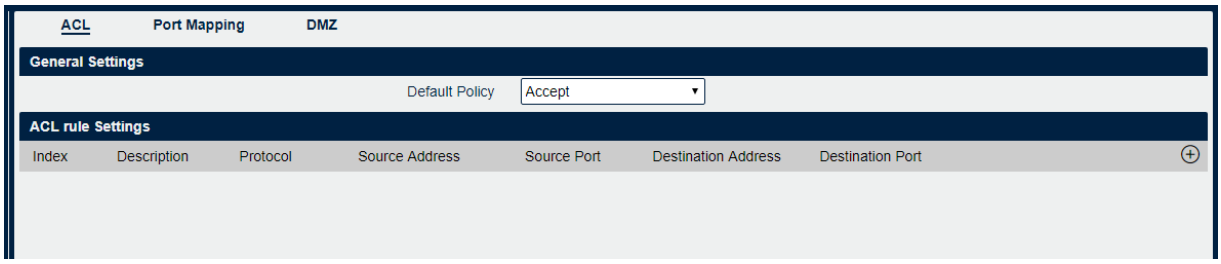
Syslog shows the switch process of link, please check below:

Jun 12 08:00:07 casecomms user.debug connection_manager[1126]: setup active link wan
Jun 12 08:00:07 casecomms user.debug connection_manager[1126]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jun 12 08:00:07 casecomms daemon.info dnsmasq[1139]: reading /etc/resolv.conf
Jun 12 08:00:11 casecomms user.debug connection_manager[1126]: WAN ICMP detecting failed (1/3)
Jun 12 08:00:12 casecomms user.debug modem[1294]: AT+CGDCONT=1,"IP"
Jun 12 08:00:12 casecomms user.debug modem[1294]: OK
Jun 12 08:00:12 casecomms user.debug modem[1294]: AT+CMGF=0
Jun 12 08:00:12 casecomms user.debug modem[1294]: OK
Jun 12 08:00:12 casecomms user.debug modem[1294]: AT+CNMI=2,1
Jun 12 08:00:12 casecomms user.debug modem[1294]: OK
Jun 12 08:00:12 casecomms user.debug modem[1294]: AT+CGREG?
Jun 12 08:00:12 casecomms user.debug modem[1294]: +CGREG: 2,1,"2508","6016C02",7
Jun 12 08:00:13 casecomms user.debug modem[1294]: OK
Jun 12 08:00:13 casecomms user.debug modem[1294]: modem is ready
Jun 12 08:00:14 casecomms daemon.notice procd: /etc/rc.d/S96led: /etc/rc.common: line 165: uci_load: not found
Jun 12 08:00:14 casecomms user.debug connection_manager[1126]: timer proc status = 2
Jun 12 08:00:14 casecomms user.debug connection_manager[1126]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jun 12 08:00:14 casecomms user.debug modem[1294]: OK
Jun 12 08:00:14 casecomms user.err modem[1294]: stopping quectel_cm failed
Jun 12 08:00:14 casecomms user.debug modem[1294]: set apn(3gnet) interface(wwan1)
Jun 12 08:00:17 casecomms user.debug connection_manager[1126]: connection_manager proc_icmp_detection
Jun 12 08:00:17 casecomms user.debug connection_manager[1126]: WAN ICMP detecting failed (2/3)
Jun 12 08:00:20 casecomms user.debug connection_manager[1126]: timer proc status = 2
Jun 12 08:00:20 casecomms user.debug connection_manager[1126]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jun 12 08:00:23 casecomms user.debug connection_manager[1126]: connection_manager proc_icmp_detection
Jun 12 08:00:23 casecomms user.debug connection_manager[1126]: WAN ICMP detecting failed (3/3)
Jun 12 08:00:23 casecomms user.debug connection_manager[1126]:
Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: started, v1.25.1
Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: sending discover
Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: sending select for 10.169.103.152
Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: lease of 10.169.103.152 obtained, lease time 7200
Jun 12 08:00:29 casecomms user.debug udhcpc: dhcpc get configuration of wwan1
Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: connection_manager proc_connected
Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: connection_manager proc_icmp_detection
Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: WWAN1 ICMP detecting success

8 Network Security

8.1. Firewall and ACL

Firewall rules are security rule-sets used to implement control over users, applications or network objects in an organisation. Using the firewall rule, you can create blanket or specialized traffic transit rules based on the requirement.



Router Configuration

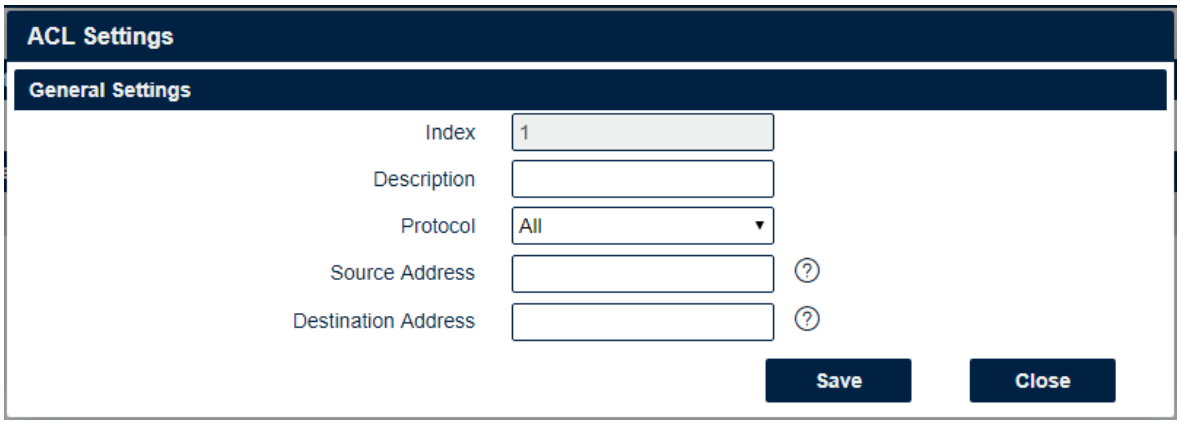
Firewall->ACL

- **Default Policy**

Select the "Accept" or "Drop" from the list, the packets which are not included in the access control list will be processed by the default filter policy.

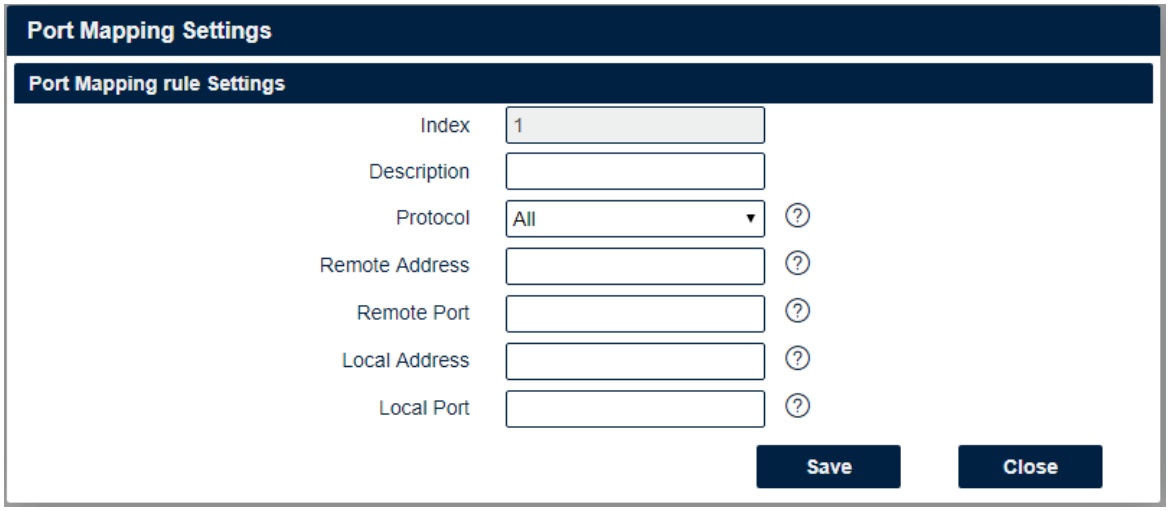
- **Access Control List.**

An Access Control List (ACL), with respect to a computer file system, is a list of permissions attached to an object. An ACL specifies which users or system processes are granted access to objects, as well as what operations are allowed on given objects.



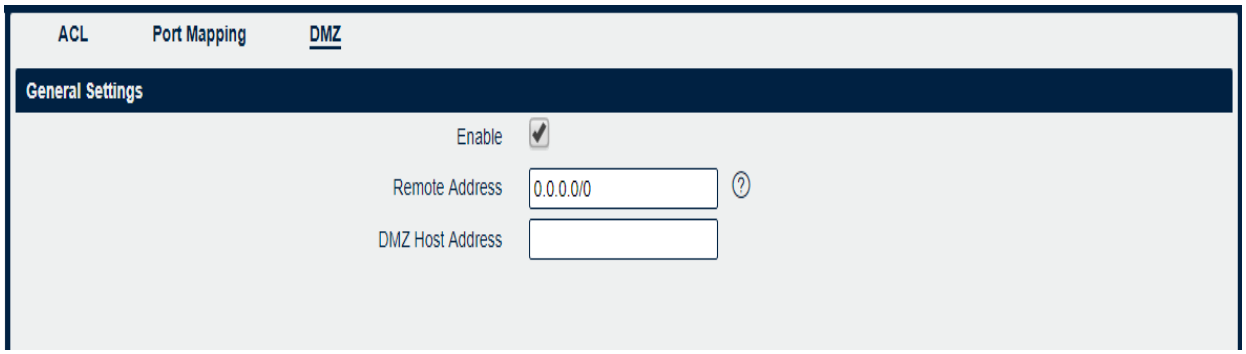
Firewall->ACL

- **Description -** Add a description for this rule.
- **Protocol** All: Any protocol such as;
  TCP: The TCP protocol.
  UDP: The UDP protocol.
  TCP & DUP: both TCP and UDP protocol
  ICMP: The ICMP protocol.
- **Source Address -** A specific host IP address can also be specified, or a range of IP addresses via a bitmask (in the box following the /).
- **Destination Address -** A specific IP address can also be specified, or a range of IP addresses via a bitmask (in the box following the /).



Firewall->Port Mapping

- **Description -** Add a description for this rule.
- **Protocol: - All**: Selects any protocol. TCP protocol, UDP protocol.
- **Remote Address -** Enter a WAN IP address that is allowed to access the unit.
- **Remote Port -** Enter the external port number range for incoming requests.
- **Local Address -** Sets the LAN address of a device connected to one of the 6944's LAN interfaces. Inbound requests will be forwarded to this IP address.
- **Local Port: -** Sets the LAN port number range used when forwarding to the destination IP address.



Firewall->DMZ

- **Enable**
  Check this box to enable DMZ function.
- **Remote Address**
  Optionally restricts DMZ access to only the specified WAN IP address.
  NOTE: If set to 0.0.0.0/0, the DMZ is open to all incoming WAN IP addresses.
- **DMZ Host Address**
  The WAN IP address which has all ports exposed except ports defined in the Port Forwarding configuration.

8.2. AN028-Configuring SSH with a Public Key

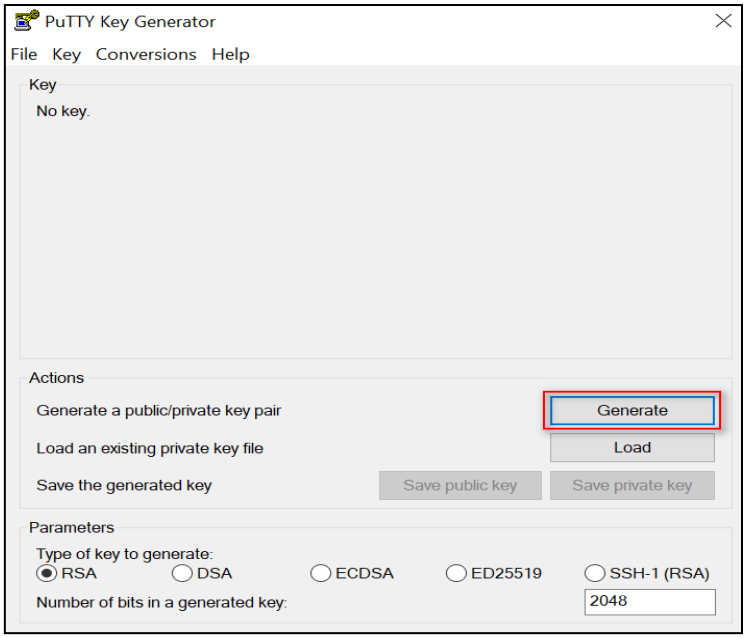
Router Configuration

Step 1: Go to **Maintenance>System>SSH/Security**, to specify the SSH port and enable Remote SSH Access, as shown below.

Step 2: Click Save>Apply.

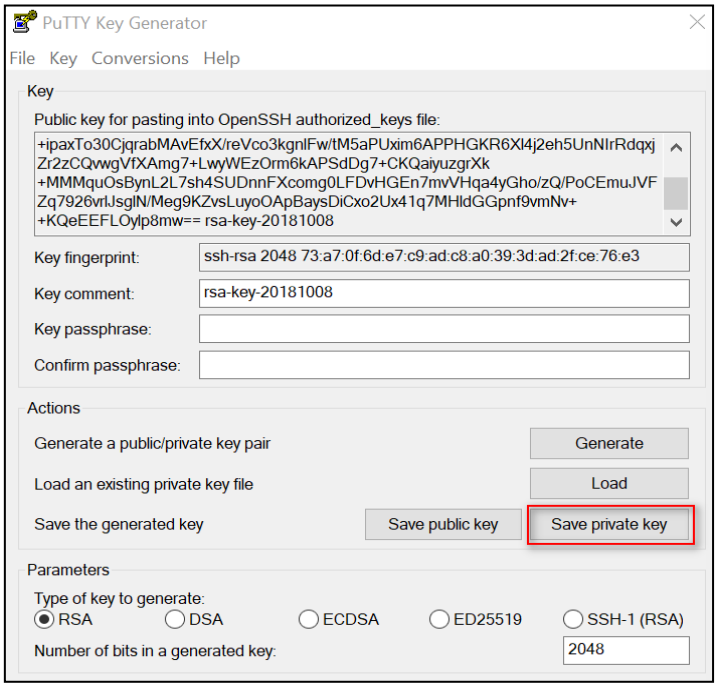
Public/Private Key Generated

Step 1: Run the software "puttygen.exe" to build the public key, as shown below:



Step 2: Copy the public key string to Maintenance>System>SSH, click Save>Apply.

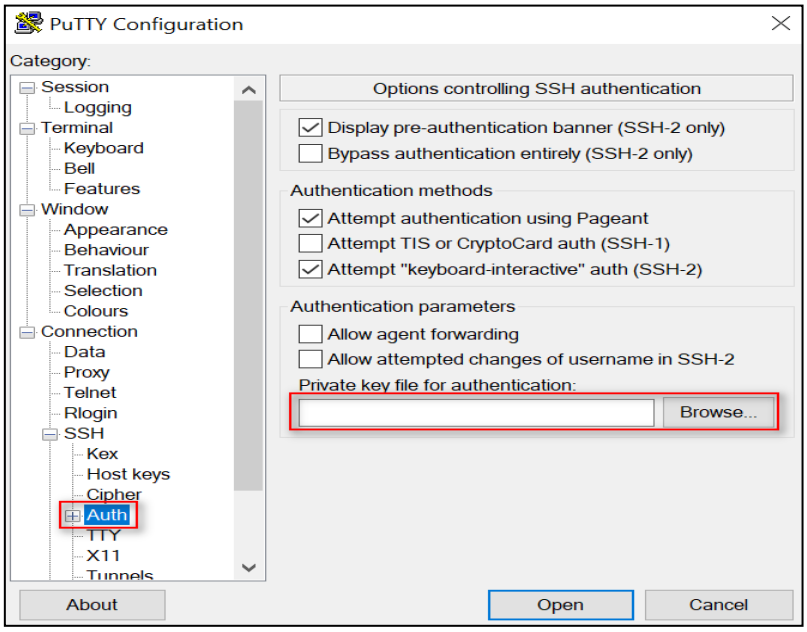
Step 3: Save the Private Key, as shown below:



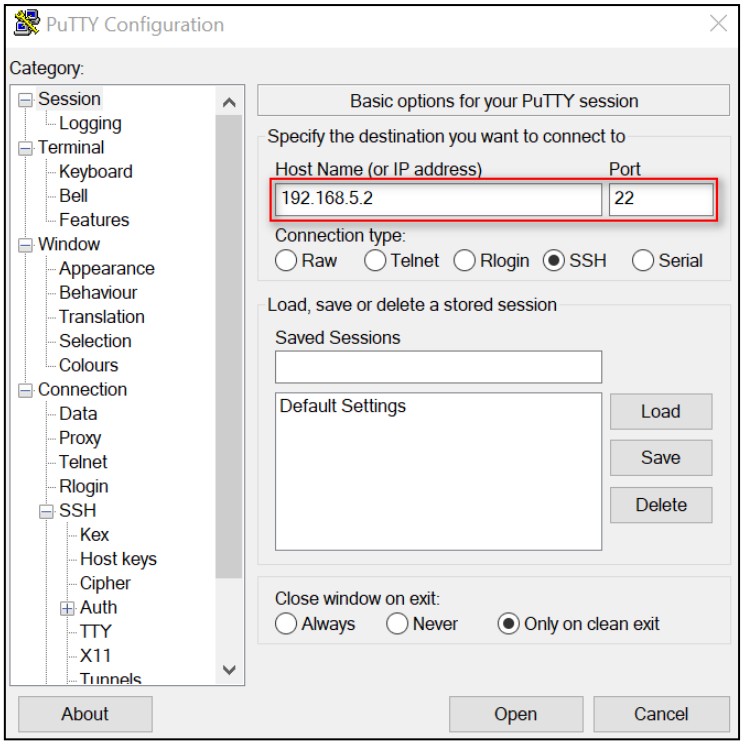
Note: we now need to import the private key to the SSH tool, so that it can provide SSH to the router successfully.

Testing SSH

Step 1: Enable an SSH tool "putty.exe" and import the private key, as shown below:



Step 2: Enter the host name and port to SSH to the router.



Step 3: Test successful.

```
192.168.5.2 - Putty                                    -   □   X
Login as:                    admin
Authenticating with public Key "rsa-key-20181008"
>
>
```

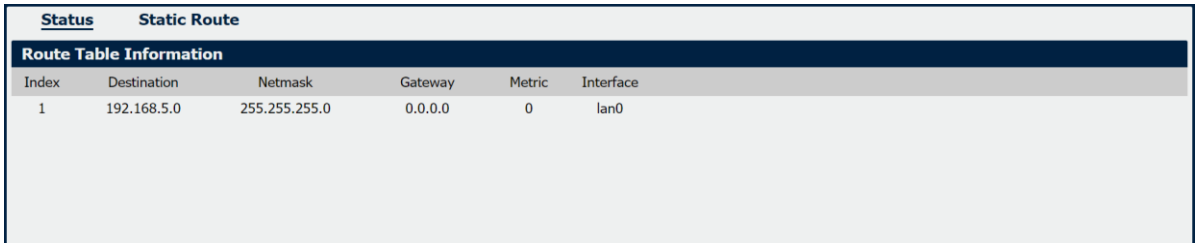
This page left blank intentionally

9 Routing

9.1. Static Routing

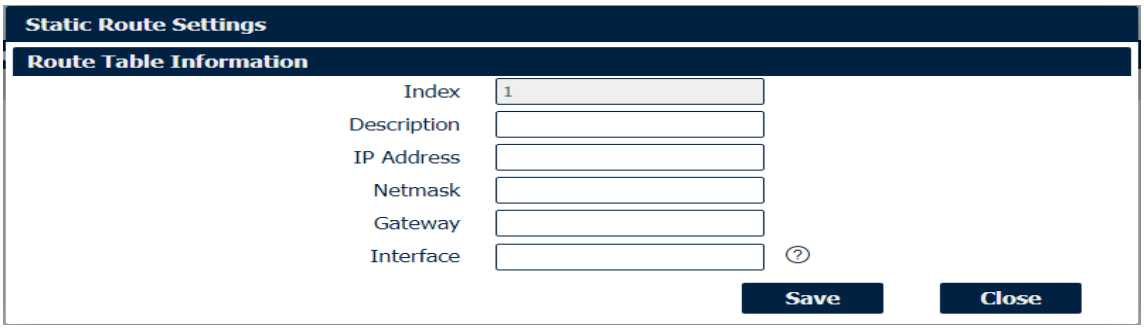
Static Routing refers to a manual method of setting up routing between networks. Select the Static Routing tab to add static routes to the Static Route Table.

Please refer current route table as below.



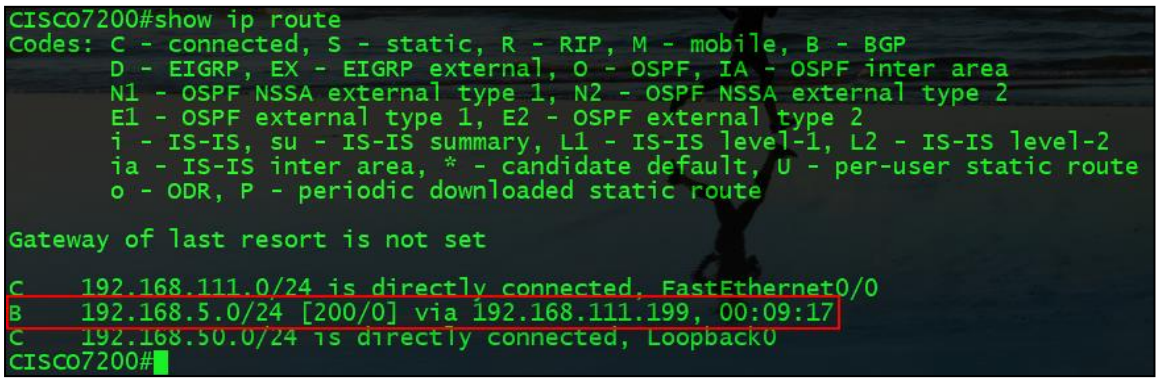
Route->Route Table Information

- **Destination -** Displays the destination of routing traffic.
- **Netmask -** Displays the subnet mask of this routing.
- **Gateway -** Displays the gateway for the 6944. This is used for routing packets to remote networks.
- **Metric -** Displays the metric value of this interface.
- **Interface -** Displays the outbound interface of this route.



Route->Static Route Settings

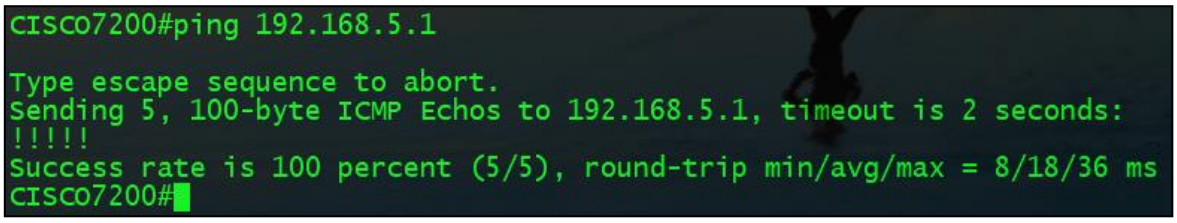
- **Description -** Enter the description of current static route rule.
- **IP Address -** Enter the IP address of the destination network.
- **Netmask -** Enter the subnet mask of the destination network.
- **Gateway -** Enter the IP address of the local gateway.
- **Interface -** Please refer to the Network->Route->Status interface.



Step 2: Checking the 6944 Routing table for reference

Testing

Step 1: Ping from the CISCO router to the 6944 Router



Step 2: Test successful.

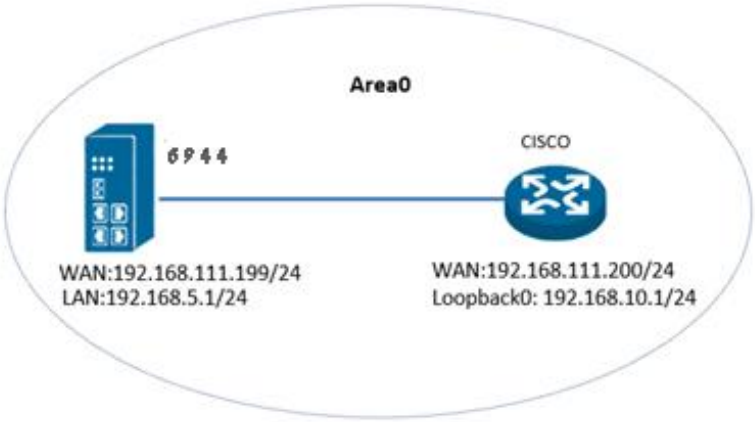
9.2. Dynamic Routing Using RIP

Introduction.

In order to run dynamic routing on the 6944 it's necessary to ensure you have the dynamic routing software installed. This can be obtained from Case Communications and is shown below

Release Date	Doc Version	Firmware Version	Additional Software	Change Description
2018/12/12	V1.1	V1.1.4 (0c0c09fa)	Dynamic Routing Software V1.0.1 642848	First release

Dynamic Routing Topology



- Check both the 6944 and CISCO are running RIP.
- Check both the 6944 and CISCO declare an IP of LAN and loopback0.

Configuration

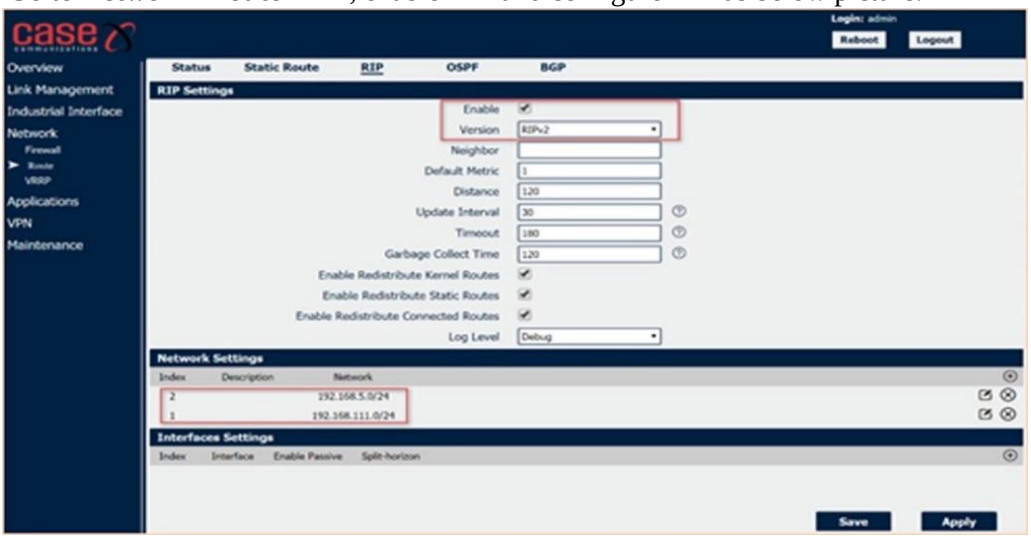
CISCO Configuration

==========

```
CISCO7200#show running-config
Building configuration...
Current configuration : 1165 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO7200
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
 hidekeys
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.200 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router rip
 version 2
 network 192.168.10.0
 network 192.168.111.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
exec-timeout 0 0
privilege level 15
logging synchronous
stopbits 1
line vty 0 4
 login
!
!
end
CISCO7200#
```

6944 Configuration

Step 1: Go to **Network>Route>RIP**, enable RIP and configure RIP as below picture.



Step 2: Click Save>Apply

.

Check the Routing Tables

Step 1: Check the Routing Table on the CISCO 7200 router for reference.

```
CISCO7200#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.111.0/24 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, Loopback0
R    192.168.5.0/24 [120/1] via 192.168.111.199, 00:00:29, FastEthernet0/0
CISCO7200#
```

Step 2: Check the routing Table on the 6944 for reference.

Testing

Step 1: Ping from CISCO to 6944

Step 2: Test successful.

```
CISCO7200#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/36 ms
CISCO7200#
```

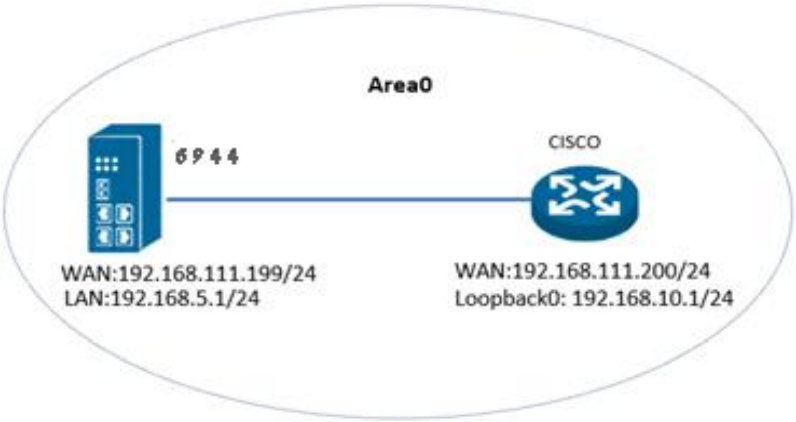
9.3. Dynamic Routing Using OSPF

Introduction.

In order to run dynamic routing and OSPF on the 6944 its necessary to ensure you have the dynamic routing software installed. This can be obtained from Case Communications and is shown below

	Doc Version	Firmware Version	Additional Software	Change Description
2018/12/12	V1.1	V1.1.4 (0c0c09fa)	Dynamic Routing Software V1.0.1 642848	First release

Dynamic Routing Topology



- The 6944 and CISCO 7200 Router run OSPF and under the same single Area 0.
- The 6944 and CISCO 7200 Router set the IP LAN to loopback 0.

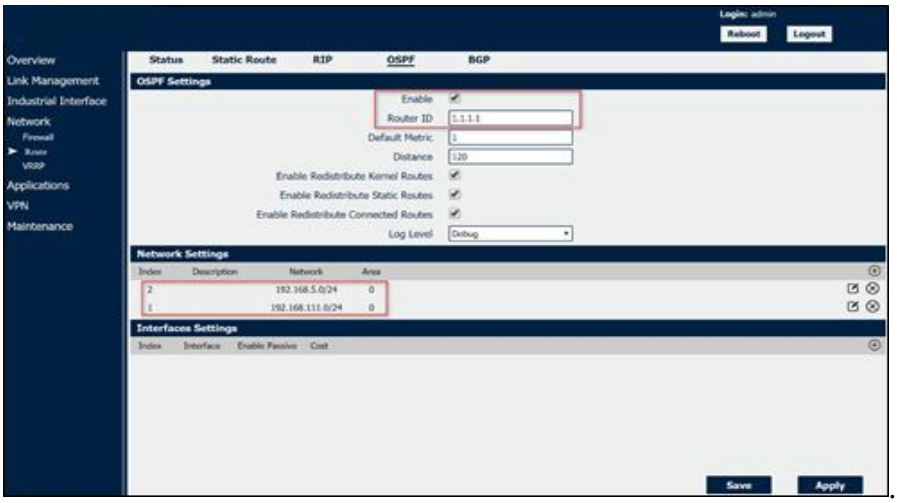
Configuration

CISCO 7200 OSPF Configuration

```
CISCO7200#show running-config
Building configuration...
Current configuration : 1218 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO7200
!
boot-start-marker
boot-end-marker
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
  hidekeys
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.200 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router ospf 110
 router-id 2.2.2.2
 log-adjacency-changes
 network 192.168.10.0 0.0.0.255 area 0
 network 192.168.111.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
end
CISCO7200
```

6944 OSPF Configuration

Step1. Go to **Network>Route>OSPF**, enable OSPF and configure OSPF as below picture.



Step 2: Click Save>Apply.

Checking the Routing Tables

Check the Cisco 7200 routing table for reference

```
CISCO7200#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.111.0/24 is directly connected, FastEthernet0/0
C    192.168.10.0/24 is directly connected, Loopback0
O    192.168.5.0/24 [110/11] via 192.168.111.199, 00:17:32, FastEthernet0/0
CISCO7200#
```

Check the 6944 routing table for reference.

Testing

Ping from CISCO to the 6944 Test Successful

```
CISCO7200#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!.!
Success rate is 80 percent (4/5), round-trip min/avg/max = 4/344/988 ms
CISCO7200#
```

9.4. Dynamic Routing Using BGP

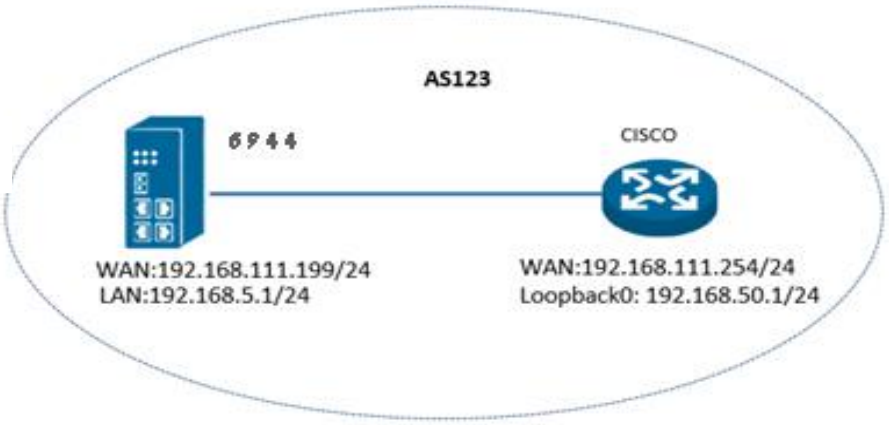
Introduction

This document shows how to configure BGP on a 6944 to a Cisco 7200 Router

In order to run dynamic routing and OSPF on the 6944 its necessary to ensure you have the dynamic routing software installed. This can be obtained from Case Communications and is shown below

Release Date	Doc Version	Firmware Version	Additional Software	Change Description
2018/12/12	V1.1	V1.1.4 (0c0c09fa)	Dynamic Routing Software V1.0.1 642848	First release

Topology



Configuration

Cisco 7200 Configuration.

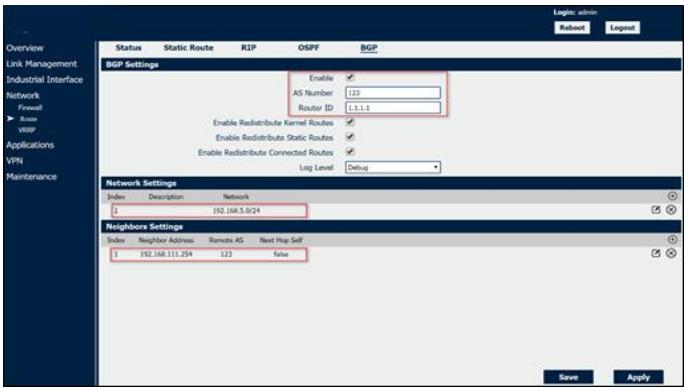
```
CISCO7200#show run
Building configuration...
Current configuration : 1293 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO7200
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
  hidekeys
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
#
```

Configuration Continued

```
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router bgp 123
 no synchronization
 bgp router-id 3.3.3.3
 bgp log-neighbor-changes
 network 192.168.50.0
 neighbor 192.168.111.199 remote-as 123
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
end
CISCO7200
```

6944 BGP Configuration

Step 1: Go to **Network>Route>BGP**, enable BGP and configure BGP as below picture.



Step 2: Click Save>Apply.

Checking the Routing Tables

Step 1: Check the 7200 Routing Table for reference

```
CISCO7200#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

C    192.168.111.0/24 is directly connected, FastEthernet0/0
B    192.168.5.0/24 [200/0] via 192.168.111.199, 00:09:17
C    192.168.50.0/24 is directly connected, Loopback0
CISCO7200#
```

Step 2: Checking the 6944 Routing table for reference

Testing

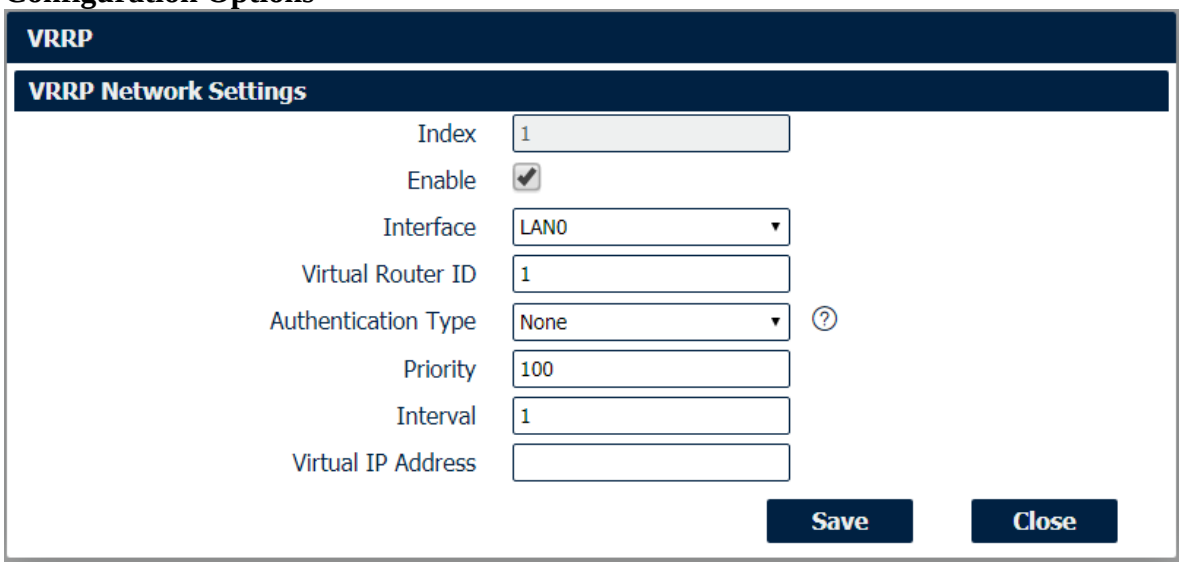
Ping from the CISCO router to the 6944 Router: Test Successful

```
CISCO7200#ping 192.168.5.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/18/36 ms
CISCO7200#
```

10 V.R.R.P

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. The VRRP router that has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup. If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

Configuration Options



Network->VRRP

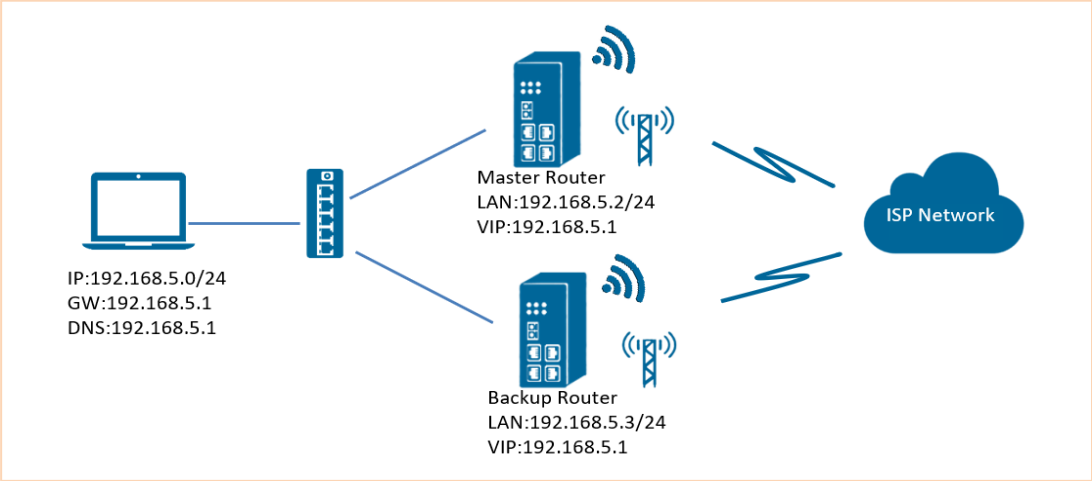
- **Enable**
  Select this box will enable VRRP.
- **Interface**
  Select the interface of Virtual Router.
- **Virtual Router ID**
  User-defined Virtual Router ID. Range: 1-255.
- **Authentication Type**
  Select the authentication type for VRRP.
- **Priority**
  Enter the VRRP priority range is 1-254 (a bigger number indicates a higher priority).
- **Interval**
  Heartbeat package transmission time interval between routers in the virtual IP group. Range: 1-255.
- **Virtual IP Address**
  Enter the virtual IP address of virtual gateway.

10.1. Configuring VRRP between Two 6944 Routers

Overview

This part of the manual shows how to configure VRRP between two 6944 Routers

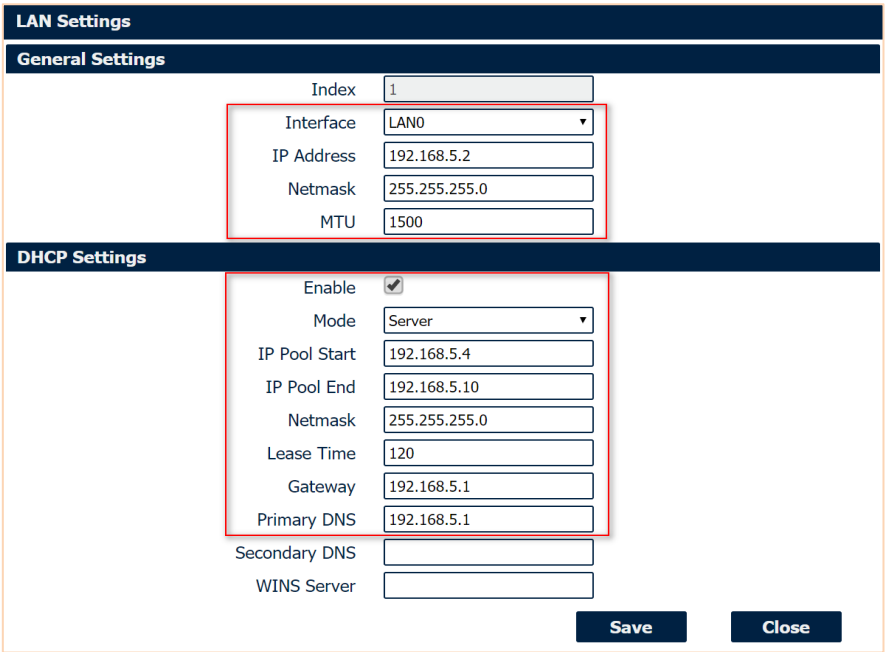
Testing Topology



- The 6944 runs as VRRP Master router and Backup router and connects to the Internet via a SIM card.
- A PC connects to the Internet via the Master 6944 router under normal running Conditions.
- If the Master 6944 router goes down, the PC will switchover to Backup 6944 router to access the Internet.
- When the Master router comes up, then PC will switch back to Master 6944 router to access the Internet.

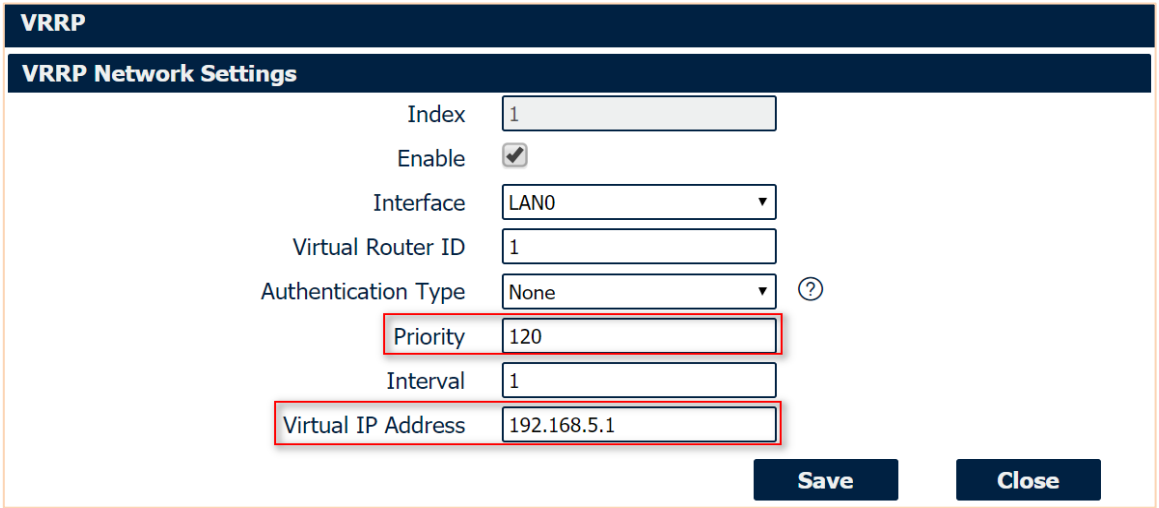
<u>Configuring the Master 6944</u>

Step 1: Go to Link **Management>Ethernet>LAN**, to specify the LAN information as shown below.



Step 2: Go to **Network>VRRP>VRRP**, Click the VRRP Edit button, as shown below.

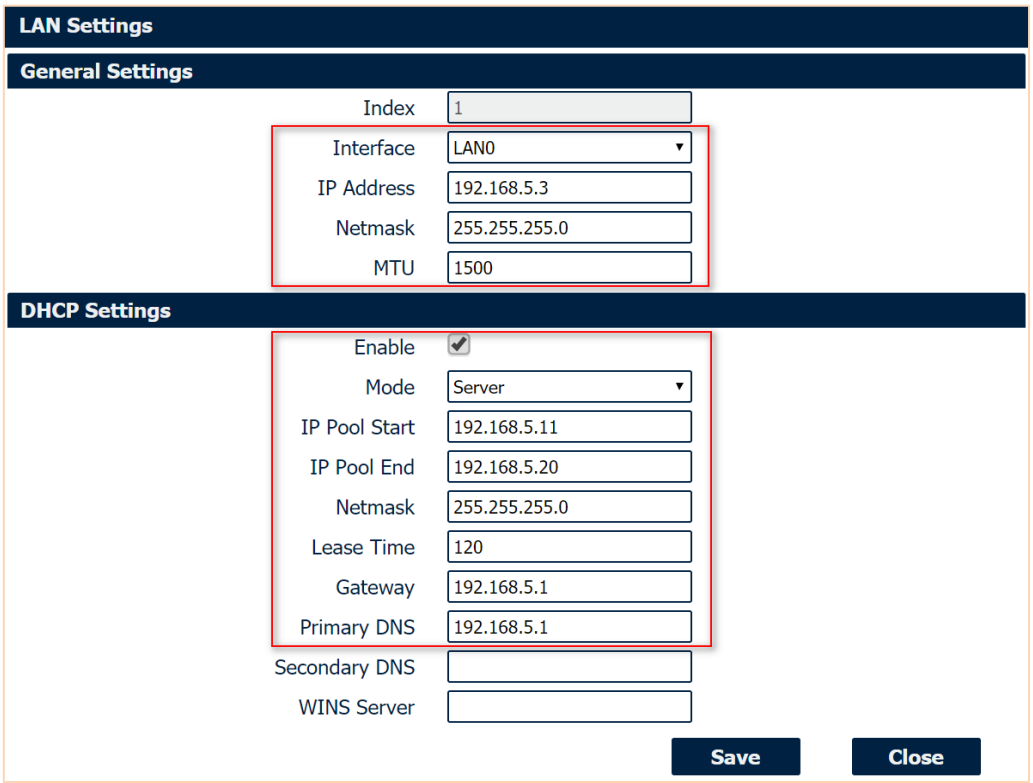
Step 3: Configure VRRP as shown below:



Step 4: Click Save>Apply.

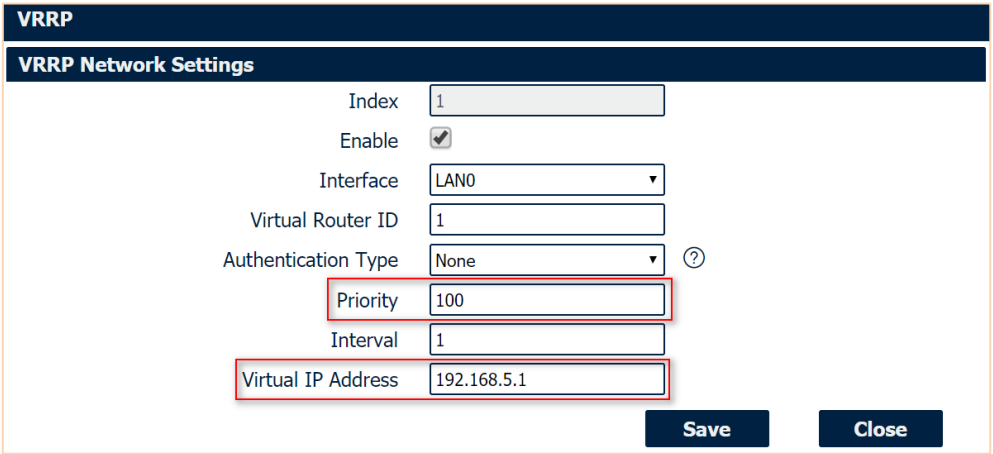
<u>Configuring the Backup Router</u>

Step 1. Go to Link **Management>Ethernet>LAN**, to specify the LAN information like below.



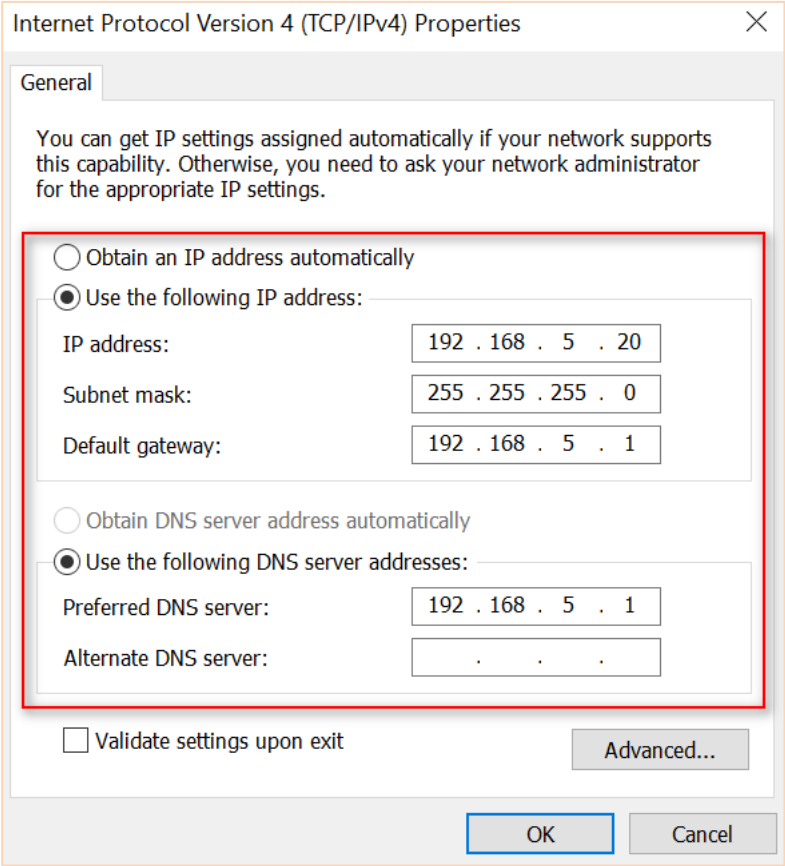
Step 2: Go to **Network>VRRP>VRRP**, Click the VRRP Edit button as shown below:

Step 3: Configure VRRP on the 6944 as shown below. Then Click Save> Apply



PC Configuration

Step 1: Enable DHCP on your PC or configure the static IP on PC as shown here:



Testing VRRP between 6944's

Now the PCs communicate with the Internet via Master Router;

Administrator Command prompt – tracert 8.8.8.8

C:\Users \ Administrator ping 8.8.8.8
Pinging 8.8.8.8. with 32 bytes of data
Reply from 8.8.8.8: bytes=32 time-16ms TTL=120
Reply from 8.8.8.8: bytes=32 time-16ms TTL=120
Reply from 8.8.8.8: bytes=32 time-16ms TTL=120

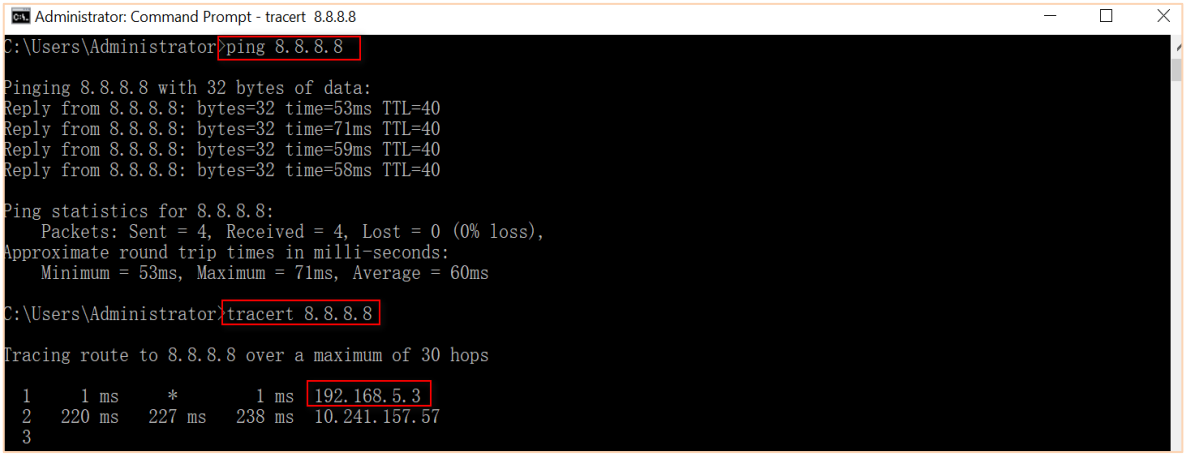
Ping statistics for 8.8.8.8:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 51ms, Maximum = 98ms, Average = 64ms

C:\Users \ Administrator tracert 8.8.8.8

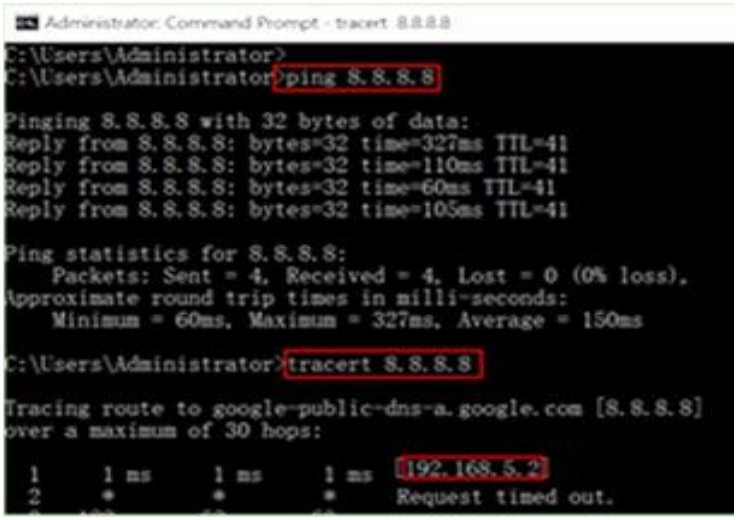
Tracing route to google public dns-a-google.com (8.8.8.8)
Over a maximum of 30 hops

1. 1ms 1ms 1ms (192.168.5.2)
2. 85ms 89ms 130ms logon (172.29.5.17)

Remove the Ethernet cable between the 6944 Master router and Switch, the PC will access the Internet via the 6944 Backup Router.



Put the Ethernet cable back, the PC will access the Internet via the 6944 Master Router.



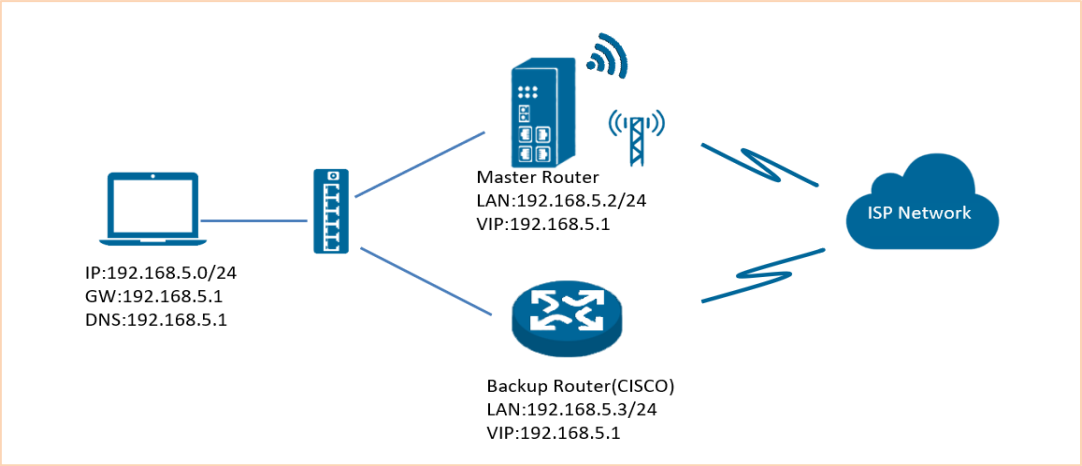
Test Successful

10.2. Configuring VRRP Between 6944 and Cisco Routers

Overview

This document contains information regarding configuring VRRP between 6944 Series Routers and a Cisco router

Testing Topology

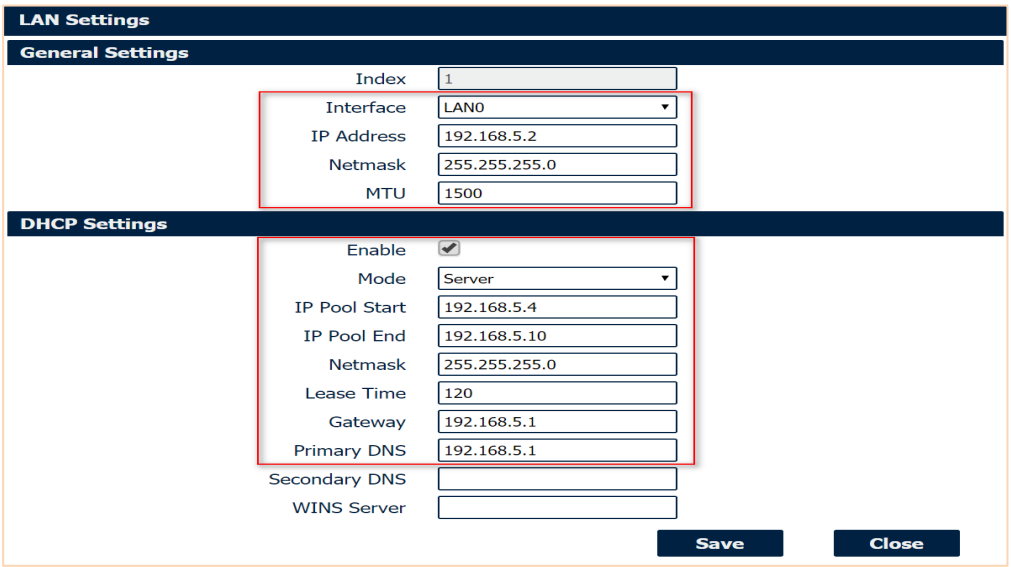


- The 6944 runs as the VRRP Master router and the CISCO router runs as the Backup router.
- A PC communicates with the Internet via the 6944 Master router under normal circumstances.
- If the 6944 master router fails the, PC will switch over to the Cisco Backup router
- If the 6944master router recovers, then PC will switch back to the 6944 master router to access the Internet.

Configuration

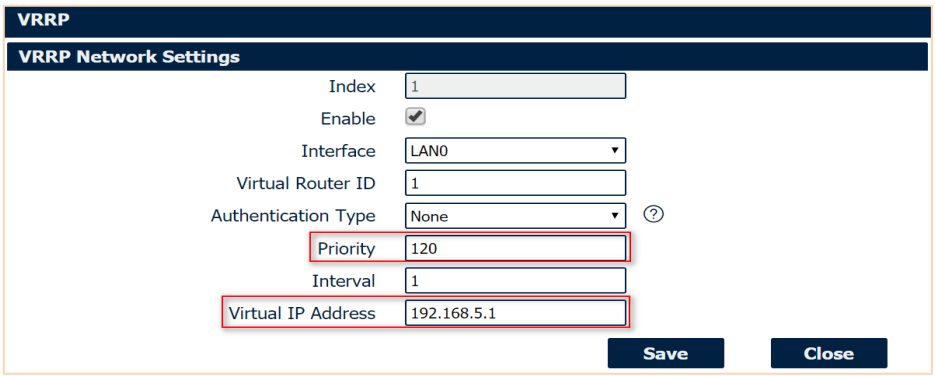
Master Router Configuration

Step 1: Go to Link **Management>Ethernet>LAN**, to specify the LAN configuration as shown below



Step 2: Go to **Network>VRRP>VRRP**, Click the Edit button of VRRP, as shown below:

Step 3: Configure VRRP as shown below and then click Save > Apply



Backup Router (CISCO) Configuration

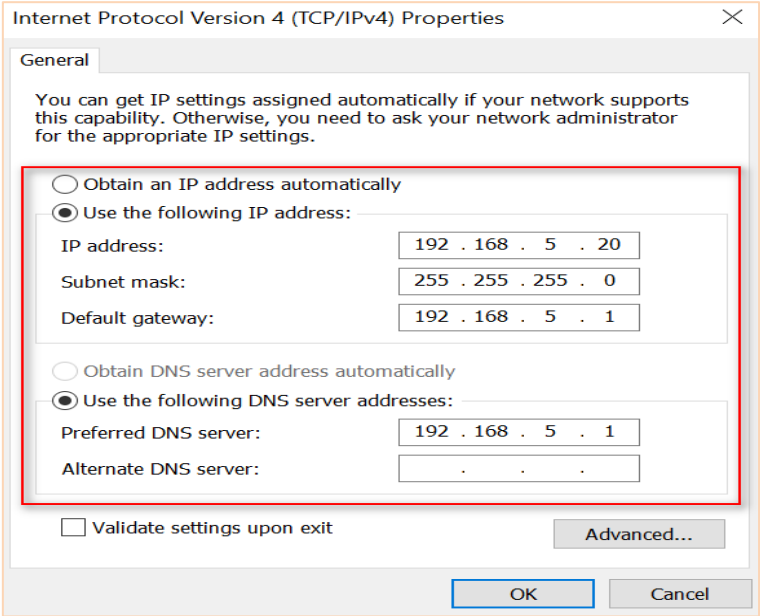
The configuration on CISCO router as shown below

==========

```
cisco2811#
cisco2811#show run
Building configuration...
Current configuration : 3316 bytes
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname cisco2811
!
boot-start-marker
boot-end-marker
!
logging message-counter syslog
enable secret 5
$1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
!
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
multilink bundle-name authenticated
!
username admin password 0 admin
archive
 log config
  hidekeys
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.3 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
 vrrp 1 ip 192.168.5.1
 vrrp 1 timers advertise 10
 vrrp 1 priority 110
 vrrp 1 track 1 decrement 50
!
ip route 0.0.0.0 0.0.0.0 192.168.111.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
snmp-server community public RO
!
ccm-manager fax protocol cisco
!
scheduler allocate 20000 1000
end
cisco2811#
```

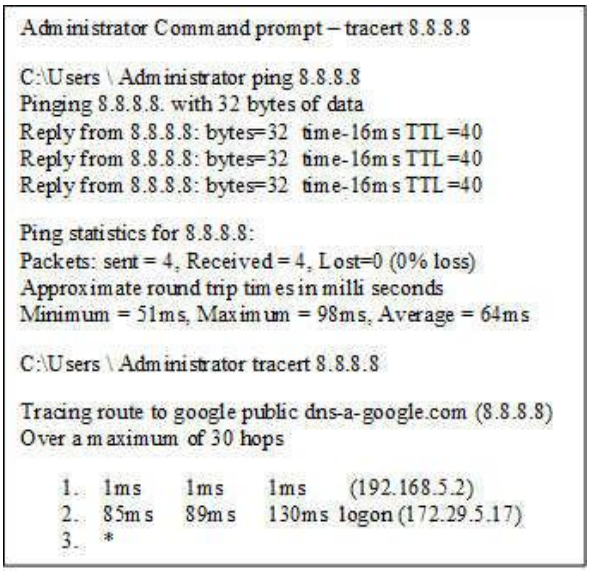
PC Configuration

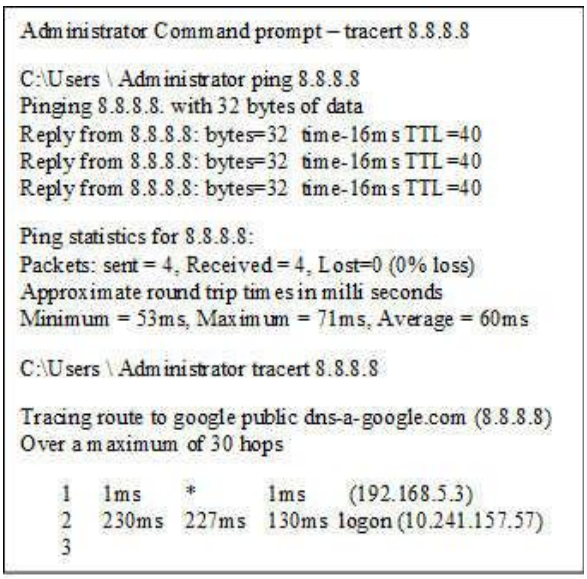
Step 1: Please enable the DHCP on your PC or configure a static IP address as shown below:



Testing VRRP Between the 6944 and Cisco

The PC should be able to communicate with the Internet via the 6944 Master Router.





1. Remove the Ethernet cable between the 6944 master router and the Switch, the PC will access the Internet via the Cisco Backup Router.

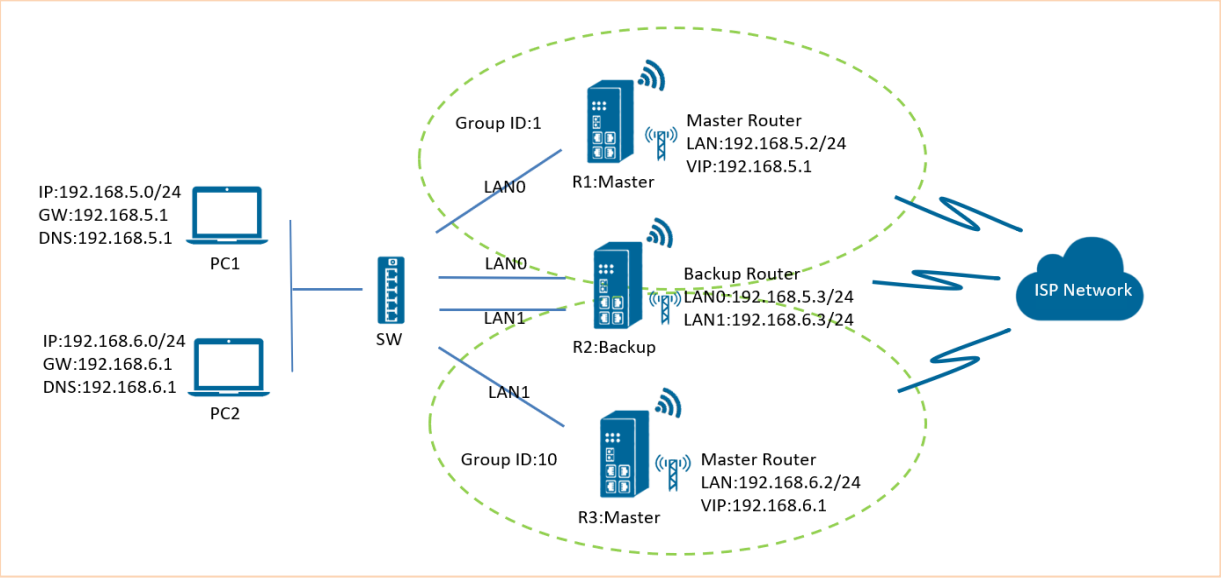
2. Replace the Ethernet cable, the PC will then access the Internet via the 6944 Master Router.

10.3. VRRP Between Multiple 6944 Routers

Overview

This part of the manual shows how to configure VRRP between multiple 6944 Routers

Testing Topology

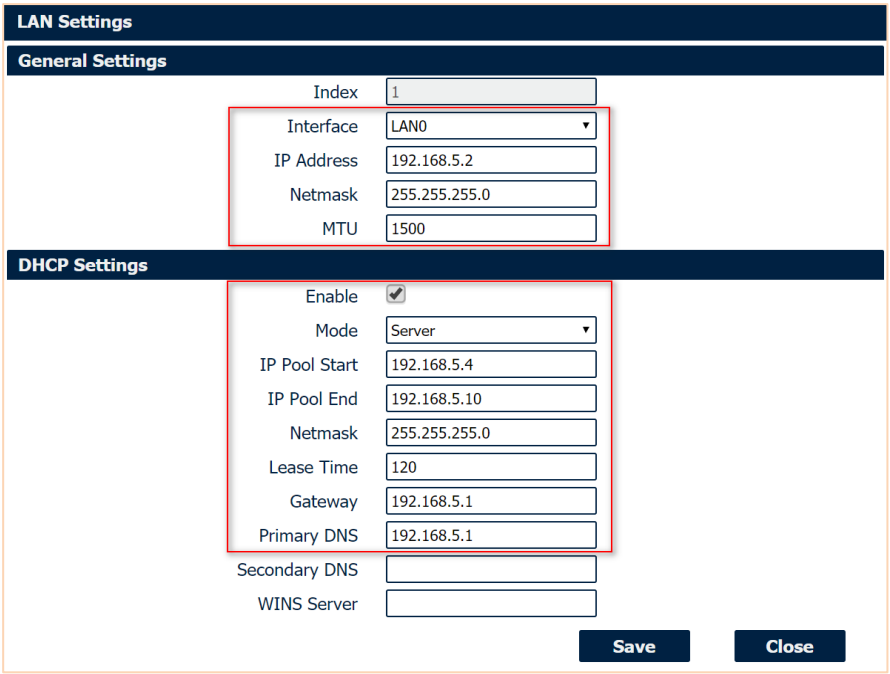


- 6944 R1 and 6944 R3 run as 6944 VRRP Master routers.
- 6944 R2 runs as a VRRP Backup router.
- Both of the 6944 routers connect to Internet with their SIM cards.
- 6944 R1 establishes VRRP with 6944 R2 via its LAN0 interface.
- 6944 R3 establish VRRP with R2 via its LAN1 interface.
- PC1 communicates with Internet via the 6944 R1 Master router under normal operation.
- If the 6944 R1 master router fails, PC1 will switch over to 6944 R2 the Backup router.
- If the 6944 R1 master router recovers, then PC1 will switch back to R1 to access the Internet.
- PC2 communicates with the Internet via the 6944 R3 master router under normal conditions.
- If the 6944 R3 master router fails, then PC2 will switch over to the 6944 R2 Backup router.
- If the 6944 R3 master router recovers, then PC2 will switch back to the 6944 R3 master router to access the Internet

Configuration

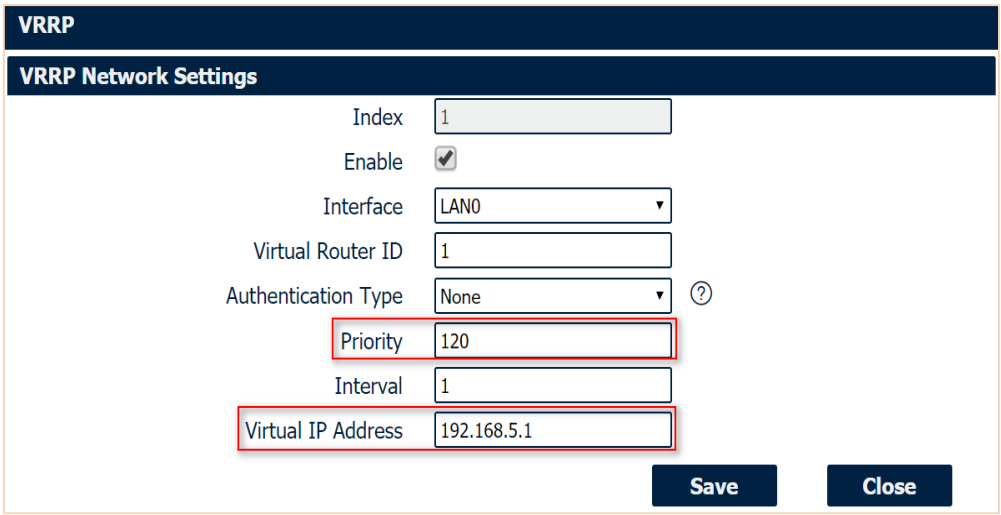
R1 Master Router Configuration

Step 1: Go to Link **Management>Ethernet>LAN**, to specify the LAN0 information like below.



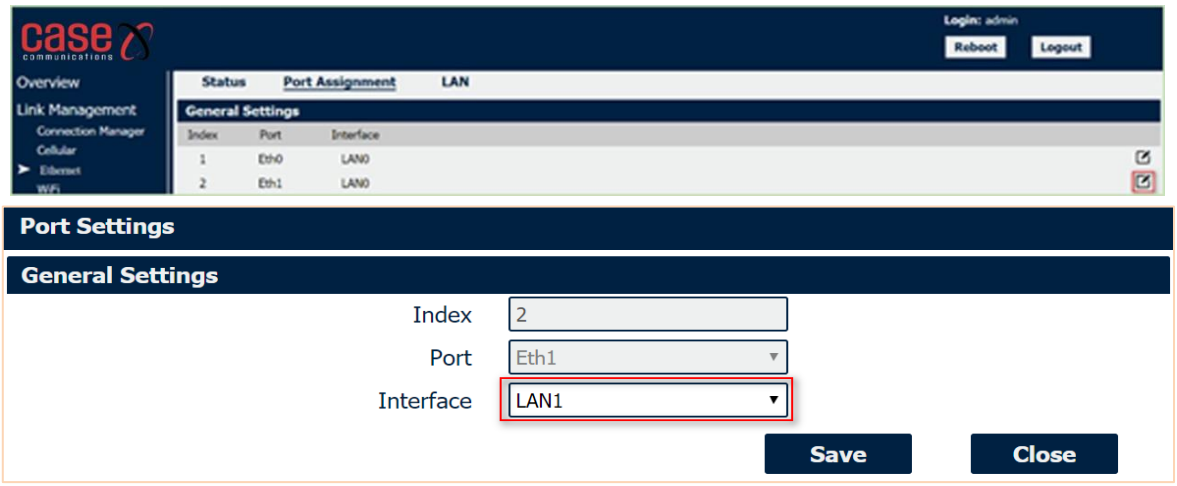
Step 2: Go to **Network>VRRP>VRRP**, Click the Edit button of VRRP, as shown below:

Step 3: Configure VRRP like as shown below then **click Save > Apply**

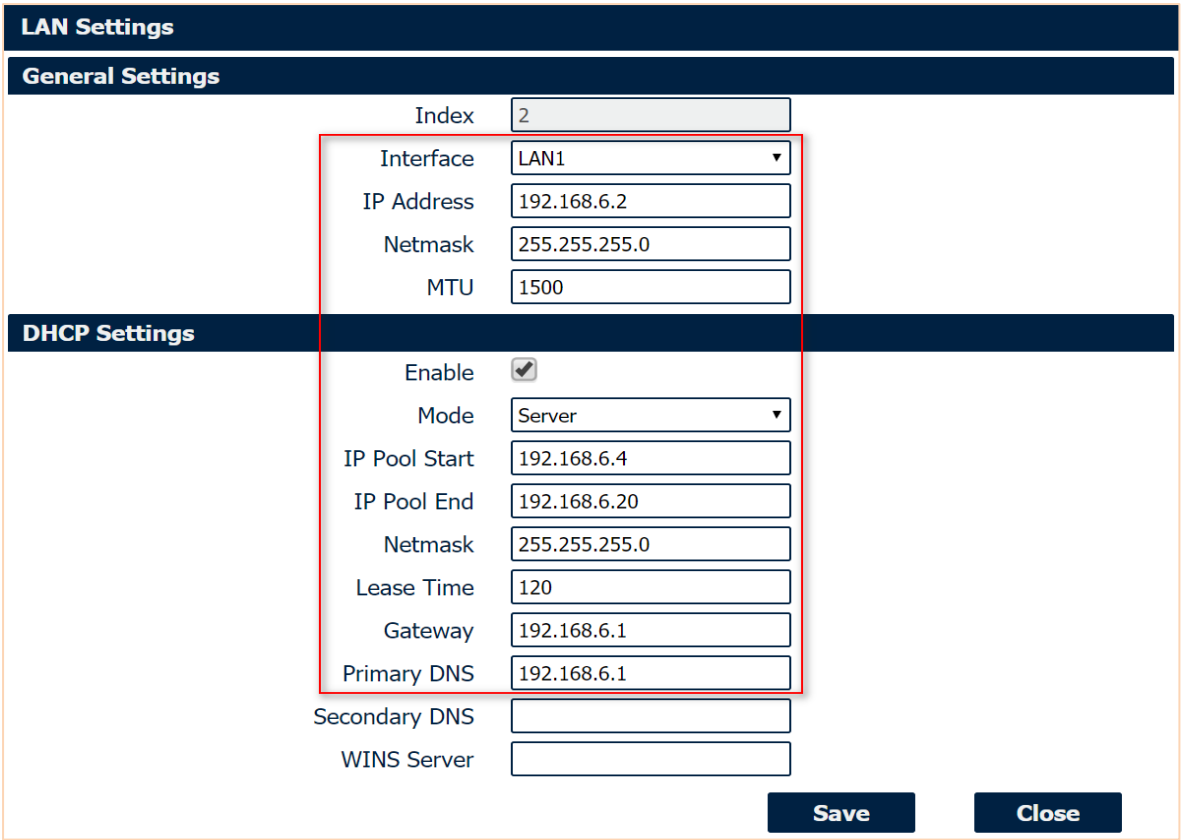


R3 Master Router Configuration

Step 1: Go to Link **Management>Ethernet>Port Assignment**, click Index2 to assign the LAN1 to ETH1, click Save>Apply.



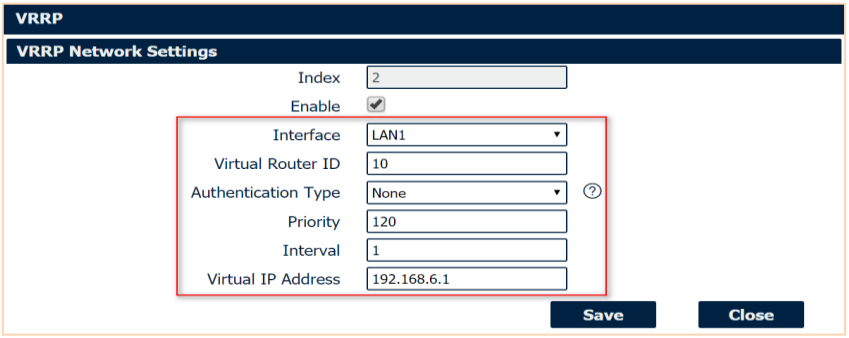
Step 2: Go to Link **Management>Ethernet>LAN**, to specify LAN1 information as shown below.



Step 3: Go to **Network>VRRP>VRRP**, Click the Edit button of VRRP, as shown below

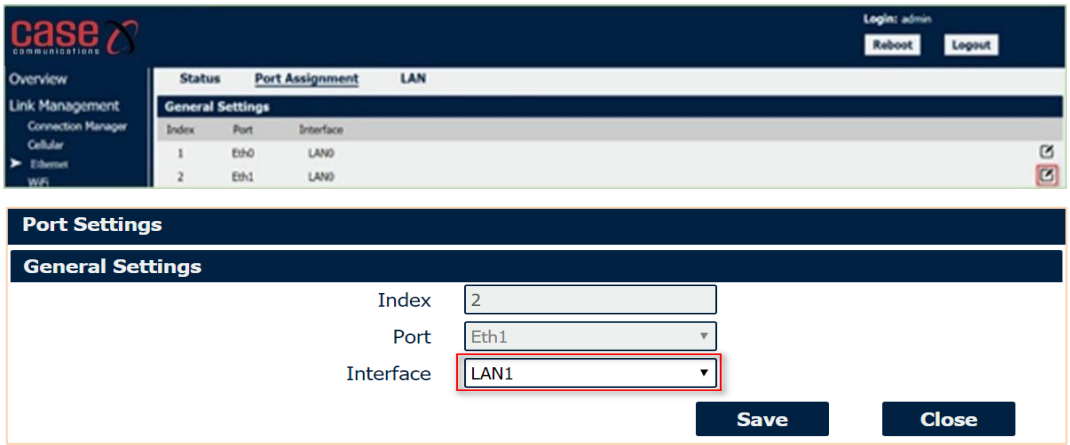
Step 4: Configure VRRP as shown below. Then click Save> Apply

R2 Backup **Router**

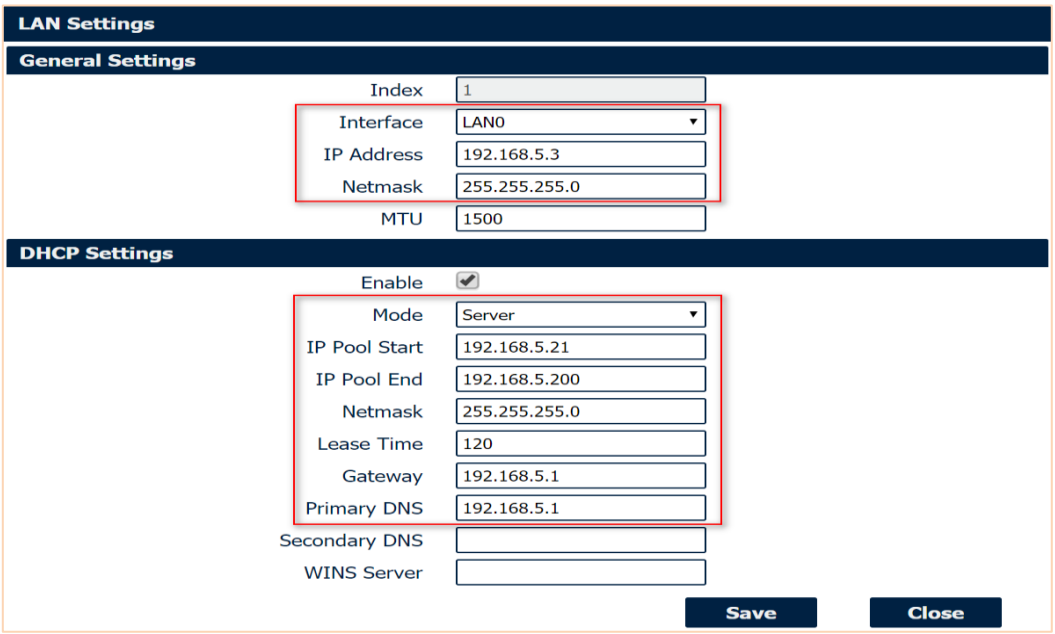


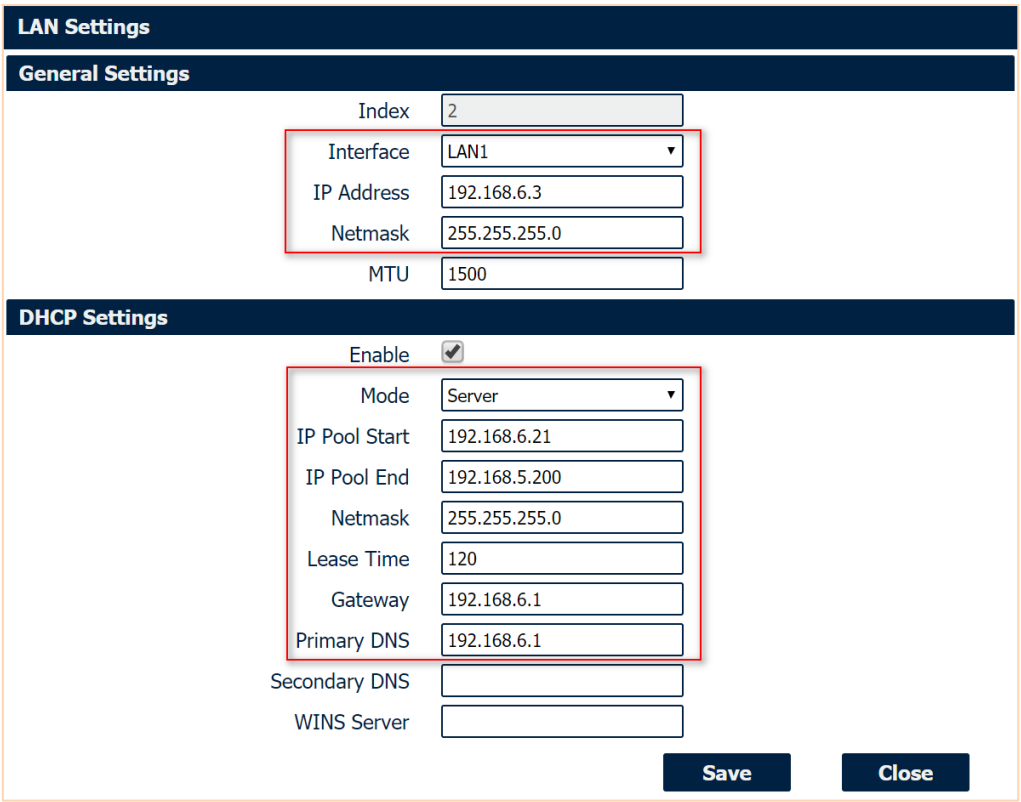
Configuration

Step 1. Go to Link **Management>Ethernet>Port Assignment**, click the Index2 to assign the LAN1 to ETH1, click Save>Apply.



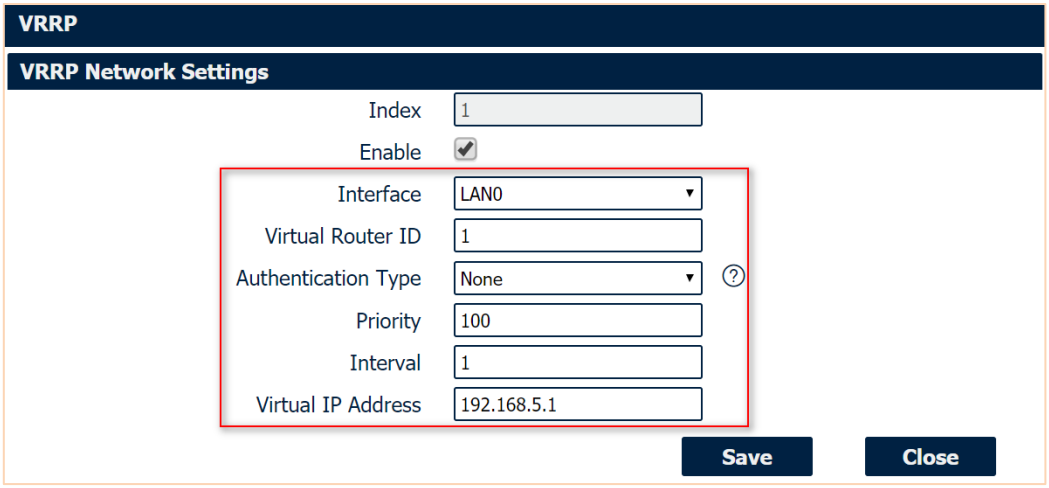
Step 2: Go to Link **Management>Ethernet>LAN**, click the **Edit button** to add one more LAN1 interface, to specify the LAN0 and LAN1 as shown below. Then Click Apply > Save

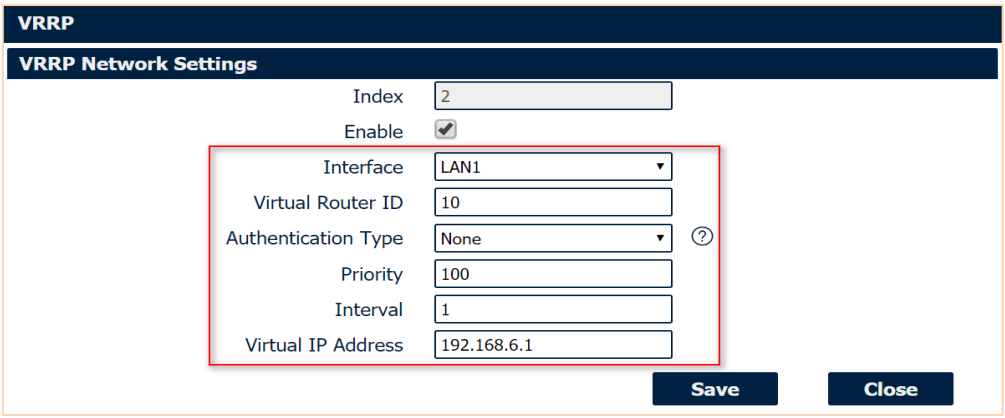




Step 3: Go to **Network>VRRP>VRRP**, Click the **Edit button** on VRRP to add two VRRP's routers as shown below.

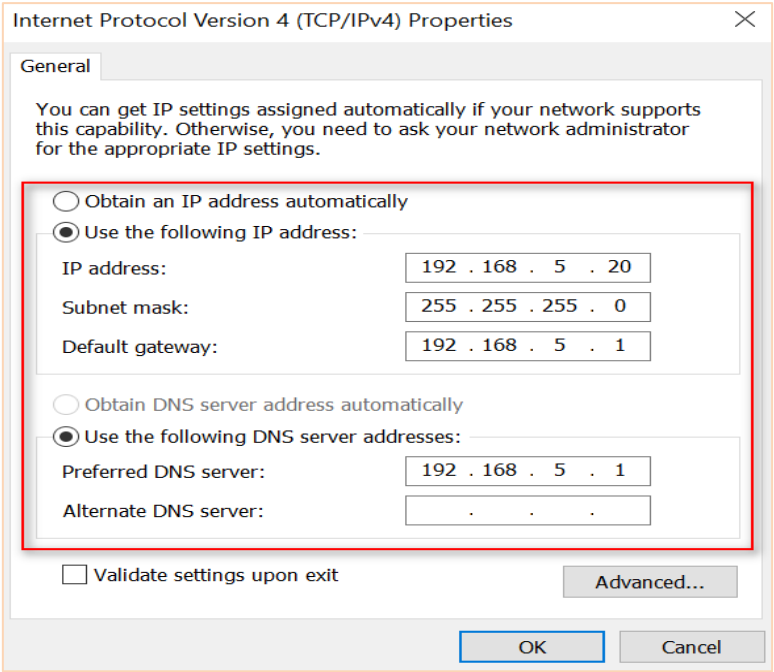
Step 4: Configure VRRP on LAN0 and LAN1 as shown below. Then click Apply > Save



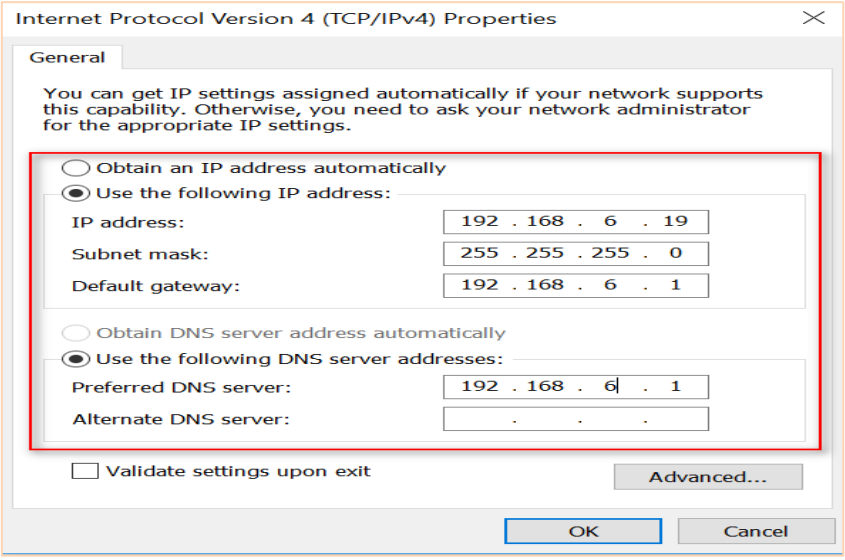


PC Configuration

Step 1: Enable the DHCP on PC1 or configure a static IP address on PC1 as shown below.



Step 2: Enable the DHCP on PC2 or configure a static IP on PC2 as shown below



Testing VRRP between multiple 6944's

Test on PC1: - Make sure PC1 can communicate with Internet via the 6944 Master Router

```
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=98ms TTL=40
Reply from 8.8.8.8: bytes=32 time=52ms TTL=40
Reply from 8.8.8.8: bytes=32 time=58ms TTL=40
Reply from 8.8.8.8: bytes=32 time=51ms TTL=40

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 98ms, Average = 64ms

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  navigateworx.router [192.168.5.2]
  2    85 ms    89 ms   130 ms  bogon [172.29.5.17]
  3     *
```

```
Administrator: Command Prompt - tracert 8.8.8.8
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=53ms TTL=40
Reply from 8.8.8.8: bytes=32 time=71ms TTL=40
Reply from 8.8.8.8: bytes=32 time=59ms TTL=40
Reply from 8.8.8.8: bytes=32 time=58ms TTL=40

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 53ms, Maximum = 71ms, Average = 60ms

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

  1     1 ms     *        1 ms  192.168.5.3
  2   220 ms   227 ms   238 ms  10.241.157.57
  3
```

Remove the Ethernet cable between the 6944 Master router and Switch. PC1 will access the Internet via the 6944 Backup Router

Replace the Ethernet cable, PC1 will access to Internet via the 6944 Master Router.

A Reply to your ping shows the link is successful.

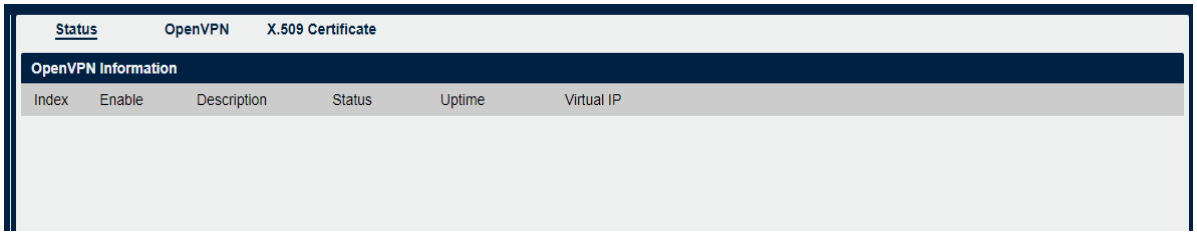
```
Administrator: Command Prompt - tracert 8.8.8.8
C:\Users\Administrator>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=98ms TTL=40
Reply from 8.8.8.8: bytes=32 time=52ms TTL=40
Reply from 8.8.8.8: bytes=32 time=58ms TTL=40
Reply from 8.8.8.8: bytes=32 time=51ms TTL=40

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 51ms, Maximum = 98ms, Average = 64ms

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:

  1     1 ms     1 ms     1 ms  [192.168.5.2]
  2    85 ms    89 ms   130 ms  bogon [172.29.5.17]
  3     *
```

This page left blank intentionally

11 VPN (Virtual Private Networks)

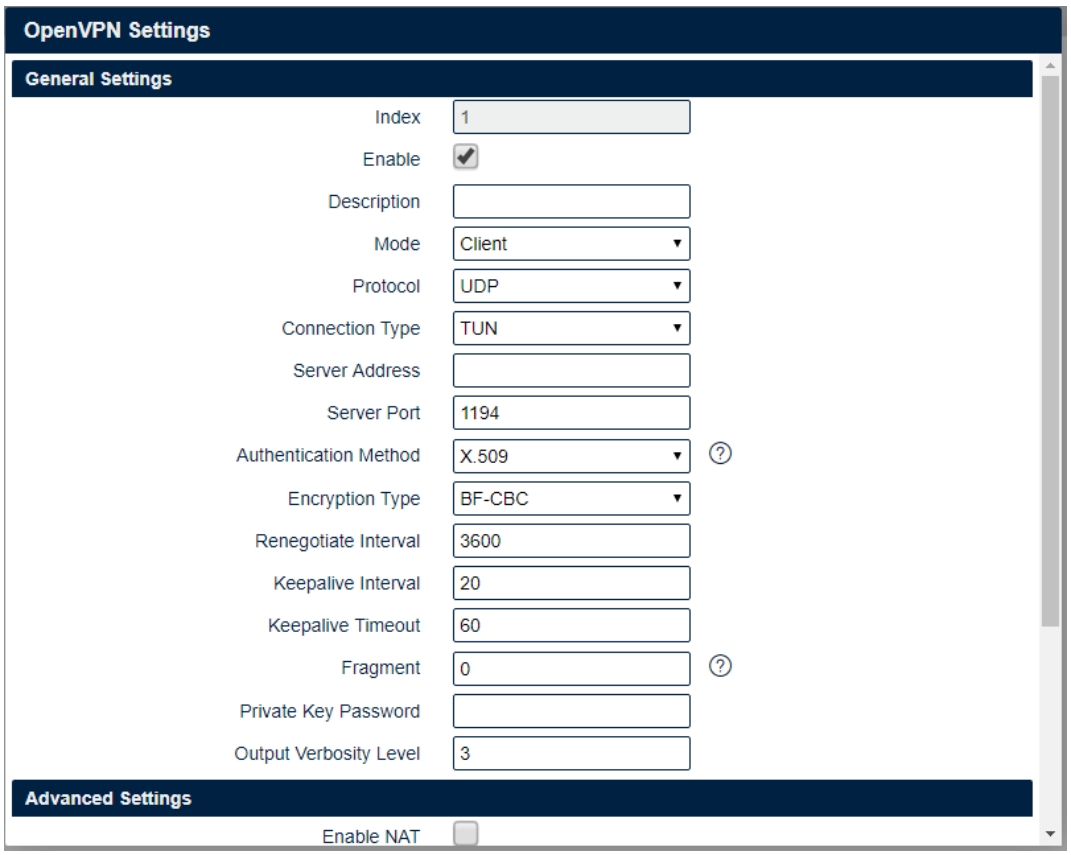
11.1. OpenVPN Introduction

OpenVPN is an 'Open Source' virtual private network (VPN) piece of software that offers a simplified security framework, modular network design, and cross-platform portability.
It can be quite difficult to configure as it has so many variables even different versions of Linux can be configured differently. You can review all OpenVPN connections on the 6944 as shown below.



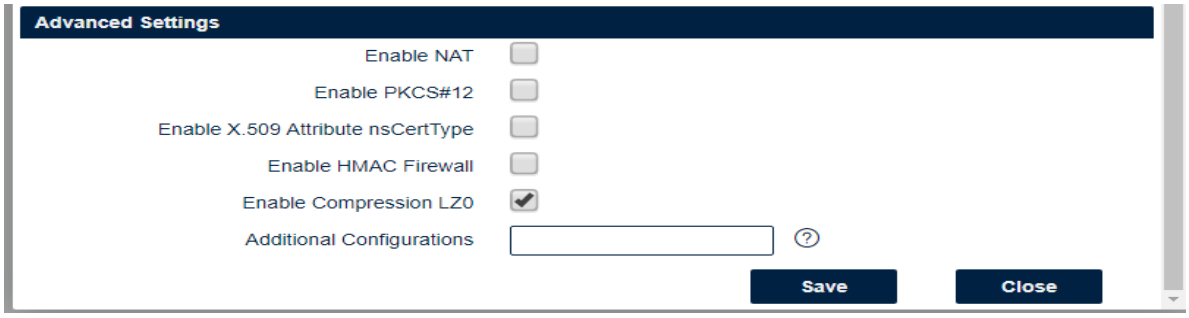
VPN->OpenVPN->Status

- **Enable -** Displays current OpenVPN settings is enable or disable.
- **Status -** Displays the current VPN connection status.
- **Uptime -** Displays the connection time since VPN is established.
- **Virtual IP -** Displays the virtual IP address obtain from remote side.



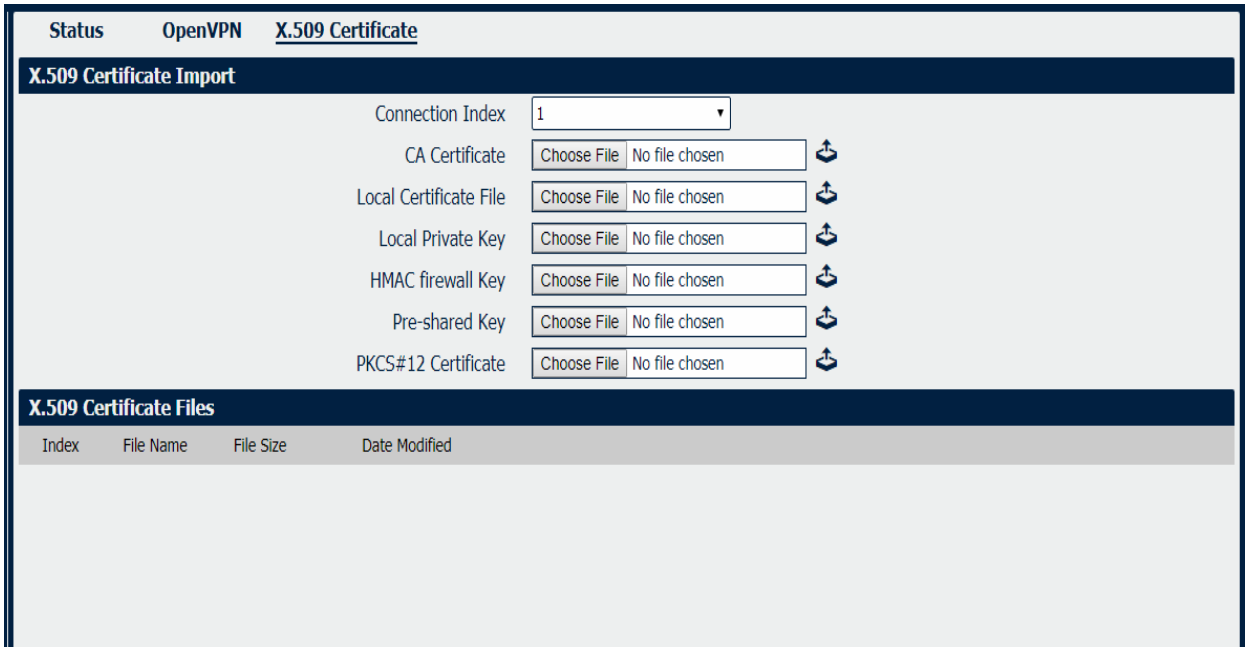
VPN > Open VPN

- **Enable -** Check this box to enable OpenVPN tunnel.
- **Description -** Enter a description for this OpenVPN tunnel.
- **Mode -** Select from “Client” or “P2P”.
- **Protocol -** Select from “UDP” or “TCP Client”.
- **Connection Type -** Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is that a TUN device is a point-to-point virtual device on network while a TAP device is a virtual device on Ethernet.
- **Server Address -** Enter the IP address or domain of remote server.
- **Server Port -** Enter the negotiate port on OpenVPN server.
- **Authentication Method -** Select from "X.509", "Pre-shared", "Password", and "X.509 And Password".
- **Encryption Type -** Select from "BF-CBC", "DES-CBC", "DES-EDE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC".
- **Username -** Enter the username for authentication when selection from “Password” or “X.509 And Password”.
- **Local IP Address -** Enter the local virtual IP address when select “P2P” mode.
- **Password -** Enter the password for authentication when selection from “Password” or “X.509 And Password”
- **Local IP Address -** Enter the local virtual IP address when select “P2P” mode.
- **Remote IP Address -** Enter the remote virtual IP address when select “P2P” mode
- **Local Netmask -** Enter the local netmask when select “TAP” connection type
- **Renegotiate Interval -** Enter the renegotiate interval if connection is failed.
- **Keepalive Interval -** Enter the keepalive interval to check the tunnel is active or not.
- **Keepalive Timeout -** Enter the keepalive timeout, once connection is failed it will trigger the OpenVPN reconnect
- **Fragment -** Enter the fragment size, 0 means disable
- **Private Key Password -** Enter the private key password for authentication when selection from “X.509” or “X.509 And Password”.
- **Output Verbosity Level -** Enter the level of the output log and values.



VPN->OpenVPN->Advanced Settings

- **Enable NAT -** Check this box to enable NAT, the source IP of host behind router will be disguised before accessing the remote end.
- **Enable PKCS#12 -** It is an exchange of digital certificate encryption standard, used to describe personal identity information.
- **Enable X.509 Attribute nsCertType -** Require that peer certificate was signed with an explicit nsCertType designation of “server”.
- **Enable Compression LZO -** Compress the data.
- **Additional Configurations -** Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.



VPN->OpenVPN->X.509 Certificate

- **Connection Index**

Displays the current connection index for OpenVPN channel.

- **CA Certificate**

Import CA certificate file.

- **Local Certificate File**

Import Local Certificate file.

- **Local Private Key**

Import Local Private Key file.

- **HMAC Firewall Key**

Import HMAC Firewall Key file.

- **Pre-shared Key**

Import the pre-shared key file.

- **PKCS#12 Certificate**

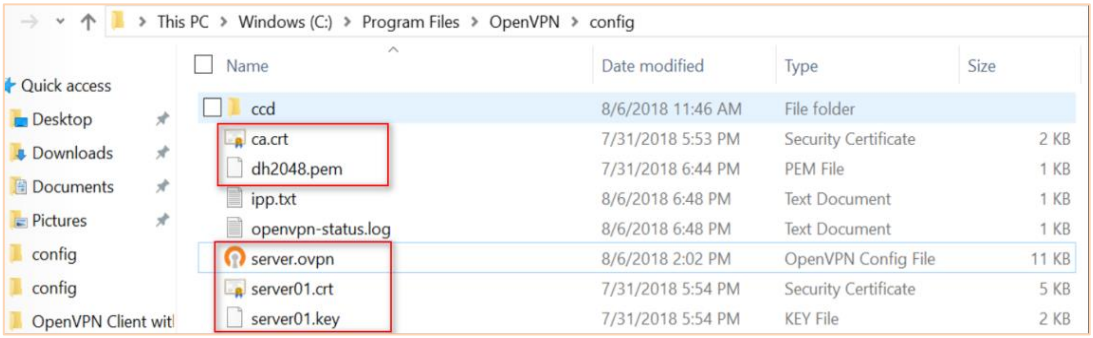
Import PKCS#12 Certificate

11.2. Example Configuration VPN a 6944 Client and PC running as an Open VPN Server

This section of the manual shows how to configure a 6944 running an Open VPN to a PC

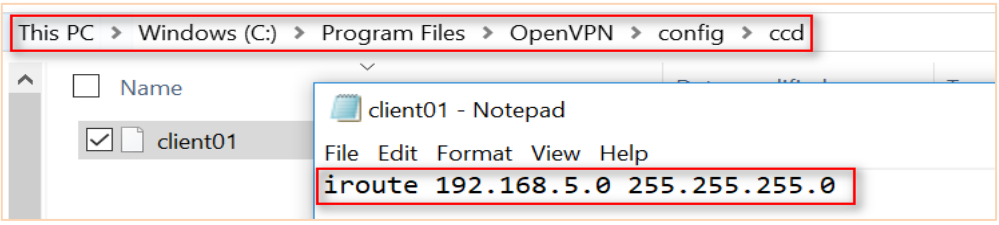
Configuration

Step 1 - Install OpenVPN software on your PC and copy the related certifications and configuration as shown below:



Note**: a) Download OpenVPN software from: **https://openvpn.net/
*b) Install and run OpenVPN software with **administrator authority**.*

***Step 2** -* Add a "ccd" folder, and create a new notepad, rename it without suffix, configure it like below:



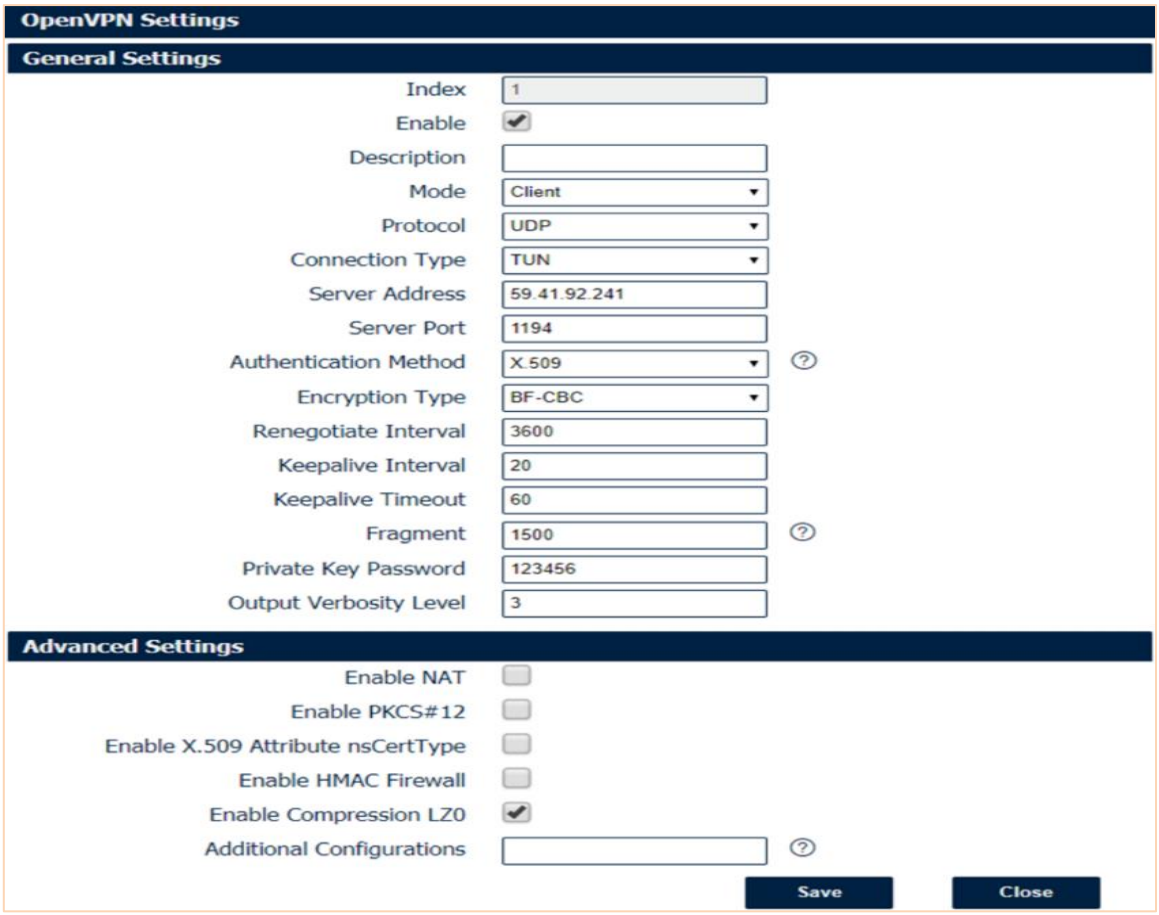
***Note**: client01 is the common name; 192.168.5.0/24 is the subnet behind the Case Communications 6944*

Step 3 - Configure the **server.ovpn** as shown below:

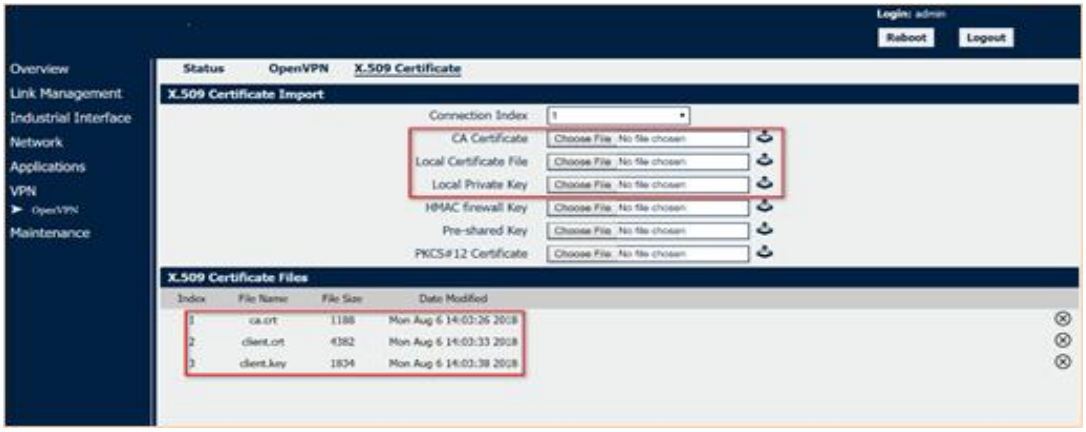
```
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key  # This file should be kept
secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

<u>Configure the Client</u>

Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. **Click Save > Apply**



Step 5 - Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, **Click Apply.**



Step 6 - The Route has connected to the OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

Step 7 - Check the Routing Table on the OpenVPN Server for reference.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.10.1   192.168.10.10     291
          0.0.0.0          0.0.0.0      192.168.111.1  192.168.111.19    291
         10.8.0.0    255.255.255.0          10.8.0.2        10.8.0.1      35
         10.8.0.0  255.255.255.252          On-link         10.8.0.1     291
         10.8.0.1  255.255.255.255          On-link         10.8.0.1     291
         10.8.0.3  255.255.255.255          On-link         10.8.0.1     291
        127.0.0.0        255.0.0.0          On-link        127.0.0.1     331
        127.0.0.1  255.255.255.255          On-link        127.0.0.1     331
  127.255.255.255  255.255.255.255          On-link        127.0.0.1     331
      192.168.5.0    255.255.255.0          10.8.0.2        10.8.0.1      35
     192.168.10.0    255.255.255.0          On-link      192.168.10.10    291
    192.168.10.10  255.255.255.255          On-link      192.168.10.10    291
   192.168.10.255  255.255.255.255          On-link      192.168.10.10    291
```

Step 8 – Check the Routing Table on the OpenVPN Client for reference.

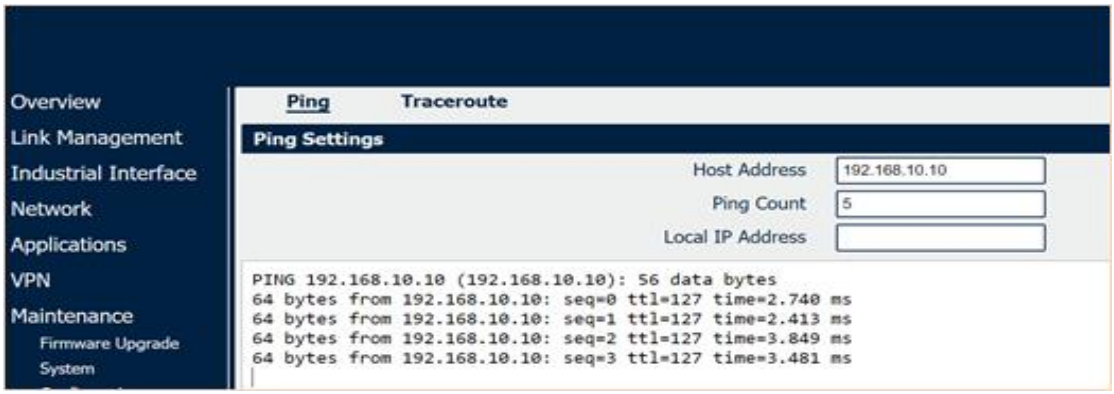
Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.10.0	255.255.255.0	10.8.0.5	tun1
6	192.168.111.0	255.255.255.0	0.0.0.0	wan

Step 9 Testing - Enable CMD and Ping from the OpenVPN Server to the OpenVPN client LAN.

```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=2ms TTL=64
Reply from 192.168.5.1: bytes=32 time=8ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

Step 10 - Go to **Maintenance>Debug Tool>Ping** and Ping from the OpenVPN client to the OpenVPN Server.

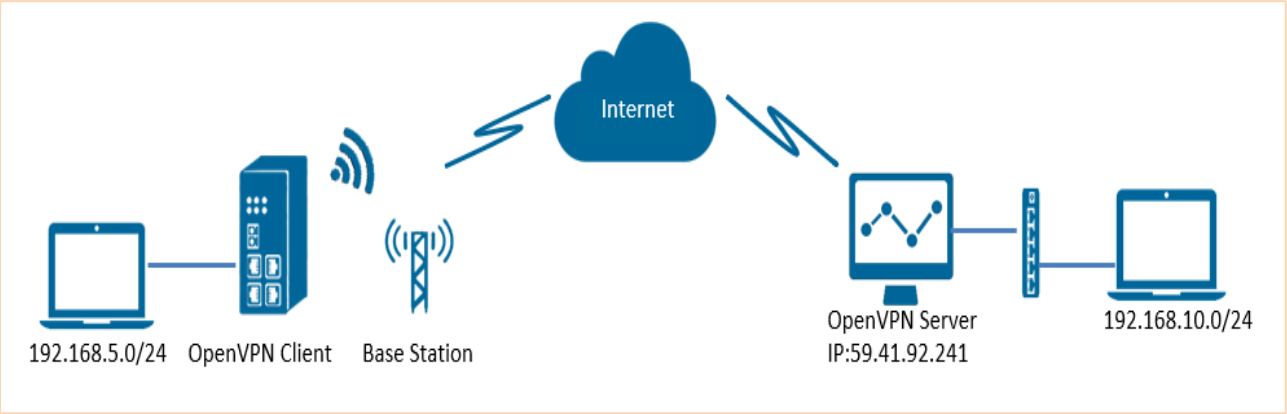


11.3. AN006 – 6944 Open VPN Client with X.509 Certificate.

Introduction

This section contains information regarding the configuration and use of an Open VPN Client using an X.509 certificate.

Testing Topology



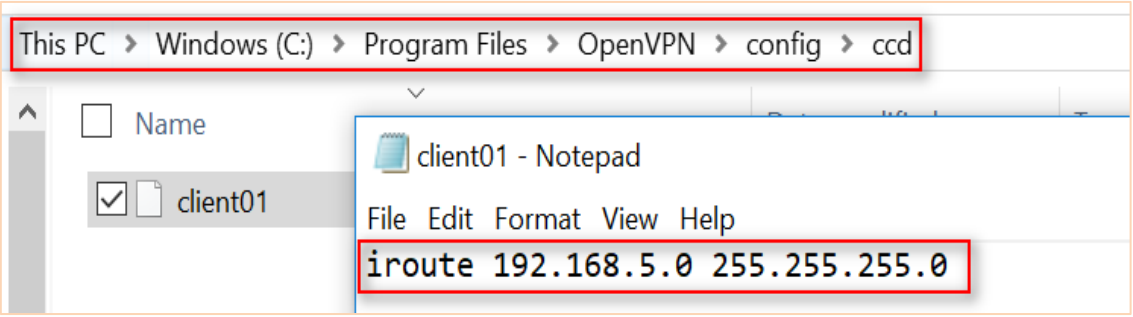
Configuration

Server Configuration

Step 1: Install OpenVPN software on the PC and copy the relevant certificates and configure the PC as shown below:

PC > Windows (C) > Program Files > Open VPN > Config	
ccd	File Folder
Ca.crt	Security Certificate
Dh2048.pem	PEM File
Ipp.txt	Text Document
Openvpn-status.log	Text document
Server.ovpn	Open VPN Config File
Server01.crt	Security Certificate
Server01.key	Key File

Step 2: Add a "ccd" folder, and create a new notepad, rename it without suffix, configure as shown below



***Note**: client01 is the common name; 192.168.5.0/24 is the subnet behind the 6944*

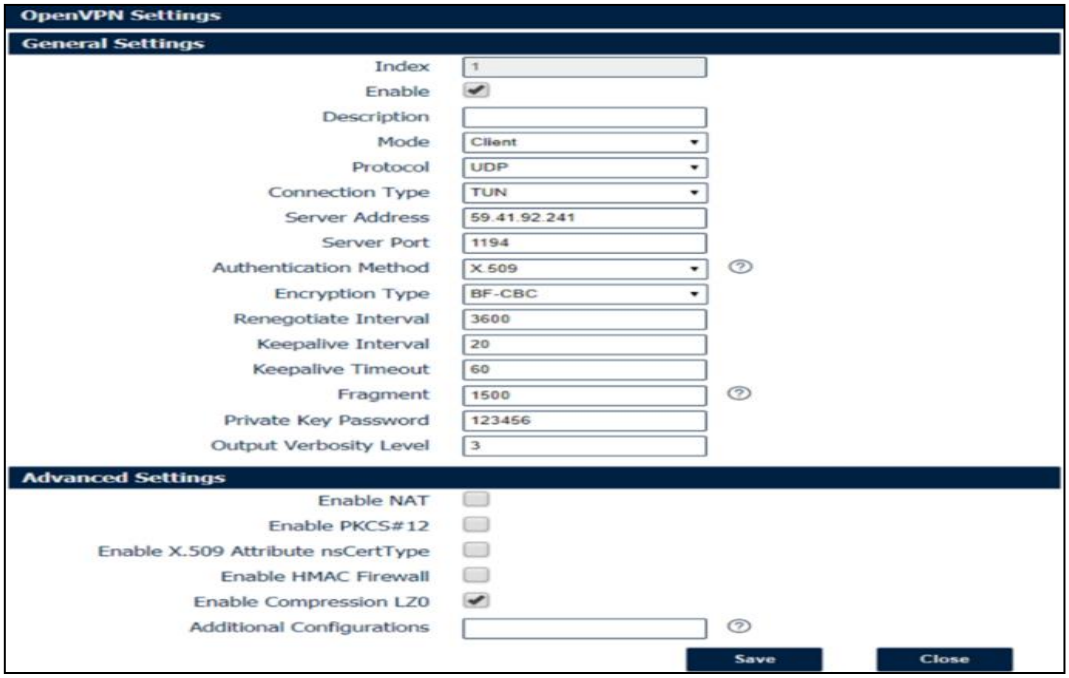
Step3: The configuration for the Server should be as shown below **server.ovpn**

==========

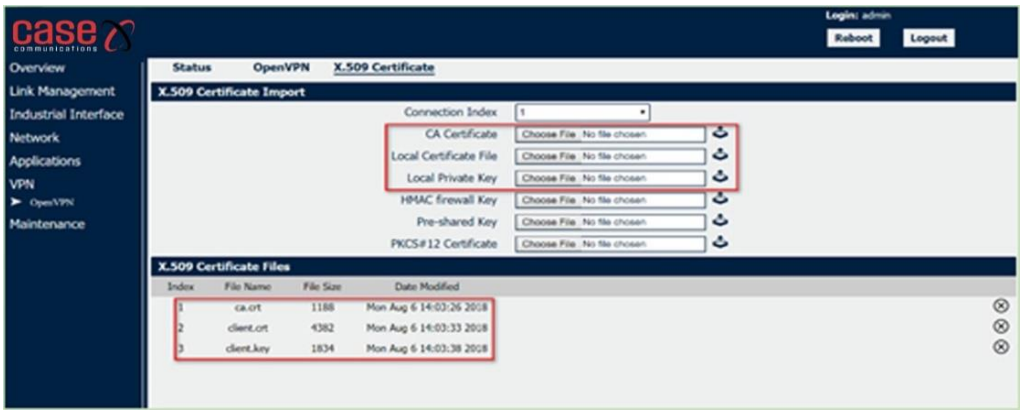
```
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key  # This file should be kept
secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

6944 Client Configuration

Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure the OpenVPN as shown below. **Click Save> Apply**

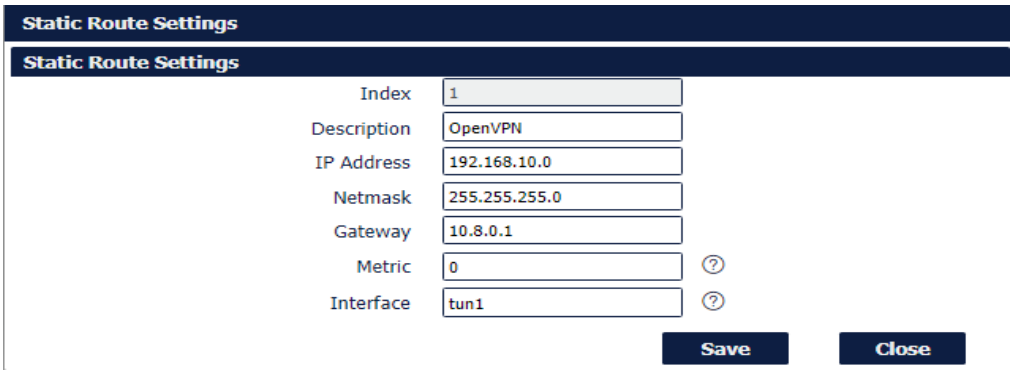


. **Step 2**: Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, Click Apply.



Step 3: To ensure the Route has connected to the OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

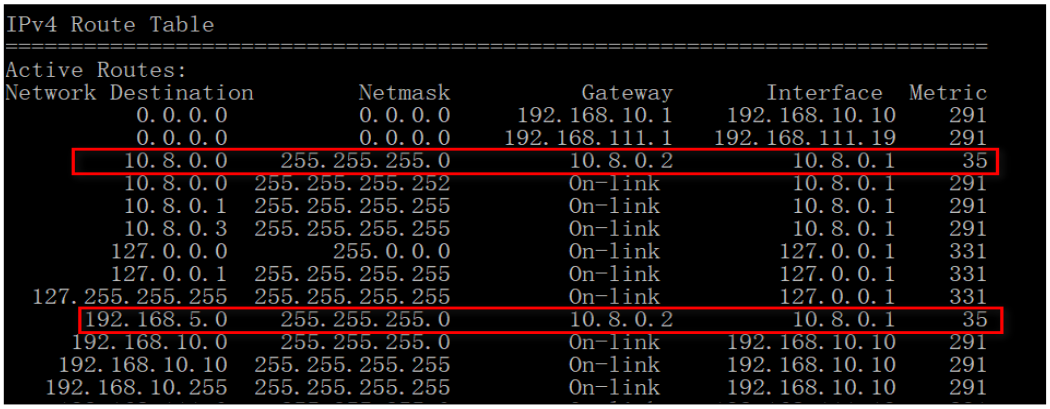
Step 4: Go to **Network>Route>Static Route** and add a new Static Route.



Step 5: Enter the remote IP range details and set the Gateway as the virtual IP address, that the OpenVPN server will assign itself, in this case 10.8.0.1. Set the Interface as tun1 which is the OpenVPN tunnel. **Click Save>Apply**

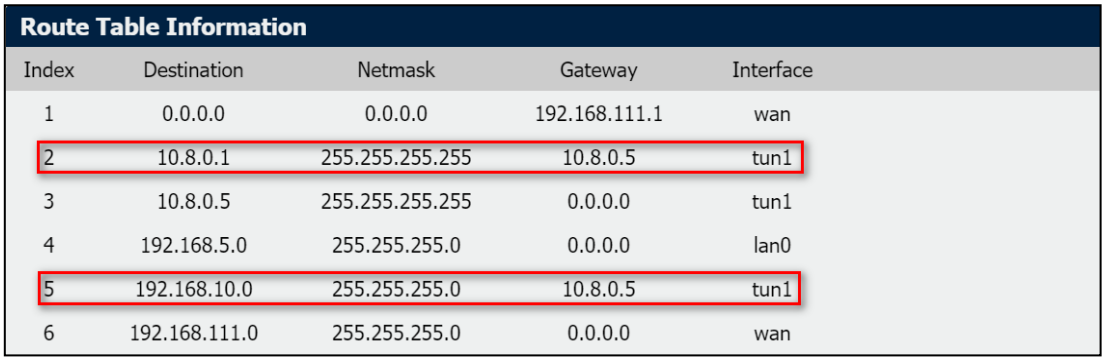
<u>Checking the Routing Table on the Open VPN Server</u>

Check the Routing Table on the OpenVPN Server for reference.



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.10.1    192.168.10.10     291
          0.0.0.0          0.0.0.0      192.168.111.1   192.168.111.19    291
         10.8.0.0      255.255.255.0        10.8.0.2        10.8.0.1       35
         10.8.0.0    255.255.255.252        On-link         10.8.0.1      291
         10.8.0.1    255.255.255.255        On-link         10.8.0.1      291
         10.8.0.3    255.255.255.255        On-link         10.8.0.1      291
        127.0.0.0        255.0.0.0          On-link        127.0.0.1      331
        127.0.0.1    255.255.255.255        On-link        127.0.0.1      331
  127.255.255.255    255.255.255.255        On-link        127.0.0.1      331
      192.168.5.0      255.255.255.0        10.8.0.2        10.8.0.1       35
     192.168.10.0      255.255.255.0        On-link      192.168.10.10     291
    192.168.10.10    255.255.255.255        On-link      192.168.10.10     291
   192.168.10.255    255.255.255.255        On-link      192.168.10.10     291
```

<u>Check the Routing Table on the OpenVPN Client for reference.</u>

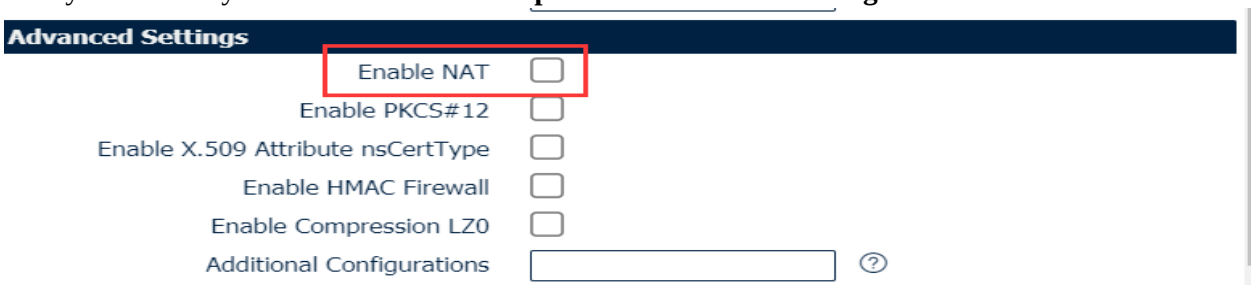


Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.10.0	255.255.255.0	10.8.0.5	tun1
6	192.168.111.0	255.255.255.0	0.0.0.0	wan

Setting NAT

It may be necessary to enable **NAT VPN>OpenVPN>Advanced Settings**

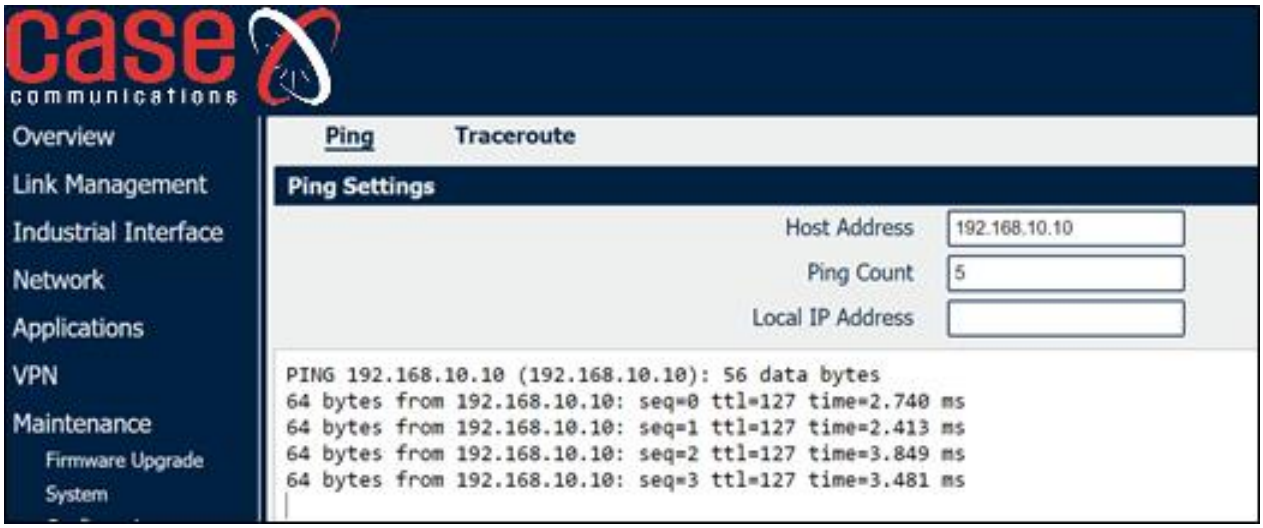


Testing the VPN

Step 1: Enable CMD and Ping from OpenVPN Server to LAN of OpenVPN client.

```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1 with 32 bytes of data:
Reply from 192.168.5.1: bytes=32 time=2ms TTL=64
Reply from 192.168.5.1: bytes=32 time=8ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64
Reply from 192.168.5.1: bytes=32 time=3ms TTL=64

Ping statistics for 192.168.5.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 8ms, Average = 4ms
```

Step 2: Go to **Maintenance>Debug Tool>Ping** and Ping from the OpenVPN client to OpenVPN Server.



Test successful.

11.4. AN016- How to generate the certificates for OpenVPN on Windows OS.

Introduction

This document contains information on how to generate certificates for an Open VPN for Windows.

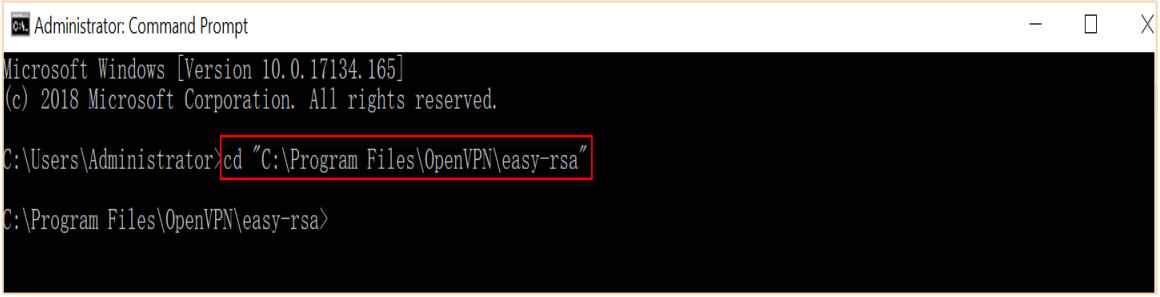
Configuration

Installing OpenVPN Software

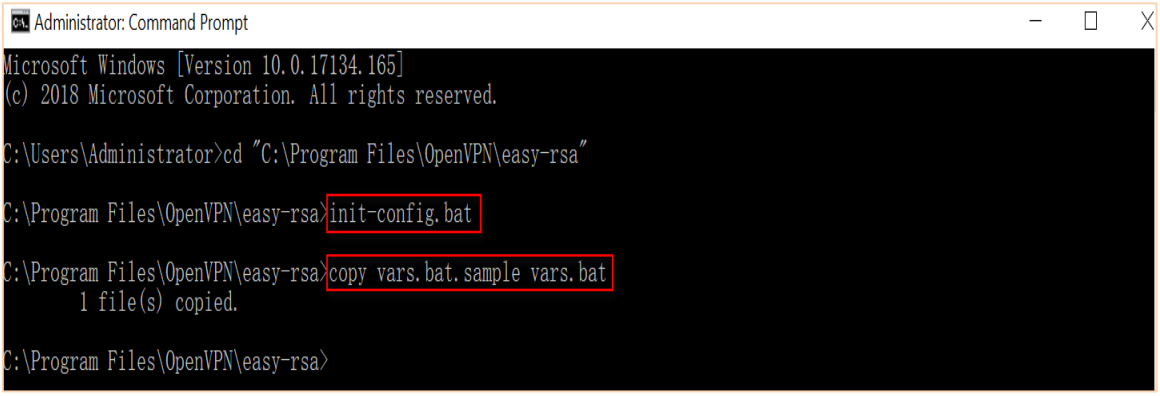
Please download OpenVPN software and install onto a Windows PC: **http://openvpn.net/index.php**

Generating Certificates

Step 1 Open the command line with Administrator authority on Windows and **cd** to **C:\Program Files\OpenVPN\easy-rsa**



Step 2 - Run the **init-config.bat** to copy configuration files to **vars.bat** (this command would overwrite the previous vars.bat and openssl.cnf files).



Step 3 - Edit the **vars.bat** and set the KEY_COUNTRY, KEY_PROVINCE, KEY_CITY, KEY_ORG, KEY_EMAIL parameters and so on.

Note: The parameters enter without any space between them.

```
@echo off
rem Edit this variable to point to
rem the openssl.cnf file included
rem with easy-rsa.

rem Automatically set PATH to openssl.exe
FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"

rem Alternatively define the PATH to openssl.exe manually
rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"

set HOME=%ProgramFiles%\OpenVPN\easy-rsa
set KEY_CONFIG=openssl-1.0.0.cnf

rem Edit this variable to point to
rem your soon-to-be-created key
rem directory.
rem
rem WARNING: clean-all will do
rem a rm -rf on this directory
rem so make sure you define
rem it correctly!
set KEY_DIR=keys

rem Increase this if you
rem are paranoid.  This will slow
rem down TLS negotiation performance
rem as well as the one-time DH parms
rem generation process.
set DH_KEY_SIZE=2048

rem Private key size
set KEY_SIZE=4096

rem These are the default values for fields
rem which will be placed in the certificate.
rem Change these to reflect your site.
rem Don't leave any of these parms blank.

set KEY_COUNTRY=CN
set KEY_PROVINCE=GD
set KEY_CITY=Guangzhou
set KEY_ORG=OpenVPN
set KEY_EMAIL=mail@navigateworx.domain
set KEY_CN=OpenVPN
set KEY_NAME=OpenVPN
set KEY_OU=OpenVPN
set PKCS11_MODULE_PATH=changeme
set PKCS11_PIN=1234
```

Step 4 - Run the following commands to initialise the environment.

```
Administrator: Command Prompt

C:\Program Files\OpenVPN\easy-rsa>vars.bat

C:\Program Files\OpenVPN\easy-rsa>clean-all.bat
        1 file(s) copied.
        1 file(s) copied.

C:\Program Files\OpenVPN\easy-rsa>
```

Step 5 - The command (**build-ca.bat**) will build the certificate authority(CA) certificate and the private key by invoking the interactive openssl command.

```
Administrator: Command Prompt

C:\Program Files\OpenVPN\easy-rsa>build-ca.bat
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.............................++
.....................................................++
writing new private key to 'keys\ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [UK]:
State or Province Name (full name) [HW]:
Locality Name (eg, city) [ Wycombe ]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:CA
Name [OpenVPN]:
Email Address [    support@case.uk.com    ]:

C:\Program Files\OpenVPN\easy-rsa>
```

Note: *In the above sequence, most of queried parameters were defaulted to the values set in the vars.bat file. The only parameter which must be explicitly entered is the Common Name.*

Step 6. Generate a certificate and private key for the server by using **build-key-server.bat server01**. Enter **server01** when the Common Name is queried.

```
Select Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>build-key-server.bat server01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.....................................++
.....................................................++
writing new private key to 'keys\server01.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ ]:
State or Province Name (full name) [ ]:
Locality Name (eg, city) [ ]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:server01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :PRINTABLE:'Bucks
localityName          :PRINTABLE:'Wycombe '
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'server01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'  mail.support@case.Domain '
Certificate is to be certified until Sep 11 11:54:49 2028 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

***Note**: **server01** in "**build-key-server.bat server01**" is the file name of the certificate(the name of public key and private key).*

Step 7 - Generate a certificate and a private key for client by using **build-key-pass.bat client01.**

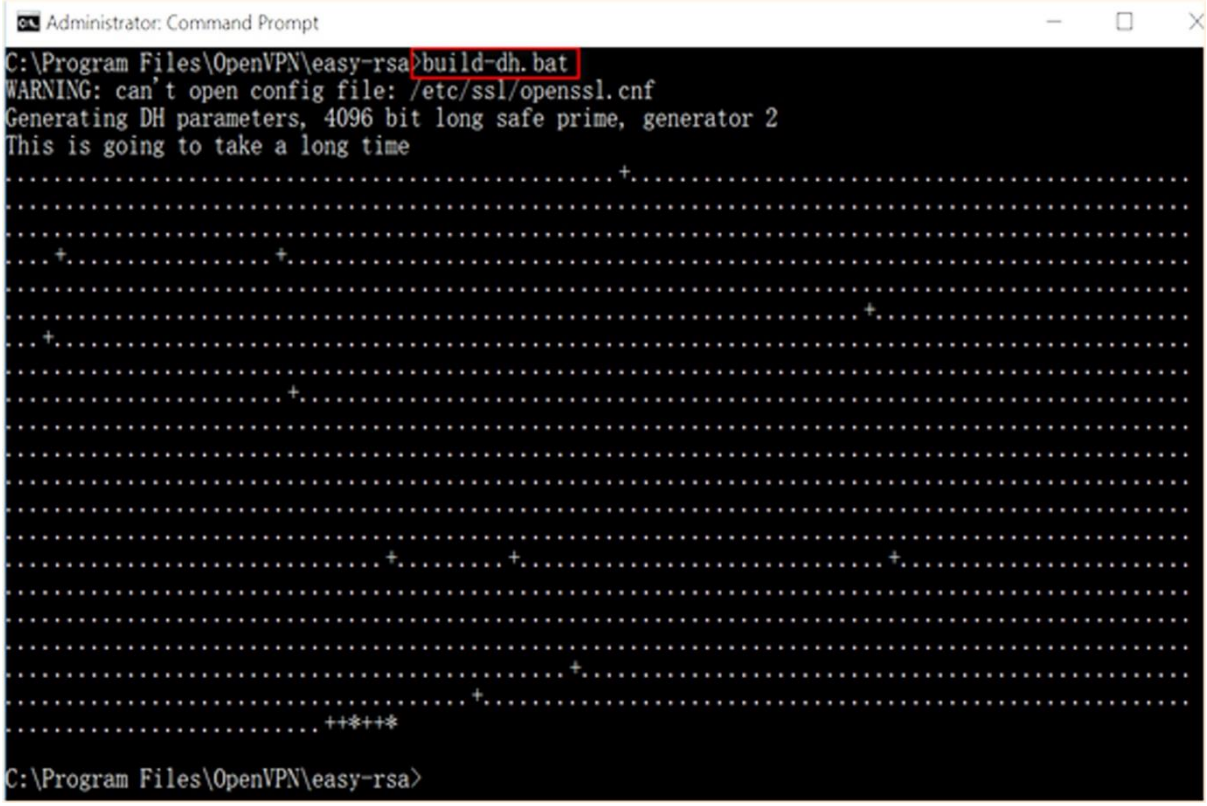
Note: that **pass phrase** is generated as following. It will be necessary to help the key authentication in the OpenVPN client setting. Enter **client01** when the Common Name is queried.

```
Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa>build-key-pass.bat client01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
...............++
.......................++
writing new private key to 'keys\client01.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [ ]:
State or Province Name (full name) [ ]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]:client01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'UK'
stateOrProvinceName   :PRINTABLE:'Bucks
localityName          :PRINTABLE:'High Wycombe
organizationName      :PRINTABLE:'OpenVPN'
organizationalUnitName:PRINTABLE:'OpenVPN'
commonName            :PRINTABLE:'client01'
name                  :PRINTABLE:'OpenVPN'
emailAddress          :IA5STRING:'support@case.uk.com
Certificate is to be certified until Sep 11 12:05:27 2028 GMT (3650 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated

C:\Program Files\OpenVPN\easy-rsa>
```

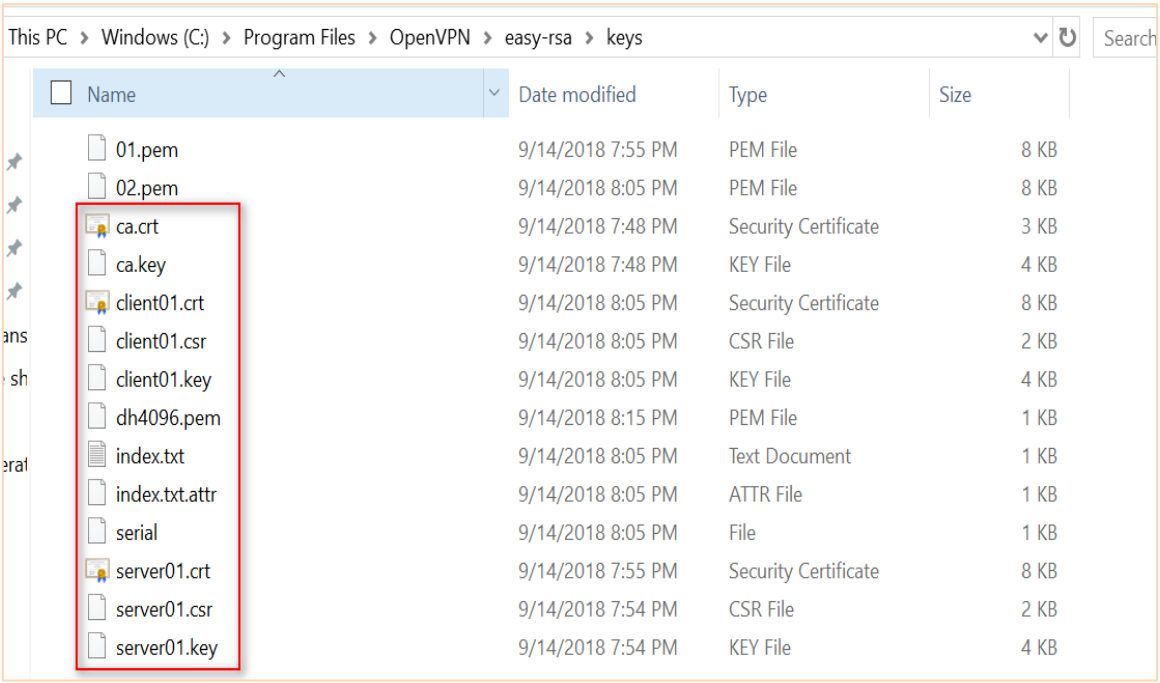
Setup Private Key Password

***Note**: client01 in "**build-key-pass.bat client01**" is the file name of the certificate(the name of public key and private key). **Always use a unique common name for each client**.*

Step 8. Generate Diffie Hellman parameters.



Step 9. Make sure Certificates have been generated, go to the path to check : **C:\Program Files\OpenVPN\easy-rsa\keys**

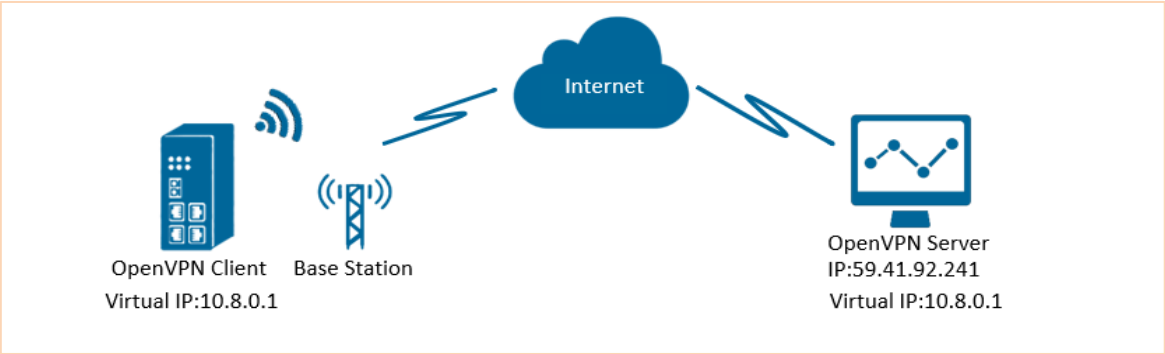


11.5. AN007-Configuring an Open -VPN Client with a Pre-shared Key

Overview

This part of the document explains how to configure and use an Open VPN Client on a 6944 with a Pre-Shared Key talking to an Open VPN Server.

Testing Topology

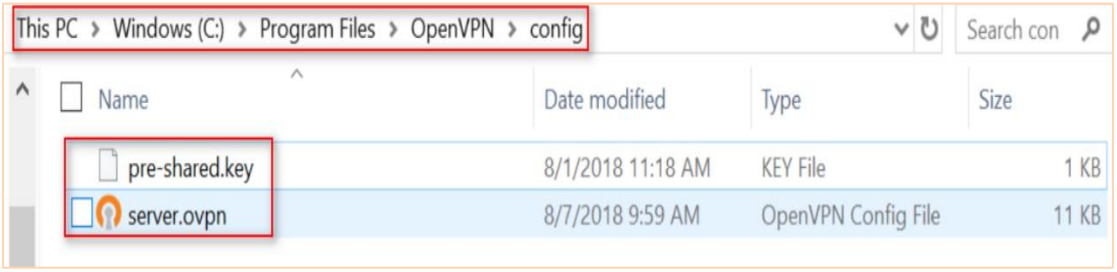


- The 6944 runs as an OpenVPN Client on an IP Network capable of pinging an IP OpenVPN server successfully.
- A PC runs as an OpenVPN Server with a **static** public IP address and opens a specified listening port for OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, allowing the devices to PING each other successfully. This is a point-to-point application.

Configuring an Open VPN Client with a pre-shared key

Server Configuration

Install OpenVPN software on a PC and copy the related certifications and configuration to the PC as shown below:



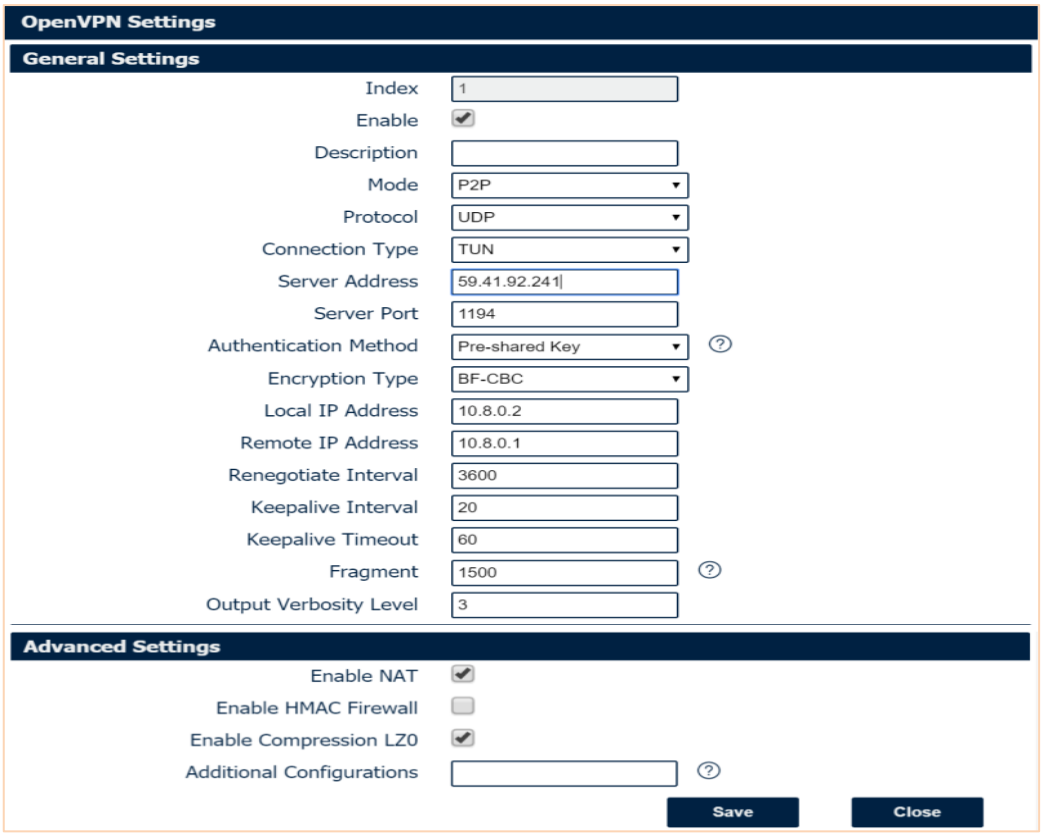
Note: Install and run OpenVPN software with ***administrator authority***

Step 1 - Configure the **server.ovpn** as shown below:

```
local 59.41.92.241
proto udp
dev tun
tun-mtu 1500
fragment 1500
ifconfig 10.8.0.1 10.8.0.2
keepalive 10 120
secret pre-shared.key
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
    verb 3
```

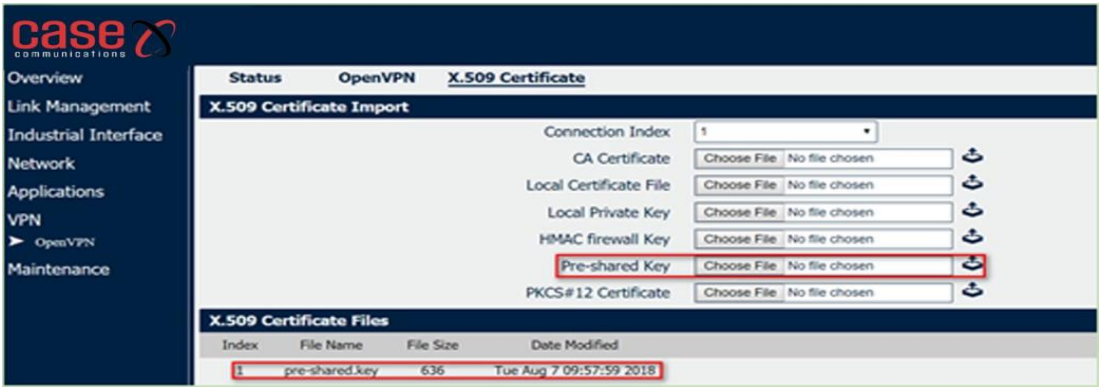
Client Configuration

Step 1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



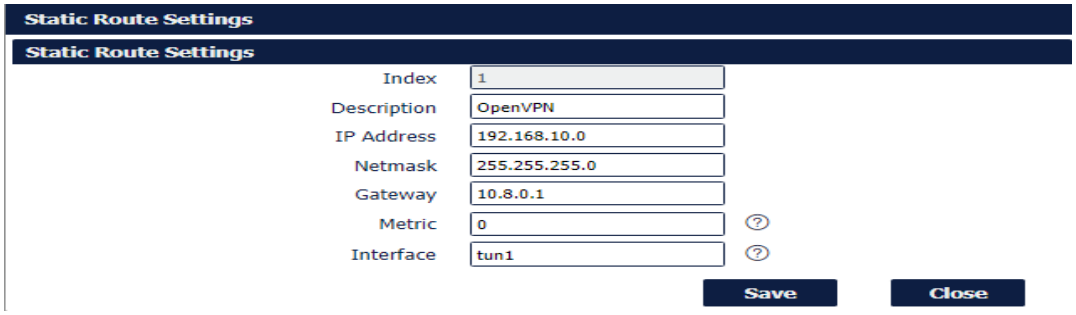
Step 2. Click Save>Apply.

Step 3. Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, Click Apply.



Step 4: Check the Route has connected to the OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

Step 5: Go to **Network>Route>Static Route** and add a new Static Route.



Step 6: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. Click Save

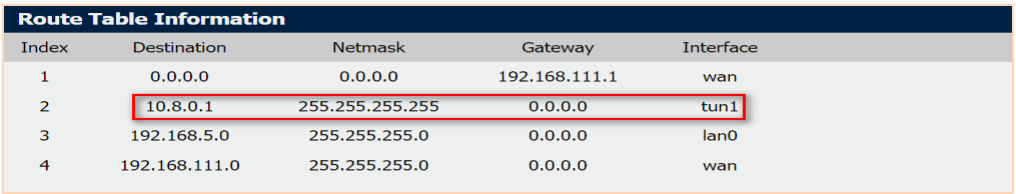
Step7: Click Save>Apply

Checking the Routing Table

Step 1: Check the Routing Table on the PC for reference.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19     291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     291
         10.8.0.0  255.255.255.252          On-link          10.8.0.1     291
         10.8.0.1  255.255.255.255          On-link          10.8.0.1     291
         10.8.0.3  255.255.255.255          On-link          10.8.0.1     291
        127.0.0.0        255.0.0.0          On-link         127.0.0.1     331
```

Step 2: Check the 6944 Routing Table on the Router for reference.



Route Table Information

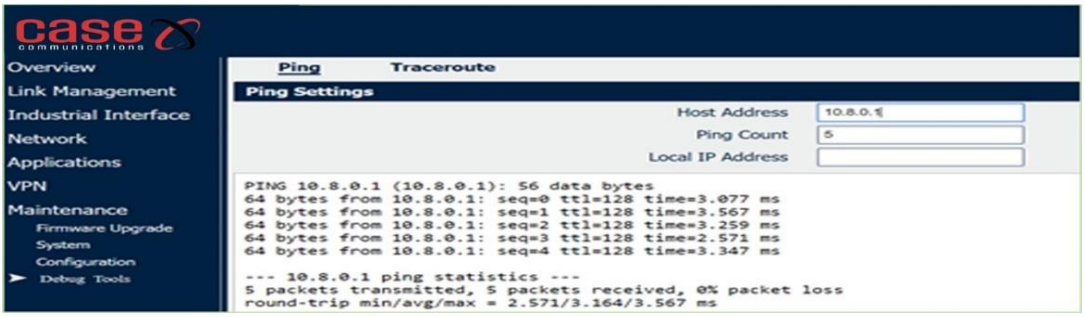
Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Testing the Open VPN with a Pre-Shared Key

Step 1: Enable CMD and Ping the virtual IP from PC to router.

```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Step 2: Go to **Maintenance>Debug Tool>Ping** and Ping the virtual IP from router to PC.

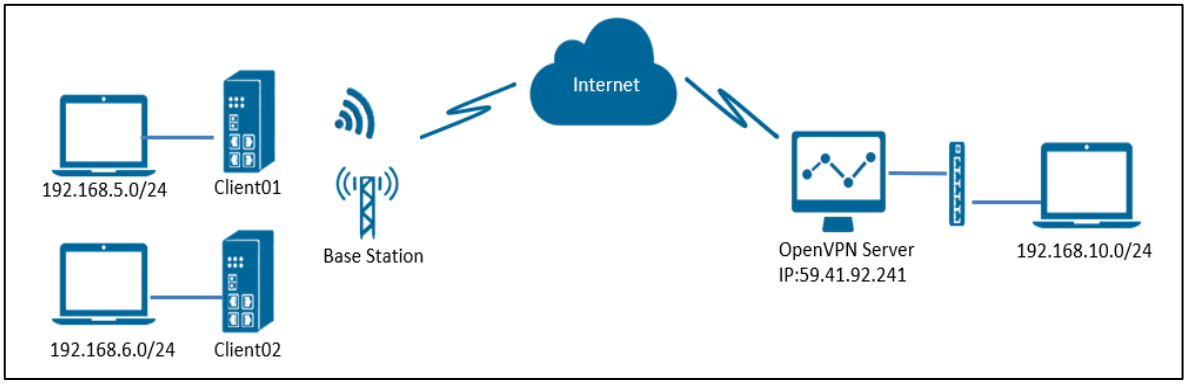


11.6. AN008-Open VPN Client with Username and Password

Overview

This section relates to the configuration of an Open VPN Client with a Username and Password on the Case Communications 6944 Industrial Router

Testing Topology

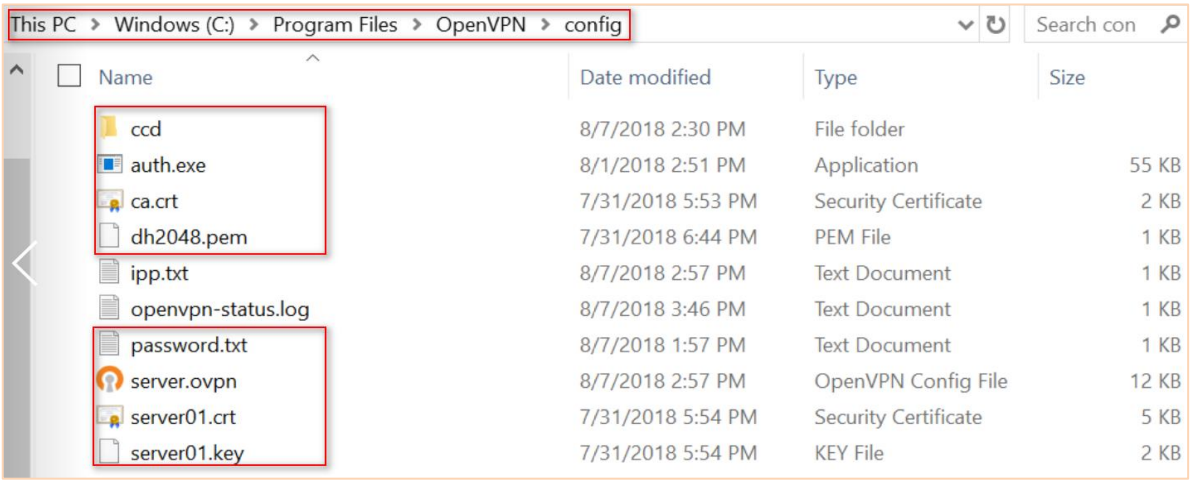


- Two 6944s run as OpenVPN Clients, Client01 and Client02 on an IP network, which can ping an OpenVPN server IP successfully.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified port for listening for the OpenVPN.
- The OpenVPN tunnel is established between the Server and the Client. Client01 can ping Client02 successfully and vice versa.

Configuration

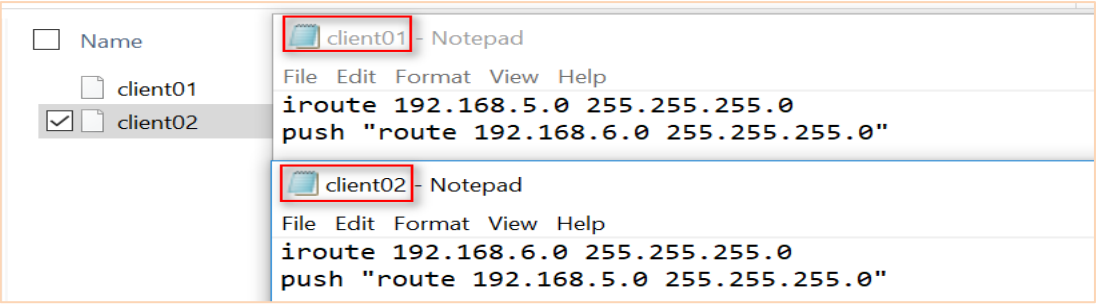
Server Configuration

Step1. Install OpenVPN software on your PC and copy the related certificates and configuration to the PC as shown below:



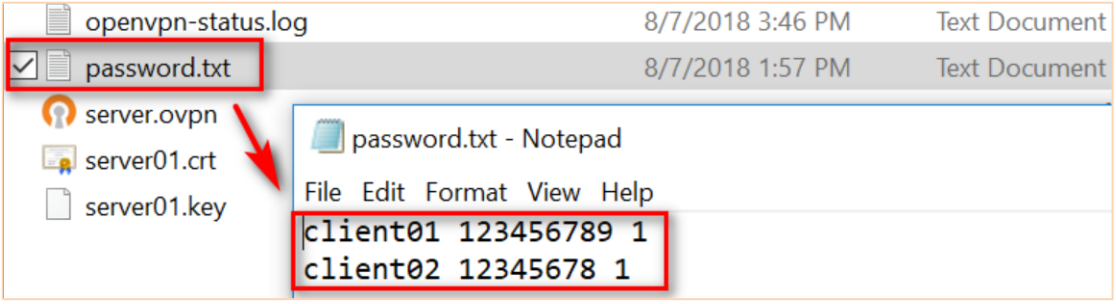
Note**: a) Download OpenVPN software with: **https://openvpn.net/
*b) Install and run OpenVPN software logged on with **administrator authority**.*

Step 2. Add a "ccd" folder, and create a new notepad, rename it without a suffix, configure as shown below:



***Note**: client01 and client02 are the common name.*

Step 3.Create a "password.txt" file, which including below content:



The format would be: ***common name password 1or 0(1=enable,0=disable)***

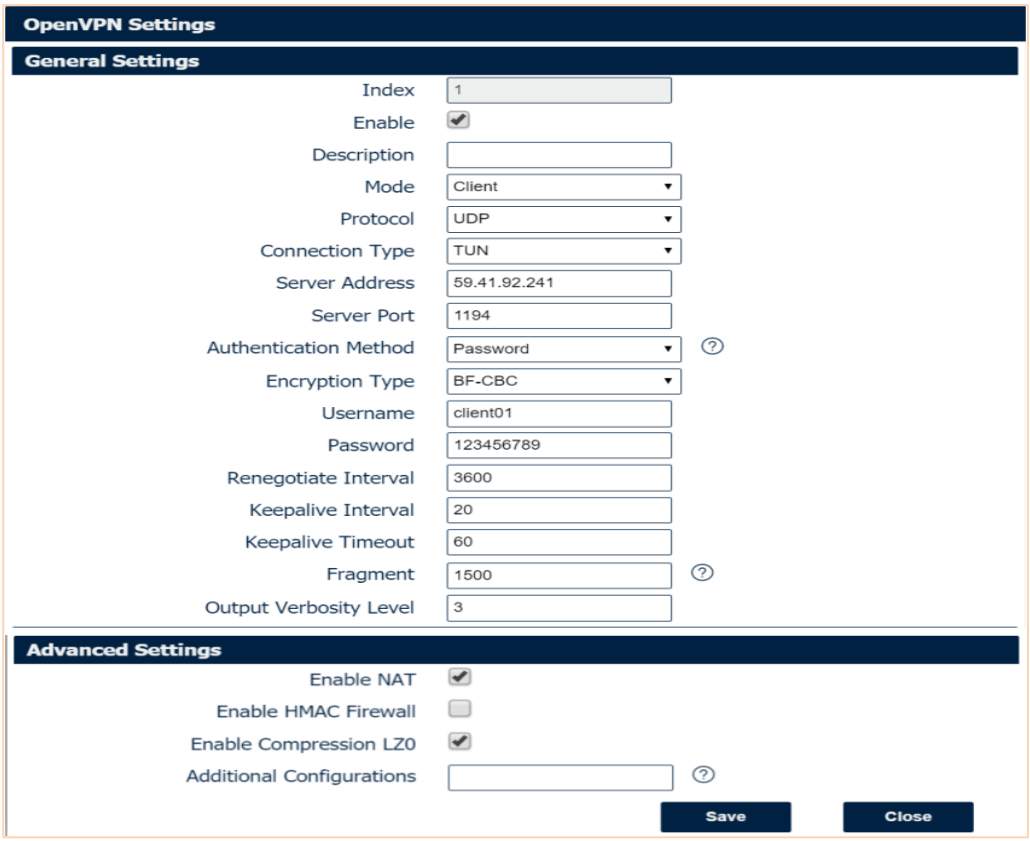
Step 4: Configure the **server.ovpn** as shown below:

==========

```
local 59.41.92.241
mode server
port 1194
proto udp
client-cert-not-required
username-as-common-name
auth-user-pass-verify auth.exe via-env
script-security 3 system
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key  # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0
ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
route 192.168.6.0 255.255.255.0
client-to-client
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Client01 Configuration

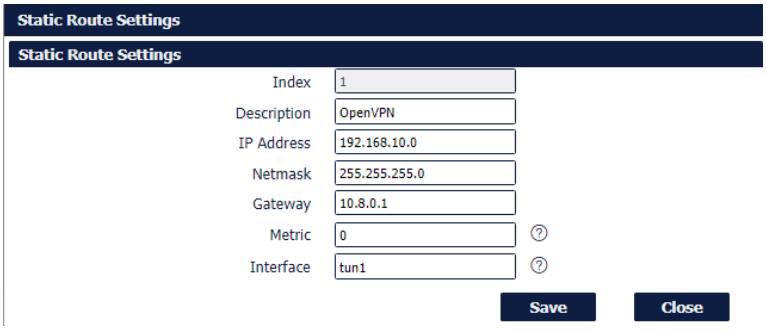
Step 1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. **Click Save > Apply.**



Step 2: Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, **Click Save >Apply.**

Step 3: If the Route has connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

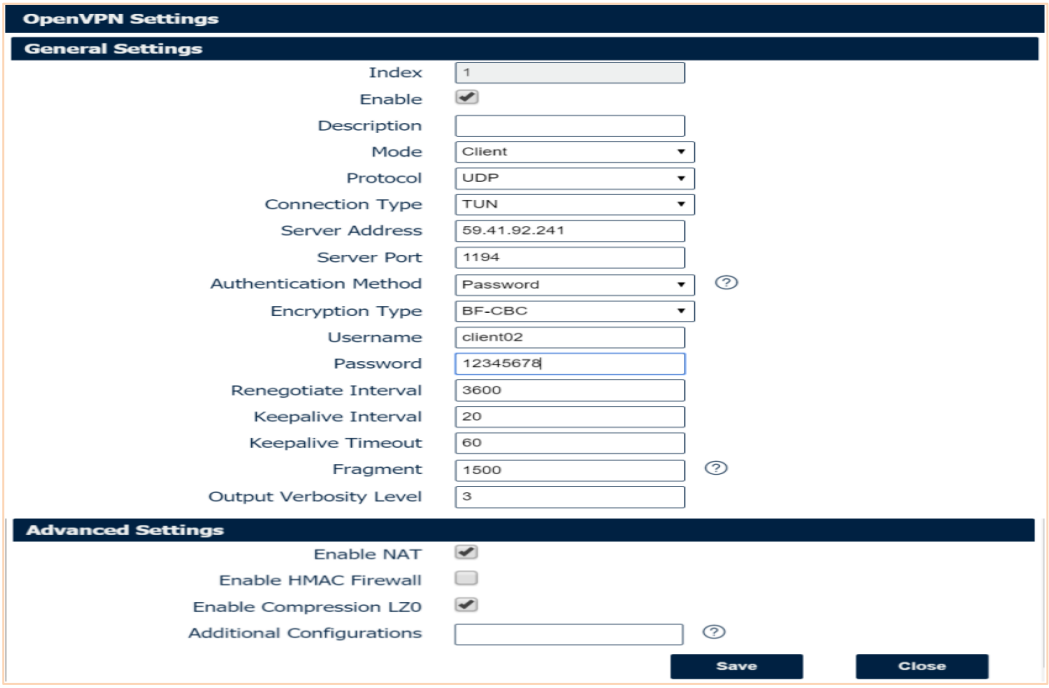
Step 4: Go to Network>Route>Static Route and add a new Static Route.



Step 5: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. **Click Save > Apply**

<u>Client02 Configuration</u>

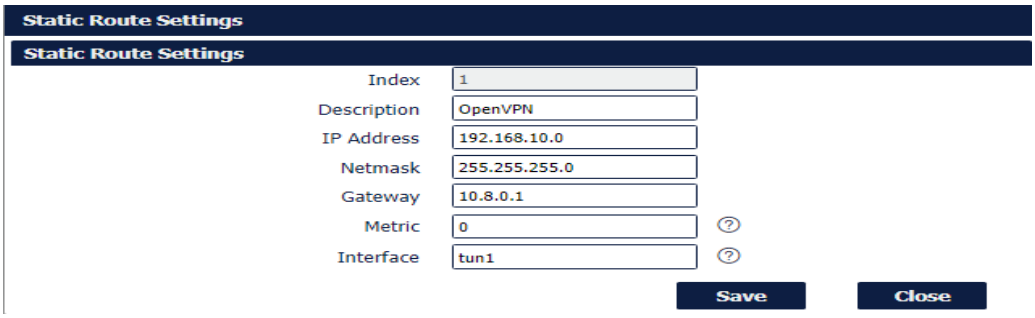
Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as shown below. **Click Save > Apply**.



Step 2. Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, **Click Save > Apply.**

Step 3: If the Route has connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

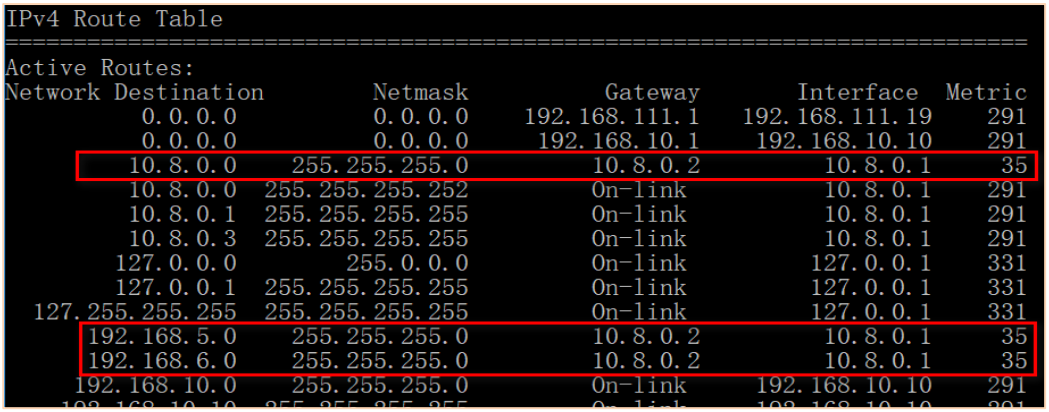
Step 4: Go to **Network>Route>Static Route** and add a new Static Route.



Step 5: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. **Click Save > Apply**

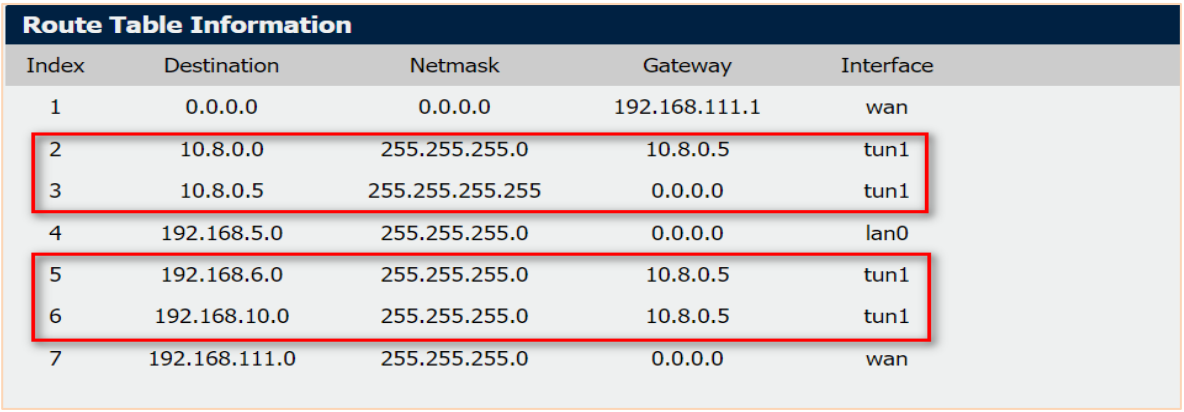
<u>Checking the Routing Tables</u>

Step 1: Open the Routing Table on the OpenVPN Server for reference.



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19     291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     291
         10.8.0.0      255.255.255.0         10.8.0.2         10.8.0.1      35
         10.8.0.0    255.255.255.252         On-link          10.8.0.1     291
         10.8.0.1    255.255.255.255         On-link          10.8.0.1     291
         10.8.0.3    255.255.255.255         On-link          10.8.0.1     291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
        127.0.0.1    255.255.255.255         On-link         127.0.0.1     331
  127.255.255.255    255.255.255.255         On-link         127.0.0.1     331
      192.168.5.0      255.255.255.0         10.8.0.2         10.8.0.1      35
      192.168.6.0      255.255.255.0         10.8.0.2         10.8.0.1      35
     192.168.10.0      255.255.255.0         On-link     192.168.10.10     291
```

Step 2: Check the Routing Table on Client01 for reference.



Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.5	tun1
3	10.8.0.5	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	0.0.0.0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.5	tun1
6	192.168.10.0	255.255.255.0	10.8.0.5	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

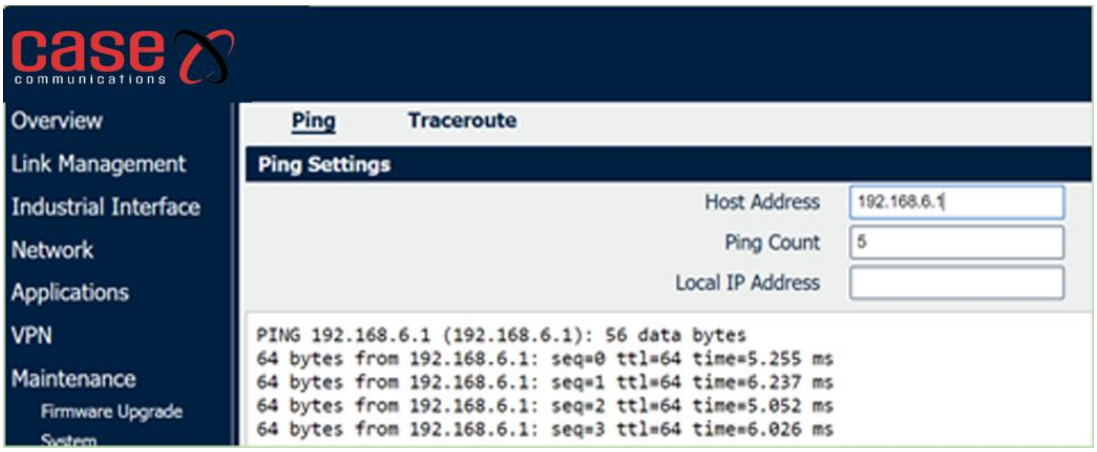
Step 3: Check the Routing Table on Client02 for reference.

Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.0	255.255.255.0	10.8.0.9	tun1
3	10.8.0.9	255.255.255.255	0.0.0.0	tun1
4	192.168.5.0	255.255.255.0	10.8.0.9	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	lan0
6	192.168.10.0	255.255.255.0	10.8.0.9	tun1
7	192.168.111.0	255.255.255.0	0.0.0.0	wan

Testing

Step 1: Ping from Client01 to Client02 and check the result as shown below:



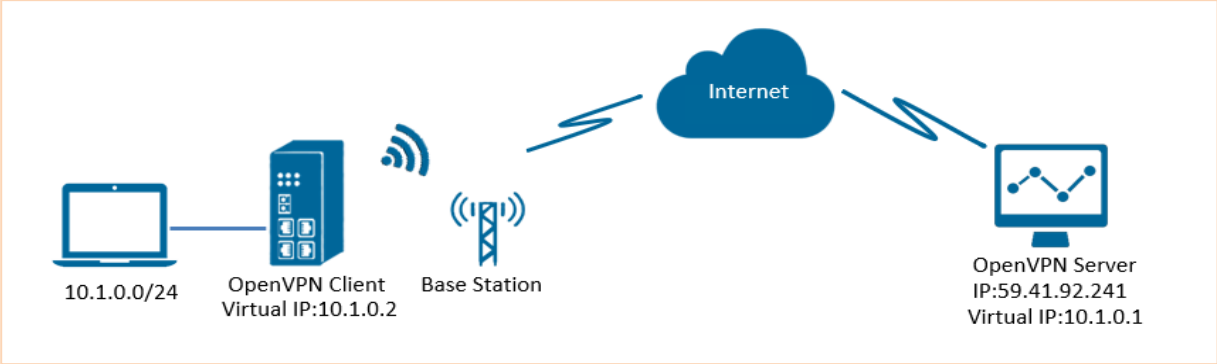
Step 2 and 3: Repeat the Ping test from Client 02 to client 01

11.7. AN009-Open VPN Client Running TAP Pre-shared key P2P Mode

Overview

This section covers the use of an Open VPN running TAP with a pre-shared key and running in P2Pmode on a Case Communications 6944 Industrial Router.

Testing Topology

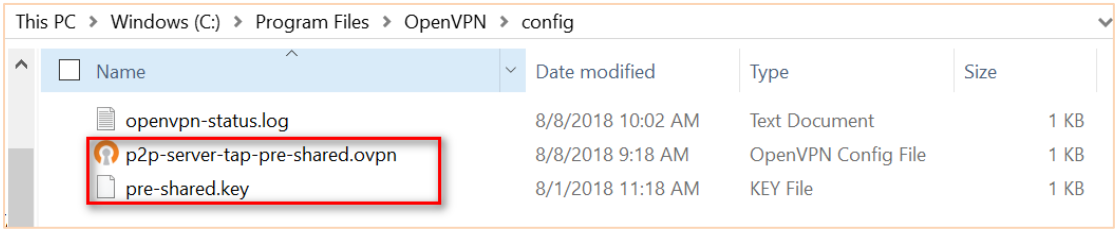


- The 6944 runs as an OpenVPN Client which can ping the OpenVPN IP servers.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified port a listening for an OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, the virtual IP can PING each other successfully. The Server can ping the LAN PC and vice versa.

Configuration

Server Configuration

Step 1: Install OpenVPN software on a PC and copy the related certifications and configuration to the PC as shown below:



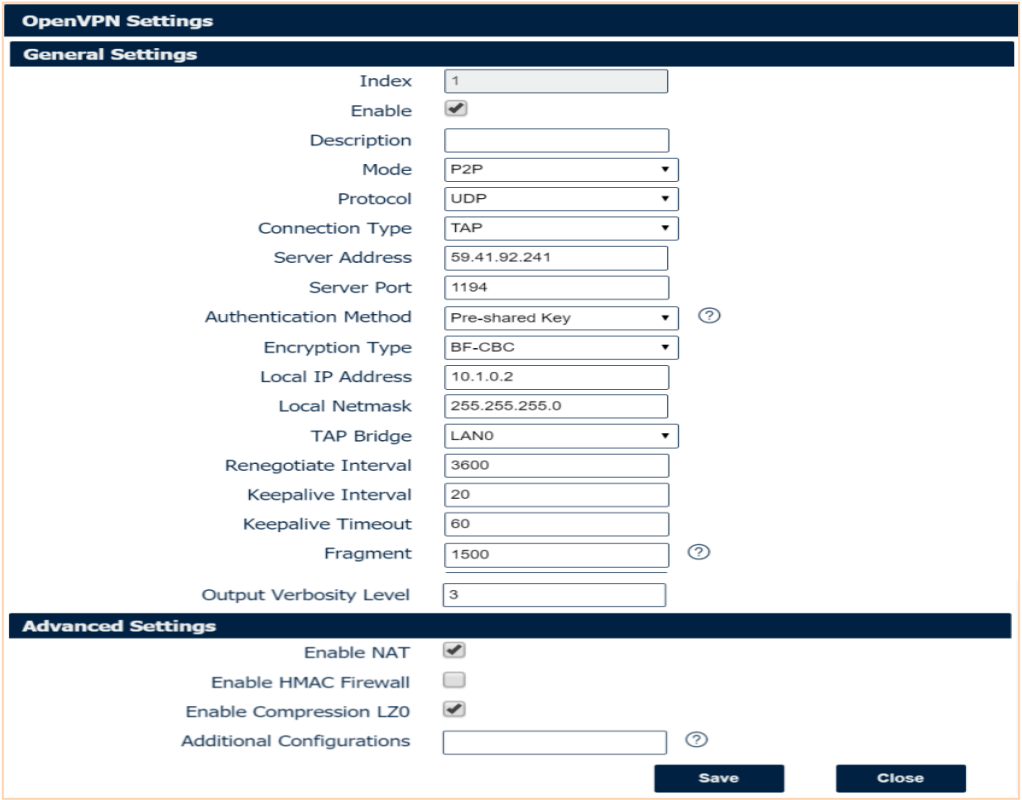
Note: *Install and run OpenVPN software logged on with* ***administrator authority****.*

Step2: The configure the "p2p-server-tap-pre-shared.ovpn" as shown below:

```
==================================================================
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
secret pre-shared.key   # None TLS Mode
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

Client Configuration

Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as shown below. **Click Save > Apply.**

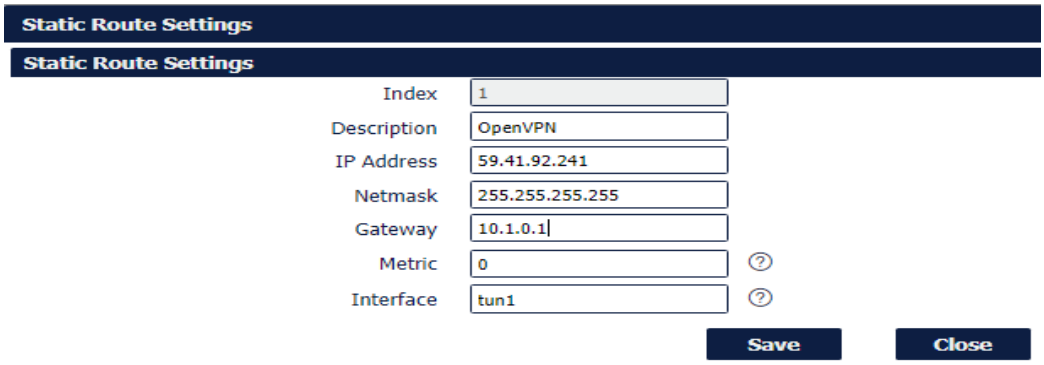


Step 2: Click Save>Apply.

Step 3: Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, Click Apply.

Step 4: Route had connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

Step 5: Go to **Network>Route>Static Route** and add a new Static Route.



Step 6: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. Click Save

Step 7: Click Save>Apply

Routing Table

Step 1: Check the Routing Table on the PC for reference.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.10.1    192.168.10.10     291
          0.0.0.0          0.0.0.0     192.168.111.1   192.168.111.19     291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1     291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1     291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1     291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
```

Step 2: Check the Routing Table on the Router for reference.

Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Testing

Step 1: Enable CMD and Ping from the PC on the 6944 to the virtual LAN on the Server.

```
C:\Users\Administrator>ping 10.1.0.10

Pinging 10.1.0.10 with 32 bytes of data:
Reply from 10.1.0.10: bytes=32 time=2ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64
Reply from 10.1.0.10: bytes=32 time=3ms TTL=64

Ping statistics for 10.1.0.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Step 2: Ping from LAN device of the router to PC.

Step 3: Receive the Ping Reply to for success.

11.8. AN010- OpenVPN Client_with_TAP_under_P2P_mode

Overview

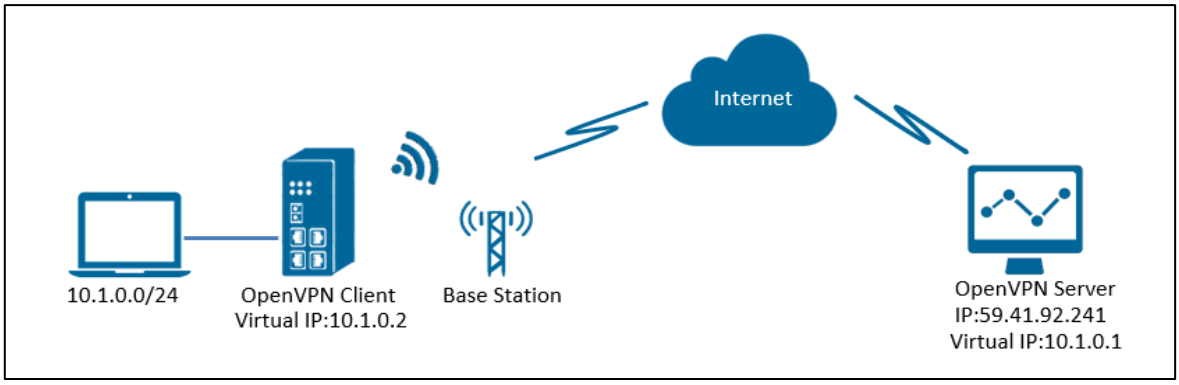
This document contains information regarding the configuration and use of a 6944 Industrial router running OpenVPN with TAP running under P2P mode,

Software Version

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
3.8.2018	V1.1	V1.1.1.4 (0c0c9fa)	Std Software	First released

Testing Topology

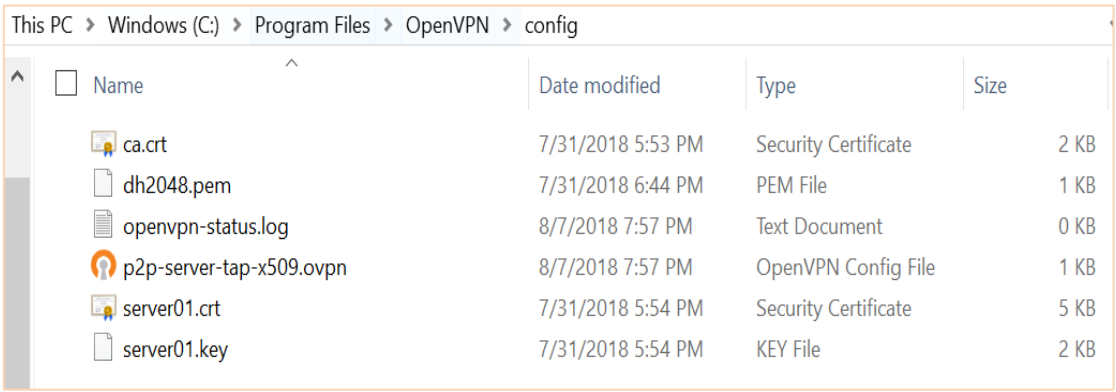


- The 6944 runs as an OpenVPN Client with any kind of IP, which can ping an OpenVPN IP server successfully.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified a port listening for an OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, the virtual IP can PING each other successfully. The Server should be able to ping the LAN PC device and vice versa.

Configuration

Server Configuration

1. Install OpenVPN software on PC and copy the related certifications and configuration to the PC as shown below:



Note: Install and run the OpenVPN software using ***administrator authority****.*

2. Configure the “p2p-server-tap-x.509.ovpn” as shown below:

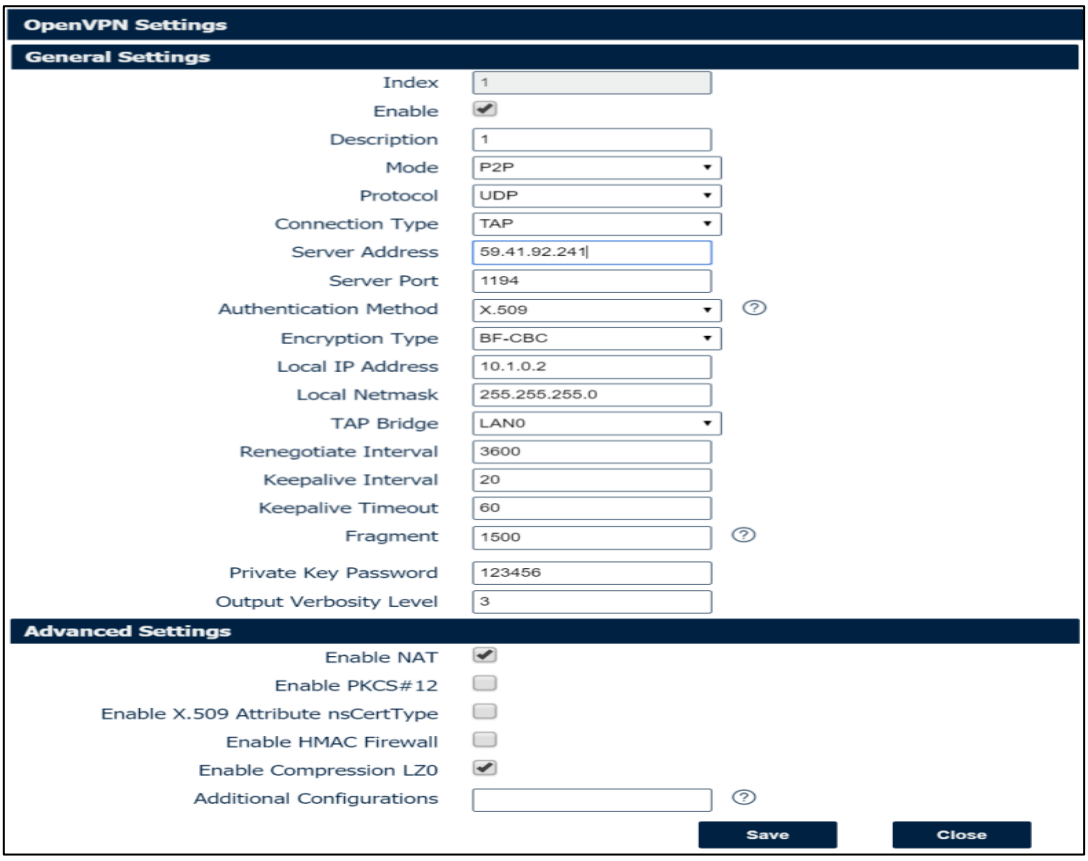
==========

```
mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem
#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
```

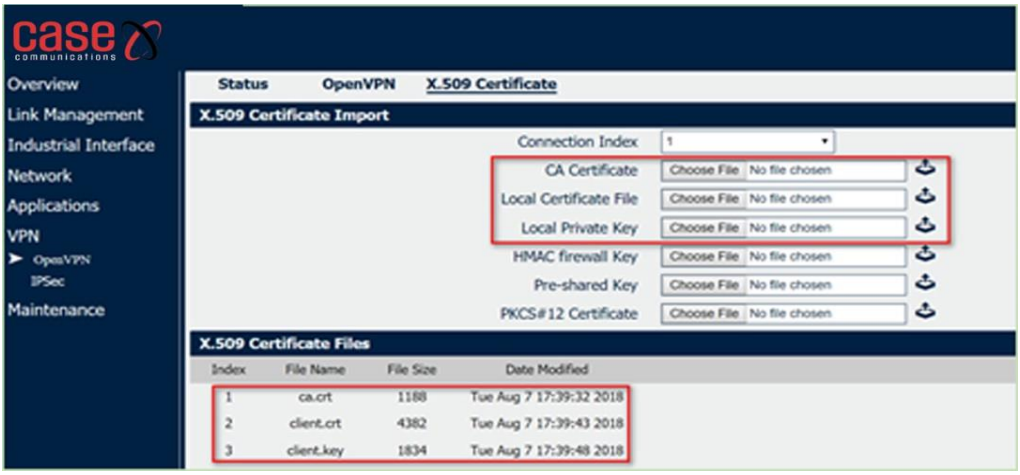
==========

Router Configuration

Step 1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. **Click Save > Apply**

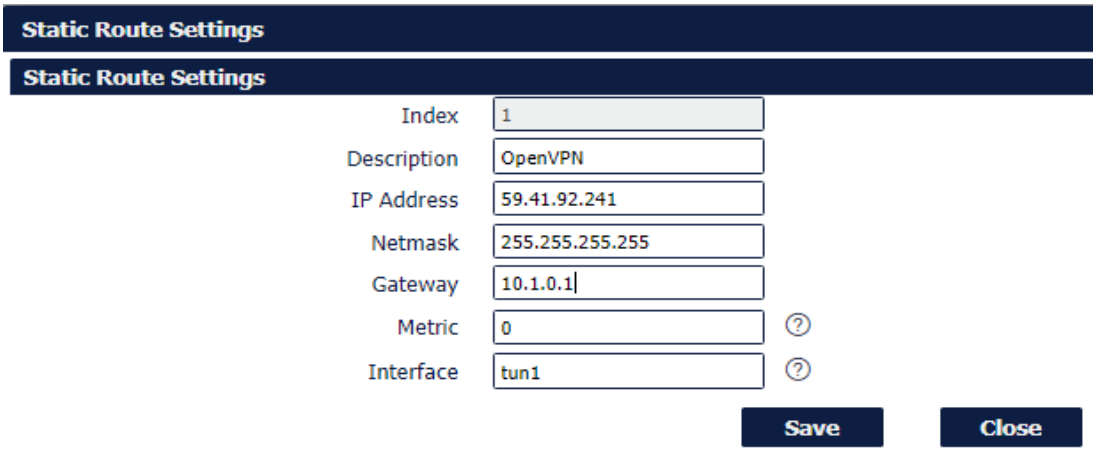


Step 3: Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, Click Apply.



Step 4: If the Route has connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

Step 5: Go to **Network>Route>Static Route** and add a new Static Route.



Step 6: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. **Click Save > Apply**

Routing Table

Step 1: Look at the Routing Table on the PC for reference.

```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19     291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     291
         10.1.0.0    255.255.255.0         On-link          10.1.0.1     291
         10.1.0.1  255.255.255.255         On-link          10.1.0.1     291
       10.1.0.255  255.255.255.255         On-link          10.1.0.1     291
```

Step 2: Look at the Routing Table on the 6944 router

Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.1.0.0	255.255.255.0	0.0.0.0	lan0
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

Testing

Step 1: Enable CMD and Ping from PC side to LAN device of router.

```
C:\Users\Administrator>ping 10.1.0.20

Pinging 10.1.0.20 with 32 bytes of data:
Reply from 10.1.0.20: bytes=32 time=5ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128
Reply from 10.1.0.20: bytes=32 time=3ms TTL=128

Ping statistics for 10.1.0.20:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 5ms, Average = 3ms
```

Step 2: Ping from LAN device on router to Open VPN Virtual LAN

```
C:\Users\Administrator>ping 10.1.0.1

Pinging 10.1.0.1 with 32 bytes of data:
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128
Reply from 10.1.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 10.1.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

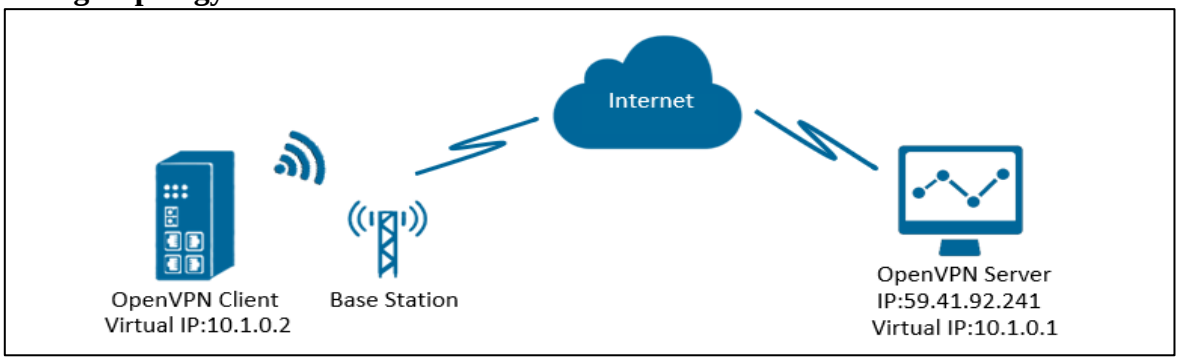
Step 3: Test successfully.

11.9. AN011-OpenVPN with TUN and X.509 certificate P2P Mode

Overview

This section relates to the configuration of a 6944 Industrial router running an OpenVPN with TUN and an X.509 certificate running under P2P mode.

Testing Topology

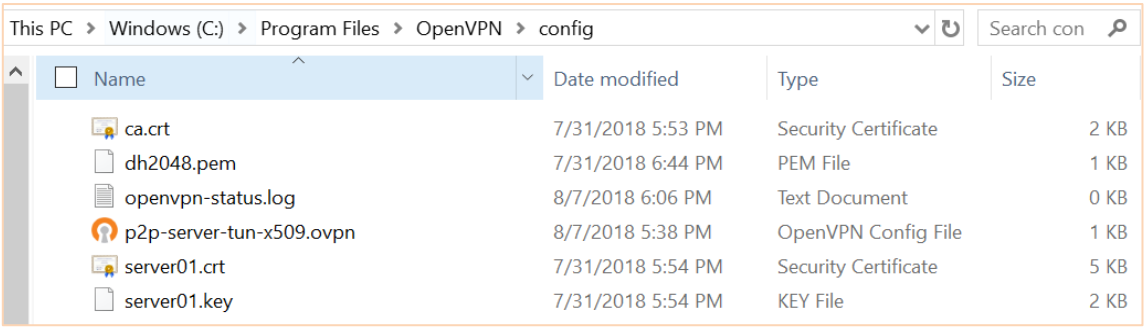


- The 6944 runs as an OpenVPN Client with any kind of IP, which can ping an OpenVPN IP server successfully.
- A PC runs as an OpenVPN Server with a static public IP address and opens a specific listening port for an OpenVPN.
- If the OpenVPN tunnel is established between the Server and Client, the virtual IP can PING each other successfully.

Configuration

Server Configuration

Step 1: Install OpenVPN software on PC and copy the related certifications and configuration to the PC as shown below:



This PC > Windows (C:) > Program Files > OpenVPN > config

Name	Date modified	Type	Size
ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
openvpn-status.log	8/7/2018 6:06 PM	Text Document	0 KB
p2p-server-tun-x509.ovpn	8/7/2018 5:38 PM	OpenVPN Config File	1 KB
server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
server01.key	7/31/2018 5:54 PM	KEY File	2 KB

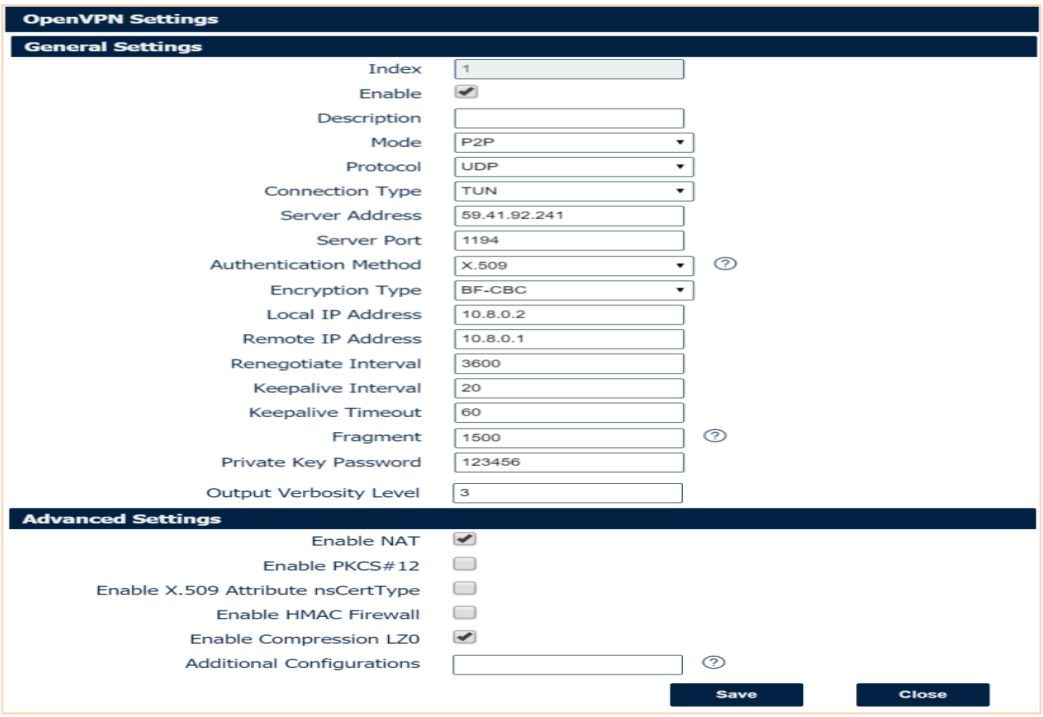
*Note: Install and run OpenVPN software logged on with **administrator authority**.*

Step 2: Configure the "p2p-server-tun-x.509" as shown below:

```
==================================================================
mode p2p                        persist-key                 #tls-auth ta.key 0
port 1194                       persist-tun                 cipher BF-CBC
proto udp                       tls-server                  comp-lzo
dev tun                         ca ca.crt                   status openvpn-status.log
# tun                           cert server01.crt           verb 3
ifconfig 10.8.0.1 10.8.0.2      key server01.key            tun-mtu 1500
keepalive 20 120                dh dh2048.pem               fragment 1500
```

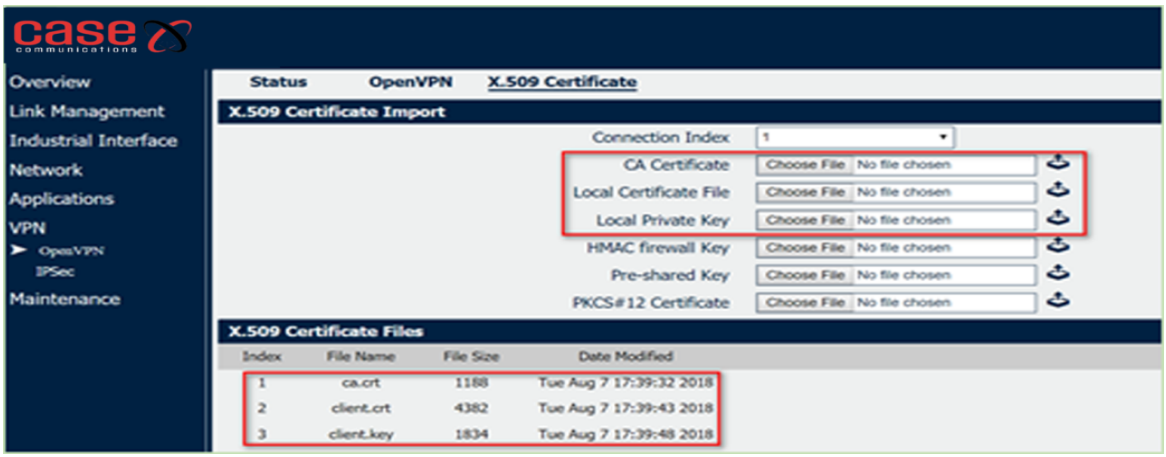
Router Configuration

Step 1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



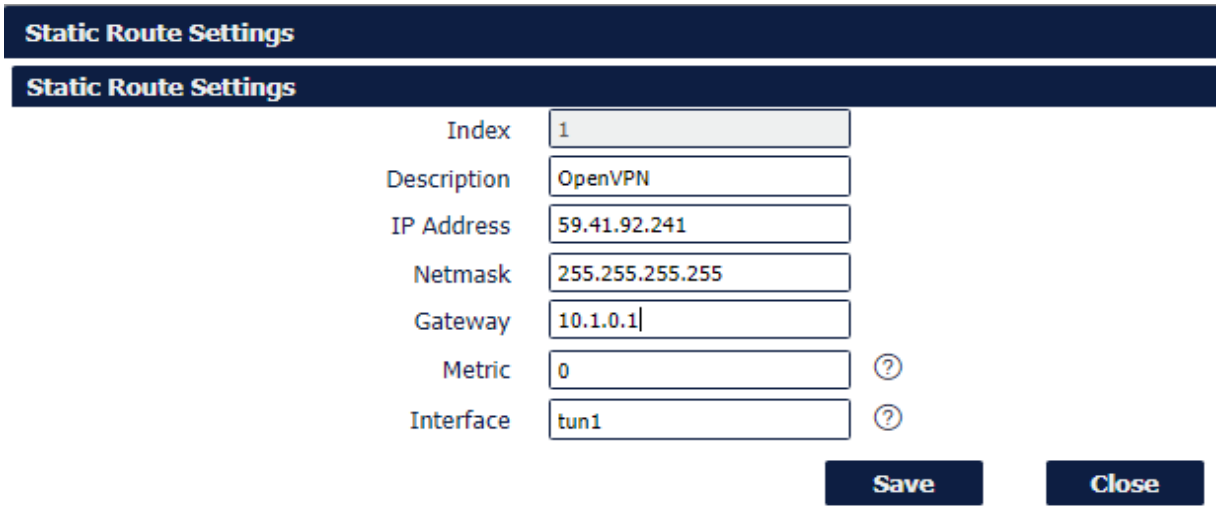
Step 2: Click Save>Apply.

Step 3: Go to **VPN>OpenVPN>X.509 Certificate,** to import the related certification, Click Apply.



Step4. If the Route has connected to OpenVPN server. Go to **VPN>OpenVPN>Status** to check the connection status.

Step 5: Go to **Network>Route>Static Route** and add a new Static Route.

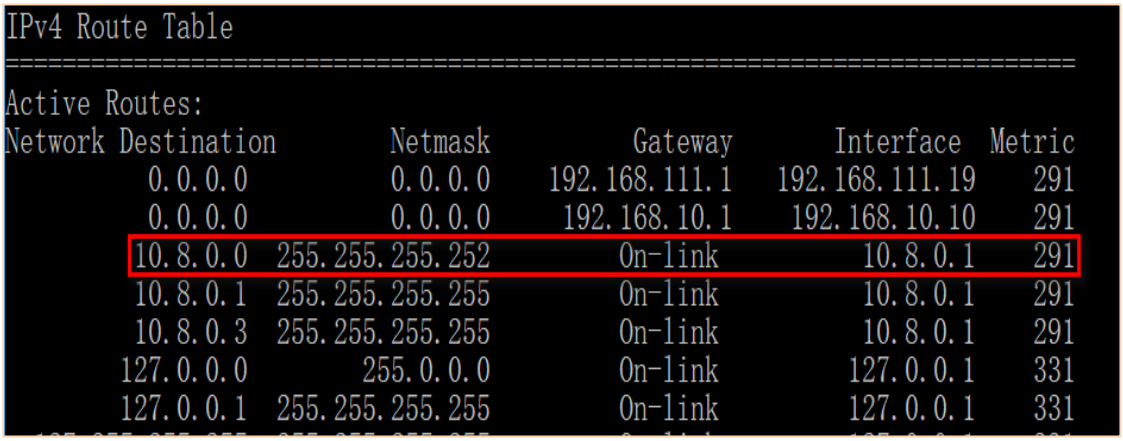


Step 6: Enter the required remote IP range details and set the Gateway as the virtual IP address the OpenVPN server will assign to itself, in this case 10.8.0.1 and set Interface as tun1 which is the OpenVPN tunnel. Click Save

Step 7: Click Save>Apply

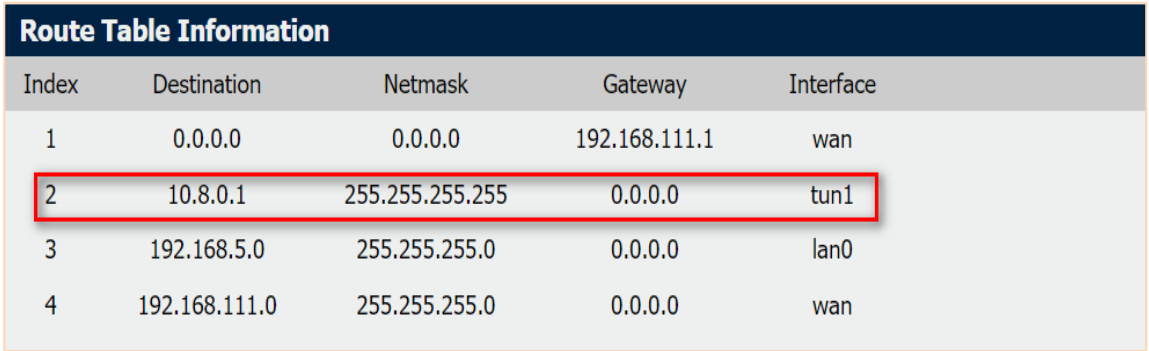
<u>Checking the Routing Table</u>

Step 1: Check the Routing Table on your PC



```
IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    192.168.111.1   192.168.111.19     291
          0.0.0.0          0.0.0.0     192.168.10.1    192.168.10.10     291
         10.8.0.0  255.255.255.252          On-link          10.8.0.1     291
         10.8.0.1  255.255.255.255          On-link          10.8.0.1     291
         10.8.0.3  255.255.255.255          On-link          10.8.0.1     291
        127.0.0.0        255.0.0.0          On-link         127.0.0.1     331
        127.0.0.1  255.255.255.255          On-link         127.0.0.1     331
```

Step 2: Check the Routing Table on router



Route Table Information

Index	Destination	Netmask	Gateway	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	wan
2	10.8.0.1	255.255.255.255	0.0.0.0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	lan0
4	192.168.111.0	255.255.255.0	0.0.0.0	wan

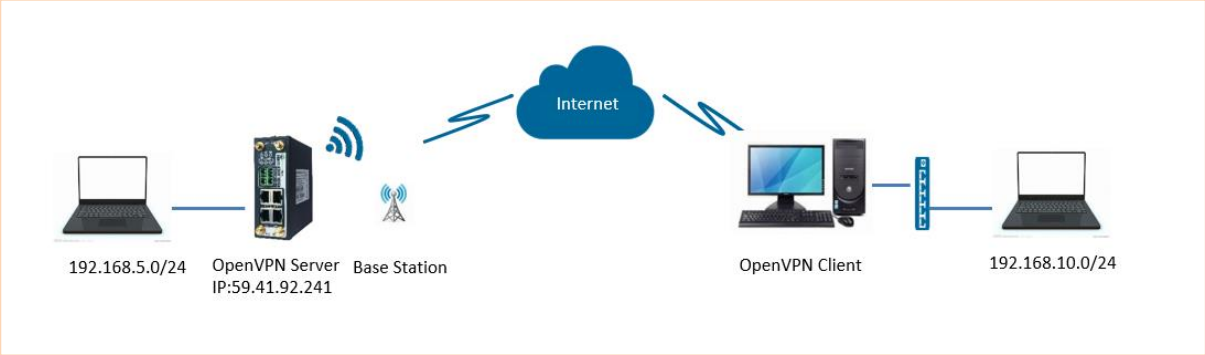
Step 3: Test Successful

11.10. AN050-6944 as an Open VPN Server with X.509 Certificate

Overview

This section relates to the configuration and use of OpenVPN Server with x.509 certification.

Testing Topology

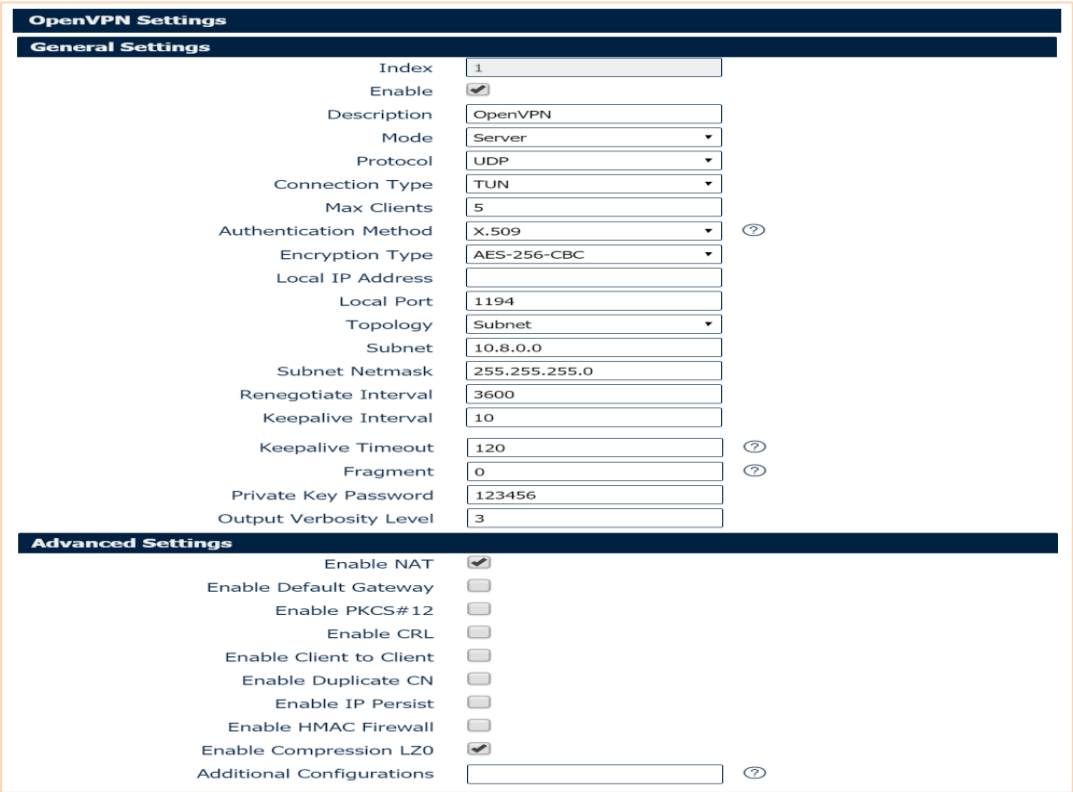


- The 6944 Router runs as OpenVPN Server with Public IP address or Domain Name, which can respond to a ping from OpenVPN Client successfully.
- A PC runs as OpenVPN Client with an IP connection, able to connect to internet.
- An OpenVPN tunnel is established between the Server and Client, the subnets can PING each other successful.

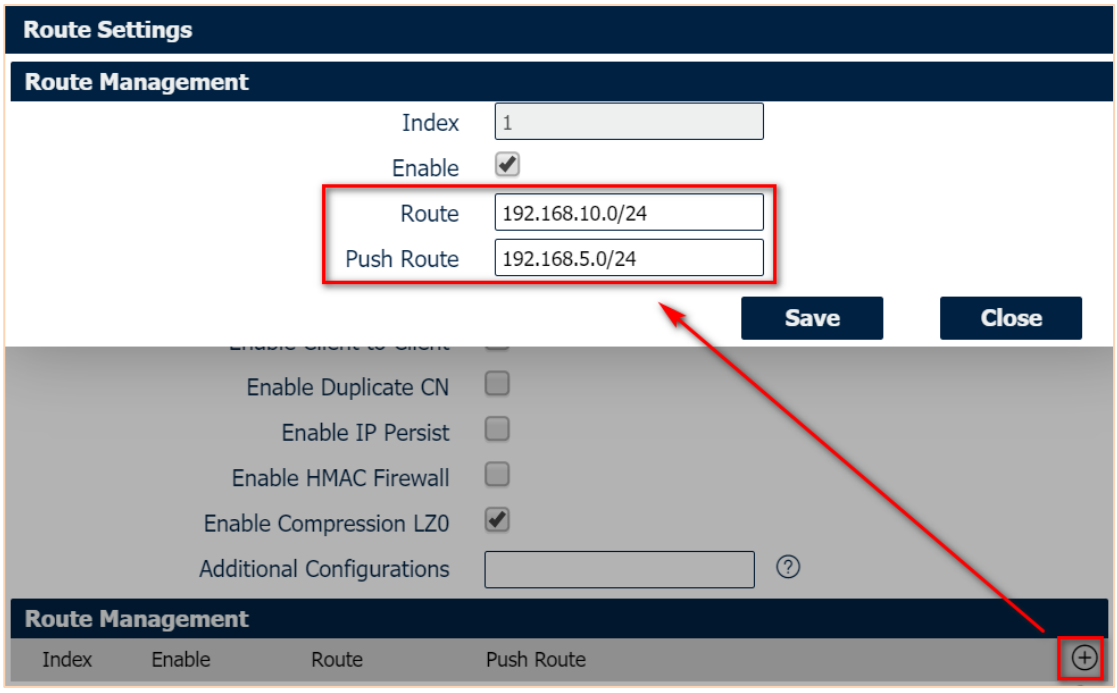
Configuration

Server Configuration

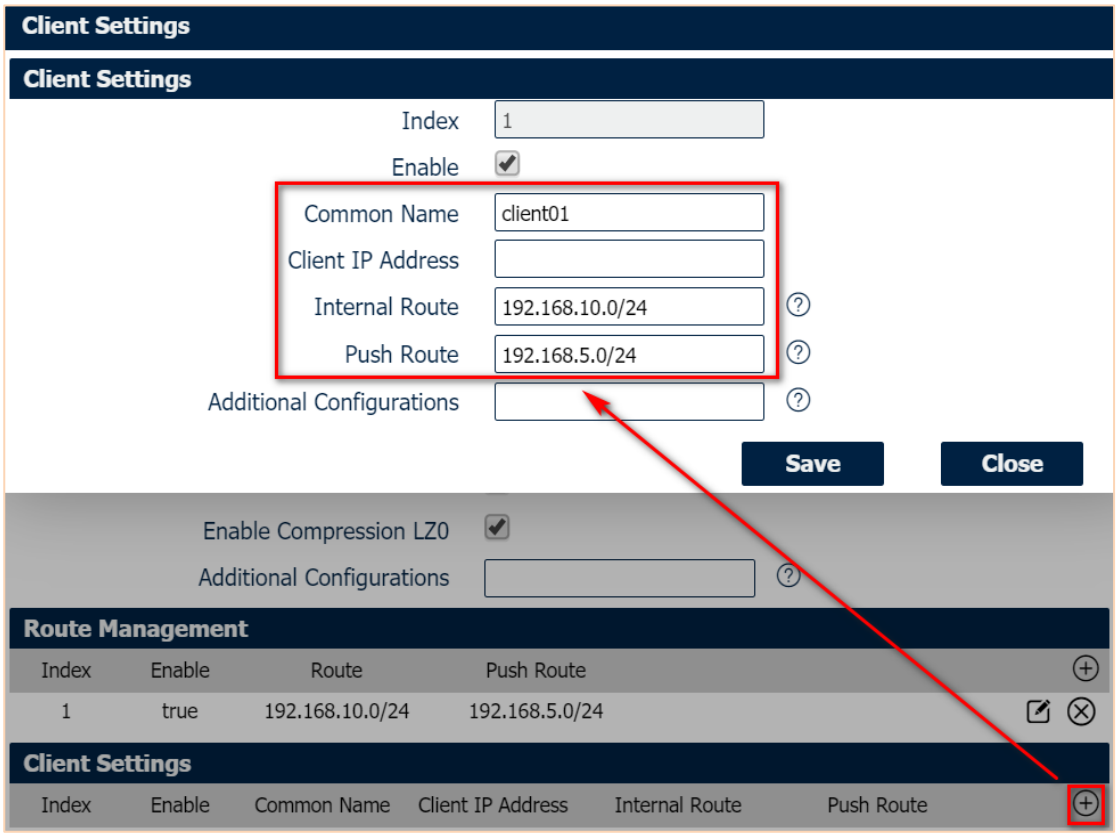
1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure the OpenVPN as shown below. Click Save.



Step 2: Configure the 6944Route Management as shown below click “Save”.

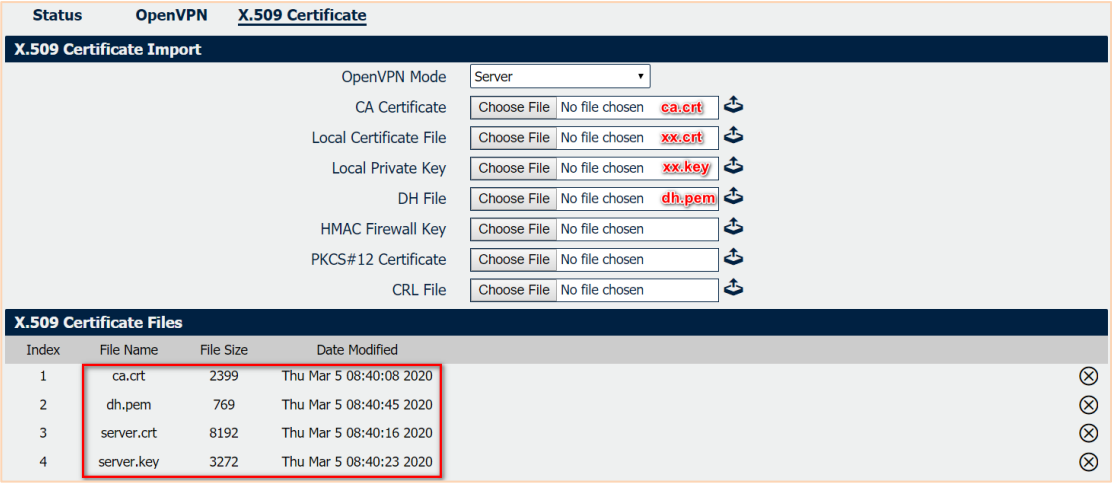


Step 3: Setting on Client Settings like below, click "Save":



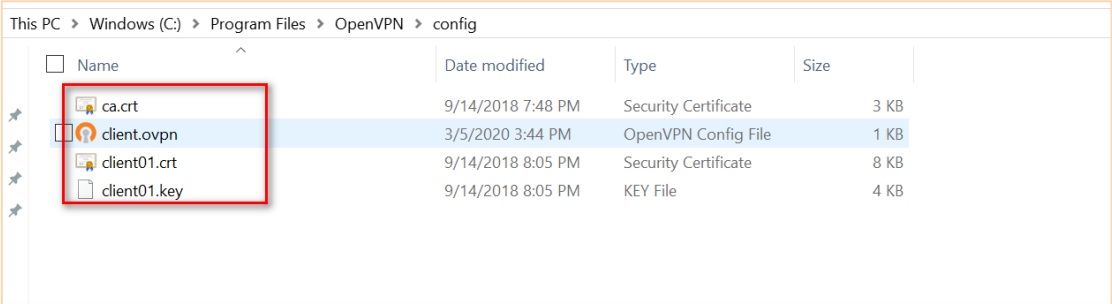
Step 4: After that, click Save>Apply.

Step 5: Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:



Client Configuration

Step 1: Install OpenVPN software on PC and copy the related certifications and configuration to the PC like below:



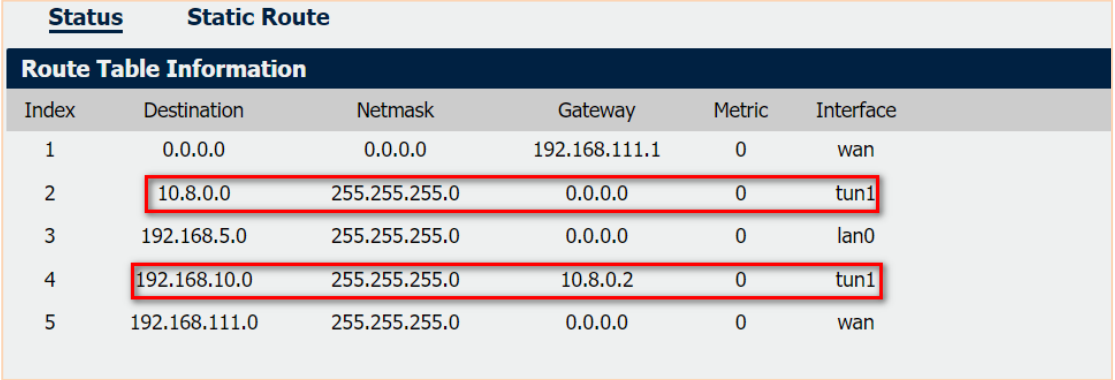
Note**: a) Download OpenVPN software from a suitable site for example: **https://openvpn.net/
*b) Install and run OpenVPN software with **administrator authority**.*

Step 2: Configure your Open VPN Client **client.ovpn** as shown below:

```
==================================================================
client
remote 59.41.92.241 1194
dev tun
proto udp
resolv-retry infinite
nobind
persist-key
persist-tun
ca ca.crt
cert client01.crt
key client01.key
remote-cert-tls server
cipher AES-256-CBC
keepalive 10 120
comp-lzo
verb 3
```

Routing Table

Step 1: Check the Routing Table on OpenVPN Server for reference.

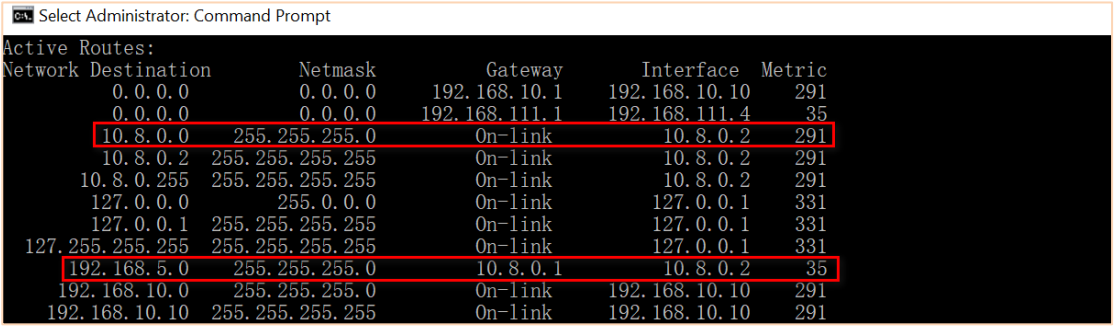


Status Static Route

Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	0	wan
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
4	192.168.10.0	255.255.255.0	10.8.0.2	0	tun1
5	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

Step 2: Route Table on OpenVPN Client for reference.

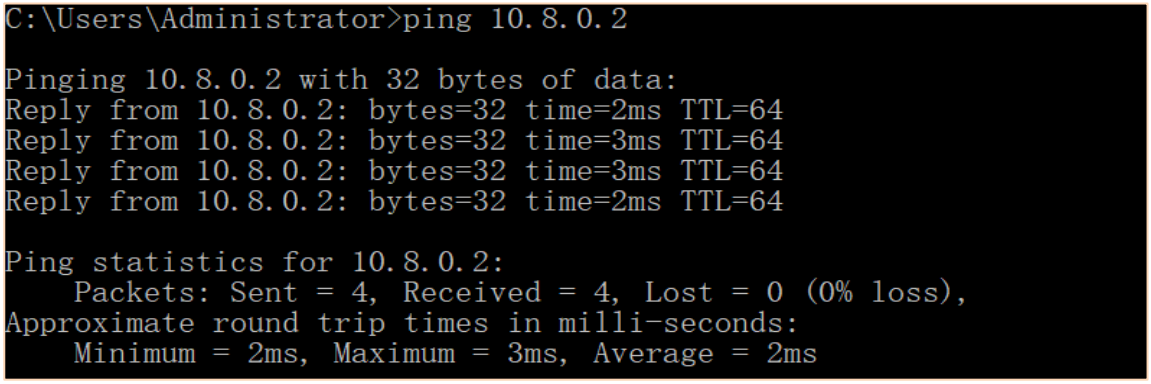


Select Administrator: Command Prompt

```
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0      192.168.10.1    192.168.10.10     291
          0.0.0.0          0.0.0.0      192.168.111.1   192.168.111.4      35
         10.8.0.0    255.255.255.0         On-link          10.8.0.2     291
         10.8.0.2  255.255.255.255         On-link          10.8.0.2     291
       10.8.0.255  255.255.255.255         On-link          10.8.0.2     291
        127.0.0.0        255.0.0.0         On-link         127.0.0.1     331
        127.0.0.1  255.255.255.255         On-link         127.0.0.1     331
  127.255.255.255  255.255.255.255         On-link         127.0.0.1     331
      192.168.5.0    255.255.255.0         10.8.0.1         10.8.0.2      35
     192.168.10.0    255.255.255.0         On-link      192.168.10.10     291
    192.168.10.10  255.255.255.255         On-link      192.168.10.10     291
```

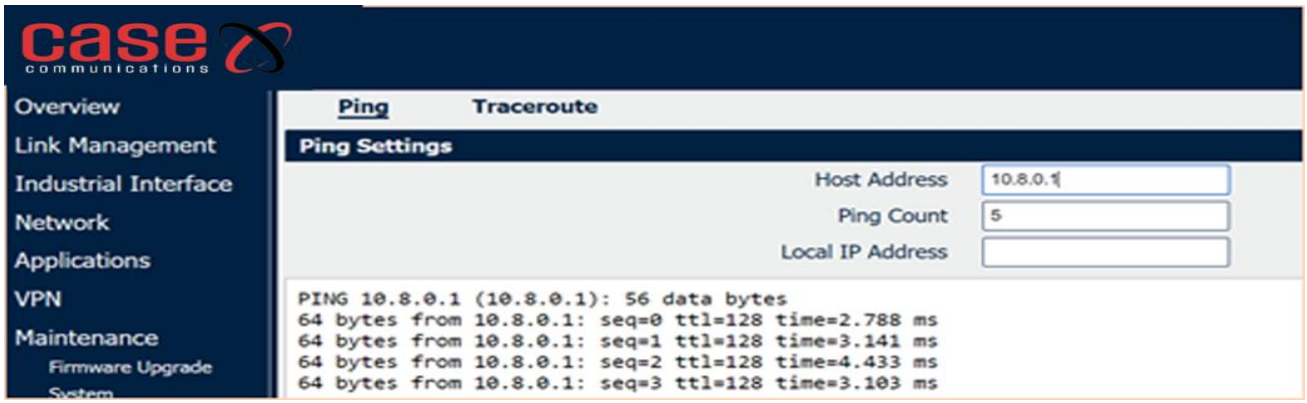
Testing

Step 1: Enable CMD and Ping from your PC to the 6944 router.



```
C:\Users\Administrator>ping 10.8.0.2

Pinging 10.8.0.2 with 32 bytes of data:
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=3ms TTL=64
Reply from 10.8.0.2: bytes=32 time=2ms TTL=64

Ping statistics for 10.8.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 2ms, Maximum = 3ms, Average = 2ms
```

Step 2: Go to **Maintenance>Debug Tool>Ping** and Ping from router to your PC



Overview
Link Management
Industrial Interface
Network
Applications
VPN
Maintenance
Firmware Upgrade
System

Ping Traceroute

Ping Settings

Host Address: 10.8.0.1
Ping Count: 5
Local IP Address:

```
PING 10.8.0.1 (10.8.0.1): 56 data bytes
64 bytes from 10.8.0.1: seq=0 ttl=128 time=2.788 ms
64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.141 ms
64 bytes from 10.8.0.1: seq=2 ttl=128 time=4.433 ms
64 bytes from 10.8.0.1: seq=3 ttl=128 time=3.103 ms
```

11.11. AN57-Open VPN between 6944 routers with X.509Certificate.

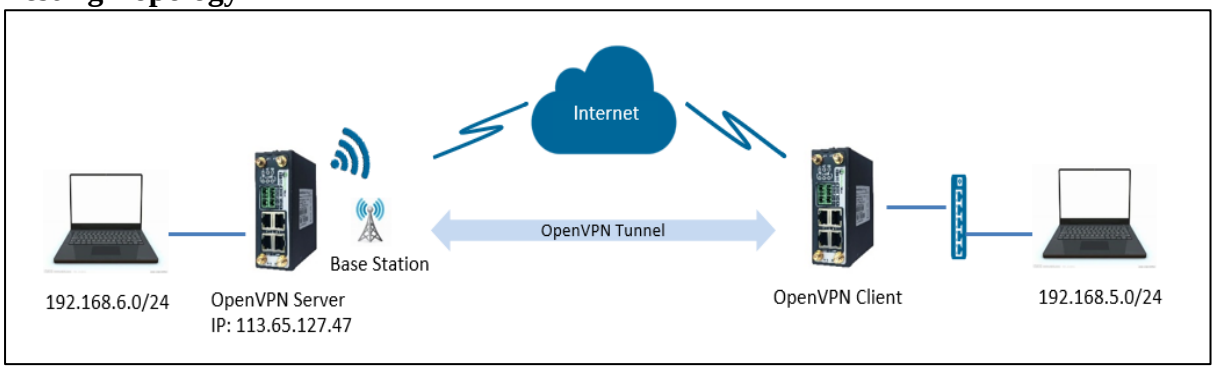
Overview

This part of the manual explains how to configure and use of OpenVPN with x.509 certificate between 6944 Routers, one working as a server and one working as a client.

Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
5.3.2020	V1.1	V1.1.4 (0c0c9fa)	Std Software	First release

Testing Topology

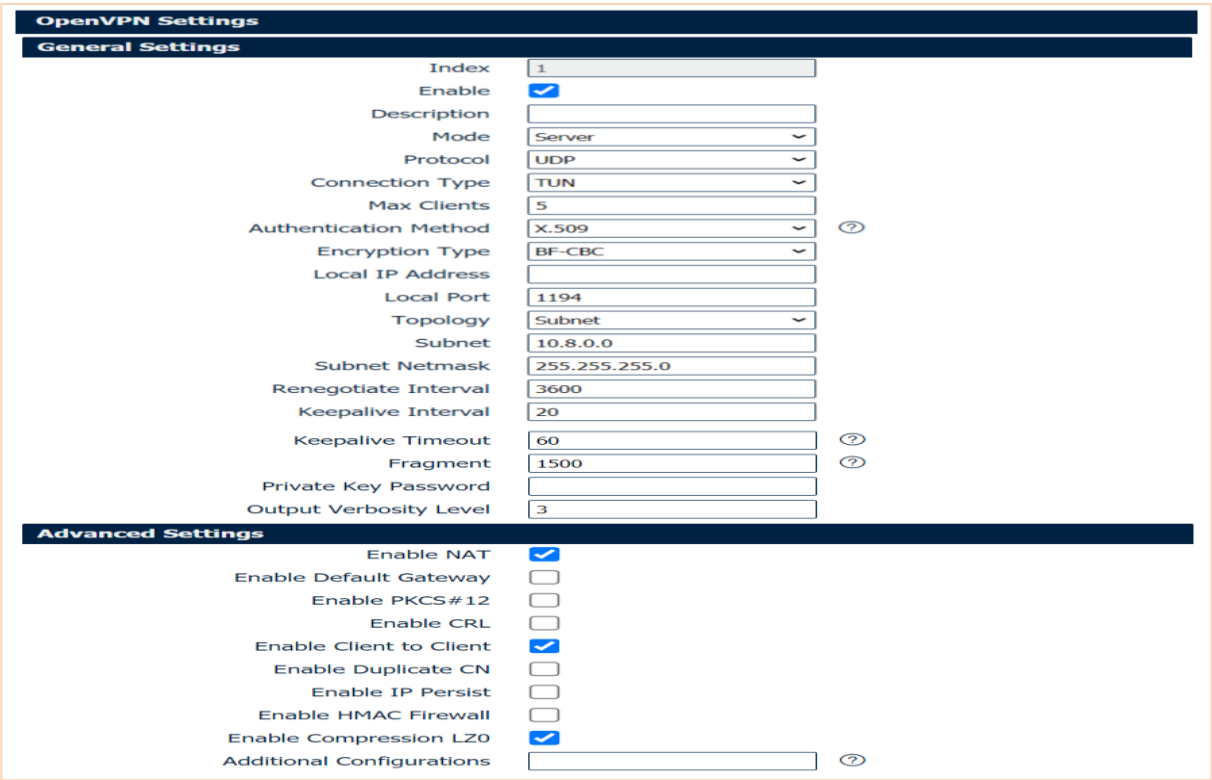


- A 6944 Router runs as OpenVPN Server with a Public IP address or Domain Name, which can be accessed by another 6944 running an OpenVPN Client.
- Two PCs are connected to the LAN ports of the of OpenVPN Server and OpenVPN Client as the subnet.
- An OpenVPN tunnel is established between the Server and Client, the subnets can PING each other successfully

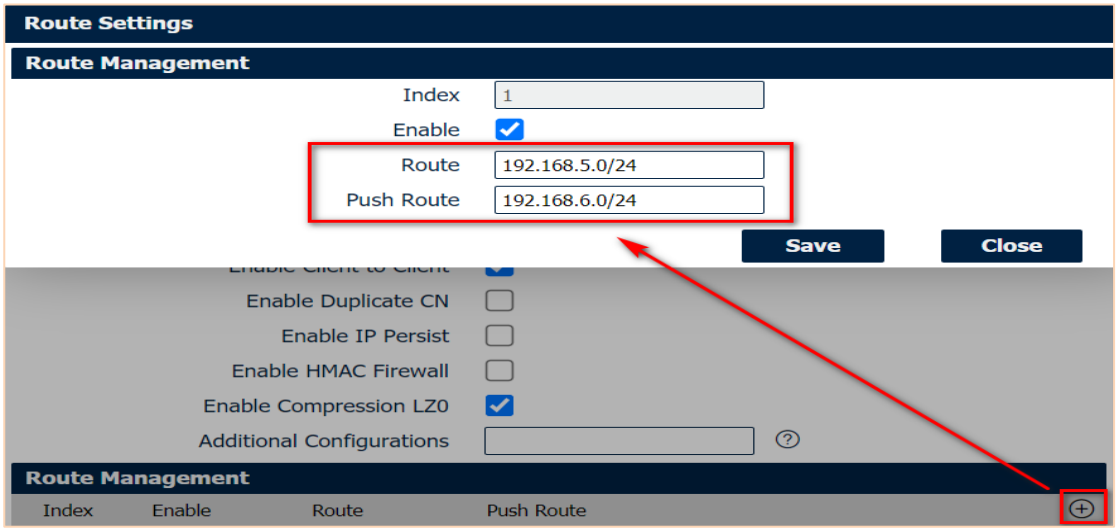
Configuration

Server Configuration

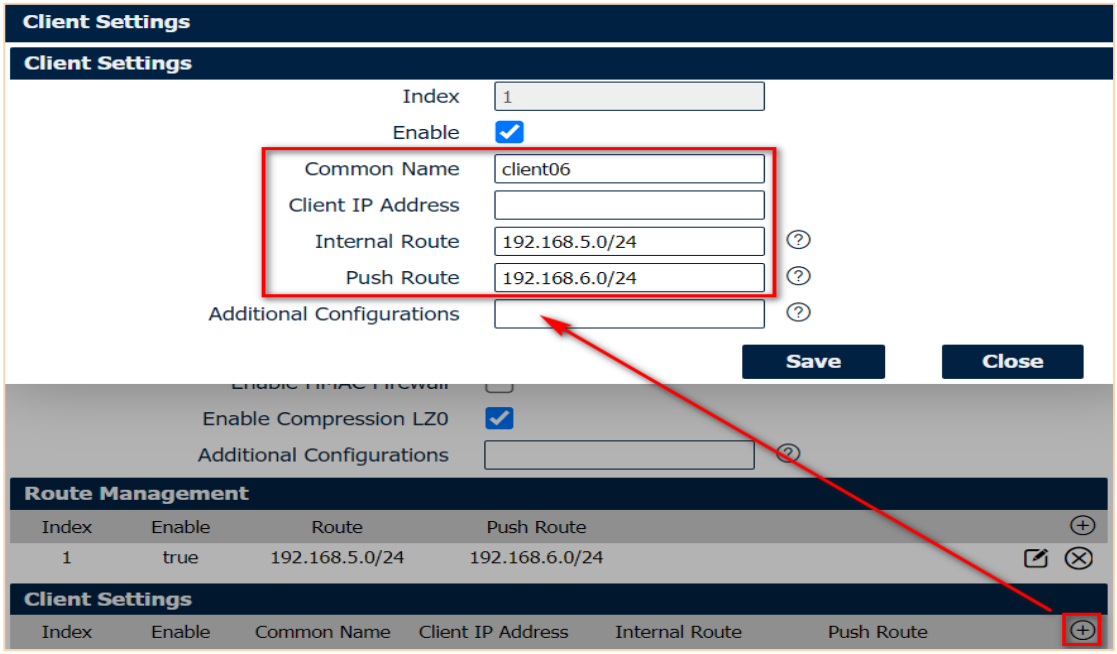
Step 1. Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as shown below. Click Save.



Step 2. Go to Router Management and configure the route as shown below, then, click "Save".

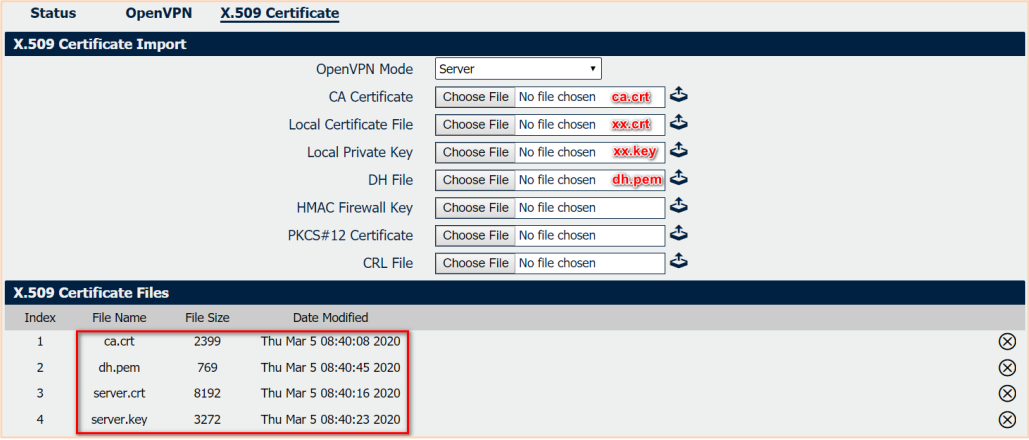


Step 3: Go to Client Settings as shown below, click "Save":



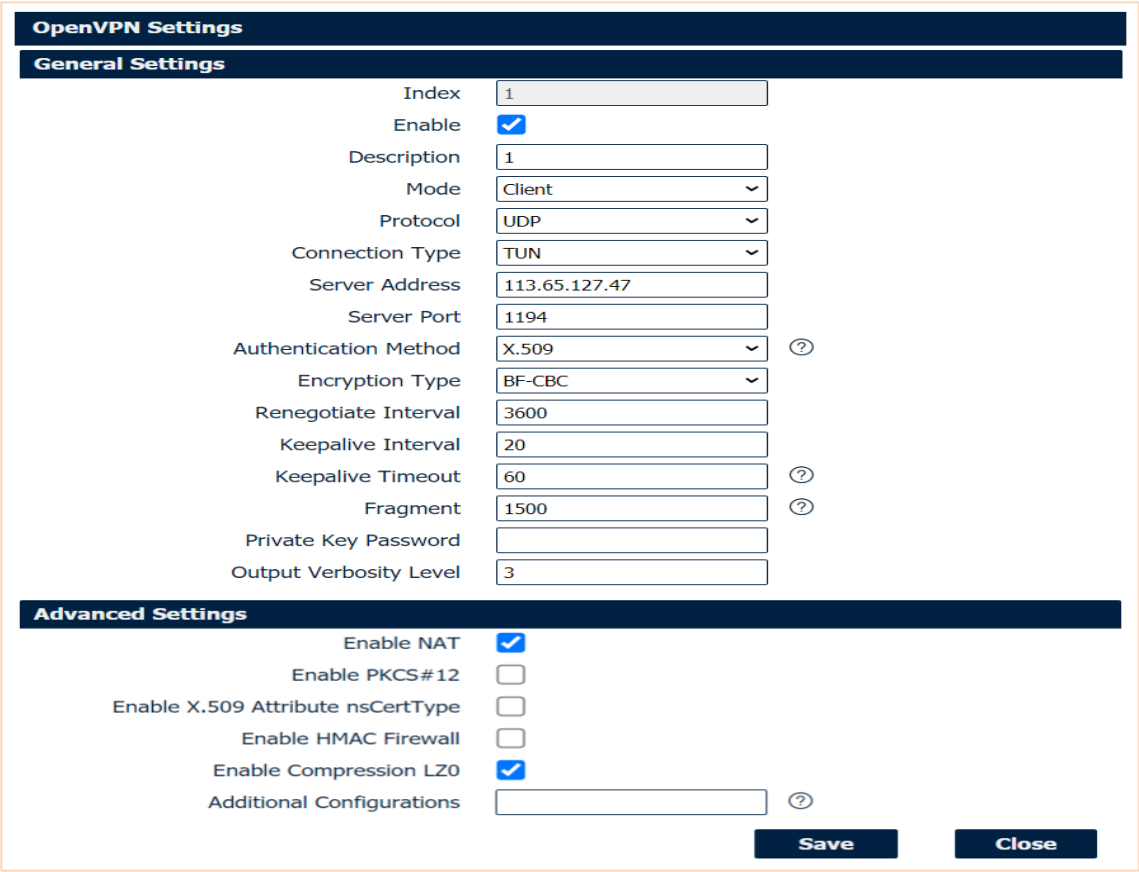
Step 4: After that, click Save>Apply.

Step 5: Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:

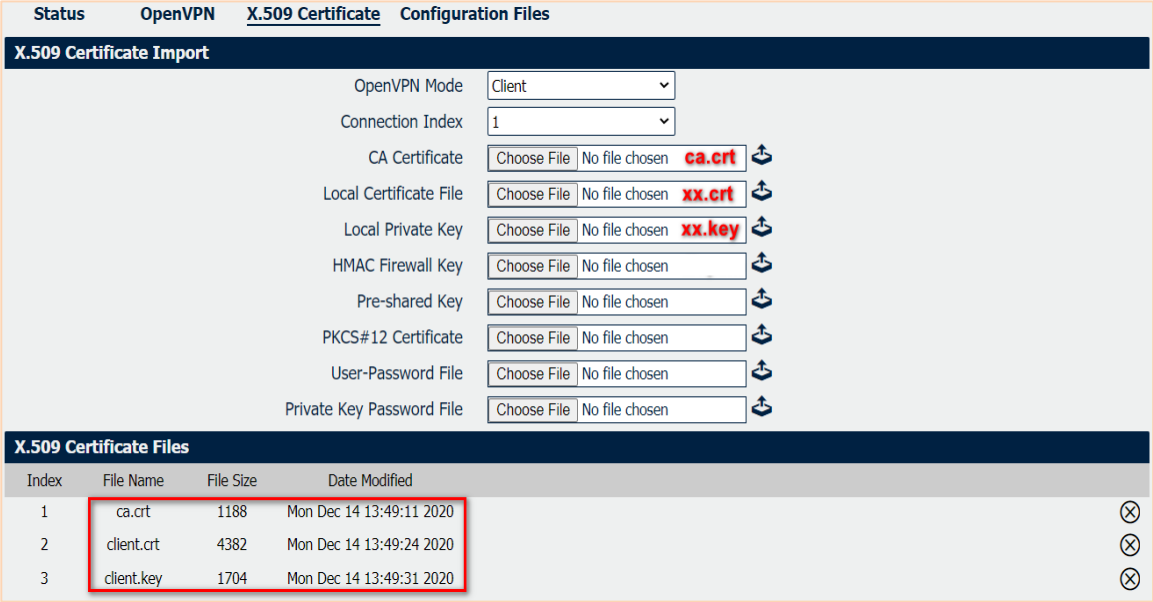


Client Configuration

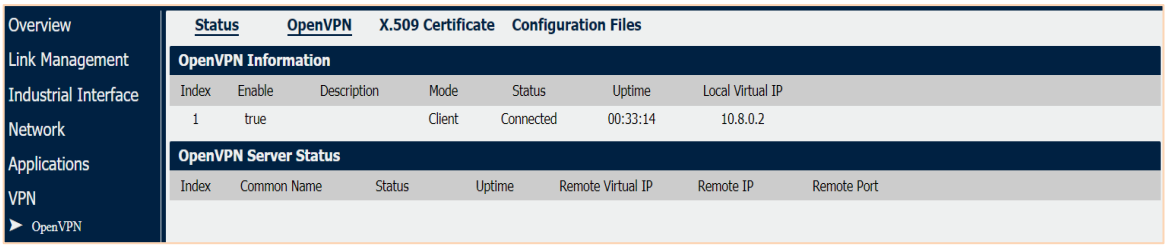
Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



Step 2: Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:

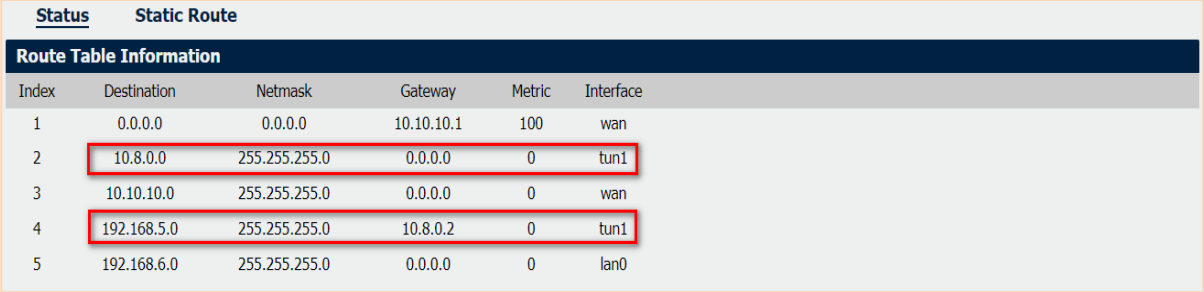


Step 3: Click Apply. The Client has connected to the Server successfully:



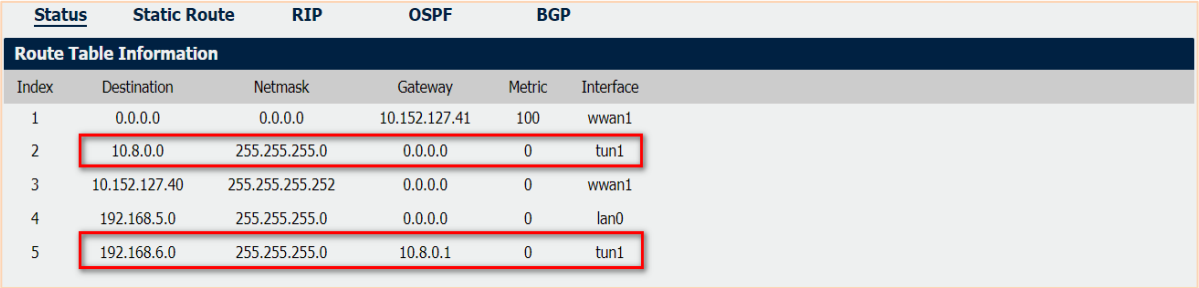
Routing Tables

Step 1: Check the Routing Table on the OpenVPN Server for reference.



Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.10.10.1	100	wan
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.10.10.0	255.255.255.0	0.0.0.0	0	wan
4	192.168.5.0	255.255.255.0	10.8.0.2	0	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	0	lan0

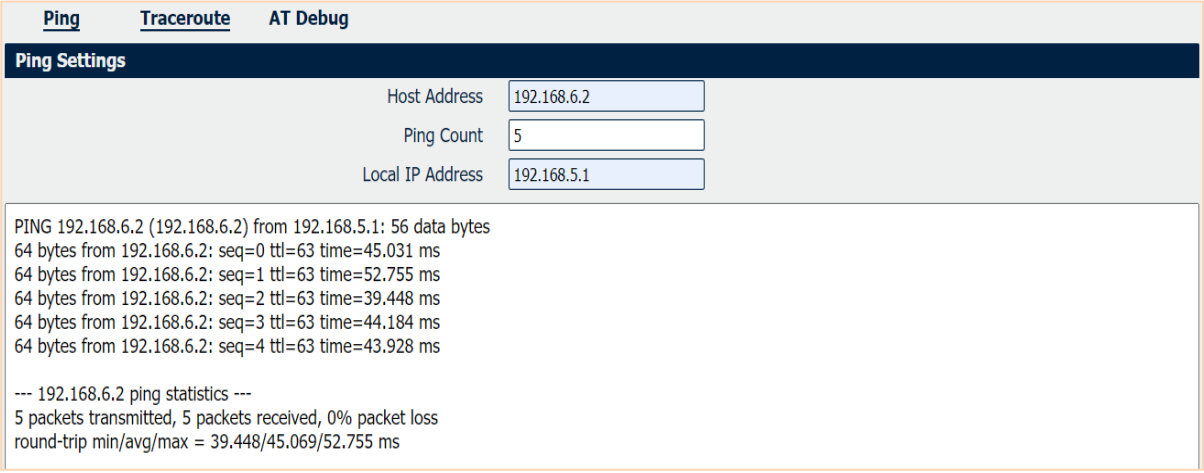
Step 2: Check the Routing Table on the OpenVPN Client for reference.



Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.152.127.41	100	wwan1
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.152.127.40	255.255.255.252	0.0.0.0	0	wwan1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.1	0	tun1

Testing

Step 1: Go to **Maintenance>Debug Tool>Ping** and Ping from OpenVPN Client to OpenVPN Server LAN Device.



Step 2: Go to **Maintenance>Debug Tool>Ping** and Ping from OpenVPN Server to OpenVPN Client LAN Device.

Step 3: Test successfully.

11.12. AN058-Open VPN using passwords between two 6944's

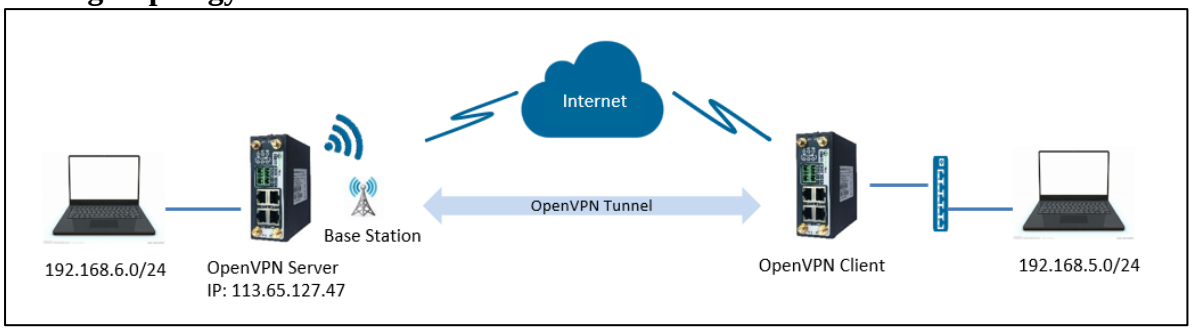
Overview

This document contains information regarding the configuration and use of OpenVPN with passwords between two 6944's, one working as a client and the other as a server

Software Version

Release Date	Doc. Version	Firmware	Additional Software	Change Description
14.12.2020	V1.1	V1.1.4 (0c0c9fa)	Standard Software	First release

Testing Topology

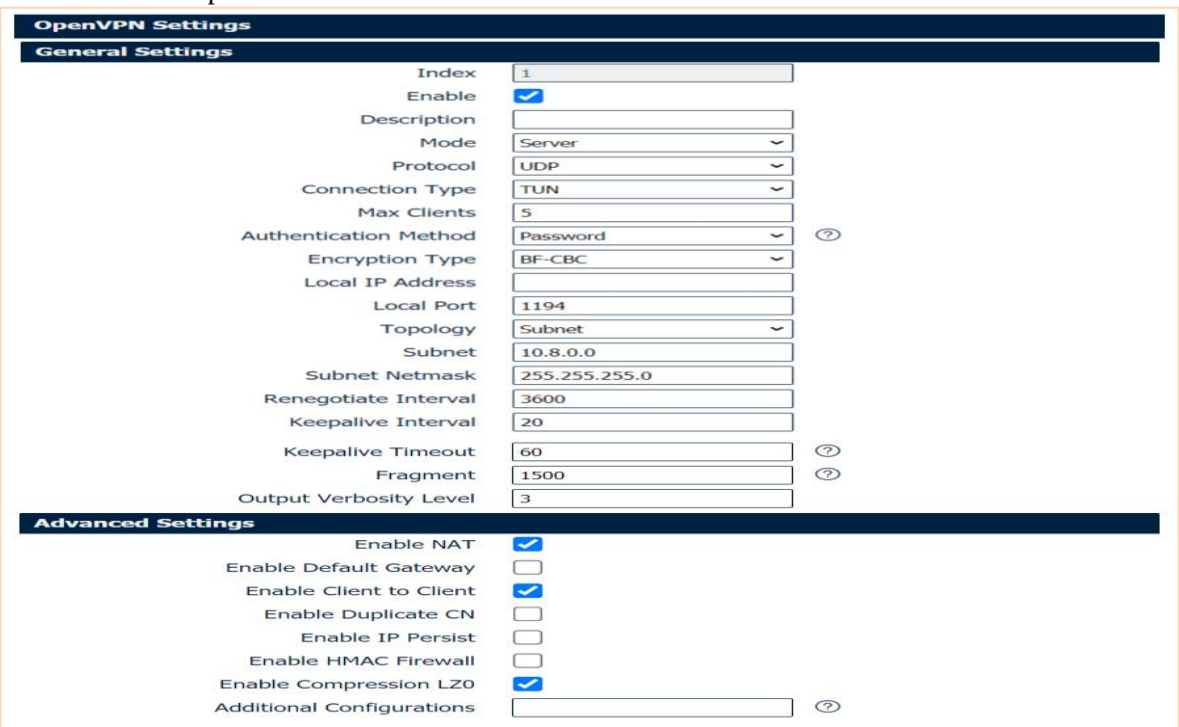


- The 6944 Router runs as OpenVPN Server with Public IP address or Domain Name, which can be accessed by another 6944 as OpenVPN Client successfully.
- Two PCs are connected, one to the LAN of the OpenVPN Server and one to the OpenVPN Client on their subnets.
- An OpenVPN tunnel is established between the Server and the Client, the subnet can PING each other successfully

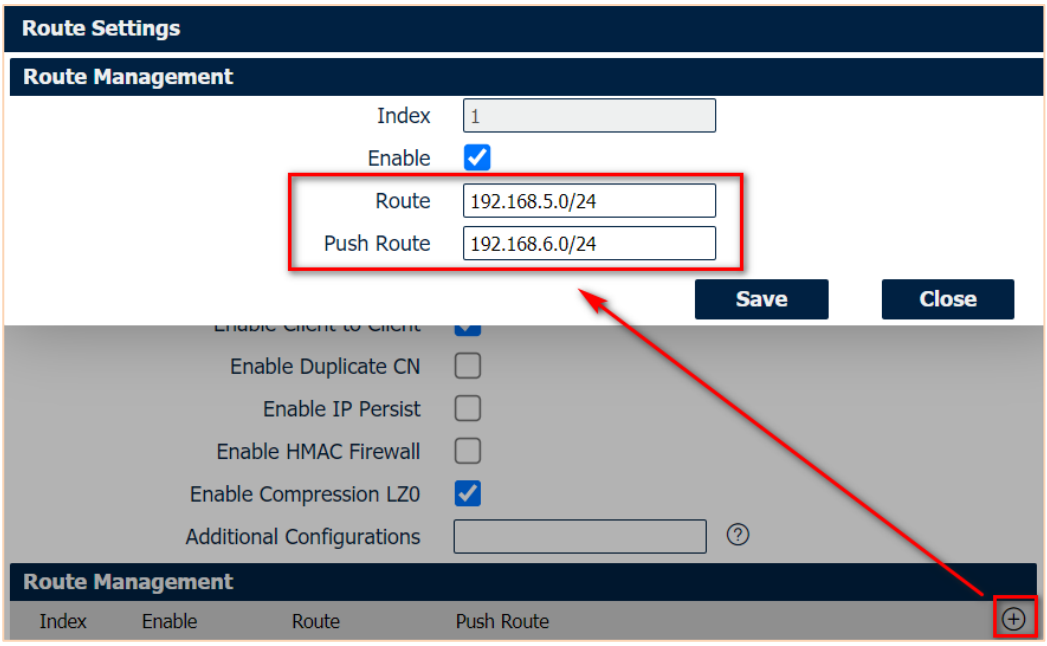
Configuration

Server Configuration

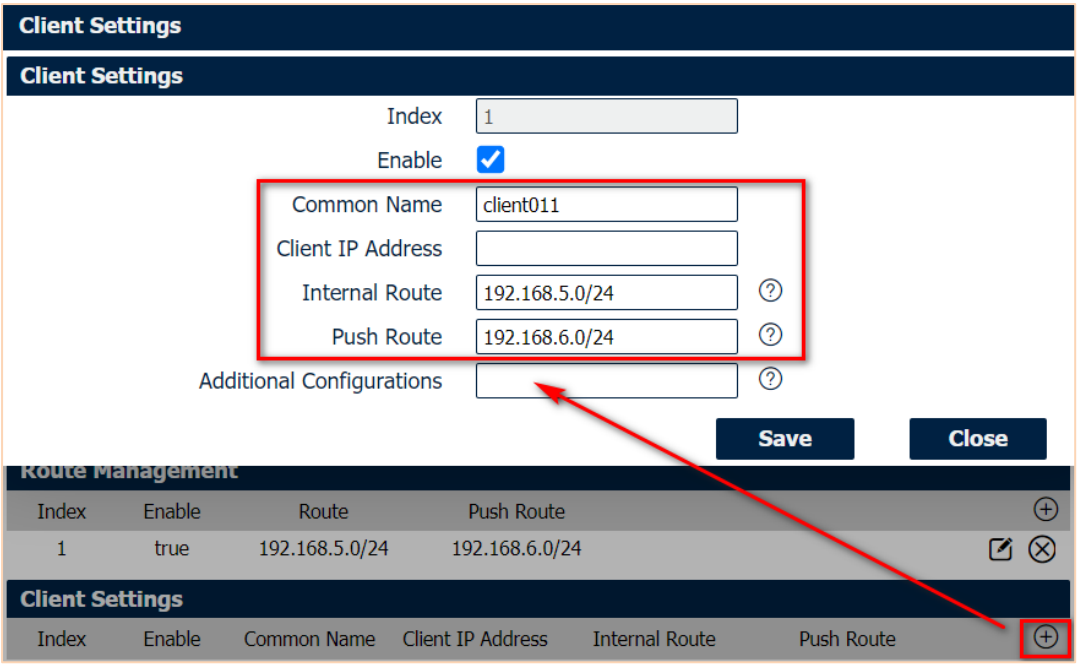
Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as below picture. Click Save.



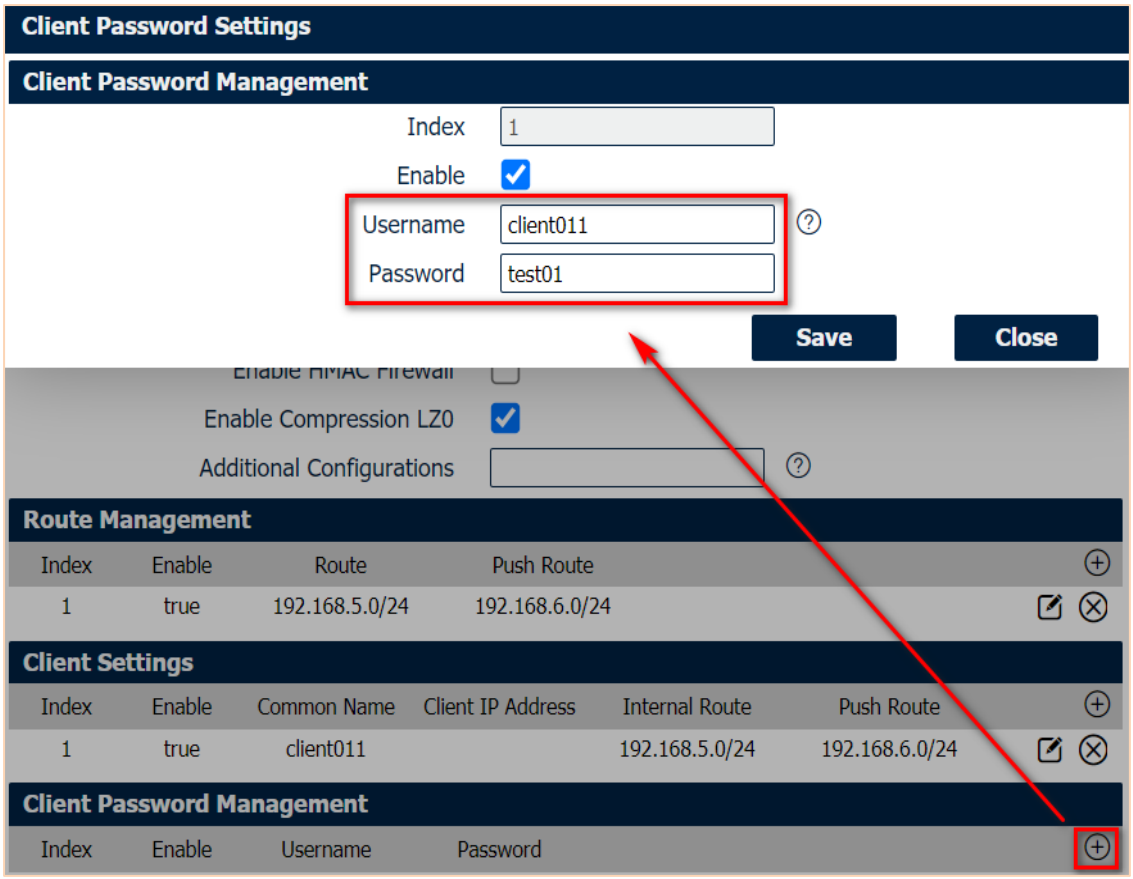
Step 2: Configure the Router Management as shown below, click "Save".



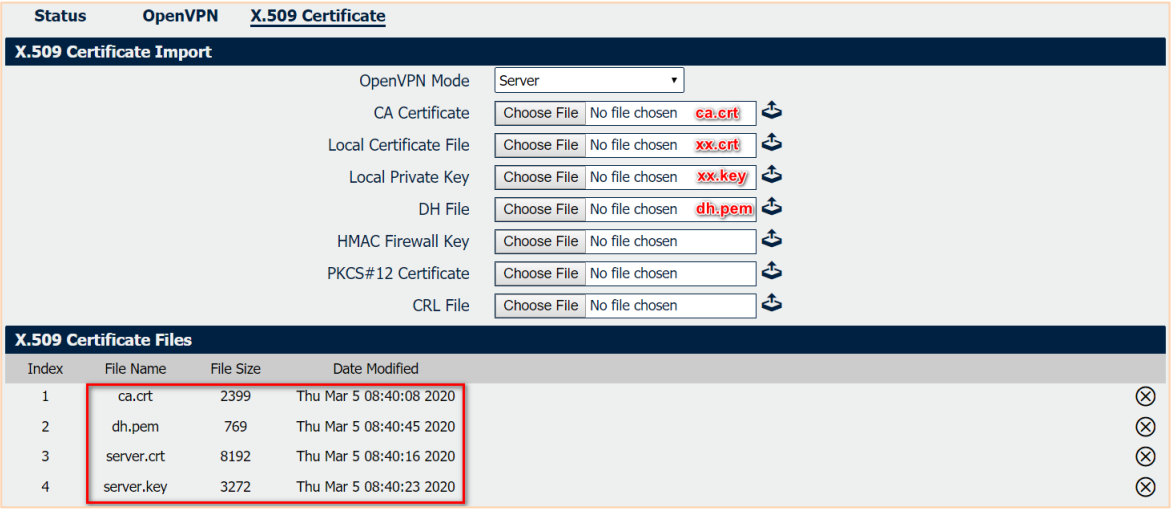
Step 3: Configure the 6944 Client as shown below, then click "Save":



Step 4: Configure the Client Password Management as shown below, then click "Save":



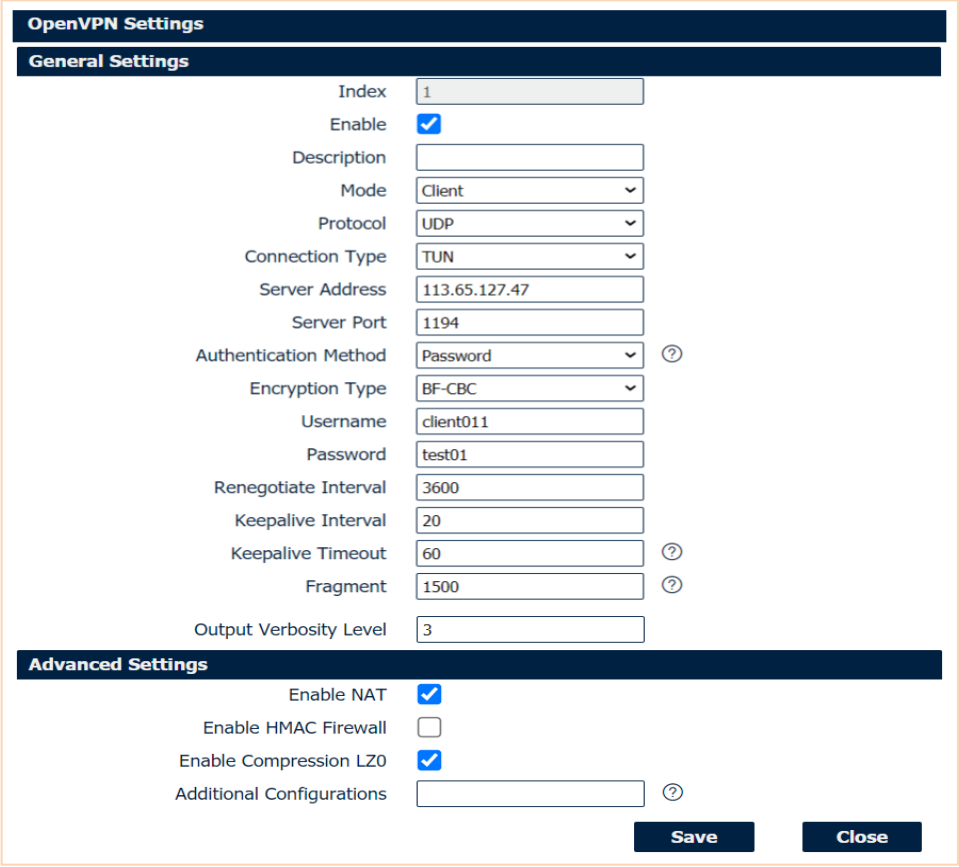
Step 5: Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:



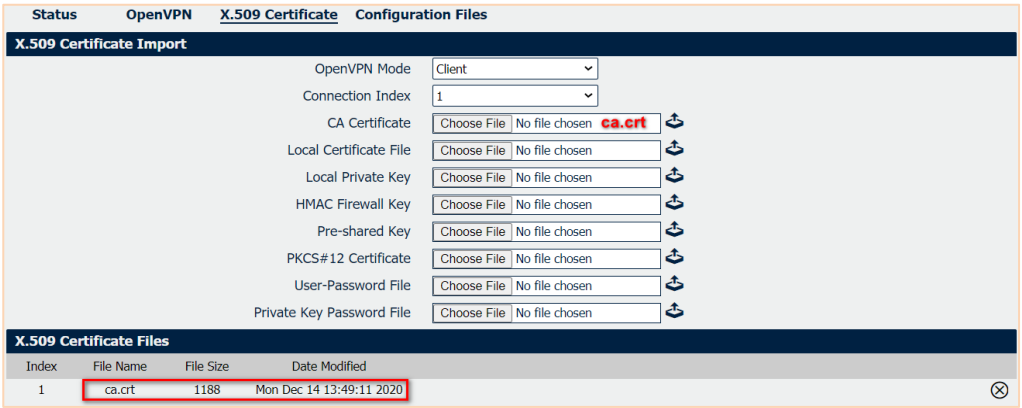
Step 6: Click Apply.

Client Configuration

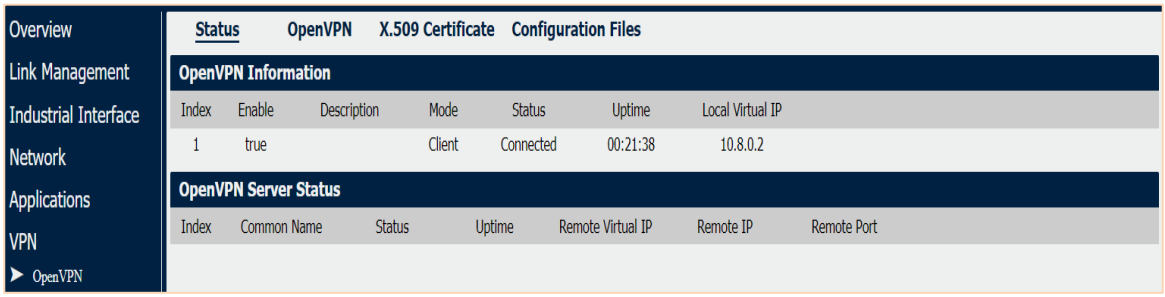
Step 1: Go to **VPN>OpenVPN>OpenVPN>General Settings**, click the Edit Button and configure OpenVPN as shown below. Click Save



Step 2: Go to VPN>OpenVPN>X.509 Certificate, import the related certificates:



Step 3: Click Apply. Ensure the Client has connected to the Server:



Checking the Routing Table

Step 1: Check the Routing Table on the OpenVPN Server for reference.

Status Static Route

Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.10.10.1	100	wan
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.10.10.0	255.255.255.0	0.0.0.0	0	wan
4	192.168.5.0	255.255.255.0	10.8.0.2	0	tun1
5	192.168.6.0	255.255.255.0	0.0.0.0	0	lan0

Step 2: Check the Routing Table on the OpenVPN Client for reference.

Status Static Route RIP OSPF BGP

Route Table Information

Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	10.152.127.41	100	wwan1
2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	10.152.127.40	255.255.255.252	0.0.0.0	0	wwan1
4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	192.168.6.0	255.255.255.0	10.8.0.1	0	tun1

Testing

Step 1: Go to **Maintenance>Debug Tool>Ping** and Ping from the OpenVPN Client to OpenVPN Server LAN Device.

Ping Traceroute AT Debug

Ping Settings

Host Address: 192.168.6.2
Ping Count: 5
Local IP Address: 192.168.5.1

```
PING 192.168.6.2 (192.168.6.2) from 192.168.5.1: 56 data bytes
64 bytes from 192.168.6.2: seq=0 ttl=63 time=45.031 ms
64 bytes from 192.168.6.2: seq=1 ttl=63 time=52.755 ms
64 bytes from 192.168.6.2: seq=2 ttl=63 time=39.448 ms
64 bytes from 192.168.6.2: seq=3 ttl=63 time=44.184 ms
64 bytes from 192.168.6.2: seq=4 ttl=63 time=43.928 ms

--- 192.168.6.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 39.448/45.069/52.755 ms
```

Step 2: Go to **Maintenance>Debug Tool>Ping** and Ping from the OpenVPN Server to the OpenVPN Client's LAN Device

Ping Traceroute AT Debug

Ping Settings

Host Address: 192.168.5.2
Ping Count: 5
Local IP Address: 192.168.6.1

```
PING 192.168.5.2 (192.168.5.2) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.5.2: seq=0 ttl=63 time=34.432 ms
64 bytes from 192.168.5.2: seq=1 ttl=63 time=44.027 ms
64 bytes from 192.168.5.2: seq=2 ttl=63 time=38.660 ms
64 bytes from 192.168.5.2: seq=3 ttl=63 time=44.314 ms
64 bytes from 192.168.5.2: seq=4 ttl=63 time=54.063 ms

--- 192.168.5.2 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 34.432/43.099/54.063 ms
```

12 IP SEC

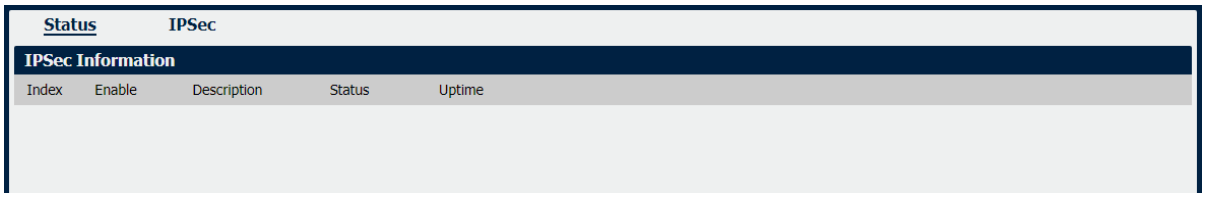
12.1. IP Sec Overview

Overview

IPSec provides secure communication tunnels between devices. The various tunnel configurations will be displayed in the Tunnel Table at the bottom of the page. All tunnels are created using the ESP (Encapsulating Security Payload) protocol.

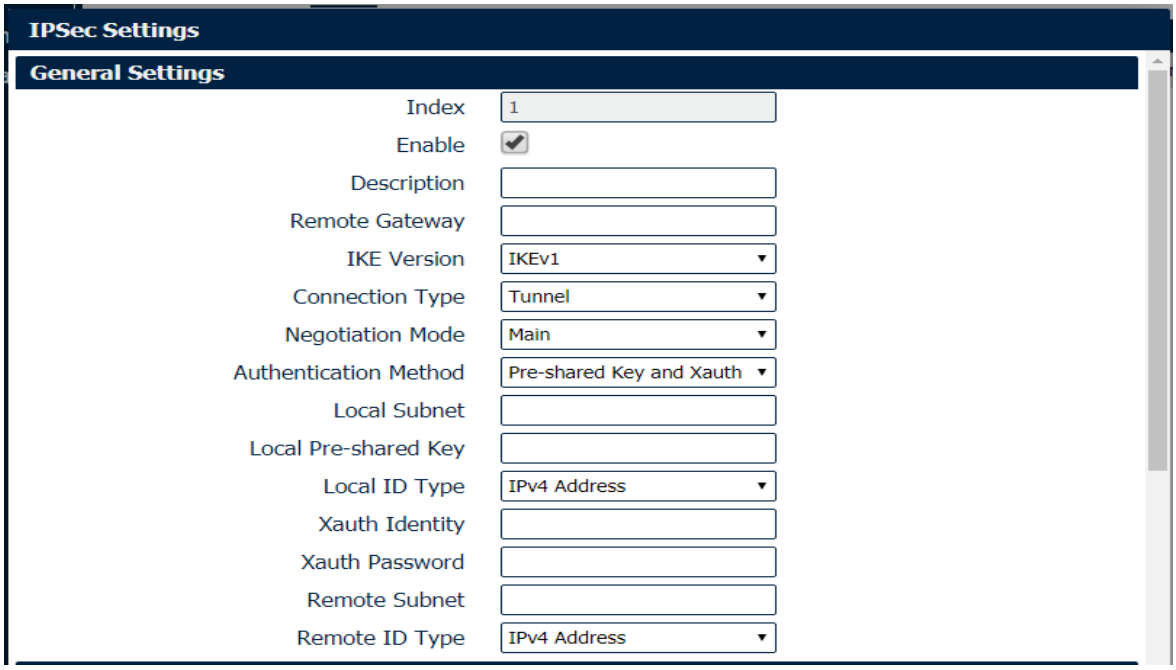
Basic Configuration

Go to VPN> IP Sec



VPN->IPSec->Status

- **Enable**
  Displays current IPSec settings is enable or disable.
- **Description**
  Displays the description of current VPN channel.
- **Status**
  Displays the current VPN connection status.
- **Uptime**
  Displays the connection time since VPN is established.

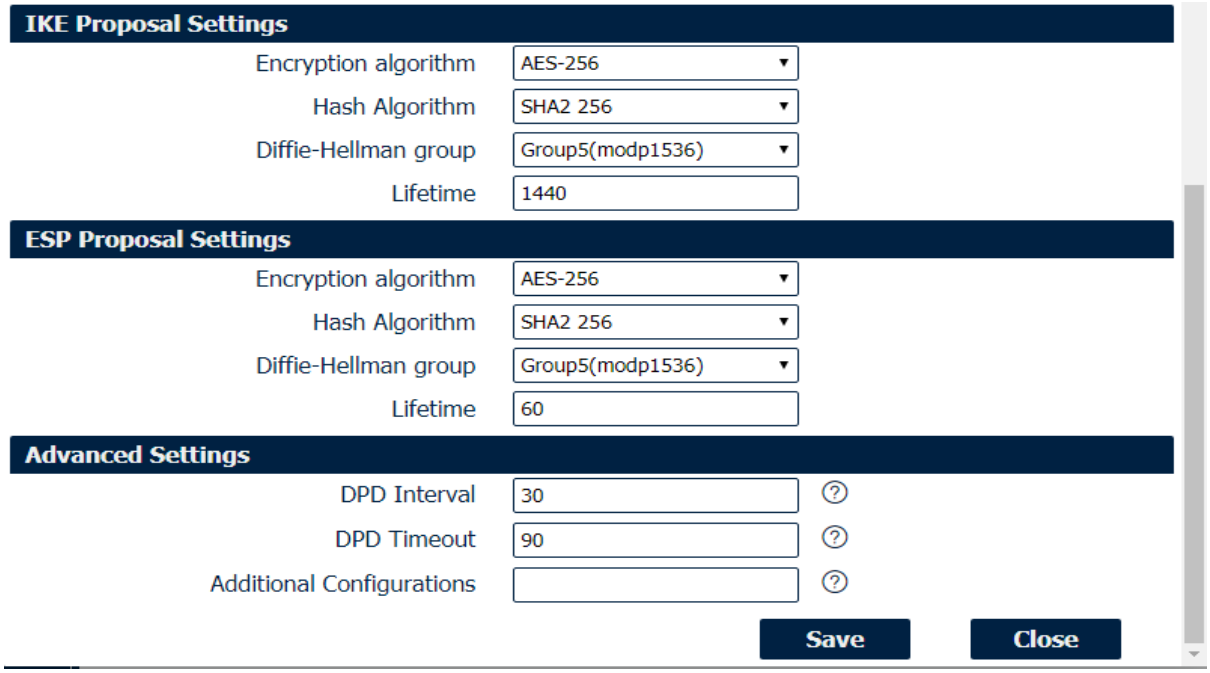


VPN->IPSec

- **Enable -** Select Enable will launch the IPSec process.
- **Description -** Enter a description for this IPSec VPN tunnel.
- **Remote Gateway -** Enter the IP address of the remote endpoint of the tunnel.
- **IKE Version -** Internet Key Exchange, select from “IKEv1” or “IKEv2”.
- **Connection Type**
  Select from “Tunnel” or “Transport”.

  Tunnel: In tunnel mode, the entire IP packet is encrypted and authenticated. It is then encapsulated into a new IP packet with a new IP header. Tunnel mode is used to create virtual private networks for network-to-network communications.

  Transport: In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted.
- **Negotiation Mode -** Select from “Main” or “Aggressive”.
- **Authentication Method -** Select from “Pre-shared Key” or “Pre-shared Key and Xauth”.
- **Local Subnet -** Ener the IP address with the sub-mask if the network beyond the local LAN will be sending packets through the tunnel.
  NOTE: The Remote subnet and Local subnet addresses must not overlap!
- **Local Pre-shared Key -** Enter the pre-shared key which match the remote endpoint.
- **Local ID Type -** The local endpoint's identification. The identifier can be a host name or an IP address.
- **Xauth Identity -** Enter Xauth identity after “Pre-shared Key and Xauth” on authentication Method is enabled.
- **Xauth Password -** Enter Xauth password “Pre-shared Key and Xauth” on authentication Method is enabled.
- **Remote Subnet -** Enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address.
  NOTE: The Remote subnet and Local subnet addresses must not overlap!
- **Remote ID Type -** The authentication address of the remote endpoint.



VPN->IPSec

- **Encryption Algorithm (IKE) -** Select 3DES AES-128, AES-192, or AES-256 encryption.
- **Hash Algorithm (IKE) -** Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- **Diffie-Hellman Group (IKE) -** Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- **Lifetime (IKE) -** How long the keying channel of a connection should last before being renegotiated.
- **Encryption Algorithm (ESP) -** Select 3DES AES-128, AES-192, or AES-256 encryption.
- **Hash Algorithm (ESP) -** Select from MD5, SHA1, SHA2 256, SHA2 384 or SHA2 512 hashing.
- **Diffie-Hellman Group (ESP) -** Negotiate (None) or use 768 (Group 1), 1024 (Group 2), 1536 (Group 5) or 2048 (Group 14) etc.
- **Lifetime (ESP) -** How long a particular instance of a connection should last, from successful negotiation to expiry.
- **Dead Peer Interval -** Enter the interval after which DPD is triggered if no IPsec protected packets is received from the peer.
- **Dead Peer Detection – Timeout -** Enter the remote peer probe response timer.
- **Additional Configurations -** Enter some other options of IPSec in this field. Each expression can be separated by a ‘;’.

12.2. AN012 – IP Sec with Pre-Shared Key to Cisco

Overview

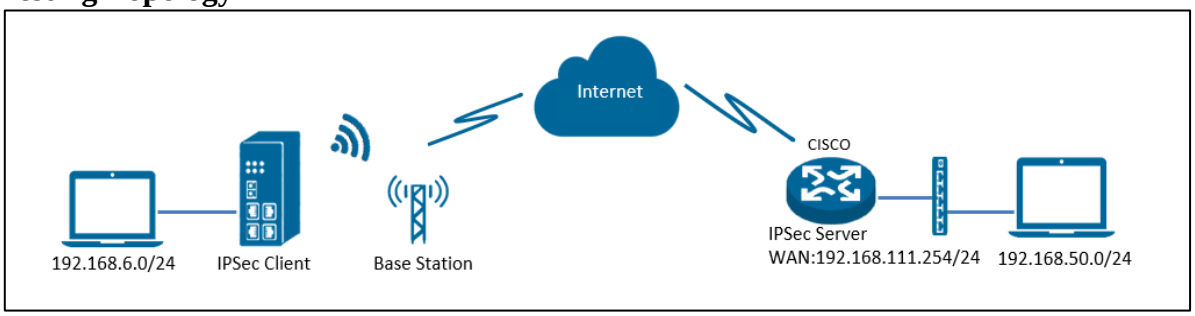
This document contains information regarding the configuration of a 6944 Industrial router running IP Sec with a pre-shared key to a Cisco router.

Software Version

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional sw	Change Description
3.8.2018	V1.1	V1.1.4 (0c0c09fa)	Std Software	First released

Testing Topology



- The 6944 runs as an IPSec Client capable of pinging an, IPSec server successfully.
- The CISCO router runs as an IPSec Server with a static public IP Address.
- An IPSec tunnel is established between the 6944 and Cisco router.

Configuration

Server Configuration

Step : Login to CISCO router and configure as shown below:

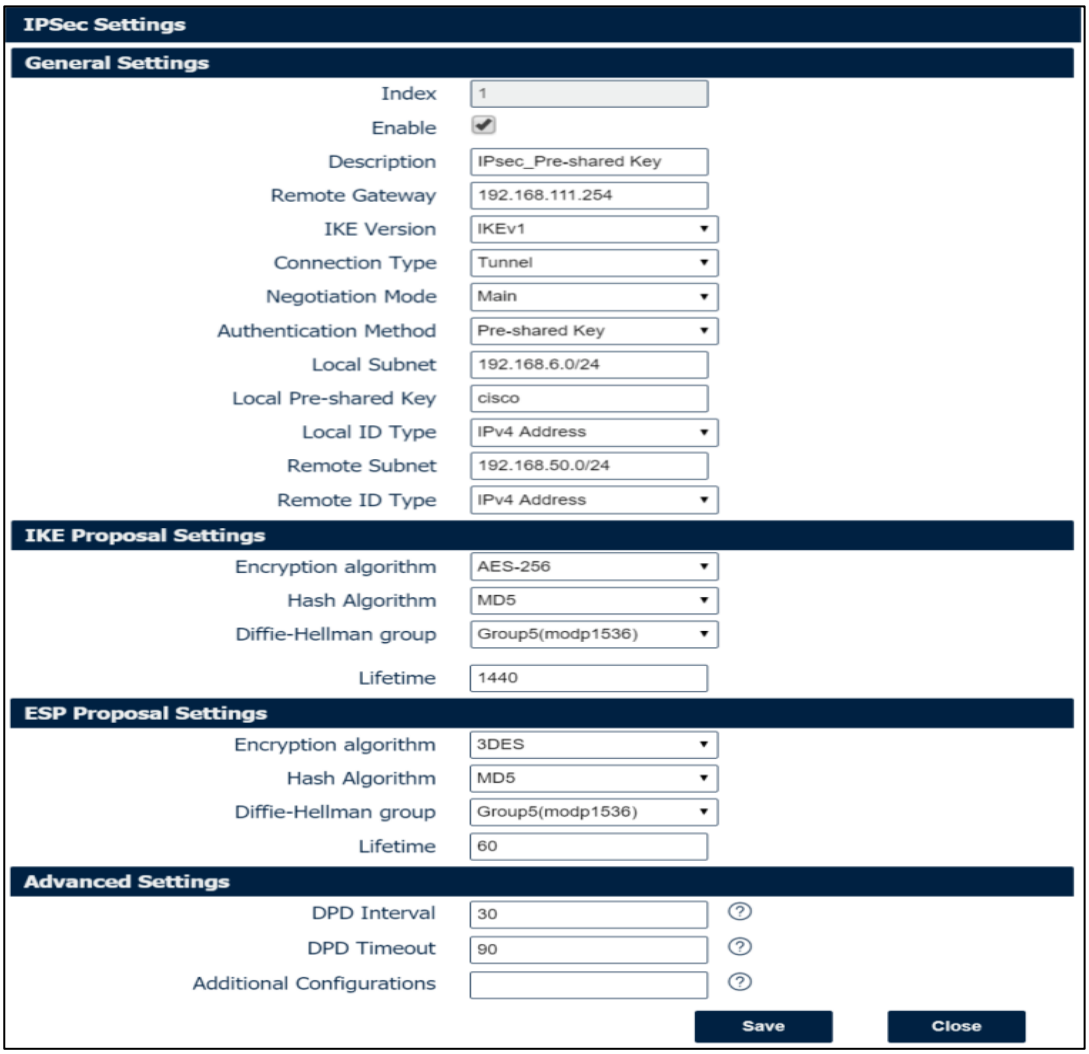
==========

```
cisco2811#show running-config
Building configuration...
Current configuration : 3071 bytes
!
version 12.4
hostname cisco2811
logging message-counter syslog
enable secret 5
$1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
!
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
 hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0
0.0.0.0
!
crypto ipsec transform-set 6944 esp-3des esp-
md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set 6944
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic
DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
```

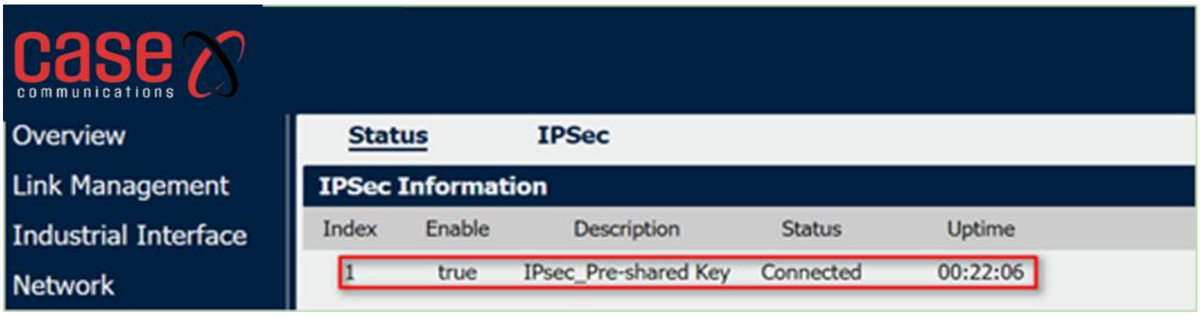
```
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
end
cisco2811#
```

Client Configuration (on 6944)

Step 1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as shown below . **Click Save> Apply**



Step 3: Check to see if the IP-Sec tunnel has connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

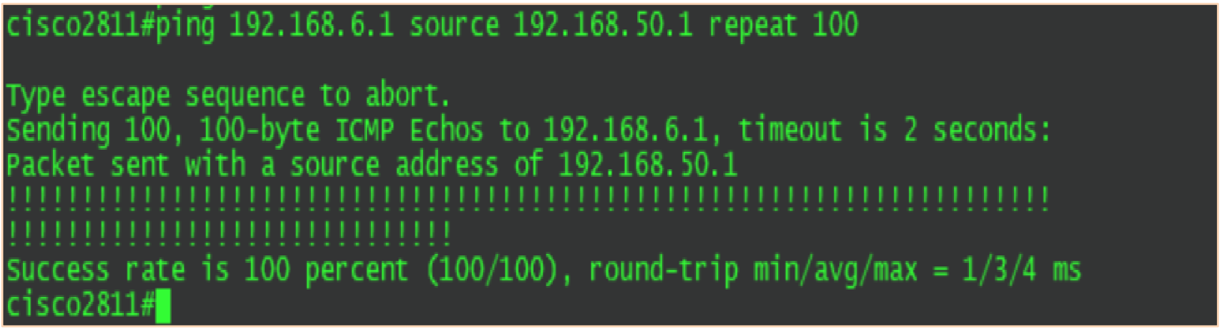


IPSec Information

Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

Testing

Step 1: Ping from the CISCO router to the 6944, LAN to LAN to make sure its working correctly



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

1. Ping from the 6944 to the CISCO router, LAN to LAN communication is working correctly.

12.3. AN013 - IP Sec and FQDN to a Cisco router

Overview

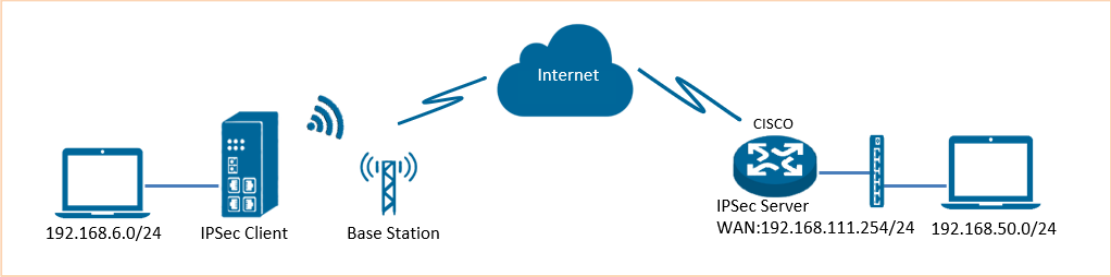
This document contains information regarding a 6944 running IP Sec and FQDN to a Cisco router

Software Version

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional software	Change Description
3.8.2018	V1.1	V1.1.4 (0c0c09fa)	Std Software	First released

Testing Topology



- The 6944 runs as an IPSec Client with an IP address, which can ping an IP Server using IPSec
- The CISCO router runs as an IPSec Server with a static public IP Address.
- An IPSec tunnel is established between the 6944 and the Cisco router

Configuration

Server Configuration

Step 1: Login to the CISCO router and configure it as shown below:

==========

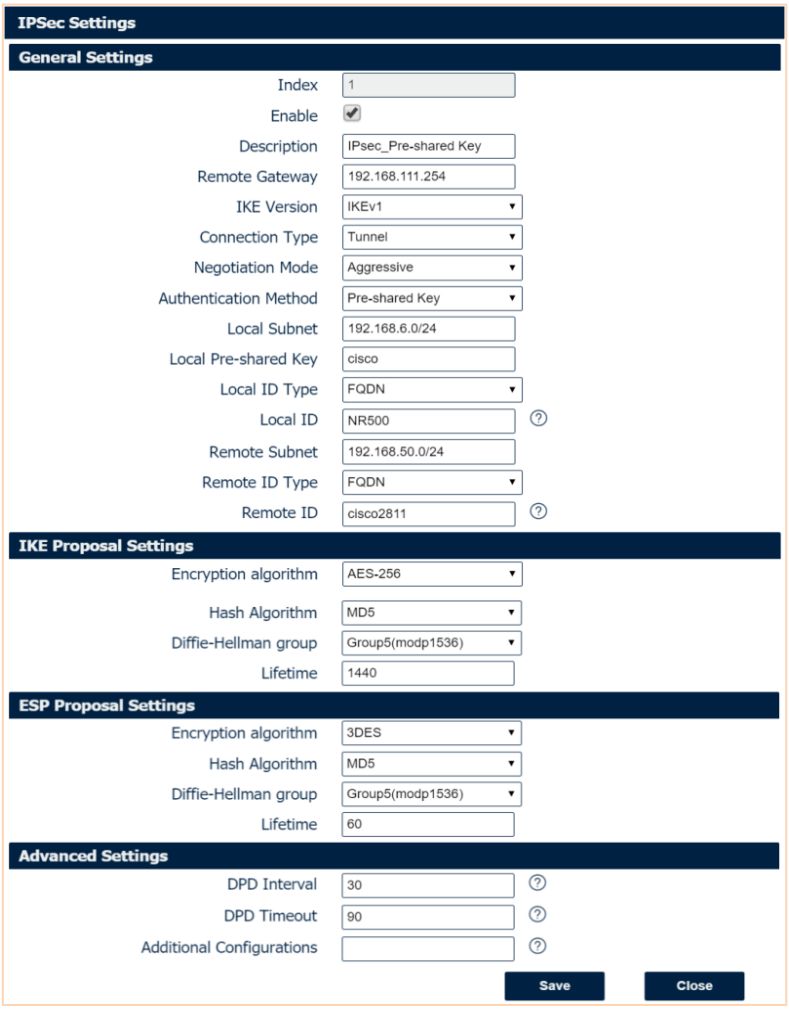
```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5
$1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
ip cef
!
ip name-server 192.168.111.1
ip address-pool local
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco hostname 6944
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password cisco
 set aggressive-mode client-endpoint fqdn
6944
!
crypto ipsec transform-set 6944 esp-3des esp-
md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set 6944
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic
DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
```

```
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map SMAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
!
end
cisco2811#
```

==========

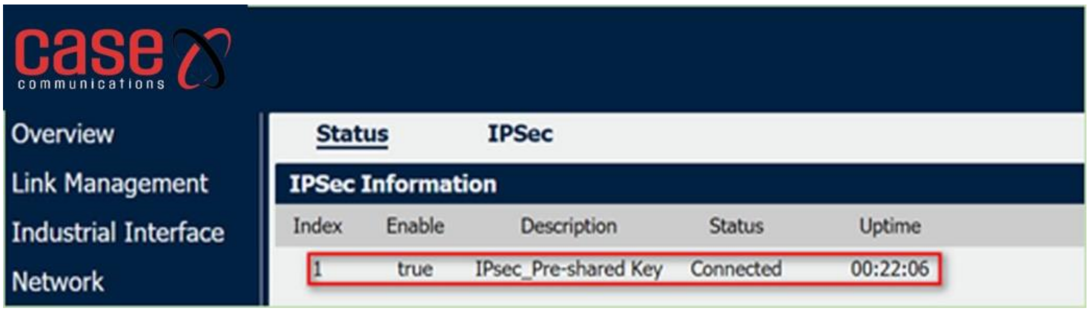
Client Configuration

Step 1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as shown below. Click Save.



Step 2: Click Save>Apply.

Step 3: IPSec had been connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

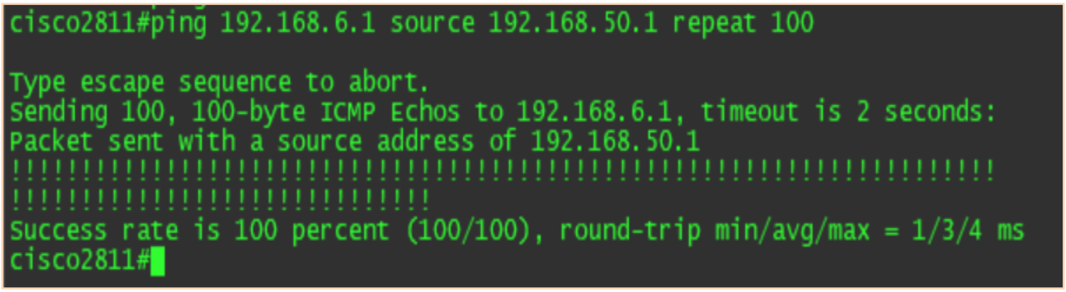


Index	Enable	Description	Status	Uptime
1	true	IPsec_Pre-shared Key	Connected	00:22:06

s

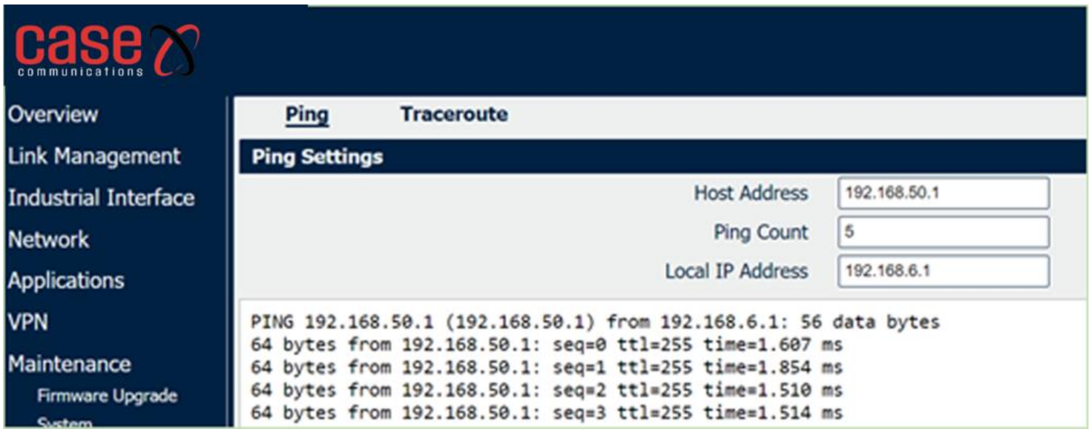
Testing

Step 1: Ping from a CISCO router to the 6944, LAN to LAN communication is working correctly.



```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Step 2: Ping from the 6944 to the CISCO router, LAN to LAN communication is working correctly.



Host Address: 192.168.50.1
Ping Count: 5
Local IP Address: 192.168.6.1

```
PING 192.168.50.1 (192.168.50.1) from 192.168.6.1: 56 data bytes
64 bytes from 192.168.50.1: seq=0 ttl=255 time=1.607 ms
64 bytes from 192.168.50.1: seq=1 ttl=255 time=1.854 ms
64 bytes from 192.168.50.1: seq=2 ttl=255 time=1.510 ms
64 bytes from 192.168.50.1: seq=3 ttl=255 time=1.514 ms
```

Step 3: Test successful.

12.4. AN014 -IP Sec with Pre-Shared Key to a Cisco Router

Overview

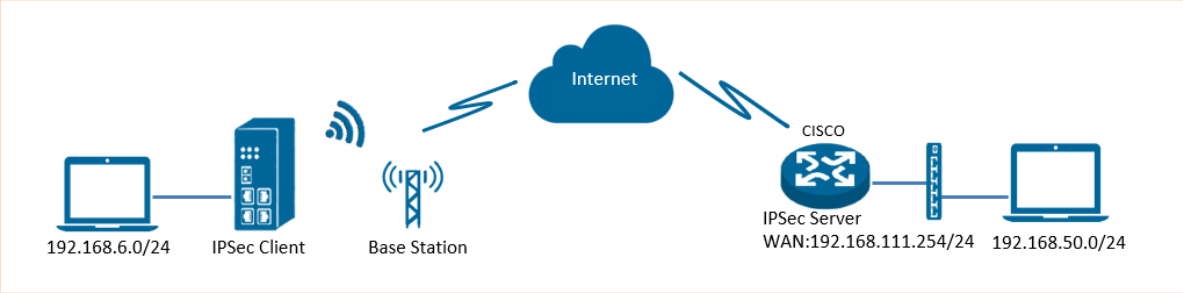
This document contains information regarding configuring a 6944 running IP Sec with a Pre-Shared Key to a Cisco router.

Software Version

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional software	Change Description
3.8.2018	V1.1	V1.1.4 (0c0c09fa)	Std Software	First release

Testing Topology



- The 6944 runs as an IPSec Client which can run over an IPSec Tunnel to an IP Server.
- The CISCO router runs as an IPSec Server with a static public IP address.
- An IPSec tunnel is established between the 6944 and Cisco router.

Configuration

Server Configuration

Step 1. Login to the CISCO router and setting like below:

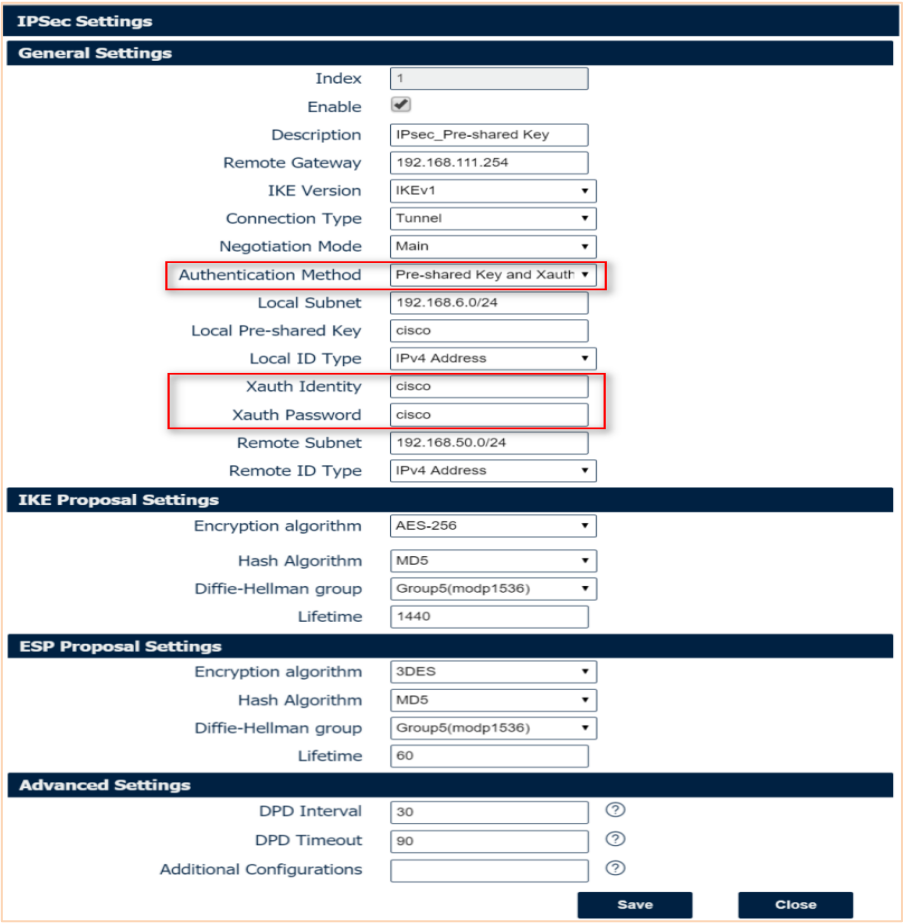
==========

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
enable secret 5
$1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.
aaa new-model
aaa authentication login LOGIN local
!
aaa session-id common
dot11 syslog
ip source-route
!
ip cef
ip domain name cisco.com
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco address 0.0.0.0
0.0.0.0
!
crypto ipsec transform-set 6944 esp-3des esp-
md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set 6944
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list
LOGIN
crypto map MAP 10 ipsec-isakmp dynamic
DYN
!
track 1 interface FastEthernet0/0 line-protocol
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
```

```
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
!!
line con 0
line vty 5 15
 exec-timeout 5 2
end
```

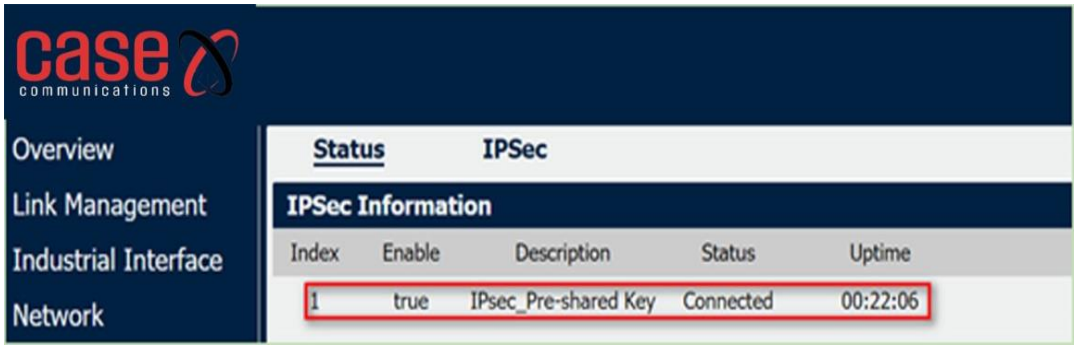
Client Configuration

Step1: Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as shown below. Click Save.



2. Click Save>Apply.

Step 3: If the IPSec tunnel has connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

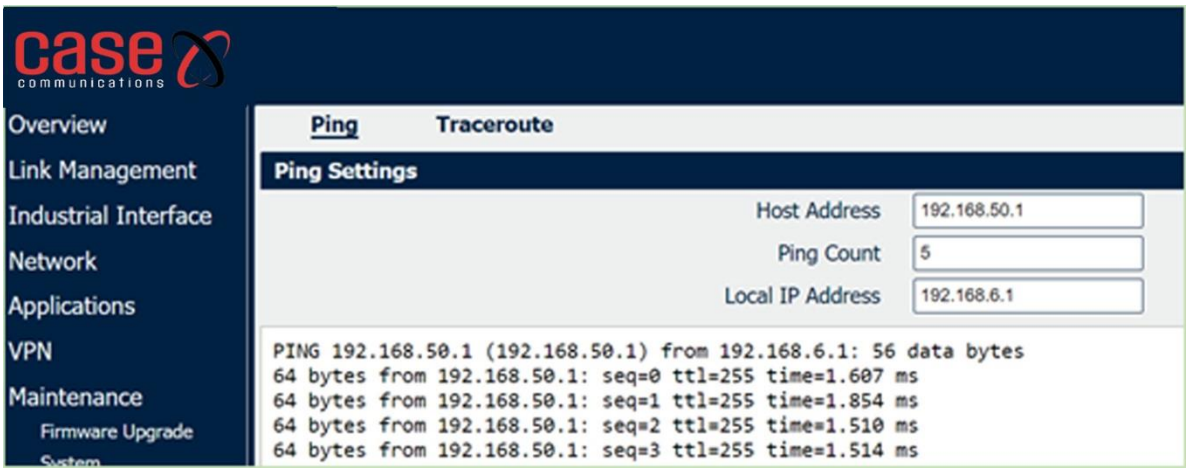


Testing

Step 2: Ping from the CISCO router to the 6944, LAN to LAN to ensure the VPN is working.

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Step 3: Ping from the 6944 to the CISCO router, to ensure LAN to LAN communication is working correctly.



Step 4: Test successful.

12.5. AN015 - IP Sec with a Pre-shared Key to Cisco Router

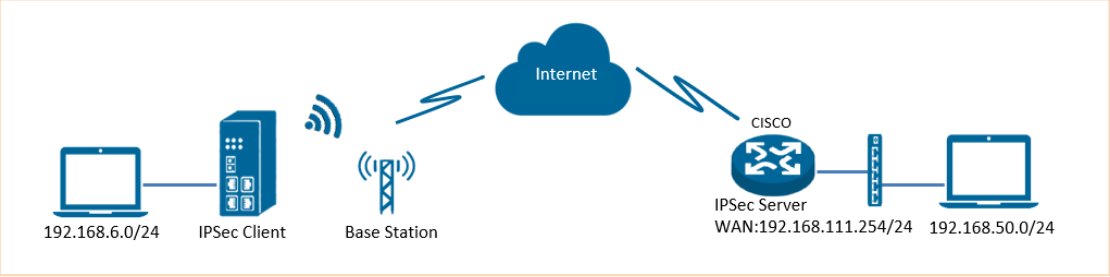
Overview

This document contains information regarding the configuration of a 6944 Industrial router running IP Sec and FQDN with a pre-shared Key to a Cisco router

Software Versions

Release Date	Doc. Version	Firmware Version	Change Description
2018/08/03	V1.0.0	V1.0.0(903.0)	First released

Testing Topology



- The 6944 runs as an IPSec Client which can ping over an IPSec Tunnel to an IP Server.
- The CISCO router runs as an IPSec Server with a **static public IP** address.
- An IP-Sec tunnel is established between the 6944 and Cisco router.

Configuration

Server Configuration

Step1: Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure IPSec VPN as Shown below then. Click Save.

Step 2: Login to CISCO router and configure as shown below:

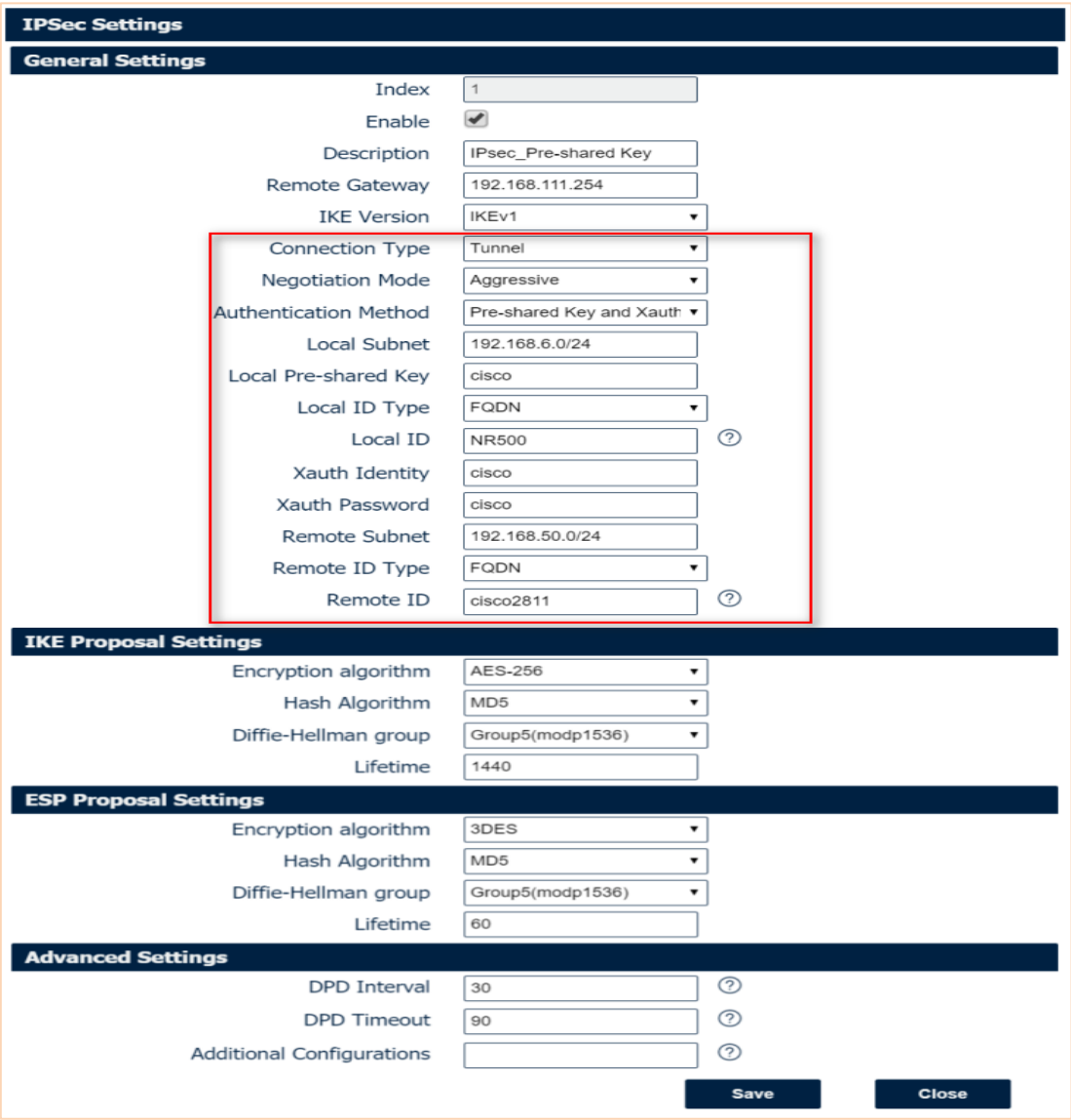
==========

```
cisco2811#show running-config
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5
$1$tw/d$UQQ3Xh06n.2HHFeAVIgXJ.!
aaa new-model
!
aaa authentication login LOGIN local
!
aaa session-id common
!
ip name-server 192.168.111.1
ip address-pool local
!
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key cisco hostname 6944
crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password ken
 set aggressive-mode client-endpoint fqdn
cisco2811
!
crypto ipsec transform-set 6944 esp-3des esp-
md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set 6944
 set pfs group5
 match address 101
 reverse-route
!
crypto map MAP client authentication list
LOGIN
crypto map MAP 10 ipsec-isakmp dynamic
DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
```

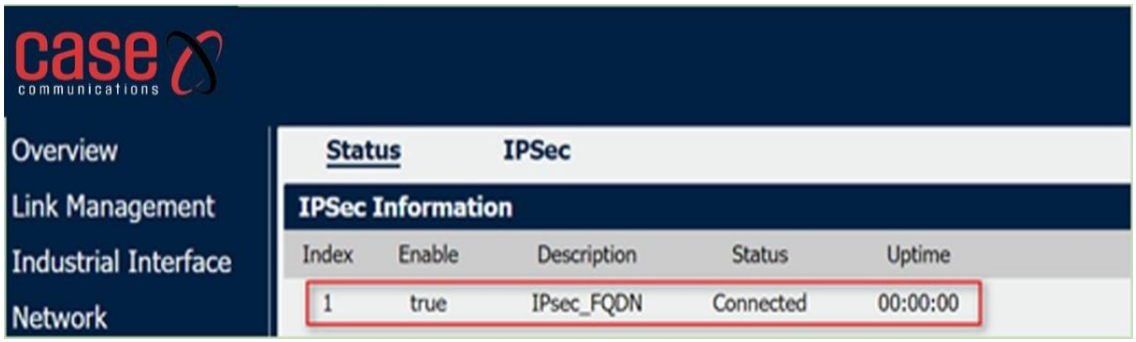
```
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.5.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
 permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
line con 0
line vty 5 15
end
==========================================================
```

Client Configuration

Step 1. Go to **VPN>IPSec>IPSec>General Settings**, click the Edit Button and configure an IPSec VPN as shown below. **Click Save> Apply**



Step 2: If IPSec has connected successfully. Go to **VPN>IPSec>Status** to check the connection status.

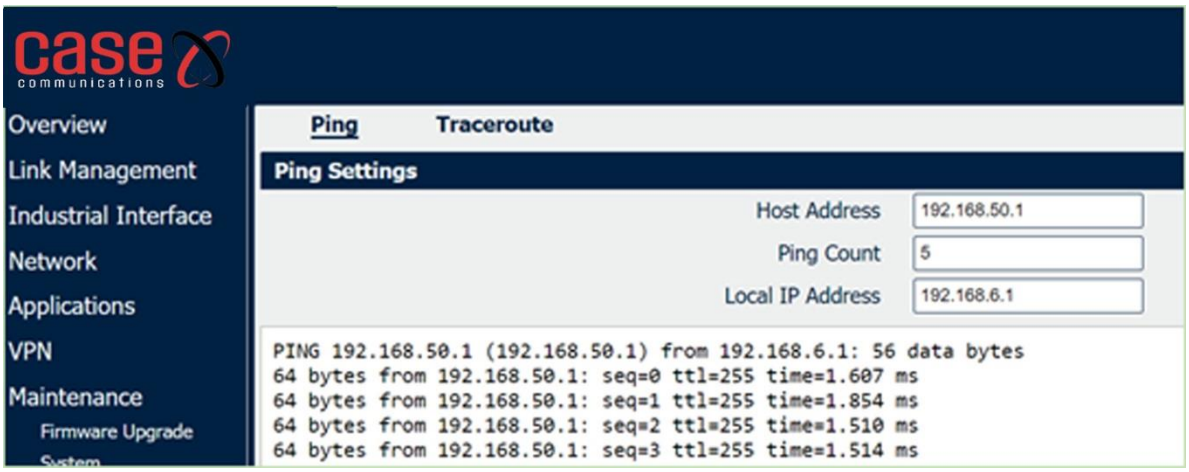


Testing

Step 1: Ping from the CISCO router to 6944 router, to ensure the LAN to LAN communication is working correctly.

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

Type escape sequence to abort.
Sending 100, 100-byte ICMP Echos to 192.168.6.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (100/100), round-trip min/avg/max = 1/3/4 ms
cisco2811#
```

Step 2: Ping from the 6944 to the CISCO router, to ensure LAN to LAN communication is working correctly.



Step 3: Test successful.

This page left blank intentionally.

13 GRE Generic Routing Encapsulation

Overview

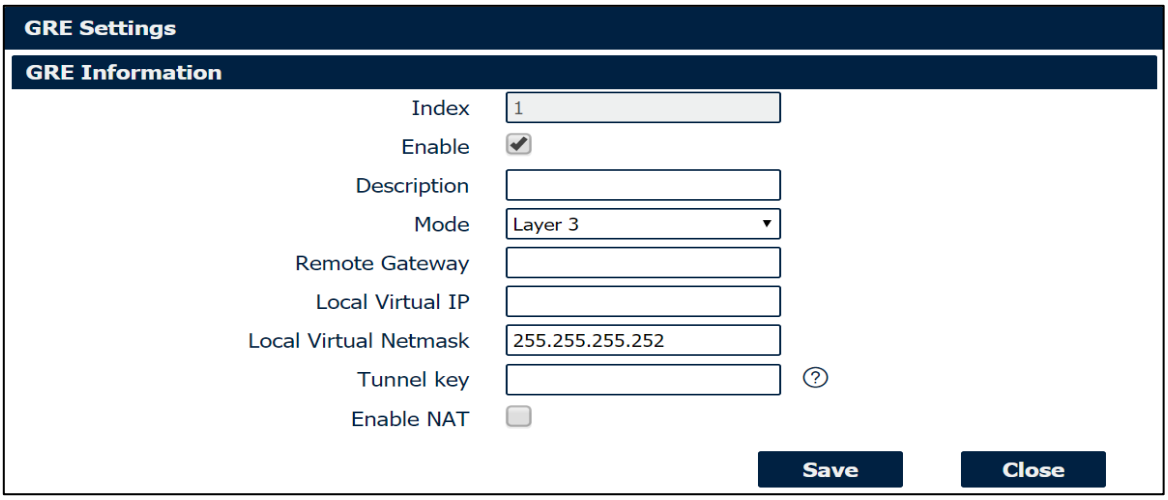
Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunnelling technology that provides a channel through which encapsulated data messages can be transmitted over the network encapsulating and decapsulating at each end.

Checking the 6944 GRE Status

– Go to Status>GRE

VPN->GRE->Status

- **Enable -** Displays current GRE settings and enable if you want to configure a GRE Tunnel.
- **Description -** Displays the description of current the VPN channel.
- **Mode -** Displays the current VPN mode.
- **Status -** Displays the current VPN connection status.



VPN->GRE

Enable Check this box to enable a GRE Tunnel.

Description Enter the description of the current VPN channel.

Mode Specify the running mode of the GRE, optional are "Layer 2 / Layer 3".

Remote Gateway Enter the remote IP address of the Peer GRE tunnel.

Local Virtual IP Enter the local tunnel IP address of the GRE tunnel.

Local Virtual Netmask Enter the local virtual netmask of GRE tunnel.

Tunnel Key Enter the authentication key for the GRE tunnel.

Enable NAT Check this box to enable the NAT function.

Bridge Interface Specify the bridge interface to work in Layer 2 mode.

13.1. AN027 – How to Configure a GRE VPN 6944 to Cisco Router

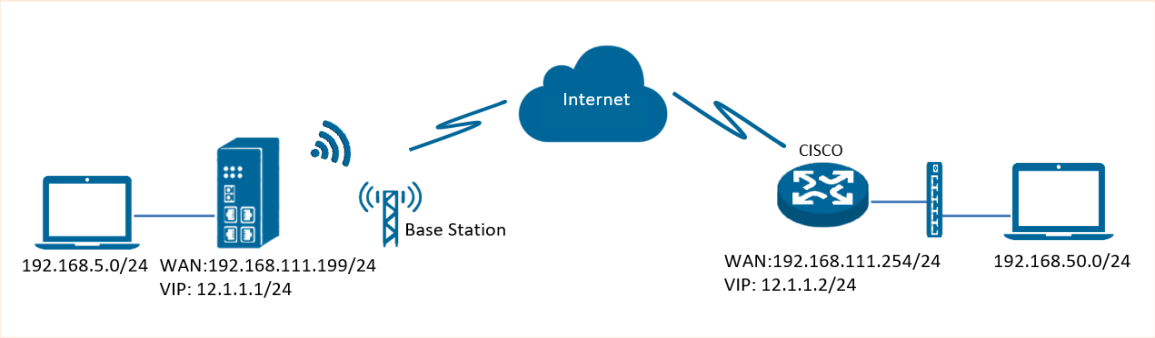
Overview

The application note shows how to configure a GRE VPN from a 6944 to a Cisco router.

6944 Software Version

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
30.9.2018	V1.1	V1.1.4 (0c0c09fa)	Standard Software	First release

Testing Topology



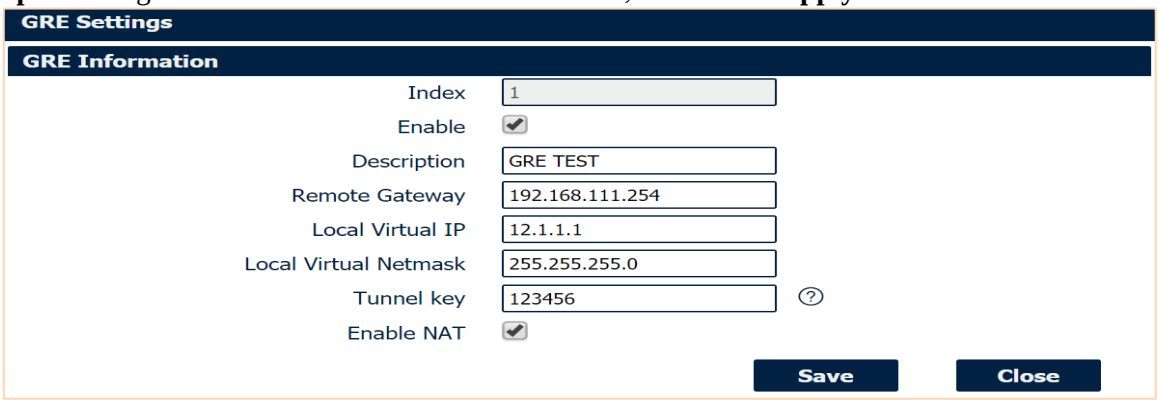
- The 6944 is used with a static public IP Address or dynamic public IP address with a domain name .
- The CISCO router runs as central router with a static public IP address or dynamic public IP address with domain name.
- GRE VPN tunnel establish between the 6944 and CISCO router.

Configuration

6944 Configuration

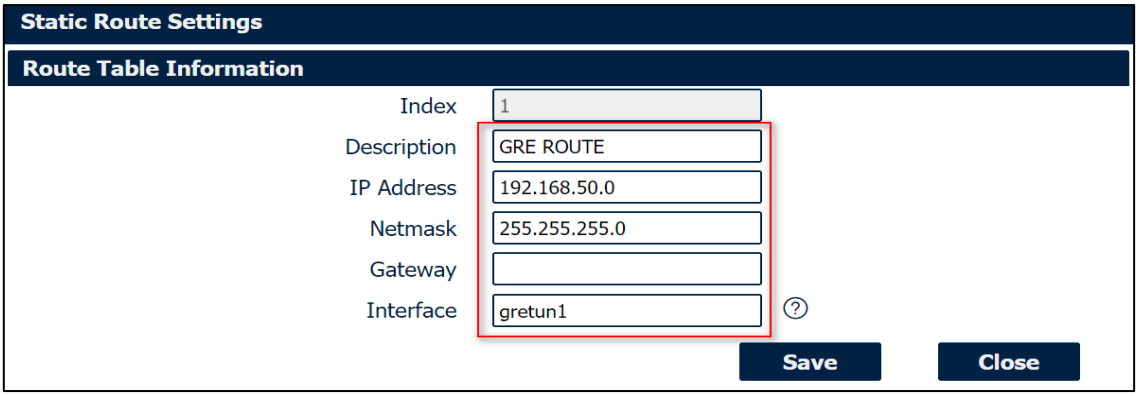
Step1. Go to **VPN>GRE>GRE**, Click the Edit button of GRE, like below:

Step 2. Configure the 6944 GRE VPN as shown below, click **Save>Apply**



Step 3: Go to **Network>Route>Route**, to configure the route to the subnet of Cisco, to make sure that the subnets can reach each other.

Configure the static route settings as shown below



Configuring the CISCO Router

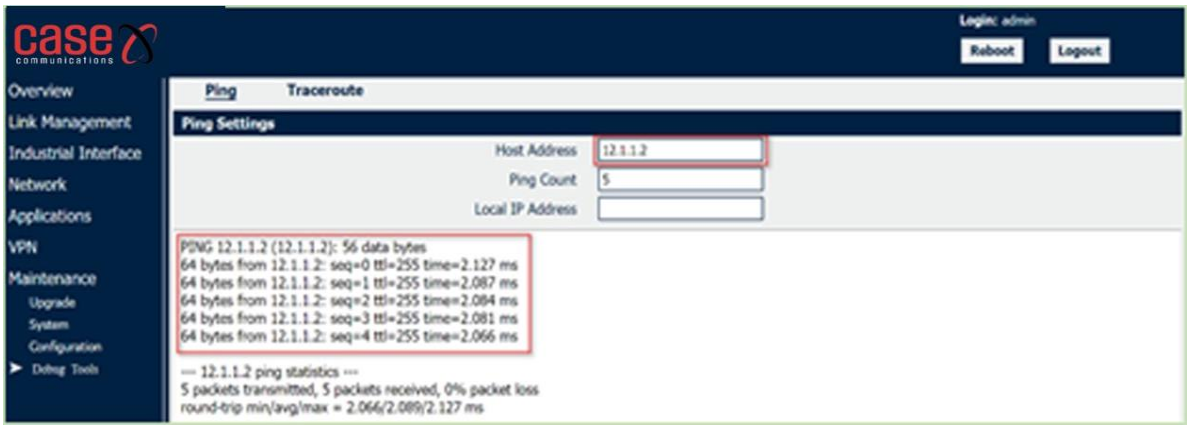
Step 1: Telnet to the Cisco router and configure the Cisco route GRE VPN as shown below:

==========

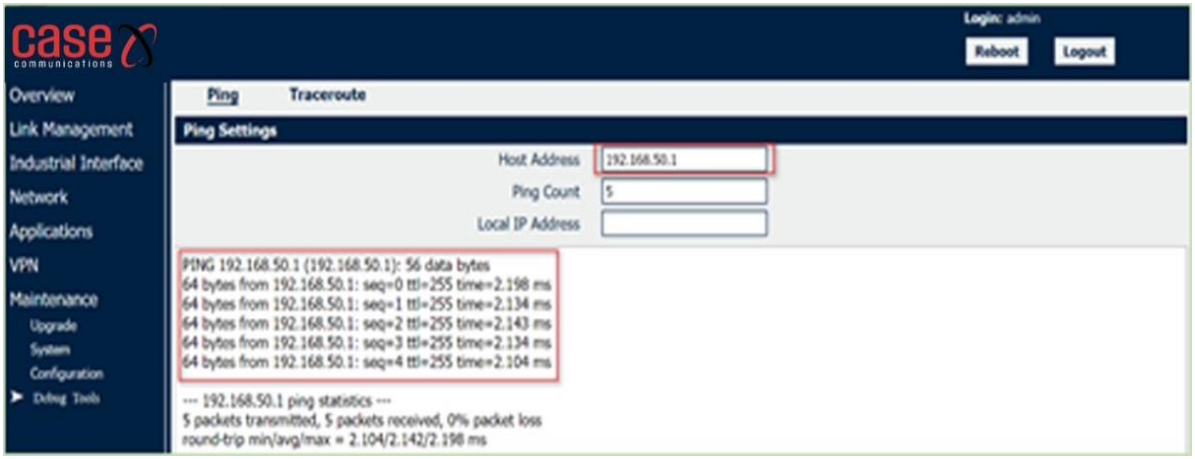
```
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 tunnel source 192.168.111.254
 tunnel destination 192.168.111.199
 tunnel key 123456
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
 crypto map MAP
!
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
ip route 192.168.5.0 255.255.255.0 12.1.1.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
!
end
```

Testing

Step1: Ping the virtual IP address from the 6944 to the Cisco router.



Step 2: Ping from the 6944 the subnet to the Cisco.



Step 3: Ping the virtual IP and subnet from the CISCO to 6944

```
cisco2811#
cisco2811#ping 12.1.1.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 12.1.1.1, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
cisco2811#
cisco2811#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
cisco2811#
```

Step 4: Test successful

13.2. AN056- GRE VPN Redundancy to Cisco Router

Overview

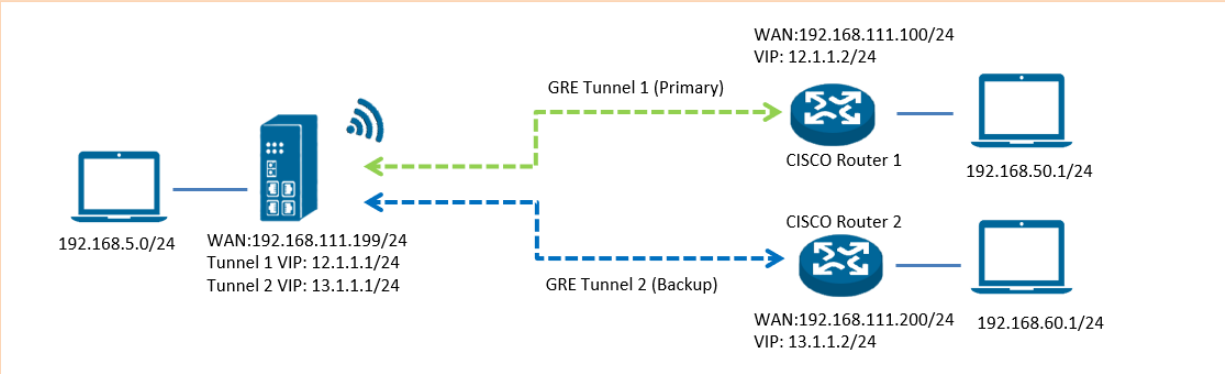
This document contains information regarding the configuration and use of GRE VPN redundancy between a 6944 router and CISCO router.

Software Compatibility

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
24.8.2020	V1.1	V1.1.4 (0c0c9fa)	V1.1.5 (19adafb)	First release

Testing Topology



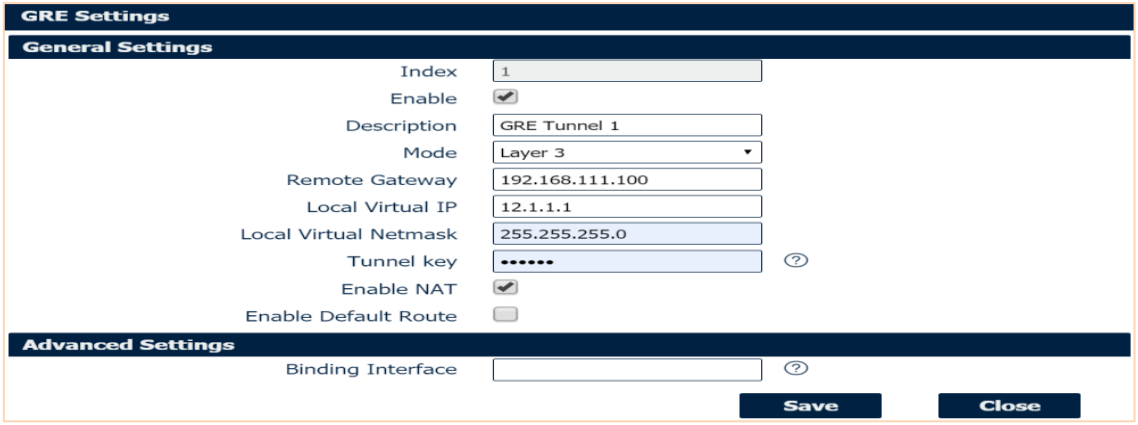
- A 6944 establishes two GRE VPN tunnels to two remote CISCO routers.
- Enable VPN redundancy and set GRE Tunnel 1 as primary tunnel and check it works. The subnets between 6944 and remote CISCO router 1 can communicate with each other. At this moment, the GRE VPN tunnel 2 is a backup tunnel and is inactive.
- When GRE tunnel 1 goes down, GRE Tunnel 2 will automatically come up and provide a path.. If GRE tunnel 1 recovers and comes up again, then the router will switch back from GRE tunnel 2 to GRE tunnel 1 automatically

Configuration

6944Router Configuration

Step 1. Go to **VPN>GRE>GRE**, Click the GRE Edit button as shown below

Step 2: Configure **GRE Tunnel 1** as shown below, then click: Save>Apply

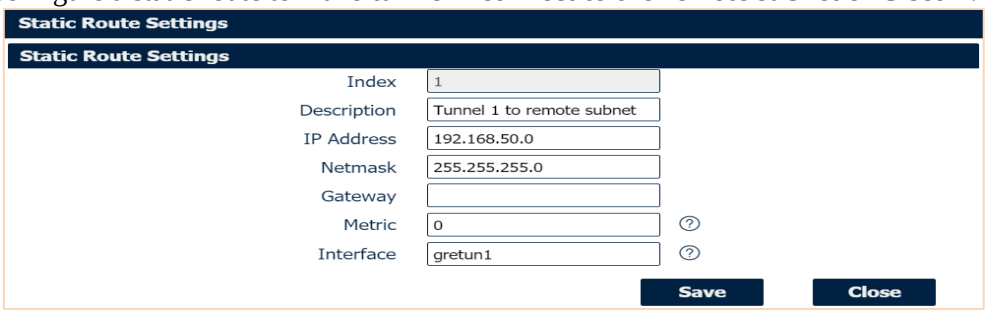


Step 3: Follow step 1 and configure the GRE Tunnel 2 as shown below. **Click Save > Apply**

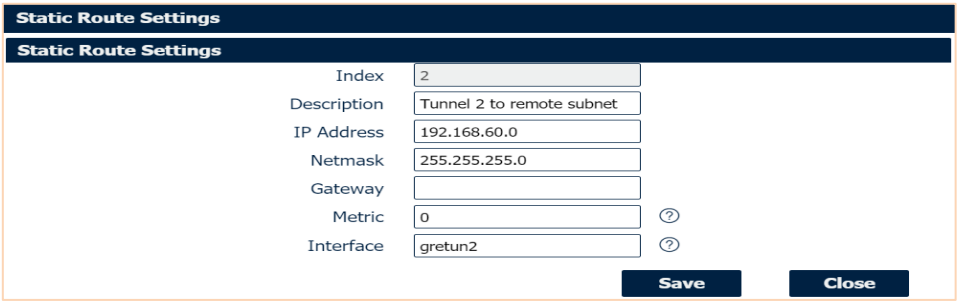
GRE Settings	
General Settings	
Index	**2**
Enable	**Tick**
Mode	**Layer 3**
Remote Gateway	**192.168.111.200**
Local Virtual IP	**13.1.1.1**
Local Virtual Netmask	**255.255.255.0**
Tunnel Key	************
Enable NAT	**Tick**
Enable Default Route	**Leave Un-ticked**
Advanced Settings	
Advanced Settings	
Binding Interface	**Leave Un-ticked**

Step 4: Go to **Network>Route>Route**, to configure two static routes to the subnet of Cisco 1 and Cisco2, to make sure that the subnet's can reach each other. Link Management>Static Route Setting

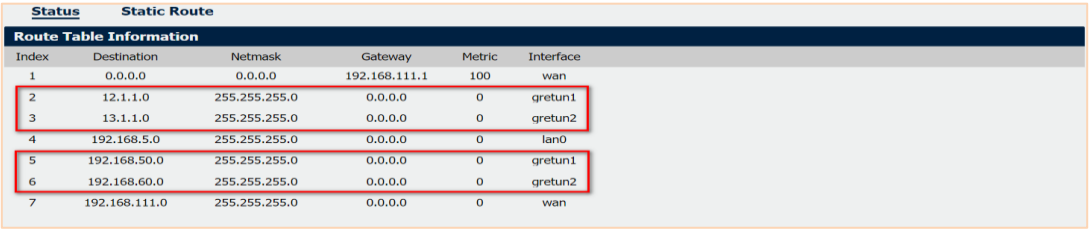
Step 5: Configure a static route to make **tunnel 1 connect to the remote subnet of Cisco 1**:



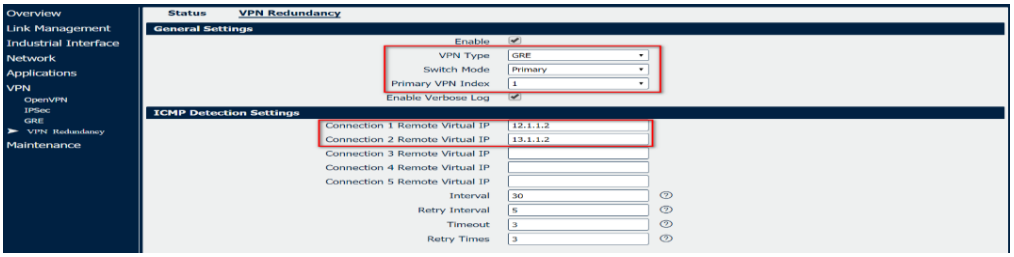
Step 6: Configure a static route to make **tunnel 2 go to the remote subnet of Cisco 2**:



Step7: After that, can check the 6944 routing table:



Step 8: Go to **VPN>VPN Redundancy** to enable the VPN Redundancy feature, as shown below:



Step 9: Click Save > Apply

CISCO Router 1 and CISCO Router 2 Configuration

CISCO Router 1 Configuration

Step 1: Telnet to the cisco route and configure cisco router 1 GRE VPN as shown below:

```
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 tunnel source 192.168.111.100
 tunnel destination 192.168.111.199
 tunnel key 123456
!
interface FastEthernet0/0
 ip address 192.168.111.100 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
ip route 192.168.5.0 255.255.255.0 12.1.1.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0 overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
!
end
```

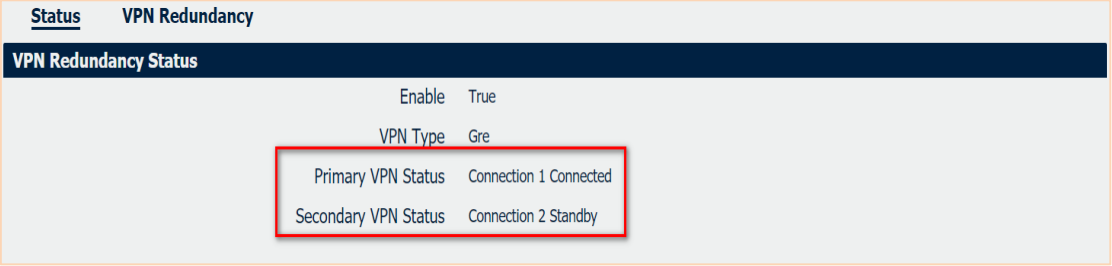
CISCO Router 2 Configuration

Step1. Telnet to the cisco router and configure cisco router 2 GRE VPN as shown below:

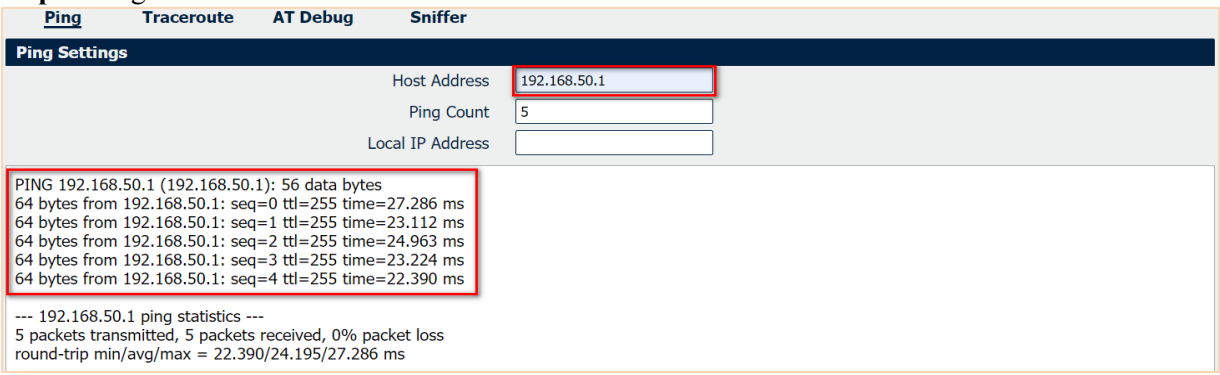
```
cisco2811#
cisco2811#SHOW RUNning-config
Building configuration...
version 12.4
!
hostname cisco2811
ip name-server 192.168.111.1
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
username admin password 0 admin
archive
 log config
  hidekeys
!
interface Loopback0
 ip address 192.168.60.1 255.255.255.0
!
interface Tunnel1
 ip address 13.1.1.2 255.255.255.0
 tunnel source 192.168.111.200
 tunnel destination 192.168.111.199
 tunnel key 123456
!
interface FastEthernet0/0
 ip address 192.168.111.200 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
interface FastEthernet0/1
 ip address 192.168.0.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
ip route 192.168.5.0 255.255.255.0 13.1.1.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface FastEthernet0/0
overload
!
access-list 10 permit 192.168.5.0 0.0.0.255
!
end
```

Testing

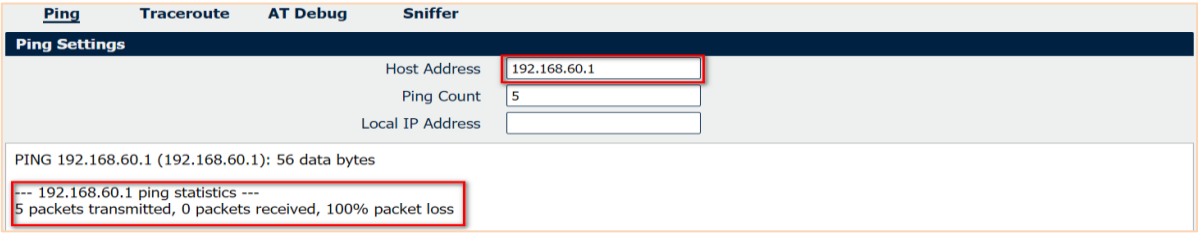
Step 1: Go to VPN>VPN Redundancy, the primary tunnel is connected, and the secondary tunnel is standby:



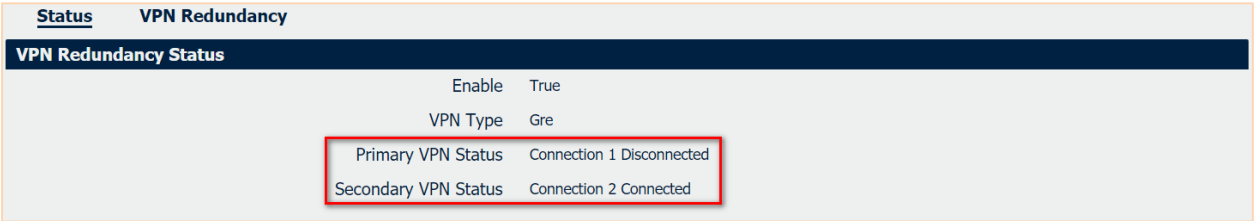
Step 2: Ping **Cisco router 1**'s subnet from the 6944.



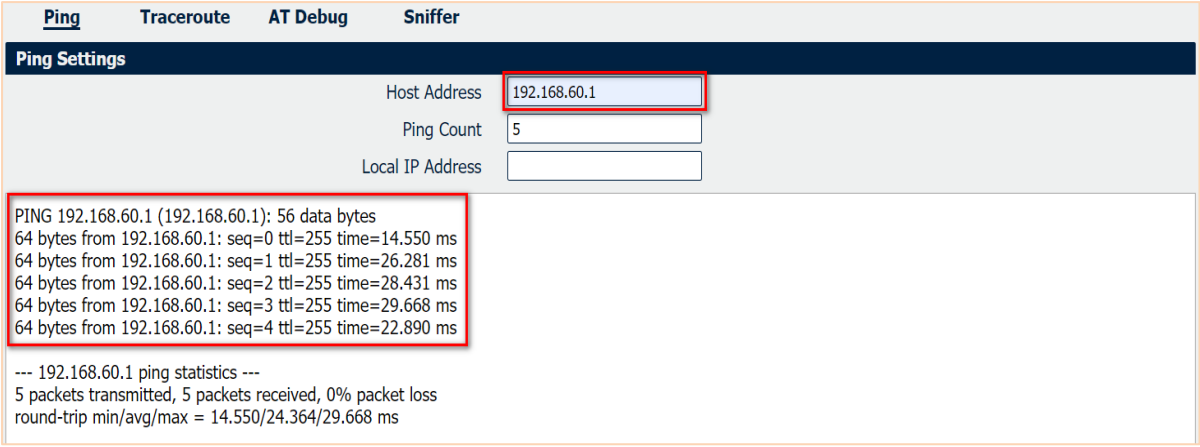
Step 3: Ping **Cisco router 2's subnet** from the 6944. It should **fail**, because GRE Tunnel 2 is in standby mode.



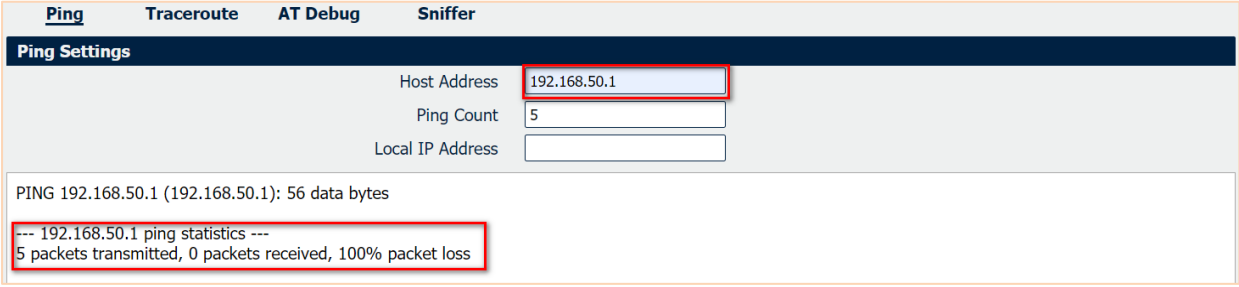
Step 4: Shut down GRE VPN Tunnel 1 on the CISCO side, Tunnel 2 should come up automatically:



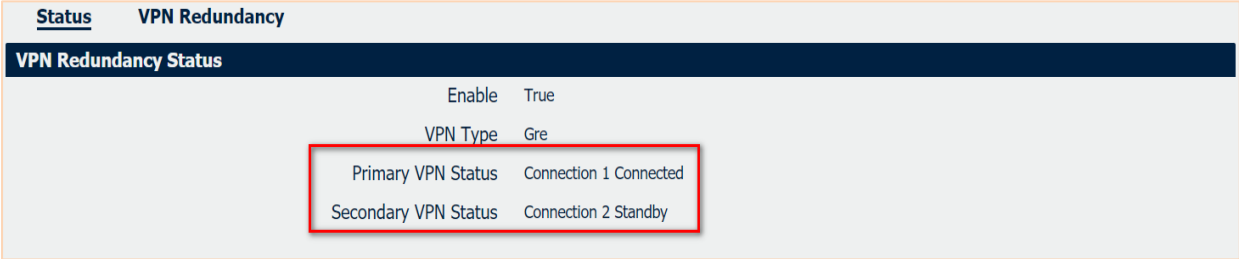
Step 5: Ping **Cisco router 2's subnet** from the 6944.

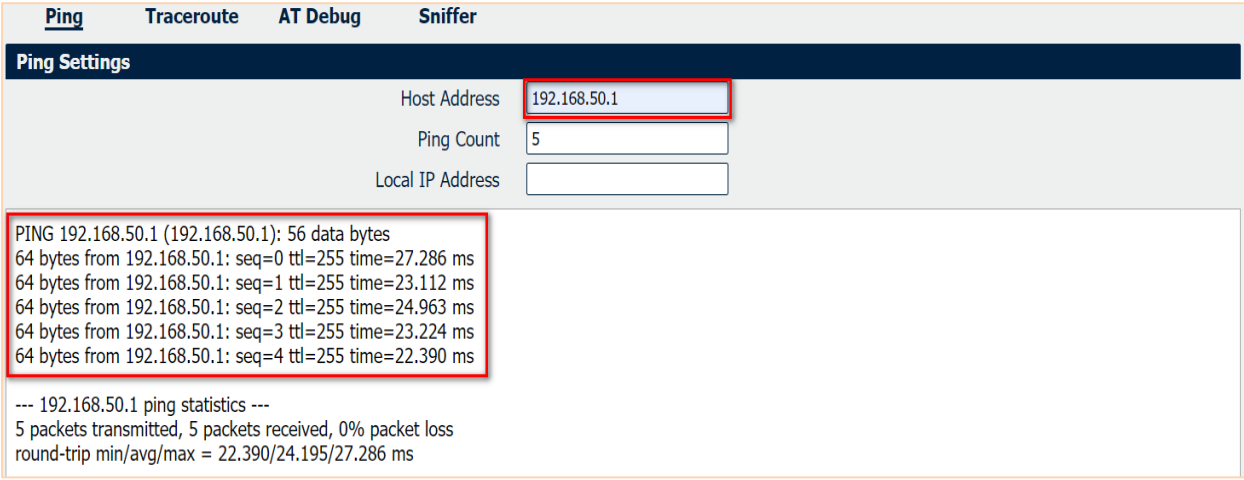


Step 6: Ping **Cisco router 1's subnet** from the 6944 and it should **fail**, because GRE Tunnel 1 is disconnected:



Step 7: Turn on the GRE VPN Tunnel 1 on the Cisco side, it will switch back from Tunnel 2 to Tunnel 1 automatically and ping the subnet on Cisco router 1, this should now work,





Step 8: Test successful.

This page left blank intentionally

14 Layer Two Tunneling Protocol (L2TP)

14.1. AN044_L2TP_between_two_6944_Routers

Overview

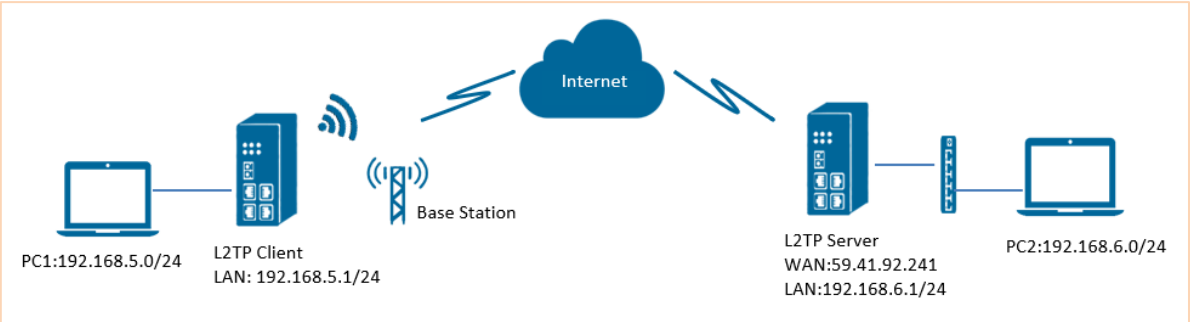
This document contains information regarding configuring an L2TP VPN between two 6944 routers.

Version

The latest document will include all the content of previous versions. Note for L2TP additional software is required, this is available from Case Communications.

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
24.9.2018	V1.1	V1.1.4 (0c0c09fa)	L2TP_1.0.1 (e9b6efe)	First release

Testing Topology

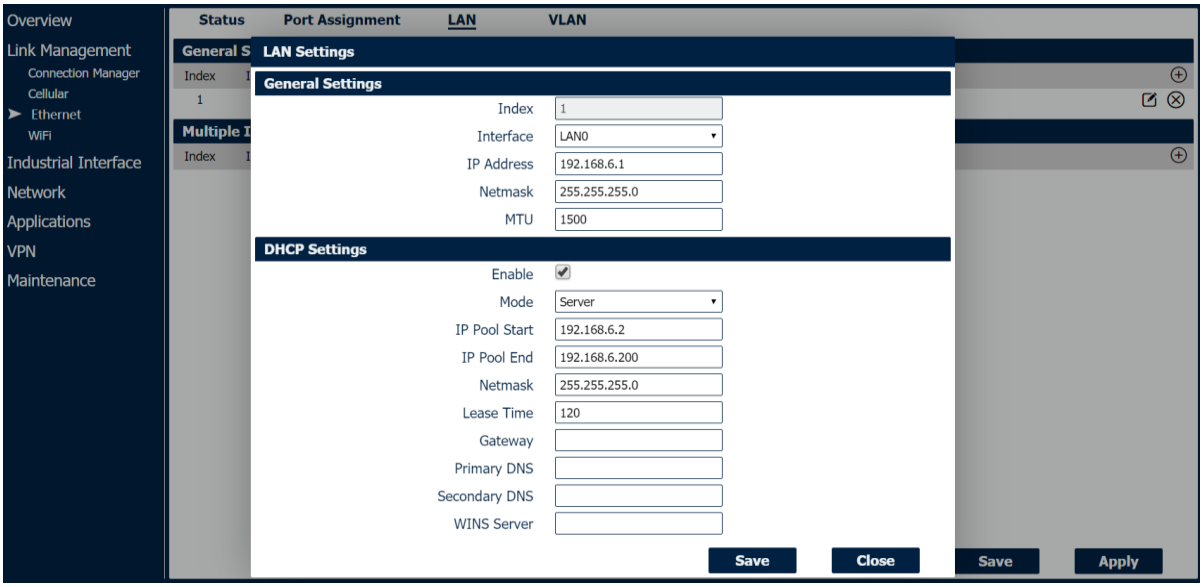


- One 6944 runs as an L2TP server and connects to the Internet using a Sim card with a Fixed Public IP Address.
- A second 6944 run as L2TP client with any type of SIM card which will allow a connection to the internet.
- An L2TP VPN tunnel is established between the two 6944 routers and the subnet PCs will be able to communicate with each other.

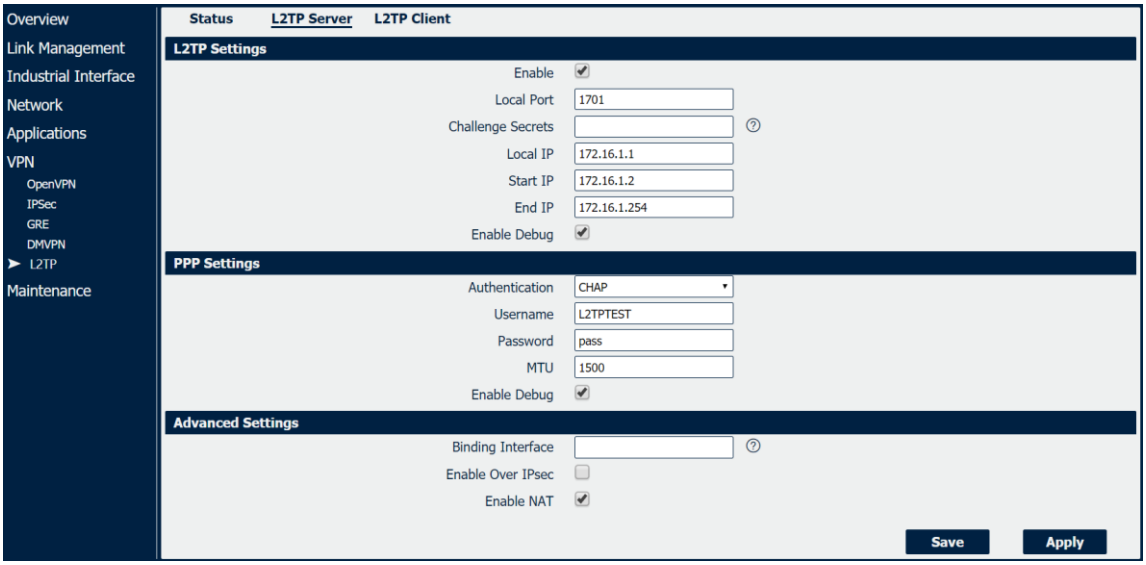
Configuration

L2TP Server Configuration

Step 1:Go to **Link Management>Ethernet>LAN**, specify the LAN IP address as 192.168.6.0/24, as shown below

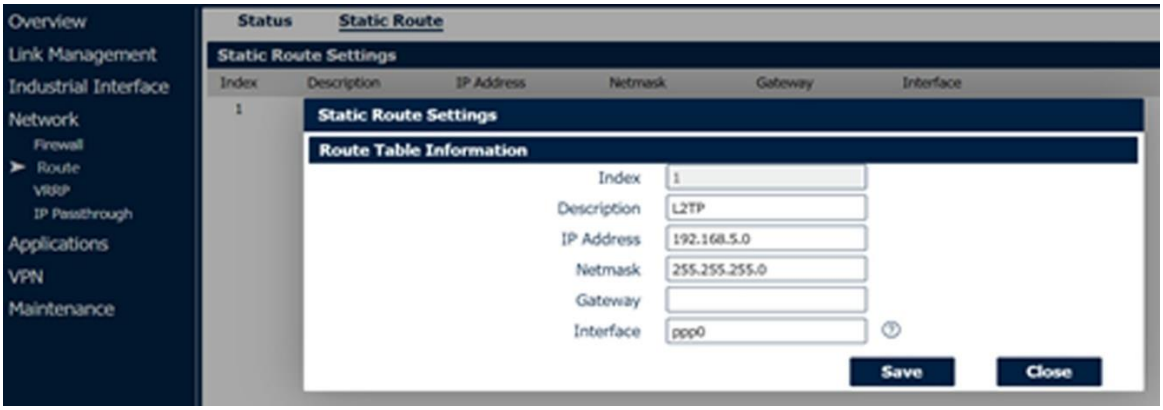


Step 2: Go to **VPN>L2TP>L2TP Server**, enable L2TP server and configuration as shown below.



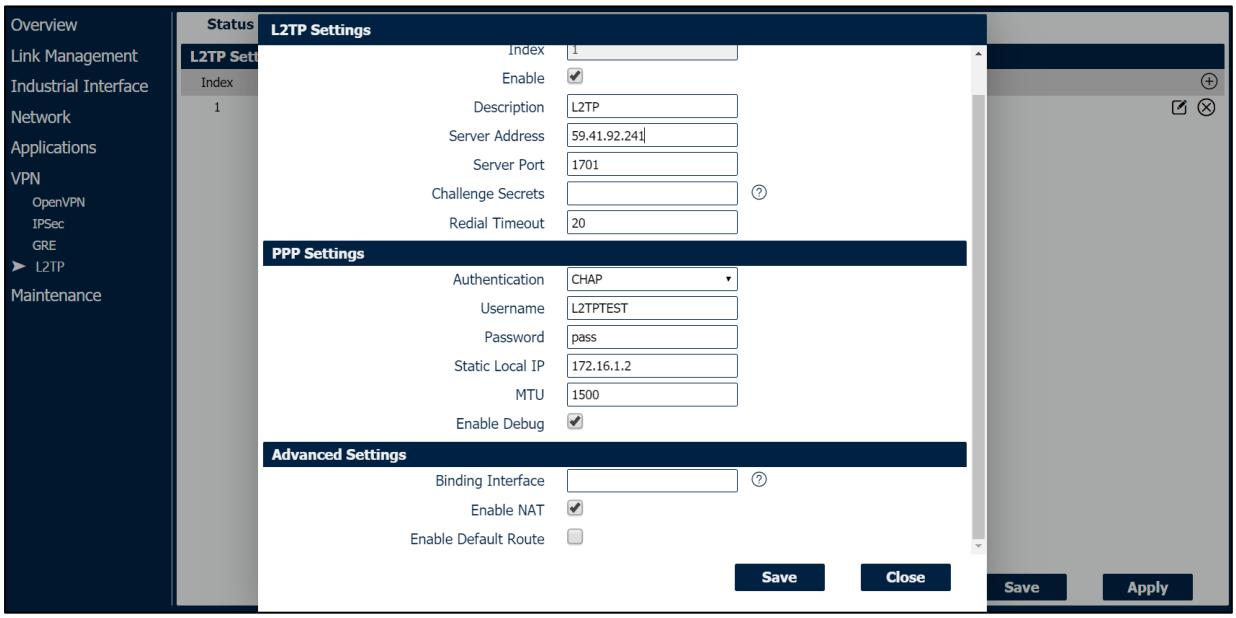
Click Save > Apply

Step 3: Go to **Network>Route>Static Route**, specify the static route, so that the subnet behind the L2TP Server can reach the subnet behind the L2TP Client. Click Save > Apply



L2TP Client Configuration

Step 1: Go to **VPN>L2TP>L2TP Client**, enable L2TP client and configure as shown below. **Then click Save > Apply**



Step 2: Go to **Network>Route>Static Route**, specify the static route, so that the subnet behind L2TP Client can reach the subnet behind the L2TP Server.

Testing

Step 1: Ping from PC1 to PC2 as shown below and ensure you get a reply.

```
C:\Users \ Administrator>ping 192.168.6.2
Pinging 192.168.6.2. with 32 bytes of data
Reply from 192.168.6.2: bytes=32  time<1ms TTL=128
Reply from 192.168.6.2: bytes=32  time<1ms TTL=128
Reply from 192.168.6.2: bytes=32  time<1ms TTL=128
Reply from 192.168.6.2: bytes=32  time<1ms TTL=128

Ping statistics for 192.168.6.2:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Step 2: Ping from PC2 to PC1 shown below and ensure you get a reply:

```
C:\Users \ Administrator>ping 192.168.5.2
Pinging 192.168.5.2. with 32 bytes of data
Reply from 192.168.5.2: bytes=75ms  time<1ms TTL=62
Reply from 192.168.5.2: bytes=75ms  time<1ms TTL=62
Reply from 192.168.5.2: bytes=75ms  time<1ms TTL=62
Reply from 192.168.5.2: bytes=75ms  time<1ms TTL=62

Ping statistics for 192.168.5.2:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 64ms, Maximum = 87ms, Average = 77ms
```

14.2. AN045-L2TP Server to Windows Operating System

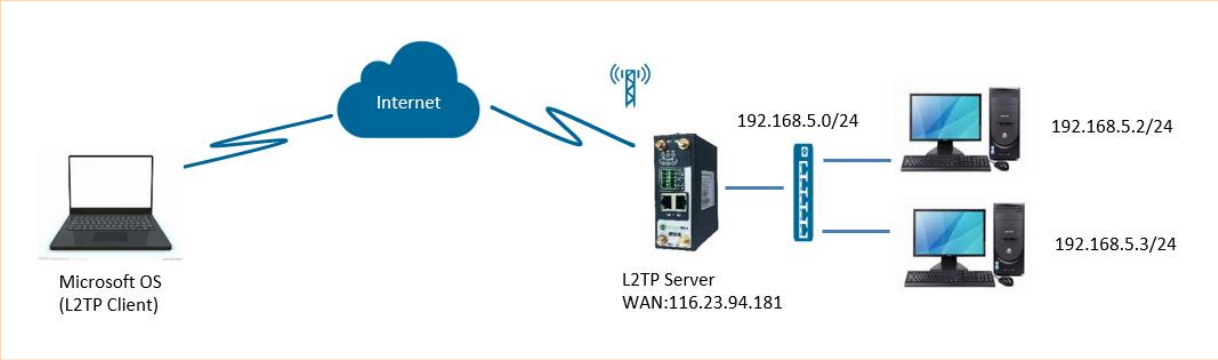
Overview

This document contains information regarding the configuration and use of L2TP server with Windows OS.

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
29.2.2020	V1.1	V1.1.4 (0c0c9fa)	V1.0.1 (e9b6efe)	First release

Testing Topology

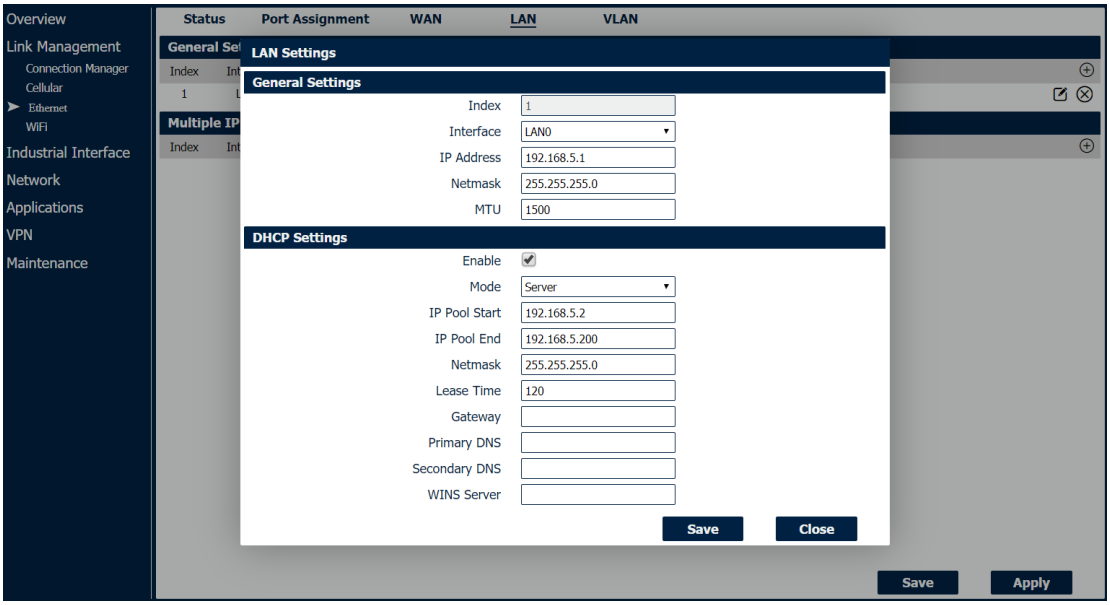


- The 6944 Router run as an L2TP server with a public IP address.
- A PC runs with a Microsoft Windows Operating system working as L2TP client.
- A L2TP VPN tunnel is established between the 6944 router and the PC, The PC can access the LAN devices behind the 6944 Router.

Configuration

L2TP Server Configuration

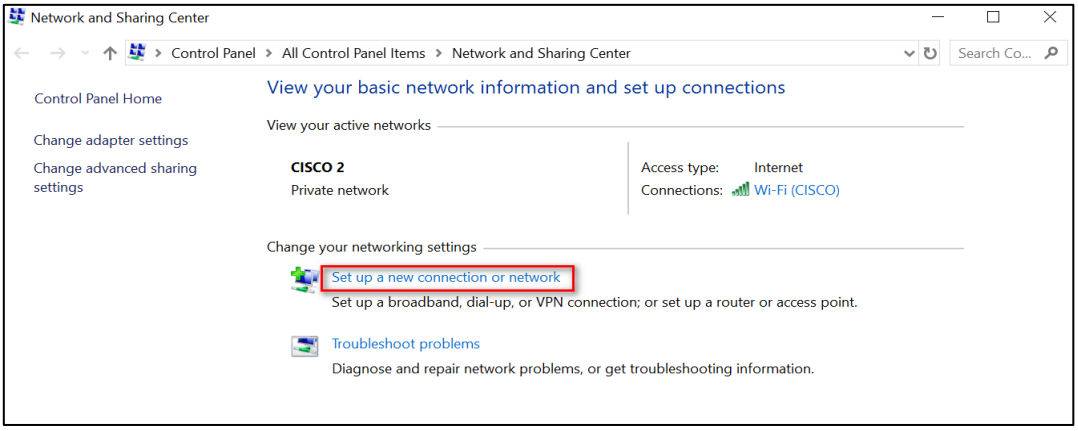
Step 1: Go to **Link Management>Ethernet>LAN**, specify the LAN IP address as 192.168.5.0/24, as shown below: **Then click Save > Apply**



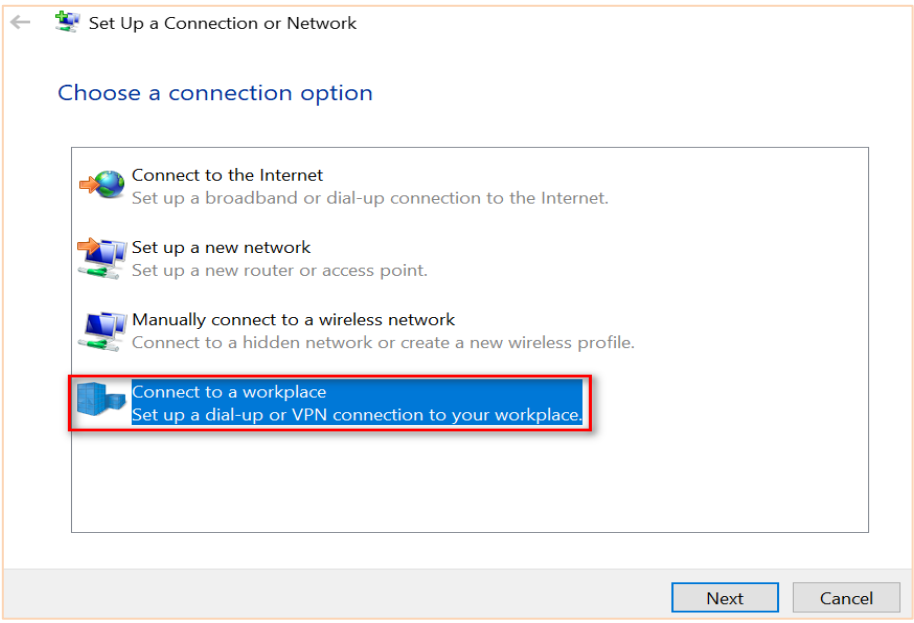
Step 2: Go to **VPN>L2TP>L2TP Server**, enable L2TP server and configuration as shown below: **Click Save > Apply**

L2TP Client Configuration

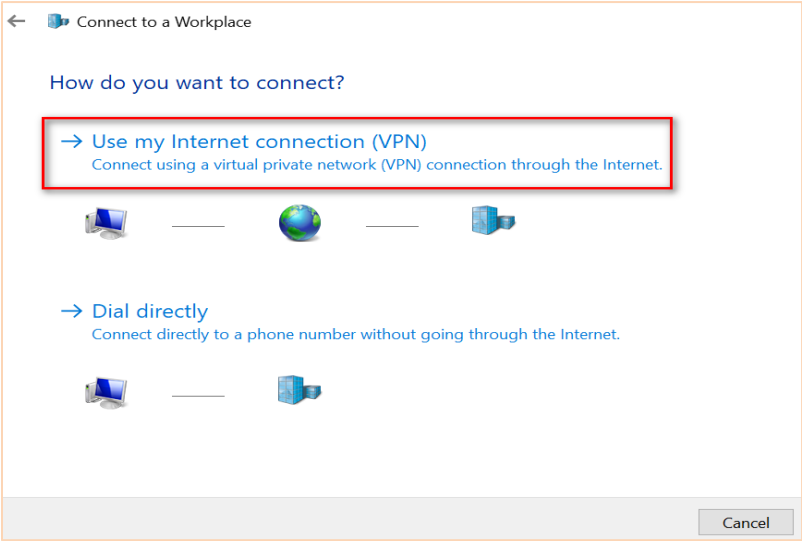
Step 1: Open the PC and go to Network and Sharing Center, click "Set up a new connection or network:



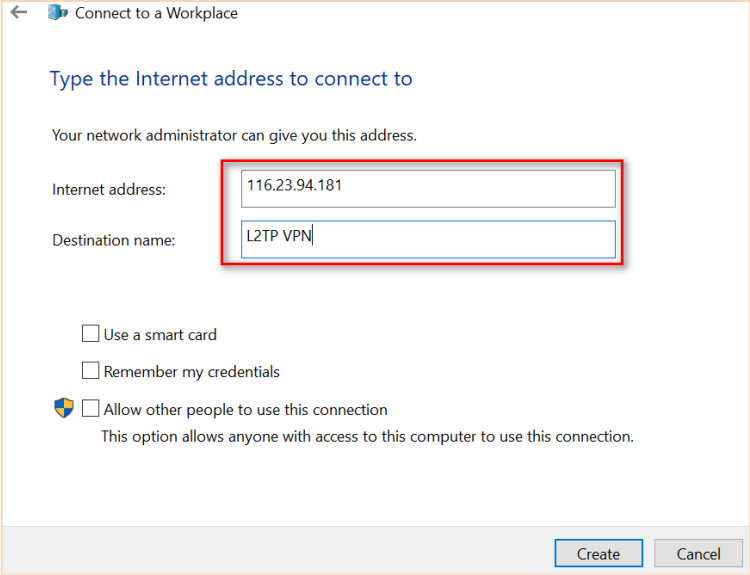
Step 2: Choose "Connect to a workplace" and click "Next":



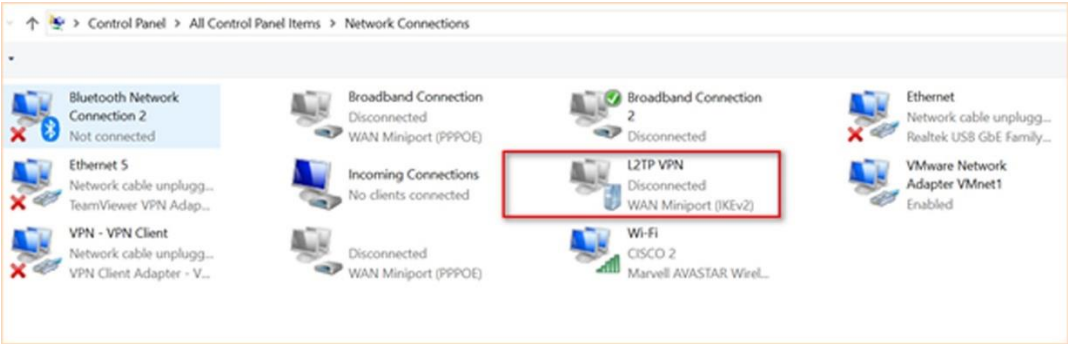
Step 3: Click "Use my Internet connection (VPN).



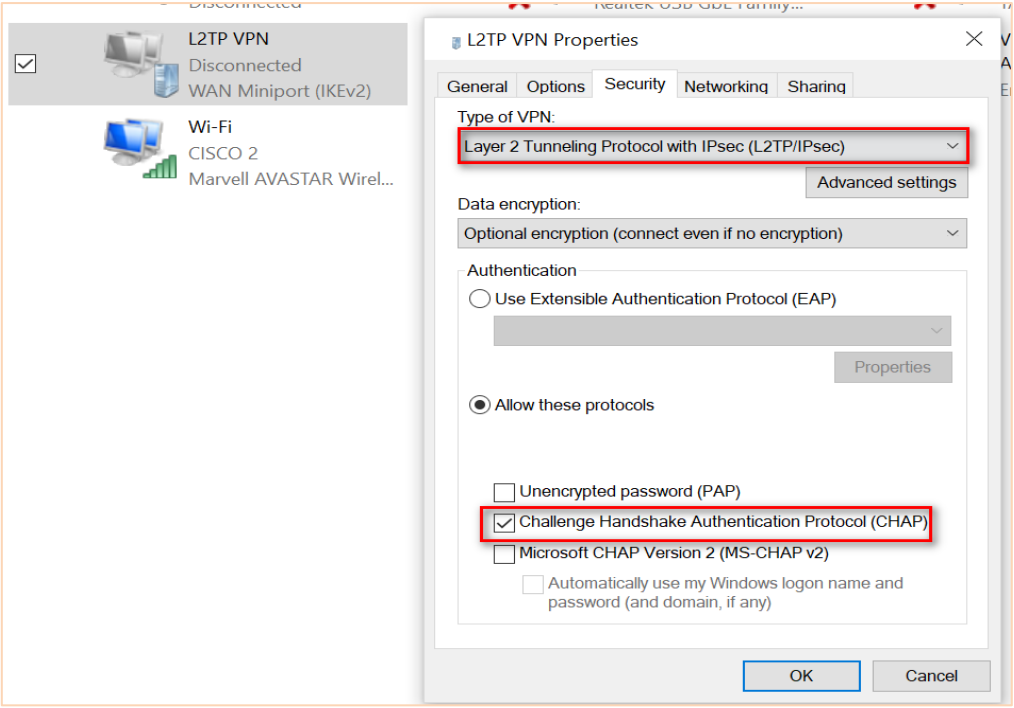
Step 4: Enter the L2TP Server IP address and Destination name, click "Create".



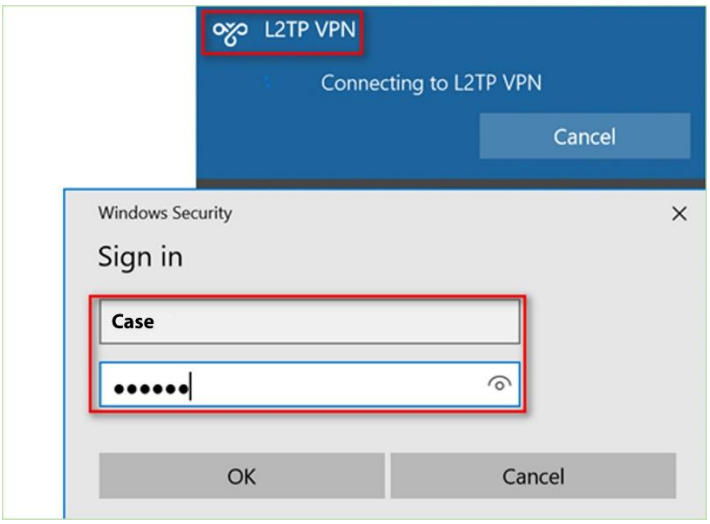
Step 5: After that, create an L2TP connection, as shown below:



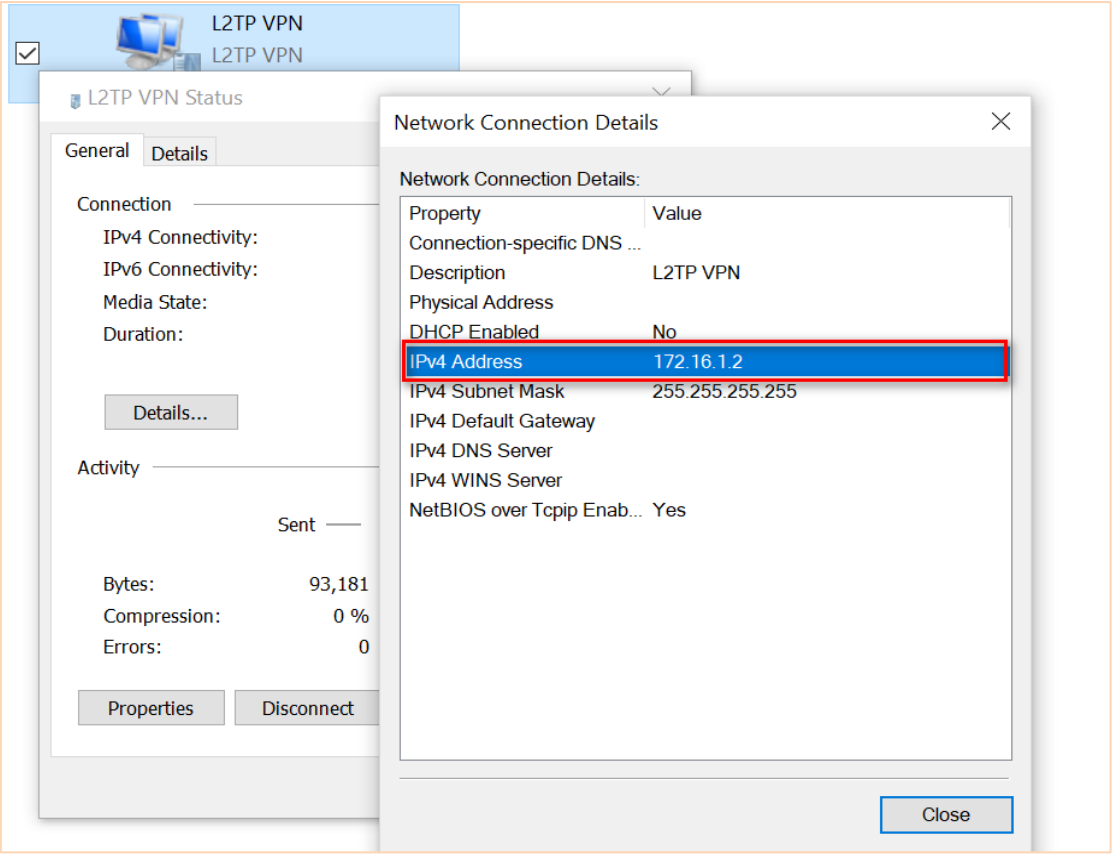
Step 6: Right Click "L2TP VPN", and choose "Properties", go to "Security" and specify the Type of VPN and Authentication, as shown below:



Step 7: After finishing all above settings, click to connect "L2TP VPN", and sign in with the Username and Password, Click "OK", as shown below:



Step 8: If the L2TP Client has connected to L2TP Server successfully. Right Click the "L2TP VPN", choose "Status", go to "Details", then we can see that the L2TP Server has assigned an IP address to the L2TP Client.



Testing

Step 1: Ping from the L2TP Client to the L2TP Server and ensure you get a response as shown below.

```
C:\Users \ Administrator ping 192.168.5.1

Pinging 192.168.5.1. with 32 bytes of data
Reply from 192.168.5.1: bytes=32  time-13ms TTL=64
Reply from 192.168.5.1: bytes=32  time-1ms TTL=64
Reply from 192.168.5.1: bytes=32  time-1ms TTL=64
Reply from 192.168.5.1: bytes=32  time-1ms TTL=64

Ping statistics for 192.168.5.1:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

14.3. AN046 - 6944 L2TP Client to Cisco L2TP Server

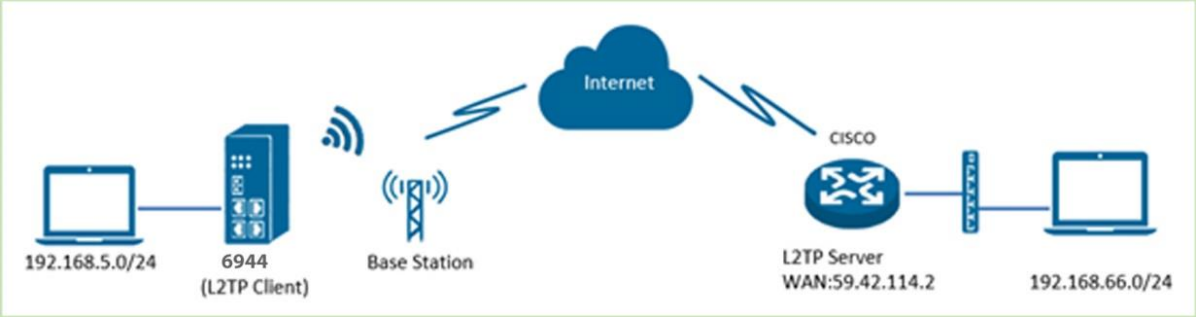
Overview

This document contains information regarding the configuration and use of L2TP client with cisco.

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
27.11.2019	V1.1	V1.1.4 (0c0c9fa)	V1.0.1 (e9b6efe)	First release

Testing Topology



- The 6944 runs as an L2TP client and connects to the Internet.
- The CISCO router runs as an L2TP server with a public IP Address.
- An L2TP VPN tunnel is established between the 6944 router and the CISCO router. The subnet PCs should be able to communicate with each other.

Configuration

L2TP Server Configuration

Step 1: Configure the L2TP server on the CISCO as shown below:

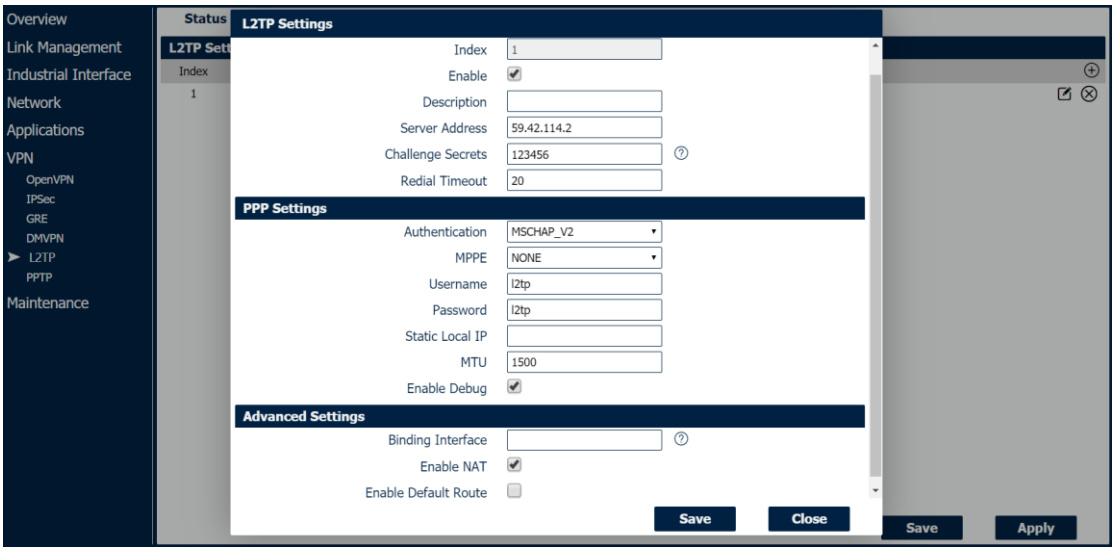
```
cisco2811#show run
Building configuration...
Current configuration : 5447 bytes
version 12.4
ip cef
ip dhcp excluded-address 10.10.10.1
ip dhcp pool ABC
  network 10.10.10.0 255.255.255.0
  default-router 10.10.10.1
ip name-server 8.8.8.8
ip name-server 202.96.128.166
ip address-pool local!
vpdn enable
vpdn-group l2tp
! Default L2TP VPDN group
 accept-dialin
  protocol l2tp
 virtual-template 1
 l2tp tunnel password 0 123456
username l2tp password 0 l2tp
interface Loopback2
 ip address 192.168.66.1 255.255.255.0
!
interface FastEthernet0/0
 bandwidth 640
 no ip address
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
 no cdp enable
 no mop enabled
!
interface FastEthernet0/1
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Virtual-Template1
 ip address 10.5.5.1 255.255.255.0
 peer default ip address pool l2tp
 keepalive 20 3
 ppp authentication ms-chap-v2
!
interface Dialer1
 bandwidth 640
 ip address negotiated
```

```
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip tcp adjust-mss 1452
no ip mroute-cache
dialer pool 1
dialer idle-timeout 0
dialer hold-queue 100
dialer persistent
dialer-group 1
no cdp enable
 ppp authentication pap chap callin
 ppp pap sent-username
020xxxxxxxxxx@163.gd password 0
XVGZW
 crypto map SMAP
!
ip local pool l2tp 10.5.5.2 10.5.5.200
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 192.168.5.0 255.255.255.0 10.5.5.2
access-list 10 permit 10.10.10.0 0.0.0.255
cisco2811#
```

L2TP Client Configuration

Step 1: Go to **VPN>L2TP>L2TP Client**, enable L2TP client and configuration as shown below:

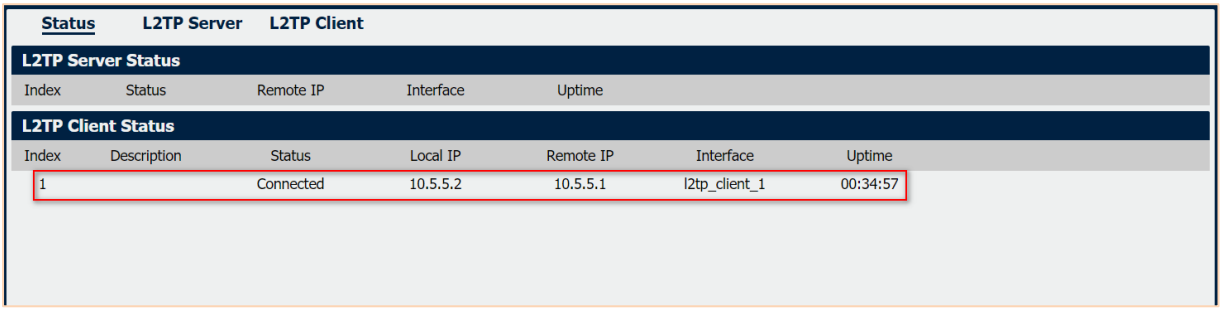
Click Save > Apply



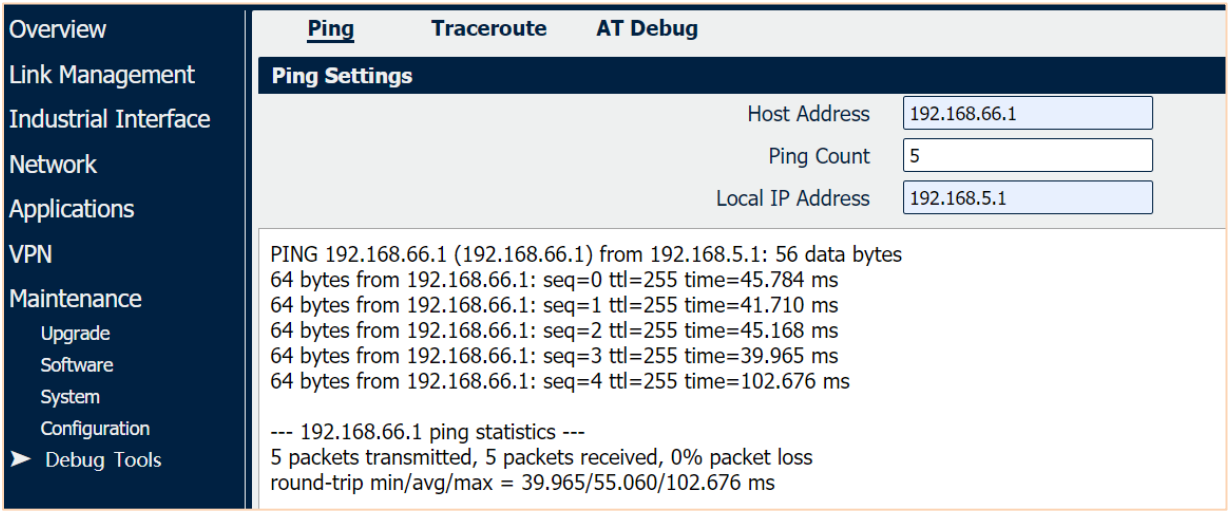
Step 2: Go to **Network>Route>Static Route**, specify the static route, so that the subnet behind L2TP Client can reach the subnet behind L2TP Server. **Click Save > Apply**

Testing

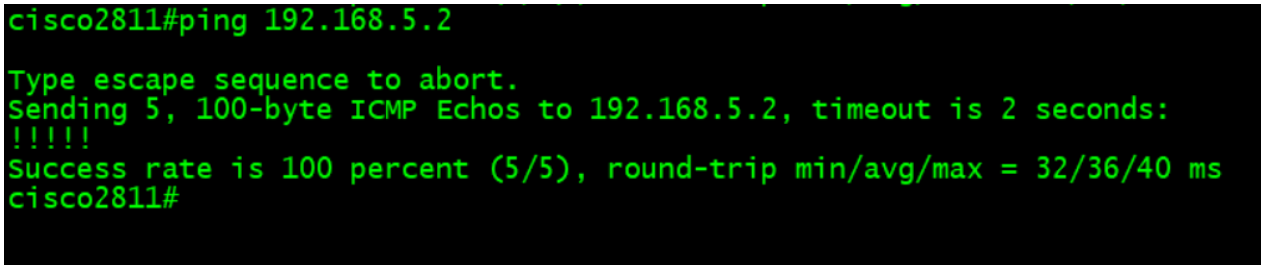
Step 1: The 6944 L2TP Client has connected the CISCO L2TP Server successfully. Go to **VPN>L2TP>Status**, to check the connection status.



Step 2: Ping from the 6944 to the CISCO's subnet to ensure you get a reply.



Step 3: Ping from the CISCO to the 6944's LAN.



```
cisco2811#ping 192.168.5.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/36/40 ms
cisco2811#
```

Step 4: Test is successful

This page left blank intentionally.

15 Point to Point Tunneling Protocol (PPTP)

15.1. AN 051 PPTP Client to CISCO Server

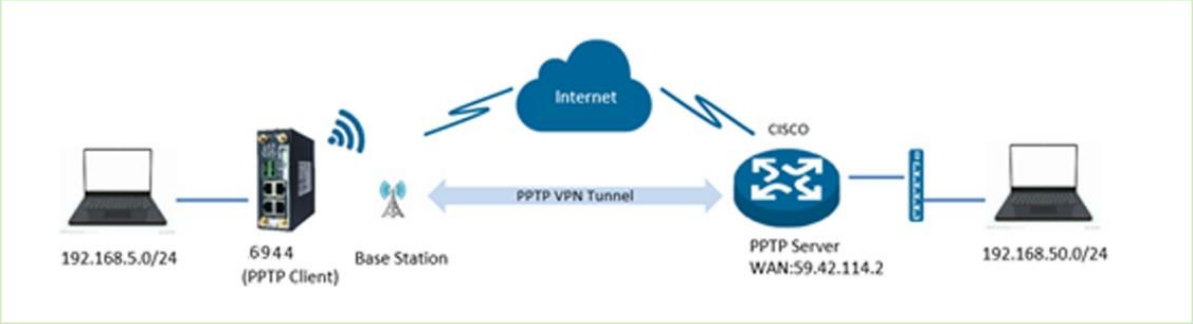
Overview

This document contains information regarding the configuration and use of the 6944 running as a PPTP Client to a Cisco Server

Software Compatibility

Release Date	Doc. Version	Firmware	Additional Software	Change Description
17.3.2020	V1.1	V1.1.4(0c0c9fa)	PPTP_1.0.2 (6424848)	First release

Testing Topology



- The 6944 router runs as PPTP client, make sure it communicates with Internet.
- CISCO router runs as PPTP server and has a static public IP address.
- The PPTP VPN tunnel is established between the 6944 router and CISCO router. The PC's on the subnets are able to communicate with each other.

Configuration

PPTP Server Configuration

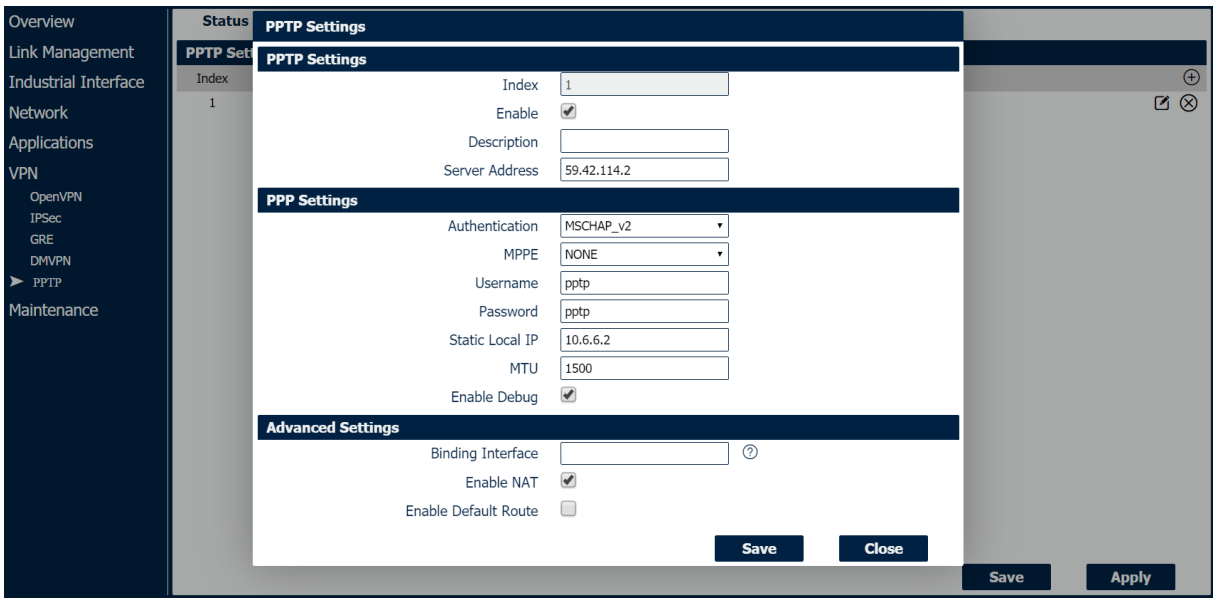
Step 1: The configuration of PPTP server on CISCO as shown below:

```
cisco2811#show run
Building configuration...
Current configuration : 5611 bytes
!
version 12.4
hostname cisco2811
ip dhcp excluded-address 10.10.10.1
ip dhcp pool ABC
   network 10.10.10.0 255.255.255.0
   default-router 10.10.10.1
ip name-server 8.8.8.8
ip name-server 202.96.128.166
ip address-pool local
no ipv6 cef
vpdn enable
!
vpdn-group 2
! Default PPTP VPDN group
 accept-dialin
  protocol pptp
  virtual-template 2
!
vpdn-group PPPOE
 request-dialin
  protocol pppoe
!
username pptp password 0 pptp
archive
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 bandwidth 640
 no ip address
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 pppoe enable group global
 pppoe-client dial-pool-number 1
 no cdp enable
 no mop enabled
!
interface FastEthernet0/1
```

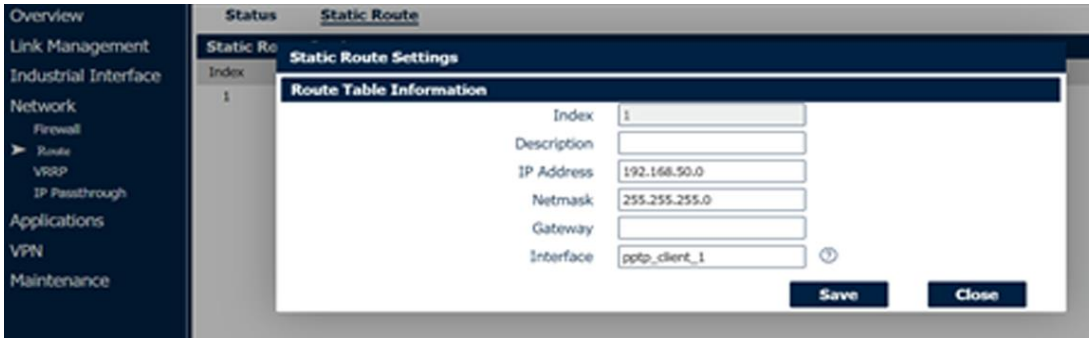
```
 ip address 10.10.10.1 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
 no cdp enable
!
interface Virtual-Template2
 ip address 10.6.6.1 255.255.255.0
 ip nat inside
 ip virtual-reassembly
 peer default ip address pool pptp
 ppp encrypt mppe auto
 ppp authentication ms-chap-v2
!
interface Dialer1
 bandwidth 640
 ip address negotiated
 ip mtu 1492
 ip nat outside
 ip virtual-reassembly
 encapsulation ppp
ip tcp adjust-mss 1452
 no ip mroute-cache
 dialer pool 1
 dialer idle-timeout 0
 dialer hold-queue 100
 dialer persistent
 dialer-group 1
 no cdp enable
 ppp authentication pap chap callin
 ppp pap sent-username
0203XXXXXXXX@163.gd password 0
FSOXXXXXX
 crypto map SMAP
!
ip local pool pptp 10.6.6.2 10.6.6.200
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 192.168.5.0 255.255.255.0 10.6.6.2
!
ip nat inside source list 11 interface Dialer1
overload
!
access-list 11 permit 10.6.6.0 0.0.0.255
snmp-server community public RO
!
cisco2811#
```

PPTP Client Configuration

Step 1: Go to **VPN>PPTP>PPTP Client**, enable PPTP client and configuration as shown below: **Click Save > Apply**

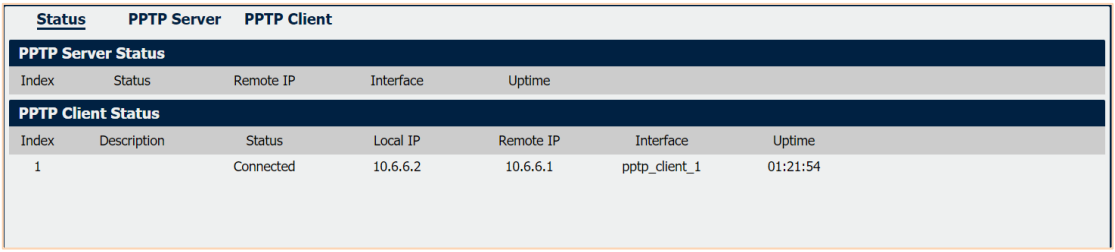


Step 2: Go to **Network>Route>Static Route**, specify the static route, so that the subnet behind PPTP Client can reach the subnet behind PPTP Server.

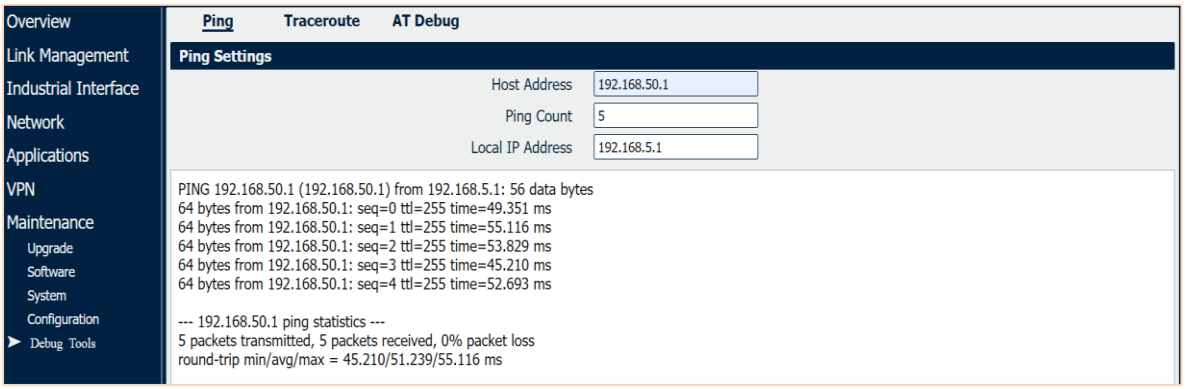


Testing

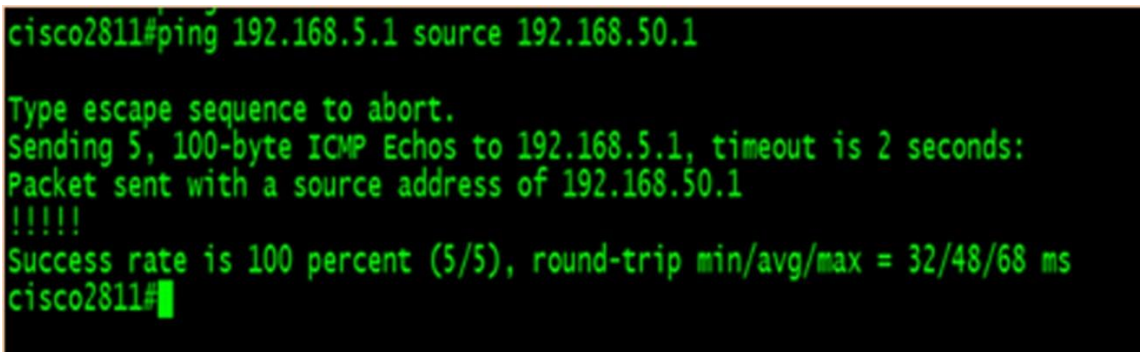
Step 1: If the 6944 PPTP Client has connected to the CISCO PPTP Server successfully. Go to **VPN>PPTP>Status**, to check the connection status.



Step 2: Ping from the 6944 to the CISCO's subnet to ensure the connection has been established.



Step 3: Ping from the CISCO to the 6944 LAN and check to see if the ping is replied to.



15.2. AN052 6944 PPTP Server to Windows PC

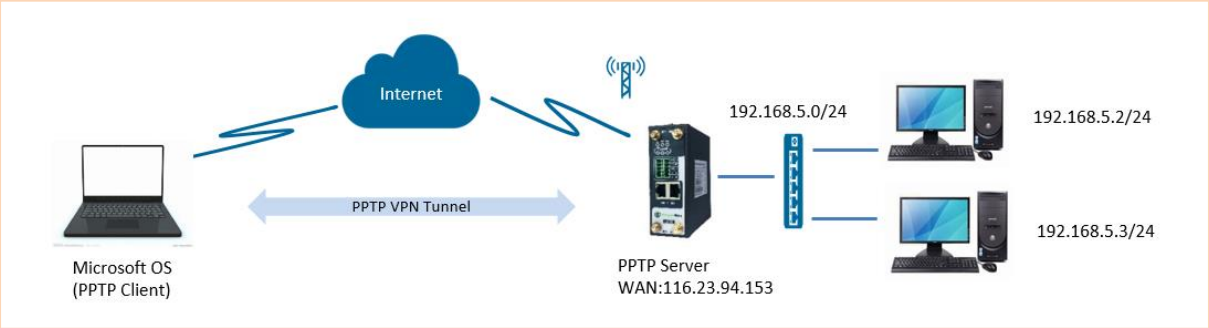
Overview

This document contains information regarding the configuration and use of the 6944 running as a PPTP Server with a Windows Operating system

Software Compatibility

Release Date	Doc. Version	Firmware	Additional Software	Change Description
17.3.2020	V1.1	V1.1.4(0c0c9fa)	PPTP_1.0.2 (6424848)	First release

Testing Topology

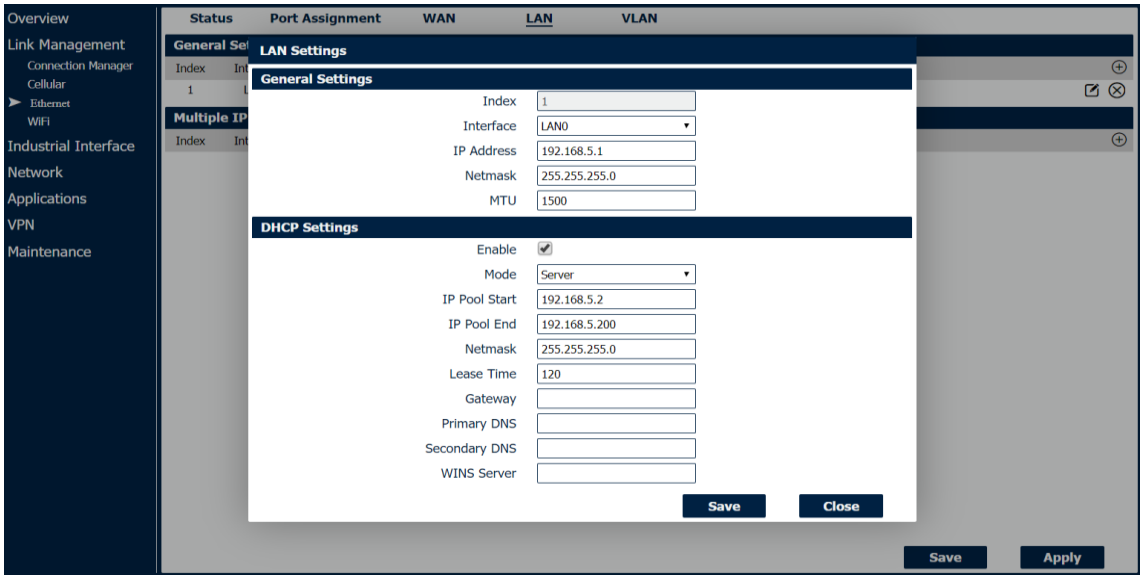


- The 6944 Router run as a PPTP server with a static public IP address.
- A PC with a Microsoft Windows Operating System works as a PPTP client.
- A PPTP VPN tunnel is established between the6944 router and the PC, allowing the PC to access the LAN device behind the 6944 Router.

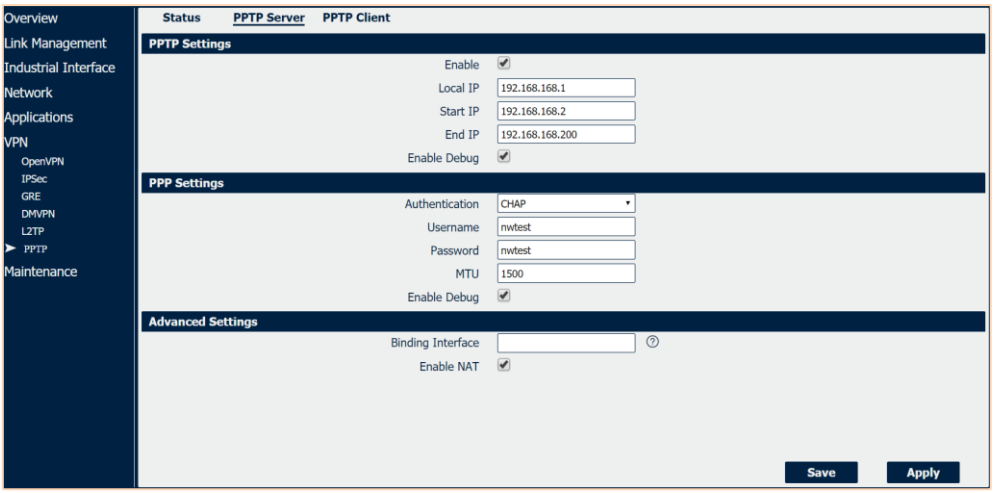
Configuration

PPTP Server Configuration

Step 1: Go to **Link Management>Ethernet>LAN**, specify the LAN IP address as 192.168.5.0/24, as shown below: **Then Click Save > Apply**

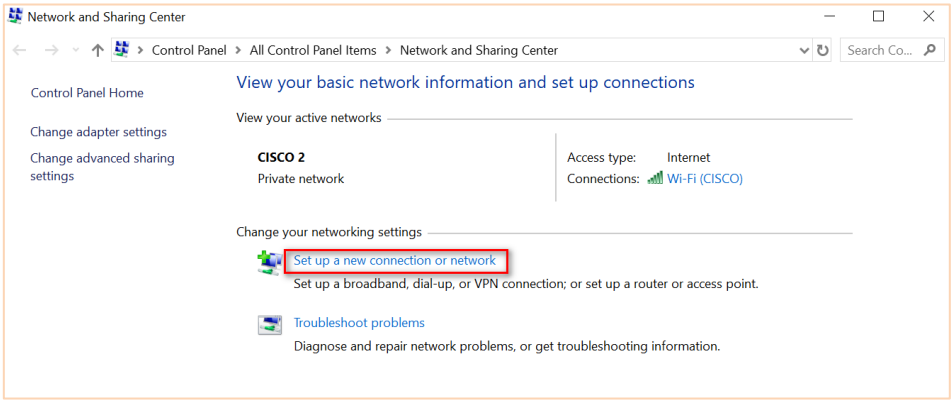


Step 2: Go to **VPN>PPTP>PPTP Server**, enable PPTP server and configure as shown below. **Click Save > Apply.**

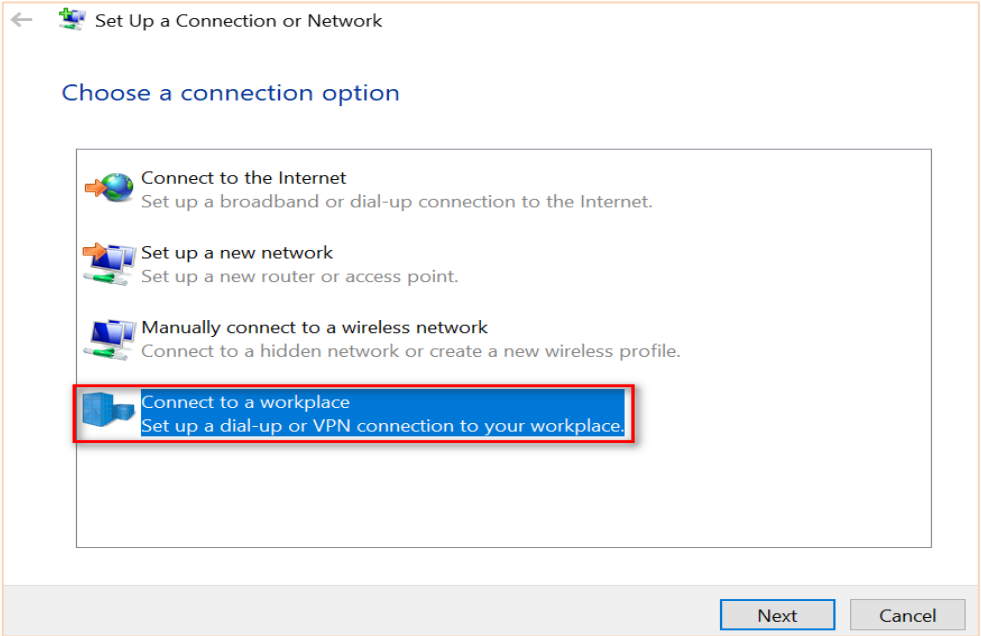


PPTP Client Configuration

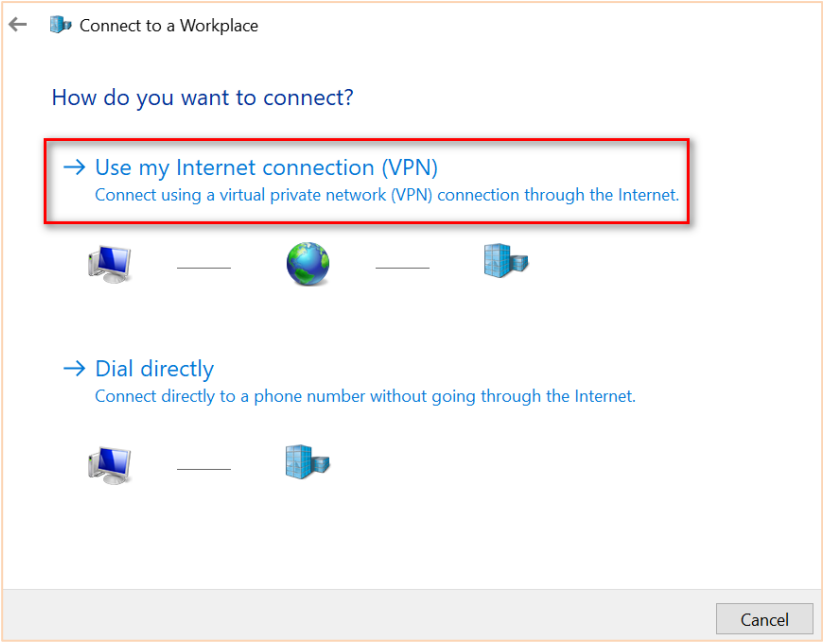
Step 1: Open the PC and go to "Network and Sharing Center", click "Set up a new connection or network:



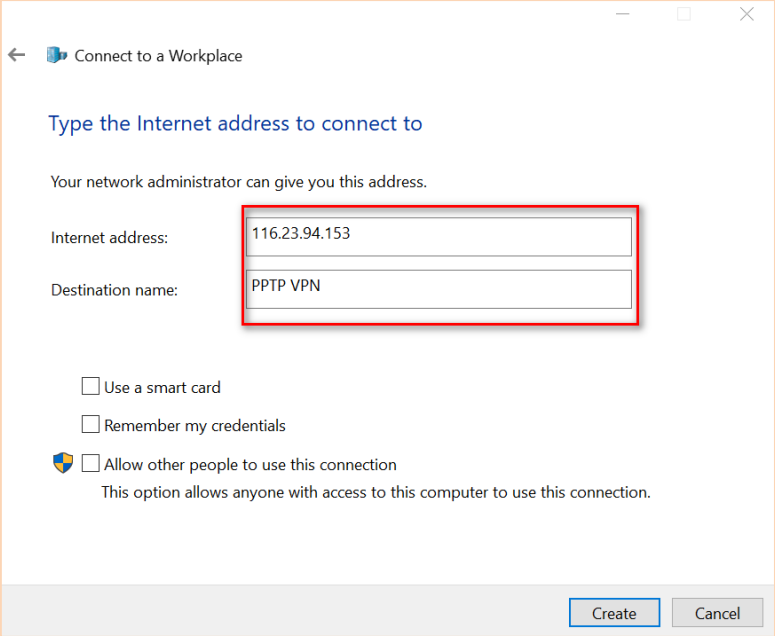
Step 2: Choose "Connect to a workplace" and click "Next":



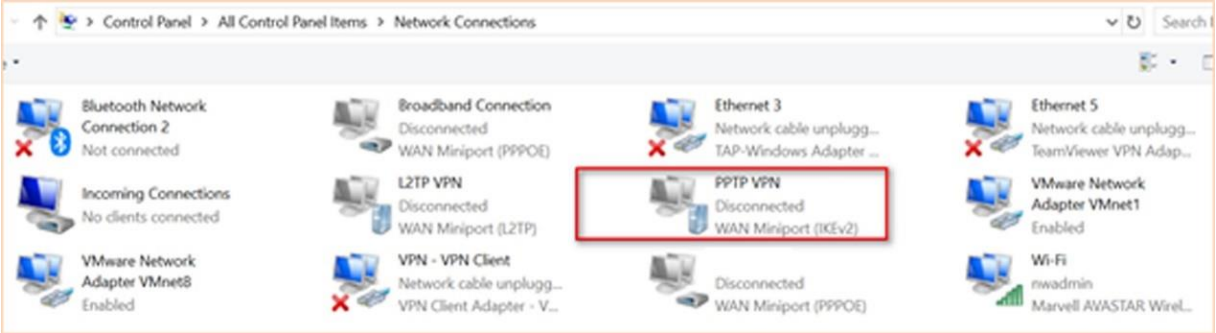
Step 3: Click "Use my Internet connection (VPN).

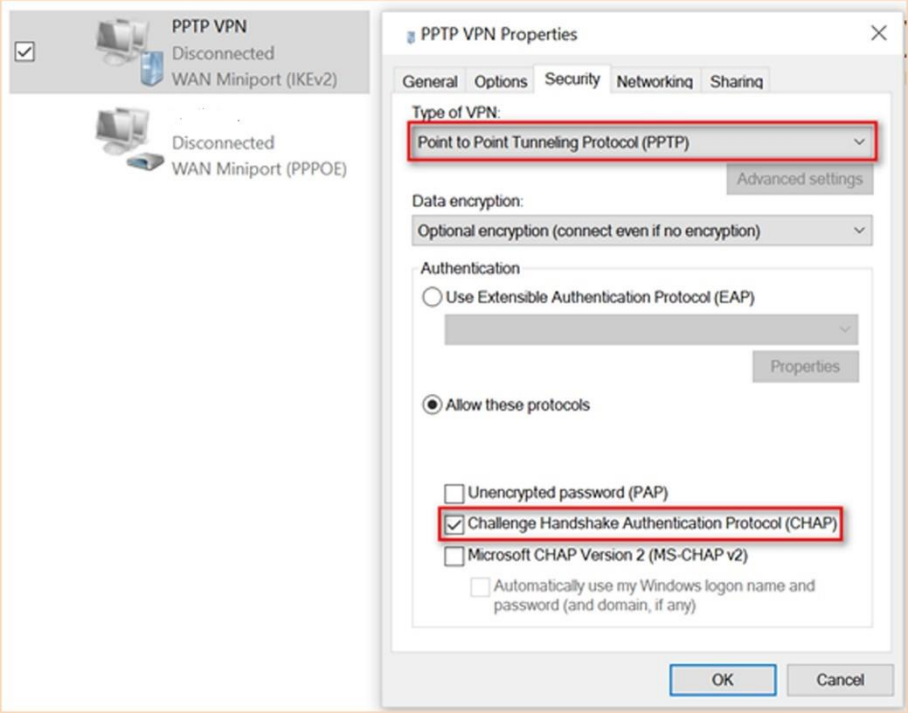


Step 4: Enter the PPTP Server IP address and Destination name, click "Create".

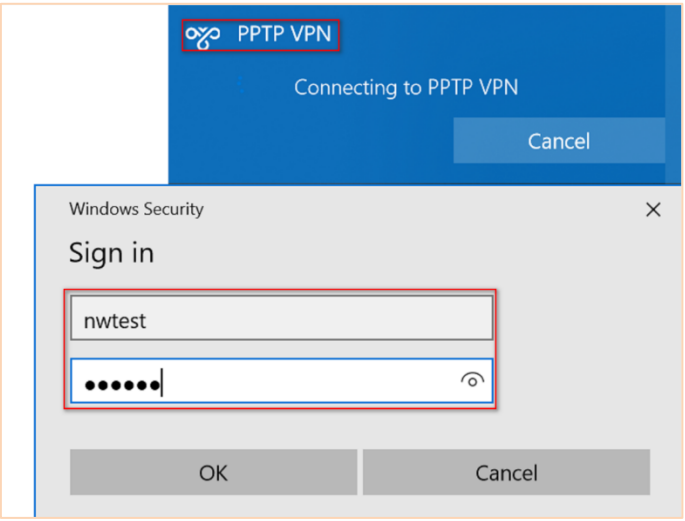


Step 5: After that, we create a PPTP connection, as shown below:

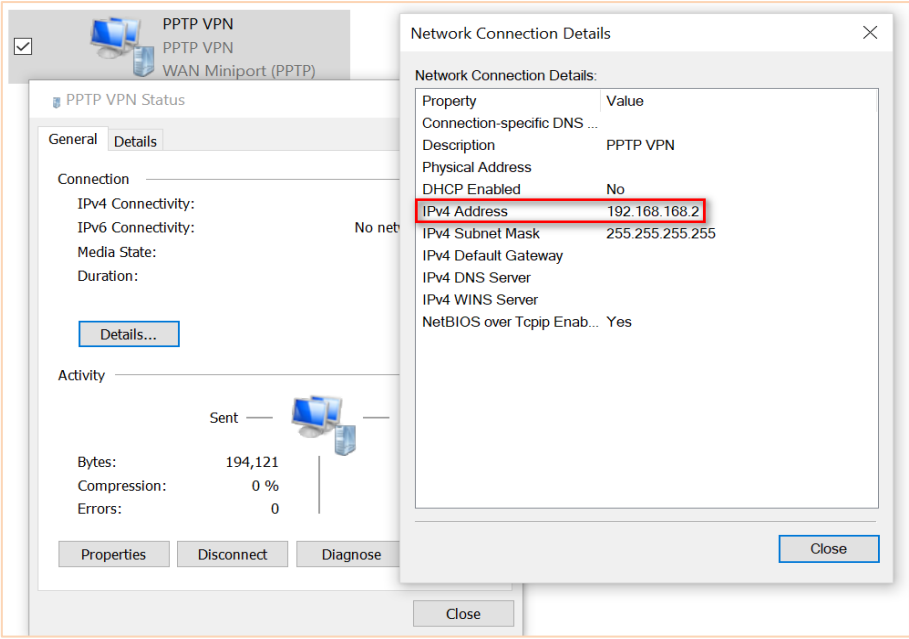




Step 6: After finishing all above settings, click to connect "PPTP VPN", and sign in with the Username and Password, Click "OK", as shown below

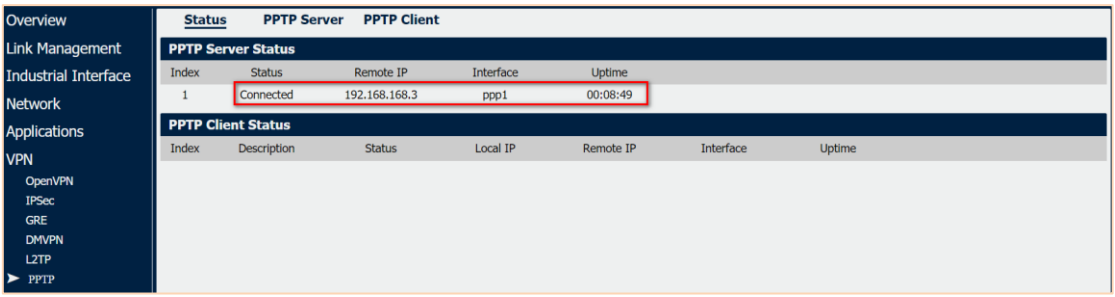


Step 7: Check the PPTP Client has connected to the PPTP Server successfully.
Right Click the "PPTP VPN", choose "Status", and go to "Details", then we can see that the PPTP Server had assigned an IP address to the PPTP Client.



Testing

Step 1: Go to **VPN>PPTP>Status**, the PPTP Client had connected to the PPTP Server successfully:



Step 2: Ping from the PPTP Client to the PPTP Server and ensure you receive a reply.

```
C:\>Users\Administrator>ping 192.168.5.1

Pinging 192.168.5.1. with 32 bytes of data
Reply from 192.168.5.1: bytes=32  time-13ms TTL=64
Reply from 192.168.5.1: bytes=32  time-1ms TTL=64
Reply from 192.168.5.1: bytes=32  time-1ms TTL=64
Reply from 192.168.5.1: bytes=32  time-4ms TTL=64

Ping statistics for 192.168.5.1
Packets: sent = 4, Received = 4, Lost=0   (0% loss)
Approximate round trip times in milli-seconds
Minimum = 1ms, Maximum = 13ms, Average = 4ms
```

16 Configuring DMVPN on the 6944

16.1. AN029 Configuring DMVPN with RIP to a Cisco Router

Introduction

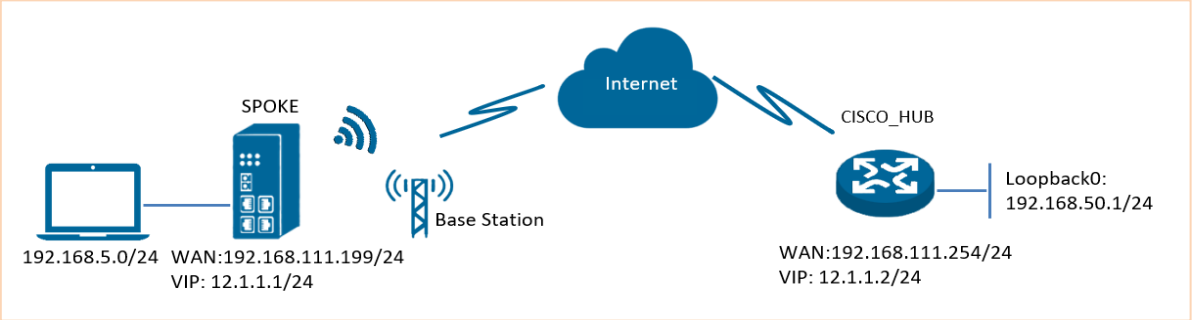
This document contains information explaining how to configure and use DMVPN with RIP on the Case Communications 6944 to a Cisco router. Software Versions

Software Compatibility

This feature requires the addition of Dynamic Routing software.

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
7/12/2018	V1.1	V1.1.4 (0c0c09fa)	DR:V1.0.1 (642848) DMVPN:V1.0.1(42ccf3e)	First release

Topology



- The 6944 runs as a DMVPN spoke remotely to an IP device, which can ping the DMVPN hub.
- The CISCO router is connected to the internet with a static IP Address and runs as a DMVPN hub.
- A tunnel is established between the spoke and hub, the subnets can PING each other successfully.
- Both the 6944 and the CISCO run RIP

Configuration

CISCO Hub Configuration

Step 1: The configuration of **CISCO** as shown below:

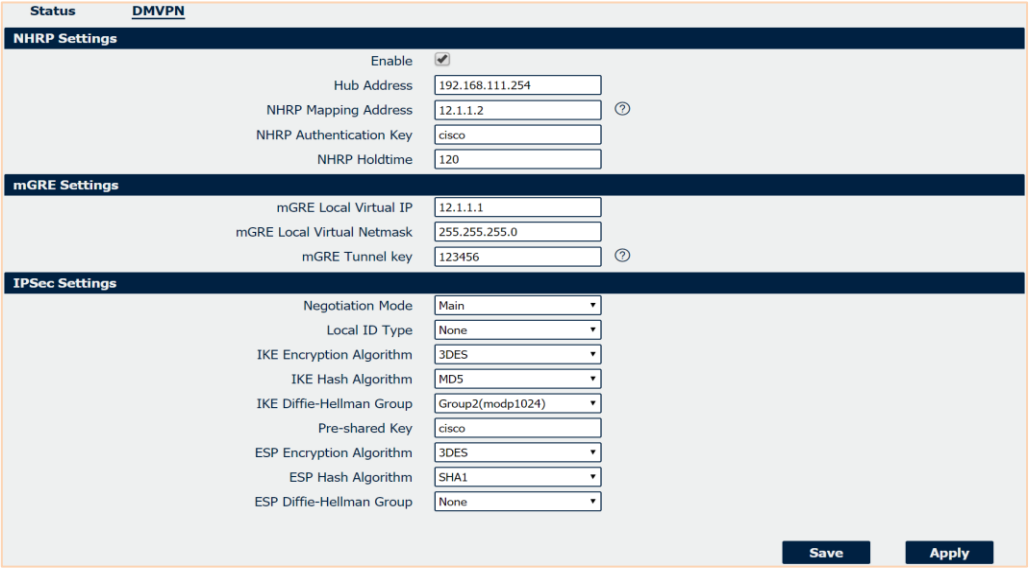
==========

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 cisco address 0.0.0.0
0.0.0.0
!
crypto ipsec transform-set DMVPN esp-3des
esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 3
 ip nhrp holdtime 120
 ip nhrp redirect
 no ip split-horizon
 tunnel source 192.168.111.254
 tunnel mode gre multipoint
 tunnel key 123456
 tunnel protection ipsec profile DMVPN-
PROFILE
!
interface FastEthernet0/0
```

```
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.6.3 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
router rip
 version 2
 network 12.0.0.0
 network 192.168.50.0
 no auto-summary
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.6.0 0.0.0.255
snmp-server community public RO
cisco2811#
```

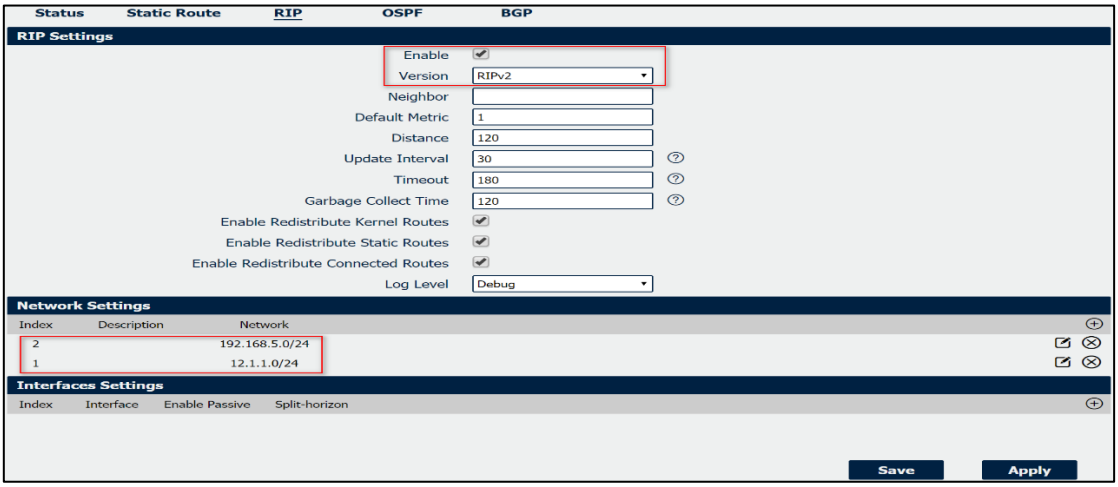
Spoke Configuration

Step 1: Go to **VPN>DMVPN**, enable DMVPN and configure DMVPN as shown below.



Step 2: Click Save>Apply.

Step 3: Go to **Network>Route>RIP,** enable RIP and configure RIP as shown below



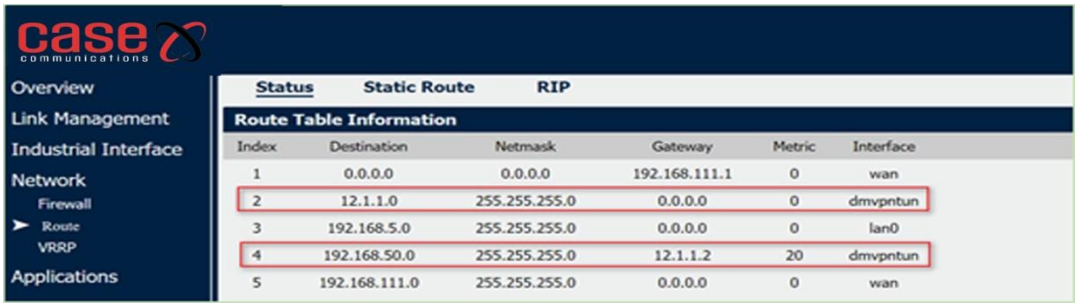
Step 4: Check the Router has connected to the CISCO HUB. Go to **VPN>DMVPN>Status** to check the connection status.

Check the Cisco Routing Table

Step 1: Check the Routing Table on the CISCO HUB for reference.

```
cisco2811#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

C    192.168.88.0/24 is directly connected, Loopback3
C    192.168.111.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
R    192.168.5.0/24 [120/1] via 12.1.1.1, 00:00:17, Tunnel1
     12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Tunnel1
C    192.168.50.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#
```

Step 2: Check the Routing Table on the 6944 SPOKE for reference.



Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.1	0	wan
2	12.1.1.0	255.255.255.0	0.0.0.0	0	dmvpntun
3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
4	192.168.50.0	255.255.255.0	12.1.1.2	20	dmvpntun
5	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

Testing

Step 1: Enable CMD and Ping from the end device attached to the 6944 SPOKE to the Cisco Hub subnet

```
Administrator: Command Prompt
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\Administrator>
```

Step 2: Ping from the CISCO HUB to the device connected to the 6944 SPOKE.

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
cisco2811#
```

16.2. AN030-Configuring DMVPN with OSPF

Introduction

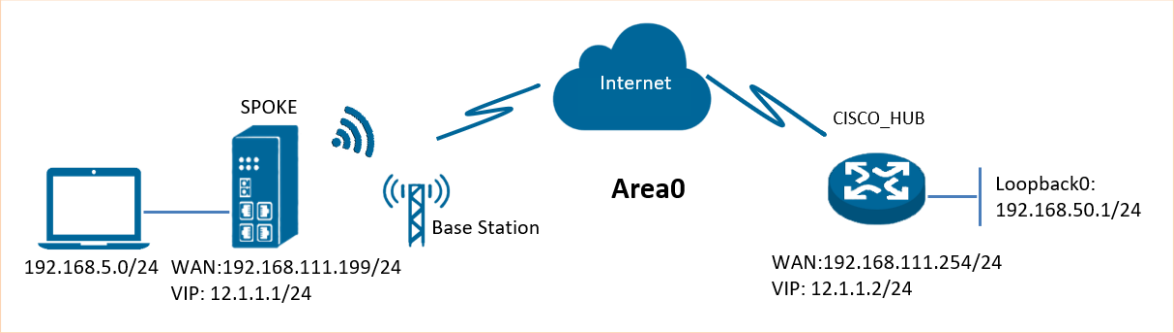
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running OSPF

6944 Software Versions

This feature requires the addition of Dynamic Routing software.

Release Date	Doc.Version	Firmware Version	Additional Software	Change Description
7/12/2018	V1.1	V1.1.4 (0c0c9fa)	DR:V1.0.1 (642848) DMVPN:V1.0.1(42ccf3e)	First release

Topology



- The 6944 runs as a DMVPN spoke with an IP device, which can ping the DMVPN hub.
- The CISCO router runs as a DMVPN hub with a static public IP Address.
- A tunnel is established between the spoke and hub, ensurethe subnets can PING each other.
- Both the 6944 and CISCO run OSPF within a same Area0.

Configuration

CISCO Configuration

Step 1: The configure the CISCO router as shown below:

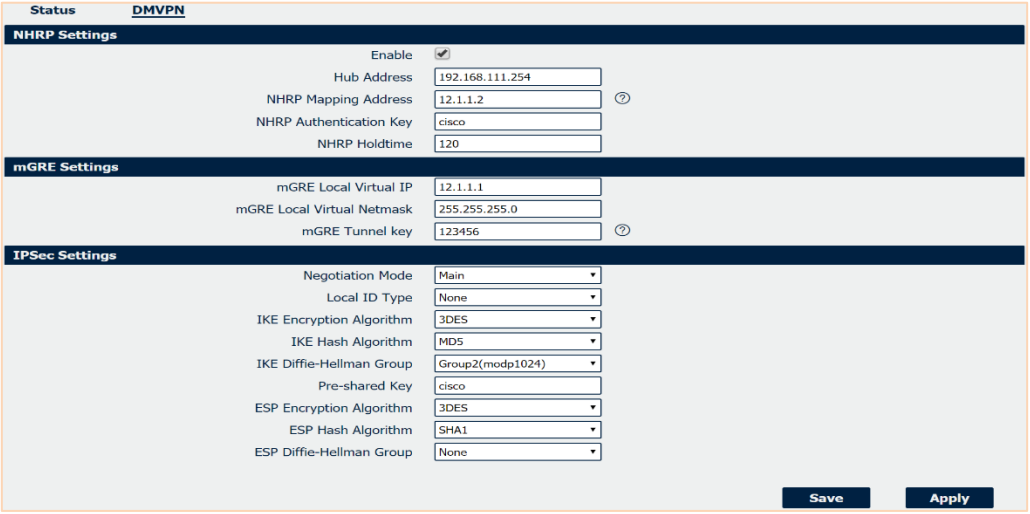
==========

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 cisco address 0.0.0.0
0.0.0.0
!
crypto ipsec transform-set DMVPN esp-3des
esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 3
 ip nhrp holdtime 120
 ip nhrp redirect
 no ip split-horizon
 ip ospf network non-broadcast
//Set to "non-broadcast" due to the limitation of
protocol
 tunnel source 192.168.111.254
 tunnel mode gre multipoint
 tunnel key 123456
 tunnel protection ipsec profile DMVPN-
PROFILE
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
```

```
 ip virtual-reassembly
 duplex full
 speed auto
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.6.3 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
router ospf 1
 router-id 9.9.9.9
 log-adjacency-changes
 network 12.1.1.0 0.0.0.255 area 0
 network 192.168.50.0 0.0.0.255 area 0
 neighbor 12.1.1.2
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.6.0 0.0.0.255
snmp-server community public RO
cisco2811#
```

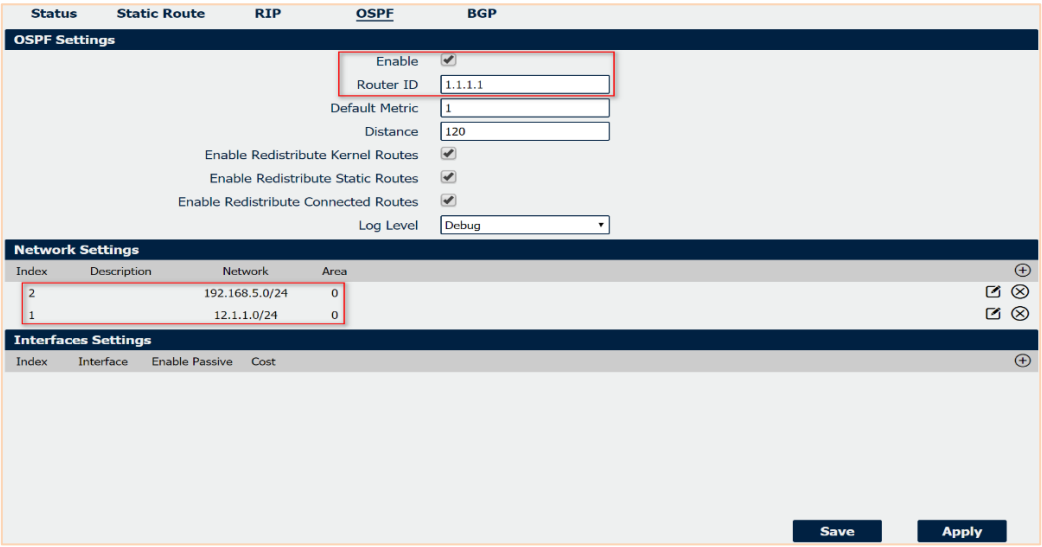
Spoke Configuration

Step 1: Go to **VPN>DMVPN**, enable DMVPN and configure DMVPN as shown below.

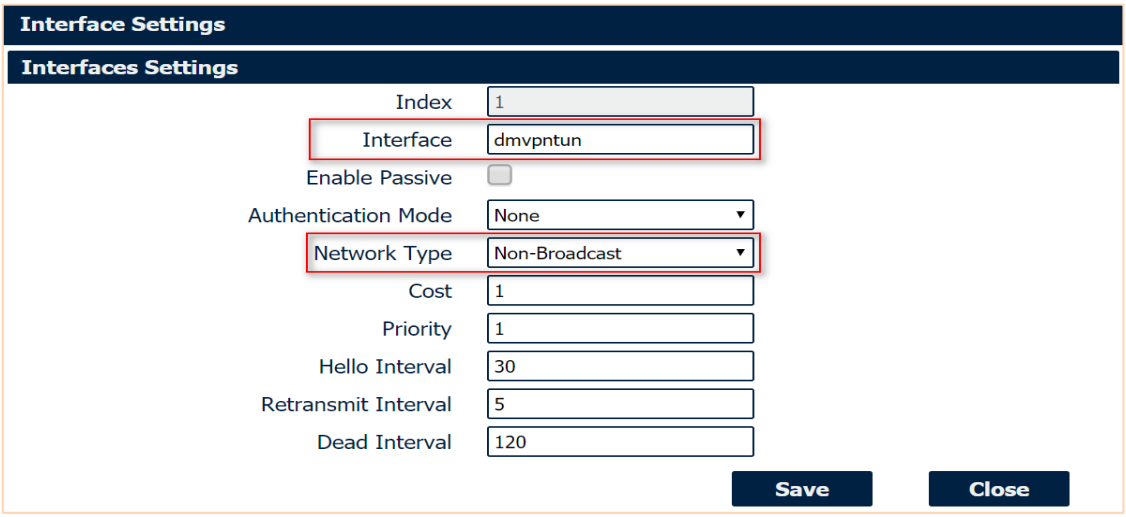


Step 2. Click Save>Apply.

Step 3. Go to **Network>Route>OSPF,** enable OSPF and configure OSPF as shown below.



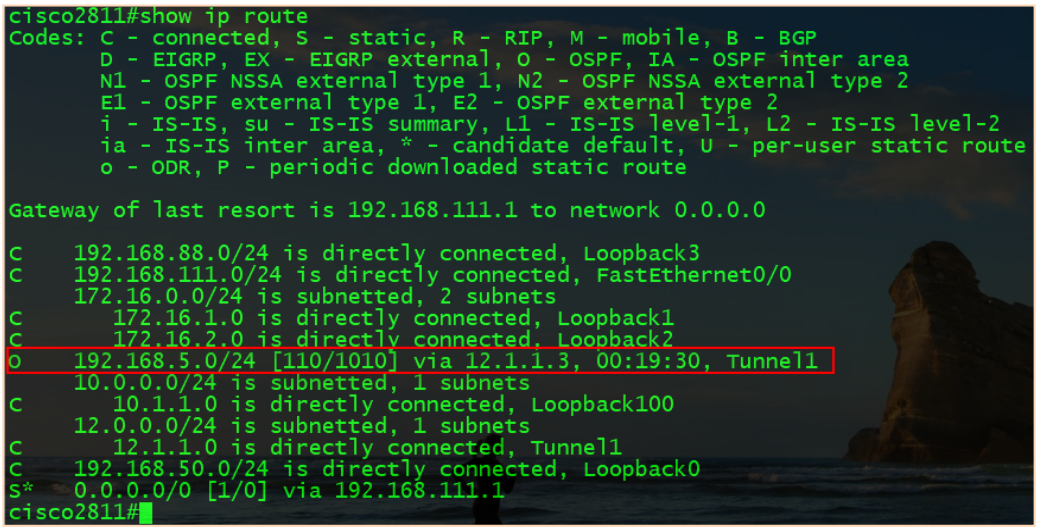
Step 4. Go to **Network>Route>OSPF>Interface Settings**, to specify the Interface Network Type as "**Non-Broadcast**" as shown below



Step 5.Check the Router has connected to the CISCO HUB. Go to **VPN>DMVPN>Status** to check the connection status.

Check the Routing Tables

Step 1: Check the Routing Table on the CISCO HUB for reference.



```
cisco2811#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

C    192.168.88.0/24 is directly connected, Loopback3
C    192.168.111.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
O    192.168.5.0/24 [110/1010] via 12.1.1.3, 00:19:30, Tunnel1
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback100
     12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Tunnel1
C    192.168.50.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#
```

Step 2: Check the Routing Table on the 6944 SPOKE for reference.

Testing

Step 1: Enable a CMD Ping from the end device of the 6944 SPOKE to the subnet on the CISCO HUB.

```
Administrator: Command Prompt
C:\Users\Administrator>
C:\Users\Administrator>ping 192.168.50.1

Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254
Reply from 192.168.50.1: bytes=32 time=4ms TTL=254

Ping statistics for 192.168.50.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 4ms, Maximum = 4ms, Average = 4ms

C:\Users\Administrator>
```

Step 2: Ping from the device connected to the CISCO HUB to the device connected to the 6944 SPOKE.

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
cisco2811#
```

Step 3: Test successful.

16.3. AN031 - Configuring DMVPN with BGP to a Cisco Router

Introduction

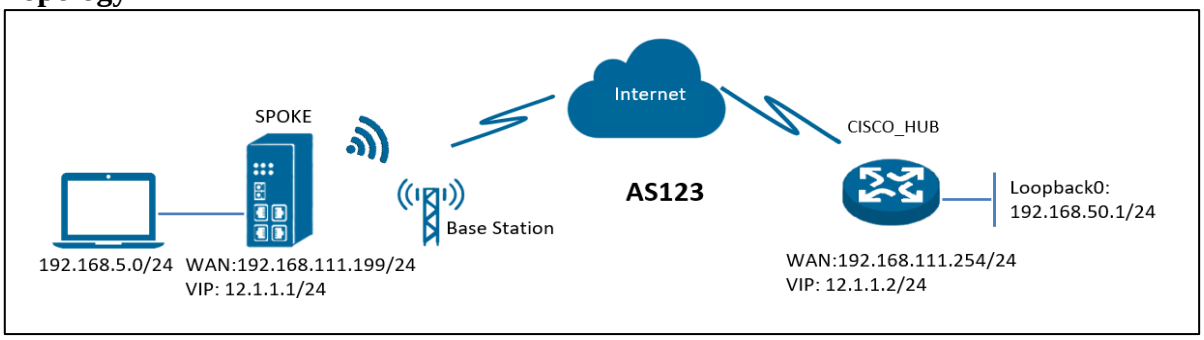
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running BGP

Software Compatibility

This applications requires the addition of Dynamic Routing software.

Release Date	Doc. Version	Firmware Version	Software Version	Change Description
7/12/2018	V1.1	Devel (baba6c2) or newer	DR:V1.0.1 (642848) DMVPN:V1.0.1(42ccf3e)	First release

Topology



- The 6944 runs as a DMVPN spoke with an IP device, which can ping the DMVPN hub.
- The CISCO router runs as DMVPN hub and has a static public IP Address.
- A tunnel is established between the 6944 spoke and Cisco hub, the subnets can PING each other.
- Both the 6944 and CISCO Router run BGP within a same AS123.

Configuration

CISCO Configuration

Step 1: Configure the CISCO router as shown below:

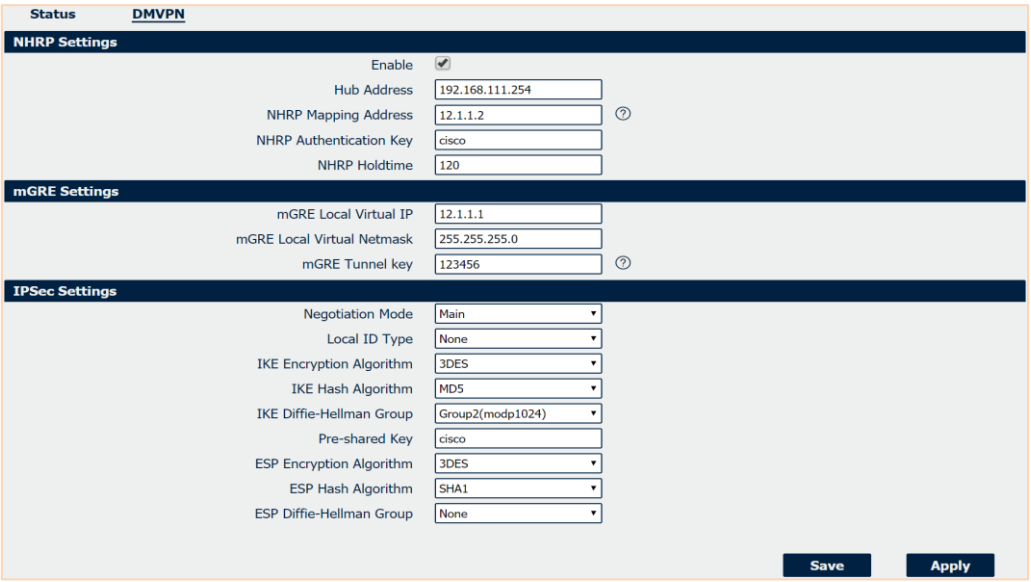
==========

```
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
ip address-pool local
no ipv6 cef
!
username cisco password 0 cisco
!
crypto isakmp policy 10
 encr 3des
 hash md5
 authentication pre-share
 group 2
crypto isakmp key 6 cisco address 0.0.0.0
0.0.0.0
!
crypto ipsec transform-set DMVPN esp-3des
esp-sha-hmac
mode transport
!
crypto ipsec profile DMVPN-PROFILE
 set transform-set DMVPN
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface Tunnel1
 ip address 12.1.1.2 255.255.255.0
 no ip redirects
 ip nhrp authentication cisco
 ip nhrp map multicast dynamic
 ip nhrp network-id 3
 ip nhrp holdtime 120
 ip nhrp redirect
 no ip split-horizon
tunnel source 192.168.111.254
 tunnel mode gre multipoint
 tunnel key 123456
 tunnel protection ipsec profile DMVPN-
PROFILE
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
 ip nat enable
 ip virtual-reassembly
 duplex full
 speed auto
```

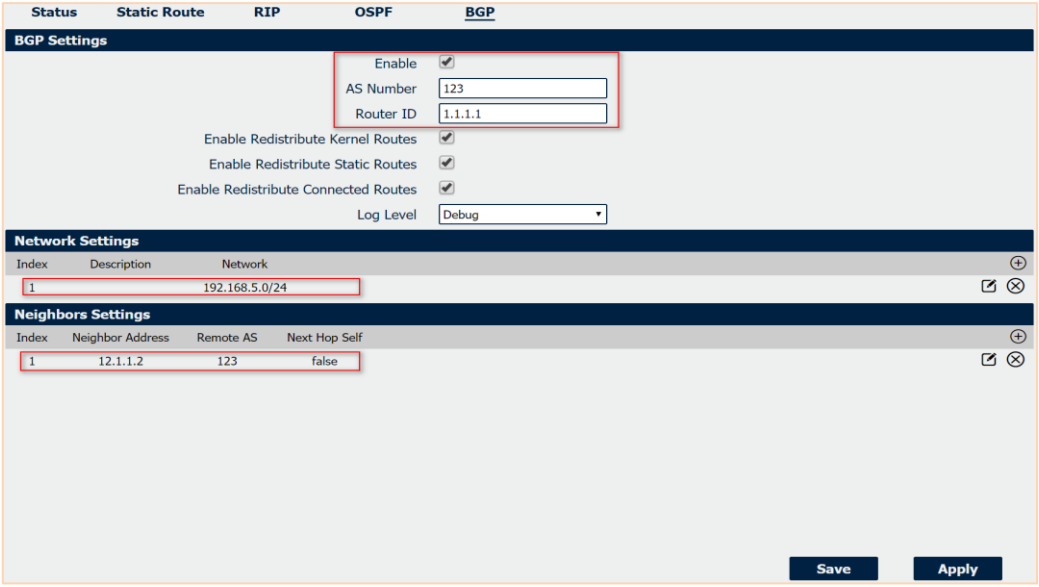
```
 no mop enabled
!
interface FastEthernet0/1
 ip address 192.168.6.3 255.255.255.0
 ip nat inside
 ip nat enable
 ip virtual-reassembly
 duplex auto
 speed auto
!
router bgp 123
 no synchronization
 bgp router-id 2.2.2.2
 bgp log-neighbor-changes
 network 192.168.50.0
 neighbor 12.1.1.1 remote-as 123
 no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.6.0 0.0.0.255
snmp-server community public RO
cisco2811#
```

Spoke Configuration

Step 1: Go to **VPN>DMVPN**, enable DMVPN and configure DMVPN as shown below



Step 2: Go to Network>Route>BGP, enable BGP and configure BGP as shown below



Step 3: A Route has connected to the CISCO HUB. Go to **VPN>DMVPN>Status** to check the connection

Routing Tables

Step 1: Check the Routing Table on the CISCO HUB for reference.

```
cisco2811#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

C    192.168.88.0/24 is directly connected, Loopback3
C    192.168.111.0/24 is directly connected, FastEthernet0/0
     172.16.0.0/24 is subnetted, 2 subnets
C       172.16.1.0 is directly connected, Loopback1
C       172.16.2.0 is directly connected, Loopback2
B    192.168.5.0/24 [200/0] via 12.1.1.3, 00:03:14
     10.0.0.0/24 is subnetted, 1 subnets
C       10.1.1.0 is directly connected, Loopback100
     12.0.0.0/24 is subnetted, 1 subnets
C       12.1.1.0 is directly connected, Tunnel1
C    192.168.50.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#
```

Step 2: Check the 6944 SPOKE Routing Table for reference.

Testing

Step 1: Send a Ping from the device on the 6944 SPOKE to the subnet of CISCO HUB.

```
C:\>\Users\Administrator>Ping 192.168.50.1
Pinging 192.168.50.1. with 32 bytes of data
Reply from 192.168.50.1 bytes=32  time= 4ms TTL=254
Reply from 192.168.50.1 bytes=32  time= 4ms TTL=254
Reply from 192.168.50.1 bytes=32  time=4ms TTL=254
Reply from 192.168.50.1 bytes=32  time=4ms TTL=254

Ping statistics for 192.168.50.1
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip times in milli seconds
Minimum = 4ms, Maximum = 4ms, Average = 4ms
```

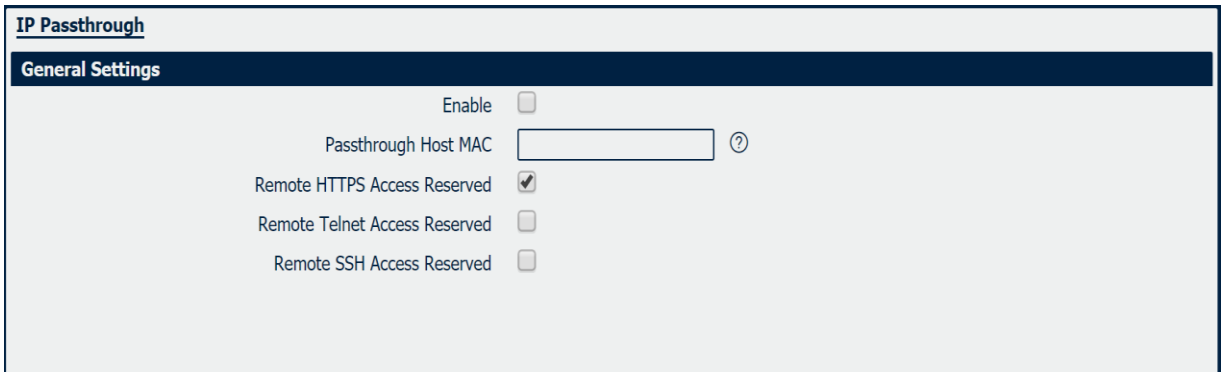
Step 2: Ping from the CISCO HUB to the device connected to the 6944 SPOKE.

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms
cisco2811#
```

17 IP Pass through

Overview

IP Pass through mode, disables NAT and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of Network Address Translation (NAT) in order to make the router "transparent" in the communication process.



Network->IP Passthrough

- **Enable**
  Check this box will enable IP Passthrough.
- **Passthrough Host MAC**
  Enter the MAC of passthrough host to receive the WAN IP address.
- **Remote HTTPS Access Reserved**
  Check this box to allow to remote access the router via https while enable IP Passthrough mode.
- **Remote Telnet Access Reserved**
  Check this box to allow to remote telnet to the router while enable IP Passthrough mode.
- **Remote SSH Access Reserved**
  Check this box to allow to remote SSH to the router while enable IP Passthrough mode.

This page left blank intentionally

18 Industrial Interface.

18.1. Industrial Interface Overview on the 6944

The Industrial page contains tabs for making configuration settings to the Serial RS232 and RS485, Digital input and output. Select Serial & Digital IO from the main navigation menu to navigate to this page.

Serial Connection

Review the status of serial connection.

Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status
1	false	RS485	Transparent	TCP Client	Disconnected
2	false	RS232	Transparent	TCP Client	Disconnected

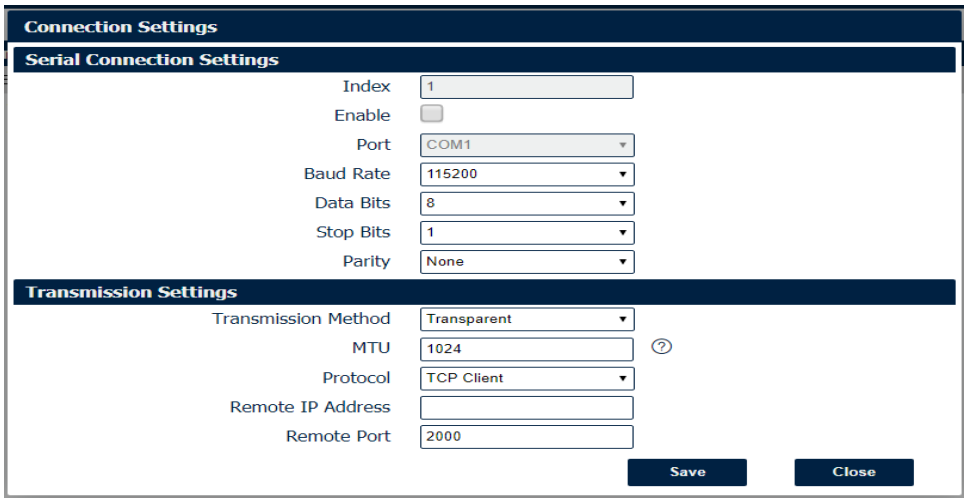
Serial->Status

- **Enable -** Displays status of current serial function.
- **Serial Type -** Displays the serial type of COM port.
- **Transmission Method -** Displays the transmission method of this serial port.
- **Protocol -** Displays the protocol used by this serial port.
- **Connection Status -** Displays the connection status of this serial port.

Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity
1	false	COM1	115200	8	1	None
2	false	COM2	115200	8	1	None

Serial->Connection

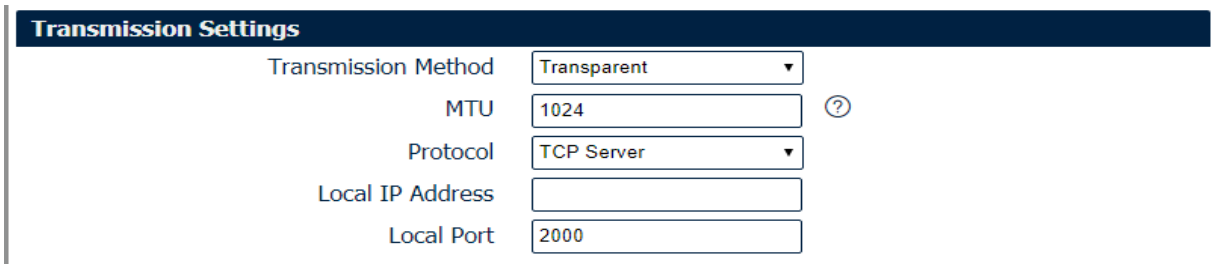
- **Enable -** Displays status of current serial function.
- **Port -** Displays the serial type of COM port.
- **Baud Rate -** Displays the serial port baud rate.
- **Data Bits -** Displays the serial port Data Bits.
- **Stop Bits -** Displays the serial port Stop Bits.
- **Parity -** Displays the serial port parity.



Serial->Connection Settings

- **Baud Rate -** Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.
- **Data Bits -** Select the values from 7 or 8.
- **Stop Bits -** Select the values from 1 or 2.
- **Parity -** Select values from none, even, odd.
- **Transmission Method -** Select the transmission method for serial port. Optional for "Transparent", "Modbus RTU Gateway" and "Modbus ASCII Gateway".
- **MTU -** Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1024 in most cases.
- **Protocol -** Select the mode for Serial IP communication. Supported modes are UDP, TCP Server, or TCP Client.
- **Remote IP Address -** Enter the IP address of the remote server.
- **Remote Port -** Enter the port number of the remote server.

The screen titled Transmission Settings (shown below) displays different settings when you select **TCP Server** on Protocol.

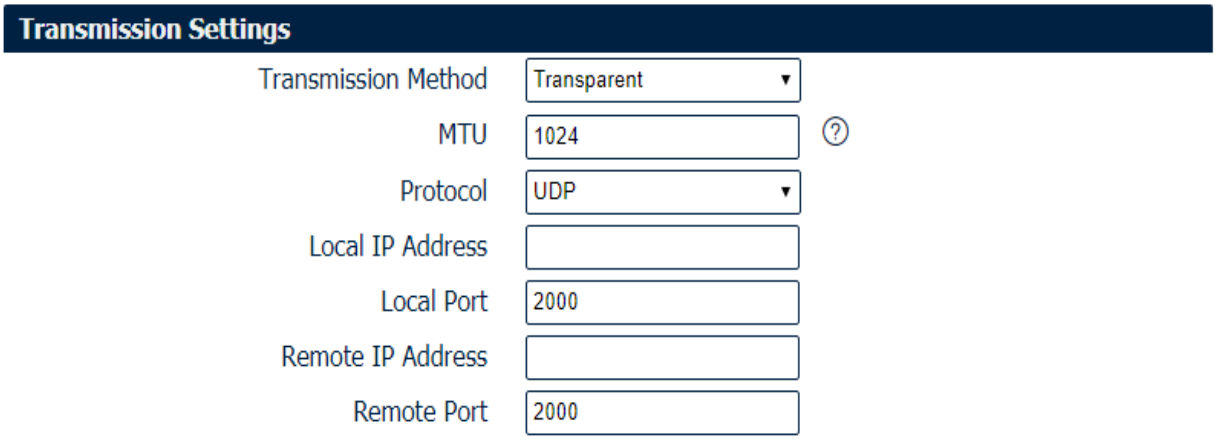


Serial->Connection Settings

- **Local IP Address**
  Enter the IP Address of the local endpoint.
- **Local Port**

The port number assigned to the serial IP port on which communications will take place.

Below window displays different settings when you select **UDP** on Protocol.



- **Local IP Address -** Enter the IP Address of the local endpoint.
- **Local Port -** The port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address -** Enter the IP address of the remote server.
- **Remote Port -** Enter the port number of the remote server.

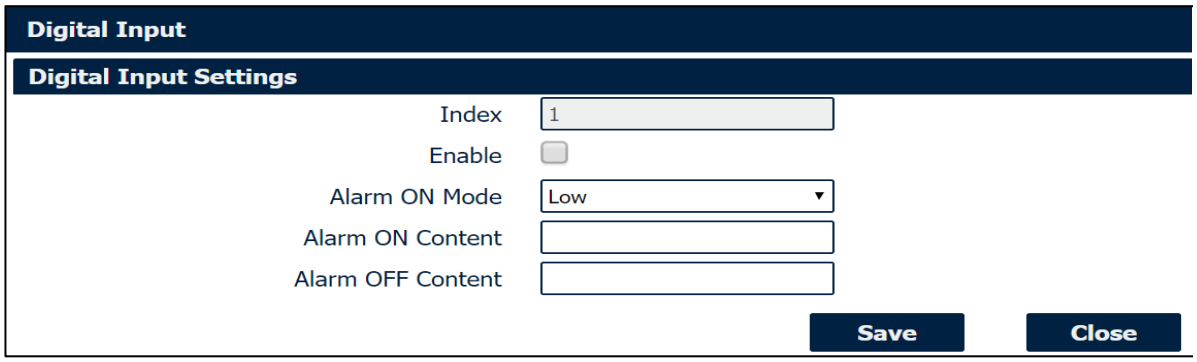
Digital IO

This section allows you to set the Digital IO parameters. The Digital input can be used for triggering an alarm, and Digital output or could be used for controlling a slave device by digital signal.
You could review the status of Digital IO as below.

Status	Digital IO		
Digital Input Information			
Index	Enable	Logic Level	Status
1	false	High	Alarm OFF
2	false	High	Alarm OFF
Digital Output Information			
Index	Enable	Logic Level	Status
1	false	Low	Alarm OFF
2	false	Low	Alarm OFF

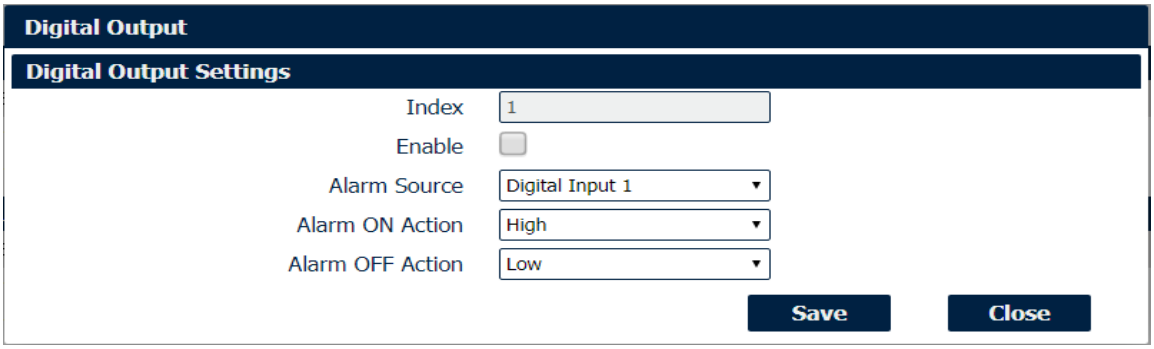
Digital IO->Status

- **Enable -** Displays status of current digital IO function.
- **Logic Level -** Displays the electrical level of digital IO port.
- **Status -** Displays the alarm status of digital IO port.



Digital IO->Digital Input

- **Enable -** Check this box to enable digital Input function.
- **Alarm ON Mode -** Select the electrical level to trigger alarm. Option are “Low” and “High”.
- **Alarm ON Content -** Specify the alarm on content to be sent out via SMS message
- **Alarm OFF Content -** Specify the alarm off content to be sent out via SMS message.



Digital IO->Digital Output

- **Enable**
  Check this box to enable digital output function.
- **Alarm Source**
  Select from “Digital Input1”, “Digital Input2” or “SMS”, Digital output triggers the related action when there is alarm comes from Digital Input or SMS.
- **Alarm ON Action**
  Select from “High”, “Low” or “Pulse”. High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.
- **Alarm OFF Action**
  Initiates when alarm disappeared. Select from “High”, “Low” or “Pulse”. High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.
- **Pulse Width**
  This parameter is available when select “Pulse” as “Alarm ON Action/Alarm OFF Action”. The selected digital output channel will generate a square wave as specified in the pulse mode parameters.

18.2. AN004 Transparent Mode with TCP Client on RS232

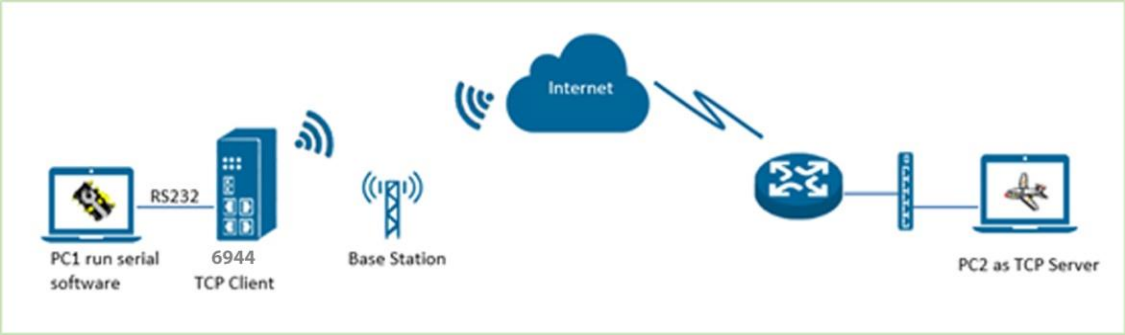
Overview

This document contains information on how to configure and use RS232 Transparent Mode with a TCP Client.

Software Version - This feature works with standard software

Release Date	Doc. Version	Firmware Version	Additional sw	Change Description
3.8.2018	V1.1	V1.1.1.4 (0c0c09fa)	Std Software	First released

Testing Topology



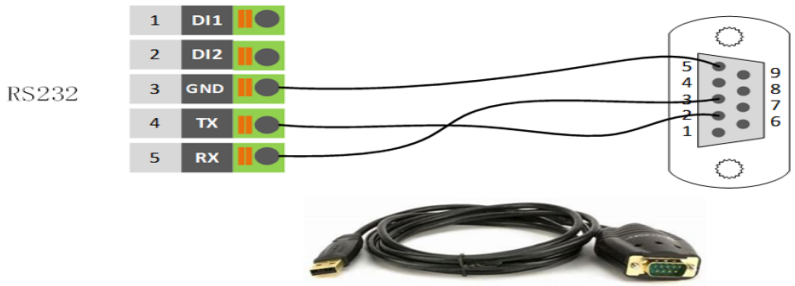
- The 6944 runs as a TCP Client and connects to the Internet via its SIM card.
- PC1 simulates as a serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through 6944 in TCP transparent mode.
- PC2 runs as a TCP server getting its Public Static IP address from the Internet. PC2 enables TCP software, such as TCPUDPDbg. TCPUDPDbg allowing it to receive the data from TCP Client side.

Configuration

RS232 Cable - Step 1: **Please see the image below on how to make the RS232 cable:**

- **Serial Port & DIDO**

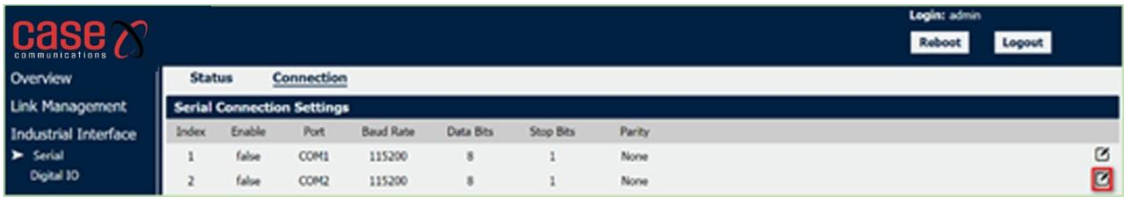
PIN	RS232	RS485	DI	DO	Direction
1	--	--	--	DO1	Router-->Device
2	--	--	--	DO2	Router-->Device
3	--	--	--	COM	--
4	--	A	--	--	Router<-->Device
5	--	B	--	--	Router<-->Device
6	--	--	DI1	--	Router<--Device
7	--	--	DI2	--	Router<--Device
8	GND	--	--	--	--
9	TX	--	--	--	Router-->Device
10	RX	--	--	--	Router<--Device



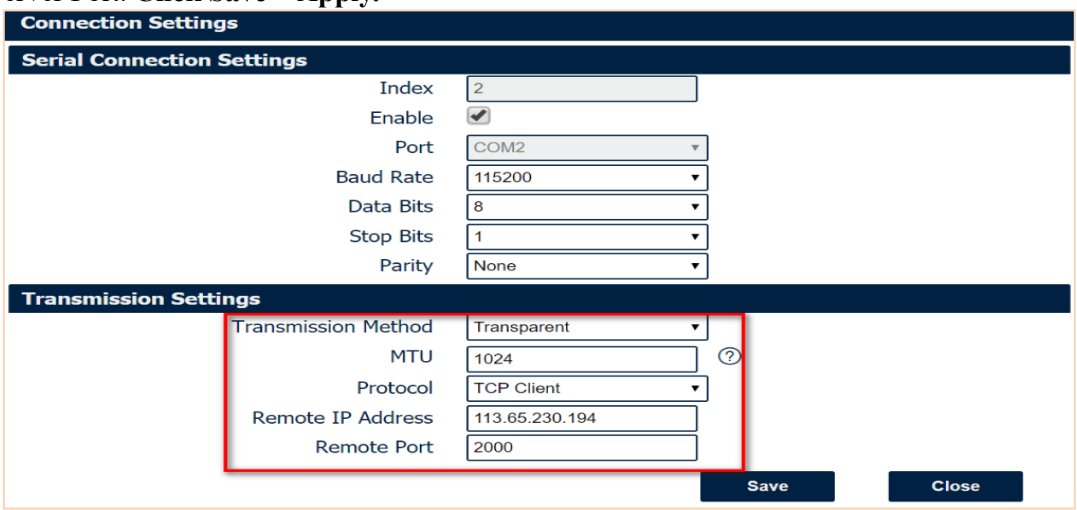
Configuration

RS232 Configuration

Step1. Go to Link **Industrial Interface>Serial>Connection>Index 2**, Click the **Edit button** of COM2.

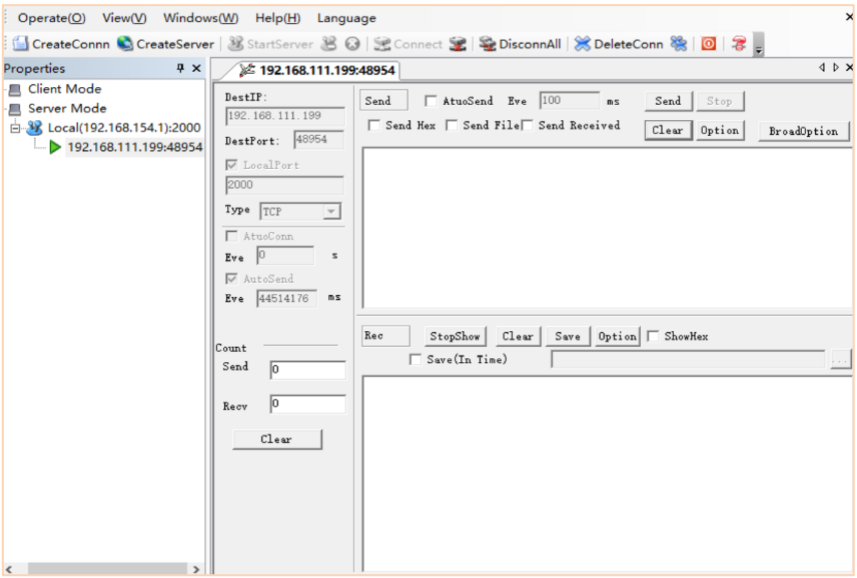


Step 1: Enable the RS232 setting, select the Protocol as "TCP Client" and enter the Server IP address and Server Port. **Click Save > Apply.**

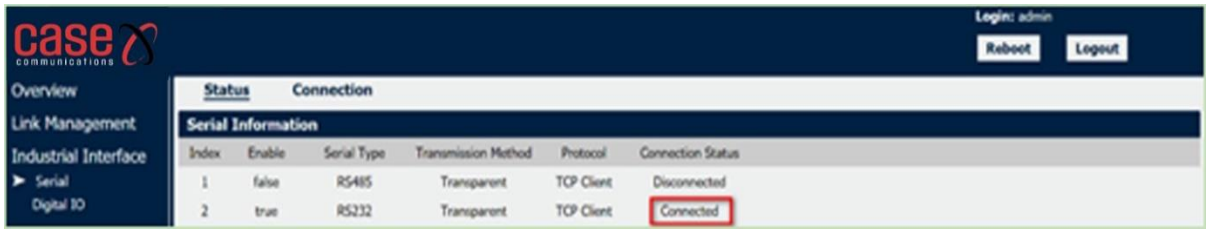


TCP Server Configuration

Step 1. Run the TCP Software "TCPUDPDbg" on server PC2, the 6944 will connect to the TCP Server automatically.

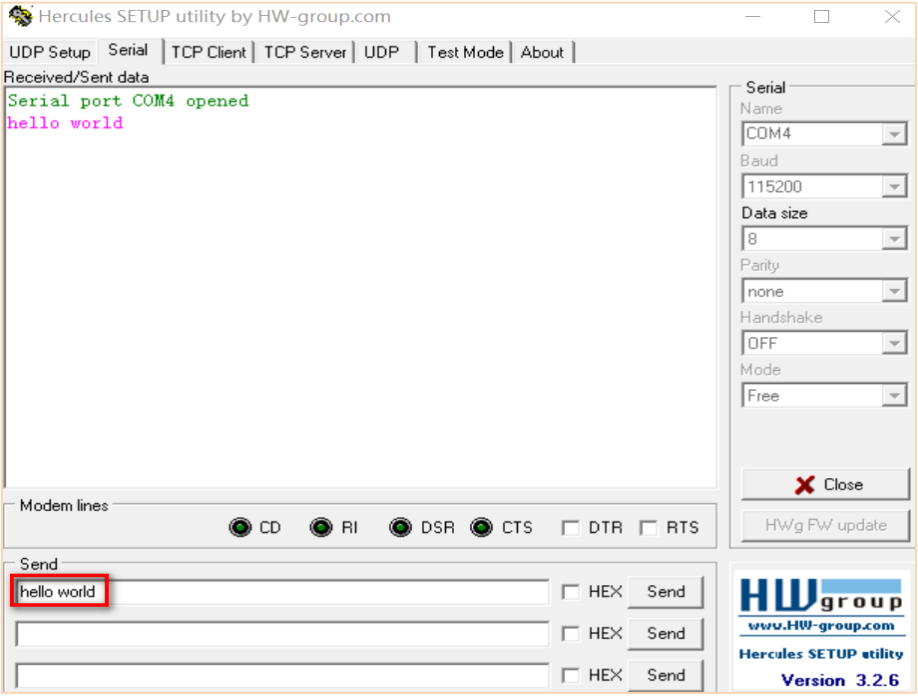


Step 2: Go to **Industrial Interface>Serial>Status>Serial Information>Index2**, it will show the connection status.



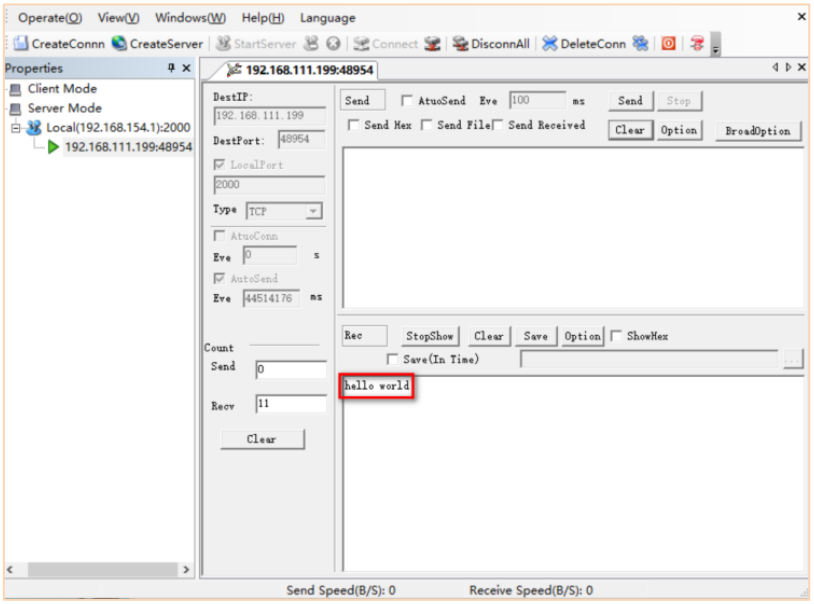
Testing

Step 1: Run the serial software "Hercules" on PC1, send the data "hello world".



Step 2: Test Result

Step 3: TCP Server side can receive the data "hello world"



18.3. AN005 RS485 Transparent Mode

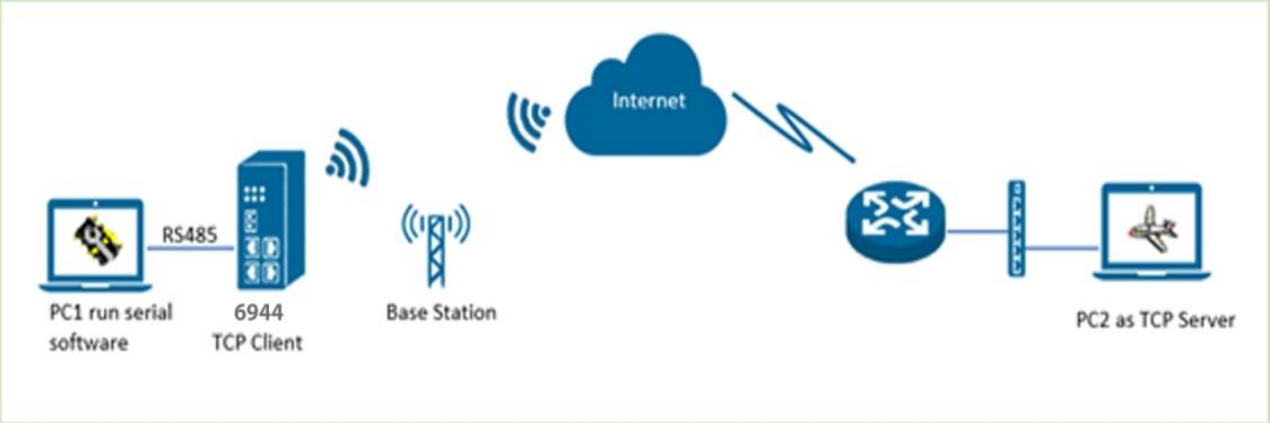
Overview

This document contains information regarding the configuration of RS485 in Transparent Mode with using a TCP Client on the 6944.

Software Version

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
3.8.2018	V1.0.0	V1.1.4 (0c0c9fa)	Std Software	First released

Testing Topology

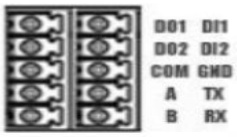


- The 6944 runs as a TCP Client and connect to the Internet with a SIM card.
- PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server through the 6944 with TCP transparent mode.
- PC2 runs as a TCP server and connected to the Internet via a Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg allowing it to receive the data from TCP Client side.

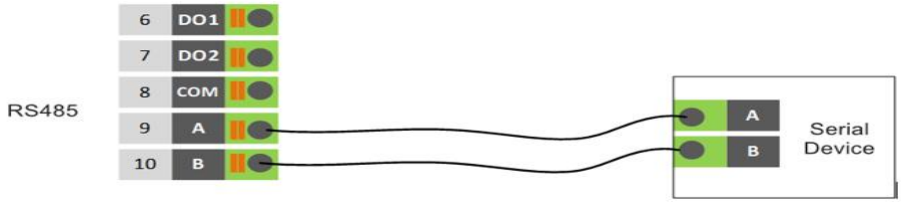
Configuration

RS485 Cable - Step1. **Please follow below picture to make the RS485 cable:**

- **Serial Port & DIDO**



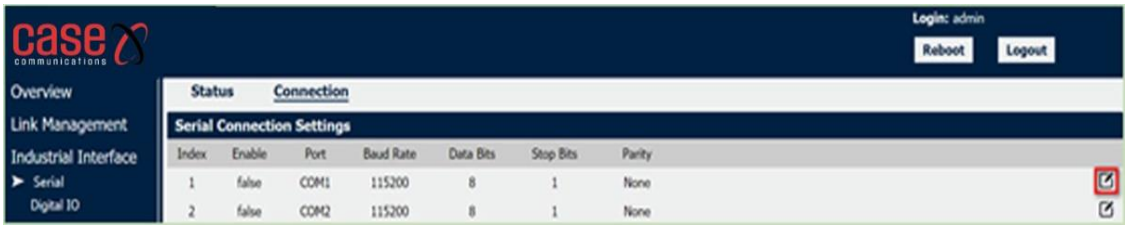
PIN	RS232	RS485	DI	DO	Direction
1	--	--	--	DO1	Router-->Device
2	--	--	--	DO2	Router-->Device
3	--	--	--	COM	--
4	--	A	--	--	Router<-->Device
5	--	B	--	--	Router<-->Device
6	--	--	DI1	--	Router<--Device
7	--	--	DI2	--	Router<--Device
8	GND	--	--	--	--
9	TX	--	--	--	Router-->Device
10	RX	--	--	--	Router<--Device



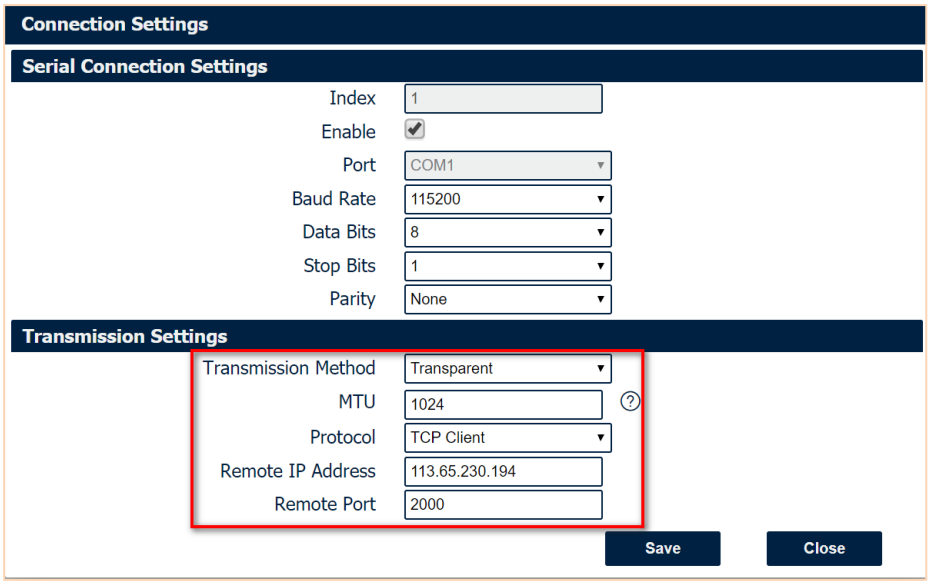
Configuration

<u>RS485 Configuration</u>

Step1. Go to Link **Industrial Interface>Serial>Connection>Index 1**, Click the **Edit button** of COM1.

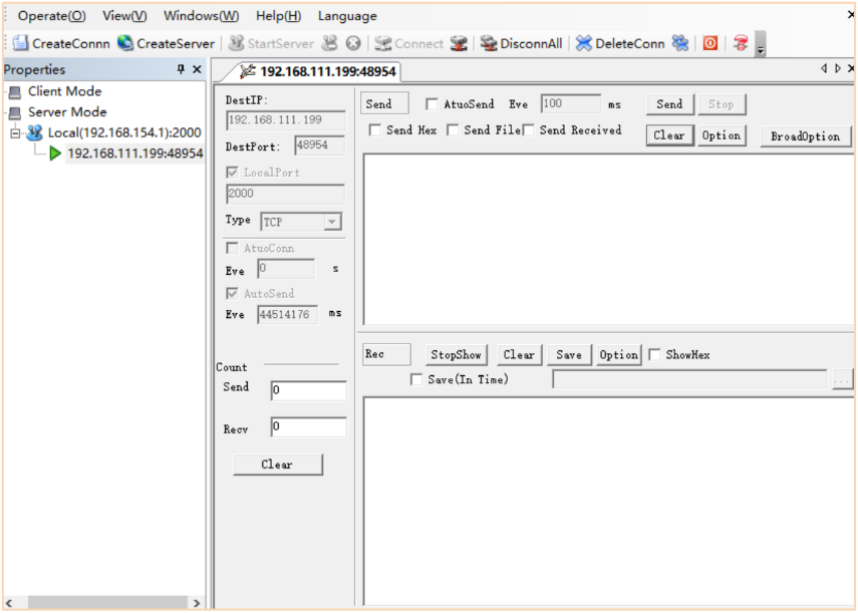


Step 2: Enable the RS485 setting, select Protocol as "TCP Client" and enter the Server IP address and Server Port. **Click Save > Apply**



TCP Server Configuration

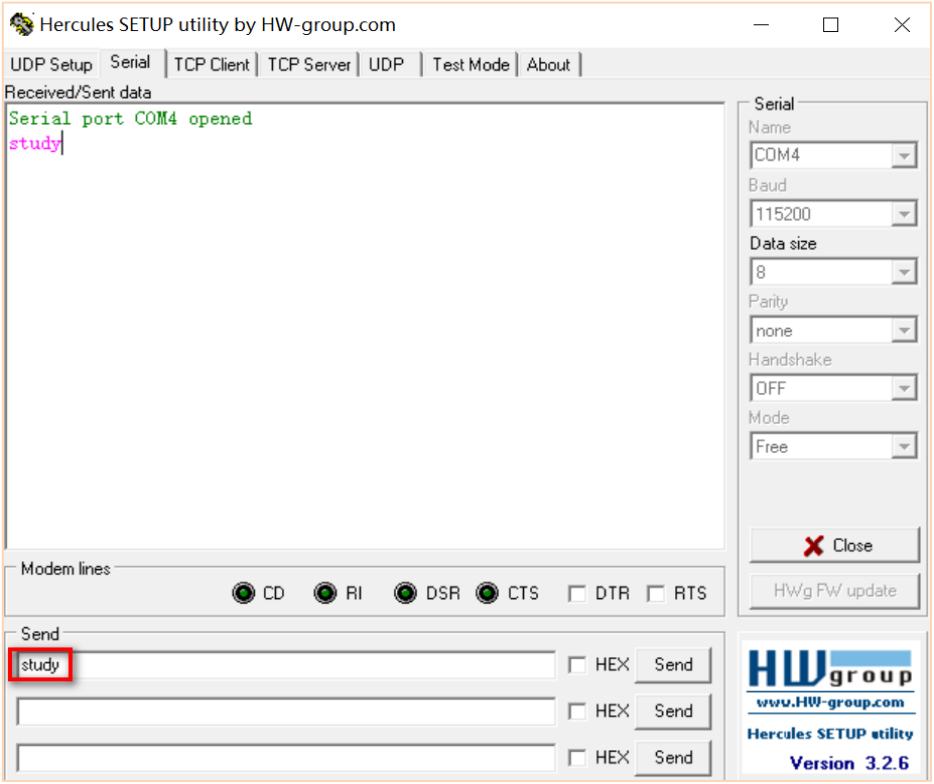
Step1. Run TCP Software "TCPUDPDbg" on server PC2, the 6944 will connect to the TCP Server automatically.



Step 2. Go to **Industrial Interface>Serial>Status>Serial Information>Index1**, to show the connection status.

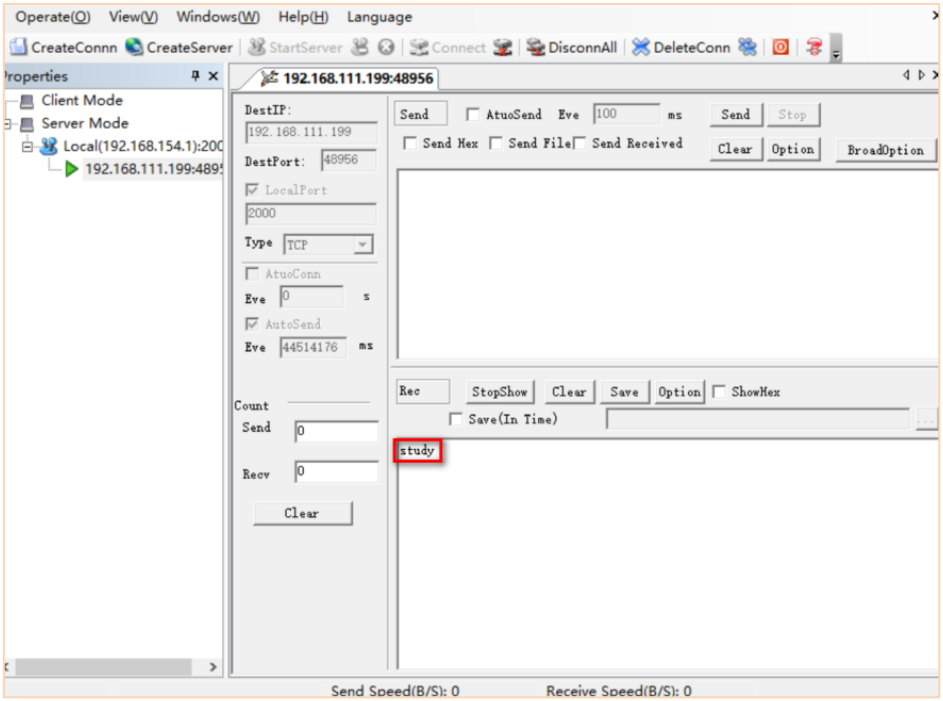
Testing

Step1. Run the serial software as an example using the word ”Hercules” on PC1, send the data, for example the word “study”.



Test Results

Step1. Ensure the TCP Server side can receive the data “study”

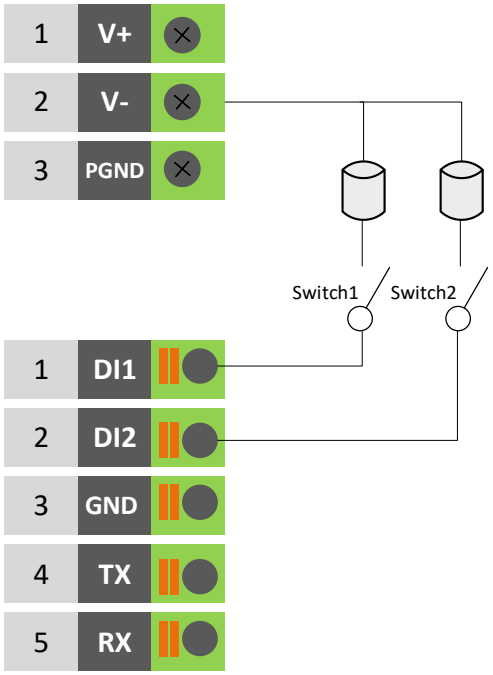


This page left blank intentionally

19. Digital I / O Ports

19.1. Digital Input Port

Typical Application Diagram

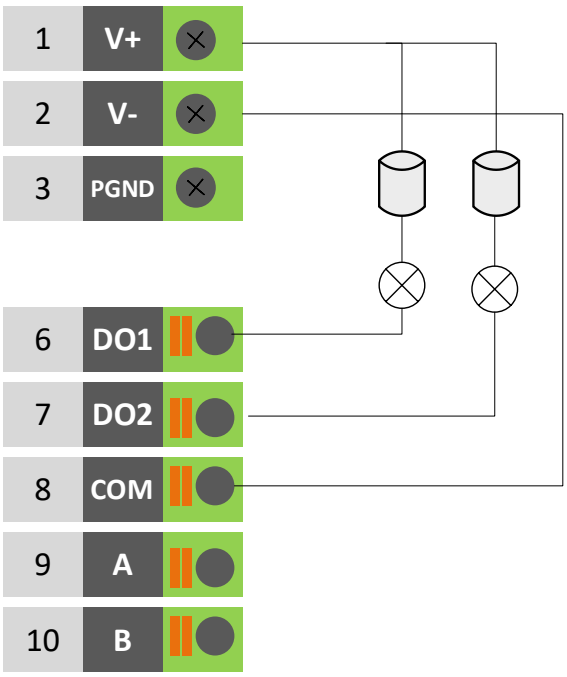


DI ELECTRICAL CHARACTERISTICS
1. Galvanic isolation;
2. Over-Voltage Protection: 36 VDC
3. Over-Current Protection：100mA per channel @ 25°C

Dry Contact Typical Application
Switch ON(Short to V-): DI Logic LOW
Switch OFF(Open): DI Logic HIGH

19.2. Digital Output

Typical Application Diagram



DO ELECTRICAL CHARACTERISTICS
1. Galvanic isolation;
2. Over-Voltage Protection: 36 VDC
3. Over-Current Protection：50mA per channel @ 25°C

Wet Contact Typical Application
DO Logic LOW: Switch ON(Led ON)
DO Logic HIGH: Switch OFF(Led OFF)

This page left blank intentionally

20 MODBUS

20.1 MODBUS Slave

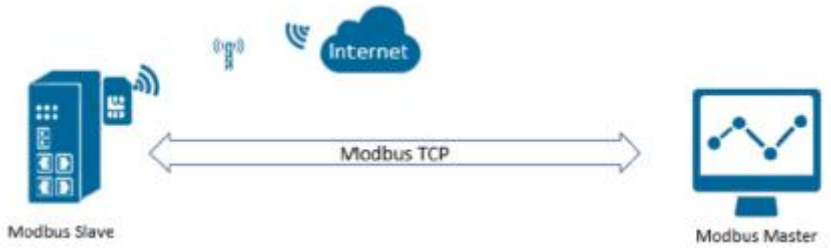
Overview

This document contains information regarding the configuration and use of the Modbus Slave Application within the 6944.

Software Compatibility

Release Date	Doc. Version	Firmware Version	Change Description
18.7.2019	V1.2.1	V1.1.0 (ADcaac4)	First release

Topology



The 6944 router runs as Modbus Slave with a static public IP address with a SIM card.

The Modbus Master connects to the 6944 router (Modbus Slave) via a TCP connection.

The Modbus Master reads the status of the Digital IO and controls the DO.

Note: For this Application the 6944 will run the software titled "Modbus Poll" to simulate a Modbus Master

Digital Input - Output Register Table

Index	Item	Function	Address (Decimal)	Qty	Values
1	Digital Input 1	02 Input Status	13800	1	00 – Low 01 - High
2	Digital Input 2	02 Input Status	13801	1	00 – Low 01 - High
3	Digital Output 1	01 Coil Status	13802	2	00 - Low 01 – High 02 - Pulse
4	Digital Output 2	01 Coil Status	13804	2	00 - Low 01 – High 02 - Pulse
5	DO1 Pulse Width	03 Holding Registers	13806	1	Default:500(ms) range:1~1000
6	DO2 Pulse Width	03 Holding Registers	13807	1	Default:500(ms) range:1~1000

Example Read Di Status

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity
Tx	01.90	00.00	00.06	01	02	35E8	00.01
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Byte Length**	**Value**
Rx	01.90	00.00	00.04	01	02	01	01

Example Read Do Status

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity
Tx	04.81	00.00	00.06	01	01	35EA	00.02
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Byte Length**	**Value**
Rx	04.81	00.00	00.04	01	01	01	02

Example: Control Do-Output Pulse

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity	Byte Length	Value
Tx	07.29	00.00	00.08	01	0F	35EA	00.02	01	02
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Address**	**Quantity**		
Rx	07.29	00.00	00.06	01	0F	35EA	00.02		

Cellular 6944 Series, Cellular / Ethernet / Wi-Fi / Serial / DI/O

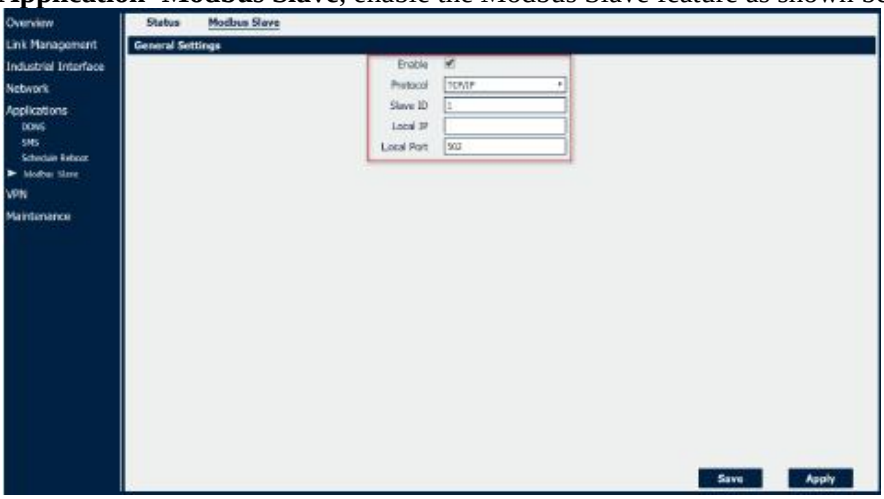
Example: Modify the width of the output pulse—500ms (The current output pulse to modify the width

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Value
Tx	07.2C	00.00	00.06	01	06	35EE	01 F4
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Address**	**Value**
Rx	07.2C	00.00	00.06	01	06	35EE	01 F4

Configuration

6944 Configuration

Step 1 Go to **Application>Modbus Slave**, enable the Modbus Slave feature as shown below:

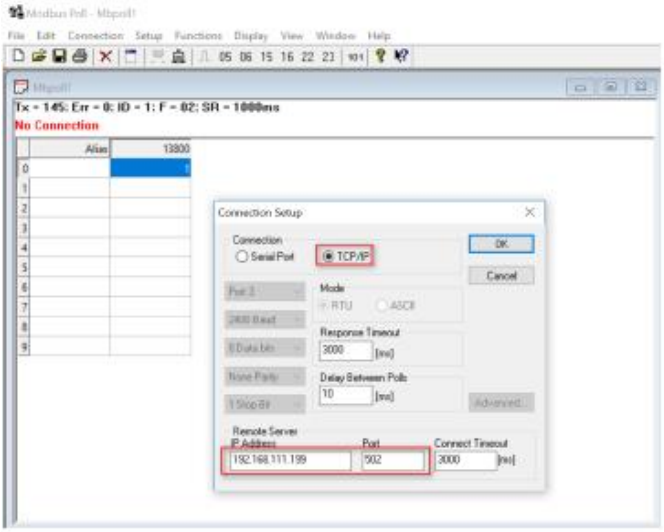


Step 2 Click Save > Apply

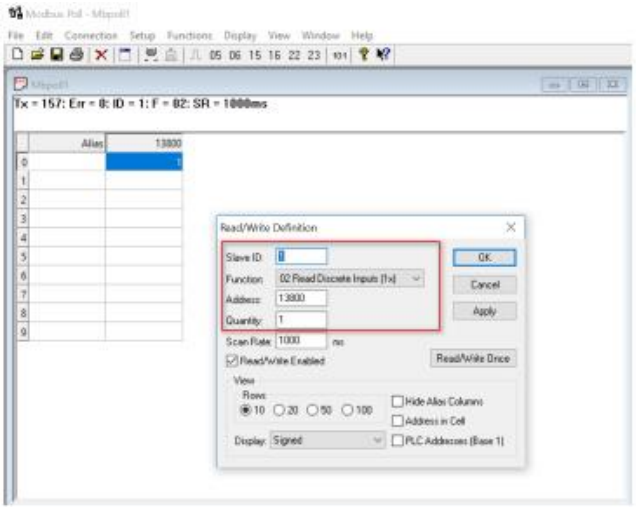
Testing

Read Digital Input Status

Run the software "MODBUS Poll" to connect to the 6944 (MODBUS Slave) as shown below (Path Connection > Connect)

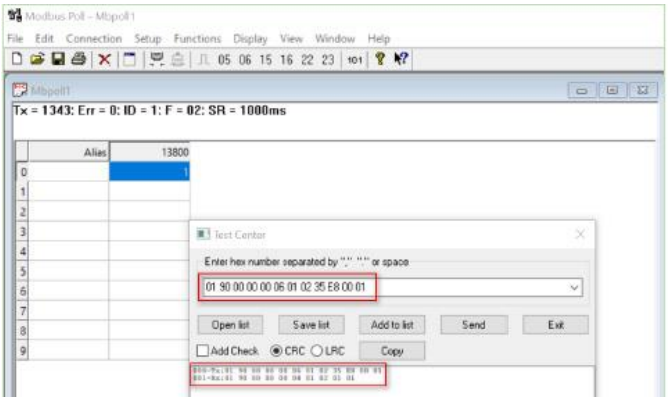


(Path: Setup> Read/ Write Definition)



Send the command to read the status of DI 1

(Path: Functions>Test Centre)



The reply Value is "00", DO1 status is "Low". Test successfully.

Read Digital Output Status

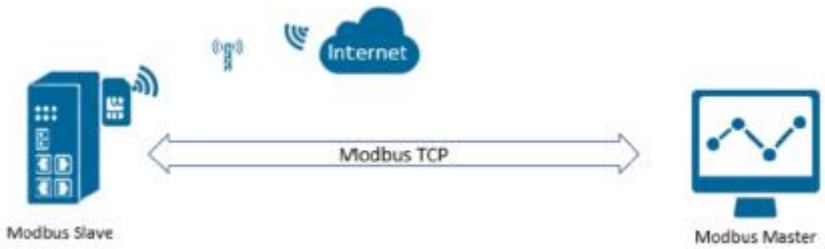
Set the Function Code to “01”, Address 13802 and the quantity is set to “2”.

Path: Setup>Read / Write Definition

Control Digital Output

Go to **Functions>15: WriteMultiple Coils**, to change the DO state from “0” to “1”.s

Topology



1. The 6944 router runs as a Modbus Slave with a static public IP address with a SIM card.
2. Modbus Master connects to the 6944 router (Modbus Slave) via a TCP connection.
3. The Modbus Master reads the status of Digital IO and control DO.

Note: For this Application the 6944 will run the software titled “Modbus Poll” to simulate a Modbus Master

Digital I/O Register Table

Index	Item	Function	Address (Decimal)	Qty	Values
1	Digital Input 1	02 Input Status	13800	1	00 – Low 01 - High
2	Digital Input 2	02 Input Status	13801	1	00 – Low 01 - High
3	Digital Output 1	01 Coil Status	13802	2	00 - Low 01 – High 02 - Pulse
4	Digital Output 2	01 Coil Status	13804	2	00 - Low 01 – High 02 - Pulse
5	DO1 Pulse Width	03 Holding Registers	13806	1	Default:500(ms) range:1~1000
6	DO2 Pulse Width	03 Holding Registers	13807	1	Default:500(ms) range:1~1000

Example Read Di Status

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity
Tx	01.90	00.00	00.06	01	02	35E8	00.01
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Byte Length**	**Value**
Rx	01.90	00.00	00.04	01	02	01	01

Example Read Do Status

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity
Tx	04.81	00.00	00.06	01	01	35EA	00.02
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Byte Length**	**Value**
Rx	04.81	00.00	00.04	01	01	01	02

Example: Control Do-Output Pulse

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Quantity	Byte Length	Value
Tx	07.29	00.00	00.08	01	0F	35EA	00.02	01	02
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Address**	**Quantity**		
Rx	07.29	00.00	00.06	01	0F	35EA	00.02		

Cellular 6944 Series, Cellular / Ethernet / Wi-Fi / Serial / DI/O

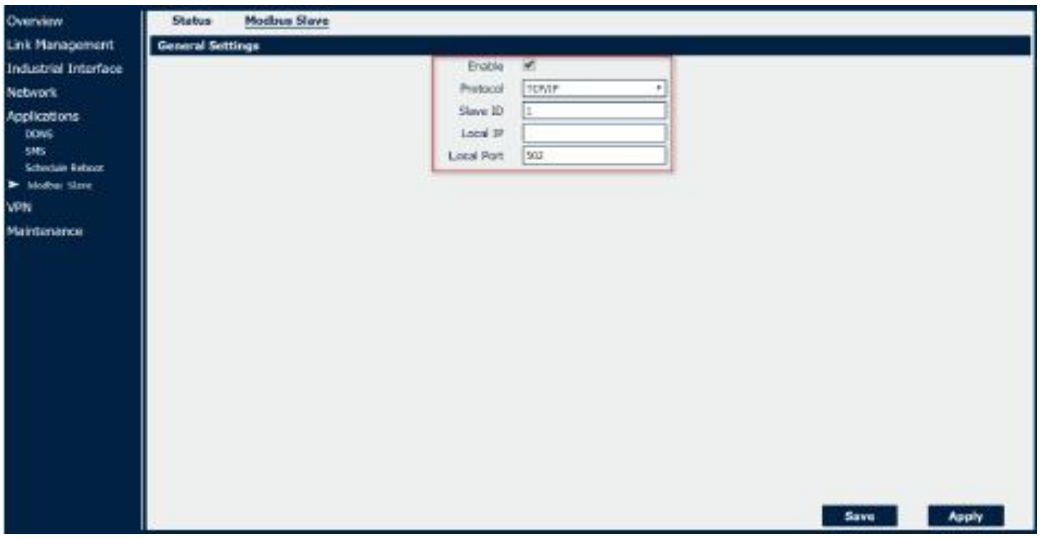
Example: Modify the width of the output pulse—500ms (The current output pulse to modify the width

Master	Transaction ID	Protocol ID	Data Length	Slave Id	Function Code	Address	Value
Tx	07.2C	00.00	00.06	01	06	35EE	01 F4
Slave	**Transaction ID**	**Protocol ID**	**Data Length**	**Slave Id**	**Function Code**	**Address**	**Value**
Rx	07.2C	00.00	00.06	01	06	35EE	01 F4

Configuration

6944 Configuration

Step 1. Go to **Application>Modbus Slave**, enable the Modbus Slave feature as shown below:

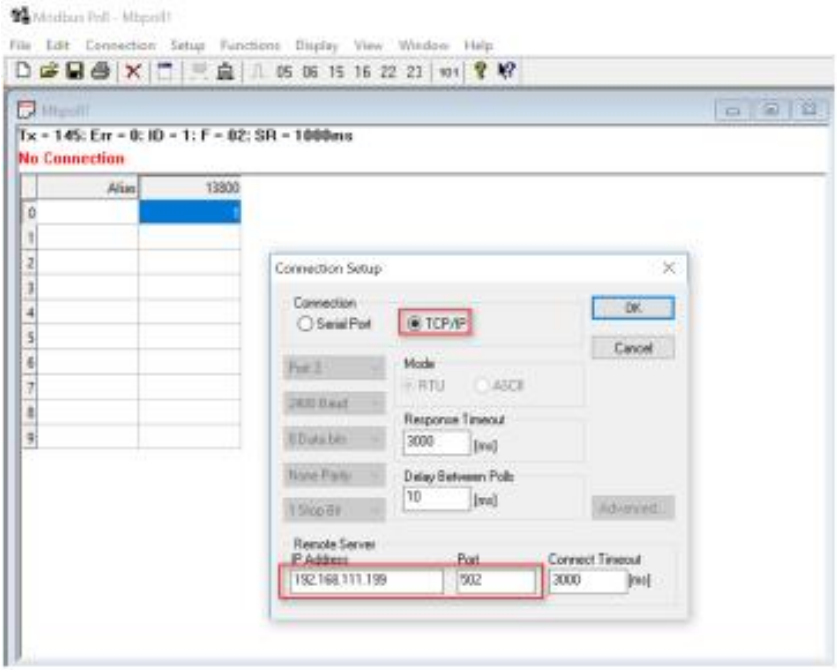


Step2. Click Save > Apply

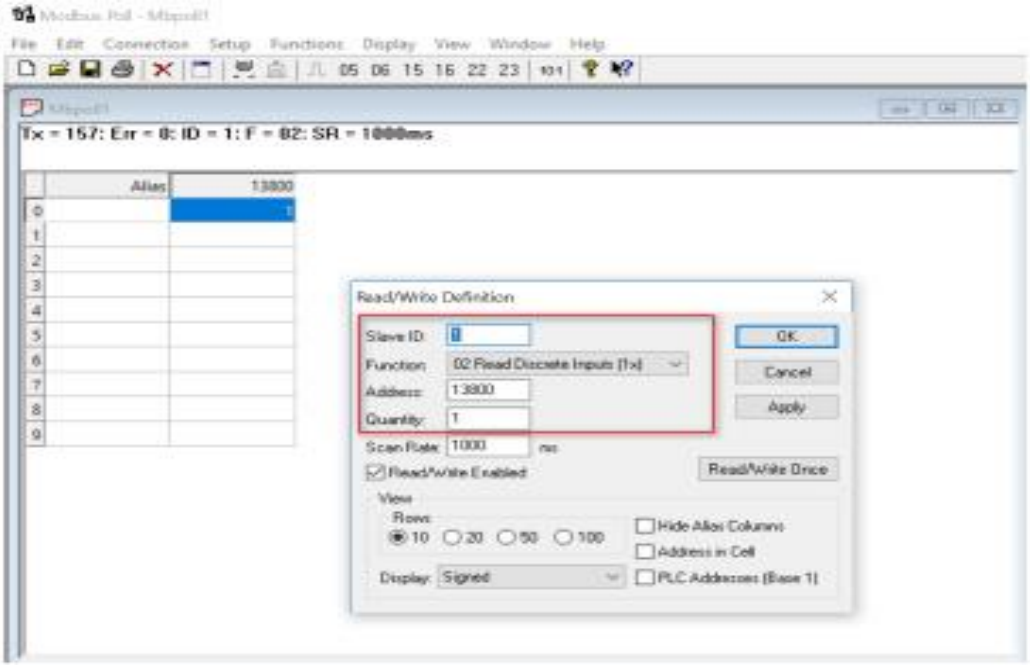
Testing

Read Digital Input Status

Step 1. Run the software "MODBUS Poll" to connect to the 6944 (MODBUS Slave) as shown below (Path Connection > Connect)

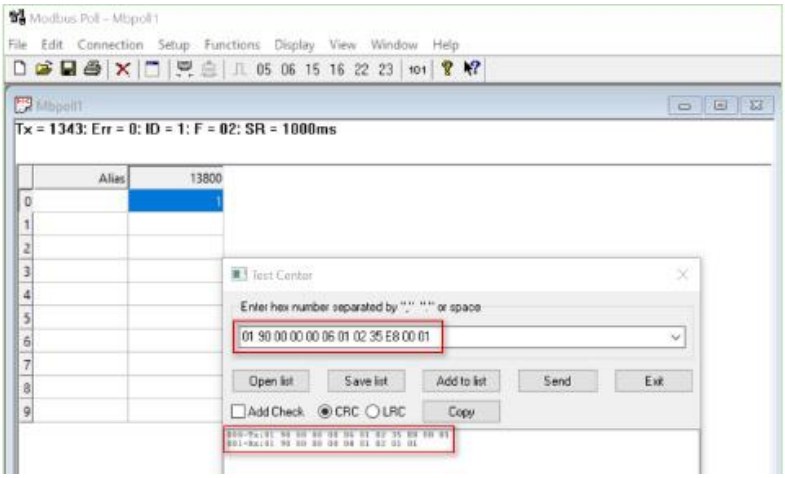


(Path: Setup> Read/ Write Definition)



Step 2. Send the command to read the status of DI 1

(Path: Functions>Test Centre)



The reply Value is “00”, DO1 status is “Low”. Then the test is successful.

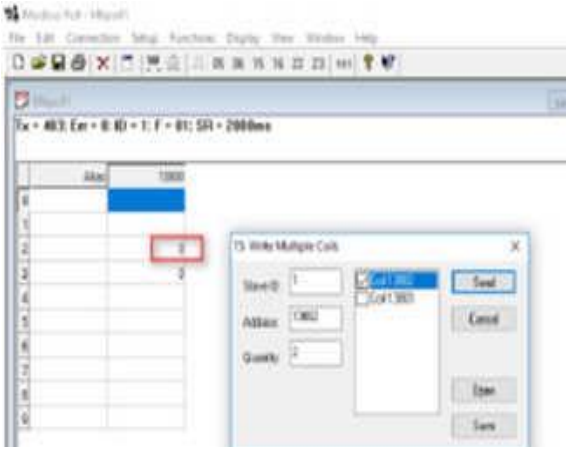
Read Digital Output Status

1. Set the Function Code to “01”, Address 13802 and the quantity is set to “2”.
Path: Setup>Read / Write Definition

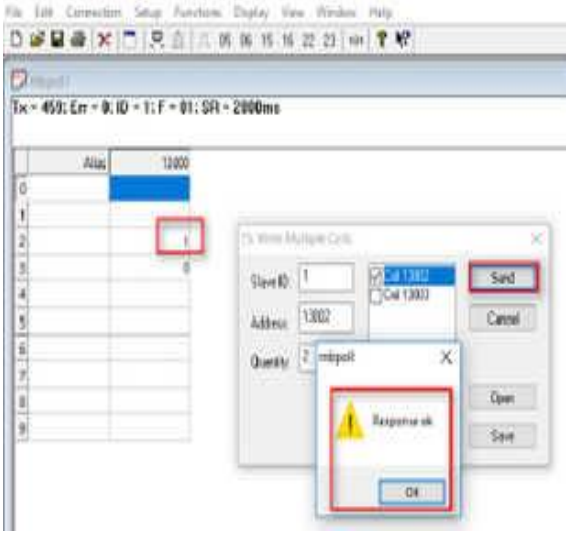
Control Digital Output

Go to **Functions>15: Write Multiple Coils**, to change the DO state from “0”to “1”.s

Test Successful



Test Successful



20.2 MODBUS Master

Introduction

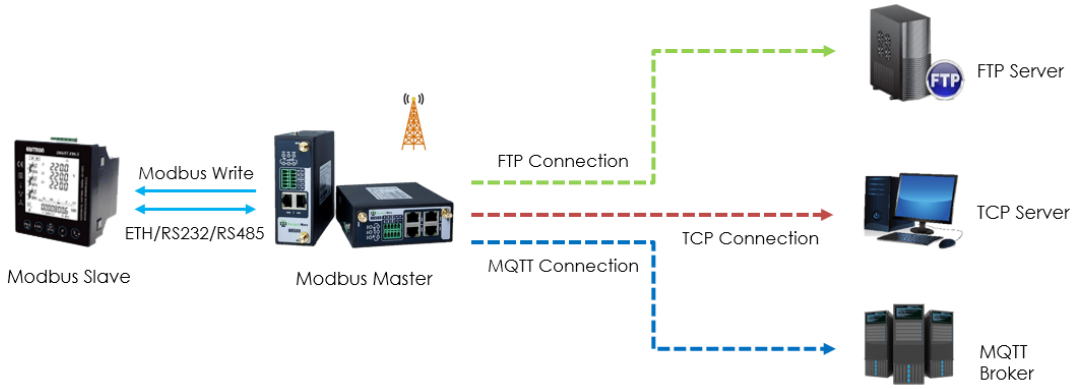
This section of the manual relates to the software for the MODBUS Master on the 6944 router. It requires the 6944 to be running the MODBUS Master software, which is version V.1.0.0 written in Feb 2020

Software Compatibility

Updates between document versions are cumulative. Therefore, the latest document will include all the contents from the previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2020/02/18	V1.0.0	V1.2.0(e958360)	MODBUS Master

Topology



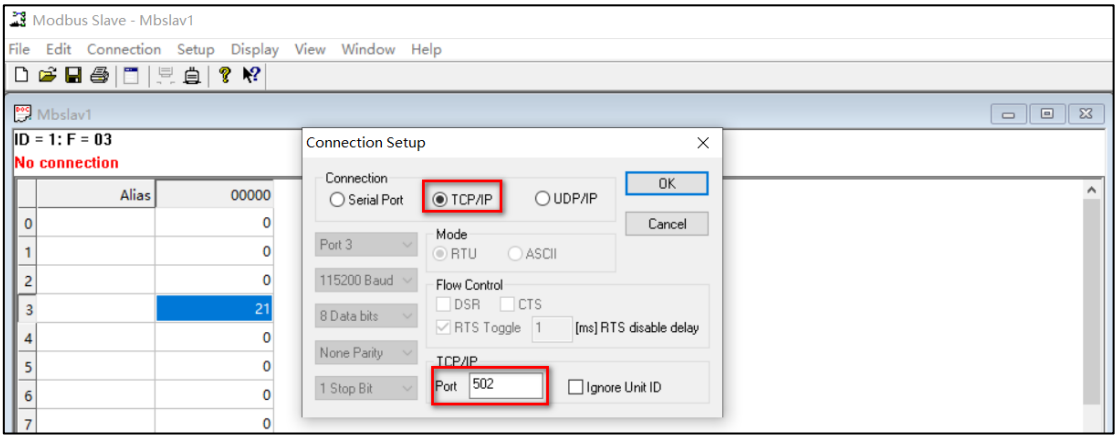
The 6944 Router runs as Modbus Master and can connect to MODBUS Slave via Ethernet, RS232 or RS485 interface.
The 6944 router polls the MODBUS data from the MODBUS slave and sends to the remote management center via TCP, FTP or MQTT protocol.
The 6944 as Modbus Master and writes to the register values or coil to Modbus Slave.

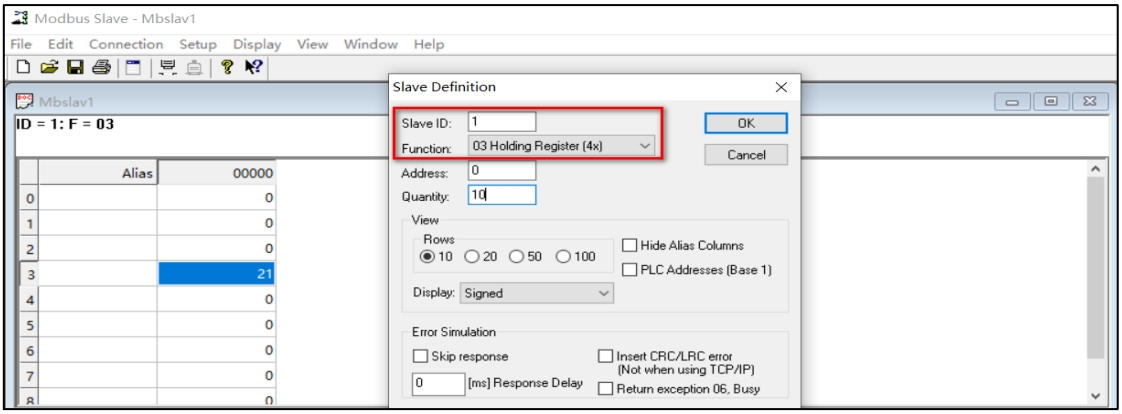
Note: For this Application Note, we will set the Connection Type as "TCP" as an example, which means that the 6944(Modbus Master) will connect to the Modbus Slave and read the value via the Ethernet port. This also works with the Serial Port (RS232/RS485).

Transport via TCP

Configuration of Modbus Slave

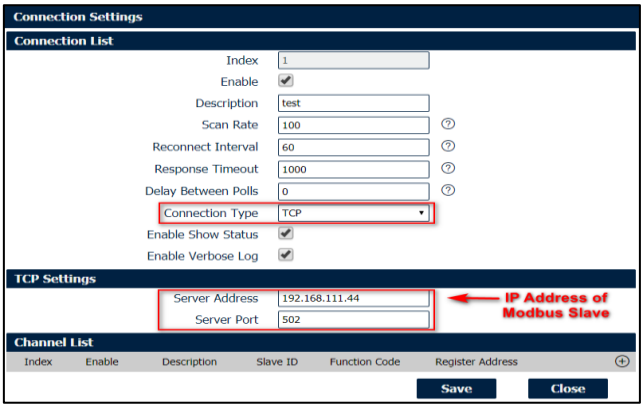
Here we use "Modbus Slave" software to simulate the end device (Modbus Slave device), and the **TCP Port: 502, Slave ID: 1, Function Code: 03-Holding-Register, as shown in the image below:**





Configuration of the Modbus Poll

Step 1 Go to **Application>Modbus Master>Modbus Poll**, add a "Connection List" and specify the "Connection Type" as **"TCP"**, specify the "**TCP Setting**" to connect to the Modbus Slave, like below:



Step 2 Click Save>Apply.

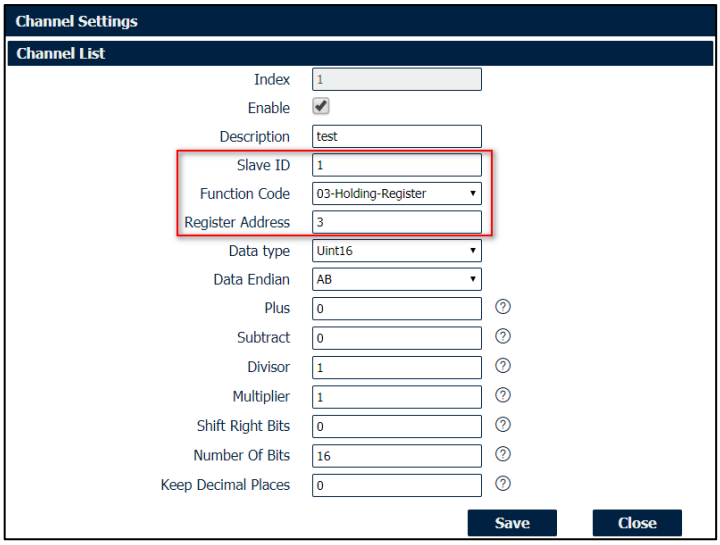
Step 3 Enable "Channel List", and specify the Slave ID as "1**"**.

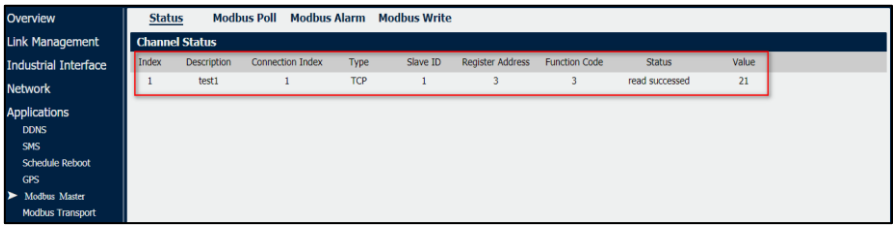
Step 4 Select Function Code as "03-**Holding -Register"**, Register Address to "3**"**, then it will poll the value from register address 3 of the Modbus Slave:

Step 5 Click Save>Save>Apply.

(Note: This is a secondary list, it needs to be double clicked to save)

Step 6 Go to **Application>Modbus Master>Status** to check the router has read the value from Modbus Slave successfully.



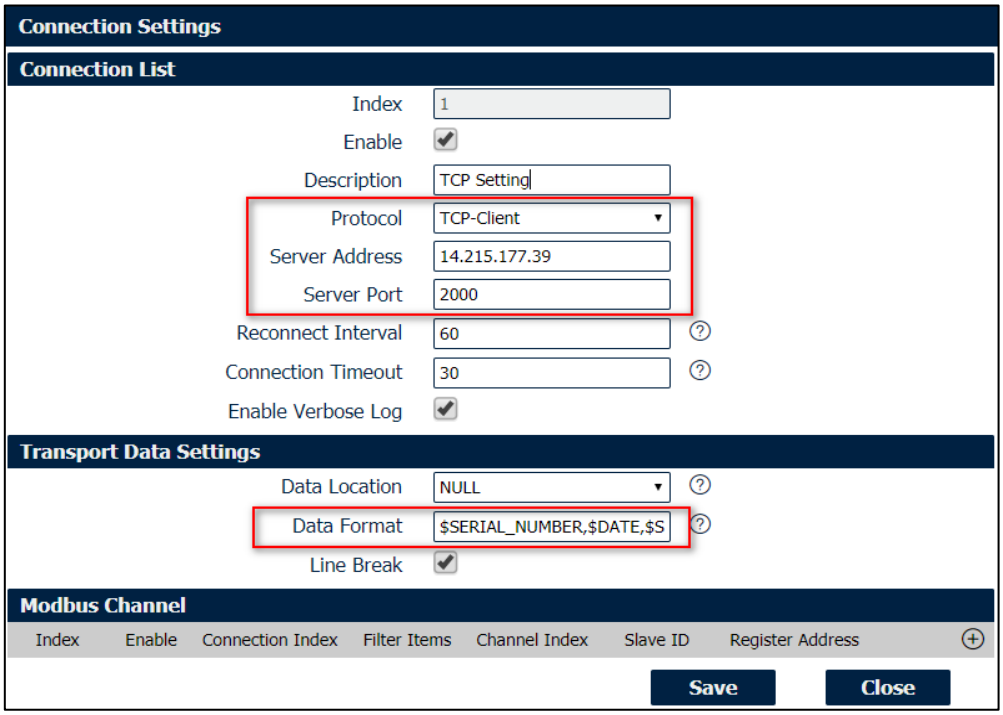


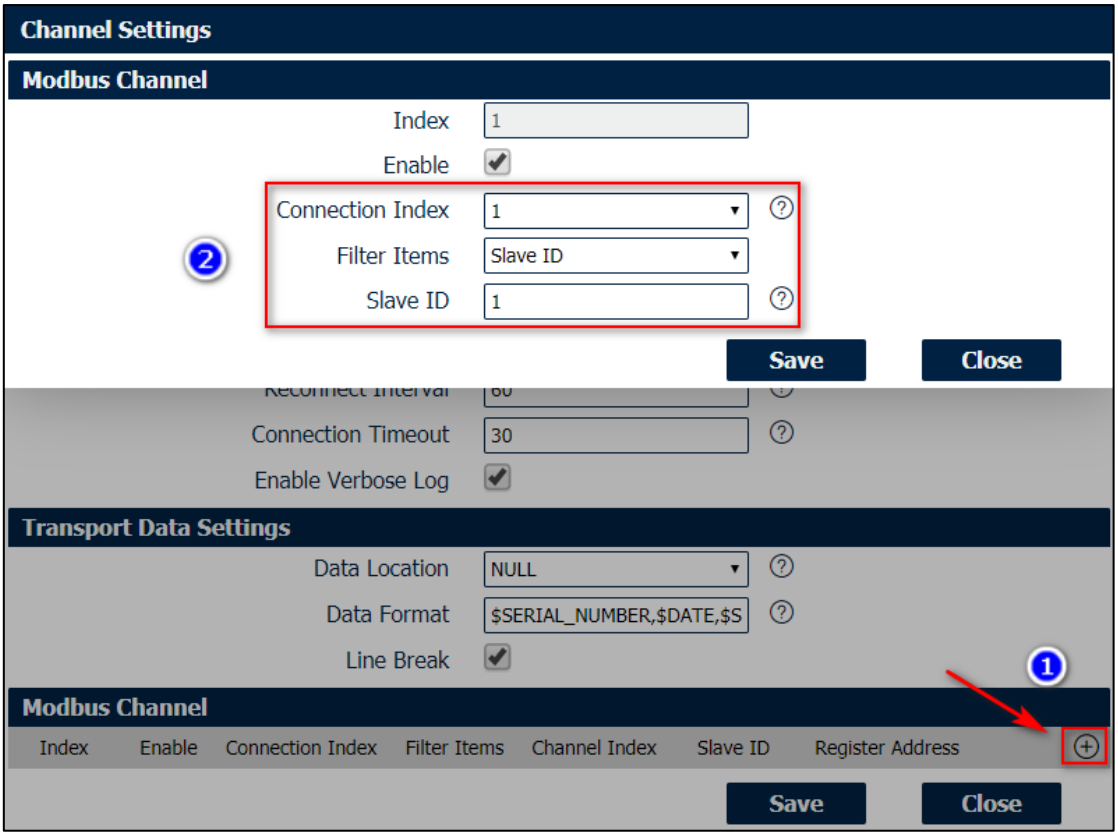
Configuring Modbus Transport

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable "Connection List", and specify the TCP server IP address and port to send the data to the remote TCP server.

Step 2 The Data Format can be defined accordingly or left as default.

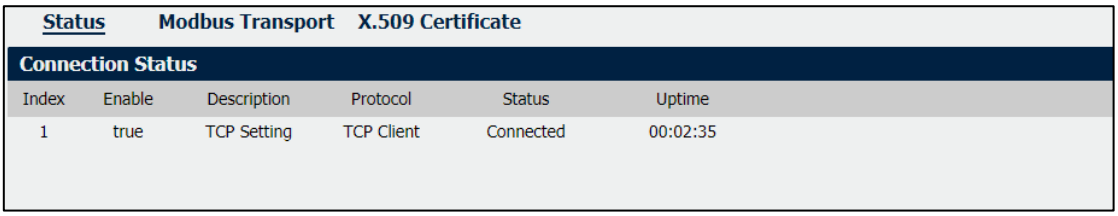
Step 3 Enable the "Modbus Channel", and the Modbus Master will select the value to send to the remote TCP server from Modbus Slave.



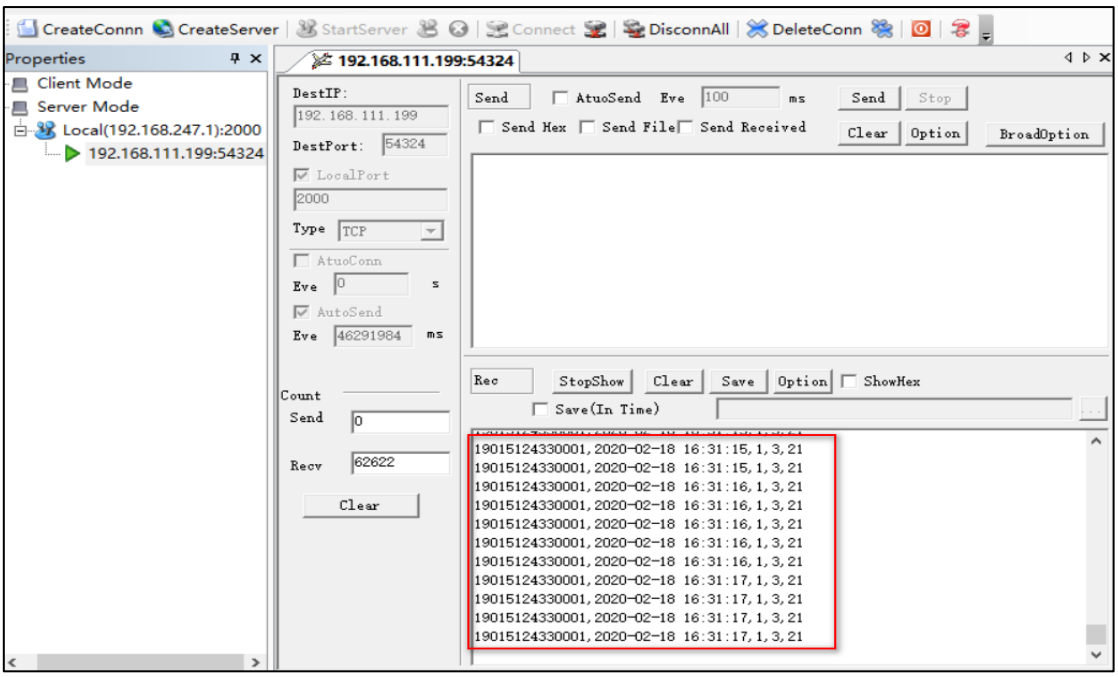


Step 4 Click Save>Save>Apply.

Step 5 Go to **Application>Modbus Transport>Status**, the 6944(Modbus Mater) has connected to the remote server successfully via the TCP protocol.



The remote TCP Server received the data successfully.

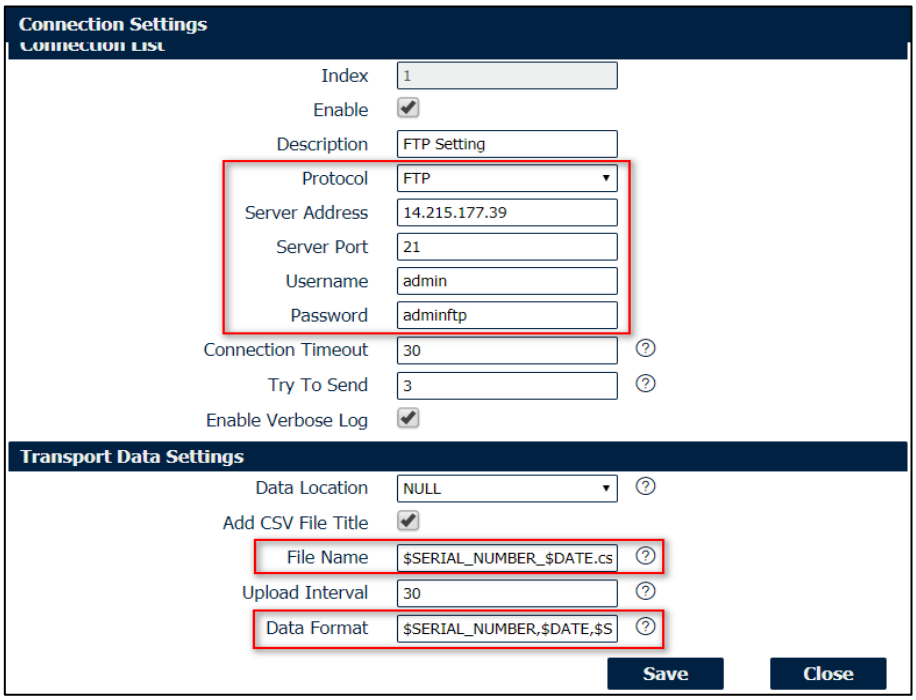


Transport via FTP

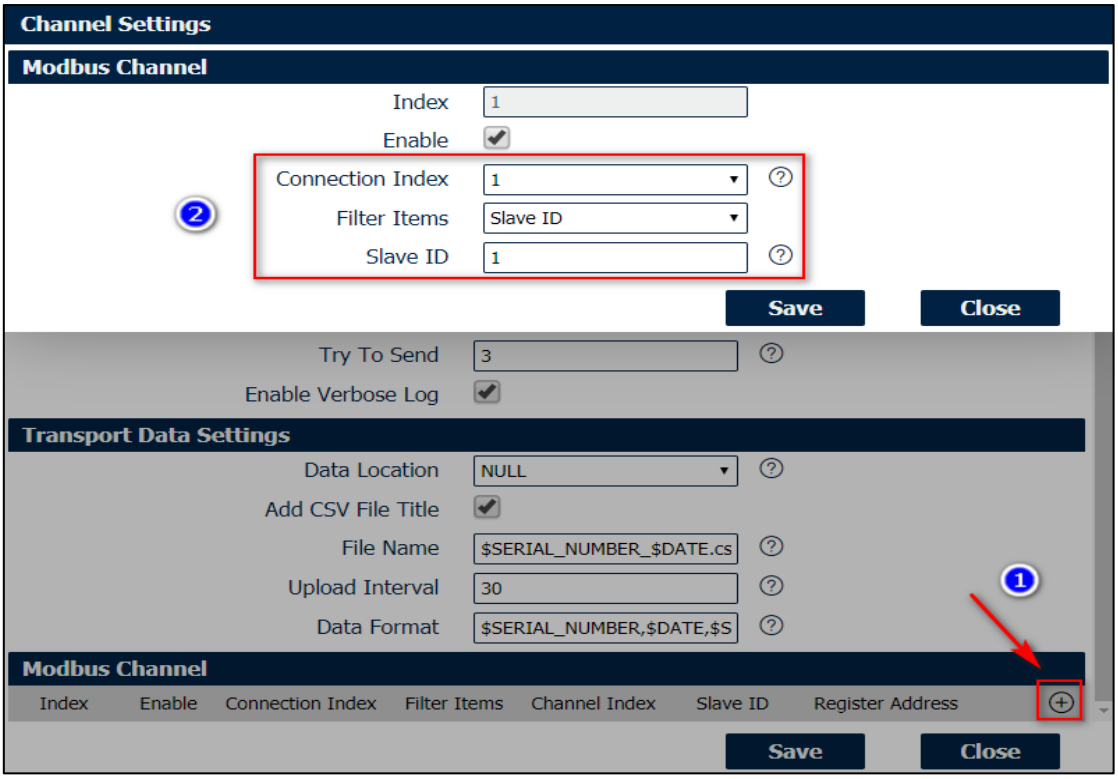
Please refer to the section on "Configuring the Modbus Slave" and Configuring the Modbus Poll" to finish the configuration.

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable "Connection List", and specify the FTP server IP address, port, username and password to send the data to remote FTP server.

Step 2 The File Name and Data Format could be defined accordingly or set it as default.

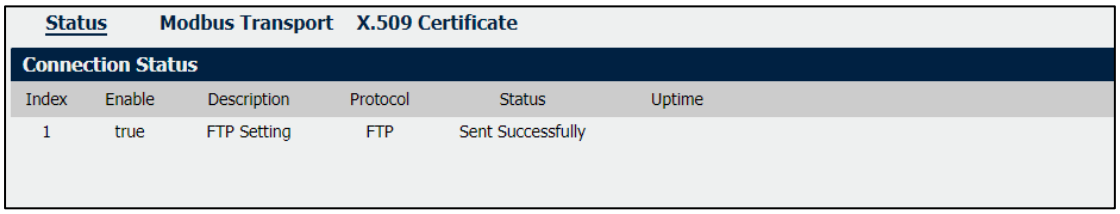


Step 3 Enable "Modbus Channel", and the Modbus Master will select the value to send to the remote FTP server from Modbus Slave.

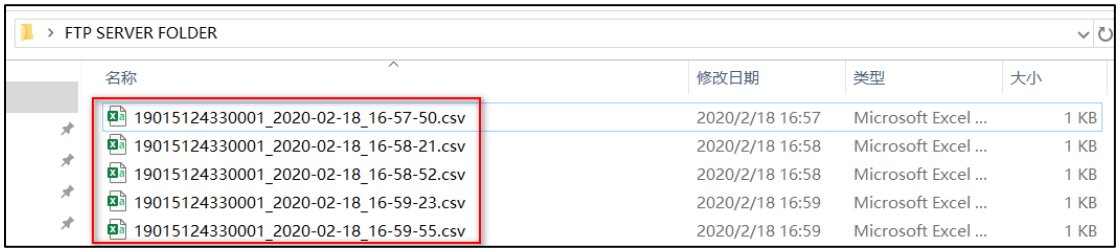


Step 4 Click Save>Save>Apply.

Step 5 Go to **Application>Modbus Transport>Status**, the 6944(Modbus Mater) has connected to the remote server successfully via the FTP protocol.



Remote FTP Server received the CSV file successfully.

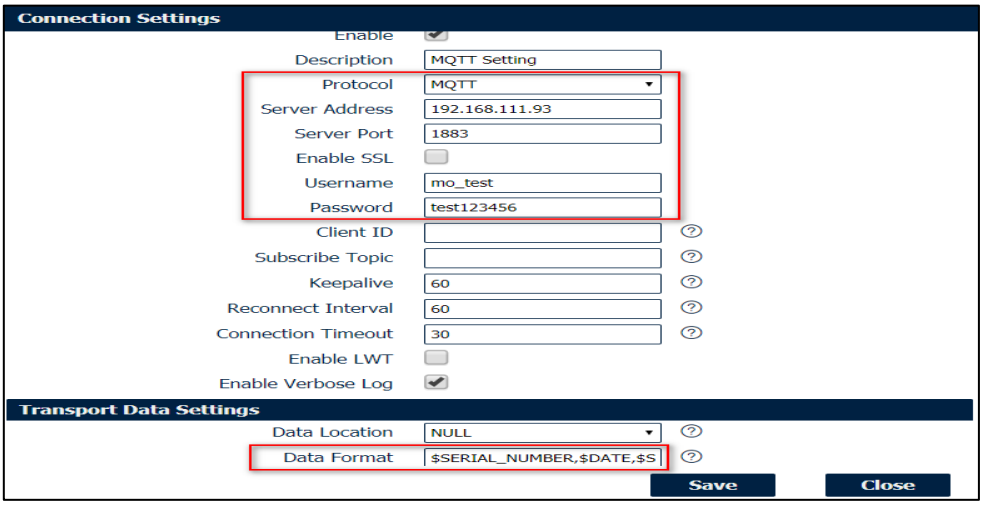


Transport via MQTT

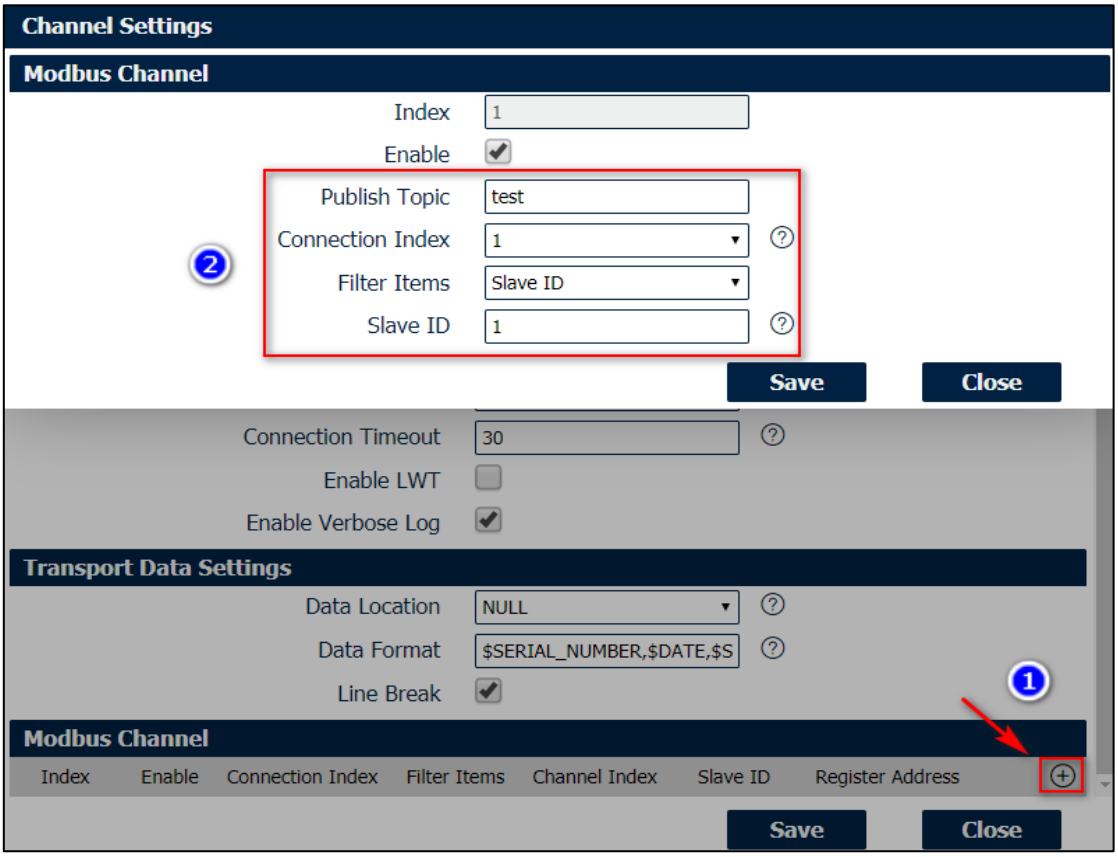
Please refer to the "Configuration for the Modbus Slave" and "Configuration of the Modbus Poll" to complete the configuration

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable "Connection List", and specify the MQTT Broker IP address, port, username and password to Publish the Topic with Modbus data to remote MQTT Broker.

Step 2 The Data Format can be defined or left as default.

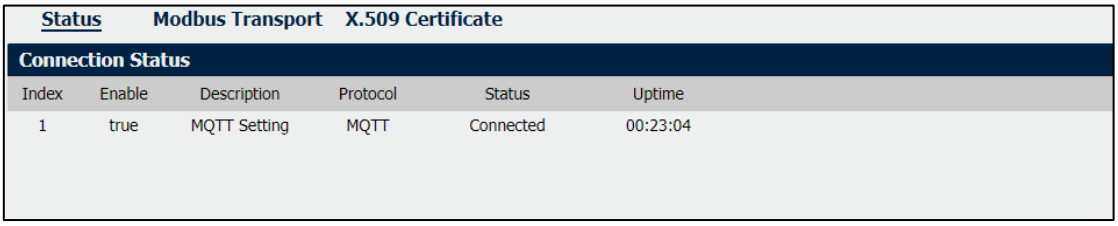


Step 3 Enable "Modbus Channel", define the "Topic" to publish to MQTT Broker with Modbus data.



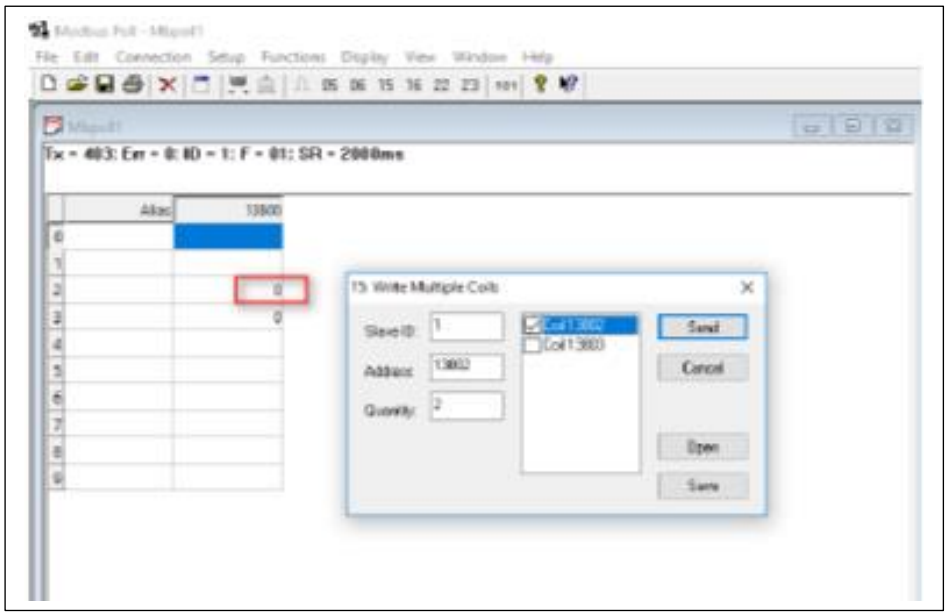
Step 4 Click Save>Save>Apply.

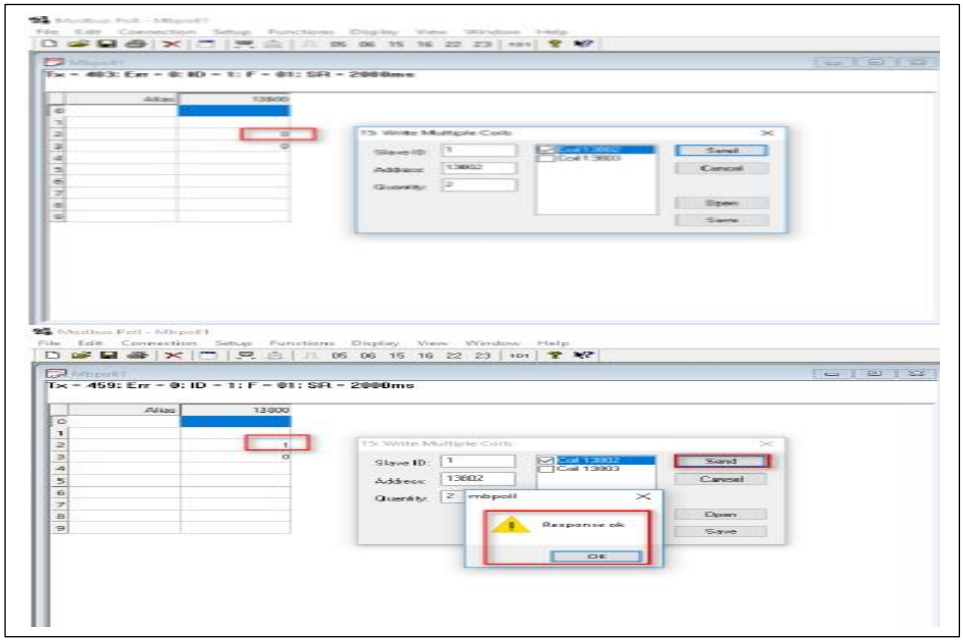
Step 5 Go to **Application>Modbus Transport>Status**, The 6944(Modbus Mater) had connected to the remote MQTT broker successfully.



Step 6 Run the MQTT Client (MQTT Subscriber), to subscribe the topic just published to MQTT broker with MODBUS data. Then you should be able to retrieve the MODBUS data successfully.

Step 7 Test Successful





Control Digital Output

Go to **Functions>15: Write Multiple Coils**, to change the DO state from “0”to “1”.s

Test Successful

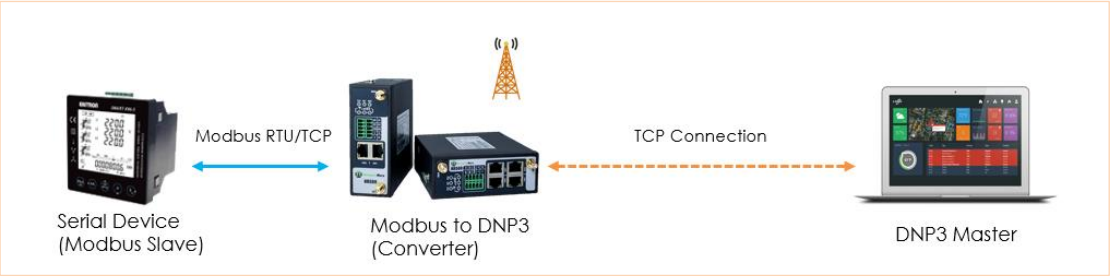
20.3 MODBUS to DNP3

This document contains information regarding the configuration and use of Modbus to DNP3 software on the 6944.

Software versions

Release Date	Doc. Version	Firmware Version	Additional software	Change Description
2020/07/17	V1.0.0	V1.1.4(0c0c9fa)	Please contact Case	First released

Testing Topology

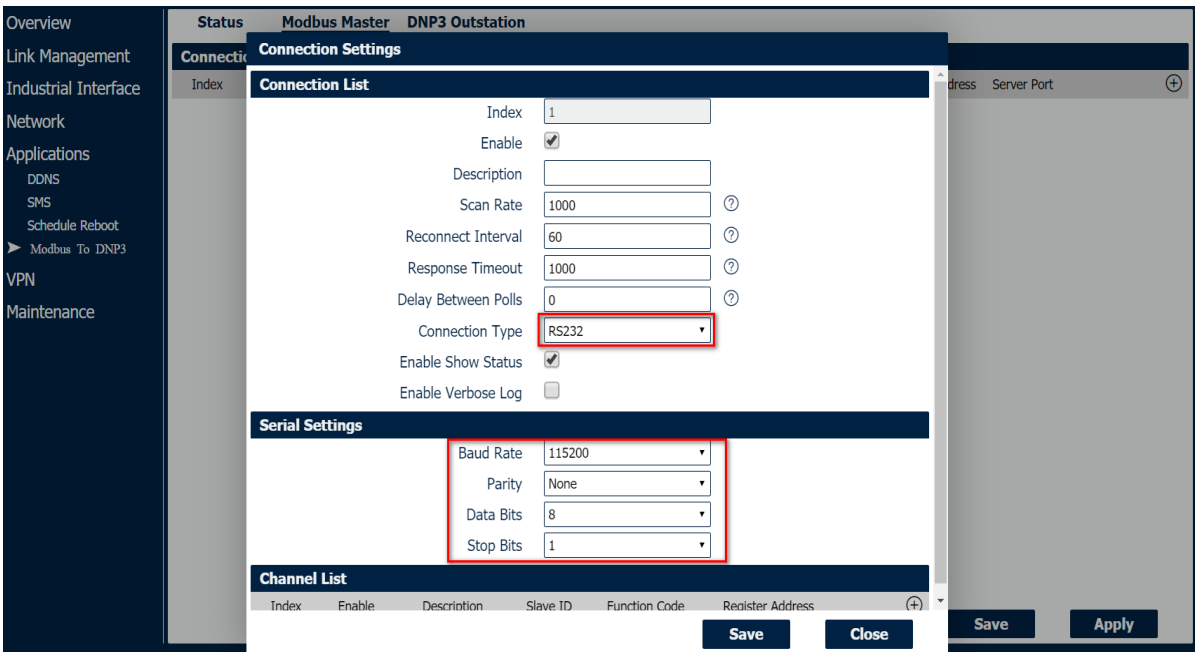


- A 6944 Router runs as a Modbus to DNP3 converter, it acts as a Modbus Master and DNP3 Outstation.
- A serial device supports Modbus protocol and acts as a Modbus Slave. It connects to the 6944 router via its serial port or Ethernet port.
- The 6944 router polls the Modbus data from the end device (Modbus Slave), then sends the data to the remote DNP3 Master.

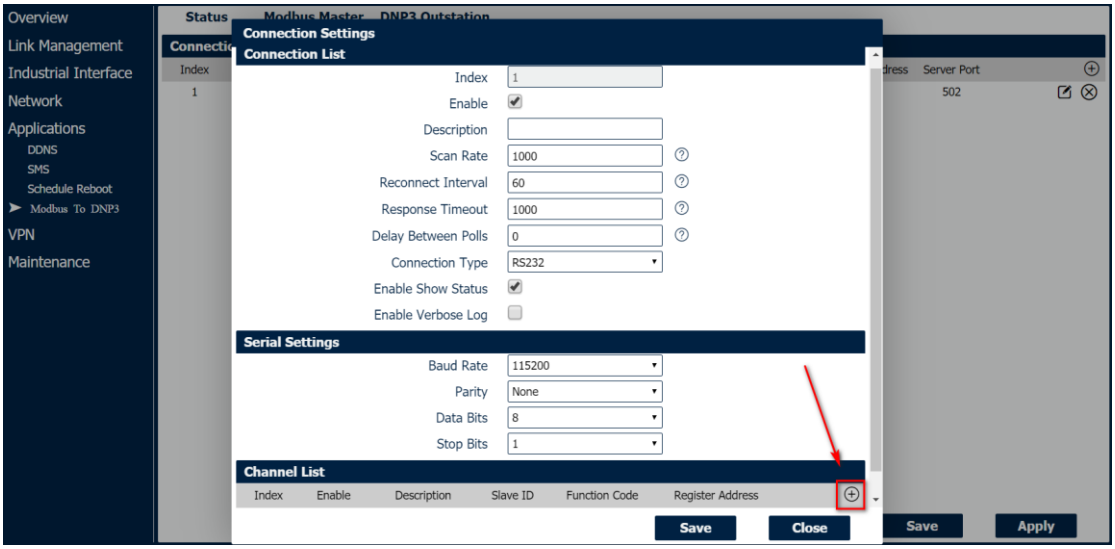
Configuration

Configuring the 6944

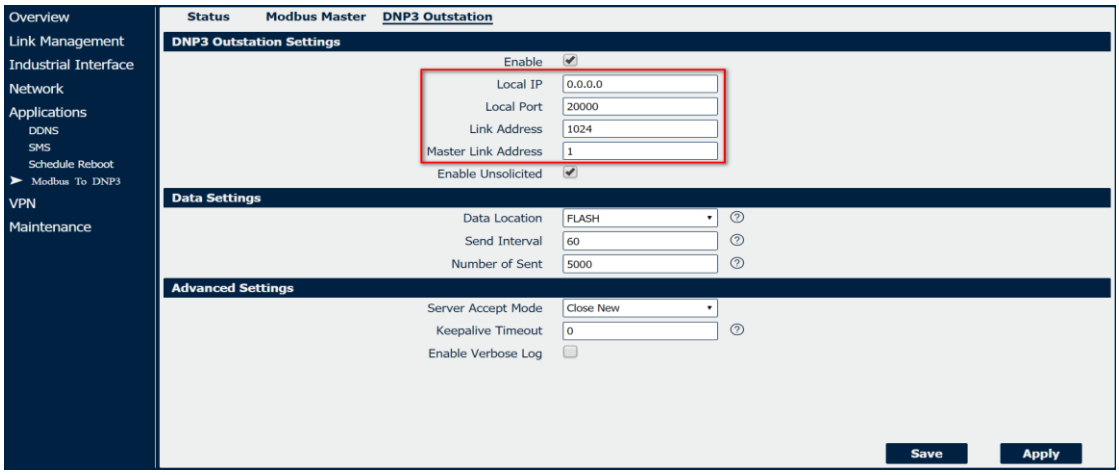
Step 1 Go to **Applications>Modbus To DNP3>Modbus Master**, specify the serial settings to make the router connect to the Modbus Slave via RS232 interface:



Step 2 Go to **Applications>Modbus To DNP3>Modbus Master>Channel List**, specify the Modbus Master settings and the DNP3 data type:



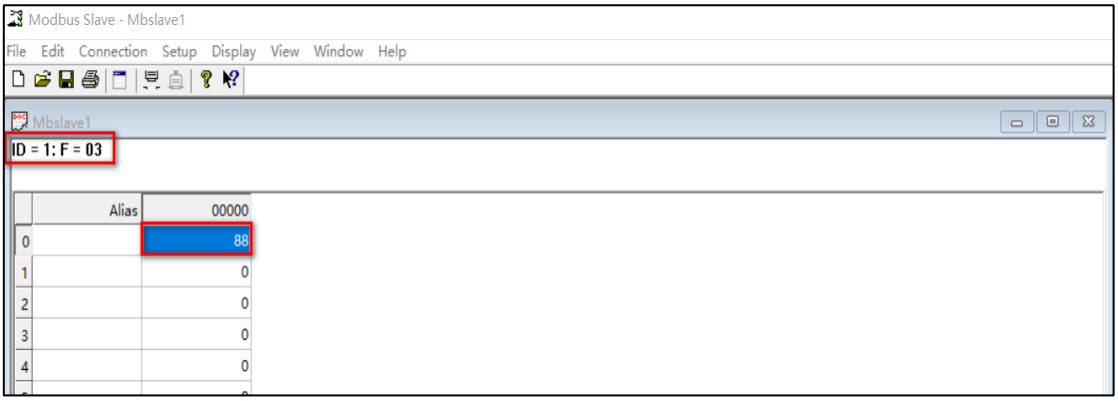
Step 3 Go to **Applications>Modbus To DNP3>DNP3 Outstation,** specify the DNP3 outstation settings as shown below:



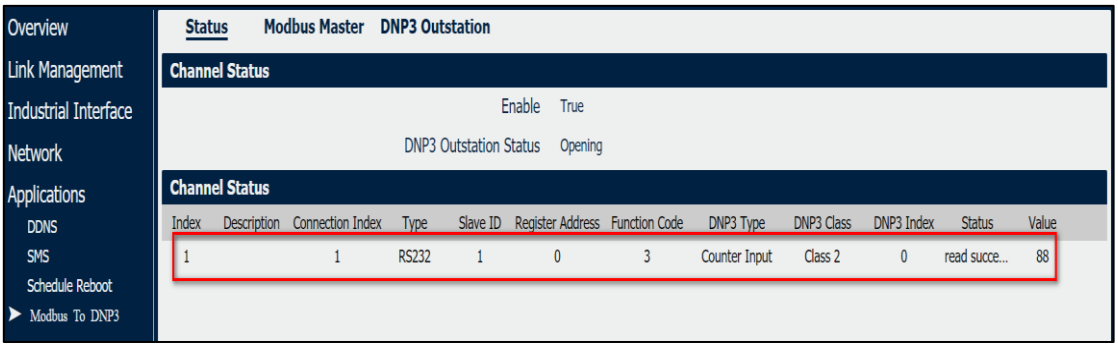
Step 4 Click Save>Apply.

Configuration of MODBUS Slave

Step 1 Set Slave ID as “1”; Function Code as “03”, and the value “88” on Register “0”:



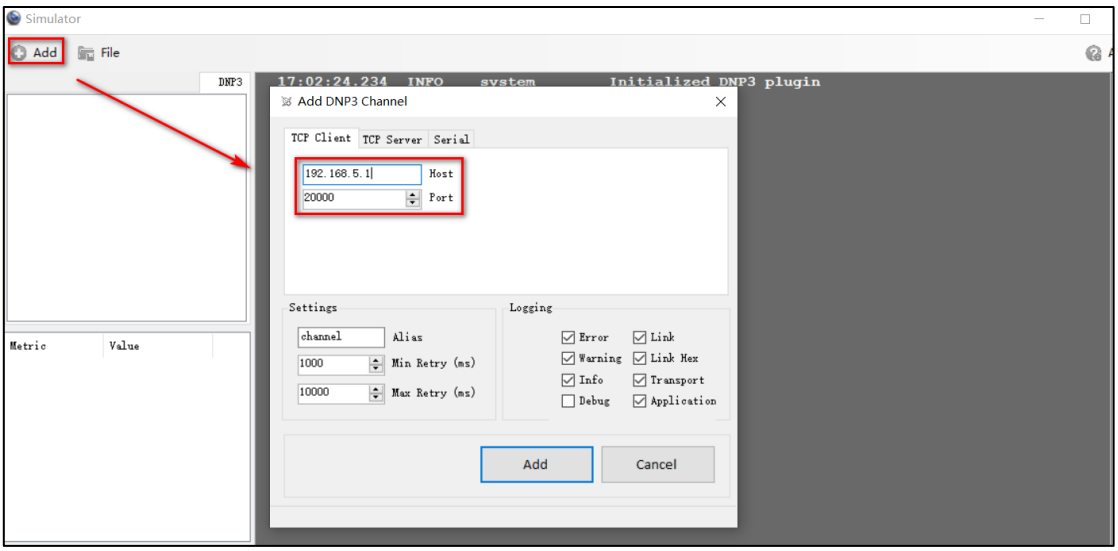
Step 2 Check that the 6944 has polled and retrieved data from the Modbus Slave successfully:



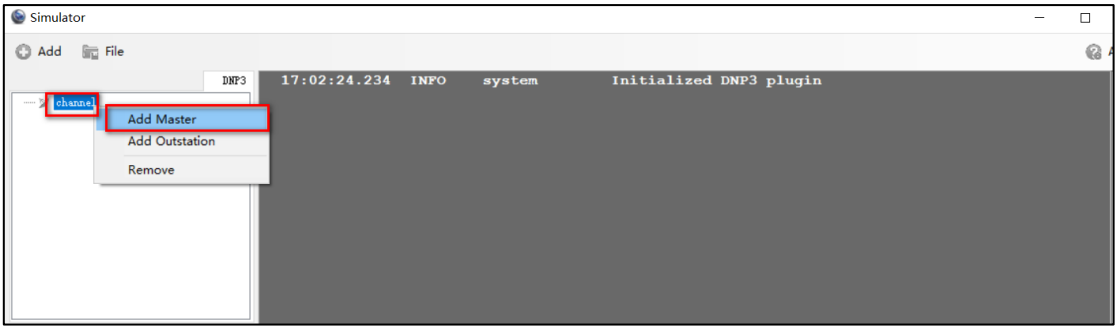
Testing

Use the DNP3 Simulator “OpenDNP3” to do the testing.

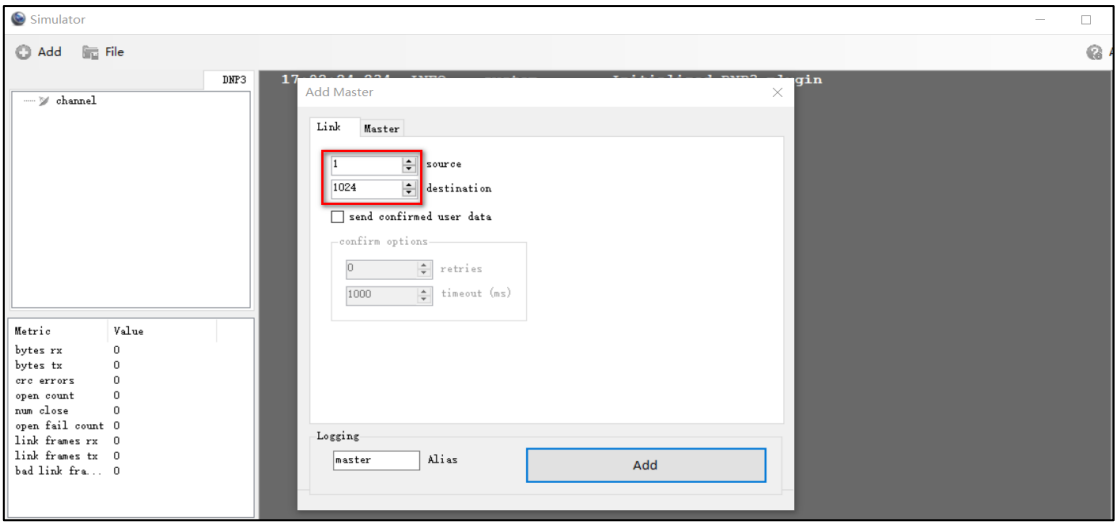
Step 1 Run DNP3 simulator and enter the IP Address and Port to make it connect to the 6944 (DNP3 Outstation):



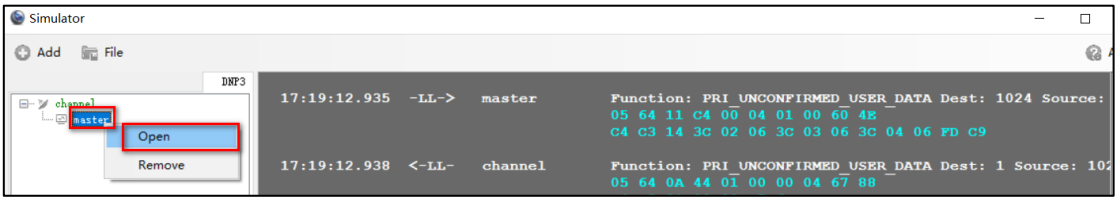
Step 2 Right Click “channel”, and Add Master:



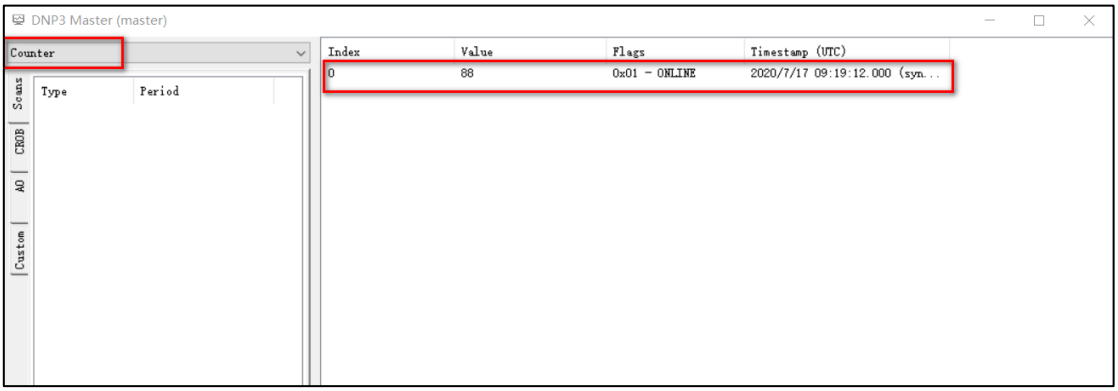
Step 3 Specify the address on the DNP3 Master, to make it match the settings on the 6944 (DNP3 Outstation):



Step 4 Right Click "Master" and open it:



Step 5 Select the data type as "Counter", then you can see the data has been sent to the DNP3 Master from the 6944(DNP3 Outstation) successfully:



Step 6 Test successful.

20.4 AN053 IEC 101 to IEC 104

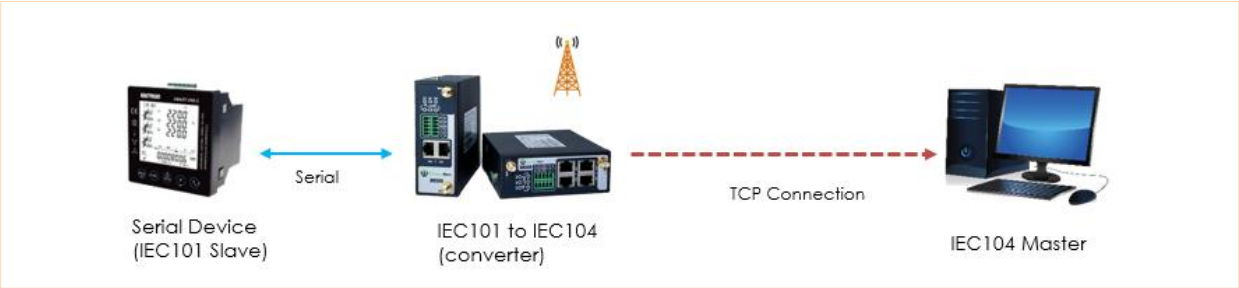
Overview.

This document contains information regarding the configuration and use of IEC101 to IEC104.

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
2020/07/17	V1.0.0	V1.1.4(0c0c9fa)	(e9b6efe)	First released

Topology

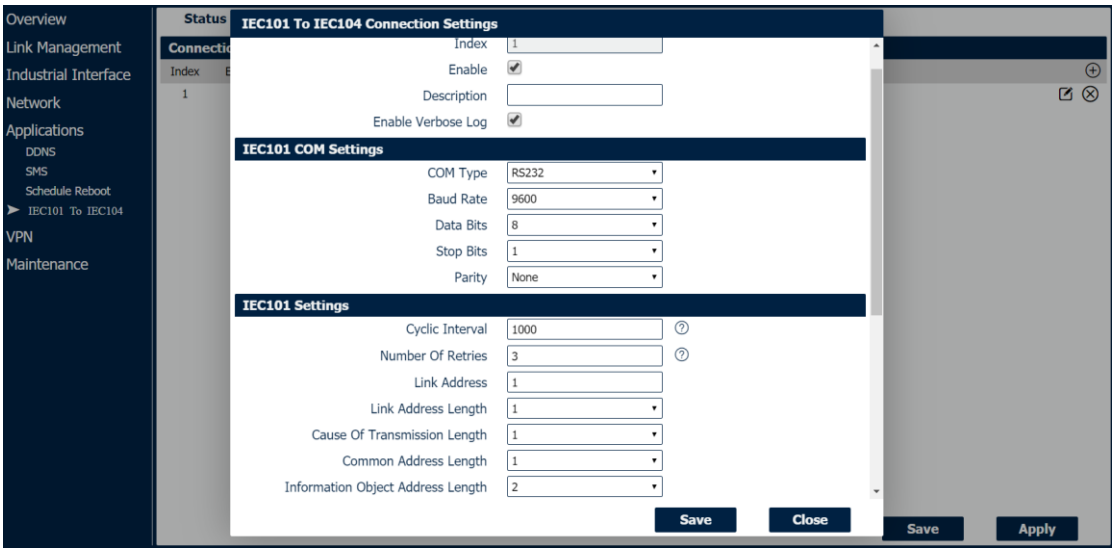


- The 6944 Router runs as an IEC101 to IEC104 converter.
- A serial device supports the IEC101 protocol and acts as slave connected to the 6944 router via a serial port.
- The IEC104 master connects to the 6944 router via TCP and requests data from the slave. After that, the slave will send the data to the master as requested.

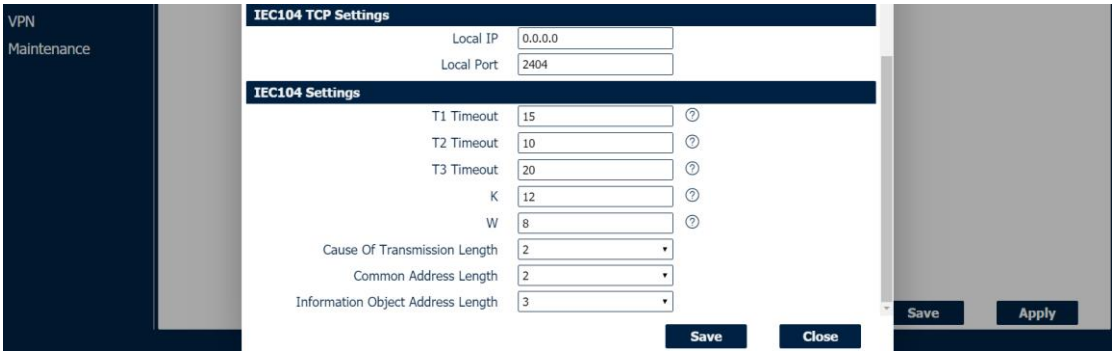
Configuration

Configuring the 6944

Step 1 Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC101 configuration, like below:



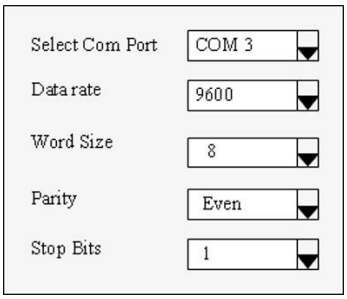
Step 2 Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC104 configuration, as shown below:



Step 3 Click Save>Apply.

Configuring an IEC101 Simulator

Step 1 Specify the serial settings on the IEC101 simulator, and make it the same as the 6944 router serial settings:



Step 2 Specify the simulator works as the Slave Station:

Step 3 Specify the IEC101 Serial Port settings on the IEC101 simulator, to make it the same as the 6944 as shown above.

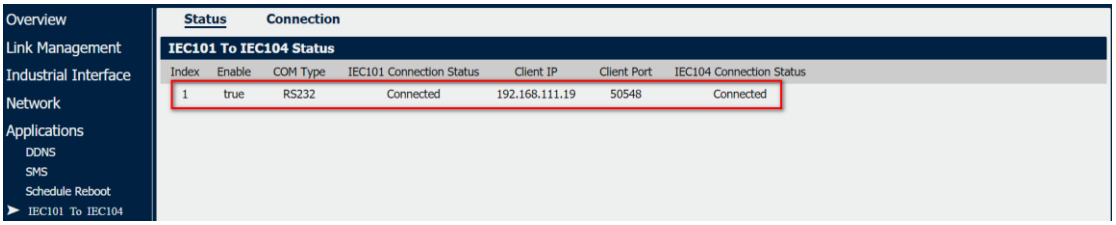
Step 4 Save and start to connect.

Configuring an IEC104 Simulator

Step 1 Enable the IEC104 simulator and configure it as a Master Station:

Step 2 Specify the settings on the IEC104 simulator, to make all the settings the same as the 6944 IEC104 setting, then connect to the 6944 via a TCP connection:

Step 3 Save and start to connect IEC104 Master to IEC101 Slave:



Step 4 Connected successfully

Testing

IEC104 Master requests data from the IEC101 Slave

IEC104 Master receives data from the IEC101 Slave

This page left blank intentionally

21. AT Commands

21.1. AT Over IP

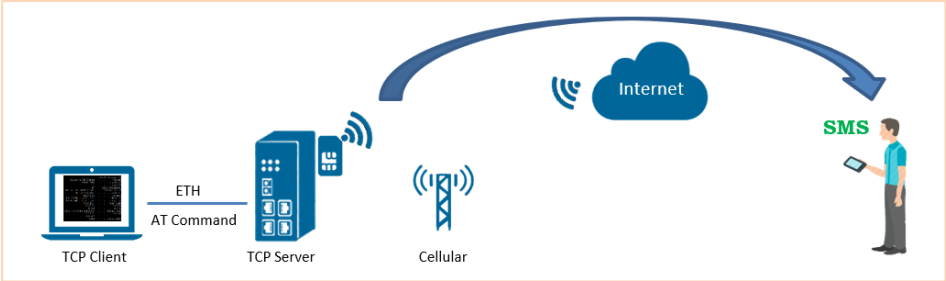
Overview

This document contains information regarding configuring the 6944 to run AT Over IP

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
4.7.2019	V1.1	V1.1.4 (0c0c09fa)	AT over IP 1.0.1 (42ccf3e)	First release

Topology



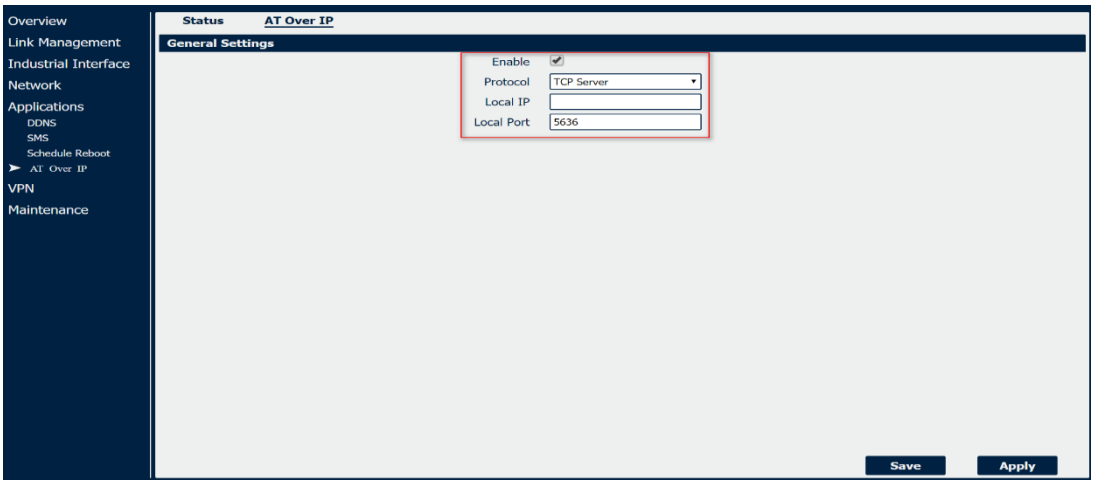
- The 6944 runs as a TCP Server and connects to the Internet via its SIM card.
- The PC runs as a TCP Client and connects to the 6944 via an Ethernet cable.
- The PC sends an AT Command to control the module on the 6944 to take some action.

Note: This application note will show how to use the AT Command via a TCP connection to control the module to send PDU mode SMS message

Configuration

6944 Configuration

Step 1 Go to **Application>AT Over IP**, enable AT Over IP feature like below:



Step 2 Click Save>Apply.

Testing

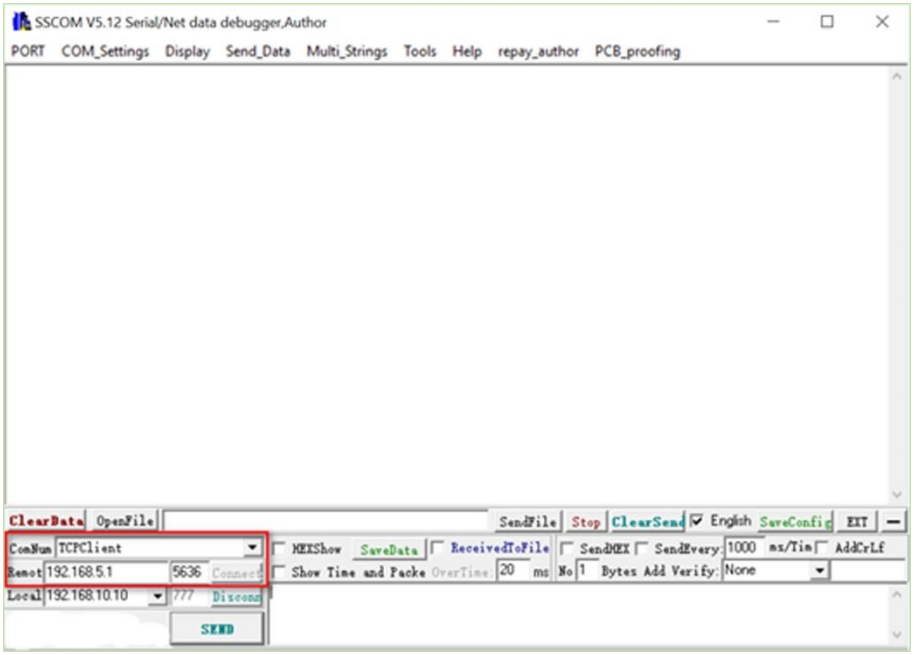
Send the message "TEST" to the mobile phone under PDU mode as an example message.

yy AT Commands and Content that needs to be sent one by one to the router.

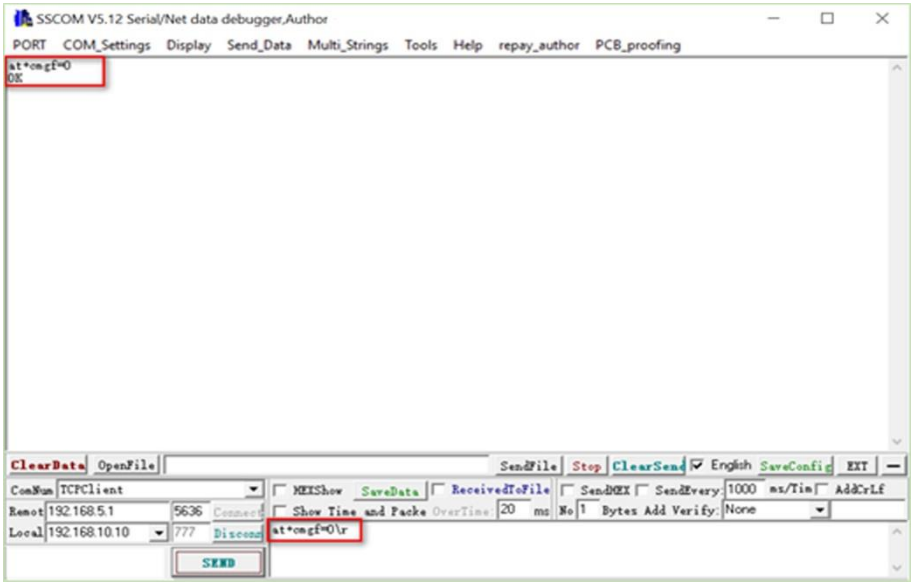
a. at+cmgf=0\r
b. at+cmgs=17\r
c. 0001000BA15119852081F0000004D4E2940A
d. 1a

Note: "\r" selects the keyboard "Enter"; Option "c" for the content to be sent under PDU mode; Option "d" is the end code to be sent with HEX.

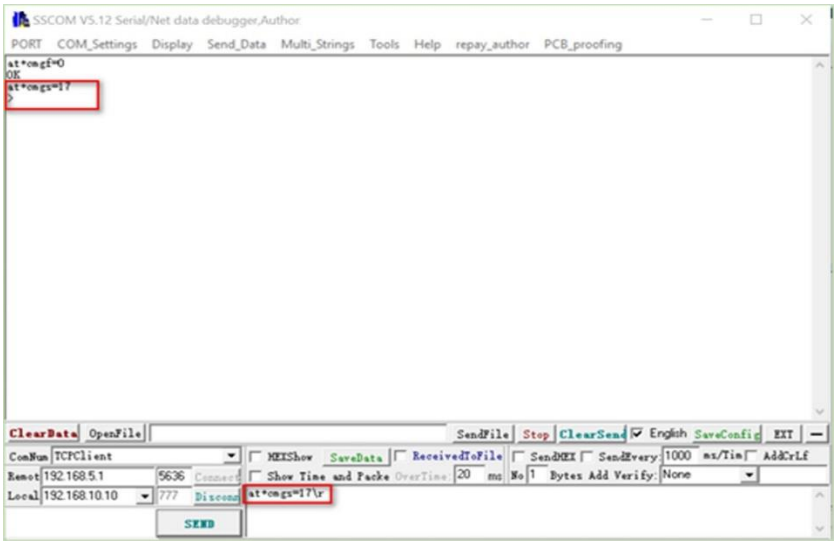
Step 1 Run SSCOM software as a TCP client and connect the 6944 router (TCP Server), as shown below.



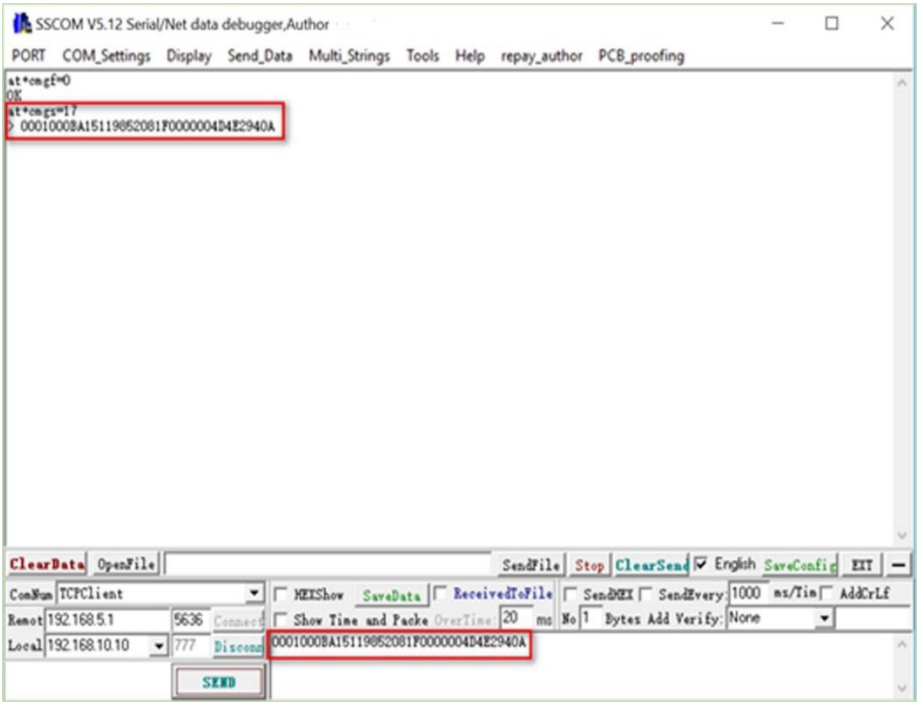
Step 2 Send the AT command "at+cmgf=0\r" to make sure it's under PDU mode.



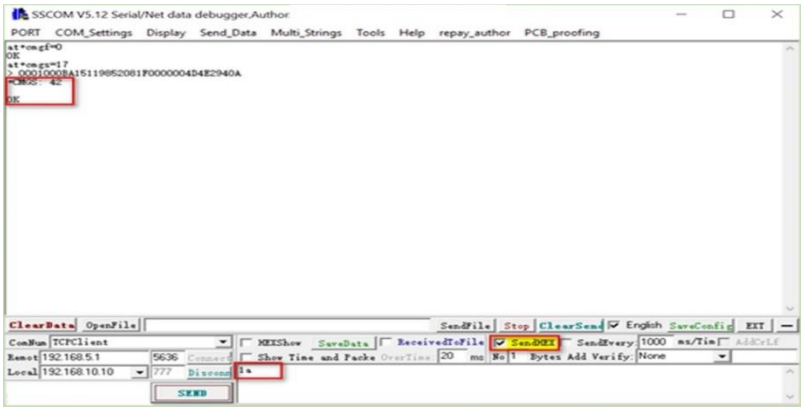
Step 3 Send the AT command "at+cmgs=17\r" to start to sending the content.



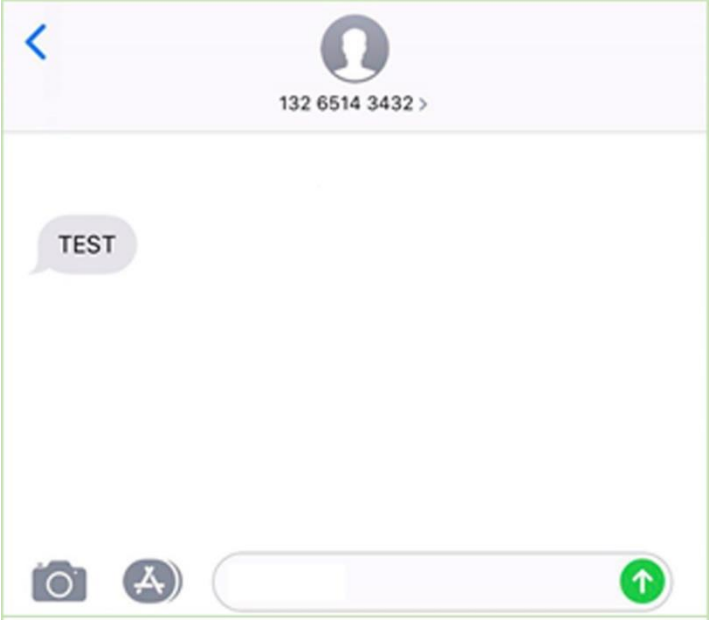
Step 4 Send the content.



Step 5 Send the ending code "1a" in HEX, if you get the reply "OK" it means the SMS has been successfully sent.



Step 6 Test successful, the mobile phone has received the SMS message.


132 6514 3432 ›
TEST

21.2. AT Over Telnet

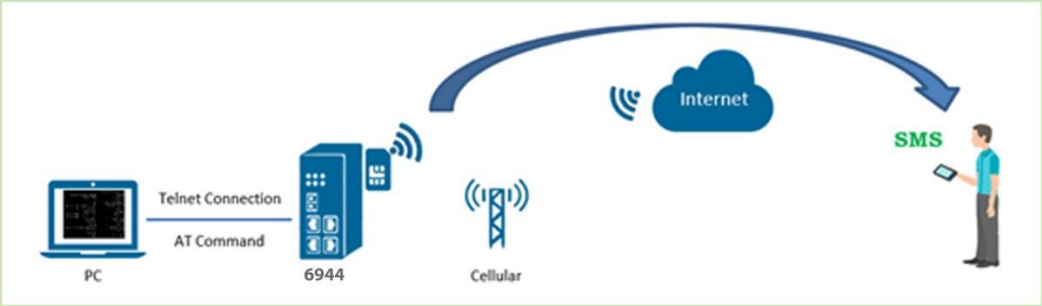
Overview

This document contains information regarding the configuration and use of AT over Telnet.

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
18.7.2019	V1.1	V1.1.4 ()	1.0.1 (42ccf3e)	First release

Testing Topology

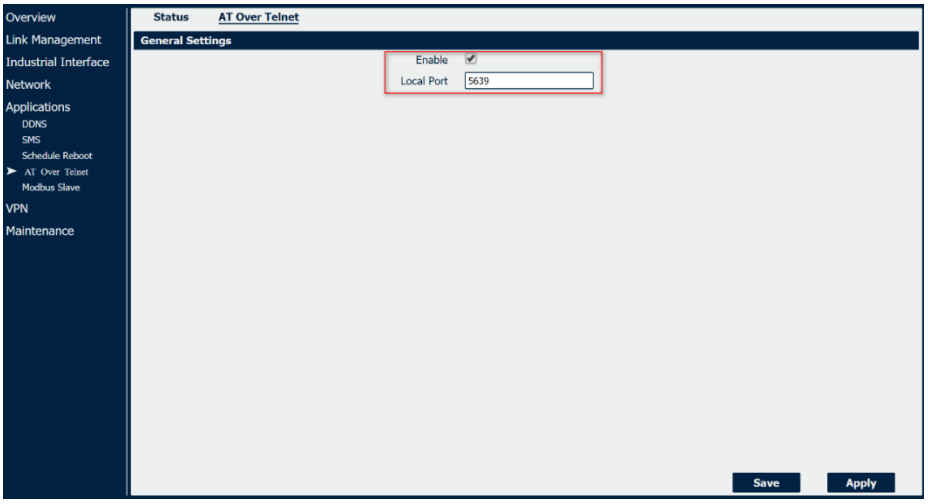


- The 6944 connects to the Internet via its SIM card.
- The PC connect to the 6944 via an ethernet cable using the Telnet protocol.
- The PC sends an AT Command to control the module in the 6944 to undertake an action.

Note: This application note will show how to use the AT Command to control module to send a text mode SMS message.

Configuration

Step 1 Go to **Application>AT Over Telnet**, enable AT Over Telnet feature like below:



Step 2 Click Save>Apply.

Testing

As a test send the content "TEST" to the mobile phone in text mode. We have shown the AT Command required to be sent to the 6944 router, with one command at a time.

at+cmgf=1

at+cmgs="15915802180"

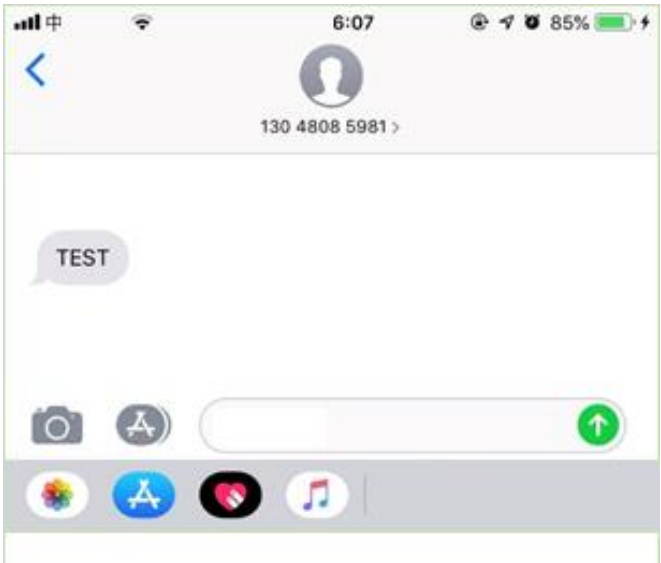
>TEST

Note: After entering the content "TEST", please press the keyboard "Ctrl+z" to send the SMS.

Step 1 Run the "putty" software and telnet to the router, enter the AT command to trigger the 6944 module to send the SMS as shown below:

```
192.168.5.1 – PuTTY
At
ERROR
At
OK
At+cmgf=1
OK
At+cmgs= 078875277882
>TEST
+CMGS: 237
OK
```

Step 2 The Mobile phone receives the SMS with content "TEST":



Step 3 Test successfully.

21.3. AT Over COM

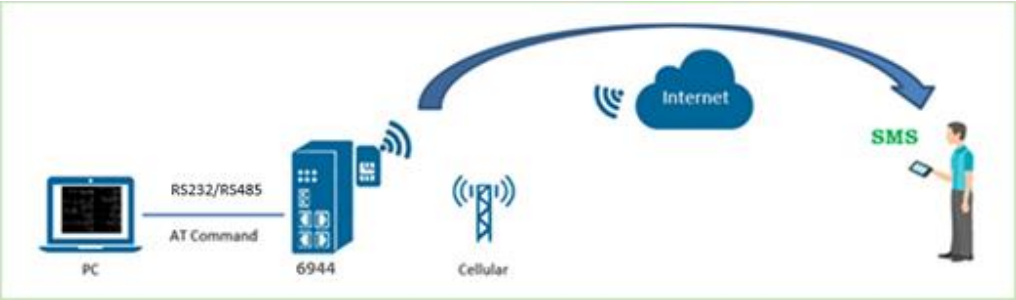
Overview

This document contains information regarding the configuration and use of AT Over Com

Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
18.7.2019	V1.1	V1.1.4 (0c0c9fa)	1.0.1 (42ccf3e)	First release

Testing Topology



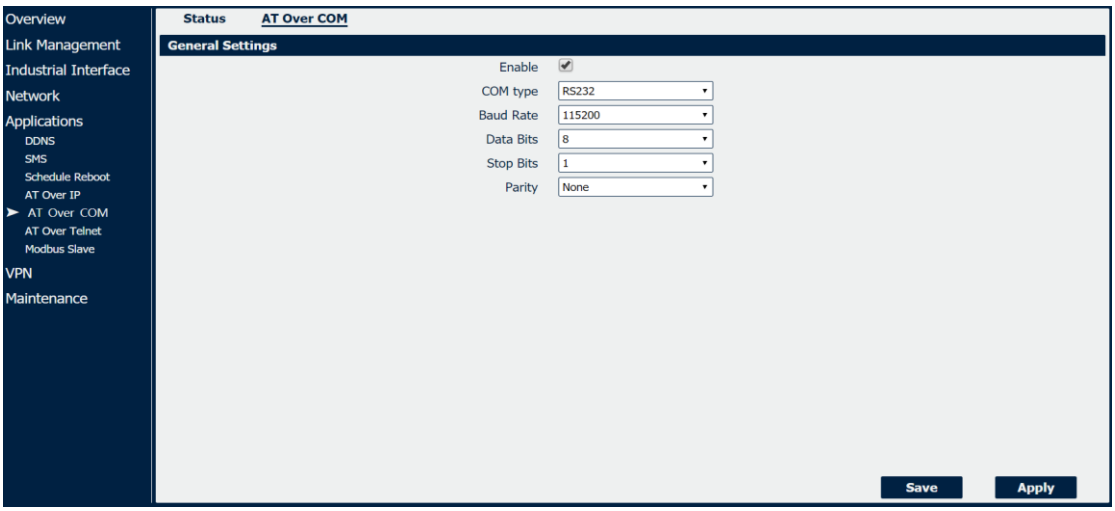
- The 6944 connects to the Internet via its SIM card.
- A PC connects to the 6944 via its serial port (RS232 or RS485).
- The PC sends an AT Command to control the 6944 to produce an action.

Note: This application note will show how to send the AT Command via RS232 interface to control the 6944 module to send an SMS message.

Configuration

6944 Configuration

Step 1 Go to **Application>AT Over COM**, enable AT Over COM as shown below



Step 2 Click Save>Apply.

Testing

Step 1 Send the content "HELLO" to the mobile phone using text mode to test.

Below is the AT Command and content need to be sent one by one to the router.

a) at+cmgf=1\r

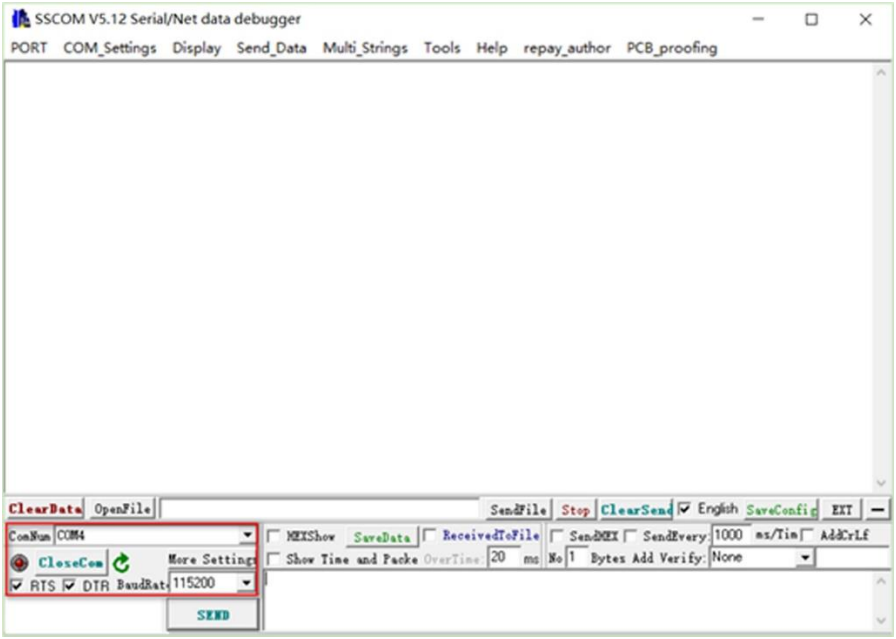
b) at+cmgs=15915802180\r

c) HELLO

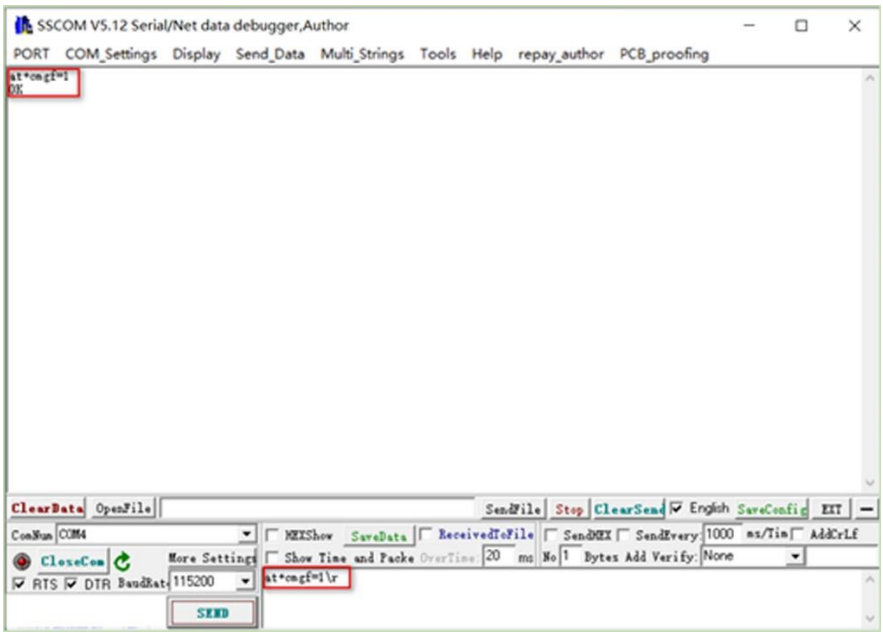
d) 1a

Note: "\r" means the keyboard "Enter"; Option "c" is the content to be sent under text mode; Option "d" is the end code to be sent with HEX.

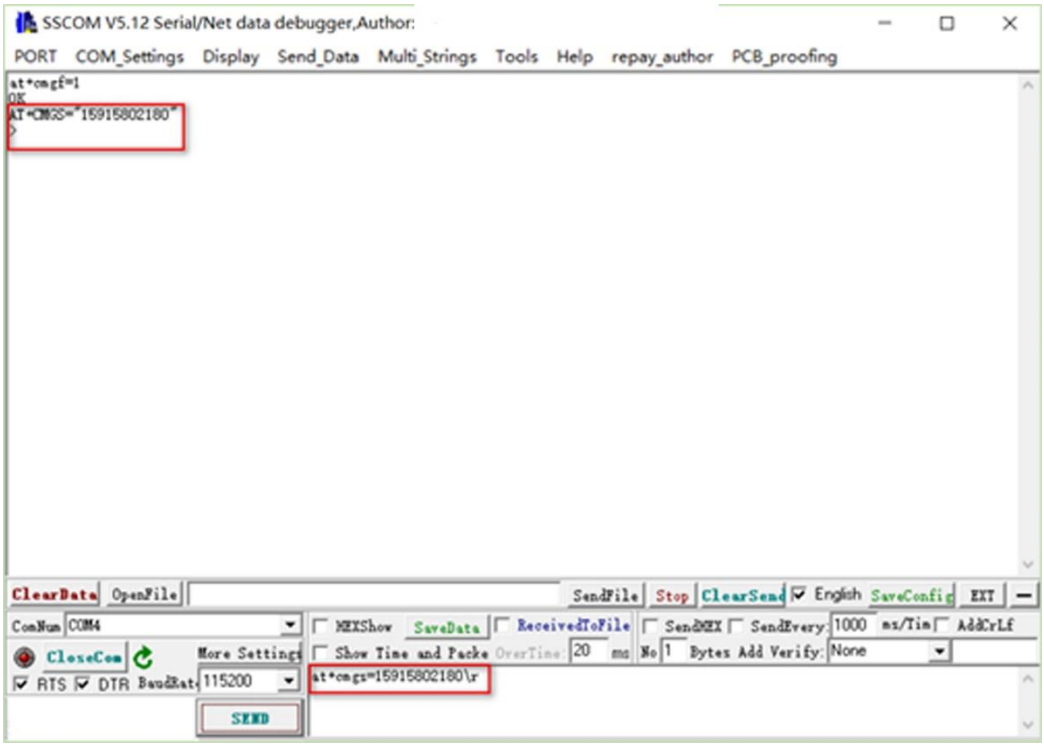
Step 2 Run SSCOM software and connect the 6944 router via its serial port, as shown below:



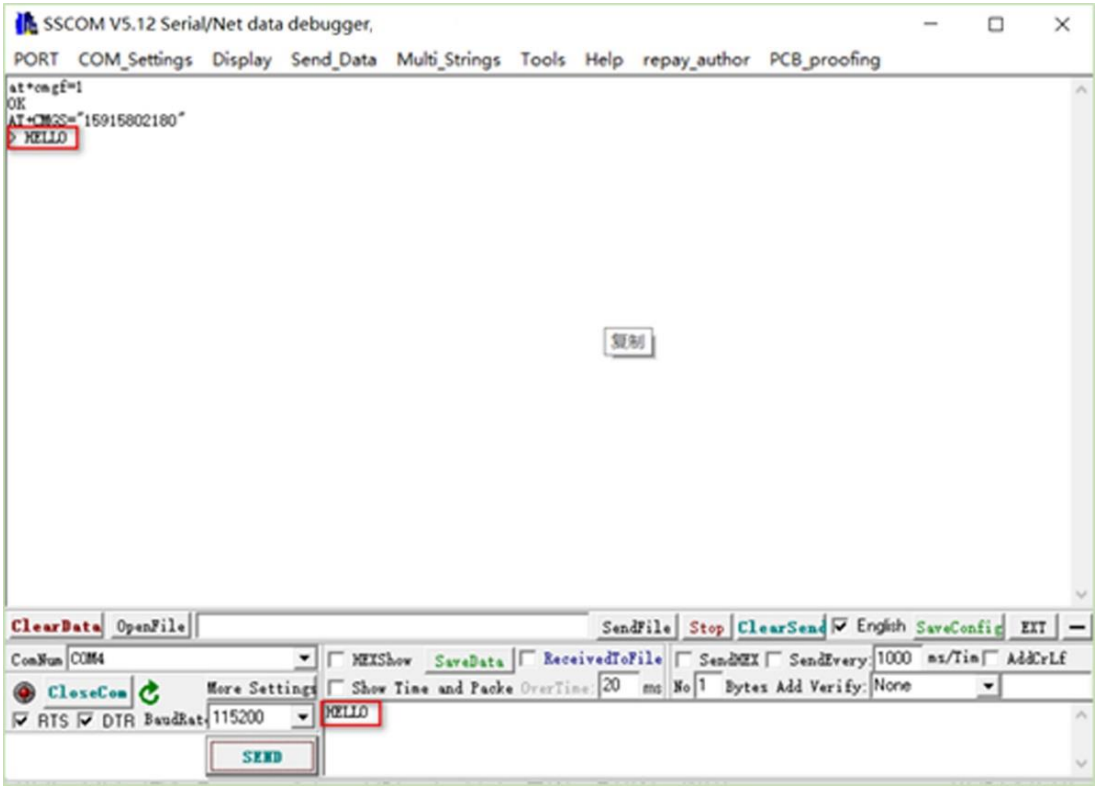
Step 3 Send the AT command "at+cmgf=1\r" in TEXT mode



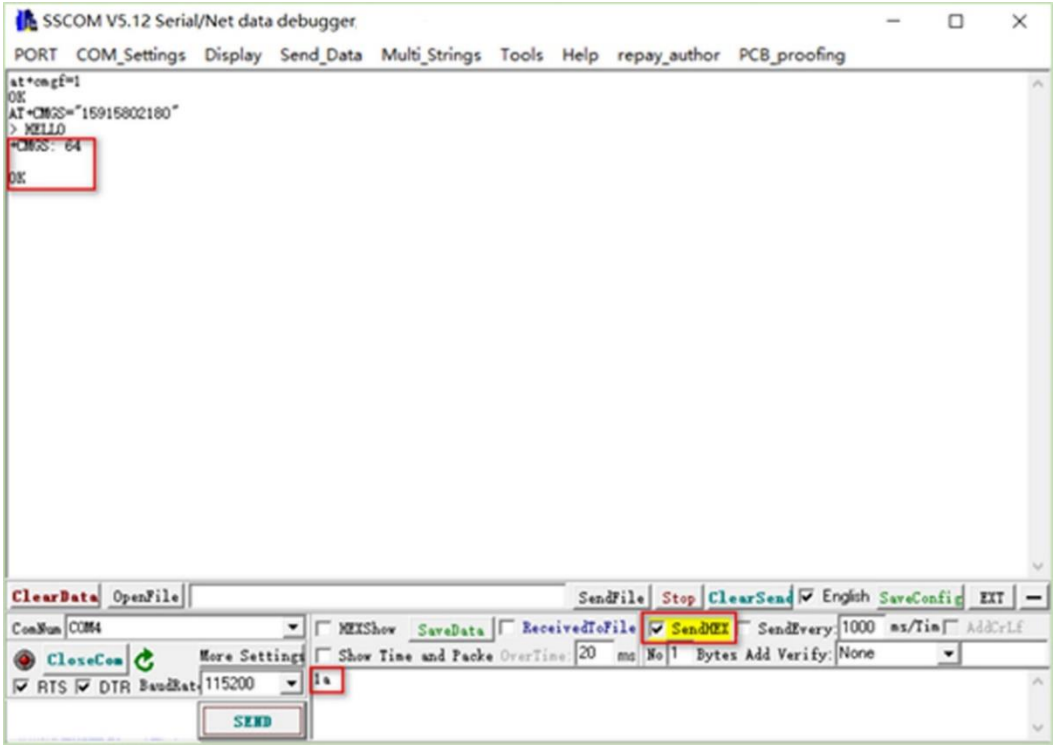
Step 4 Send the AT command “at+cmgs=15915802180\r” to start to send the content to the designated phone number.



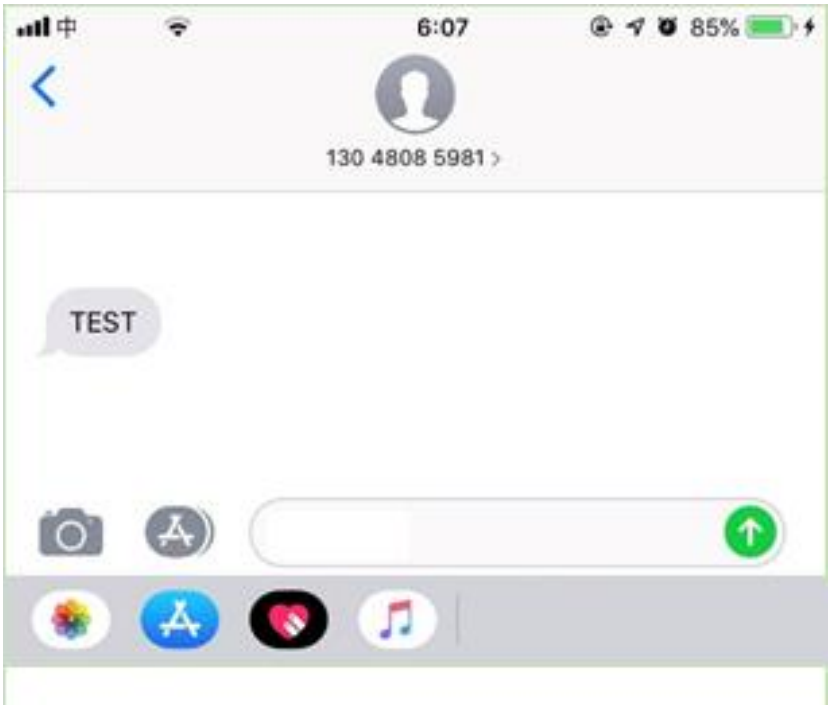
Step 5 Send the message “HELLO”.



Step 6 Send the ending code “1a” with HEX. The reply “OK” means the SMS was sent successfully.



Step 7 When the test is successful, the mobile phone will receive the SMS message.

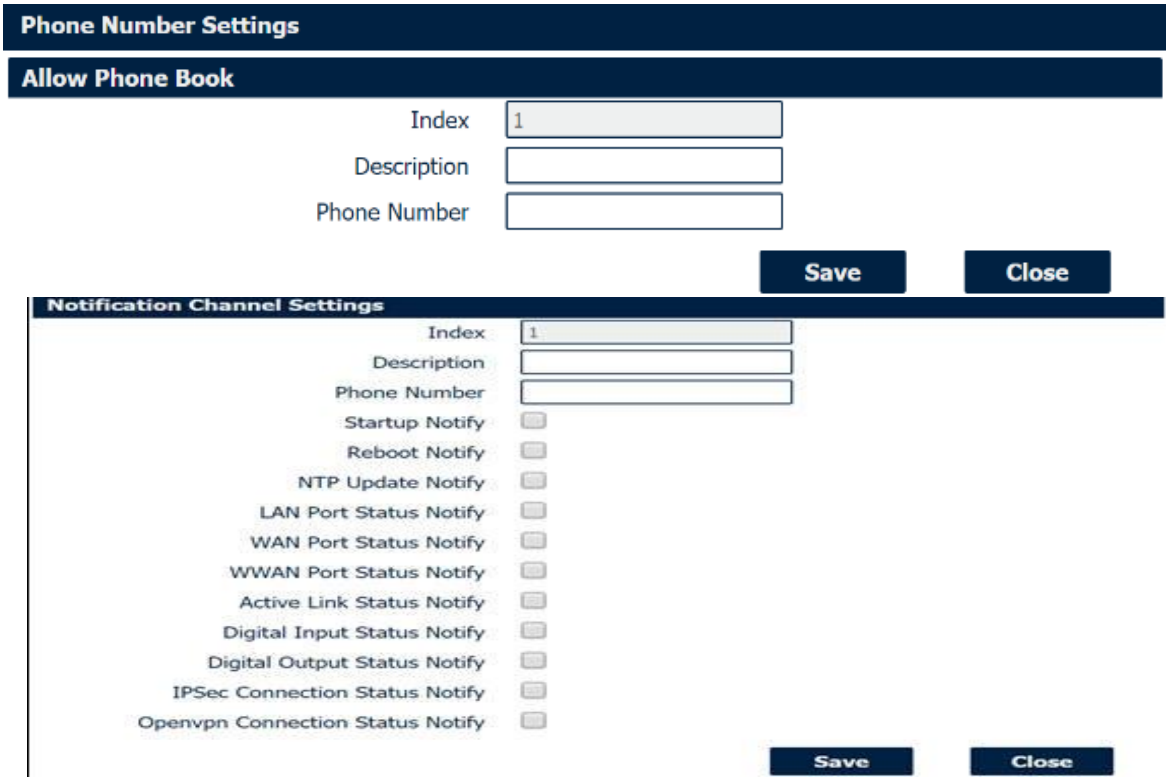


22. SMS Commands

SMS allows a user to send an SMS to monitor or control the 6944 router or get the operational status of the router. Using a Text or SMS allows the network manager to use the CLI to control the 6944

Application->SMS

- **Enable -** Select this box to enable SMS feature.
- **Authentication Type -** Specify the authentication mode for SMS, optional for "None" and "Password".
- **Description -** Enter the description of the Phone Book
- **Phone Number -** Enter the special phone number and only allow this phone number to send an SMS to the 6944 router
  The SMS Gateway sends SMS messages by using a valid syntax from the serial device or ethernet device.



Using SMS to control the Digital Input / Output

We can send the SMS message to control the Digital Output ON or OFF. Please kindly check below SMS commanc

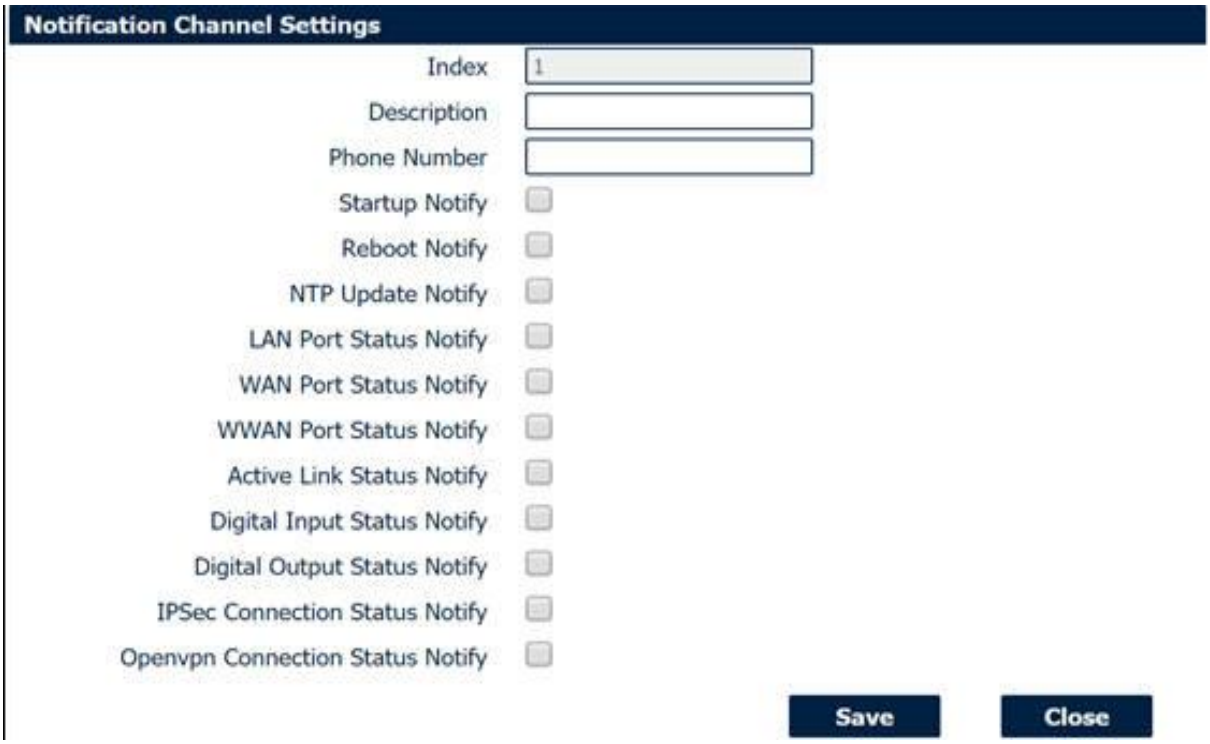
admin$admin$doctl$DO 1/2 ON
admin$admin$doctl$DO 1/2 OFF

"1" means Digital Output 1
"2" means Digital Output 2

Application->SMS>Gateway

- **Enable -** Check the box will enable SMS gateway.
- **Authentication Type -** Specify the authentication mode for SMS, optional
- for "None" and "Password".
- **SMS Source -** Specify SMS source to receive valid syntax, optional for "Serial Port" and "HTTP(S) GET/POST".
- **Serial Port -** Select the serial port from COM1 or COM2.
- **Baud Rate -** Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.
- **Data Bits -** Select the values from 7 or 8.
- **Stop Bits -** Select the values from 1 or 2.
- **Parity -** Select values from none, even, odd.

SMS Notification feature allow to send SMS notification to the pre-setting phone number when some of router status changed.

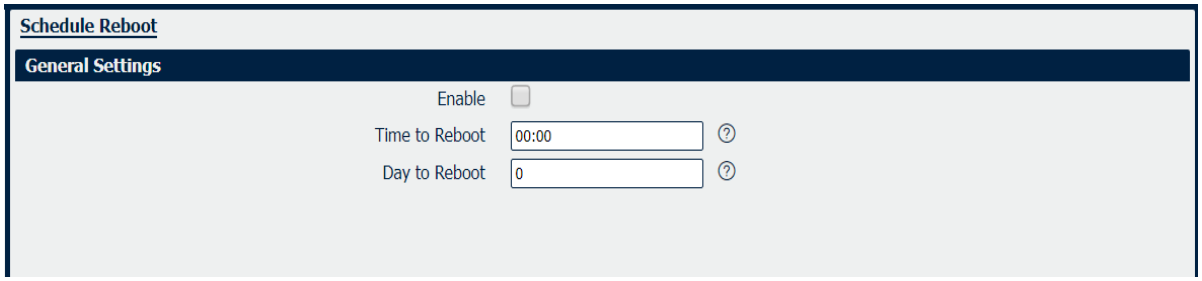


Application->SMS>Notification

- Index - **Display the index of the notification channel, maximum is 10.**
- Description **- Add the description for notification channel.**
- Phone Number **- Pre-setting phone number to receive the notification**
- Startup Notify **- Send SMS notification to the pre-setting phone number when system startup.**
- Reboot Notify **- Send SMS notification to the pre-setting phone number when system reboot.**
- NTP Update Notify **- Send SMS notification to the pre-setting phone number when NTP update successfully.**
- LAN Port Status Notify **- Send SMS notification to the pre-setting phone number when LAN port status changed.**
- WAN Port Status Notify **- Send SMS notification to the pre-setting phone number when WAN port status changed.**
- WWAN Port Status Notify **- Send SMS notification to the pre-setting phone number when WWAN port status changed.**
- Active Link Status Notify **- Send SMS notification to the pre-setting phone number when active link status changed.**
- Digital Input Status Notify - **Send SMS notification to the pre-setting phone number when DI status changed.**
- Digital Output Status Notify **- Send SMS notification to the pre-setting phone number when DO status changed.**
- IPSec Connection Status Notify **- Send SMS notification to the pre-setting phone number when IPSec connection status changed.**
- OpenVPN Connection Status Notify **- Send SMS notification to the pre-setting phone number when OpenVPN Connection Status changed.**

Schedule Reboot

Schedule reboot allows the user to define a time for 6944 router reboot itself.

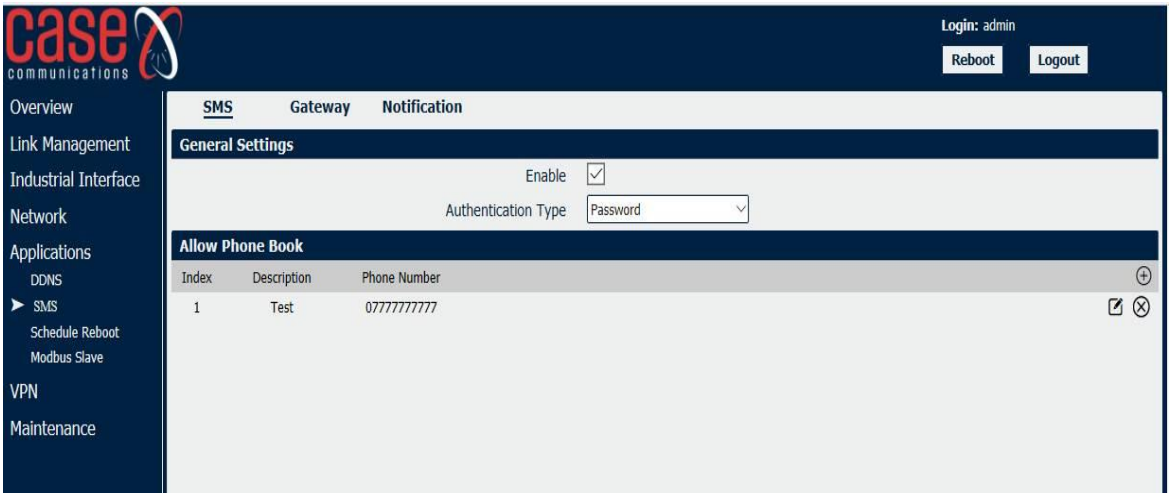


Application->Schedule Reboot

- **Enable -** Select this box to enable schedule reboot feature.
- **Time to Reboot -** Enter the time of each day to reboot device. Format: HH (00-23): MM (00-59).
- **Day to Reboot -** Enter the day of each month to reboot device. 0 means every day.

Sending SMS commands to control the 6944

It's possible to monitor and send commands to the 6944 Router using an SMS / text messages.
To do this it's necessary to send commands using the CLI on the 6944 (Command Line Interface).
Go to the Applications SMS. By default the SMS Control Function is enabled.



Under General Settings are the following options:
User Name and Password: Forces the manager to enter a user name and password (recommended)
User Name and Password: None – allows the manager to connect without using a user name and password.
Allow Phone Book: This option only allows the 6944 to send and receive SMS messages from numbers in its internal directory.

SMS Commands

<u>Authentication Type: Password</u>

1. Admin$admin$enable$version // send an SMS to check the firmware version

- *The first "admin" means the router username;*
- *The second "admin" means the router password;*
- *"Enable" means to send the CLI Command used in "enable mode".*
- *"version" is the CLI command under enable mode*

2. Admin$admin$config$set syslog level info //send SMS to set router syslog to info level

- *The first "admin" means the router username;*
- *The second "admin" means the router password;*
- *"Config" means to send the CLI Command of "config mode".*
- *"set syslog level info" is the CLI command under config mode*

We also can send SMS with **multiple** CLI Commands, like below:

1. admin$admin$enable$version;show active link //

- Send SMS to check firmware version and link information together.

2. admin$admin$config$set syslog location ram;set syslog level info //

- Send SMS to set syslog location and syslog level.

3. admin$admin$enable$reboot

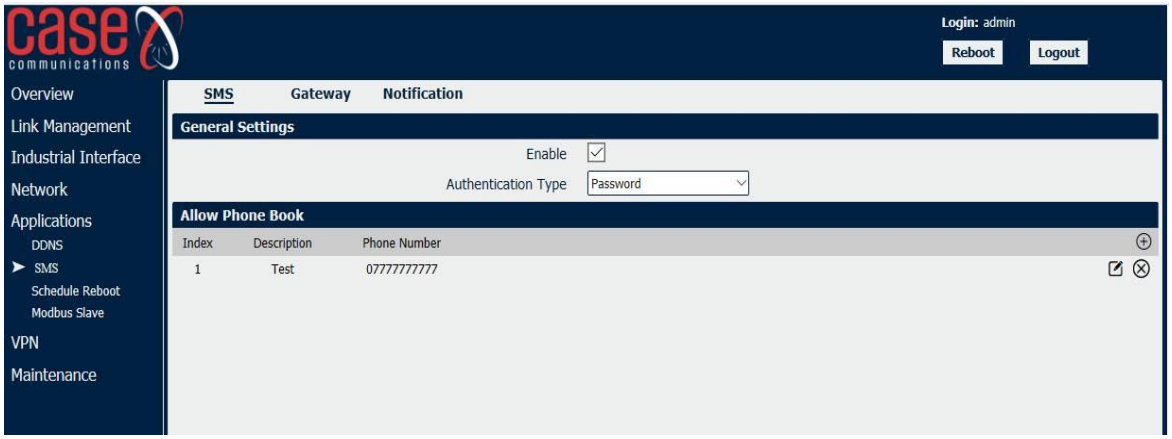
- This option reboots the 6944

Authentication Type: None (i.e. only using the 6944 telephone directory for security)

1. enable$version
2. config$set syslog level info
3. enable$version;show active_link
4. config$set syslog location ram;set syslog level info

22.1. SMS Control

Go to the Applications SMS. By default the SMS Control Function is enabled.



Under General Settings you have the following options:

User Name and Password: Force the manager to enter a user name and password (recommended)

User Name and Password: None – allows the manager to connect without using a user name and password.

Allow Phone Book: This option only allows the 6944 to send and receive SMS messages from numbers in its internal directory.

SMS Commands

Authentication Type: Password

1. admin$admin$enable$version // send an SMS to check the firmware version

- *The first "admin" means the router username;*
- *The second "admin" means the router password;*
- *"enable" means to send the CLI Command used in "enable mode".*
- *"version" is the CLI command under enable mode*

2. admin$admin$config$set syslog level info //send SMS to set router syslog to info level

- *The first "admin" means the router username;*
- *The second "admin" means the router password;*
- *"config" means to send the CLI Command of "config mode".*
- *"set syslog level info" is the CLI command under config mode*

We also can send SMS with **multiple** CLI Commands, as shown below

admin$admin$enable$version;show active_link //

- send SMS to check firmware version and link information together.

admin$admin$config$set syslog location ram;set syslog level info //

- send SMS to set syslog location and syslog level.

admin$admin$enable$reboot

- This option reboots the 6944

Authentication Type: None (i.e. only using the 6944 telephone directory for security)
1. enable$version
2. config$set syslog level info
3. enable$version;show active_link
4. config$set syslog location ram;set syslog level info

<u>CLI Command</u>

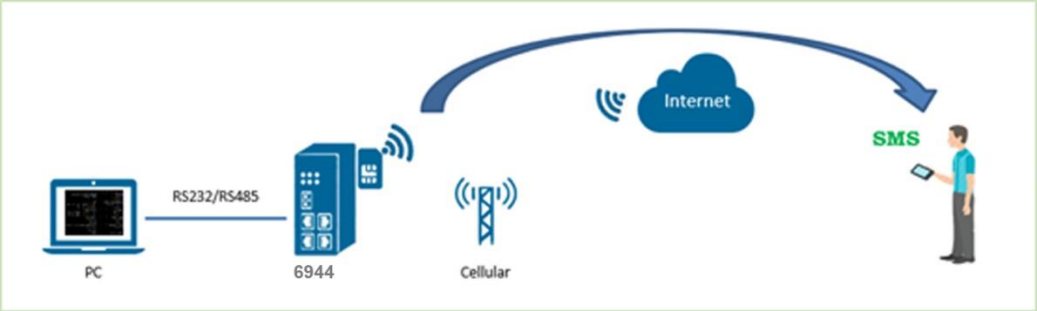
Step 1: Telnet to the router to check the CLI command under "enable mode" or "config mode".
6944.router login: admin
> ← Enable Mode (You are now in enable mode)
>
< Config
config# ← You're now in configuration mode
config#

Step 2 When you have connected to the router using telnet, it pops up with the character **">"**,
This means that the router is now in "enable mode" and you can then go into configure mode
Step 3 Using the CLI Command enter "config", then the router will go into "config mode"
Step 4 Enter the "?" or keyboard "Tab", then we can see the command options using the CLI as shown below
>

config	Change to the configuration mode
exit	Exit this CLI Session
help	Display and Overview of the options available using CLI syntax
ping	Send a Ping to a device
reboot	Reboot the 6944 router
show	Show the running configuration or running status
telnet	Telnet to a client
traceroute	Traceroute
upgrade	Upgrade the firmware
version	Display the 6944's current version of software

Step 5 For example to reboot the 6944 enter (admin$admin$enable$reboot)

22.2 SMS Gateway

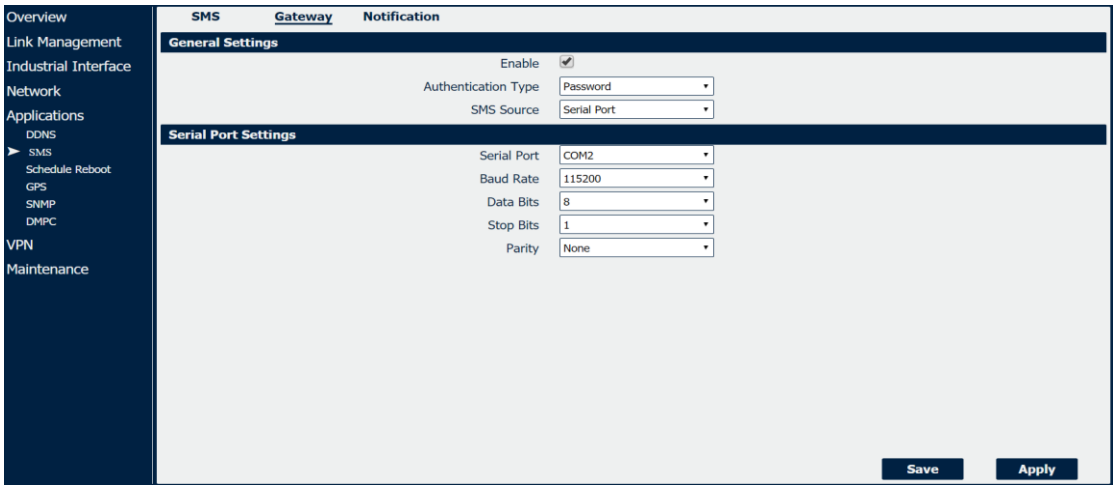


- The 6944 connects to Internet via its SIM card.
- The PC connects to the 6944 via a serial port (RS232 or RS485).
- The PC sends the special command via its serial port to the 6944 and triggers the 6944 to send the SMS to the receiver.

Note: This Application Note will show the example when the router receives the special command from the RS232 Port. This can also work on the RS485 Port.

6944 Configuration

Step 1 Go to **Application>SMS>Gateway**, enable SMS Gateway feature like below:



Step 2: Click Save>Apply.

Testing

Send a message (in our example it is "**hello**") to the mobile phone.

Here are the commands that needs to be sent to the router via RS232 Port.

a) sms_send&admin&admin&15915802180&Text_To_Send

b) 1a // it is the ending code and need to be sent with "HEX"

Here is the explanation of the command "a":

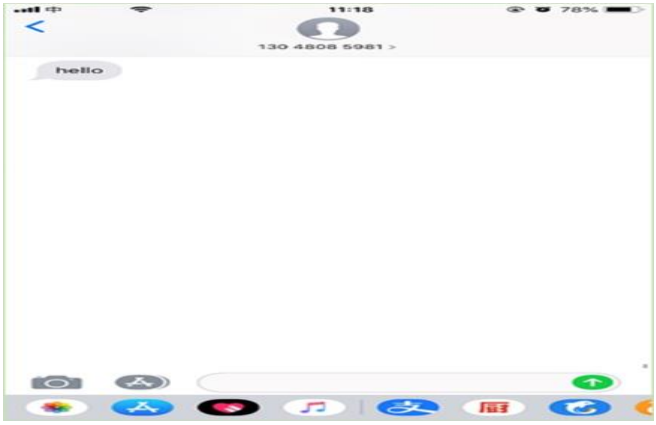
sms_send&username&password &phone number&SMS content

Step 1 Run the SSCOM software and connect the 6944 router via serial port, as below:

Step 2 Send the SMS with the content "**hello**" to a receiver phone number for example. **15915802180**".

Step 3 Send the ending code "**1a**" with "**HEX**":

Step 4. If the test is successful, the mobile phone will receive the SMS message.



22.3 SMS Notification

Overview

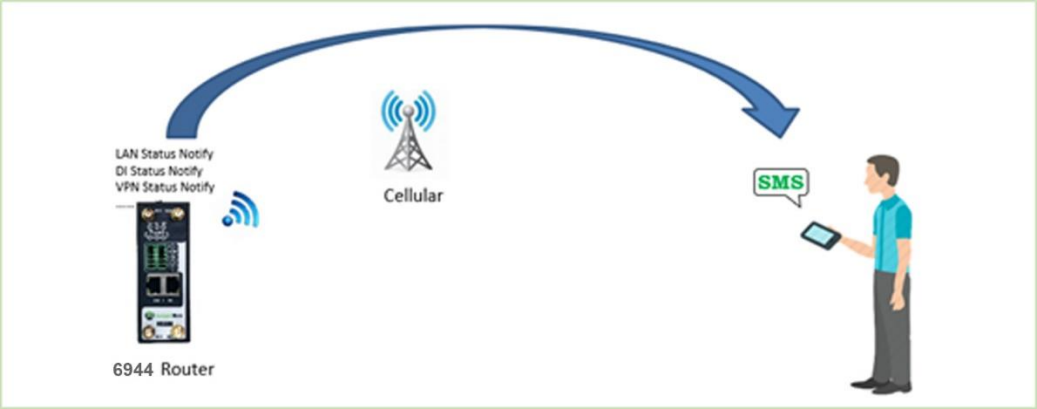
This document contains information regarding configuring the SMS Notification from the 6944 to a mobile device.

Software Version

Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
3.9.2020	V1.1	V1.1.4	Std Software	First release

Topology

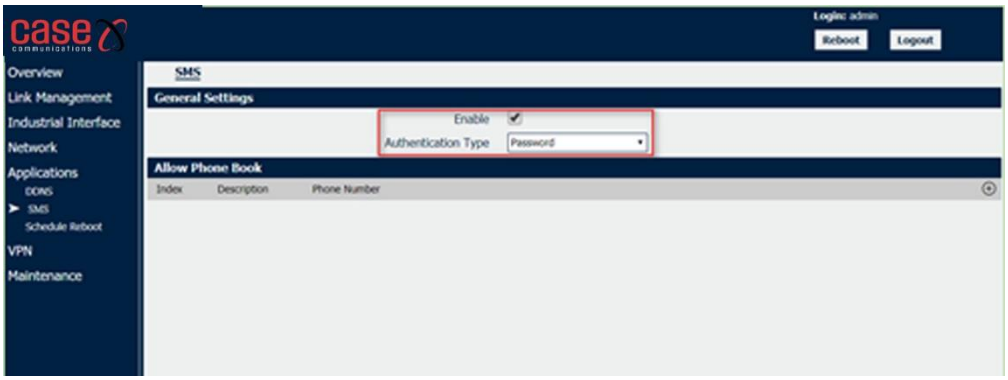


- The 6944 router connects to the Internet successfully via its SIM card.
- An engineer sends the SMS to the router with a Special SMS Command to control the 6944 router restart or configure the 6944 router.

Note:
Special SMS Command means the router CLI Command. The engineer will send SMS message with the CLI Command to control or monitor the router.

6944 Router Configuration

Step 1. Go to **Applications>SMS**, SMS control (the function) is enabled by default.



Authentication Type:
Password: SMS command with router username and password
None: SMS command without router username and password

Allow Phone Book:

The router only receives the SMS message from phone numbers listed in the phone book

SMS Command

Authentication Type: Password

1. admin$admin$enable$version // send SMS to check the firmware version

The first "admin" means the router username; the second "admin" means the router password; "enable" means to send the CLI Command of "enable mode". "Version" is the CLI command under enable mode

2. admin$admin$config$set syslog level info //send SMS to set router syslog to info level

The first "admin" means the router username; the second "admin" means the router password; "config" means to send the CLI Command of "config mode". "Set syslog level info" is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, like below:

1. admin$admin$enable$version;show active_link //send SMS to check firmware version and link information together.

2. admin$admin$config$set syslog location ram;set syslog level info // send SMS to set syslog location and syslog level.

Authentication Type: None

1. enable$version

2. config$set syslog level info

3. enable$version;show active_link

4. config$set syslog location ram;set syslog level info

CLI Command

Step 1 Telnet to the router to check the CLI command under "enable mode" or "config mode".

When you have connected to the router using telnet the following prompt appears ">", this means that the router is in "enable mode"

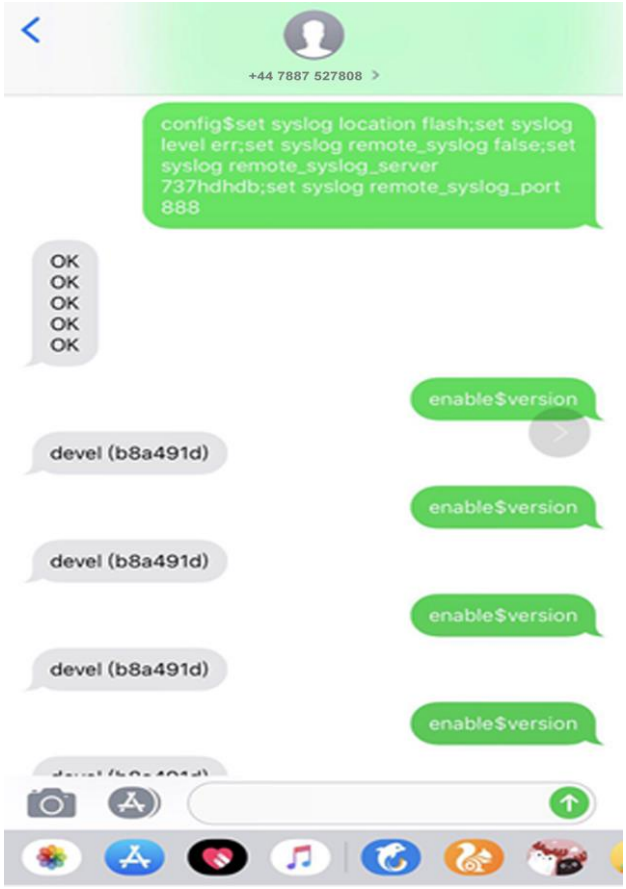
When you enter the CLI command "config", then the router will go into "config mode"

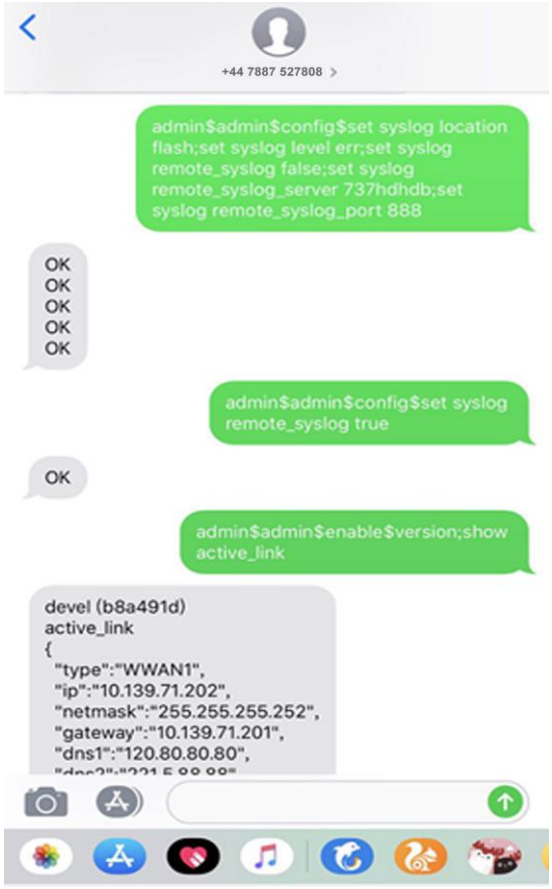
Step 2 Enter the "?" or keyboard "Tab", then we can see CLI commands as shown below:

```
>
  config      Change to the configuration mode
  exit        Exit this CLI session
  help        Display an overview of the CLI syntax
  ping        Ping
  reboot      Reboot system
  show        Show running configuration or running status
  telnet      Telnet Client
  traceroute  TraceRoute
  upgrade     Upgrade firmware
  version     Show firmware version

>
```

Testing

Step 1: Below test result for reference.

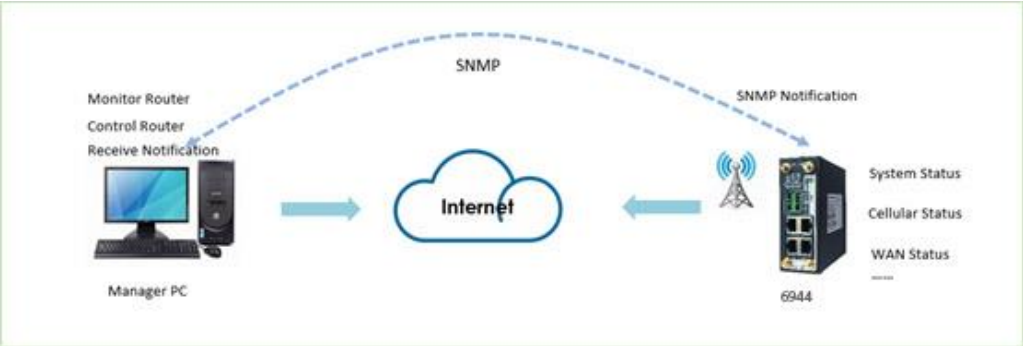




This page left blank intentionally

23. SNMP

23.1. Testing Topology



Criteria of the SNMP test

- The 6944 Manager PC can access the 6944 router using SNMP Protocol.
- The Manager PC can obtain the 6944 operational status, and control the 6944 router and receive SNMP notifications from 6944 router.

Note: For this Application Note, the Intranet was used to test the SNMP instead of the Cellular WAN. The 6944 Manager PC is connected to the LAN port of 6944. The IP address of Manager PC is set to: 192.168.5.19 / 24. The IP address of 6944 LAN port is: 192.168.5.1 / 24.

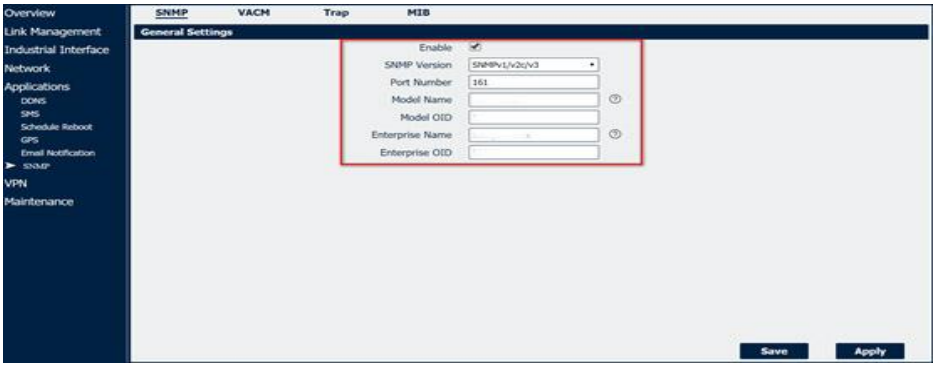
Software Compatibility

Release Date	Doc. Version	Firmware Version	Additional Software	Change Description
4.3.2020	V1.0	V1.1.4	V1.1.3(e335ec6)	First release

Configuration

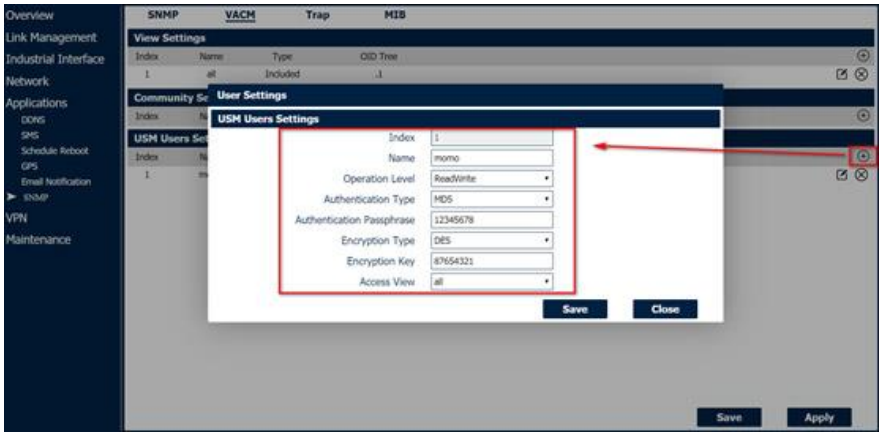
Configuration of the 6944 Router

Step 1 Go to **Applications>SNMP>SNMP**, enable SNMP and set the configuration as below:



Step 2 Click Save>Apply.

Step 3 Go to **Applications>SNMP>VACM,** Set the configuration in "**View Settings"** to default. For **"USM Users Settings"**, please configure the page as shown below:



Step 4 Click 'Save > Apply'

Step 5. Go to "**Applications>SNMP>Trap**", enable SNMP Trap configuration, and the "Notification Host" should be the IP address of the PC running the SNMP management tool, as shown below.

Step 6. Then set the "LAN Notify" as an example, when the LAN Port status is changed, the SNMP management tool will receive the event alarm.

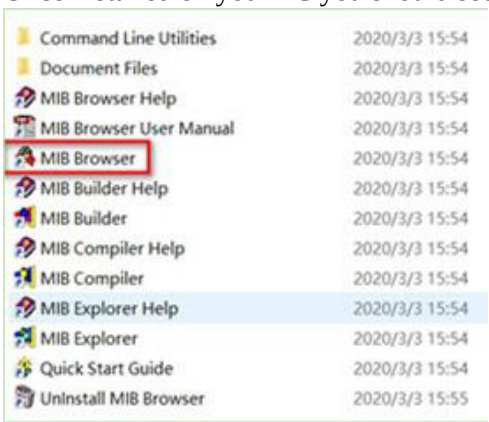
Go to "**Applications>SNMP>Trap>Events Settings**", configuration as shown below.

Step 8 Click Save>Apply

23.2. Configuring an SNMP Management Tool

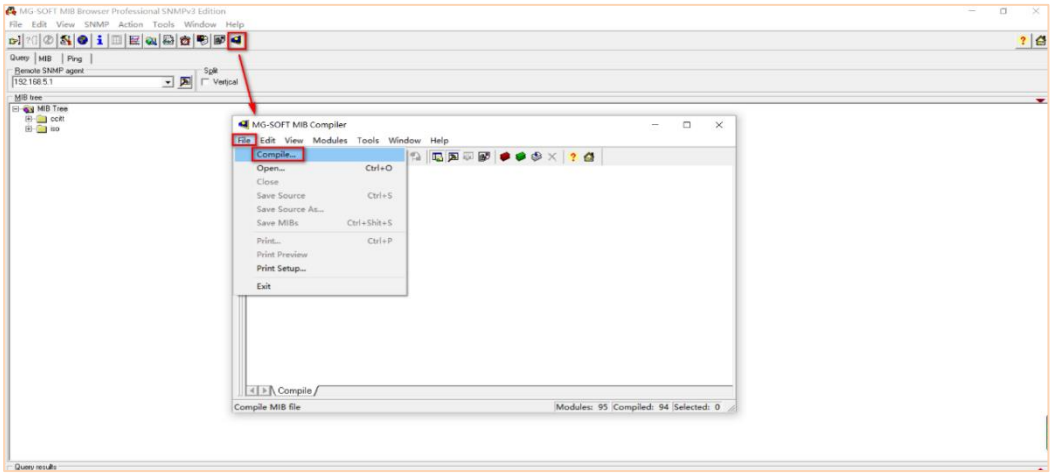
Step 1 - If you don't have an SNMP Management system (such as CaseView) it is possible to use other software such as "MG MIB Browser" as a management tool.

Once installed on your PC you should see the following screen

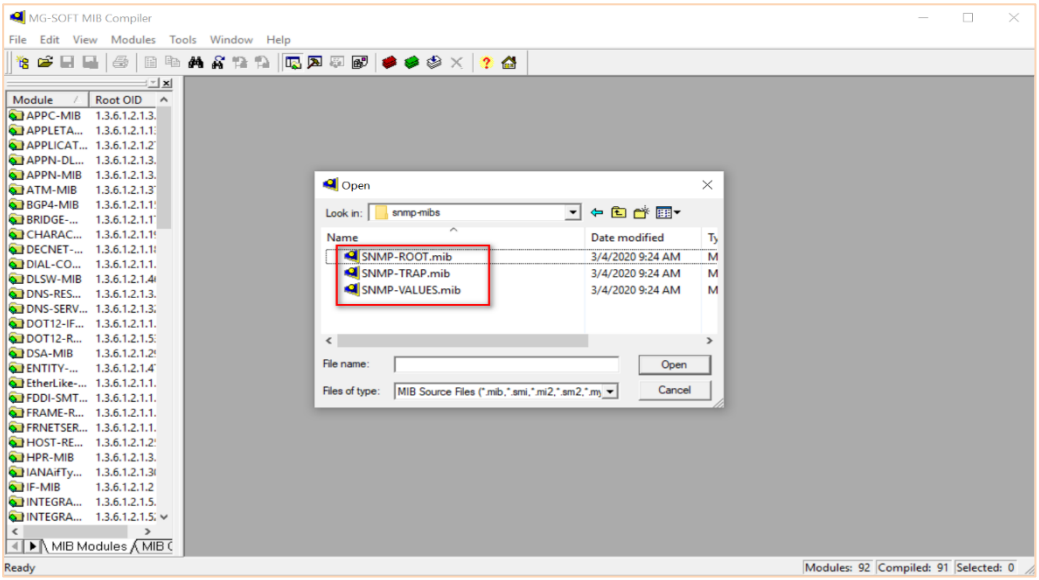


***Note**: After unzipping the "MG MibBrowser" package, install all the files into an "unzip" folder.*

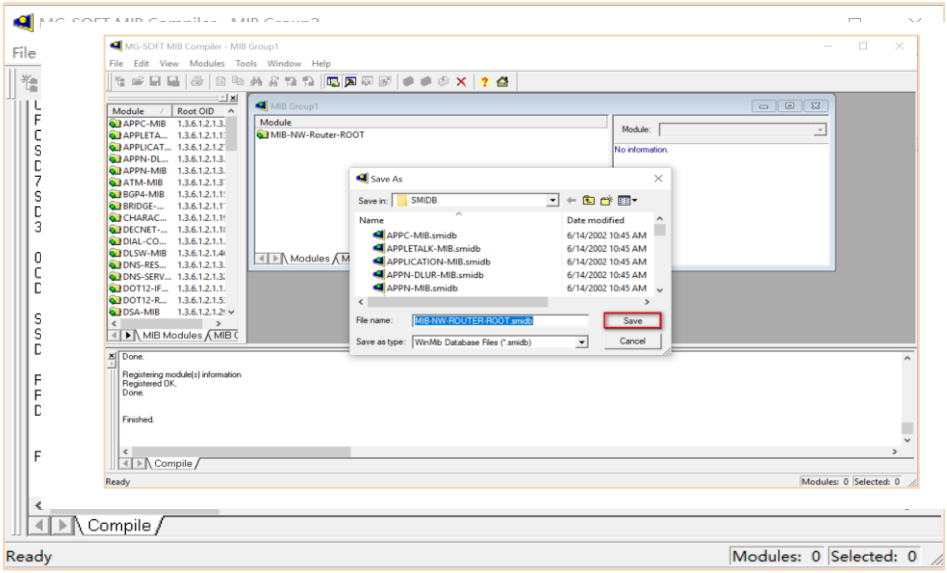
Step 2 Open MibBrowser and run the MIB Compiler as shown below:



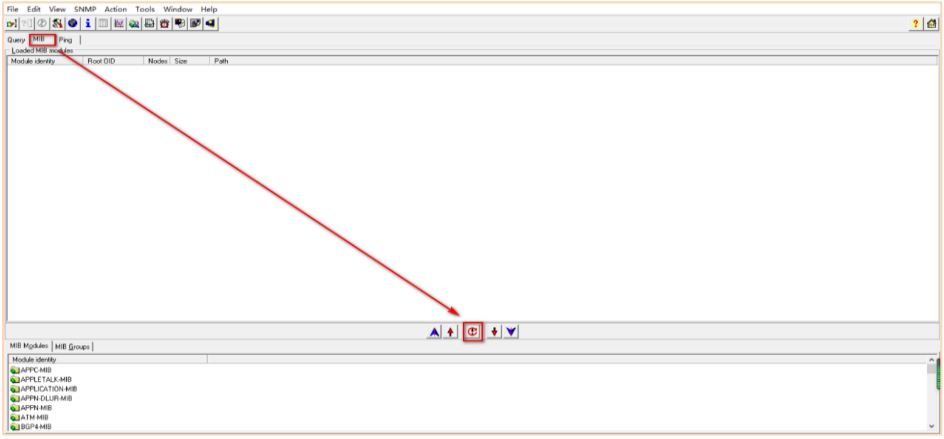
Step 3 Compile the MIB files "SNMP-ROOT.mib", "SNMP-TRAP.mib" and "SNMP-VALUES.mib" **one by one**:



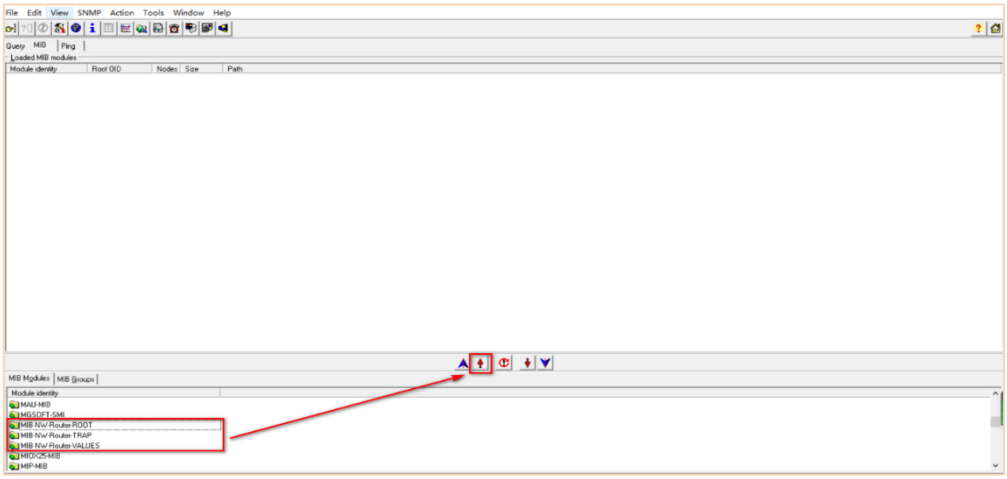
Step 3 : Save the Compiled File as default path, as shown below:

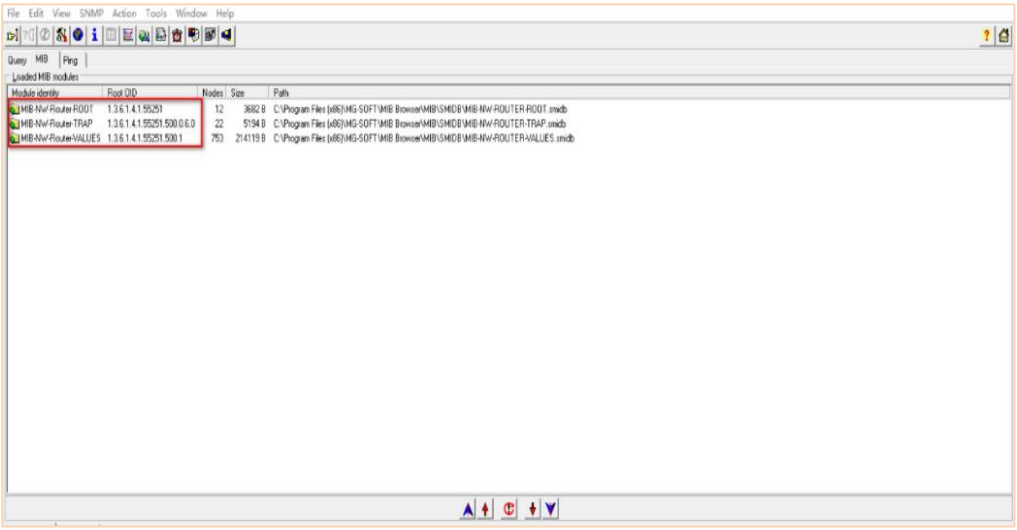


Step 5: After saving the compiled file, refresh the MIB Module:



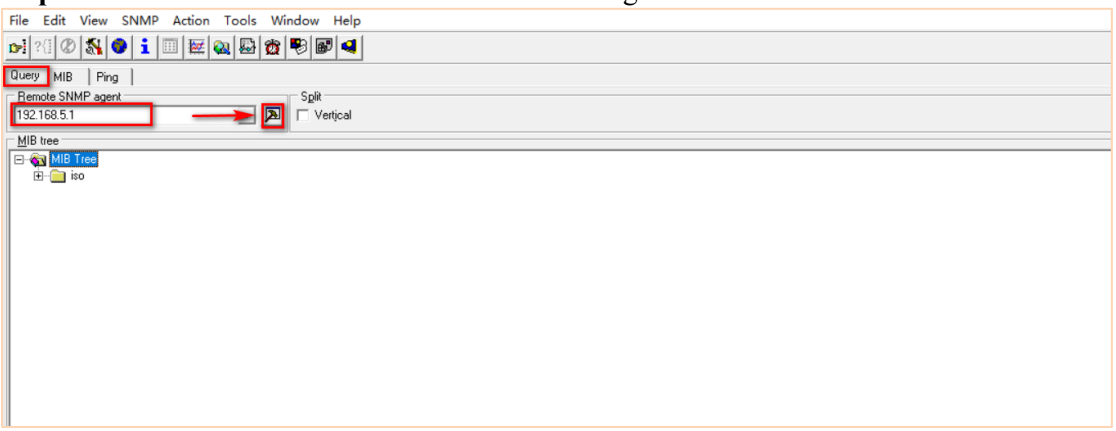
Step 6: Then check the MIB files and load them:



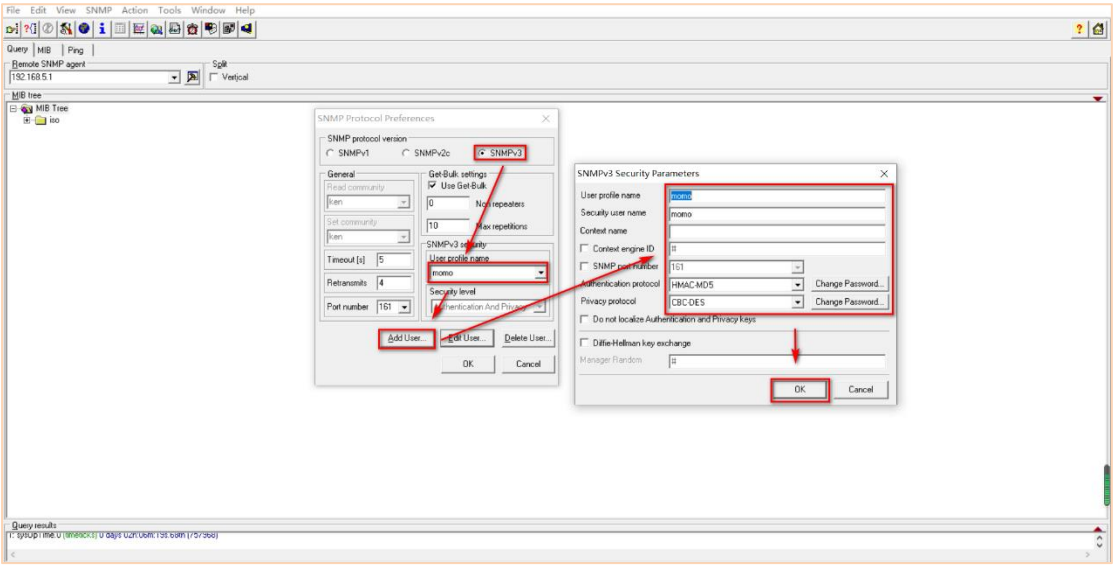


The MIB Files have been loaded

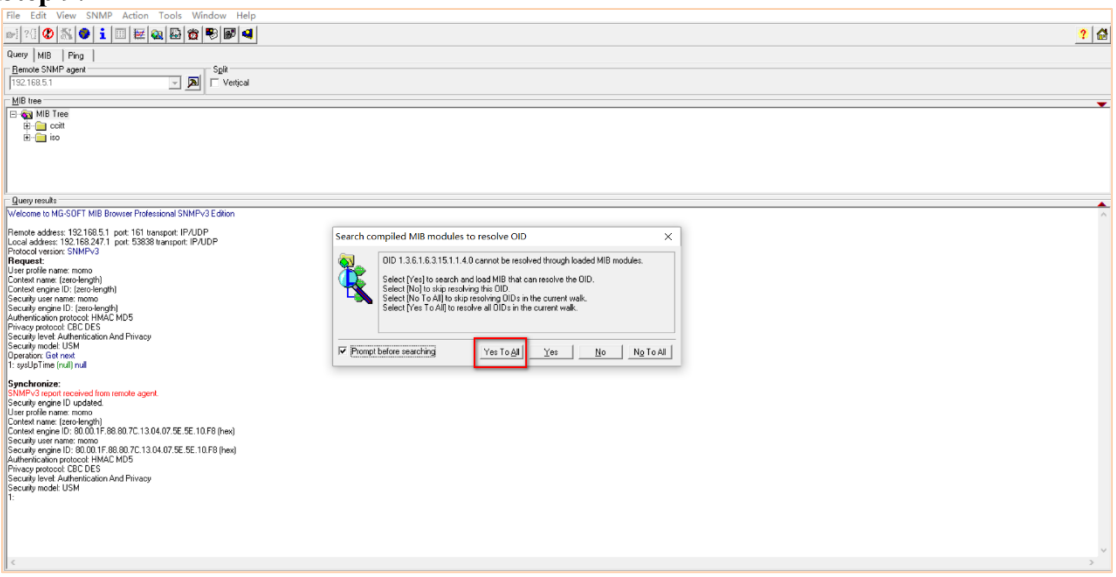
Step 7: Enter the IP address of 6944 router the management tool to the 6944



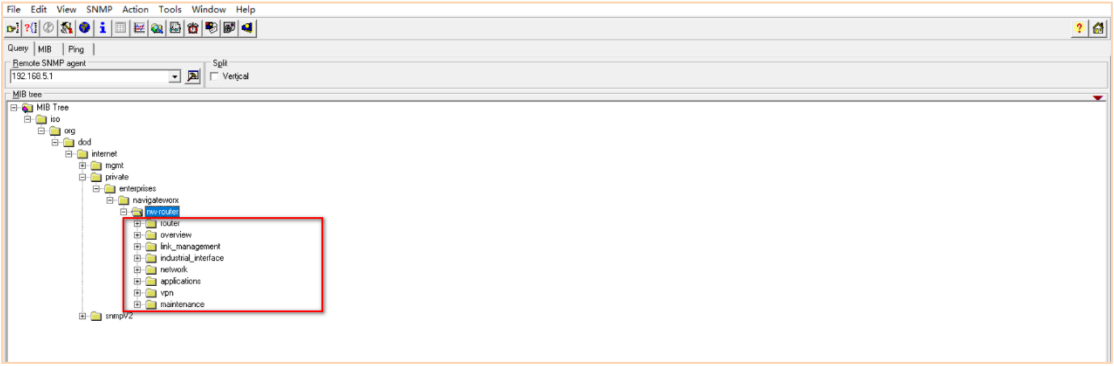
Step 8: Enter the SNMPv3, parameters such Name and the Authentication and so on, as shown below:



Step 9: Click "Yes To All":



Step 10: We should now see the menu on the 6944 router:

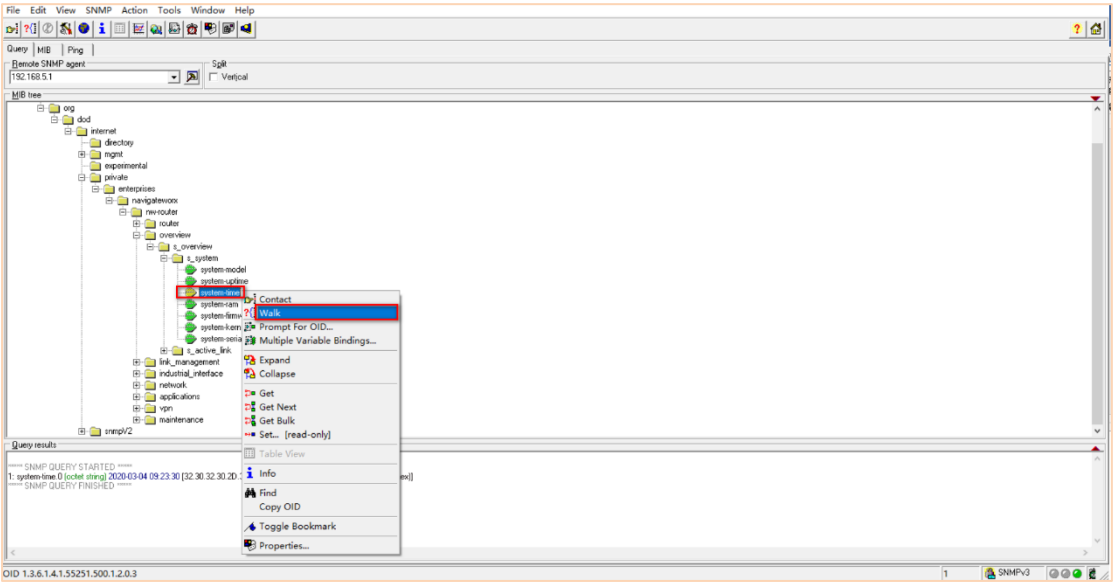


23.3. Testing SNMP

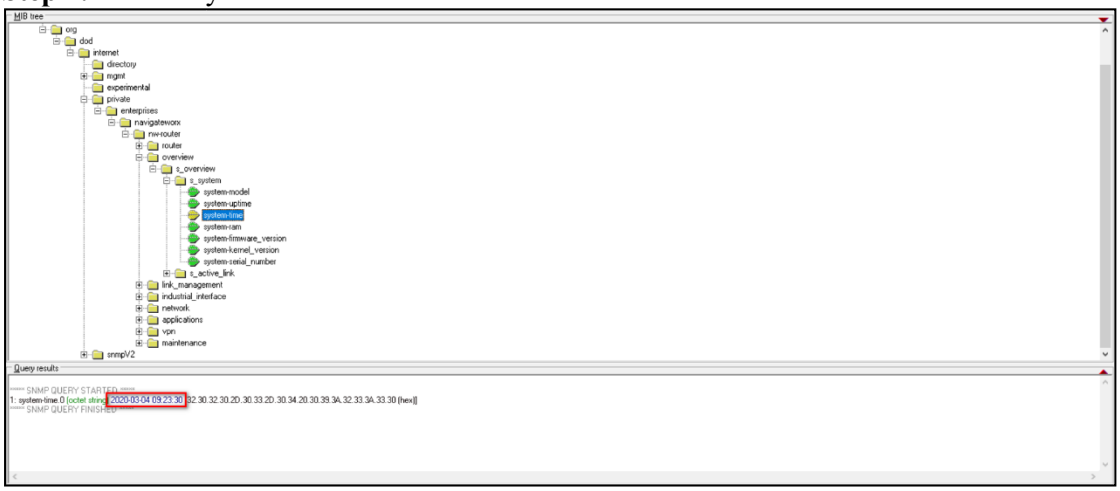
Monitor the Running Status Of The Router

Here we check the "system time" and check the "firmware version" as an example.

Step 1: Go to the "system-time" and Right Click, then click "Walk":



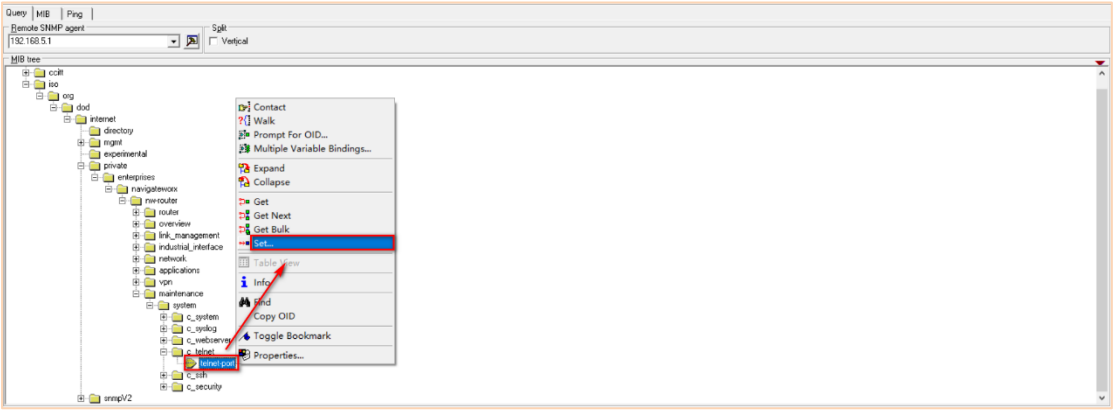
Step 2: Get the System Time of the router:



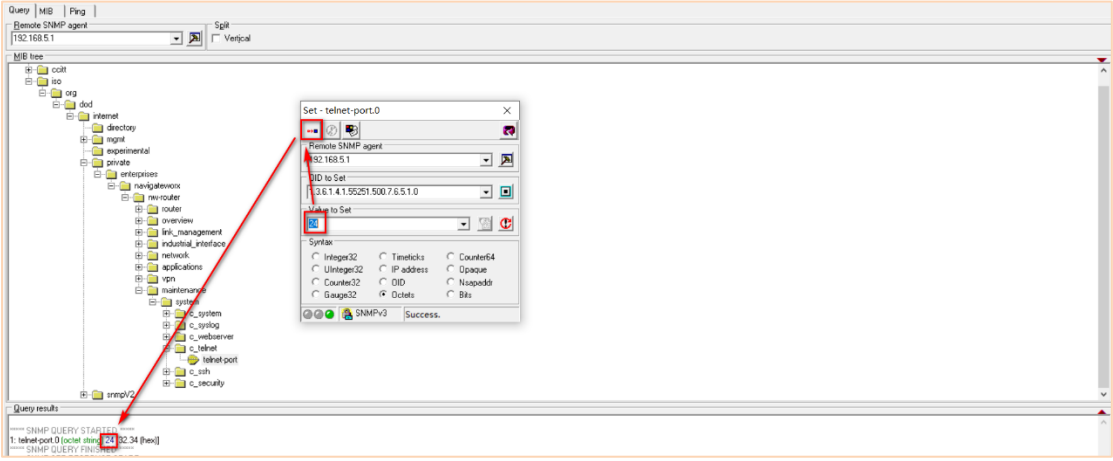
Controlling the 6944 Router

To demonstrate control of the router as an example change the Telnet Port of the 6944 router, then Save, then Apply.

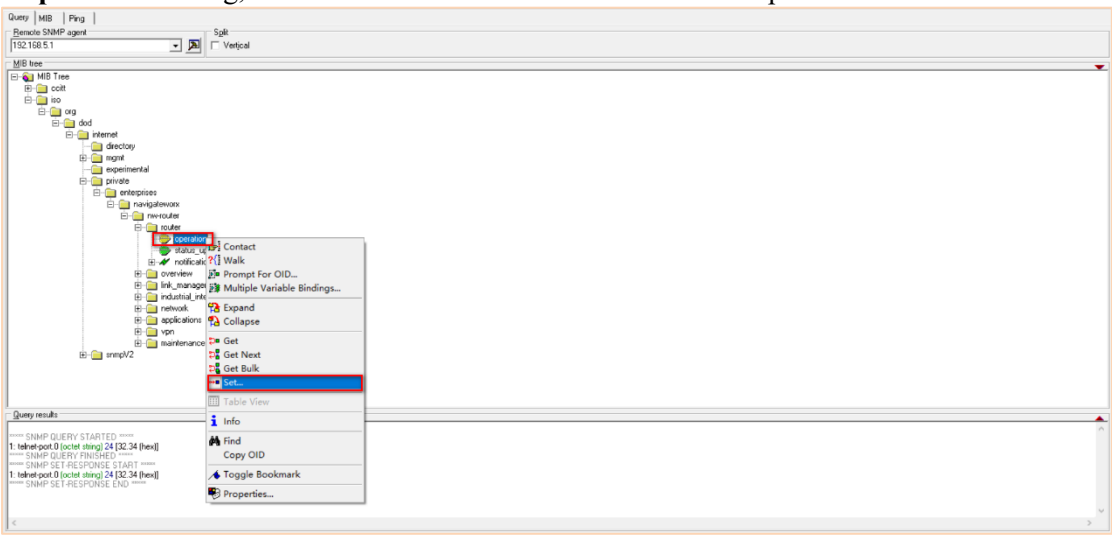
Step 1: Go to the "Telnet" Option, Right Click, then Click "Set":

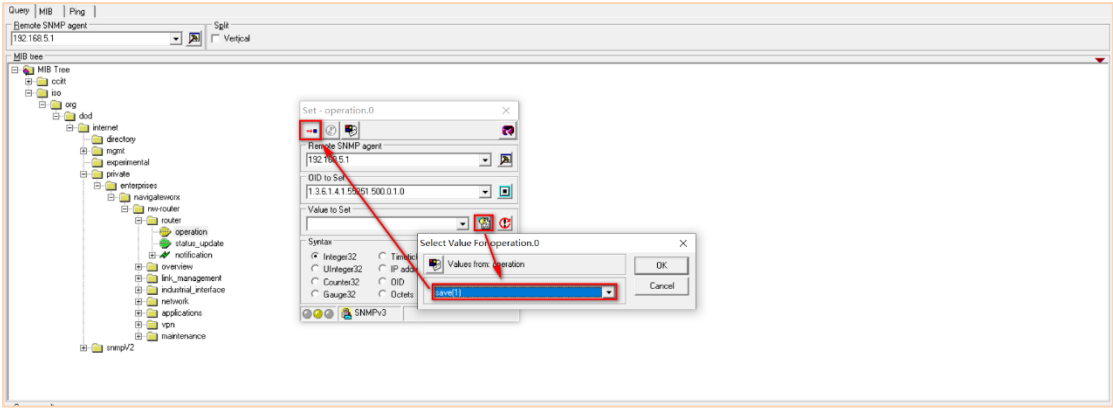


Step 2: Set the Telnet port to 24.

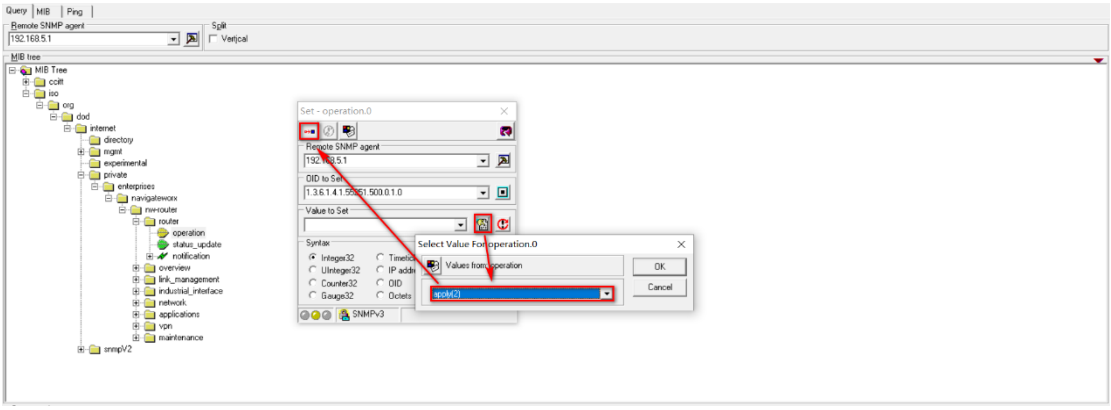


Step 3: After setting, the Port it needs to be saved. Go to "Save Operation" and save it:





Step 4: Now select "Apply":

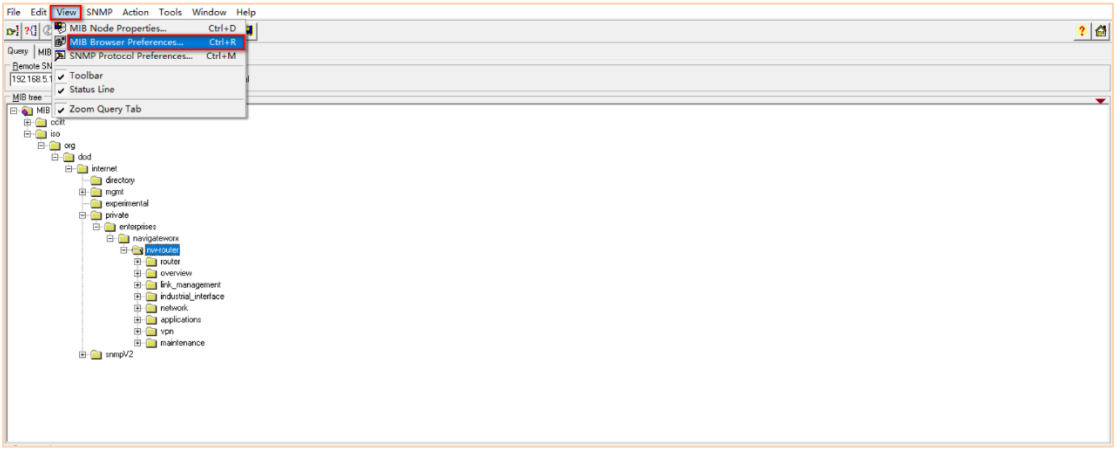


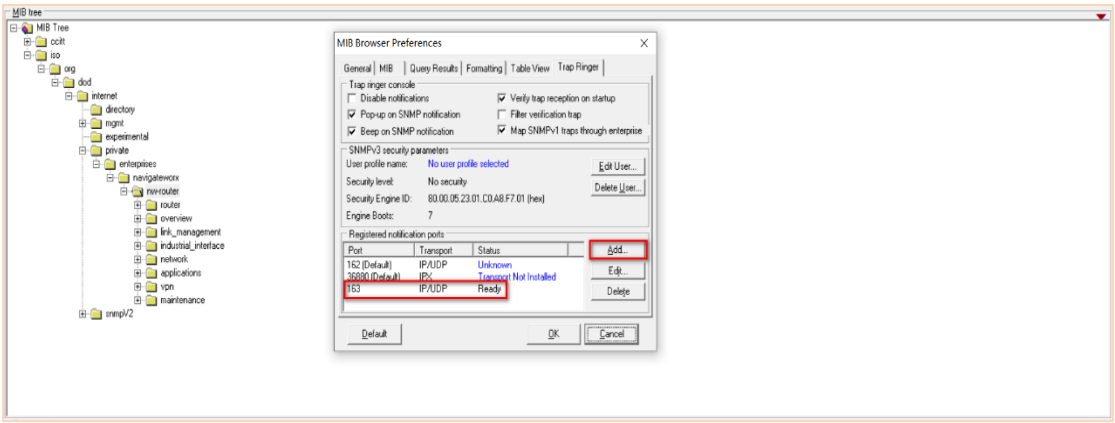
Step 5: Log in to the router and the Tenet Port had been changed to "24":

Step 6: The test is successful, now put Telnet port back to 23.

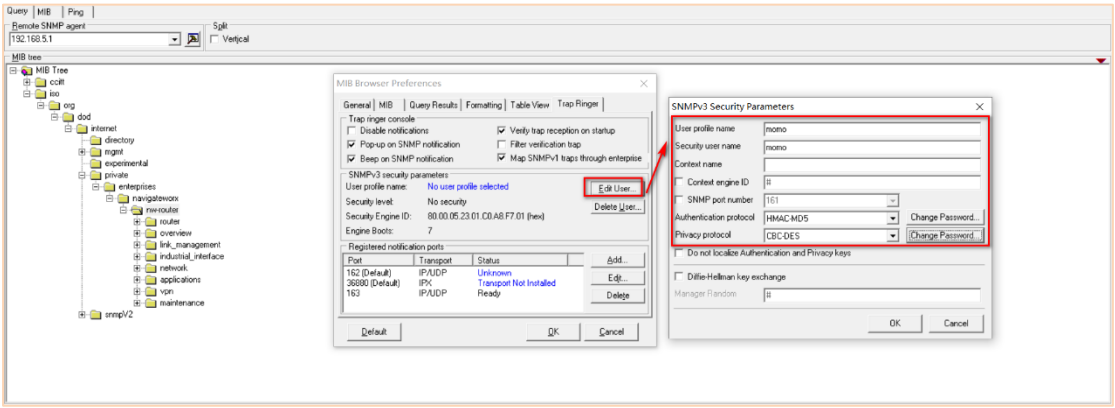
SNMP Trap Notification

For this SNMP Trap test we use UDP port 163, as shown below

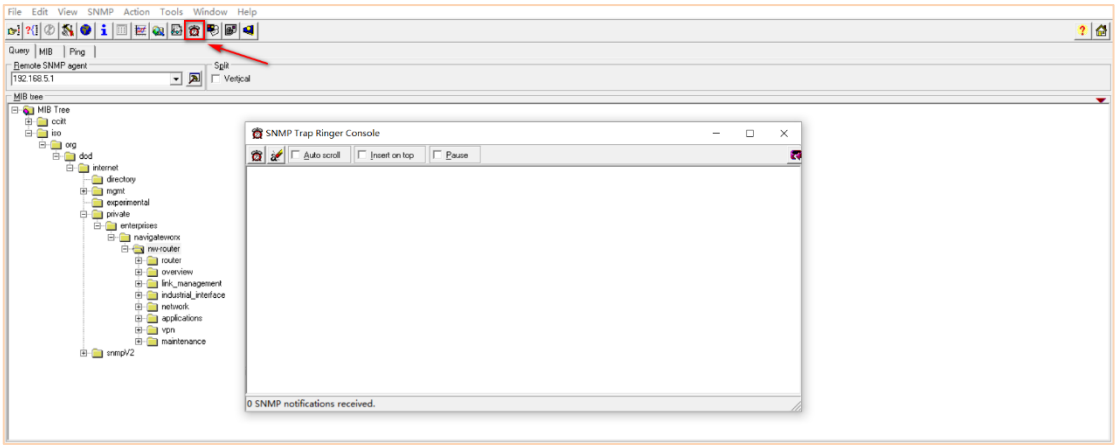




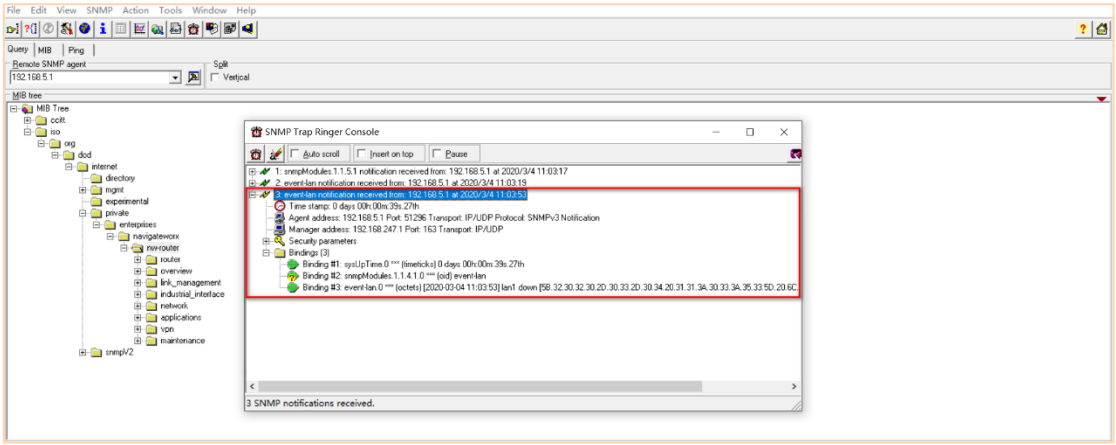
Add User and click “OK”:



Open the SNMP Trap Ringer Console:



Remove the Ethernet Cable from LAN port of the router, then receive the LAN Notification on SNMP Management tool:



Test successful.

24. TR069 management platform

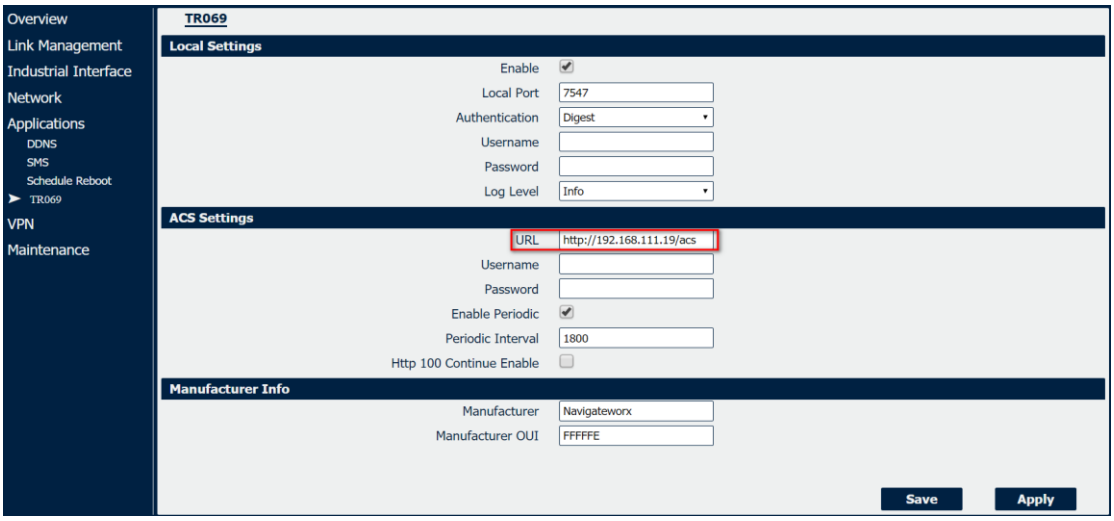
- The 6944 router connects to the TR069 management platform.
- The 6944 management platform can do the monitoring or control the router. For example, control the router restart, reset the router to factory default setting, upgrade the firmware/APPs/configuration, syslog upload, NTP configured, check the cellular, active link and NTP status.

*Note: This Application Note TR069 has been tested with the "**XACS**" TR069 management platform.*

Configuration

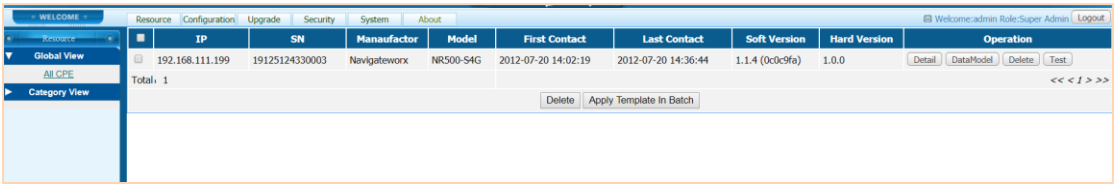
Configuration TR069 on the 6944

Step 1 Go to **Applications>TR069**, specify the settings to make the router connect to TR069 management platform:



Note: During the test without authentication on both the 6944 (CPE) and the TR069 Management Platform (XACS), there is no need to set the username and password.

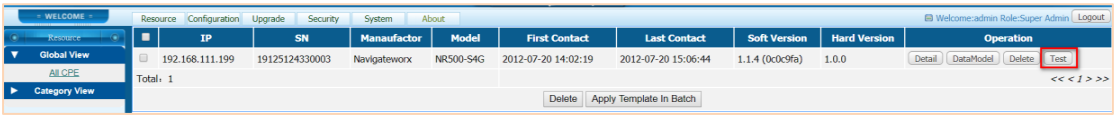
Step 2 Login to the XACS, on the homepage we can see the router has connected to the platform successfully:

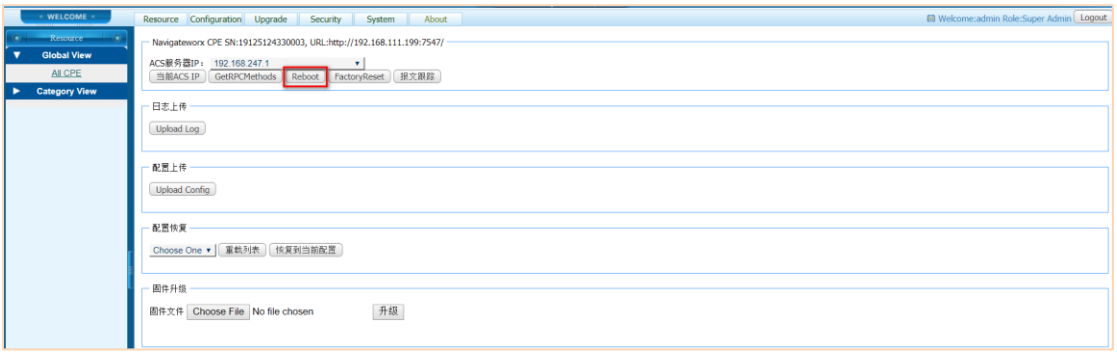


Control and Monitoring the 6944

Reboot

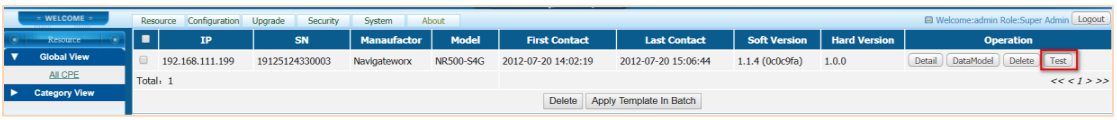
Login to the platform and go to **Resource>Test>Reboot**, the router will reboot when click the "Reboot" button:

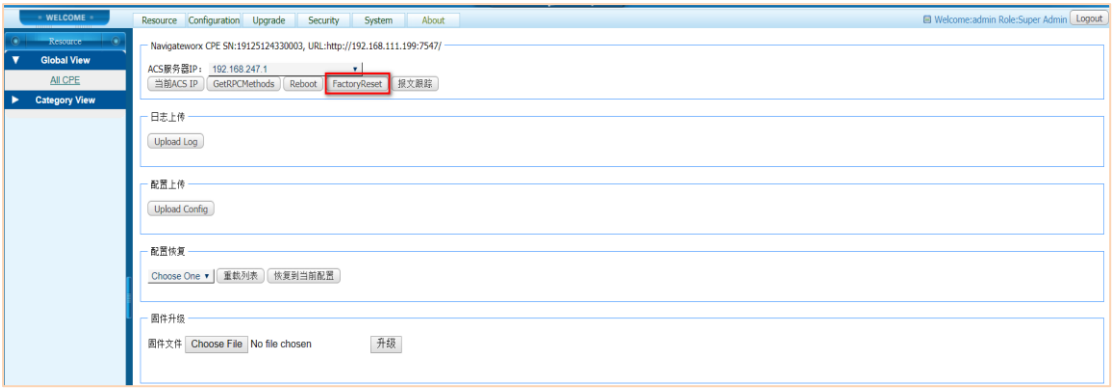




Factory Reset

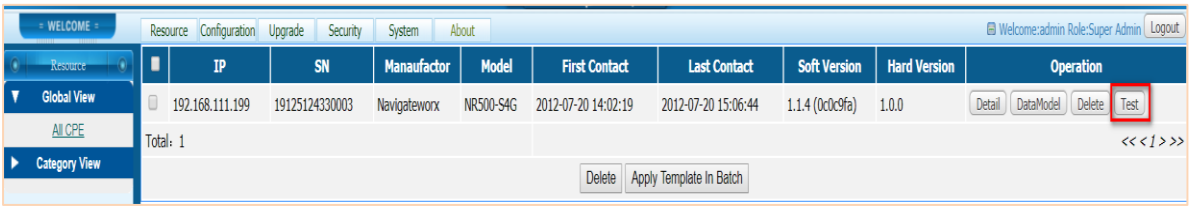
Login to the platform and go to **Resource>Test>FactoryReset**, the router will reset when click the "Factory Reset" button:





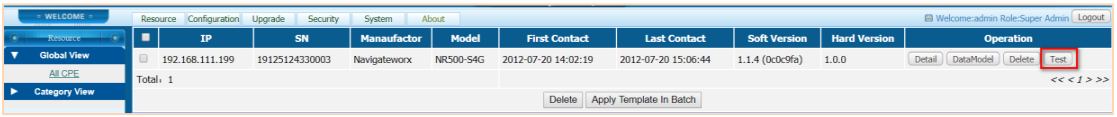
Syslog Upload

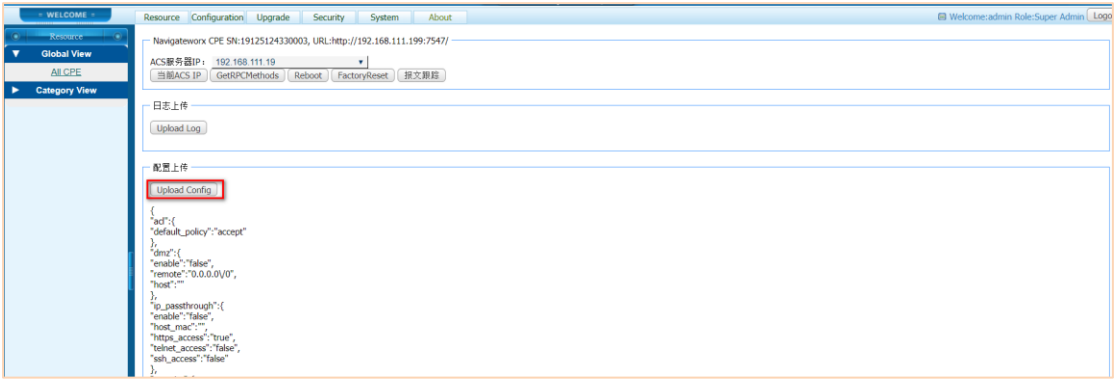
Login to the platform and go to **Resource>Test>Upload Log**, the router's syslog will display on the TR069 management platform:



Config Upload

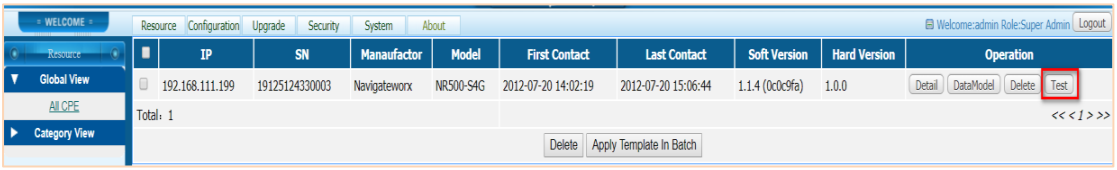
Login to the platform and go to **Resource>Test>Upload Config**, the router's config will display on the TR069 management platform:

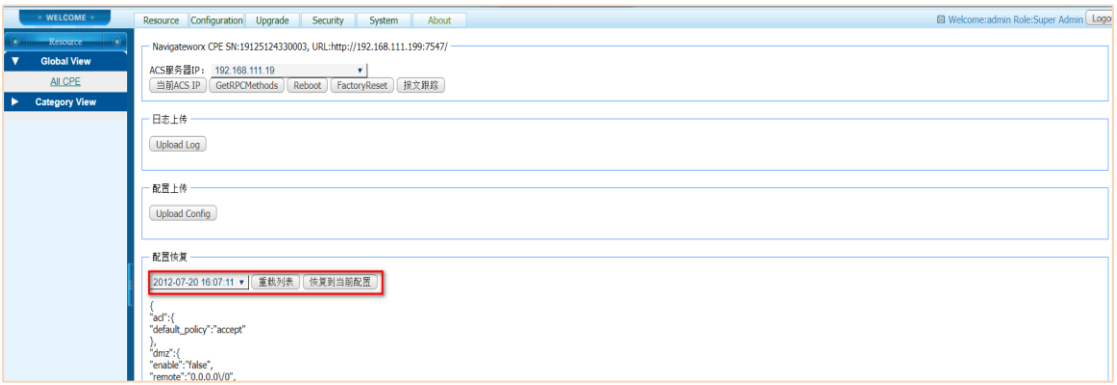




Config Update

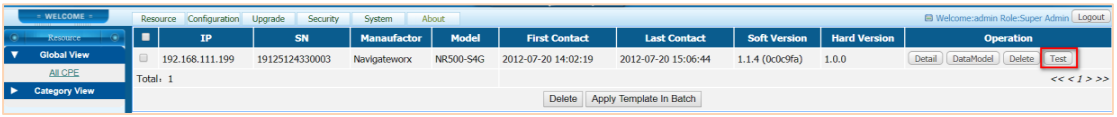
From the TR069 management platform, we can update the 6944 router. Follow the steps below and we can upload a configuration to the platform, or we can put the config file to the "uploads" installation folder, then go to **Resource>Test>Config Reset**, to download the configuration to the router:

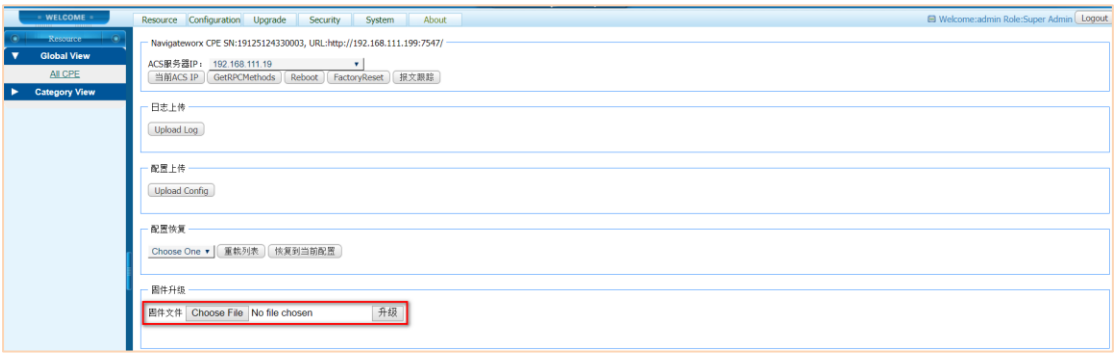




Firmware/APP Upgrade

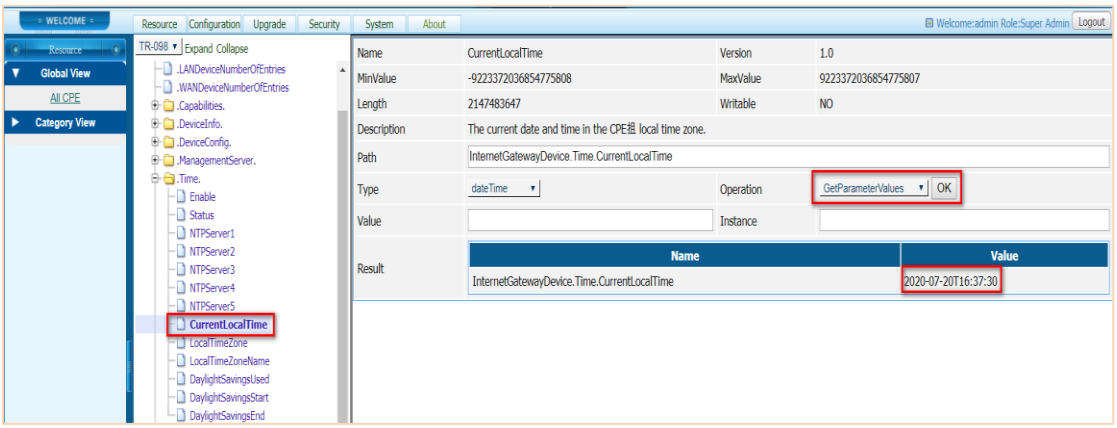
Login to the platform and go to **Resource>Test>Firmware Upgrade**, choose the firmware or APP file and upgrade to the router:



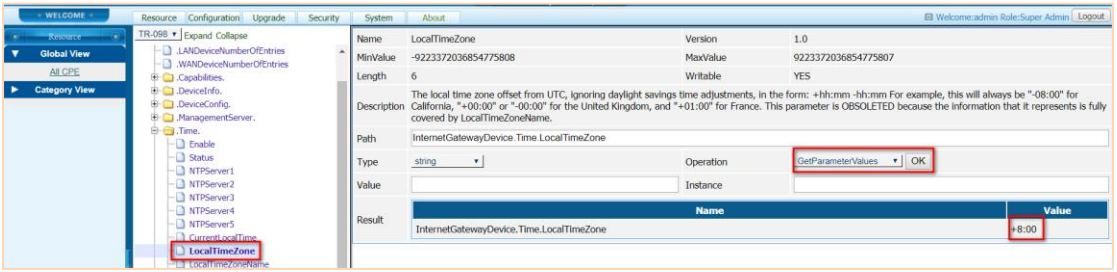


NTP Operation

Login to the platform and go to **Resource>DataModel>.Time**, we can configure NTP parameters and check the NTP status. Check the local time:

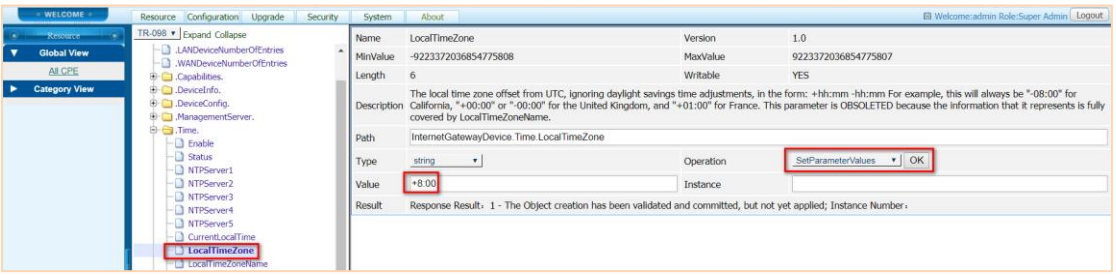


Check the time zone:



Specify the NTP server1 address:

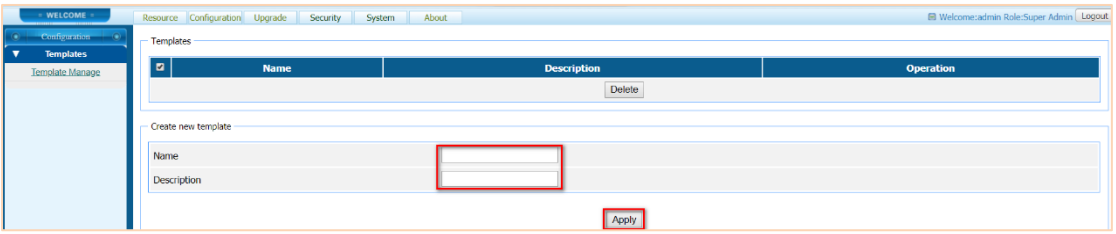
Specify the time zone:



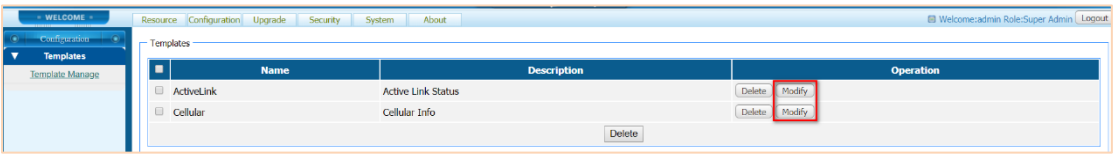
Active Link and Cellular Status

From the TR069 management platform we can check the active link and cellular status.

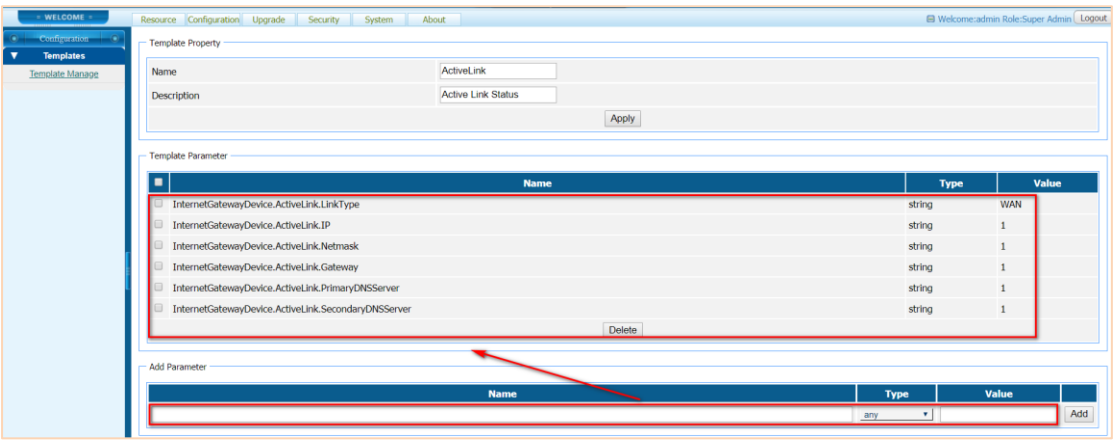
Step 1 Login to the platform and go to **Configuration>Create new template**, to create the template for active link and cellular:



Step 2 After that, add the template parameters for active link and cellular:

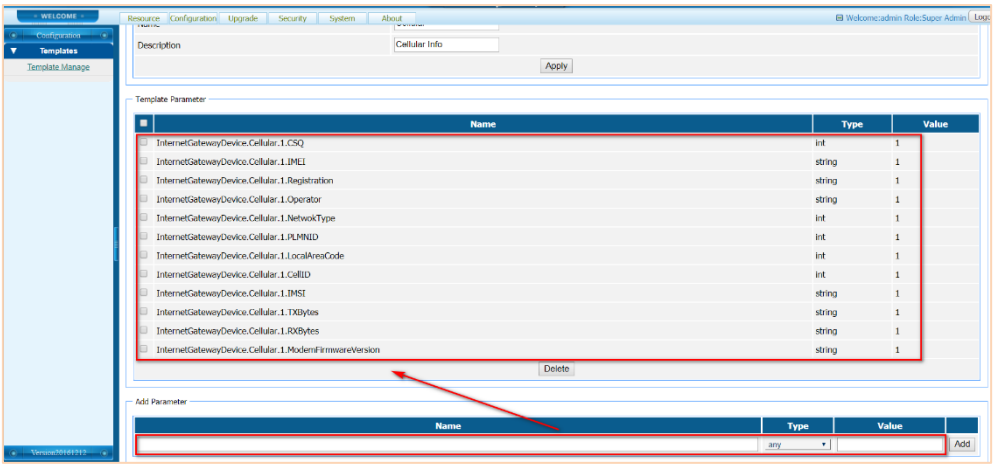


Step 3 Template Parameters for ActiveLink:



Name	Type	Value
InternetGatewayDevice.ActiveLink.LinkType	string	WAN
InternetGatewayDevice.ActiveLink.IP	string	1
InternetGatewayDevice.ActiveLink.Netmask	string	1
InternetGatewayDevice.ActiveLink.Gateway	string	1
InternetGatewayDevice.ActiveLink.PrimaryDNSServer	string	1
InternetGatewayDevice.ActiveLink.SecondaryDNSServer	string	1

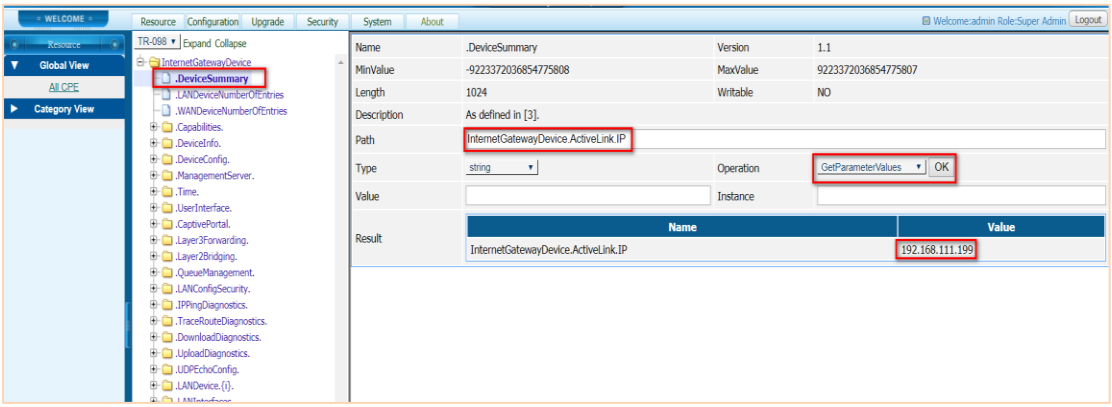
Step 4 Template Parameters for Cellular:



Name	Type	Value
InternetGatewayDevice.Cellular.1.CSQ	int	1
InternetGatewayDevice.Cellular.1.IMEI	string	1
InternetGatewayDevice.Cellular.1.Registration	string	1
InternetGatewayDevice.Cellular.1.Operator	string	1
InternetGatewayDevice.Cellular.1.NetwokType	int	1
InternetGatewayDevice.Cellular.1.PLMNID	int	1
InternetGatewayDevice.Cellular.1.LocalAreaCode	int	1
InternetGatewayDevice.Cellular.1.CellID	int	1
InternetGatewayDevice.Cellular.1.IMSI	string	1
InternetGatewayDevice.Cellular.1.TXBytes	string	1
InternetGatewayDevice.Cellular.1.RXBytes	string	1
InternetGatewayDevice.Cellular.1.ModemFirmwareVersion	string	1

Step 5 After creating the template, go to **Resource>DataModel,** click any one of the templates, and copy the Template Parameters to the "Path"

Step 6 Click "OK" then we can get the related value. Here we see the "IP address" as an example:



25. Maintenance

When newer versions of the 6944, firmware become available, the user can manually update the unit by uploading a software package to the unit.

NOTE: The unit needs to be manually rebooted once the upload completes, thus taking the 6944 out of service for approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.

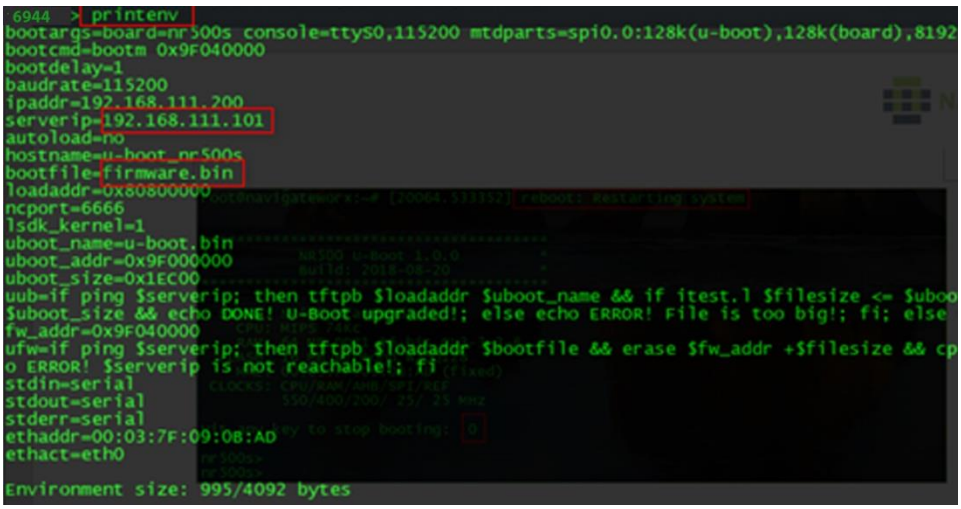
CAUTION: It is important to have a stable power source and ensure that power to the 6944 is not interrupted during a firmware upgrade.

25.1. Upgrade via Uboot

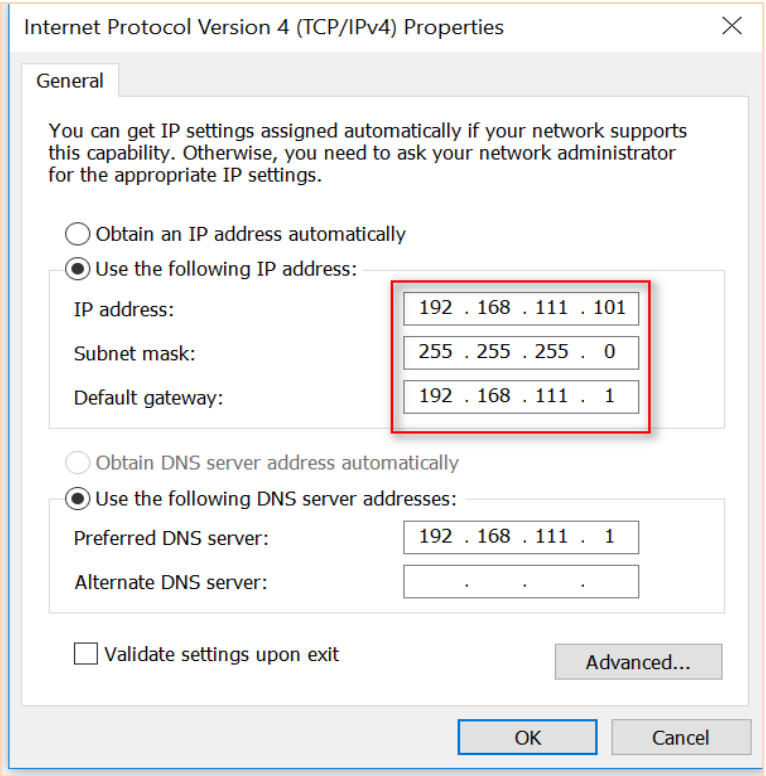
Step 1. Connected to the router with console cable, then reboot the router, when "booting" to "0", please hit any key on the keyboard to make the router go into u-boot mode.

```
************************************************************
                 6944  U-Boot 1.0.0.
              Build id: 2018 – 08 – 20
************************************************************

Board:      6944 Standard
CPU:        MIPS 74KC
RAM:        64MD DDR1  16-Bit CL3-3-3-8
FLASH:      16MB Winbon w2SQ128
MAC:        00:03:7F:09:08:AD (Fixed)
Clocks:      CPU / RAM/AMB/ SPI/REF
            550 / 400 / 200 / 25 / 25Mhz
Hit any key to stop booting    0
```

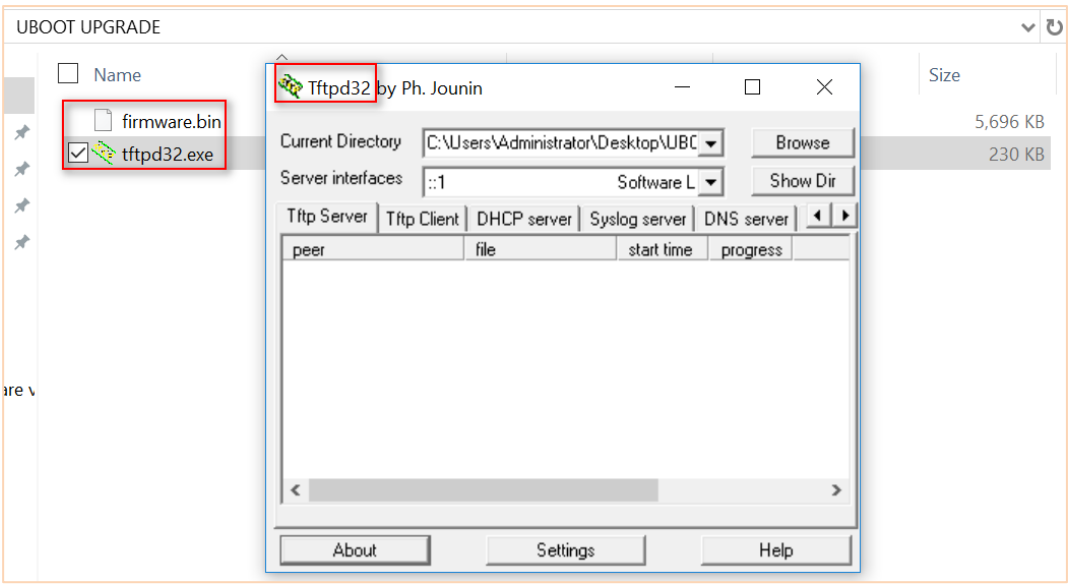
Step 2 Run the command "**printenv**" to check the info and setup the server IP on the PC accordingly.



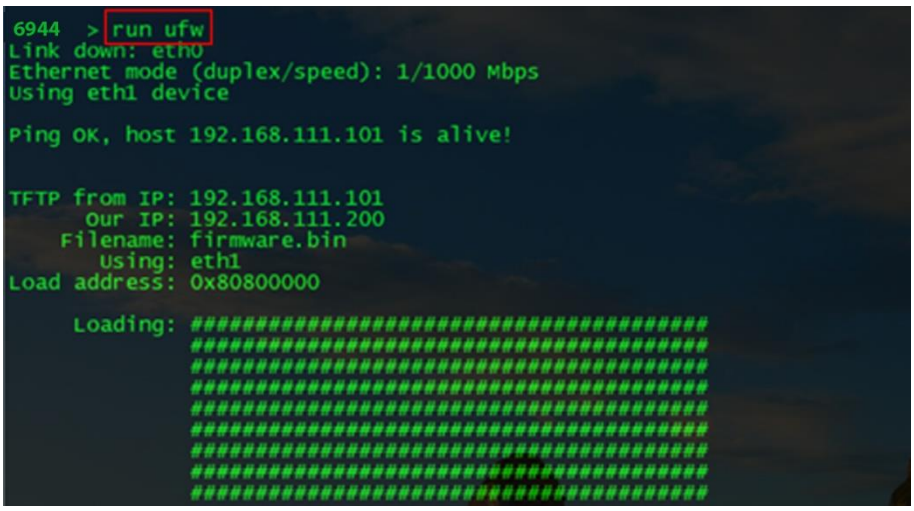
Step 3 Set a correct IP address on your PC:



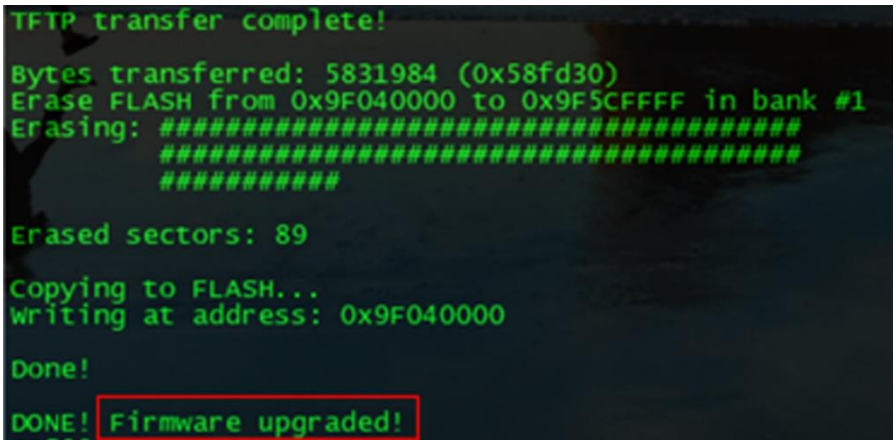
Step 4 Put the firmware and TFTP software in the same folder, and rename the firmware as "**firmware.bin**", then run the TFTP software.



Step 5 Run the command "**run ufw**" to start the firmware upgrade.



Step 6 Check firmware upgraded successfully



25.2. Scheduled Reboot

Run the command "**reset**" to reboot the router.

Case Communications Ltd

Unit 12E Norths Estate

Old Oxford Road

Piddington

High Wycombe

Bucks HP14 3BE

+44 (0) 1494 880 240

www.casecomms.com

admin@case.uk.com