

Case Communications

6944 Industrial Router

Manual



Revision V2.6

This page left blank intentionally

REVISION HISTORY

Trademarks and copyright 

Manual Revision	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

Case Communications Ltd and logo are the trademarks or registered trademarks in the United Kingdom. All other trademarks mentioned in this document are the property of their respective owners.
 ©2019 Case Communications Ltd. All Rights Reserved.

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@casecomms.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

1	PRODUCT OVERVIEW.....	1
	1.1. Overview	1
	1.2. Features and Benefits	1
	1.3. General Specifications	2
	1.4. Mechanical Specifications	4
	1.5. Package Checklist	4
2	INSTALLATION.....	6
	2.1. Product Overview	6
	2.2. LED Indicators	7
	2.3. Ethernet Port Indicator	7
	2.4. PIN Definition of Terminal blocks	7
	2.5. Reset Button	8
	2.6. Insert SIM card	8
	2.7. Install Antenna	9
	2.8. DIN-Rail Mounting	10
	2.9. Protective Grounding Installation	10
	2.10. Power Supply Installation	11
	2.11. Powering On The 6944 Router	11
3	ACCESSING THE WEB CONFIGURATION PAGE.....	12
	3.1. PC Configuration	12
	3.2. Factory Default Settings	13
	3.3. Logging in to the 6944 Web Page	14
4	BROWSER CONFIGURATION.....	15
	4.1. Web Interface Overview	15
	4.1.1. Status	16
	4.1.2. Syslog	17
	4.2. Link Management	18
	4.3. Connection Manager	18
	4.3.1. Cellular	20
	4.3.2. Ethernet	22
	4.3.3. Wi-Fi	28
	4.3.4. Wi-Fi AP	29
	4.3.5. Wi-Fi Client	30
	4.4. Industrial Interface	32
	4.4.1. Serial	32
	4.4.2. Digital IO	34
	4.5. Network Configuration	37
	4.5.1. Firewall and ACL	37
	4.6. Routing	40
	4.7. V.R.R.P	47
	4.8. IP Passthrough	48

4.9.	VPN (Virtual Private Networks)	49
4.9.1.	OpenVPN	49
4.9.2.	Testing OpenVPN between a PC and the 6944	53
4.9.3.	IPSec	56
4.9.4.	GRE	59
4.10.1.	CLI reference commands	60
4.10.2.	How to Configure the CLI	61
4.11.	SNMP	62
4.11.1.	Overview	62
4.11.2.	Topology	62
4.11.3.	Configuring the 6944 Router	62
4.11.4.	Testing	64
4.11.5.	Controlling the 6944 Router	64
4.11.6.	Receiving SNMP Traps	66
5	Digital I / O Ports.....	68
5.1.	Digital Input	68
5.2	Digital Output.....	68
6	MODBUS Slave.....	69
6.1	Overview	69
6.2	Topology	69
6.3	Digital Input - Output Register Table	70
6.4	Configuration	71
6.5	Testing	71
7	MODBUS Master.....	73
7.1.	Introduction	73
7.2.	Topology	73
7.3.	Transport via TCP	74
7.3.1.	Configuration on Modbus Slave	74
7.3.2.	Configuration of the Modbus Poll	74
7.4.	Configuring Modbus Transport	75
7.5.	Transport via FTP	77
7.6.	Transport via MQTT	79
8.	MAINTENANCE.....	82
8.1.	Upgrading Software	82
8.2.	System Settings	83
8.3.	Configuration	86
8.4.	Debug Tools	88
	Appendix A -Glossary	89
	Appendix B -Problem Solving	90

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

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

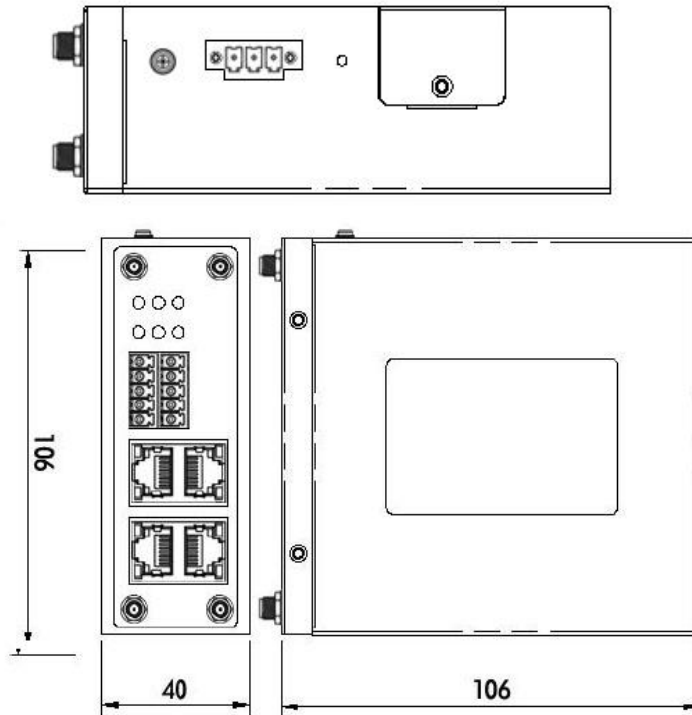
- Ingress Protection: IP30
- Housing & Weight: Metal, 300g
- Dimension: 104mm x 104mm x 38mm (excluding antenna)
- Installations: Din-rail mounting

Environmental

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

1.4. Mechanical Specifications

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



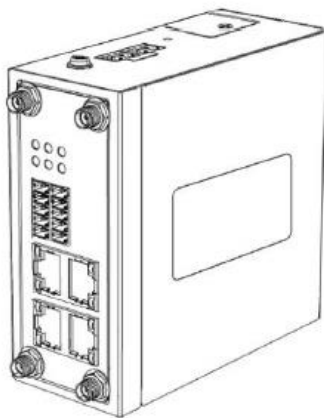
1.5. Package Checklist

The 6944 series Router includes the parts shown in below, please verify your components.

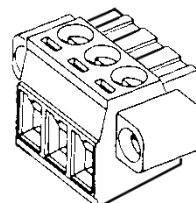
NOTE: if any of the below items is missing or damaged, please contact your sales representative.

Included equipment

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

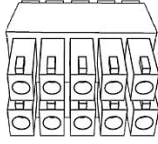


- 1 x 10-pin 3.5 mm male terminal block for RS232/RS485/DI/DO



1. PRODUCT OVERVIEW

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



- 1 x Ethernet cable



- 1 x Quick Start Guide



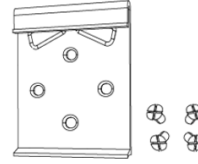
Optional Accessories (sold separately)

- 3G/4G cellular antenna

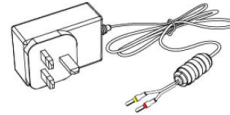
Stubby antenna



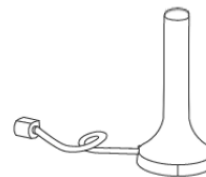
- 35mm Din-rail mounting kit



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



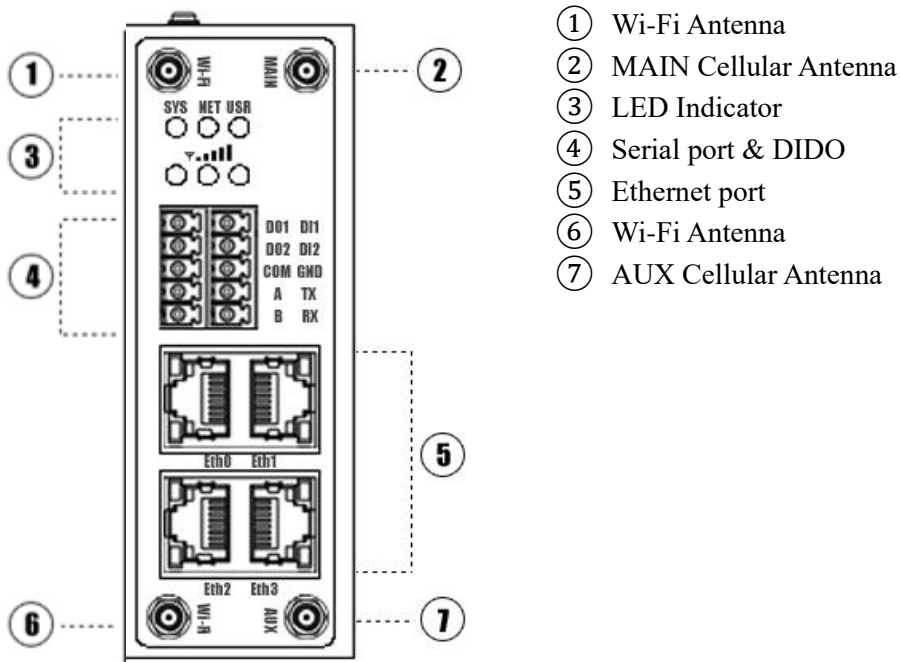
Magnet antenna



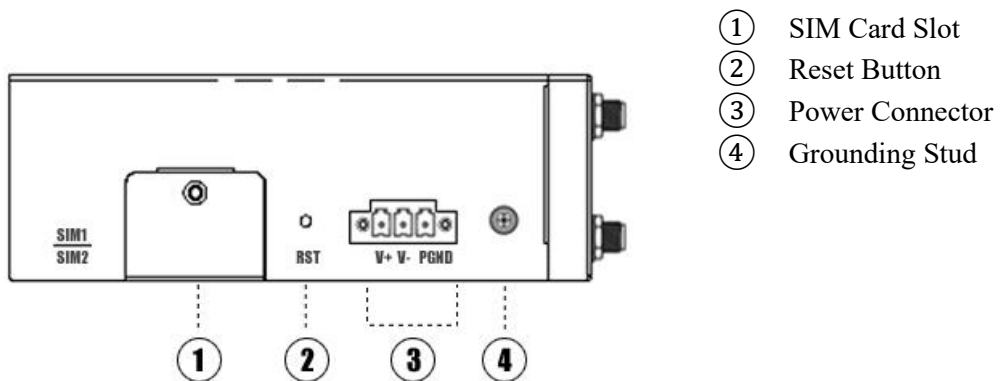
2 INSTALLATION

2.1. Product Overview


• **Front Panel**



• **Left Side Panel**



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

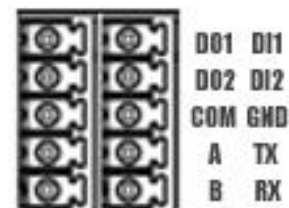
2.3. Ethernet Port Indicator

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. PIN Definition of Terminal blocks

- 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

- **Power Input**



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

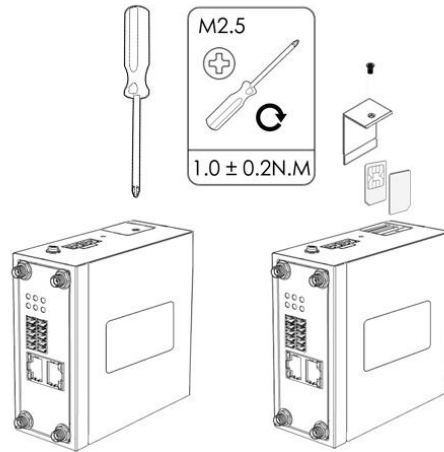
2.5. Reset Button

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

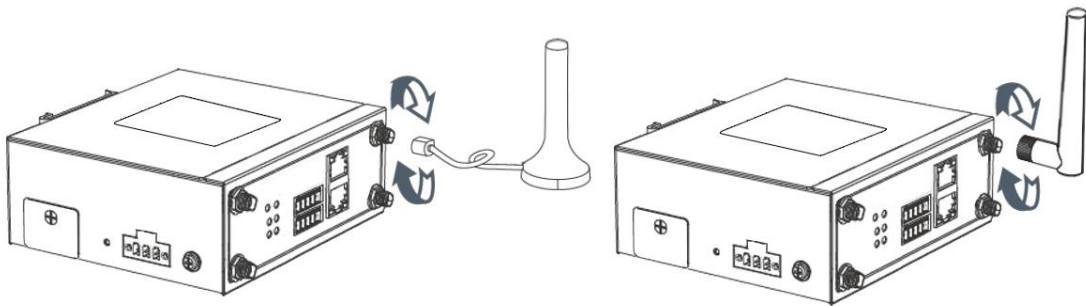
- **Insert / Remove SIM card**

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.



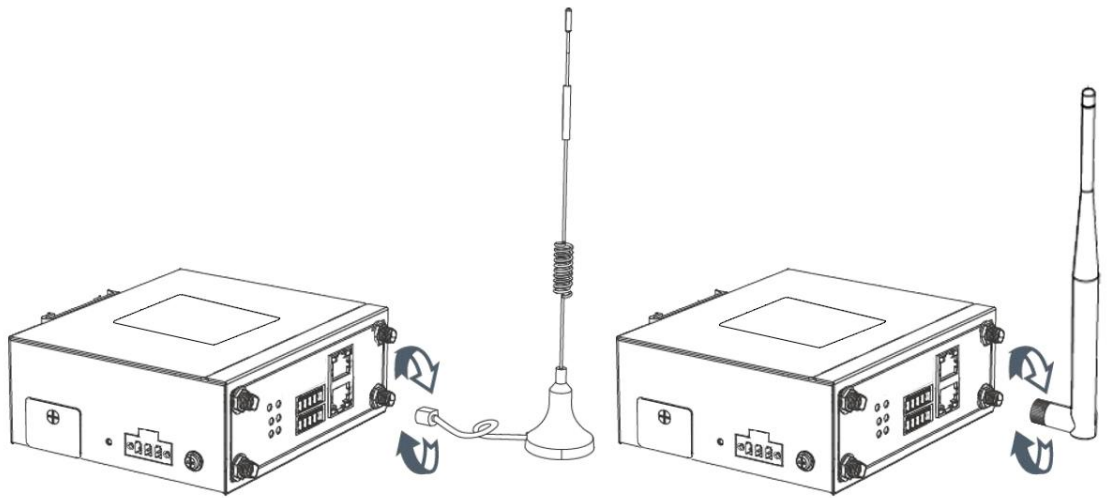
2.7. Install Antenna

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



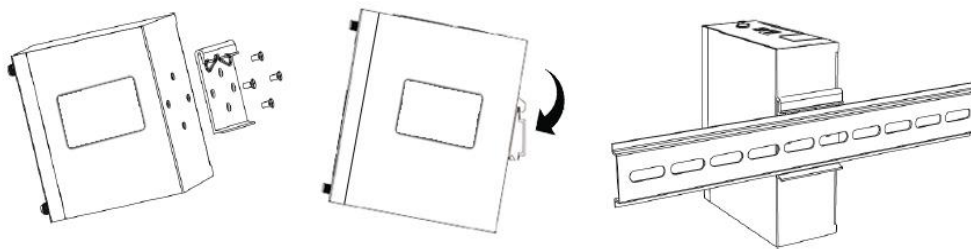
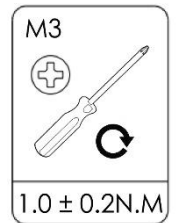
NOTE: The 6944 router supports dual antennas with MAIN and AUX connectors. The MAIN connector is for receiving and transmitting data. The AUX connector is for enhancing signal strength, and should be used with the MAIN Antenna.

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



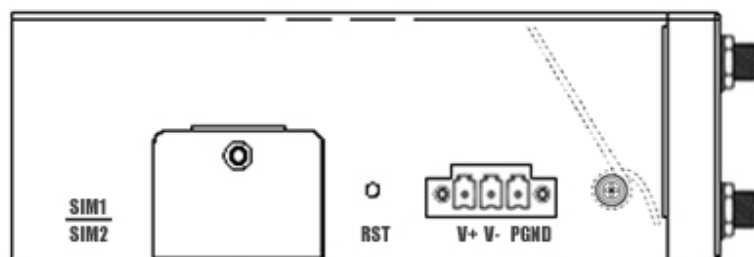
2.8. DIN-Rail Mounting

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

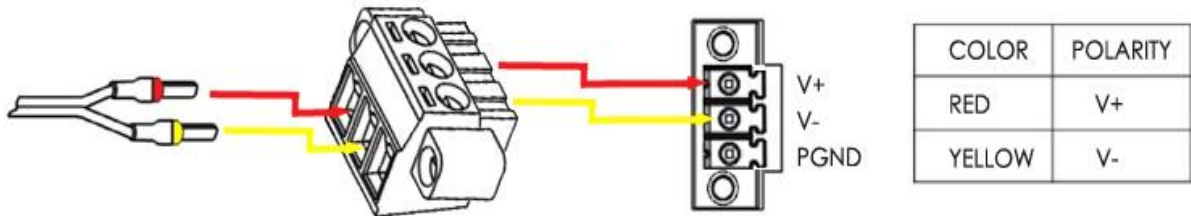
1. Remove the grounding nut.
2. Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.



NOTE: Strongly recommended the router to be grounded when deployed.

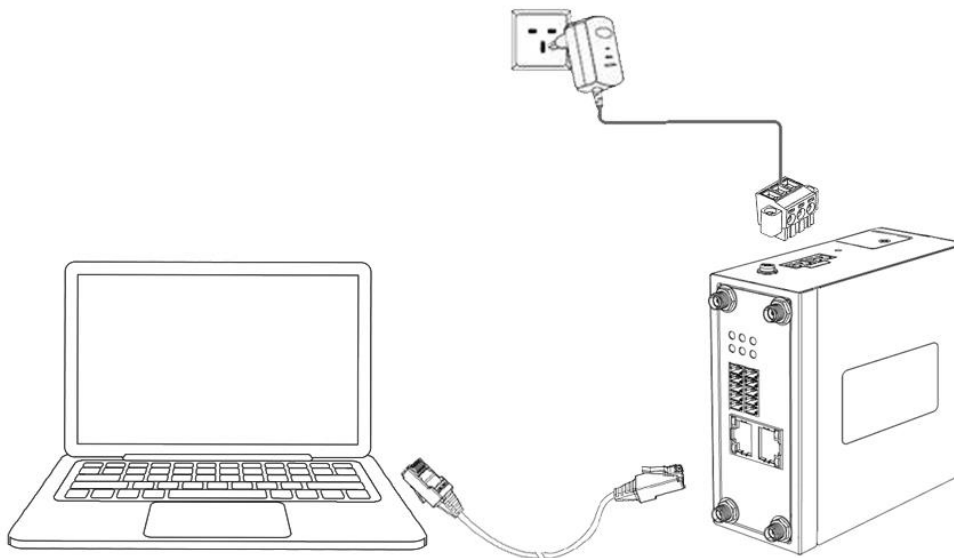
2.10. Power Supply Installation

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.



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.



3 ACCESSING THE WEB CONFIGURATION PAGE

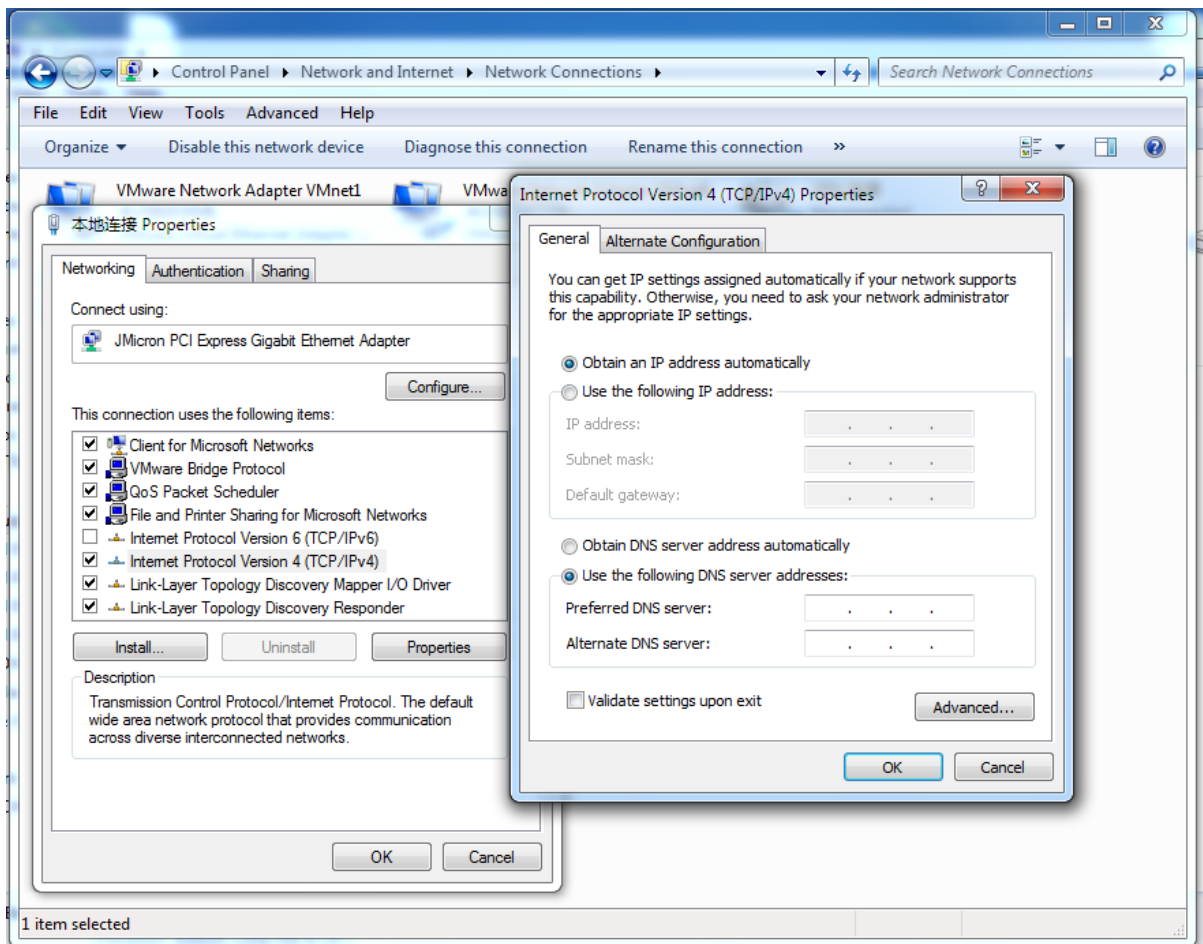
3.1. PC Configuration

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**

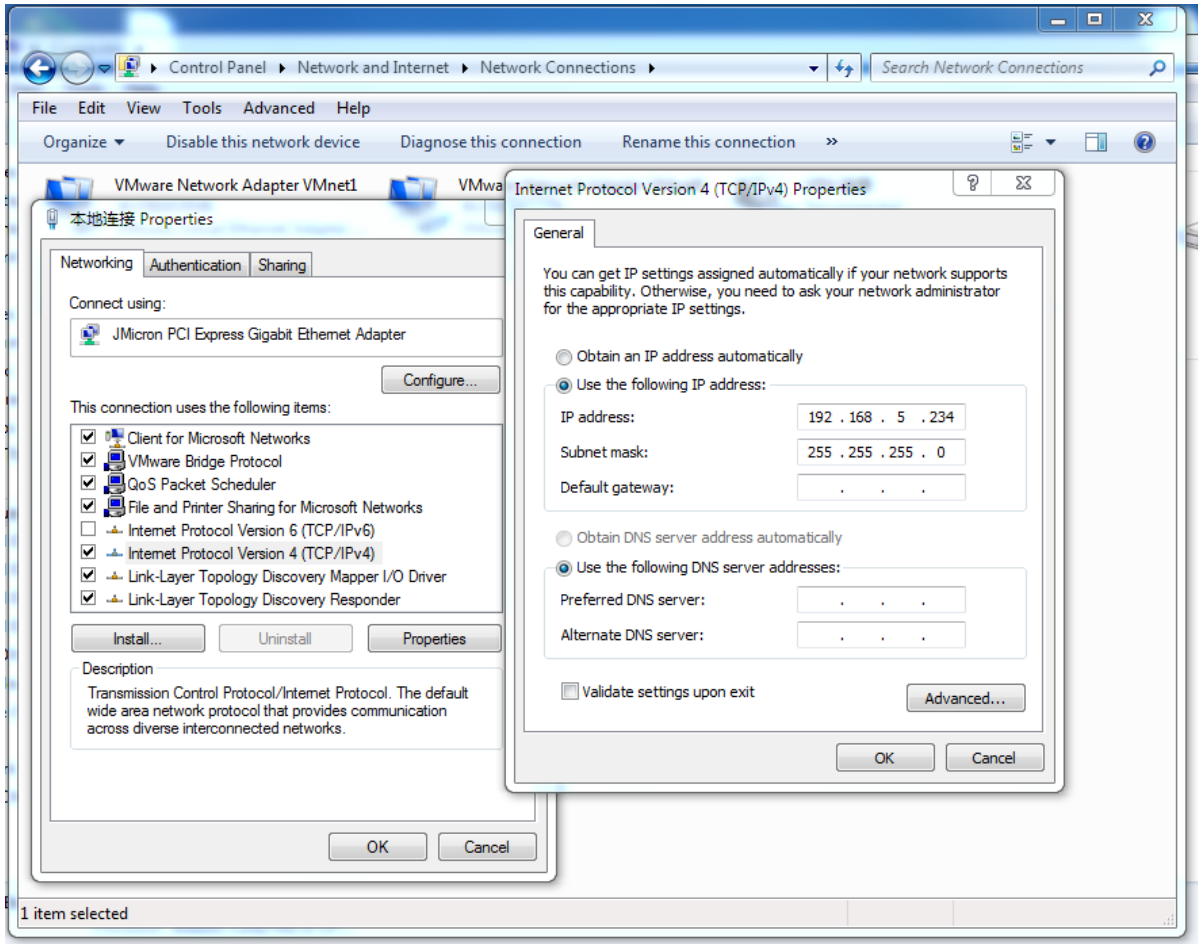
The process required to do this differs depending on the version of Windows you are using.

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 following IP address**" to assign a static IP manually within the same subnet of the router.

NOTE: *Default gateway* and *DNS server* is not necessary if 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**

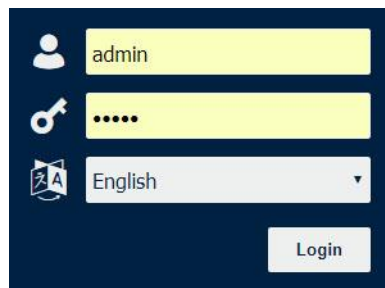
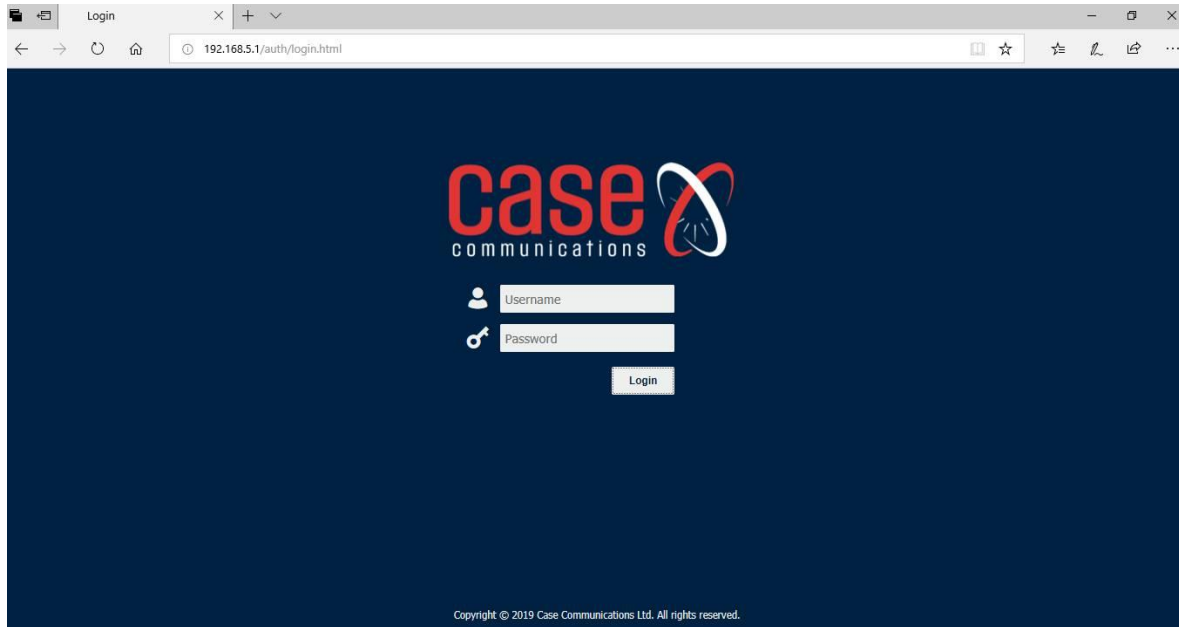
Password: **admin**

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

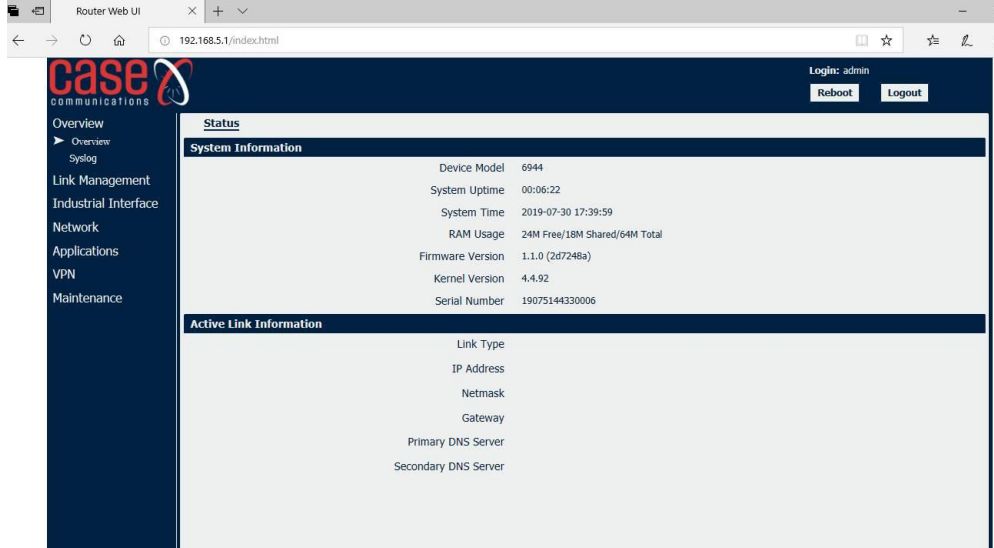
1. Start a Web browser on your PC (Chrome and IE are recommended), enter 192.168.5.1 into the address bar of the web browser.
2. Then use the default username and password(admin/admin), to log in to the router.



4 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.

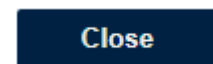
- **Reboot:** reset the router within power disconnect.
- **Logout:** logout to web authorization page.



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



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



4.1.1. Status

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

<u>Status</u>	
System Information	
Device Model	6944
System Uptime	00:01:48
System Time	2019-06-03 17:24:09
RAM Usage	24M Free/18M Shared/64M Total
Firmware Version	1.1.0 (278c6c6)
Kernel Version	4.4.92
Serial Number	18105144330005

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	WAN
IP Address	192.168.111.33
Netmask	255.255.255.0
Gateway	192.168.111.1
Primary DNS Server	192.168.129.1
Secondary DNS Server	192.168.111.1

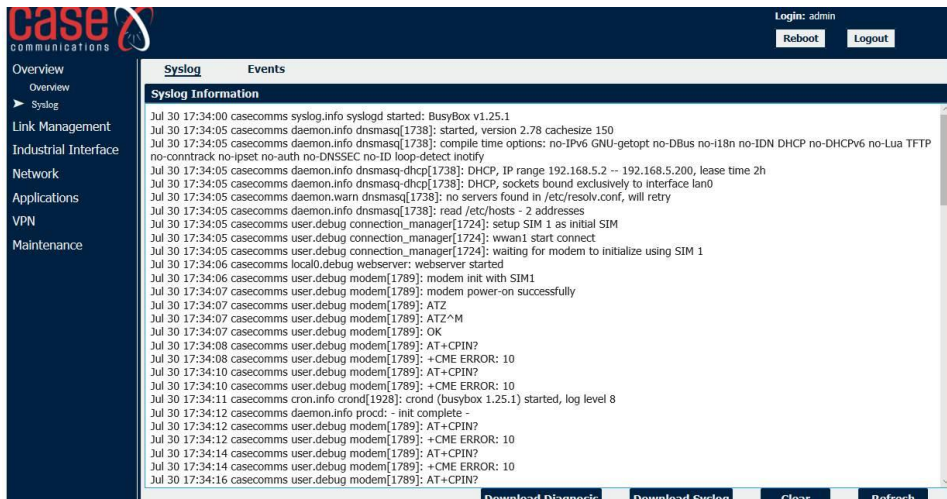
Active Link Information

- **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.

4.1.2. 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.



The screenshot shows the Case Communications web interface. The top navigation bar includes 'Login: admin', 'Reboot', and 'Logout'. The left sidebar contains menu items: Overview, Syslog, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance. The main content area is titled 'Syslog Information' and displays a list of system logs. The logs include timestamps and messages such as 'BusyBox v1.25.1', 'dnsmasq started', 'DHCP, IP range 192.168.5.2 -- 192.168.5.200', and 'modem power-on successfully'. At the bottom of the log list, there are four buttons: 'Download Diagnosis', 'Download Syslog', 'Clear', and 'Refresh'.

4.2. 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.

4.3. Connection Manager

Status		Connection	
General Settings			
Priority	Enable	Connection Type	Description
1	true	WWAN1	
2	true	WAN	

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 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.

4.3.1. Cellular

The 6944 Router main function is connecting to Internet by cellular modem.

Status		Cellular							
Cellular Information									
Index	Modem	Registration	CSQ	Operator	Network Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	31 (-51dBm)	vodafone	LTE	861107038049871	460015956236598	2992	2748
Index 1 Modem EC25 Registration Registered CSQ 31 (-51dBm) Operator vodafone Network Type LTE IMEI 861107038049871 PLMN ID 46001 Local Area Code 2508 Cell ID 6016CD2 IMSI 460015956236598 TX Bytes 2992 RX Bytes 2748 Modem Firmware EC25EFAR06A01NHG									

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.

Status		Cellular	
Modem General Settings			
Index	SIM Card	Auto APN	
1	SIM1	true	<input checked="" type="checkbox"/>
2	SIM2	true	<input checked="" type="checkbox"/>

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 Code** - 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.
- **Monthly Billing Day** - Enter the date of renew data amount every month.
- **Data Roaming** - Enable or disable the data roaming function on the router.
- **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.
- **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.

SIM Card Settings

Modem General Settings

Index	<input type="text" value="1"/>
SIM Card	<input type="text" value="SIM1"/>
Auto APN	<input checked="" type="checkbox"/>
Dial Number	<input type="text" value="*99#"/>
Authentication Type	<input type="text" value="Auto"/>
PIN Code	<input type="text" value=""/>
Monthly Data Limitation	<input type="text" value="0"/>
Monthly Billing Day	<input type="text" value="1"/>
Data Roaming	<input checked="" type="checkbox"/>
Override Primary DNS	<input type="text" value=""/>
Override Secondary DNS	<input type="text" value=""/>

Modem Network Settings

Network Type	<input type="text" value="Auto"/>
Use All Bands	<input checked="" type="checkbox"/>

4.3.2. Ethernet

The same instructions apply to settings for all Ethernet interfaces.

Status	Port Assignment	WAN	LAN	VLAN
Ethernet Port Information				
Index	Name	Status		
1	ETH0	Up		
2	ETH1	Up		
3	ETH2	Up		
4	ETH3	Up		
Interface Information				
Index	Name	MAC Address		
1	wan			
2	lan0	A8:3F:A1:E0:A2:FA		
DHCP Lease Table				
Index	MAC Address	IP Address	Lease Expires	Hostname
1	30:59:b7:16:3b:66	192.168.111.40	2019-06-05 16:01:58	KEN-COMPUTER

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**
Displays the current IP address assigned to DHCP client.

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

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.

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

Status	Port Assignment	<u>WAN</u>	LAN	VLAN
General Settings				
		Connection Type	Static IP <input type="text"/>	
		IP Address	<input type="text"/>	
		Netmask	<input type="text"/>	
		Gateway	<input type="text"/>	
		Primary DNS	<input type="text"/>	
		Secondary DNS	<input type="text"/>	

Status	Port Assignment	<u>WAN</u>	LAN	VLAN
General Settings				
		Connection Type	PPPoE <input type="text"/>	
		Authentication Type	Auto <input type="text"/>	
		Username	<input type="text"/>	
		Password	<input type="text"/>	

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.

Status	Port Assignment	WAN	<u>LAN</u>	VLAN
General Settings				
Index	Interface	IP Address	Netmask	+
1	LAN0	192.168.5.1	255.255.255.0	✎ ✕
Multiple IP Settings				
Index	Interface	IP Address	Netmask	+

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.

LAN Settings	
General Settings	
Index	<input type="text" value="1"/>
Interface	<input type="text" value="LAN0"/>
IP Address	<input type="text" value="192.168.5.1"/>
Netmask	<input type="text" value="255.255.255.0"/>
MTU	<input type="text" value="1500"/>
DHCP Settings	
Enable	<input checked="" type="checkbox"/>
Mode	<input type="text" value="Server"/>
IP Pool Start	<input type="text" value="192.168.5.2"/>
IP Pool End	<input type="text" value="192.168.5.200"/>
Netmask	<input type="text" value="255.255.255.0"/>
Lease Time	<input type="text" value="120"/>
Gateway	<input type="text"/>
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
WINS Server	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

DHCP Settings	
Enable	<input checked="" type="checkbox"/>
Mode	<input type="text" value="Relay"/>
Relay Server	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

Ethernet->LAN

- **Interface**
Select the configure 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.

Ethernet->LAN->Multiple IP Settings

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

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.

4.3.3. Wi-Fi

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 navigation menu to Wi-Fi (default as Access Point) page, which contains tabs for configuration of the Wi-Fi Access Point interface.

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

Status	Basic	WiFi AP	
WiFi Status			
Status	Ready		
SSID	6944 WAN		
MAC Address	a8:3f:a1:e0:ab:81		
Current Channel	6		
Channel Width	40 MHz		
TX Power	20.00 dBm		
Associated Station			
Index	MAC Address	Signal	Station Name
1	30:59:b7:16:3b:66	-55 dBm	KEN-COMPUTER
2	98:10:e8:67:dd:35	-64 dBm	iPhone

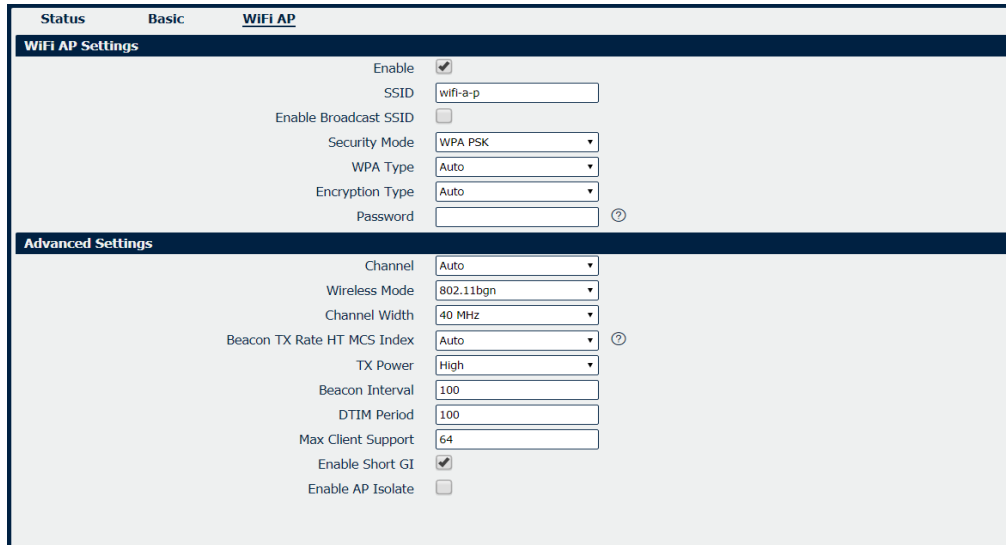
Status	Basic	WiFi AP
Basic Settings		
Running Mode	<input type="text" value="AP"/>	
Country Code	<input type="text" value="UK"/>	

Wi-Fi->Basic

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

4.3.4. Wi-Fi AP

Wi-Fi AP settings page as below.



Wi-Fi->Wi-Fi AP

- **Enable**
Check this box will 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 can't not 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 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.

4.3.5. Wi-Fi Client

Wi-Fi Client settings page as below.

Status	Basic	WiFi Client
WiFi Client Settings		
	Enable	<input checked="" type="checkbox"/>
	Connect to Hidden SSID	<input type="checkbox"/>
	SSID	<input type="text"/>
	Password	<input type="text"/>
IP Address Settings		
	Connection Type	<input type="text" value="DHCP"/>

Wi-Fi->Wi-Fi Client

- **Enable**
Check this box will enable the Wireless interface.
- **Connect to Hidden SSID**
Check this box will enable connect to hidden SSID.
- **SSID**
The SSID of the external access point.
- **Password**
Enter the password of 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 will override the automatically obtained DNS.
- **Secondary DNS**
Enter the secondary DNS server will override the automatically obtained DNS.

Status	Basic	WiFi Client
WiFi Client Settings		
Enable	<input checked="" type="checkbox"/>	
Connect to Hidden SSID	<input type="checkbox"/>	
SSID	<input type="text"/>	
Password	<input type="text"/>	
IP Address Settings		
Connection Type	Static IP	▼
IP Address	<input type="text"/>	
Netmask	<input type="text"/>	
Gateway	<input type="text"/>	
Primary DNS	<input type="text"/>	
Secondary DNS	<input type="text"/>	

4.4. Industrial Interface

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.

4.4.1. Serial

You could review the status of serial connection.

Status		Connection			
Serial Information					
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.

Status		Connection					
Serial Connection Settings							
Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity	
1	false	COM1	115200	8	1	None	<input checked="" type="checkbox"/>
2	false	COM2	115200	8	1	None	<input checked="" type="checkbox"/>

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.

Connection Settings

Serial Connection Settings

Index	<input type="text" value="1"/>
Enable	<input type="checkbox"/>
Port	<input type="text" value="COM1"/>
Baud Rate	<input type="text" value="115200"/>
Data Bits	<input type="text" value="8"/>
Stop Bits	<input type="text" value="1"/>
Parity	<input type="text" value="None"/>

Transmission Settings

Transmission Method	<input type="text" value="Transparent"/>
MTU	<input type="text" value="1024"/> ?
Protocol	<input type="text" value="TCP Client"/>
Remote IP Address	<input type="text"/>
Remote Port	<input type="text" value="2000"/>

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.

Transmission Settings

Transmission Method	<input type="text" value="Transparent"/>
MTU	<input type="text" value="1024"/> ?
Protocol	<input type="text" value="TCP Server"/>
Local IP Address	<input type="text"/>
Local Port	<input type="text" value="2000"/>

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.

Transmission Settings

Transmission Method	<input type="text" value="Transparent"/>	▼	
MTU	<input type="text" value="1024"/>		?
Protocol	<input type="text" value="UDP"/>	▼	
Local IP Address	<input type="text"/>		
Local Port	<input type="text" value="2000"/>		
Remote IP Address	<input type="text"/>		
Remote Port	<input type="text" value="2000"/>		

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.
- **Remote IP Address**
Enter the IP address of the remote server.
- **Remote Port**
Enter the port number of the remote server.

4.4.2. 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 Input

Digital Input Settings

Index	<input style="width: 90%;" type="text" value="1"/>	
Enable	<input type="checkbox"/>	
Alarm ON Mode	<input style="width: 90%;" type="text" value="Low"/>	
Alarm ON Content	<input style="width: 90%;" type="text"/>	
Alarm OFF Content	<input style="width: 90%;" type="text"/>	

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 Output

Digital Output Settings

Index	<input style="width: 90%;" type="text" value="1"/>	
Enable	<input type="checkbox"/>	
Alarm Source	<input style="width: 90%;" type="text" value="Digital Input 1"/>	
Alarm ON Action	<input style="width: 90%;" type="text" value="High"/>	
Alarm OFF Action	<input style="width: 90%;" type="text" value="Low"/>	

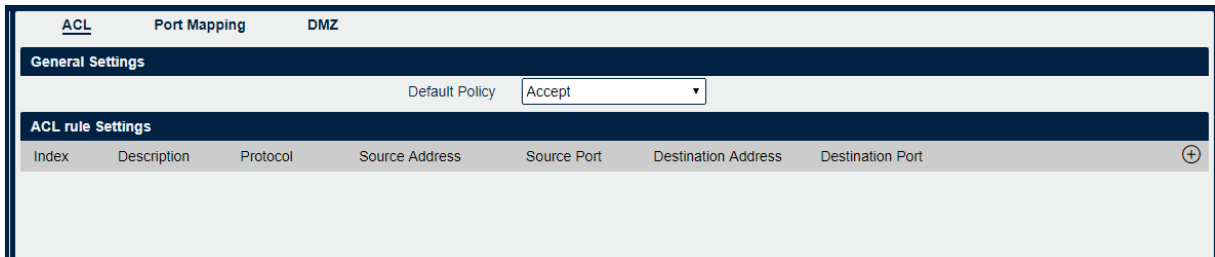
Digital IO->Digital Output

- **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.

4.5. Network Configuration

4.5.1. 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.

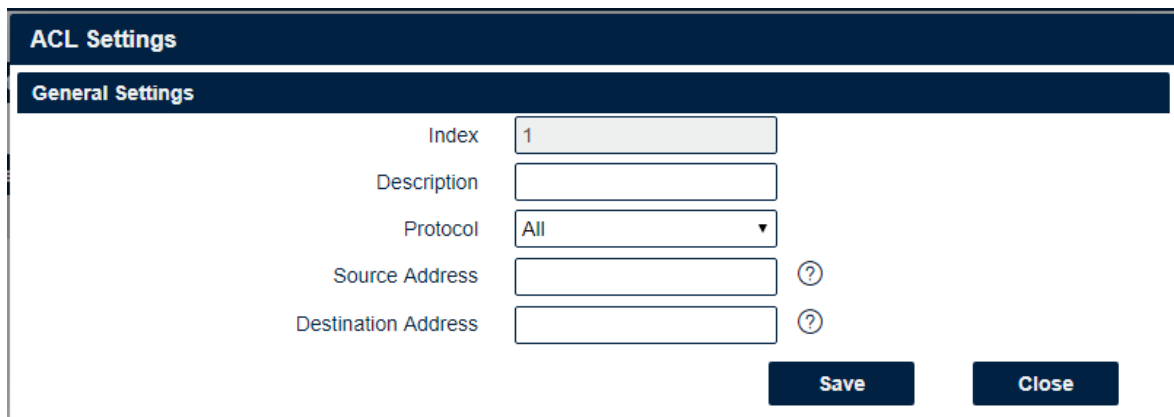


Firewall->ACL

- **Default Policy**

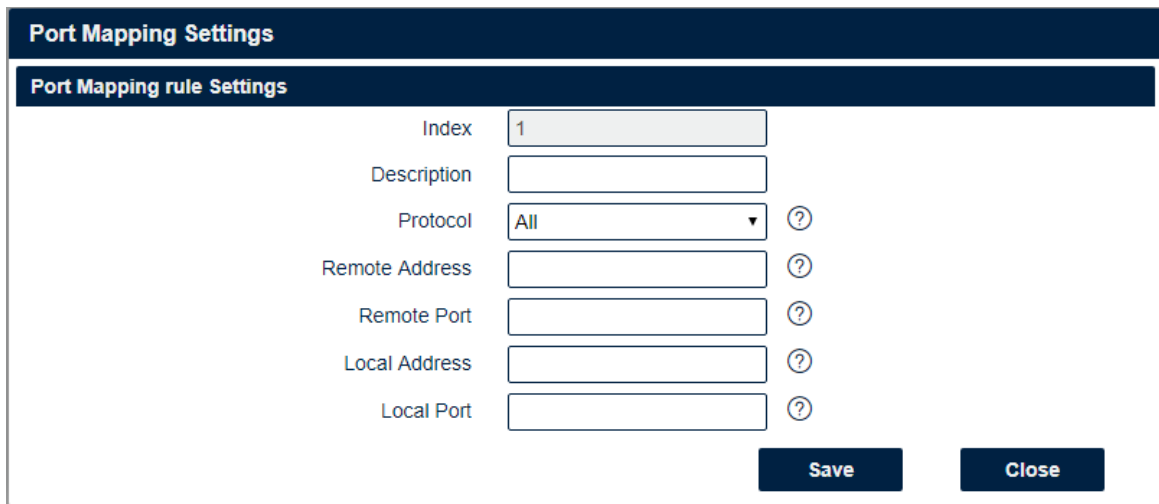
Select the “Accept” or “Drop” from the list, the packets which are not included in the access control list will be processed by the default filter policy.

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 number.
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 (the box following the /).
- **Destination Address** - A specific IP address can also be specified, or a range of IP addresses via a bitmask (the box following the /).



The screenshot shows a 'Port Mapping Settings' window with a sub-section 'Port Mapping rule Settings'. The form contains the following fields:

- Index:** A text input field containing the number '1'.
- Description:** An empty text input field.
- Protocol:** A dropdown menu currently set to 'All', with a help icon (?) to its right.
- Remote Address:** An empty text input field with a help icon (?) to its right.
- Remote Port:** An empty text input field with a help icon (?) to its right.
- Local Address:** An empty text input field with a help icon (?) to its right.
- Local Port:** An empty text input field with a help icon (?) to its right.

At the bottom right of the form are two buttons: 'Save' and 'Close'.

Firewall->Port Mapping

- **Description** - Add a description for this rule.
- **Protocol**
All: Any protocol number. TCP: The TCP protocol. UDP: The 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.

ACL Port Mapping DMZ

General Settings

Enable

Remote Address ?

DMZ Host 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.

4.6. Routing

4.6.1. 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.

Status Static Route					
Route Table Information					
Index	Destination	Netmask	Gateway	Metric	Interface
1	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0

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.

Static Route Settings

Route Table Information

Index	<input style="width: 90%;" type="text" value="1"/>
Description	<input style="width: 90%;" type="text"/>
IP Address	<input style="width: 90%;" type="text"/>
Netmask	<input style="width: 90%;" type="text"/>
Gateway	<input style="width: 90%;" type="text"/>
Interface	<input style="width: 90%;" type="text"/> ?

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.

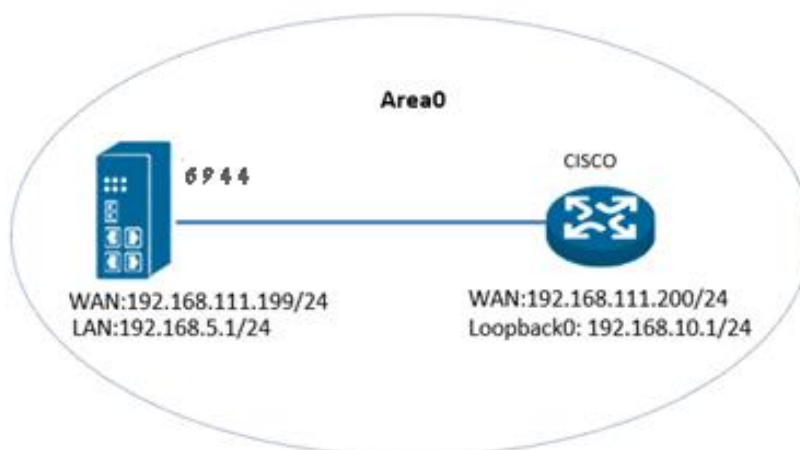
4.6.2. 6944 Dynamic Routing – OSPF to a Cisco 7200

6944 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	Change Description
2018/12/12	V1.0.0	devel(f6eb5e7)	First released
2020/06/25	V1.1	(6424848)	Update for 1.1.3 F/W

Topology



1. The 6944 and CISCO 7200 Router run OSPF and under the same single Area0.
2. The 6944 and CISCO 7200 Router set the IP of LAN and loopback0.

Cisco 7200 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
!

```

Cisco 7200 Configuration Continued

```

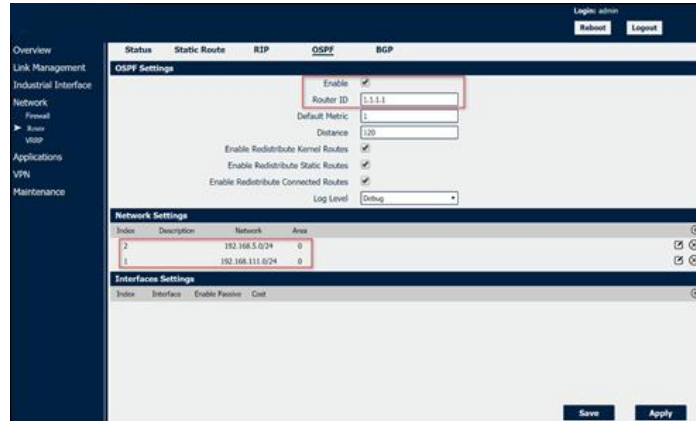
router ospf 110
  router-id 2.2.2.2
  log-adjacency-changes
  network 192.168.10.0 0.0.0.255 area 0
  network 192.168.111.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0

privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
end
CISCO7200#

```


6944 Configuration

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



2. Click Save>Apply.

Checking the Cisco 7200 Routing Table

```
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 routing Table on your 6944 router for reference.

Index	Destination	Network	Gateway	Metric	Interface
1	0.0.0.0	0.0.0.0	192.168.111.11	0	wan
2	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
3	192.168.10.1	255.255.255.255	192.168.111.200	20	wan
4	192.168.111.0	255.255.255.0	0.0.0.0	0	wan

Testing

1. Ping from CISCO to the 6944

```
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#
```

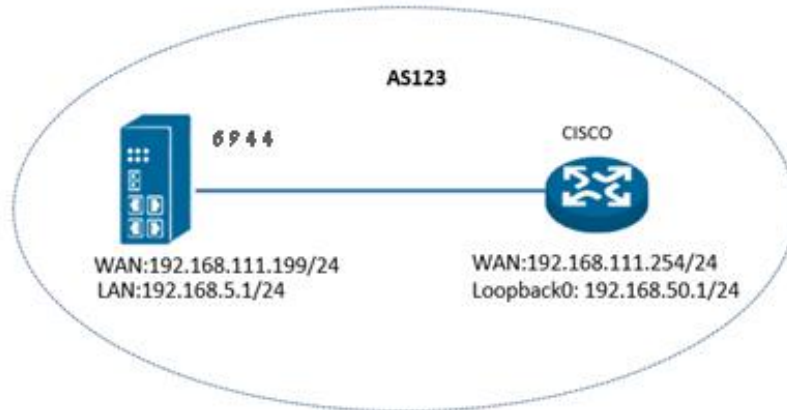
2. Test successfully.

4.6.3. Configuring BGP on the 6944 to a Cisco 7200 Router

Version

Release Date	Doc. Version	Firmware Version	Change Description
2018/12/12	V1.0.0	devel(f6eb5e7)	First released
2020/06/25	V1.1	(6424848)	Update for 1.1.3 F/W

Topology

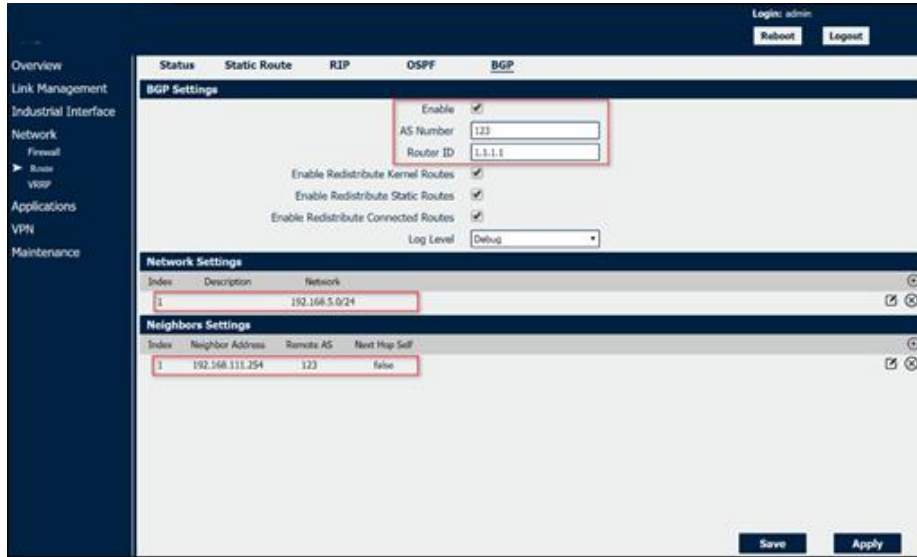


Make sure the 6944 Router and CISCO 7200 are running on the same AS123 and are neighbours.
 Make sure the 6944 and CISCO 7200 have enabled BGP and declare the IP of LAN and loopback0.

<pre> Cisco 7200 BGP 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 duplex auto speed auto ! </pre>	<pre> Cisco 7200 BGP Configuration Continued 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# </pre>
---	---

6944 Configuration

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



2. Click Save>Apply.

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#
```

Check the 6944 Routing table for reference

Testing

1. Ping from CISCO to the 6944 Router

```
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#
```

2. Test successful

4.7. 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.

Index	1
Enable	<input checked="" type="checkbox"/>
Interface	LAN0
Virtual Router ID	1
Authentication Type	None
Priority	100
Interval	1
Virtual IP Address	

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.

4.8. IP Passthrough

IP Passthrough 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.

IP Passthrough

General Settings

Enable

Passthrough Host MAC ?

Remote HTTPS Access Reserved

Remote Telnet Access Reserved

Remote SSH Access Reserved

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.

4.9. VPN (Virtual Private Networks)

4.9.1. OpenVPN

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.

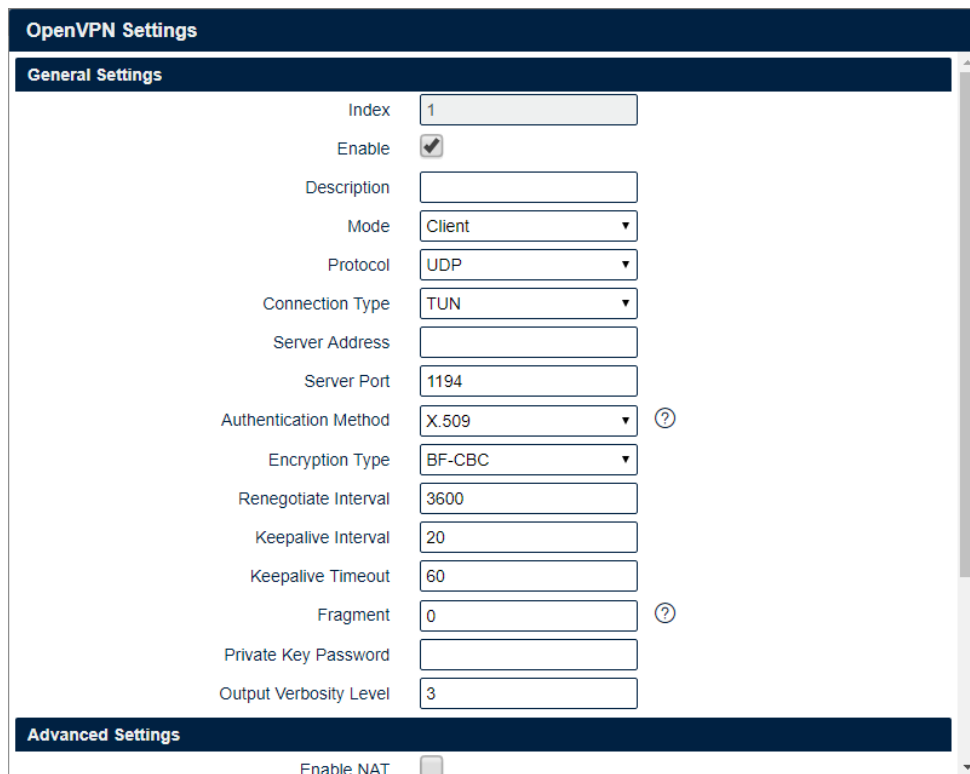
You can review all OpenVPN connections on the 6944 as shown below.



OpenVPN Information						
Index	Enable	Description	Status	Uptime	Virtual IP	

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.



OpenVPN Settings

General Settings

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Mode	<input type="text" value="Client"/>
Protocol	<input type="text" value="UDP"/>
Connection Type	<input type="text" value="TUN"/>
Server Address	<input type="text"/>
Server Port	<input type="text" value="1194"/>
Authentication Method	<input type="text" value="X.509"/> ?
Encryption Type	<input type="text" value="BF-CBC"/>
Renegotiate Interval	<input type="text" value="3600"/>
Keepalive Interval	<input type="text" value="20"/>
Keepalive Timeout	<input type="text" value="60"/>
Fragment	<input type="text" value="0"/> ?
Private Key Password	<input type="text"/>
Output Verbosity Level	<input type="text" value="3"/>

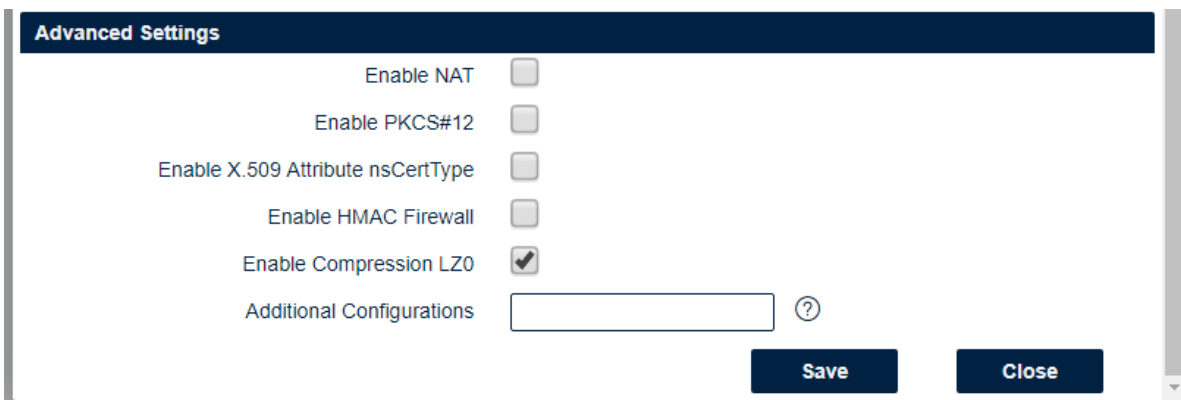
Advanced Settings

Enable NAT

VPN->OpenVPN

- **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”.
- **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 HMAC Firewall**
Add additional layer of HMAC authentication on the top of the TLS control channel to protect against DoS attacks.
- **Enable Compression LZO**
Compress the data.
- **Additional Configurations**
Enter some other options of OpenVPN in this field. Each expression can be separated by a ‘;’.

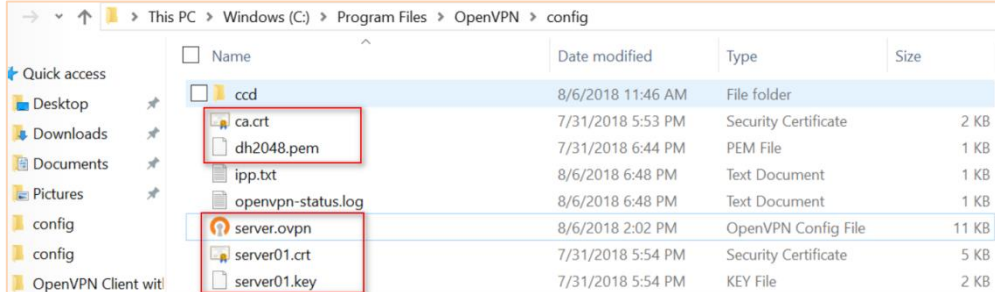
Status	OpenVPN	X.509 Certificate	
X.509 Certificate Import			
Connection Index	1		
CA Certificate	Choose File	No file chosen	
Local Certificate File	Choose File	No file chosen	
Local Private Key	Choose File	No file chosen	
HMAC firewall Key	Choose File	No file chosen	
Pre-shared Key	Choose File	No file chosen	
PKCS#12 Certificate	Choose File	No file chosen	
X.509 Certificate Files			
Index	File Name	File Size	Date Modified

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

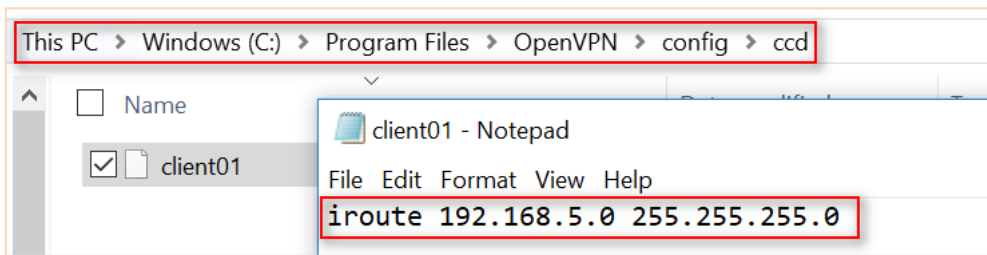
4.9.2. Testing OpenVPN between a PC and the 6944

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:

```

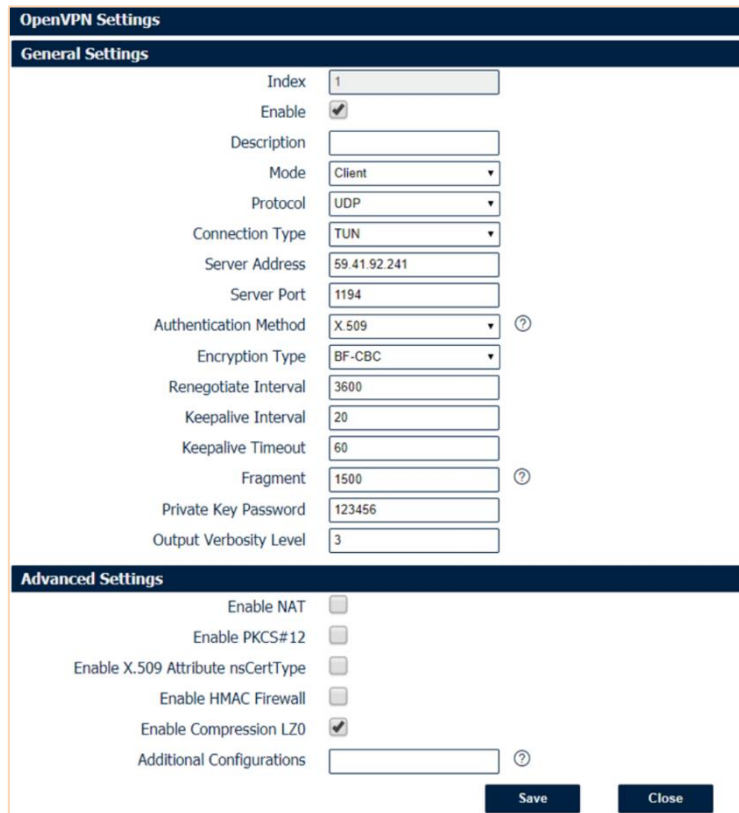
=====
local 59.41.92.241
mode server
port 1194
proto udp
dev tun
tun-mtu 1500
fragment 1500
ca ca.crt
cert server01.crt
key server01.key # This file should be kept secret
dh dh2048.pem
server 10.8.0.0 255.255.255.0

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
    
```

Step 4 - Configure the Client

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



OpenVPN Settings

General Settings

Index	1
Enable	<input checked="" type="checkbox"/>
Description	
Mode	Client
Protocol	UDP
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	X.509
Encryption Type	BF-CBC
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500
Private Key Password	123456
Output Verbosity Level	3

Advanced Settings

Enable NAT	<input type="checkbox"/>
Enable PKCS#12	<input type="checkbox"/>
Enable X.509 Attribute nsCertType	<input type="checkbox"/>
Enable HMAC Firewall	<input type="checkbox"/>
Enable Compression LZ0	<input checked="" type="checkbox"/>
Additional Configurations	

Save **Close**

Click Save>Apply.

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



X.509 Certificate Import

Connection Index: 1

CA Certificate: Choose File... No file chosen

Local Certificate File: Choose File... No file chosen

Local Private Key: Choose File... No file chosen

HMAC Firewall Key: Choose File... No file chosen

Pre-shared Key: Choose File... No file chosen

PKCS#12 Certificate: Choose File... No file chosen

X.509 Certificate Files

Index	File Name	File Size	Date Modified
1	ca.crt	1188	Mon Aug 6 14:02:26 2018
2	client.crt	4382	Mon Aug 6 14:02:33 2018
3	client.key	1834	Mon Aug 6 14:02:38 2018

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



Status **OpenVPN** **X.509 Certificate**

OpenVPN Information

Index	Enable	Description	Status	Uptime	Virtual IP
1	true		Connected	00:00:24	10.8.0.6

Step 7 - Route Table Check the Route Table on 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 Route Table on 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 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 10 - Go to Maintenance>Debug Tool>Ping and Ping from OpenVPN client to OpenVPN Server.



4.9.3. IPSec

IPSec facilitates allow the use of secured 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.

Status		IPSec		
IPSec Information				
Index	Enable	Description	Status	Uptime

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.

IPSec Settings	
General Settings	
Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Remote Gateway	<input type="text"/>
IKE Version	<input type="text" value="IKEv1"/>
Connection Type	<input type="text" value="Tunnel"/>
Negotiation Mode	<input type="text" value="Main"/>
Authentication Method	<input type="text" value="Pre-shared Key and Xauth"/>
Local Subnet	<input type="text"/>
Local Pre-shared Key	<input type="text"/>
Local ID Type	<input type="text" value="IPv4 Address"/>
Xauth Identity	<input type="text"/>
Xauth Password	<input type="text"/>
Remote Subnet	<input type="text"/>
Remote ID Type	<input type="text" value="IPv4 Address"/>

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**
 Enter the IP address with mask if a 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.

IKE Proposal Settings	
Encryption algorithm	<input type="text" value="AES-256"/>
Hash Algorithm	<input type="text" value="SHA2 256"/>
Diffie-Hellman group	<input type="text" value="Group5(modp1536)"/>
Lifetime	<input type="text" value="1440"/>
ESP Proposal Settings	
Encryption algorithm	<input type="text" value="AES-256"/>
Hash Algorithm	<input type="text" value="SHA2 256"/>
Diffie-Hellman group	<input type="text" value="Group5(modp1536)"/>
Lifetime	<input type="text" value="60"/>
Advanced Settings	
DPD Interval	<input type="text" value="30"/> ?
DPD Timeout	<input type="text" value="90"/> ?
Additional Configurations	<input type="text"/> ?

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 ‘;’.

4.9.4. GRE

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

Status		GRE		
GRE Information				
Index	Enable	Description	Mode	Status

VPN->GRE->Status

- **Enable** - Displays current GRE settings is enable or disable.
- **Description** - Displays the description of current VPN channel.
- **Mode** - Displays the current VPN mode.
- **Status** - Displays the current VPN connection status.

GRE Settings

GRE Information

Index	<input type="text" value="1"/>
Enable	<input checked="" type="checkbox"/>
Description	<input type="text"/>
Mode	<input type="text" value="Layer 3"/>
Remote Gateway	<input type="text"/>
Local Virtual IP	<input type="text"/>
Local Virtual Netmask	<input type="text" value="255.255.255.252"/>
Tunnel key	<input type="text"/> ?
Enable NAT	<input type="checkbox"/>

VPN->GRE

- **Enable** Check this box to enable GRE.
- **Description** Enter the description of current VPN channel.
- **Mode** Specify the running mode of GRE, optional are "Layer 2" and "Layer 3".
- **Remote Gateway** Enter the remote IP address of peer GRE tunnel.
- **Local Virtual IP** Enter the local tunnel IP address of GRE tunnel.
- **Local Virtual Netmask** Enter the local virtual netmask of GRE tunnel.
- **Tunnel Key** Enter the authentication key of GRE tunnel.
- **Enable NAT** Check this box to enable NAT function.
- **Bridge Interface** Specify the bridge interface work with Layer 2 mode.

4.10. CLI (Command Line Interface)

The Command-line interface (CLI) is a software interface that provide another way to set parameters on the 6944 router. Its possible to use Telnet or SSH to connect to the 6944 router for CLI input.

The 6944 CLI Access

Case Communications. 6944 router login: **admin**

Password: **admin**

>

4.10.1. CLI reference commands

>?

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
tracert	TraceRoute
upgrade	Upgrade firmware
version	Show firmware version

e.g.

```
> version          1.0.0 (1017.4)
> show wifi
wifi
{
  "status":"Ready",
  "mac":"a8:3f:a1:e0:ab:81",
  "ssid":"6944-WAN",
  "channel":"6",
  "width":"40 MHz",
  "txpower":"20.00 dBm"
}
> ping www.baidu.com
PING www.baidu.com (14.215.177.38): 56 data bytes
64 bytes from 14.215.177.38: seq=0 ttl=54 time=10.826 ms
64 bytes from 14.215.177.38: seq=1 ttl=54 time=10.284 ms
--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 10.031/10.312/10.826 ms
>
```

4.10.2. How to Configure the CLI**CONTEXT SENSITIVE HELP**

[?] - Display context sensitive help. This is either a list of possible command completions with summaries, or the full syntax of the current command. A subsequent repeat of this key, when a command has been resolved, will display a detailed reference.

AUTO-COMPLETION

The following keys both perform auto-completion for the current command line. If the command prefix is not unique then the bell will ring and a subsequent repeat of the key will display possible completions.

[enter] - Auto-completes, syntax-checks then executes a command. If there is a syntax error then offending part of the command line will be highlighted and explained.

[space] - Auto-completes, or if the command is already resolved inserts a space.

MOVEMENT KEYS

[CTRL-A] - Move to the start of the line

[CTRL-E] - Move to the end of the line.

[up] - Move to the previous command line held in history.

[down] - Move to the next command line held in history.

[left] - Move the insertion point left one character.

[right] - Move the insertion point right one character.

DELETION KEYS

[CTRL-C] - Delete and abort the current line

[CTRL-D] - Delete the character to the right on the insertion point.

[CTRL-K] - Delete all the characters to the right of the insertion point.

[CTRL-U] - Delete the whole line.

[backspace] - Delete the character to the left of the insertion point.

ESCAPE SEQUENCES

!! - Substitute the last command line.

!N - Substitute the Nth command line (absolute as per 'history' command)

!-N - Substitute the command line entered N lines before (relative)

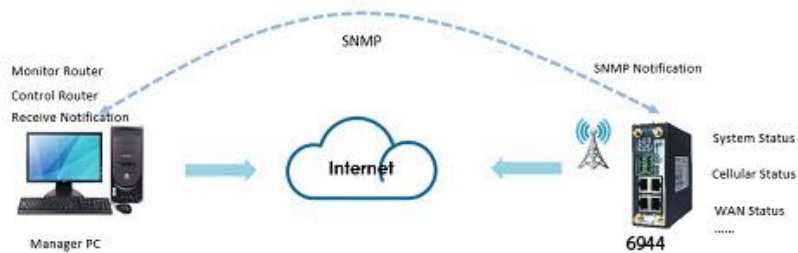
4.11. SNMP

4.11.1. Overview

This document contains information regarding the configuration and use of SNMP on the 6944 router. Updates between document versions are cumulative. Therefore, the latest document will include all the content of previous versions.

Release Date	Doc. Version	Firmware Version	Change Description
2020/03/04	V1.0.0	V1.1.3(e335ec6)	First released
2020/06/25	V1.1	(6424848)	Update for 1.1.3 F/W

4.11.2. Topology



Objectives

Use the Managers PC to access the 6944 router using the SNMP Protocol.

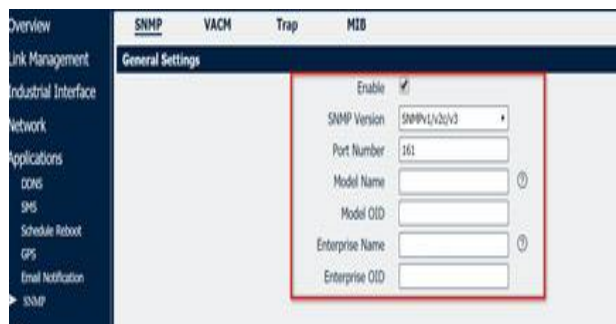
Use the Managers PC to obtain the status, control the router and receive the SNMP messages from the 6944 router.

Connect the Management PC to the LAN port of 6944. The IP address of Manager PC should be set to is: 192.168.5.19/24. The IP address of 6944 Router LAN port should be set to: 192.168.5.1/24.

4.11.3. Configuring the 6944 Router

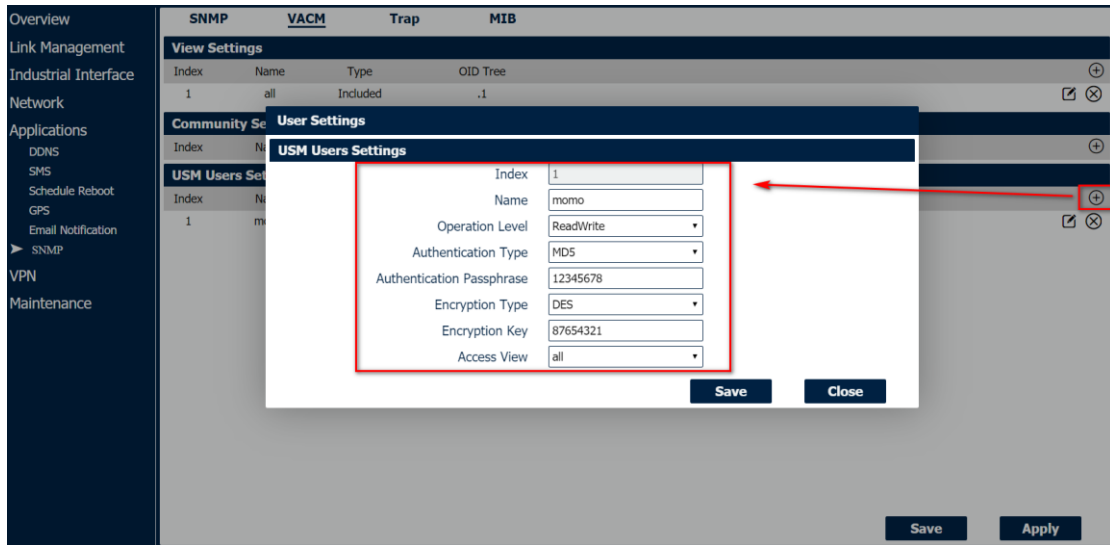
Go to **Applications>SNMP>SNMP**, enable SNMP and configure as shown here

- SNMP Version V1 / V2 / V2
- Port number 161
- Model name 6944
- Model OID – 6944.500100
- Enterprise Name – Casecomms
- Enterprise OID – 144



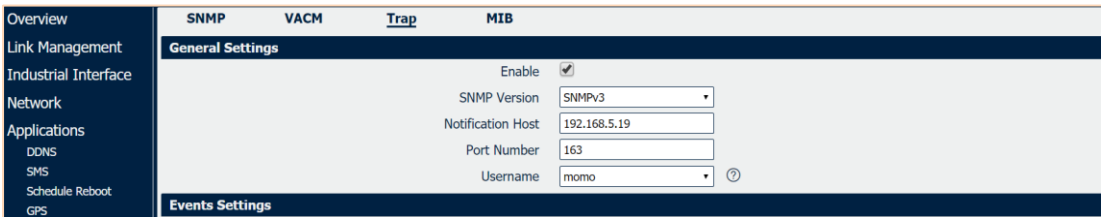
Click Save>Apply.

Go to **Applications>SNMP>VACM**, go to configuration “View Settings” as a default. For “USM Users Settings”, please use the set upshown above.



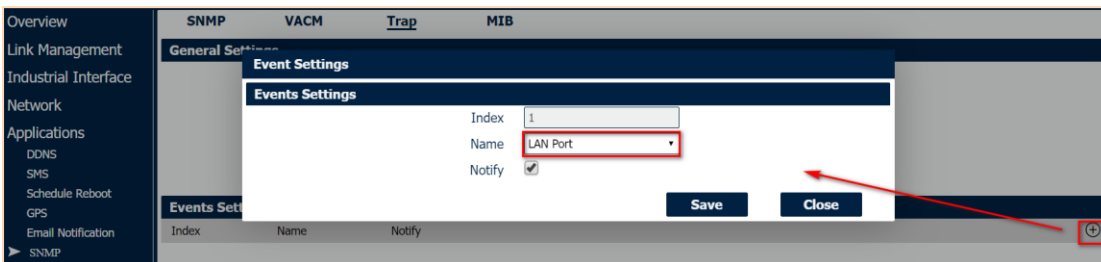
Click Save>Apply.

Go to “**Applications>SNMP>Trap**”, enable SNMP Trap configuration, and the “Notification Host” should be the IP address of the PC run with SNMP management tool, like below:



Now set the “LAN Notify” as an example, when the LAN Port status changed, the SNMP management tool will receive event alarms.

Go to “**Applications>SNMP>Trap>Events Settings**”, configuration like below:



Click Save>Apply

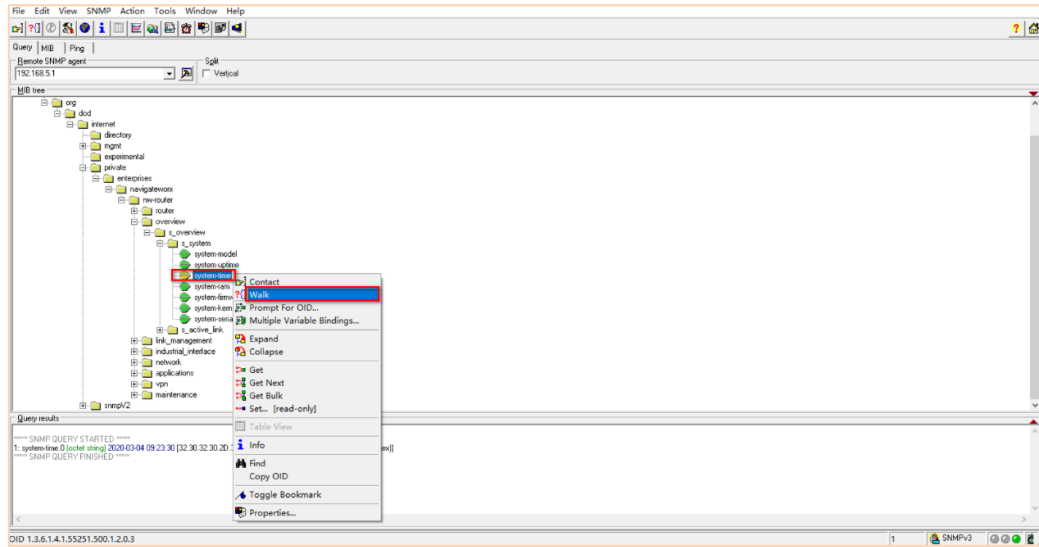
4.11.4. Testing

If you don't have an SNMP Network Management System such as CaseView it will be necessary download and install some SNMP Software such as MG MibBrowser to confirm your have configured SNMP Correctly

Monitor the operational Status Of The 6944 Router

First check the "system time" and check the "firmware version" as an example.

Go to the "system-time" and Right Click, then select "Walk":



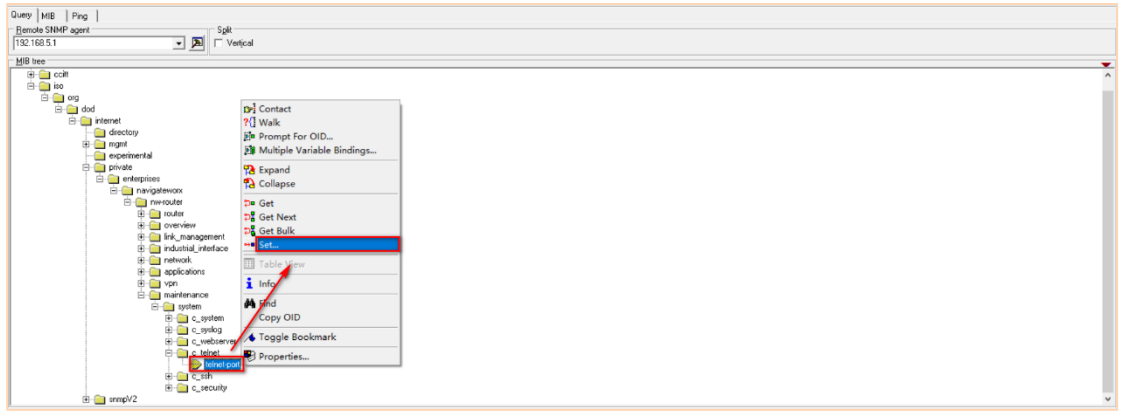
Get the System Time of the router:



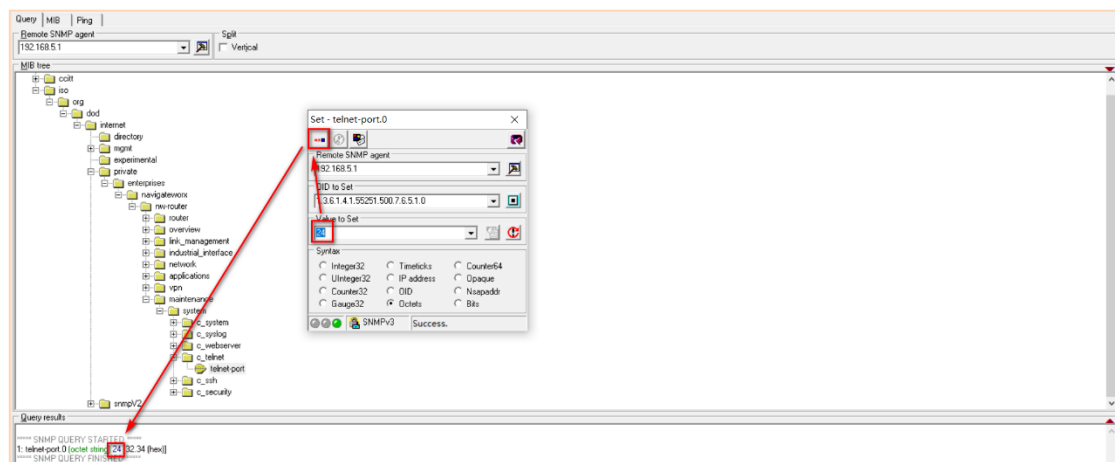
4.11.5. Controlling the 6944 Router

We change the Telnet Port of the router to make sure we can control the 6944, after checking, then we need to Save, then Apply.

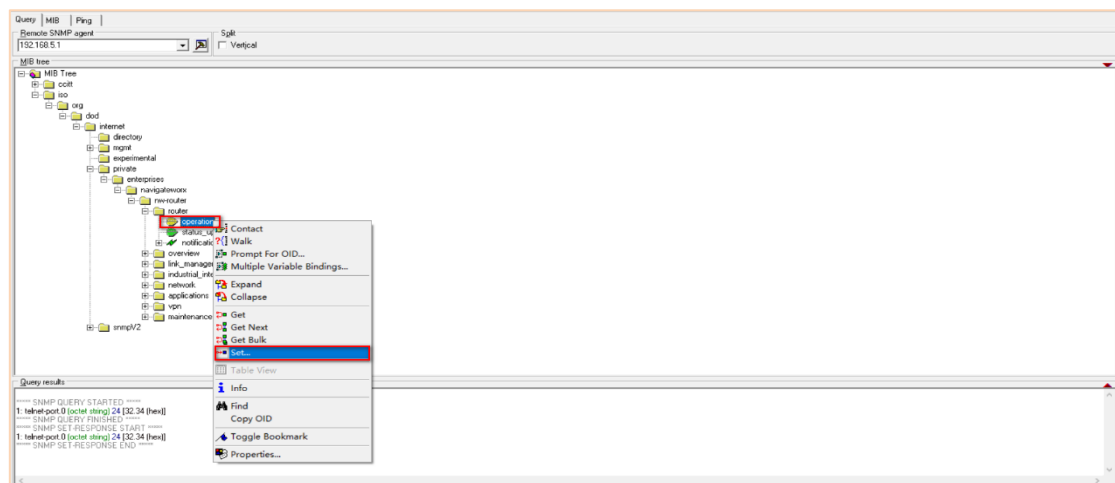
Go to the "Telnet" Option, Right Click, then Click "Set":



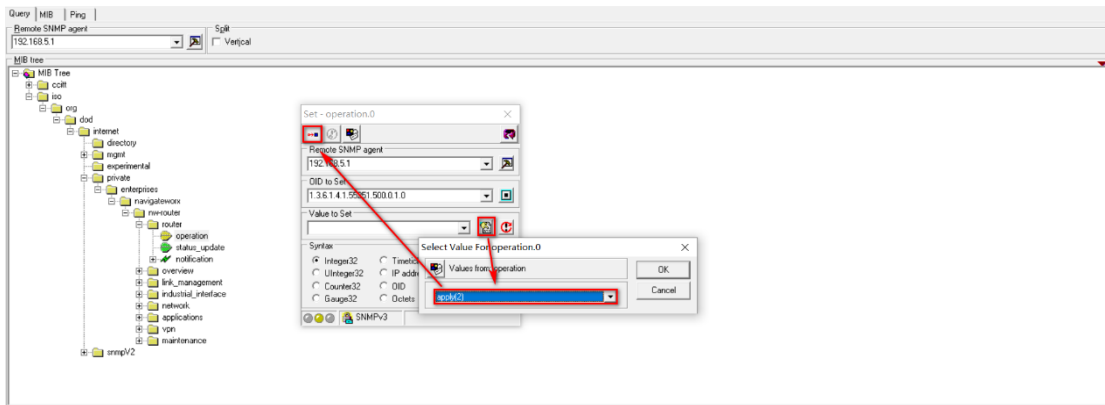
As an example change the Telnet Port from 23 to “24”, as shown below to test that we can modify settings:



After setting, the port. Go to “Save” to save the change:



Then “Apply”:



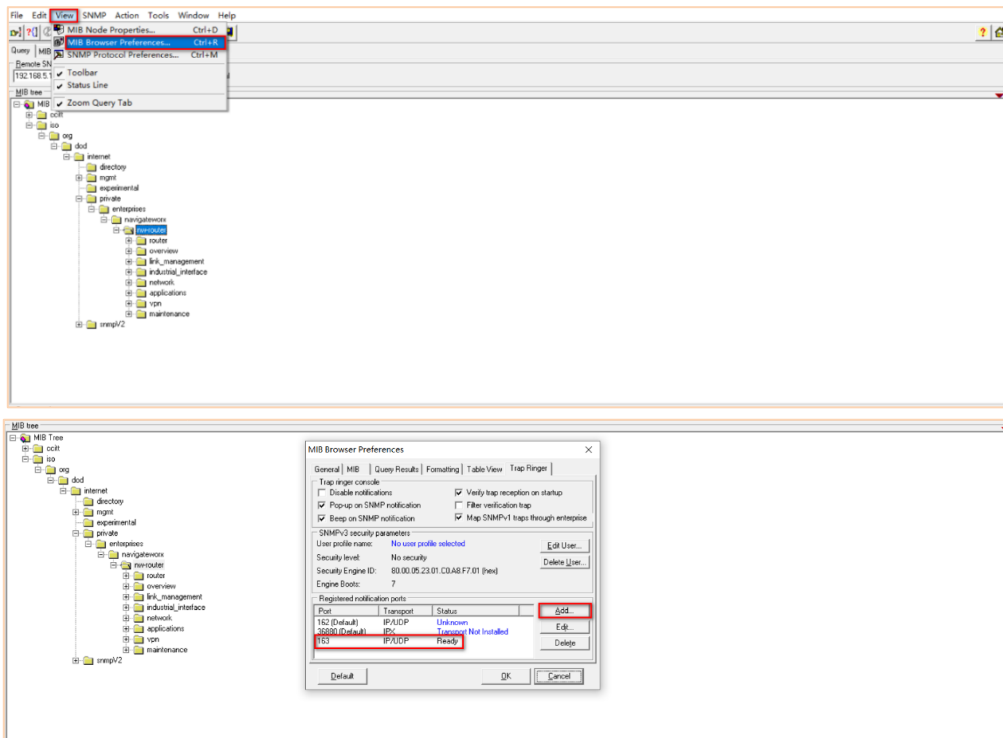
Log in to the router and make sure the Tenet Port had been changed to “24”:



Test Successful.

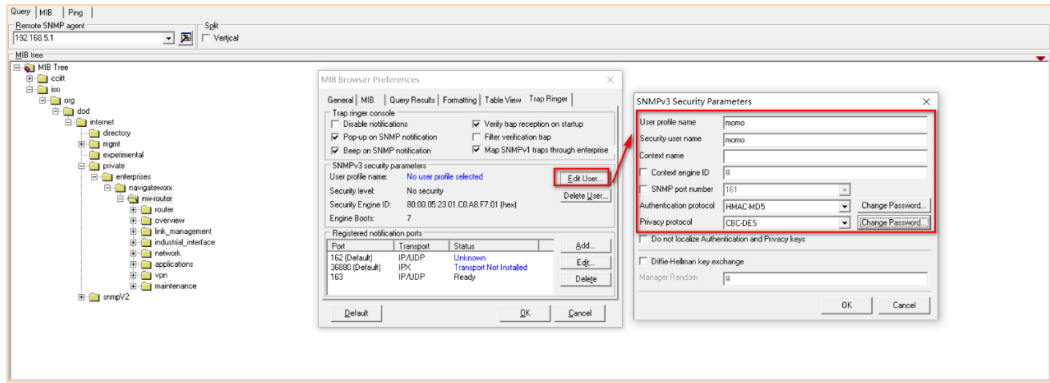
4.11.6. Receiving SNMP Traps

This tests we can receive an SNMP Trap on UDP port 163, as shown below:

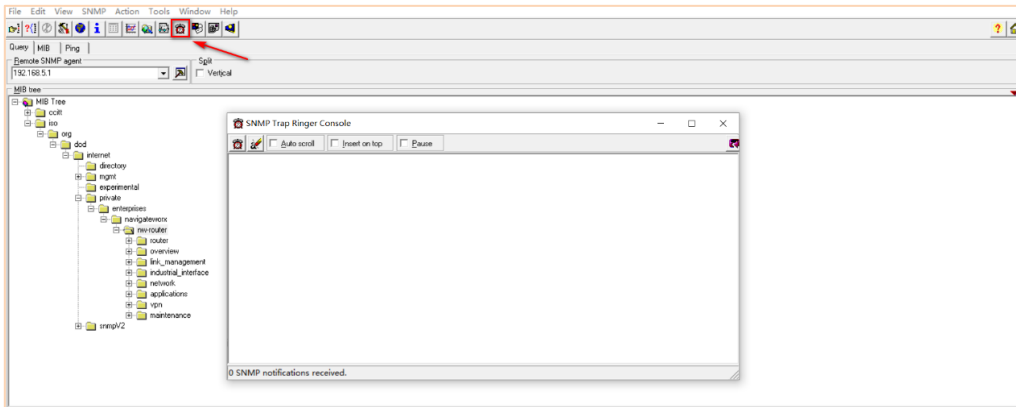


Add User and click “OK”:

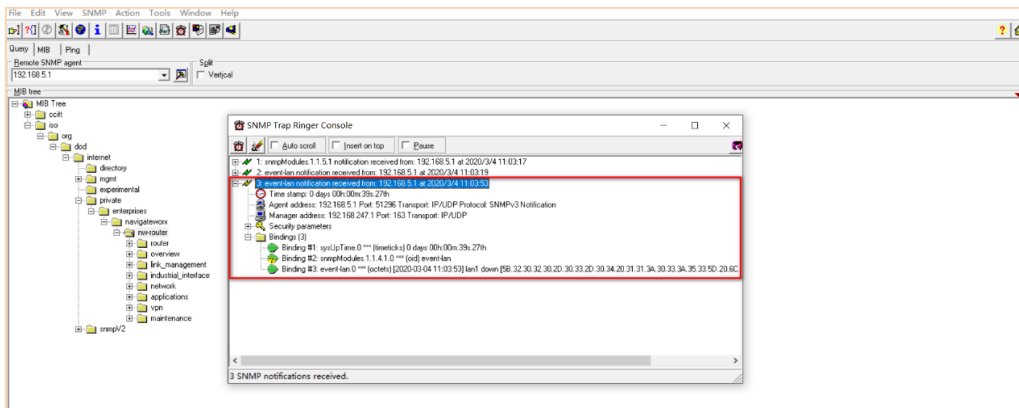
4. BROWSER CONFIGURATION



Open the SNMP Trap Ringer Console:



Remove the Ethernet Cable from LAN port of the router, then receive a Notification from that LAN Port on the SNMP Management tool:

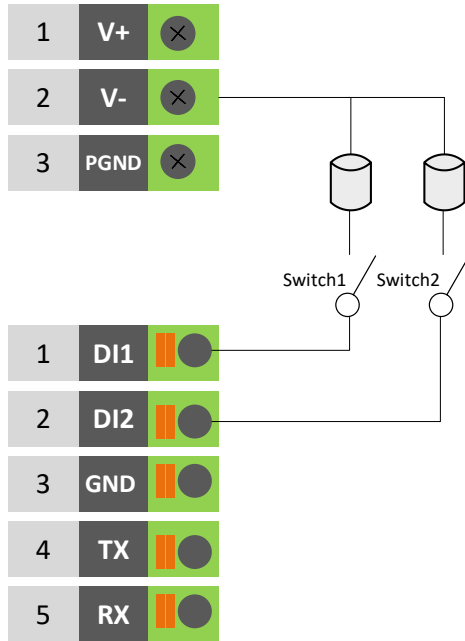


Test successful.

5. Digital I / O Ports

5.1. Digital Input

Typical Application Diagram



DI ELECTRICAL CHARACTERISTICS

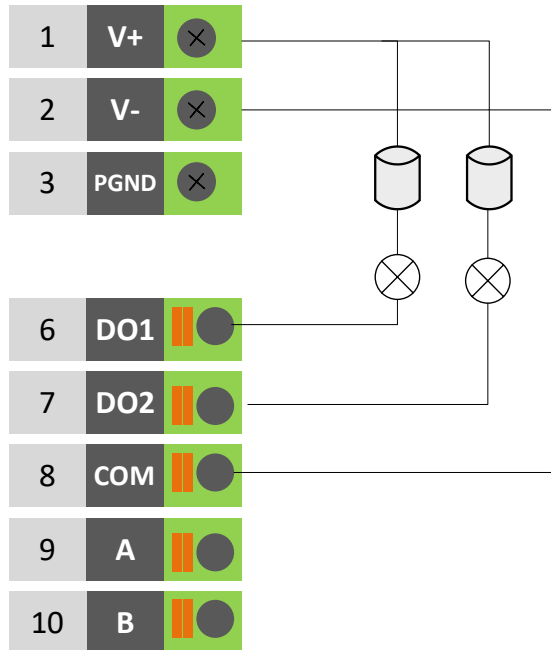
- 1. Galvanic isolation;
- 2. Over-Voltage Protection: 36 VDC
- 3. Over-Current Protection: 100mA per channel @ 25°C

Dry Contact Typical Application

- Switch ON(Short to V-): DI Logic LOW
- Switch OFF(Open): DI Logic HIGH

5.2. 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)

6. MODBUS Slave

6.1. Overview

This document contains information regarding the configuration and use of the Modbus Slave Application within the 6944.

Compatibility

This application note applies to :

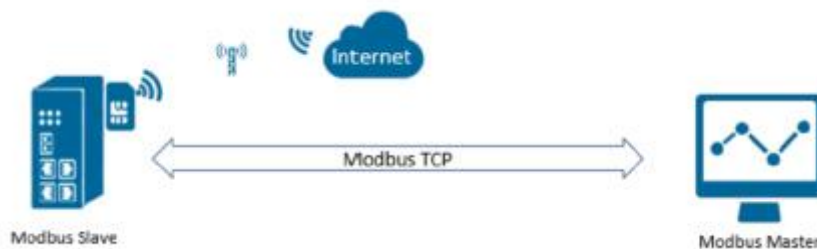
- Model:** Case 6944 series.
Firmware Version: V1.1.0 (ddcaac4) or newer
Other Compatible Models: None

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	Change Description
18.7.2019	V1.2.1	V1.1.0 (ADcaac4)	First release

6.2. Topology



The 6944 router runs as Modbus Slave with 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 statue of Digital IO and control DO.

Note: For this Application the 6944 will run the software titled “Modbus Poll” to simulate a Modbus Master

6.3. 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

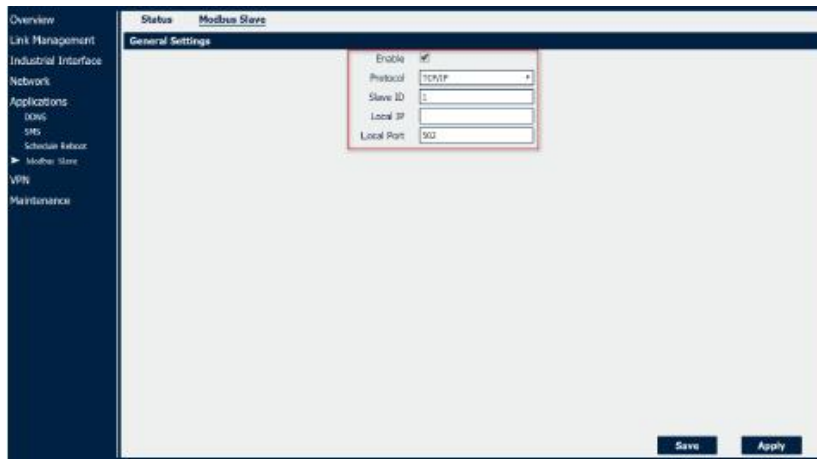
Example: Modify the width of the output pulse—500ms (The current output pulse to modify the width)

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

6.4. Configuration

6944 Configuration

Go to **Application>Modbus Slave**, enable the Modbus Slave feature as shown in the screen shot below:

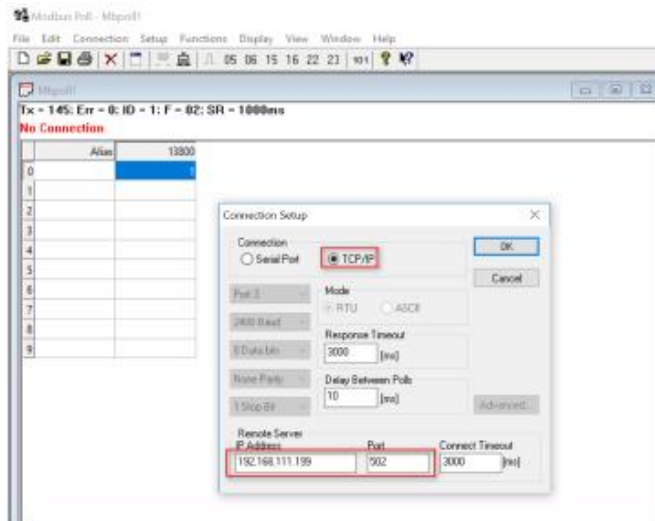


Click **Save > Apply**

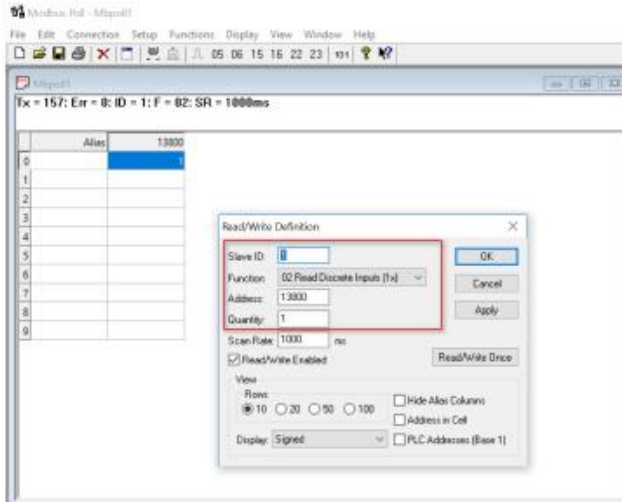
6.5. Testing

Read Digital Input Status

Run the software “MODBUS Poll” to connect to the 6944 (MODBUS Slave) as shown below (Path Connection > Connect

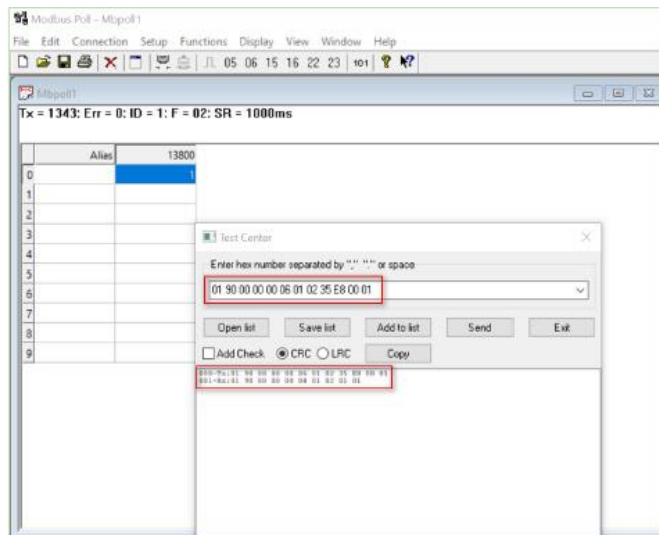


(Path: Setup> Read/ Write Definition)



Send the command to read the status of DI 1

(Path: Functions>Test Center)



The reply Value is “00”, DO1 status is “Low”. Test successfully.

Note: The meaning of “Tx” and “Rx” command, please refer to “Digital IO Register Table”.

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

7. MODBUS Master

7.1. 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

Overview

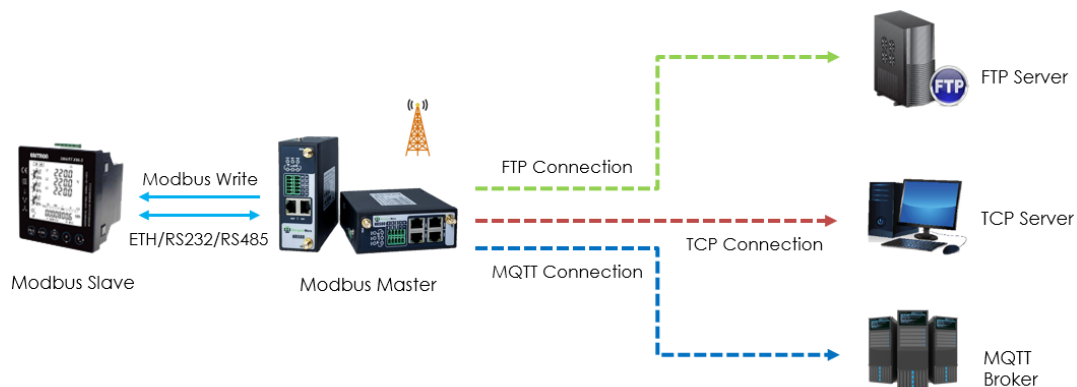
This document contains information regarding the configuration and use of the Modbus Master Software on the Case Communications 6944 router

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)	First released
18.2..2020	V1.0.0		MODBUS Master

7.2. Topology



The 6944 Router runs as Modbus Master and can connect to Modbus Slave via Ethernet, RS232 or RS485 interface.

The 6944 router poll the modbus data from modbus slave and send to the remote management center via TCP, FTP or MQTT protocol.

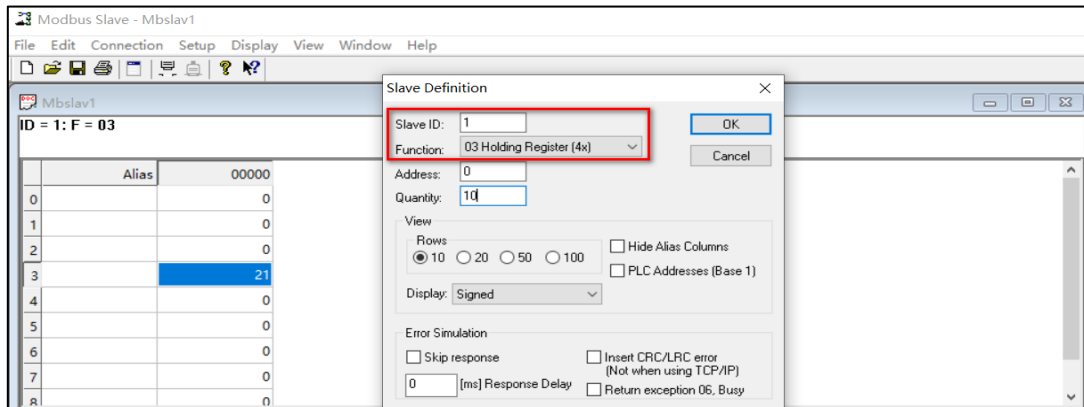
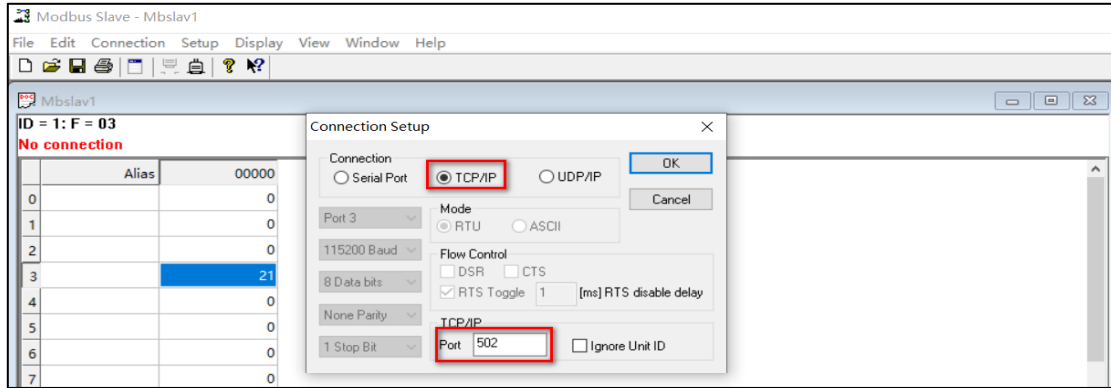
The 6944 as Modbus Master and writes to the register values or coil to Modbus Slave.

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 Ethernet port. Of course, it also works with Serial Port (RS232/RS485).

7.3. Transport via TCP

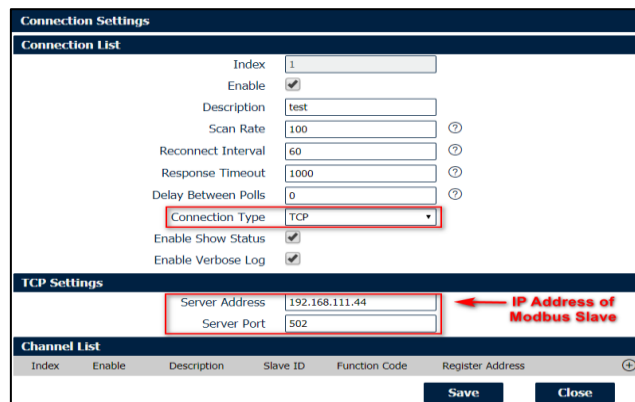
7.3.1. Configuration on Modbus Slave

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**, like below setting:



7.3.2. Configuration of the Modbus Poll

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 Modbus Slave, like below:

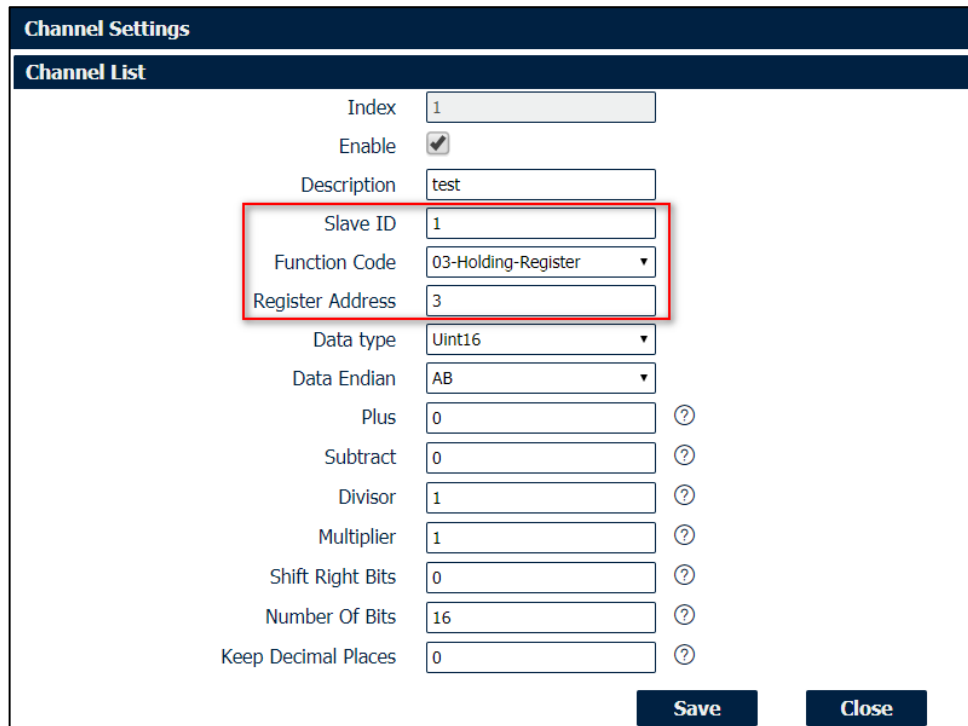


Click Save>Apply.

Enable “Channel List”, and specify the Slave ID as “1”, Function Code as “**03-Holding-Register**”, Register Address to “3”, then it will poll the value from register address 3 of Modbus Slave:

Click Save>Save>Apply. *(Note: This is a secondary list, it needs to be double clicked to save)*

Go to **Application>Modbus Master>Status**, then we can check the router had read the value from Modbus Slave successfully.



Channel Settings

Channel List

Index: 1

Enable:

Description: test

Slave ID: 1

Function Code: 03-Holding-Register

Register Address: 3

Data type: Uint16

Data Endian: AB

Plus: 0

Subtract: 0

Divisor: 1

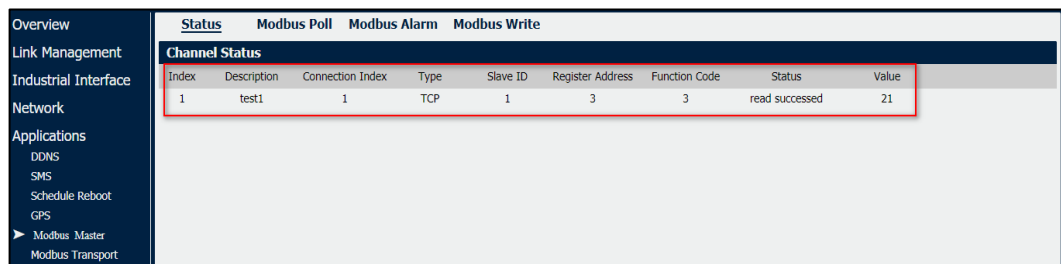
Multiplier: 1

Shift Right Bits: 0

Number Of Bits: 16

Keep Decimal Places: 0

Buttons: Save, Close



Index	Description	Connection Index	Type	Slave ID	Register Address	Function Code	Status	Value
1	test1	1	TCP	1	3	3	read succeeded	21

7.4. Configuring Modbus Transport

Go to **Application>Modbus Transport>Modbus Transport**, enable “Connection List”, and specify the TCP server IP address and port to send the data to remote TCP server. The Data Format could be defined accordingly or set it as default.

Enable “Modbus Channel”, Modbus Master will select the value send to the remote TCP server from Modbus Slave.

Connection Settings

Connection List

Index: 1
 Enable:
 Description: TCP Setting
 Protocol: TCP-Client
 Server Address: 14.215.177.39
 Server Port: 2000
 Reconnect Interval: 60
 Connection Timeout: 30
 Enable Verbose Log:

Transport Data Settings

Data Location: NULL
 Data Format: \$SERIAL_NUMBER,\$DATE,\$S
 Line Break:

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

Save Close

Channel Settings

Modbus Channel

Index: 1
 Enable:
 Connection Index: 1
 Filter Items: Slave ID
 Slave ID: 1

Save Close

Reconnect Interval: 60
 Connection Timeout: 30
 Enable Verbose Log:

Transport Data Settings

Data Location: NULL
 Data Format: \$SERIAL_NUMBER,\$DATE,\$S
 Line Break:

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

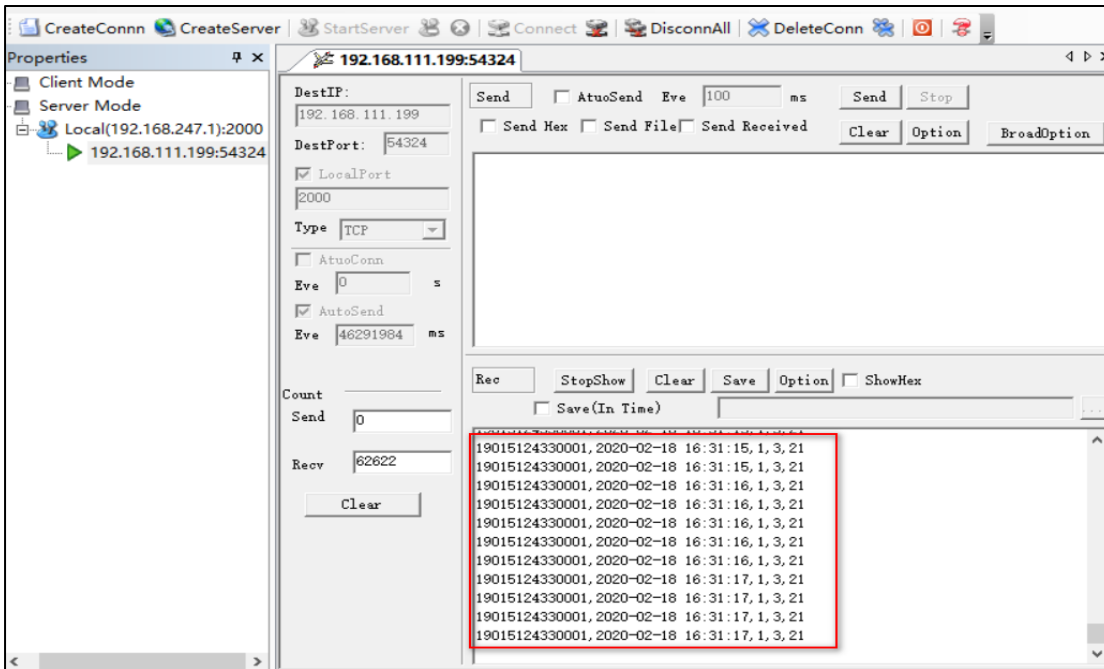
Save Close

Click Save>Save>Apply.

Go to **Application>Modbus Transport>Status**, THE 6944(Modbus Mater) had connected to the remote server successfully via TCP protocol.

<u>Status</u> Modbus Transport X.509 Certificate					
Connection Status					
Index	Enable	Description	Protocol	Status	Uptime
1	true	TCP Setting	TCP Client	Connected	00:02:35

Remote TCP Server received the data successfully.



7.5. Transport via FTP

Please refer to the Appendix “Configuration of Modbus Slave” and the Appendix’ Configuration on Modbus Poll” to finish and setting.

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. The File Name and Data Format could be defined accordingly or set it as default.

Connection Settings
CONNECTION LIST

Index: 1
 Enable:
 Description: FTP Setting

Protocol: FTP
 Server Address: 14.215.177.39
 Server Port: 21
 Username: admin
 Password: adminftp

Connection Timeout: 30
 Try To Send: 3
 Enable Verbose Log:

Transport Data Settings

Data Location: NULL
 Add CSV File Title:
 File Name: \$SERIAL_NUMBER_\$DATE.cs
 Upload Interval: 30
 Data Format: \$SERIAL_NUMBER,\$DATE,\$S

Save Close

Enable “Modbus Channel”, Modbus Master will select the value send to the remote FTP server from Modbus Slave.

Channel Settings

Modbus Channel

Index: 1
 Enable:
 Connection Index: 1
 Filter Items: Slave ID
 Slave ID: 1

Try To Send: 3
 Enable Verbose Log:

Transport Data Settings

Data Location: NULL
 Add CSV File Title:
 File Name: \$SERIAL_NUMBER_\$DATE.cs
 Upload Interval: 30
 Data Format: \$SERIAL_NUMBER,\$DATE,\$S

Modbus Channel

Index	Enable	Connection Index	Filter Items	Channel Index	Slave ID	Register Address

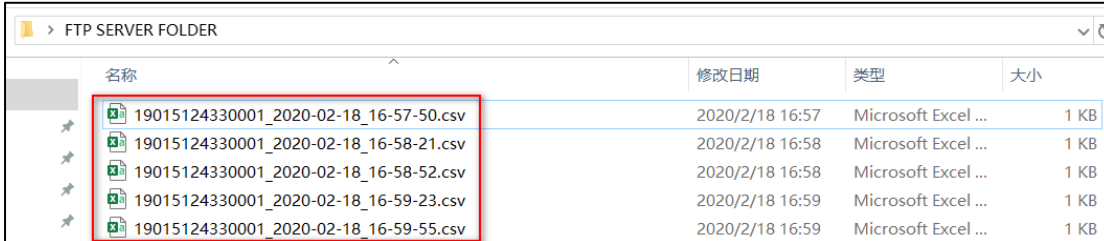
Save Close

Click Save>Save>Apply.

Go to **Application>Modbus Transport>Status**, THE 6944(Modbus Mater) had connected to the remote server successfully via FTP protocol.

Status		Modbus Transport		X.509 Certificate	
Connection Status					
Index	Enable	Description	Protocol	Status	Uptime
1	true	FTP Setting	FTP	Sent Successfully	

Remote FTP Server received the CSV file successfully.

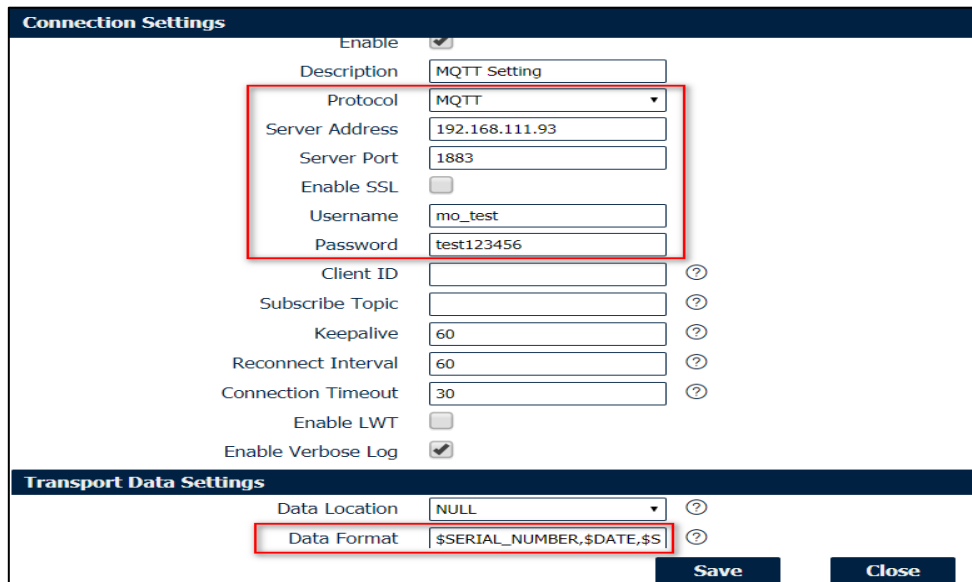


名称	修改日期	类型	大小
19015124330001_2020-02-18_16-57-50.csv	2020/2/18 16:57	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-58-21.csv	2020/2/18 16:58	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-58-52.csv	2020/2/18 16:58	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-59-23.csv	2020/2/18 16:59	Microsoft Excel ...	1 KB
19015124330001_2020-02-18_16-59-55.csv	2020/2/18 16:59	Microsoft Excel ...	1 KB

7.6. Transport via MQTT

Please refer to the “Configuration of the Modbus Slave” and “Configuration of the Modbus Poll” to finish and setting.

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. The Data Format could be defined accordingly or set it as default.



Connection Settings

Enable

Description: MQTT Setting

Protocol: MQTT

Server Address: 192.168.111.93

Server Port: 1883

Enable SSL:

Username: mo_test

Password: test123456

Client ID: ?

Subscribe Topic: ?

Keepalive: 60 ?

Reconnect Interval: 60 ?

Connection Timeout: 30 ?

Enable LWT:

Enable Verbose Log:

Transport Data Settings

Data Location: NULL ?

Data Format: \$SERIAL_NUMBER,\$DATE,\$S ?

Save Close

Enable “Modbus Channel”, define the “Topic” to publish to MQTT Broker with Modbus data.

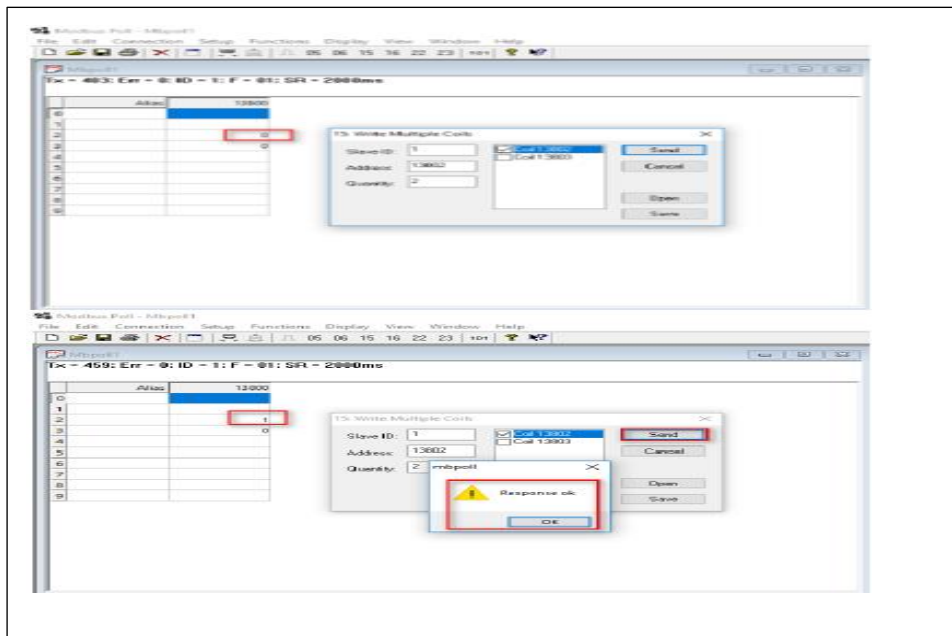
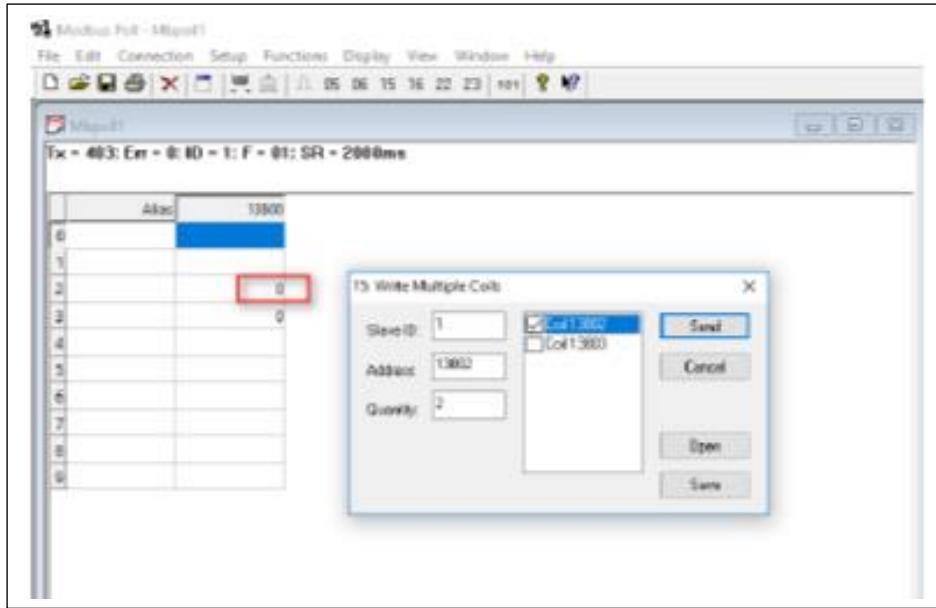
Click Save>Save>Apply.

Go to **Application>Modbus Transport>Status**, The 6944(Modbus Mater) had connected to the remote MQTT broker successfully.

Status		Modbus Transport		X.509 Certificate	
Connection Status					
Index	Enable	Description	Protocol	Status	Uptime
1	true	MQTT Setting	MQTT	Connected	00:23:04

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.

Test Successful



Control Digital Output

Go to **Functions>15:WriteMultiple Coils**, to change the DO state from “0”to “1”.

Test Successful

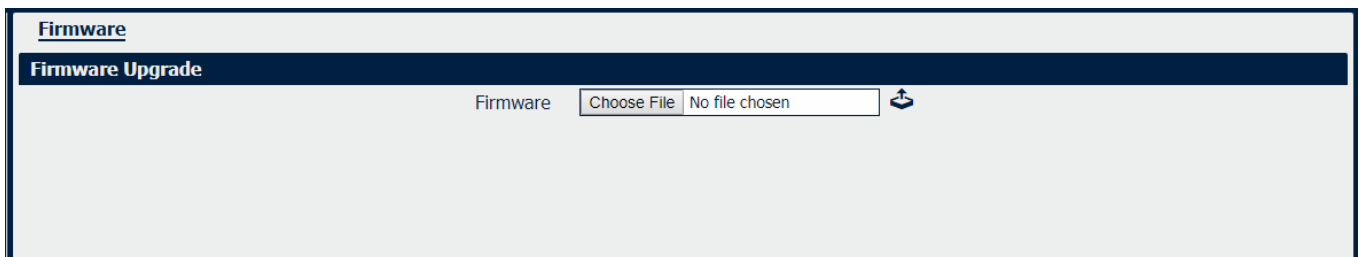
8. MAINTENANCE

8.1. Upgrading Software

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.

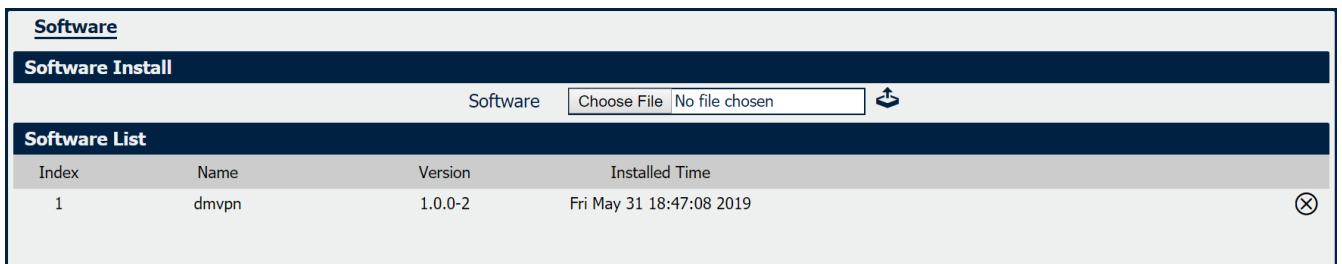
CAUTION: It is important to have a stable power source and ensure that power to the 6944 is not interrupted during a firmware upgrade.



Software

When a new feature is released (APP Package) of the 6944 router, the user can manually install to the unit by uploading a package. Or the user can uninstall this feature (APP Package) from the router.

NOTE: The unit needs to be manually rebooted once the upload/uninstall completes, thus taking the 6944 router out of service for approximately 1 minute. Unless otherwise stated, the user is not expected to take any special precautions.



Click  to upload the APP Package.

Click  to delete the APP Package.

8.2. System Settings

This section allows you to review the device system settings.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
General Settings						
Hostname	<input type="text" value="Case"/>					
User LED Type	<input type="text" value="None"/>					
Time Zone Settings						
Time Zone	<input type="text" value="UTC+08:00"/>					
Customized Time Zone	<input type="text"/> ⓘ					
Time Synchronisation						
Enable	<input checked="" type="checkbox"/>					
Primary NTP Server	<input type="text" value="pool.ntp.org"/>					
Secondary NTP Server	<input type="text" value="1.pool.ntp.org"/>					

System->General

- **Hostname**
User-defined router name, which might be use for IPSec local ID identify.
- **User LED Type**
Defined the User LED behavior.
- **Time Zone**
Select the zone where the device is in use.
- **Customized Time Zone**
Customized the zone where the device is in use.
- **Enable (NTP Client)**
Selected Enabled to utilize the NTP client to synchronize the device clock over the network using a time server (NTP server).
- **Primary NTP Server**
Enter the IP address (or host name) of the primary time server.
- **Secondary NTP Server**
Enter the IP address (or host name) of the secondary time server.

General	Accounts	Syslog	Web Server	Telnet	SSH	Security
Account Settings						
Administrator	<input type="text" value="admin"/>					
Old Password	<input type="text"/>					
New Password	<input type="text"/>					
Confirm Password	<input type="text"/>					
Visitor Settings						
Index	Username	Password	⊕			

System->Account

- **Administrator**
Displays the name of current administrator, default as “admin”.
- **Old Password**
Enter the old password of administrator.
- **New Password**
Enter the new password of administrator.
- **Confirm Password**
Confirm the new password of administrator.

Account Settings	
Account Settings	
Index	<input type="text" value="1"/>
Username	<input type="text"/>
Password	<input type="text"/>
<input type="button" value="Save"/> <input type="button" value="Close"/>	

System->Account

- **Username**
Enter a username of visitor privilege
- **Password**
Enter the new password of current visitor account.

The Syslog displays system logs that are stored in the log buffers.

General	Accounts	<u>Syslog</u>	Web Server	Telnet	SSH	Security
General Settings						
	Log Location	<input type="text" value="RAM"/>				
	Log Level	<input type="text" value="Debug"/>				
Remote Syslog Settings						
	Enable Remote Syslog	<input type="checkbox"/>				
	Remote Syslog Server	<input type="text"/>				
	Remote Syslog Port	<input type="text" value="514"/>				

System->Syslog

- **Log Location**
Select the log store location from “RAM” or “Flash”.
- **Log Level**
Select the log output level from “Debug”, “Notice”, “Info”, “Warning” or “Error”.
- **Enable Remote Syslog**
Check this box to enable remote syslog connection.
- **Remote Syslog Server**
Enter the IP address of remote syslog server.
- **Remote Syslog Port**
Enter the port for remote syslog server listening.

General	Accounts	Syslog	<u>Web Server</u>	Telnet	SSH	Security
General Settings						
		HTTP Port	<input type="text" value="80"/>			
		HTTPS Port	<input type="text" value="443"/>			
Certificate Settings						
		Private Key	<input type="text" value="Choose File"/> <input type="text" value="No file chosen"/>	↕		
		Certificate File	<input type="text" value="Choose File"/> <input type="text" value="No file chosen"/>	↕		

System->Web Server

- **HTTP Port**
Enter the port for Hypertext Transfer Protocol. A well-known port for HTTP is port 80.
- **HTTPS Port**
Enter the port for HTTPS Protocol. A well-known port for HTTPS is port 443.
- **Private Key**
Import private Key file for HTTPS connection.
- **Certificate File**
Import certificate file for HTTPS connection.

General	Accounts	Syslog	Web Server	<u>Telnet</u>	SSH	Security
General Settings						
		Telnet Port	<input type="text" value="23"/>			

System->Telnet

- **Telnet Port**
Enter the port for telnet access. The standard port for Telnet is port 23.

General	Accounts	Syslog	Web Server	Telnet	<u>SSH</u>	Security
General Settings						
				SSH Port	<input type="text" value="22"/>	
				Allow Password Authentication	<input checked="" type="checkbox"/>	
				Public Key	<input type="text"/>	

System->SSH

- **SSH Port**
Enter the port for SSH access. The standard port for SSH is port 22.
- **Allow Password Authentication**
Check this box to enable SSH authentication.
- **Public Key**
Enter the public Key SSH authentication.

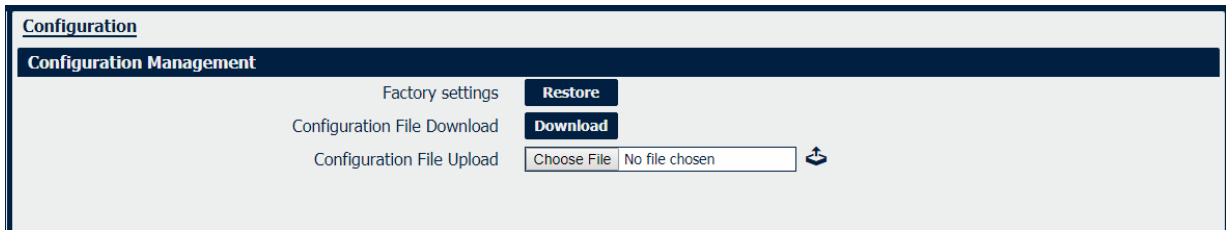
General	Accounts	Syslog	Web Server	Telnet	SSH	<u>Security</u>
Remote Access Settings						
				Remote HTTP Access	<input checked="" type="checkbox"/>	
				Remote HTTPS Access	<input checked="" type="checkbox"/>	
				Remote Telnet Access	<input type="checkbox"/>	
				Remote SSH Access	<input checked="" type="checkbox"/>	

System->Security

- **Remote HTTP Access**
Check this box to allow remote HTTP access.
- **Remote HTTPS Access**
Check this box to allow remote HTTPS access.
- **Remote Telnet Access**
Check this box to allow remote Telnet access.
- **Remote SSH Access**
Check this box to allow remote SSH access.

8.3. Configuration

The 6944 Configuration tab allows you to save parameters (settings in the Web interface) to a file. Conversely, if you have saved settings from the 6944 router to a file, you can Import these previously-saved configuration settings to the 6944 router as well.



System->Configuration

- **Restore**
Reset the unit to factory default settings.
- **Download**
Download the configuration file from the 6944 router.
- **Configuration File Upload**
Import a previously-saved configuration file.

8.4. Debug Tools

<u>Ping</u>	Traceroute	AT Debug
Ping Settings		
	Host Address	<input type="text"/>
	Ping Count	<input type="text" value="5"/>
	Local IP Address	<input type="text"/>

Debug Tools->Ping

- **Host Address**
Enter a host IP address or domain name for ping.
- **Ping Count**
Enter the ping times.
- **Local IP Address**
Enter the ping source IP address or leave it blank.

Ping	<u>Traceroute</u>	AT Debug
Traceroute Settings		
	Host Address	<input type="text"/>
	Max Hops	<input type="text" value="30"/>

Debug Tools->Traceroute

- **Host Address**
Enter a host IP address or domain name for traceroute.
- **Max Hops**
Enter the max hops for traceroute.

Ping	Traceroute	<u>AT Debug</u>
AT Debug Settings		
	AT Command	<input type="text"/>

Debug Tools->AT Debug

- **AT Command**
Enter the AT command of the module.

Appendix A -Glossary

APN:	Access Point Name
GPRS:	General Packet Radio Service
HSPA:	High Speed Packet Access
HSDPA:	High-Speed Downlink Packet Access
HSUPA:	High-Speed Uplink Packet Access
LTE:	3GPP Long Term Evolution
IMEI:	International Mobile Equipment Identity
ICCID:	Integrated Circuit Card Identifier
PIN:	Personal Identification Number
PPP:	Point-to-Point Protocol
RSSI:	Received Signal Strength Indication
SIM:	Subscriber Identity Module
SMS:	Short Message Service
DHCP:	Dynamic Host Configuration Protocol
LAN:	Local Area Network
LED:	Light-Emitting Diode
NTP:	Network Time Protocol
SMA:	SubMiniature version A (connector)
SSID:	Service Set Identifier
TCP/IP:	Transmission Control Protocol / Internet Protocol
UDP:	User Datagram Protocol
VPN:	Virtual Private Network
Wi-Fi or WiFi:	Wireless Fidelity
VDC:	Voltage, Direct Current

Appendix B -Problem Solving

No Signal

Problem

The 6944 Router modem status shows no signal.

Possible Reason

- The Antenna installation is wrong.
- The 6944 Modem has failed

Solution

- Check the LTE antenna or replace with new one.
- Check the cellular page confirm modem is detected correctly or not.

Cannot detect SIM card

Problem

The 6944 Router cannot detect the SIM card, cellular has not failed to connect to base station.

Possible Reason

- SIM card is damaged.
- SIM card has a bad contact.

Solution

- Replace the SIM card.
- Re-install the SIM card.

Poor Signal

Problem

The 6944 Router has no signal or a poor signal.

Possible Reason

- Antenna installation is wrong.
- Area signal weak.

Solution

- Check the antenna and re-connect it.
- Contact Telecom Operator to confirm if there is a signal problem.
- Change to high-gain antenna.

IPSec VPN established, but LAN to LAN cannot communicate**Problem**

IPSec VPN established, but LAN to LAN cannot communicate

Possible Reason

- Both subnets are not compatible
- IPSec second phase (ESP) settings is not match.
- Check your encryption keys are matched
- Does your Firewall support the Tunnel your using (some Firewalls need additional software to run IP Sec)

Solution

- Check the both subnet settings.
- Check IPSec second phase (ESP) setting.
- Double check your encryption keys
- Try connecting to your firewall using the 6944 Ethernet WAN locally to make sure they are compatible

Forgotten your 6944 Router Password**Problem**

Forgotten your 6944 router login password?

Solution

After the router has been powered on, press the 'RESET' button for between 3 to 10 seconds then release it. The router will then manually reboot and reset to factory default settings (Username/Password is admin/admin).