

Case Communications

6944 Industrial Router

Full Manual

With Configuration

Examples



Rev 2.8

This page left blank intentionally

REVISION HISTORY

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

Trademarks and copyright

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@case.uk.com

Web: www.casecomms.com

Interference Issues

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

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

Declaration of Conformity

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



TABLE OF CONTENTS

| | | |
|-----------|--|------------|
| 1. | PRODUCT OVERVIEW | 1-1 |
| 1.1. | Overview | 1-1 |
| 1.2. | Features and Benefits | 1-1 |
| 1.3. | General Specifications | 1-2 |
| 1.4. | Mechanical Specifications | 1-4 |
| 1.5. | Packaging Checklist | 1-4 |
| 2 | INSTALLATION | 2-1 |
| 2.1. | Product Overview | 2-1 |
| 2.2. | LED Indicators | 2-2 |
| 2.3. | Ethernet Port Indicator | 2-2 |
| 2.4. | Ethernet Port Indicator | 2-3 |
| 2.5. | Reset Button | 2-3 |
| 2.6. | Insert SIM card | 2-3 |
| 2.7. | Installing the Antenna | 2-4 |
| 2.8. | DIN-Rail Mounting | 2-4 |
| 2.9. | Protective Grounding Installation | 2-5 |
| 2.10. | Power Supply Installation | 2-5 |
| 2.11. | Powering On The 6944 Router | 2-5 |
| 3 | ACCESSING THE WEB CONFIGURATION | 3-1 |
| 3.1. | PC Configuration | 3-1 |
| 3.2. | Factory Default Settings | 3-2 |
| 3.3. | Logging in to the 6944 Web Page | 3-2 |
| 4 | BASIC BROWSER CONFIGURATION | 4-1 |
| 4.1 | Web Interface Overview | 4-1 |
| 4.1.1. | System Settings | 4-1 |
| 4.1.2. | Status | 4-1 |
| 4.1.3. | Syslog | 4-2 |
| 5 | Link Management | 5-1 |
| 5.1 | Connection Manager | 5-1 |
| 5.2 | Cellular | 5-2 |
| 5.2.1. | Cellular Configuration | 5-2 |
| 5.2.2. | Cellular Configuration Example | 5-4 |
| 5.3. | Configuring Ethernet Ports | 5-6 |
| 5.3.1. | Ethernet port status | 5-6 |
| 5.3.2. | Configuring and Ethernet LAN port | 5-7 |
| 5.3.3. | Configuring and Ethernet WAN Port | 5-7 |
| 5.3.4. | AN021 – Configuring PPPoE | 5-9 |
| 5.4 | VLAN Trunk Settings | 5-12 |
| 5.5 | Port Forwarding | 5-12 |
| 5.6 | RADIUS Authentication (IEEE 802.1x | 5-14 |
| 5.6.1. | How RADIUS Works on the 6944 | 5-14 |

| | | |
|-----------|--|-------------|
| | 5.6.2. RADIUS Configuration | 5-14 |
| 6 | Wi-Fi | 6-1 |
| 6.1 | Wi-Fi Access Point | 6-1 |
| 6.1.1. | Configuring the Wi-Fi Access Point | 6-1 |
| 6.1.2. | Configuring the Wi-Fi Access Point | 6-3 |
| 6.1.3. | Wireless Access Configuration Example | 6-3 |
| 7 | Configuring Resilient Links | 7-1 |
| 7.1 | AN001 Dual SIM Configuration | 7-1 |
| 7.2 | Link Back Up WAN to Cellular | 7-4 |
| 7.3 | AN003 - 3 Link back up WAN, WWAN1 & WWAN 2 | 7-8 |
| 8 | Network Security | 8-1 |
| 8.1. | Firewall and ACL | 8-1 |
| 8.2. | AN028-Configuring SSH with a Public Key | 8-3 |
| 9 | Routing | 9-1 |
| 9.1. | Static Routing | 9-1 |
| 9.2. | Dynamic Routing Using RIP | 9-2 |
| 9.3. | Dynamic Routing Using OSPF | 9-4 |
| 9.4. | Dynamic Routing Using BGP | 9-6 |
| 10 | V.R.R.P | 10-1 |
| 10.1. | Configuring VRRP between Two 6944 Routers | 10-2 |
| 10.2. | Configuring VRRP Between 6944 and Cisco Routers | 10-6 |
| 10.3. | VRRP Between Multiple 6944 Routers | 10-9 |
| 11 | VPN (Virtual Private Networks) | 11-1 |
| 11.1. | OpenVPN Introduction | 11-1 |
| 11.2. | Example Configuration VPN a 6944 Client and PC running as an Open VPN Server | 11-4 |
| 11.3. | AN006 – 6944 Open VPN Client with X.509 Certificate. | 11-7 |
| 11.4. | AN016- How to generate the certificates for OpenVPN on Windows OS. | 11-11 |
| 11.5. | AN007-Configuring an Open -VPN Client with a Pre-shared Key | 11-15 |
| 11.6. | AN008-Open VPN Client with Username and Password | 11-18 |
| 11.7. | AN009-Open VPN Client Running TAP Pre-shared key P2P Mode | 11-24 |
| 11.8 | AN010- OpenVPN Client_with_TAP_under_P2P_mode | 11-27 |
| 11.9. | AN011-OpenVPN with TUN and X.509 certificate P2P Mode | 11-31 |
| 11.10. | AN050-6944 as an Open VPN Server with X.509 Certificate | 11-34 |
| 11.11. | AN57-Open VPN between 6944 routers with X.509Certificate. | 11-38 |
| 11.12. | AN058-Open VPN using passwords between two 6944's | 11-42 |
| 12 | IP SEC | 12-1 |
| 12.1. | IP Sec Overview | 12-1 |
| 12.2. | AN012 – IP Sec with Pre-Shared Key to Cisco | 12-4 |
| 12.3. | AN013 - IP Sec and FQDN to a Cisco router | 12-7 |
| 12.4. | AN014 -IP Sec with Pre-Shared Key to a Cisco Router | 12-10 |
| 12.5. | AN015 - IP Sec with a Pre-shared Key to Cisco Router | 12-13 |
| 13 | GRE Generic Routing Encapsulation | 13-1 |
| 13.2. | AN056- GRE VPN Redundancy to Cisco Router | 13-5 |

| | | |
|------------|--|-------------|
| 14 | Layer Two Tunneling Protocol (L2TP) | 14-1 |
| 14.1. | AN044_L2TP_between_two_6944_Routers | 14-1 |
| 14.2. | AN045-L2TP Server to Windows Operating System | 14-4 |
| 14.3. | AN046 - 6944 L2TP Client to Cisco L2TP Server | 14-9 |
| 15 | Point to Point Tunneling Protocol (PPTP) | 15-1 |
| 15.1. | AN 051 PPTP Client to CISCO Server | 15-1 |
| 15.2. | AN052 6944 PPTP Server to Windows PC | 15-4 |
| 16 | Configuring DMVPN on the 6944 | 16-1 |
| 16.1. | AN029 Configuring DMVPN with RIP to a Cisco Router | 16-1 |
| 16.2. | AN030-Configuring DMVPN with OSPF | 16-4 |
| 16.3. | AN031 - Configuring DMVPN with BGP to a Cisco Router | 16-8 |
| 17 | IP Pass through | 17-1 |
| 18 | Industrial Interface. | 18-1 |
| 18.1. | Industrial Interface Overview on the 6944 | 18-1 |
| 18.2. | AN004 Transparent Mode with TCP Client on RS232 | 18-5 |
| 18.3. | AN005 RS485 Transparent Mode | 18-8 |
| 19. | Digital I / O Ports | 19-1 |
| 19.1 | Digital Input Port | 19-1 |
| 19.2. | Digital Output | 19-1 |
| 20 | MODBUS | 20-1 |
| 20.1 | MODBUS Slave | 20-1 |
| 20.2 | MODBUS Master | 20-8 |
| 20.3 | MODBUS to DNP3 | 20-16 |
| 20.4 | AN053 IEC 101 to IEC 104 | 20-20 |
| 21 | AT Commands | 21-1 |
| 21.1. | AT Over IP | 21-1 |
| 21.2. | AT Over Telnet | 21-5 |
| 21.3. | AT Over COM | 21-7 |
| 22. | SMS Commands | 22-1 |
| 22.1. | SMS Control | 22-5 |
| 22.2 | SMS Gateway | 22-7 |
| 22.3 | SMS Notification | 22-9 |
| 23 | SNMP | 23-1 |
| 24. | TR069 management platform | 24-1 |
| 25. | Maintenance | 25-1 |
| 25.1. | Upgrade via Uboot | 25-1 |
| 25.2. | Scheduled Reboot | 25-3 |

This page left blank intentionally

1. PRODUCT OVERVIEW

1.1. Overview

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

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

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

1.2. Features and Benefits

Industrial internet access

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

Designed for industrial usage

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

Secure and reliable remote connection

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

Easy to use and easy maintenance

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

1.3. General Specifications

Cellular Interface

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

Wi-Fi Interface (Optional)

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

Ethernet Interface

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

Serial Interface

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

DI/DO Interface

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

DI/DO Interface

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

Other Interfaces

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

Software

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

Power Supply and Consumption

- Connector: 3-pin 3.5 mm female socket with lock
- Input voltage range: 9~48VDC
- Power consumption:
Idle: 100 mA@12V
Data link: 400 mA (peak) @12V

Physical Specification

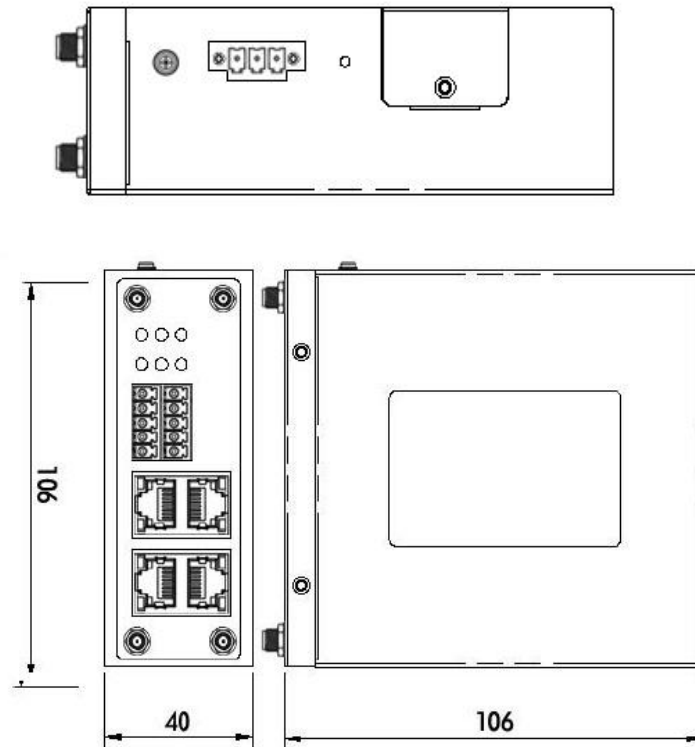
- Ingress Protection: IP30
- Housing & Weight: Metal, 300g
- Dimension: 104mm x 104mm x 38mm (excluding antenna)
- Installations: Din-rail mounting

Environmental

- Operation temperature: -40~+75°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)



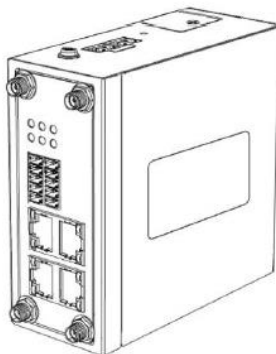
1.5. Packaging Checklist

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

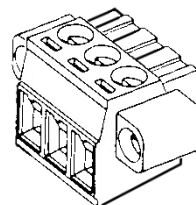
NOTE: if any of the below items is missing or damaged, please contact your sales representative.

Equipment Included

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

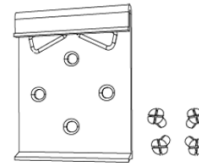
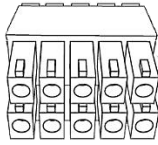


- 1 x 10-pin 3.5 mm male terminal block for RS232/RS485/DI/DO

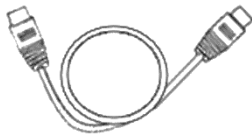


- 1 x 3-pin 3.5 mm male terminal block with lock for power supply

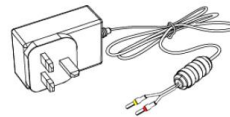
- 35mm Din-rail mounting kit



- 1 x Ethernet cable



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



- 1 x Quick Start Guide



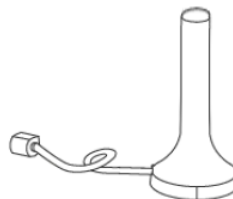
Optional Accessories (sold separately)

- 3G/4G cellular antenna

Stubby antenna



Magnet antenna



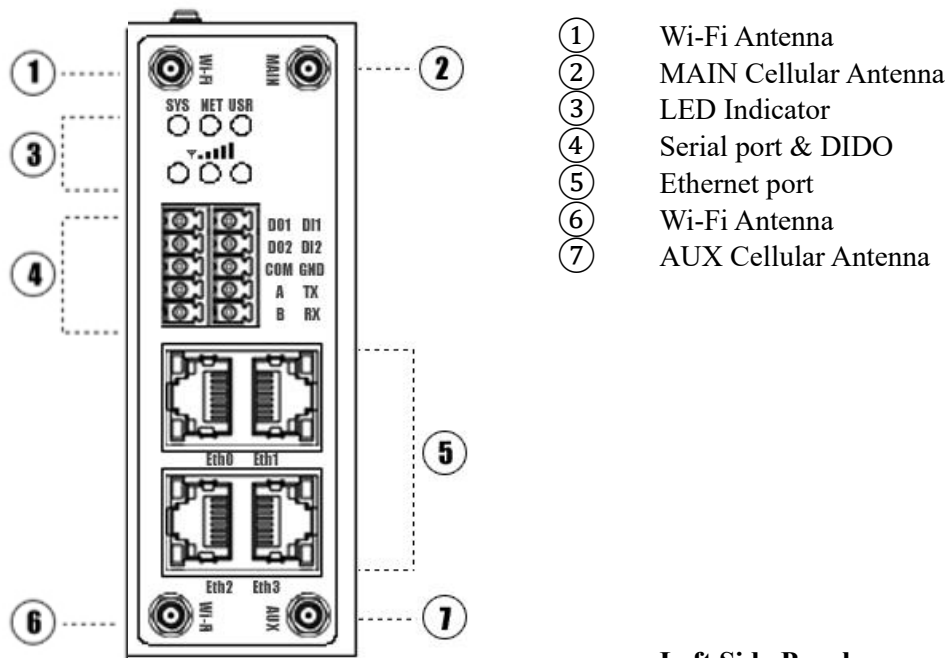
This page left blank intentionally

| | |
|--------------|-------------|
| Section Two | 6944 Manual |
| Installation | Rev 2.8 |

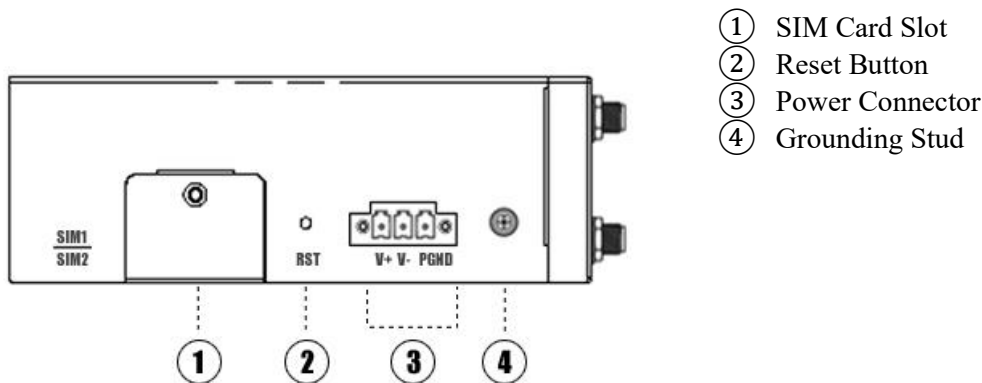
2 INSTALLATION

2.1. Product Overview

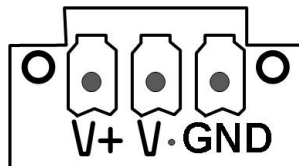
- Front Panel



- Left Side Panel




- Power Input



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

2.2. LED Indicators

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

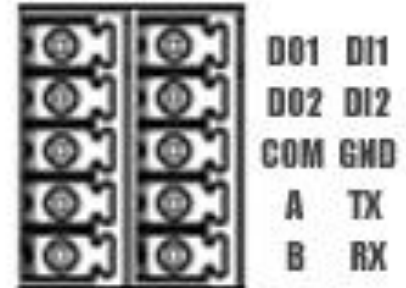
2.3. Ethernet Port Indicator

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

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

2.4. Ethernet Port Indicator

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



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

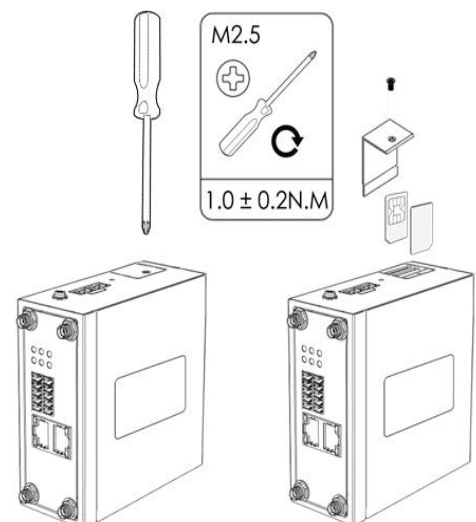
2.5. Reset Button

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

2.6. Insert SIM card

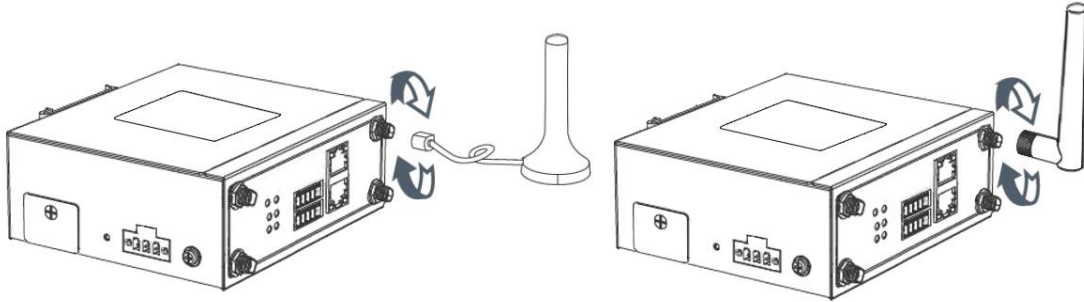
• Insert / Remove SIM card

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



2.7. Installing the Antenna

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

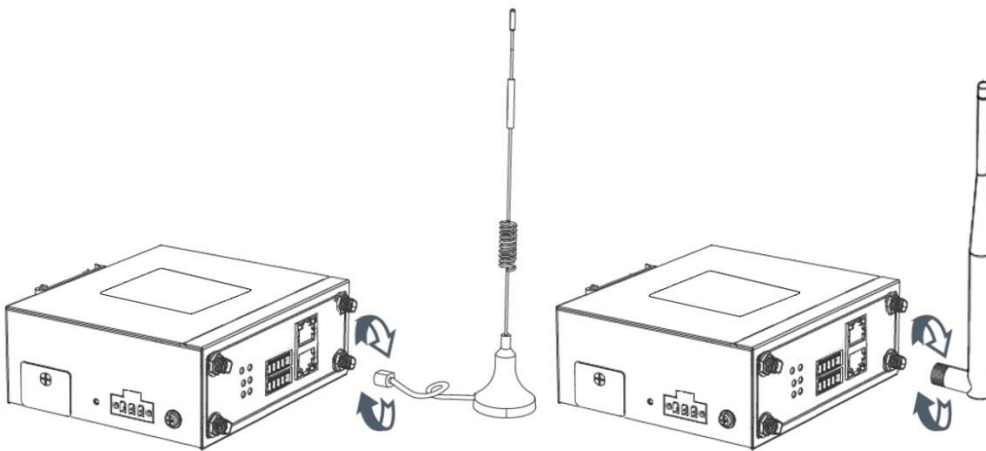


NOTE: The 6944 router supports dual antennas with MAIN and AUX connectors. The MAIN connector is for receiving and transmitting data. The AUX connector is for enhancing the signal strength, and should be used with the MAIN Antenna.

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

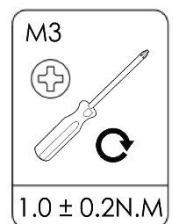
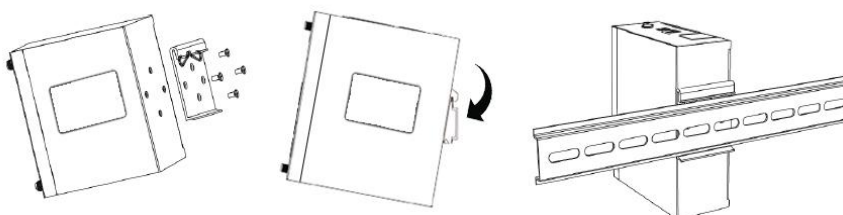
Please follow the picture below to install the Wi-Fi antenna in the right position before testing.

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



2.8. DIN-Rail Mounting

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

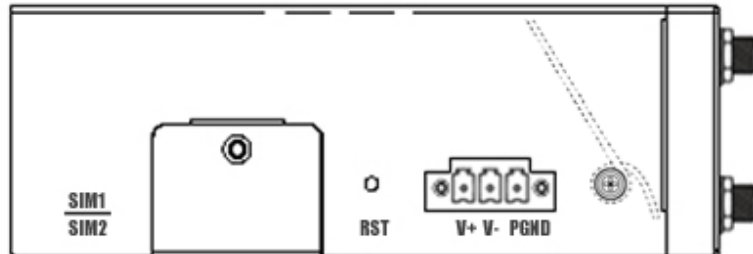


| | |
|--------------|-------------|
| Section Two | 6944 Manual |
| Installation | Rev 2.8 |

2.9. Protective Grounding Installation

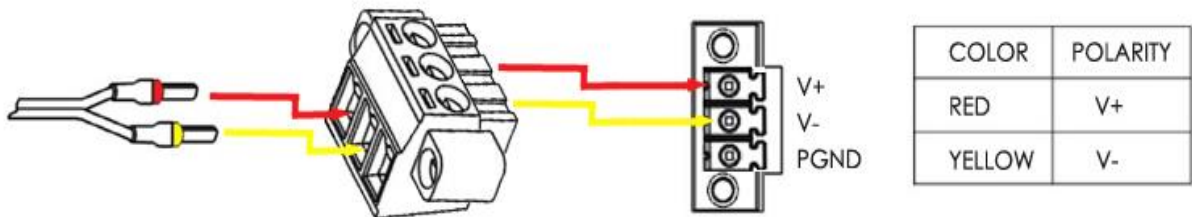
1. Remove the grounding nut.
2. Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.

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.

This page left blank intentionally

3. ACCESSING THE WEB CONFIGURATION

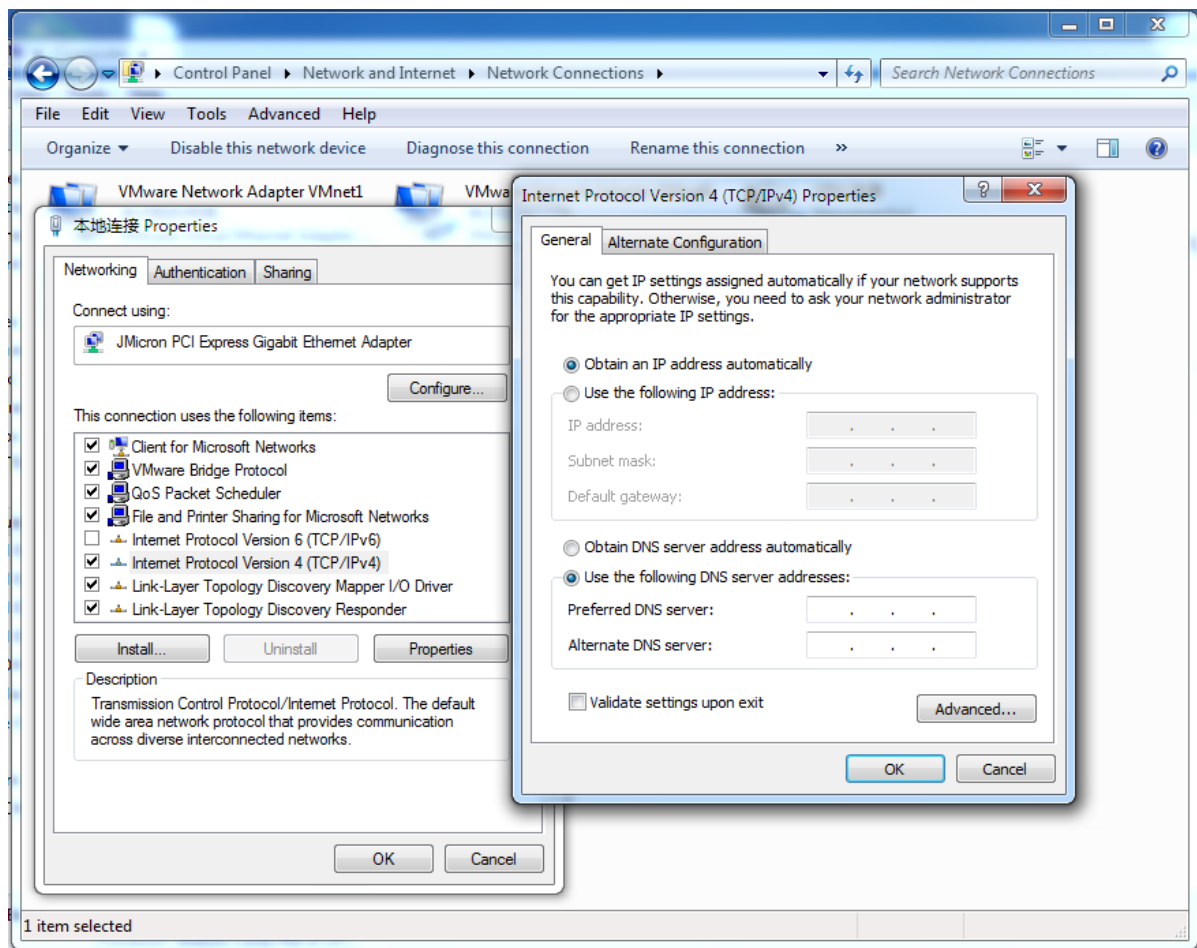
3.1. PC Configuration

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

- **Obtain an IP address automatically**

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

NOTE: The following steps are based on Windows 7.



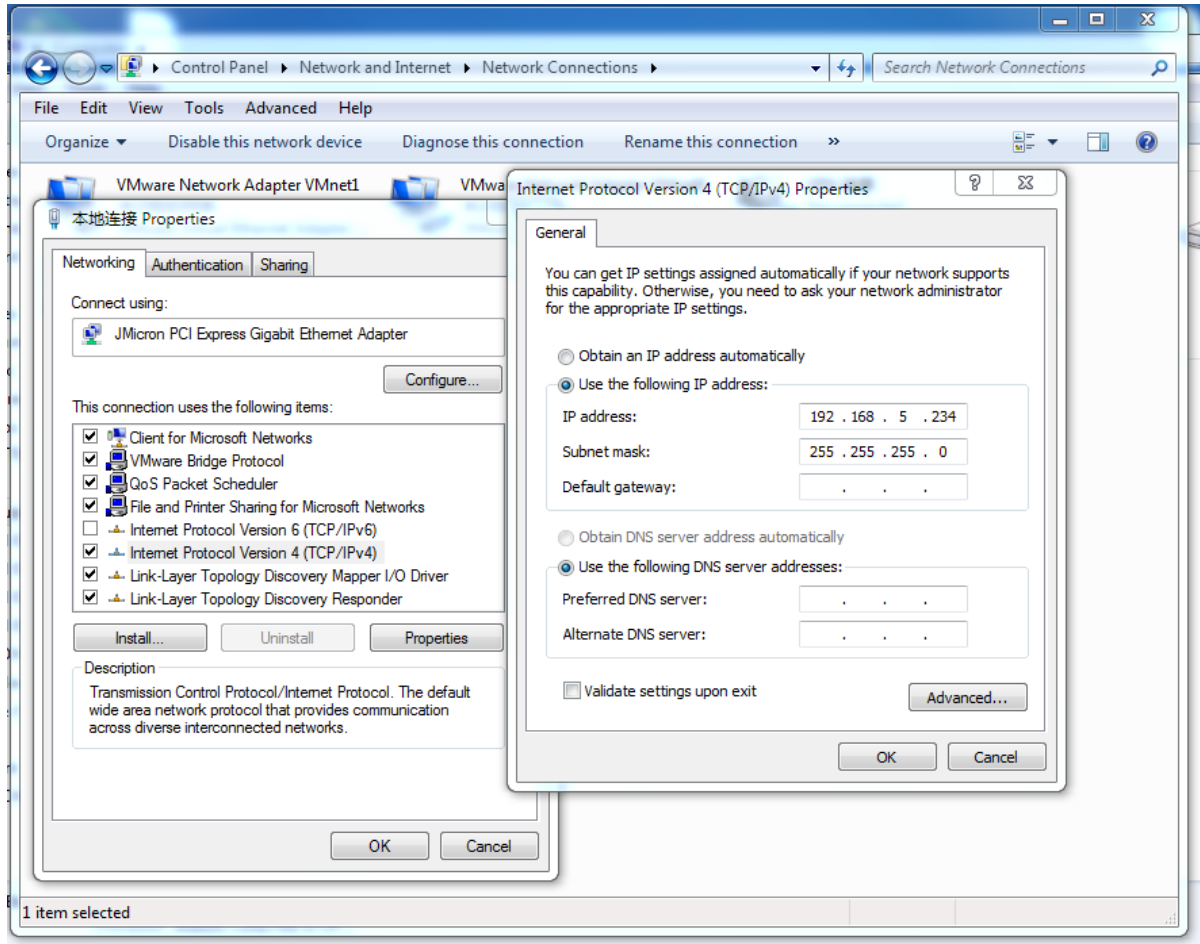
Select **Start » Control Panel » Network Connections**.

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

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

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

- **Set a static IP address**



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

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

3.2. Factory Default Settings

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

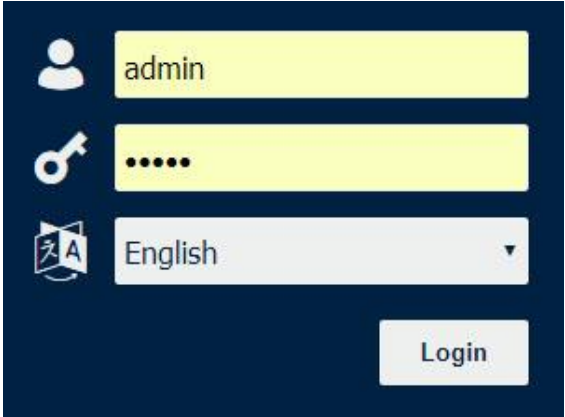
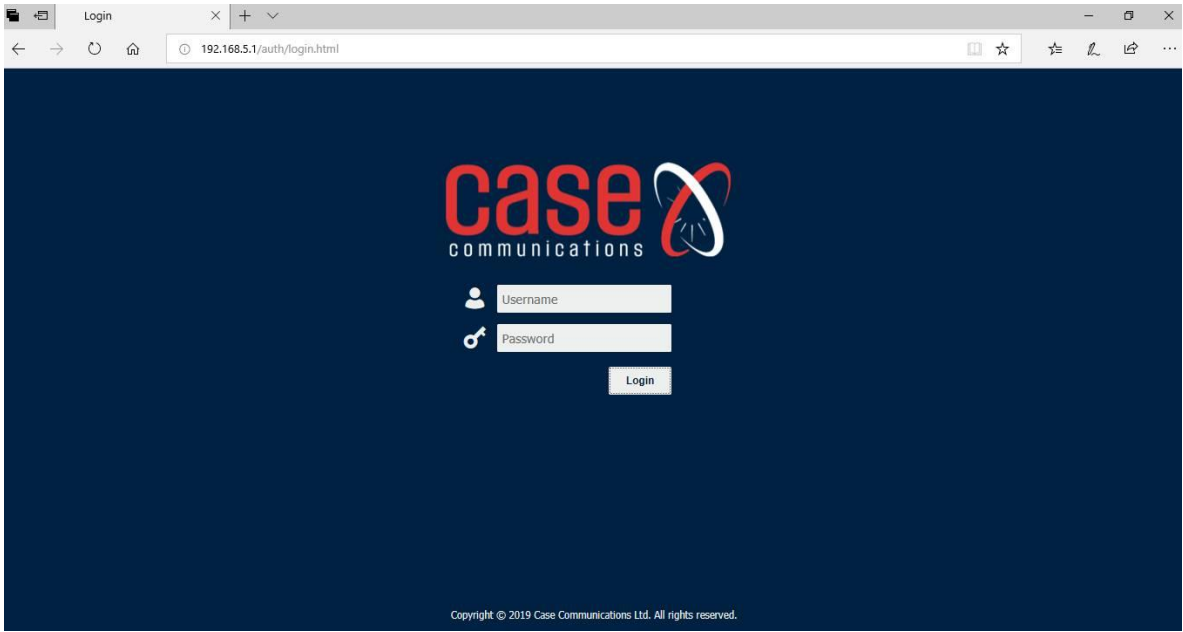
- Username: **admin**
- Password: **admin**
- LAN IP Address: **192.168.5.1** (Eth0~Eth1/Eth3 bridge as LAN mode)
- DHCP Server: **Enabled**

3.3. Logging in to the 6944 Web Page

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

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

| | |
|---------------------------------|-------------|
| Section Three | 6944 Manual |
| Accessing the web configuration | Rev 2.8 |

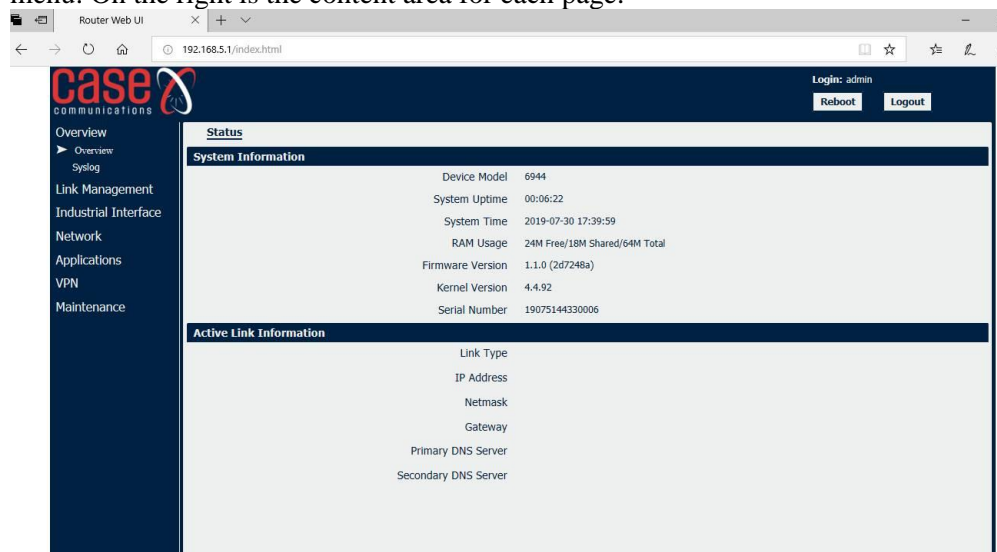


This page left blank intentionally

4. BASIC BROWSER CONFIGURATION

4.1 Web Interface Overview

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



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

4.1.1. System Settings

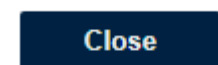
- **Reboot:** reset the router within power disconnect.
- **Logout:** logout to web authorization page.



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



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



4.1.2. Status

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

| Status | |
|--------------------|-------------------------------|
| 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 |

| | |
|-----------------------------|-------------|
| Section Four | 6944 Manual |
| Basic Browser Configuration | Rev 2.8 |

System Information

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

Active Link Information

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

4.1.3. Syslog

Syslog Information

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

The screenshot shows the Case Communications web interface. On the left is a navigation menu with options: Overview, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance. The main content area is titled 'Syslog' and 'Events'. Below this is a 'Syslog Information' section displaying a list of syslog messages. At the bottom of the page, there are four buttons: 'Download Diagnosis', 'Download Syslog', 'Clear', and 'Refresh'.

Syslog Messages:

```

Jul 30 17:34:00 casecomms syslog.info syslogd started: BusyBox v1.25.1
Jul 30 17:34:05 casecomms daemon.info dnsmasq[1738]: started, version 2.78 cachesize 150
Jul 30 17:34:05 casecomms daemon.info dnsmasq[1738]: compile time options: no-IPv6 GNU-getopt no-DBus no-IDN DHCP no-DHCPv6 no-Lua TFTP
no-contrack no-ipset no-auth no-DNSSEC no-ID loop-detect notify
Jul 30 17:34:05 casecomms daemon.info dnsmasq-dhcp[1738]: DHCP, IP range 192.168.5.2 -- 192.168.5.200, lease time 2h
Jul 30 17:34:05 casecomms daemon.info dnsmasq-dhcp[1738]: DHCP, sockets bound exclusively to interface lan0
Jul 30 17:34:05 casecomms daemon.warn dnsmasq[1738]: no servers found in /etc/resolv.conf, will retry
Jul 30 17:34:05 casecomms daemon.info dnsmasq[1738]: read /etc/hosts - 2 addresses
Jul 30 17:34:05 casecomms user.debug connection_manager[1724]: setup SIM 1 as initial SIM
Jul 30 17:34:05 casecomms user.debug connection_manager[1724]: wwan1 start connect
Jul 30 17:34:05 casecomms user.debug connection_manager[1724]: waiting for modem to initialize using SIM 1
Jul 30 17:34:06 casecomms local0.debug webserver: webserver started
Jul 30 17:34:06 casecomms user.debug modem[1789]: modem init with SIM1
Jul 30 17:34:07 casecomms user.debug modem[1789]: modem power-on successfully
Jul 30 17:34:07 casecomms user.debug modem[1789]: ATZ
Jul 30 17:34:07 casecomms user.debug modem[1789]: ATZ^M
Jul 30 17:34:07 casecomms user.debug modem[1789]: OK
Jul 30 17:34:08 casecomms user.debug modem[1789]: AT+CPIN?
Jul 30 17:34:08 casecomms user.debug modem[1789]: +CME ERROR: 10
Jul 30 17:34:10 casecomms user.debug modem[1789]: AT+CPIN?
Jul 30 17:34:10 casecomms user.debug modem[1789]: +CME ERROR: 10
Jul 30 17:34:11 casecomms cron.info crond[1928]: crond (busybox 1.25.1) started, log level 8
Jul 30 17:34:12 casecomms daemon.info procd: - init complete -
Jul 30 17:34:12 casecomms user.debug modem[1789]: AT+CPIN?
Jul 30 17:34:12 casecomms user.debug modem[1789]: +CME ERROR: 10
Jul 30 17:34:14 casecomms user.debug modem[1789]: AT+CPIN?
Jul 30 17:34:14 casecomms user.debug modem[1789]: +CME ERROR: 10
Jul 30 17:34:16 casecomms user.debug modem[1789]: AT+CPIN?
  
```





5 Link Management


This section shows you the setup of link management.


Connection Manager->Status

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

5.1 Connection Manager

| 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 | |
|----------------------------------|-------------------------------------|
| General Settings | |
| Priority | 3 |
| Enable | <input checked="" type="checkbox"/> |
| Connection Type | WWAN1 |
| Description | |
| ICMP Detection Settings | |
| Enable | <input checked="" type="checkbox"/> |
| Primary Server | 8.8.8.8 |
| Secondary Server | 114.114.114.114 |
| Interval | 300 ? |
| Retry Interval | 5 ? |
| Timeout | 3 ? |
| Retry Times | 3 ? |
| <div>Save</div> <div>Close</div> | |

Connection Settings

- **Priority**
Displays current index on the priority list.
- **Connection Type**
Select the available interface as outbound link.
NOTE: specify SIM1 carrier link as WWAN1, SIM2 carrier link as WWAN2.
- **ICMP Detection Settings->Enable**
Check this box to detect link connection status based on pings to a specified IP address.
- **Primary Server**
Enter the primary IP address to send the pings to, to detect the link state. Recommend entering the IP address of known external reachable server or network (e.g. 8.8.8.8 (Google)).
- **Secondary Server**
Enter the secondary IP address to send the pings to, if the primary server ping fails, the 6944 will try to ping the secondary server.
- **Interval**
The duration of each ICMP detection in seconds.
- **Retry Interval**
The interval in seconds between each ping if no packets have been received.
- **Timeout**
Enter timeout for received ping reply to determine the ICMP detection failure.
- **Retry Times**
Specify the retry times for ICMP detection.

5.2 Cellular

5.2.1. Cellular Configuration

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

| 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 | 6016C02 | | | | |
| | | | | IMSI | 460015956236598 | | | | |
| | | | | TX Bytes | 2992 | | | | |
| | | | | RX Bytes | 2748 | | | | |
| | | | | Modem Firmware | EC25EFAR06A01MHG | | | | |

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 | |
| 2 | SIM2 | true | |

| Cellular |
|---|
| <ul style="list-style-type: none"> • SIM Card - Displays the SIM card support on this unit. • Auto APN - Displays the Enable status of auto APN function. |
| SIM Card Settings |
| <ul style="list-style-type: none"> • SIM Card - Displays the current SIM card settings • Auto APN - Check this box enable auto checking the Access Point Name provided by the carrier. • Dial Number - Enter the dial number of the carrier. • Authentication Type - Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP. • PIN Cod - Enter a 4-8 characters PIN code to unlock the SIM. • Monthly Data Limitation - Enter the data total amount for SIM card, SIM card switchover when data reach limitation. • Override Primary DNS - Enter the primary DNS server will override the automatically obtained DNS. • Network Type - Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.). • Use All Bands - Check this box to enable all bands selection or choose specified bands. |

SIM Card Settings

Modem General Settings

Index

1

SIM Card

SIM1

Auto APN

☒

Dial Number

*99#

Authentication Type

Auto

PIN Code

Monthly Data Limitation

0

Monthly Billing Day

1

Data Roaming

☒

Override Primary DNS

Override Secondary DNS

Modem Network Settings

Network Type

Auto

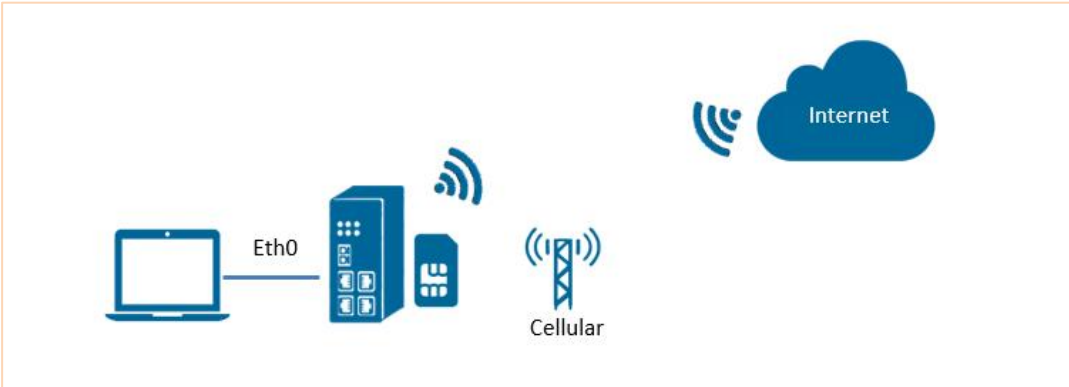
Use All Bands

☒

Save

Close

5.2.2. Cellular Configuration Example
Topology for the cellular connection test



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

6944 Cellular Configuration

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

case

communications

Overview

Link Management

Connection Manager

Cellular

Ethernet

WiFi

Status

Cellular

Modem General Settings

| Index | SIM Card | Auto APN |
|-------|----------|----------|
| 1 | SIM1 | true |
| 2 | SIM2 | true |

Login: admin

Reboot

Logout

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

| | |
|-----------------|-------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

Step 3: Click Save>Apply.

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

Step 5: Setup the parameters of WWAN1 as below:

Step 6: Click Save>Apply.

6944 Testing the Cellular Connection

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

| Active Link Information | |
|-------------------------|-----------------|
| Link Type | WWAN1 |
| IP Address | 10.164.172.139 |
| Netmask | 255.255.255.248 |
| Gateway | 10.164.172.140 |
| Primary DNS Server | 120.80.80.80 |
| Secondary DNS Server | 221.5.88.88 |

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

5.3. Configuring Ethernet Ports

5.3.1. Ethernet port status

| 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**

Ethernet->Port Assignment

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

| Port Settings | |
|--|-----------------------------------|
| General Settings | |
| Index | <input type="text" value="1"/> |
| Port | <input type="text" value="Eth0"/> |
| Interface | <input type="text" value="WAN"/> |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

Ethernet->Port Settings

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

| Status | Port Assignment | WAN | LAN | VLAN |
|------------------------|-----------------|-------------------------------------|-----|------|
| General Settings | | | | |
| Connection Type | | <input type="text" value="DHCP"/> | | |
| Advanced Settings | | | | |
| NAT Enable | | <input checked="" type="checkbox"/> | | |
| MTU | | <input type="text" value="1500"/> | | |
| Override Primary DNS | | <input type="text"/> | | |
| Override Secondary DNS | | <input type="text"/> | | |

| | |
|-----------------|-------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

5.3.2. Configuring an Ethernet LAN port

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.

5.3.3. Configuring and Ethernet WAN Port

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

Ethernet->WAN

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

| | |
|------------------------|--------------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

| Status | Port Assignment | <u>WAN</u> | LAN | VLAN |
|-------------------------|-----------------|-----------------|----------------------|------|
| General 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"/> | |

| Status | Port Assignment | <u>WAN</u> | LAN | VLAN |
|-------------------------|-----------------|---------------------|----------------------|------|
| General Settings | | | | |
| | | Connection Type | PPPoE ▼ | |
| | | Authentication Type | Auto ▼ | |
| | | 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.

| | |
|-----------------|-------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

LAN Settings

General Settings

Index 1
Interface LAN0
IP Address 192.168.5.1
Netmask 255.255.255.0
MTU 1500

DHCP Settings

Enable ☒
Mode Server
IP Pool Start 192.168.5.2
IP Pool End 192.168.5.200
Netmask 255.255.255.0
Lease Time 120
Gateway
Primary DNS
Secondary DNS
WINS Server

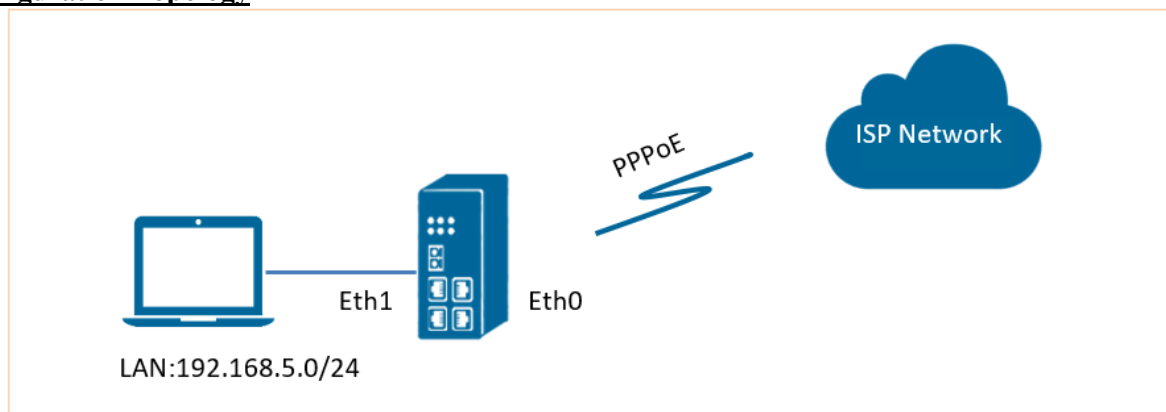
Save Close

DHCP Settings

Enable ☒
Mode Relay
Relay Server

Save Close

5.3.4. AN021 – Configuring PPPoE Configuration Topology

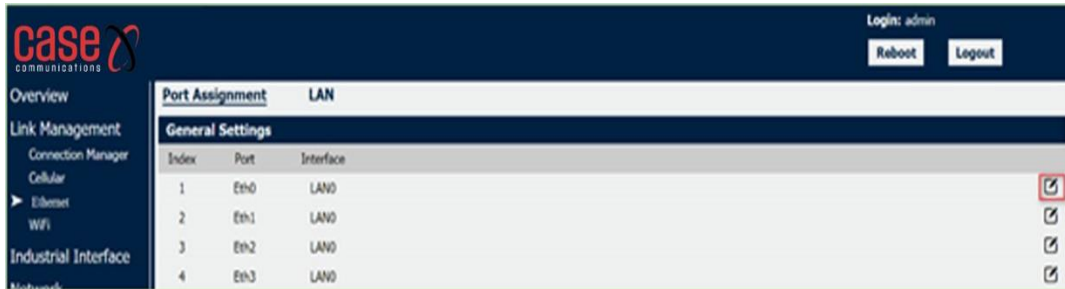


- Set Eth0 on the 6944 as a WAN Port and connect to the internet using PPPoE
- ETH1 works as a LAN Interface, enable the 6944 DHCP Server, and connect your PC allowing the 6944 to give it an IP Address.

Configuration Steps

Ethernet Configuration

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



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



Step 3: Click Save>Apply.

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

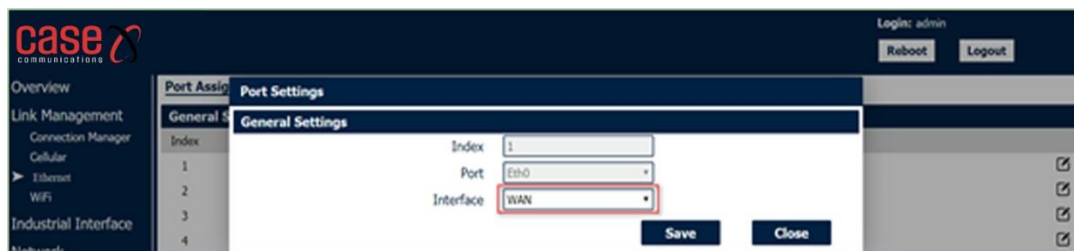
| Port Assignment | WAN | LAN |
|--|-----|-----|
| General Settings | | |
| Connection Type: PPPoE Authentication Type: Auto Username: GZHZFTTH@16900.gd Password: 16900 | | |
| Advanced Settings | | |
| NAT Enable: <input checked="" type="checkbox"/> MTU: 1500 Override Primary DNS: <input type="text"/> Override Secondary DNS: <input type="text"/> | | |

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

Step 5: Click Save>Apply.

Primary Link configuration

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



Step 2: Configure the WAN parameters as shown below:

Connection Settings

Connection Information

Priority: 1

Enable: ☒

Connection Type: WAN

Description:

ICMP Detection Settings

Enable: ☒

Primary Server: 8.8.8.8

Secondary Server: 114.114.114.114

Interval: 300

Retry Interval: 5

Timeout: 3

Retry Times: 3

Save Close

Testing

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

| Active Link Information | |
|-------------------------|-----------------|
| Link Type | WAN |
| IP Address | 10.8.151.39 |
| Netmask | 255.255.255.255 |
| Gateway | 10.8.128.1 |
| Primary DNS Server | 116.116.116.116 |
| Secondary DNS Server | 221.5.88.88 |

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

case
communications

Ping Traceroute

Ping Settings

Host Address: 8.8.8.8

Ping Count: 5

Local IP Address:

PING 8.8.8.8 (8.8.8.8): 56 data bytes
 64 bytes from 8.8.8.8: seq=0 ttl=39 time=21.422 ms
 64 bytes from 8.8.8.8: seq=1 ttl=39 time=21.083 ms
 64 bytes from 8.8.8.8: seq=3 ttl=39 time=20.962 ms
 64 bytes from 8.8.8.8: seq=4 ttl=39 time=21.033 ms

--- 8.8.8.8 ping statistics ---
 5 packets transmitted, 4 packets received, 20% packet loss
 round-trip min/avg/max = 20.962/21.125/21.422 ms

Step 3. Test successful.

Multiple IP Settings

General Settings

Index: 1

Interface: LAN0

IP Address:

Netmask:

Save Close

Ethernet->LAN->Multiple IP Settings

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

5.4 VLAN Trunk Settings

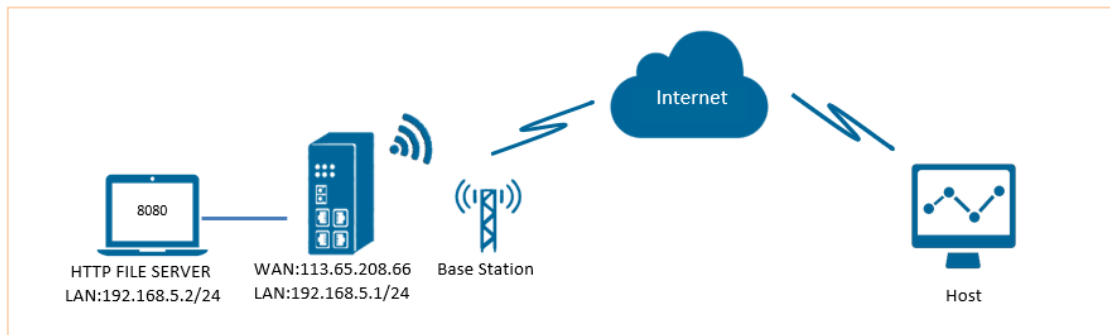
| Trunk Settings | |
|----------------------------------|------|
| VLAN Trunk Settings | |
| Index | 1 |
| Interface | LAN0 |
| VID | 10 |
| IP Address | |
| Netmask | |
| <div>Save</div> <div>Close</div> | |

Ethernet->VLAN->VLAN Trunk Settings

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

5.5 Port Forwarding

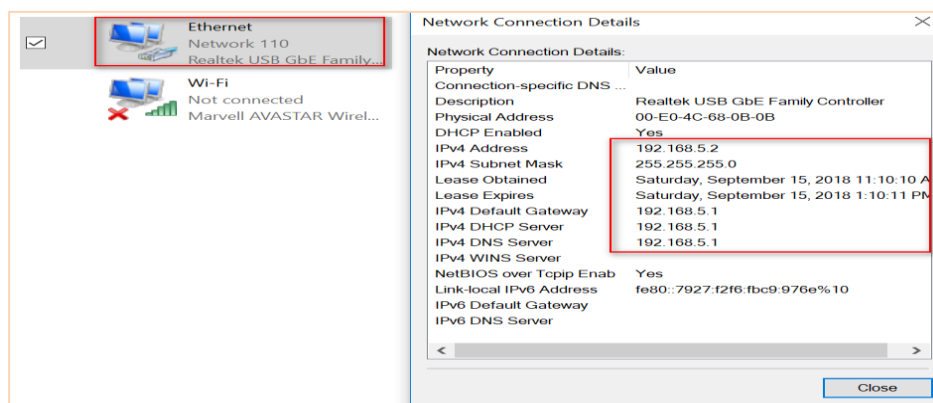
Testing Topology



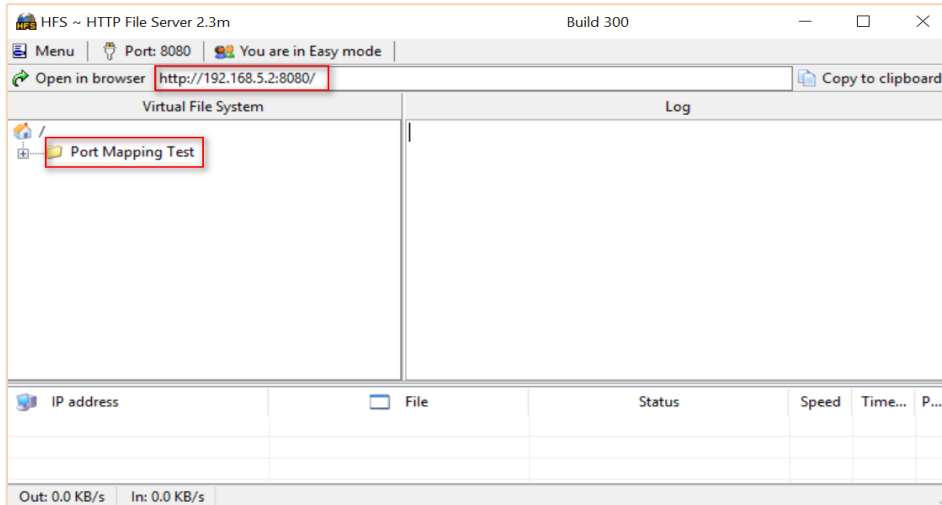
- The Case Communications 6944 works with a fixed public IP address.
- A remote host works with a PC, which can communicate with the Internet and reach the 6944
- The remote host access HTTP FILE SERVER behind 6944 via Port Mapping.

HTTP File Server Configuration

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

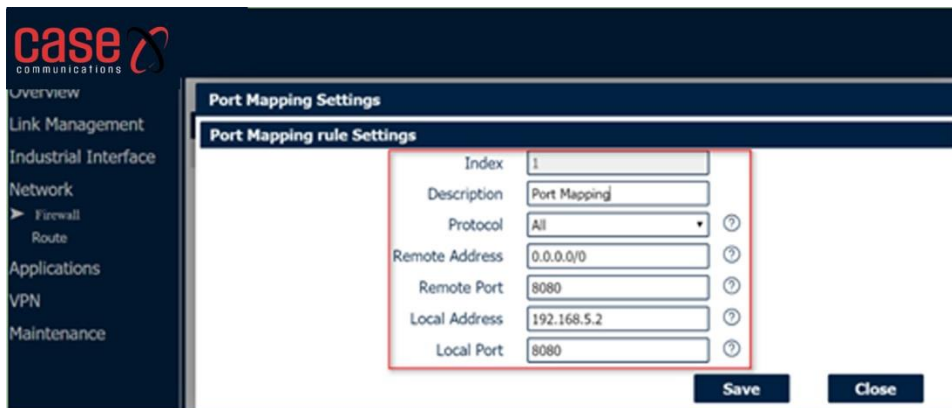


Step 2. Enable HTTP FILE SERVER on the PC.



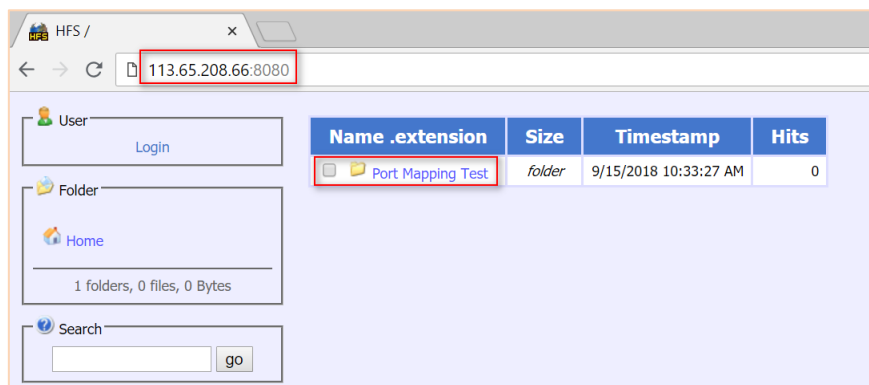
Port Mapping Configuration

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



Testing

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



Step 2: Test successful

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

| | |
|------------------------|--------------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

5.6 RADIUS Authentication (IEEE 802.1x)

RADIUS - IEEE 802.1x

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

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

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

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

5.6.1 How RADIUS Works on the 6944

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


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

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

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

5.6.2 RADIUS Configuration

Go to **Link Management>Ethernet>LAN**, to view the LAN General Settings. Select the required

LAN interface and click the  icon to edit the interface. Under IEEE 802.1X Authenticator Settings select Enable with a tick to expand all RADIUS settings.

| | |
|-----------------|-------------|
| Section Five | 6944 Manual |
| Link Management | Rev 2.8 |

IEEE 802.1X Authenticator Settings

Enable ☒

Reauthentication Period ?

Use PAE Group Address ☐

Authentication Server Settings

Radius Server Address

Radius Server Port

Radius Secret

Enable Verbose Log ☐

IEEE 802.1X Authenticator Settings

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

Authentication Server Settings

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

This page left blank intentionally

6 Wi-Fi

6.1 Wi-Fi Access Point

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

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

| 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 | AP | |
| Country Code | UK | |

Wi-Fi->Basic

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

5.7 Configuring the Wi-Fi Access Point

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

| Status | Basic | WiFi AP |
|-----------------------------|-------------------------------------|---------|
| WiFi AP Settings | | |
| Enable | <input checked="" type="checkbox"/> | |
| SSID | wifi-a-p | |
| Enable Broadcast SSID | <input type="checkbox"/> | |
| Security Mode | WPA PSK | |
| WPA Type | Auto | |
| Encryption Type | Auto | |
| Password | | |
| Advanced Settings | | |
| Channel | Auto | |
| Wireless Mode | 802.11bgn | |
| Channel Width | 40 MHz | |
| Beacon TX Rate HT MCS Index | Auto | |
| TX Power | High | |
| Beacon Interval | 100 | |
| DTIM Period | 100 | |
| Max Client Support | 64 | |
| Enable Short GI | <input checked="" type="checkbox"/> | |
| Enable AP Isolate | <input type="checkbox"/> | |

| | |
|---------------------|-------------|
| Section Six | 6944 Manual |
| Wi-Fi Configuration | Rev 2.8 |

Wi-Fi->Wi-Fi AP

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

| | |
|---------------------|-------------|
| Section Six | 6944 Manual |
| Wi-Fi Configuration | Rev 2.8 |

5.8 Configuring the Wi-Fi Access Point

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

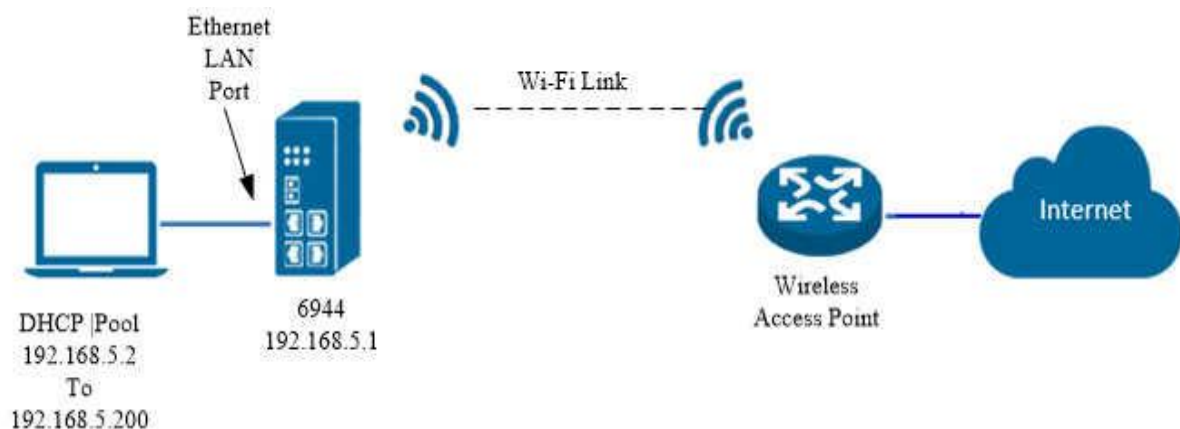
| Status | Basic | WiFi Client |
|---|-------|-------------|
| WiFi Client Settings | | |
| Enable <input checked="" type="checkbox"/> | | |
| Connect to Hidden SSID <input type="checkbox"/> | | |
| SSID <input type="text"/> | | |
| Password <input type="text"/> | | |
| IP Address Settings | | |
| Connection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

Wi-Fi->Wi-Fi Client

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

5.9 Wireless Access Configuration Example

Testing Topology



| | |
|---------------------|-------------|
| Section Six | 6944 Manual |
| Wi-Fi Configuration | Rev 2.8 |

Configuring Wi-Fi

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

| 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"/> |

| Overview | Status | Basic | WiFi Client |
|------------------------|-----------------------|-------|-------------|
| Link Management | Basic Settings | | |
| Connection Manager | Running Mode | | Client |
| Cellular | Country Code | | UK |
| Ethernet | | | |
| ► WiFi | | | |

Step 2: Select Running Mode as Client and set the correct Country code.

Step 3: Click on **Save** and then **Apply**.

Step 4: Click on **Wi-Fi Client**

| Overview | Status | Basic | WiFi Client |
|------------------------|-----------------------------|-------|-------------------------------------|
| Link Management | WiFi Client Settings | | |
| Connection Manager | Enable | | <input checked="" type="checkbox"/> |
| Cellular | Connect to Hidden SSID | | <input type="checkbox"/> |
| Ethernet | SSID | | Case_Guest_Engineering |
| ► WiFi | Password | | ***** |
| Industrial Interface | IP Address Settings | | |
| Network | Connection Type | | DHCP |
| Applications | | | |

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

Step 6: Enter the SSID name and Password

Select the required Connection Type, Probably DHCP or a Static IP Address can be used, but only if a known, free IP address is available on the router or access point.

Step 7: Click on **Save** and then **Apply**.

Step 8: Click on **Status** and after a little time the 6944 should connect.

| Overview | Status | Basic | WiFi Client |
|------------------------|--------------------|------------------------|-------------|
| Link Management | WiFi Status | | |
| Connection Manager | Status | Connected | |
| Cellular | ESSID | Case_Guest_Engineering | |
| Ethernet | Current Channel | 6 | |
| ► WiFi | Signal | -56 dBm | |
| Industrial Interface | TX Power | 20 dBm | |
| Network | | | |

| | |
|---------------------|-------------|
| Section Six | 6944 Manual |
| Wi-Fi Configuration | Rev 2.8 |

Configuring the Ethernet Ports

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

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

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

Step 2: Edit the LAN settings as required.

Step 3: Click Save and then Apply.

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

Configuring the WAN Ports

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

Step 2: Click to edit the Priority 1 entry.

| Overview | Status | Connection Settings | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|--|--|-------------------------|---|---|---|----------|---|--------|-------------------------------------|-----------------|------|-------------|------|------------|-------------------------------------|--------------------------------|--|--------|-------------------------------------|----------------|---------|------------------|-----------------|----------|-----|----------------|---|---------|---|-------------|---|
| Link Management | General S | General Settings | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| <ul style="list-style-type: none"> Connection Manager Cellular Ethernet WiFi | <table border="1"> <thead> <tr> <th>Priority</th> </tr> </thead> <tbody> <tr> <td>1</td> </tr> <tr> <td>2</td> </tr> </tbody> </table> | Priority | 1 | 2 | <table border="1"> <tbody> <tr> <td>Priority</td> <td>1</td> </tr> <tr> <td>Enable</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Connection Type</td> <td>WLAN</td> </tr> <tr> <td>Description</td> <td>WLAN</td> </tr> <tr> <td>NAT Enable</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td colspan="2">ICMP Detection Settings</td> </tr> <tr> <td>Enable</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Primary Server</td> <td>8.8.8.8</td> </tr> <tr> <td>Secondary Server</td> <td>114.114.114.114</td> </tr> <tr> <td>Interval</td> <td>300</td> </tr> <tr> <td>Retry Interval</td> <td>5</td> </tr> <tr> <td>Timeout</td> <td>3</td> </tr> <tr> <td>Retry Times</td> <td>3</td> </tr> </tbody> </table> | Priority | 1 | Enable | <input checked="" type="checkbox"/> | Connection Type | WLAN | Description | WLAN | NAT Enable | <input checked="" type="checkbox"/> | ICMP Detection Settings | | Enable | <input checked="" type="checkbox"/> | Primary Server | 8.8.8.8 | Secondary Server | 114.114.114.114 | Interval | 300 | Retry Interval | 5 | Timeout | 3 | Retry Times | 3 |
| Priority | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Priority | 1 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enable | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Connection Type | WLAN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Description | WLAN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| NAT Enable | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ICMP Detection Settings | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Enable | <input checked="" type="checkbox"/> | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Primary Server | 8.8.8.8 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Secondary Server | 114.114.114.114 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Interval | 300 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retry Interval | 5 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Timeout | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Retry Times | 3 | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Industrial Interface | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Network | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Applications | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| VPN | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Maintenance | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

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

Step 4: Give it a description.

Step 5: Edit the ICMP Detection Settings as required.

Step 6: Click on Save and then Apply.

| | |
|---------------------|-------------|
| Section Six | 6944 Manual |
| Wi-Fi Configuration | Rev 2.8 |

General Settings

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

| Overview | Status | Connection |
|----------------------|-------------------------|------------|
| Link Management | General Settings | |
| ► Connection Manager | Priority | Enable |
| Cellular | 1 | true |
| Ethernet | 2 | false |
| WiFi | | |

Checking WAN Status

Click Status to view the WAN status.

| Overview | Status | Connection |
|----------------------|-------------------------------|------------|
| Link Management | Connection Information | |
| ► Connection Manager | Index | Type |
| Cellular | 1 | WLAN |
| Ethernet | | |

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

Testing Wi-Fi

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

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

Command Prompt

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

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

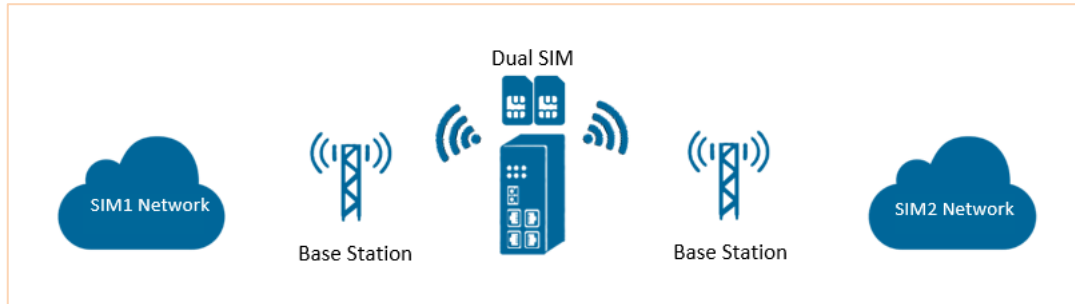
As can be seen a ping to one of Google's DNS servers is working.

7 Configuring Resilient Links

7.1 AN001 Dual SIM Configuration

Testing Topology

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



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

Internet Configuration

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

| Active Link Information | |
|-------------------------|-----------------|
| Link Type | WWAN1 |
| IP Address | 10.148.30.147 |
| Netmask | 255.255.255.248 |
| Gateway | 10.148.30.148 |

Dual SIMs Strategy Configuration

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



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

Connection Settings

General Settings

Priority

1

Enable

☒

Connection Type

WWAN1

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

Connection Settings

General Settings

Priority

2

Enable

☒

Connection Type

WWAN2

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

Testing

Checking the Internet Connection Status

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

| Active Link Information | |
|-------------------------|-----------------|
| Link Type | WWAN1 |
| IP Address | 10.148.30.147 |
| Netmask | 255.255.255.248 |
| Gateway | 10.148.30.148 |

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

case
communications

Overview

Link Management

► Connection Manager

Cellular

Ethernet

Industrial Interface

| Status | | Connection | | | |
|------------------------|-------|--------------|---------------|-----------------|---------------|
| Connection Information | | | | | |
| Index | Type | Status | IP Address | Netmask | Gateway |
| 1 | WWAN1 | Connected | 10.148.30.147 | 255.255.255.248 | 10.148.30.148 |
| 2 | WWAN2 | Disconnected | | | |

Test Results

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

| Active Link Information | |
|-------------------------|-----------------|
| Link Type | WWAN2 |
| IP Address | 10.148.236.23 |
| Netmask | 255.255.255.240 |
| Gateway | 10.148.236.24 |



| Overview | | Status | Connection |
|--------------------|----------|------------------------|-----------------|
| Link Management | | Connection Information | |
| Connection Manager | Cellular | Index | Type |
| Ethernet | | Status | IP Address |
| | | Netmask | Gateway |
| | | 1 | WWAN1 |
| | | 2 | WWAN2 |
| | | Disconnected | Connected |
| | | | 10.148.236.23 |
| | | | 255.255.255.240 |
| | | | 10.148.236.24 |

Checking the 6944 Syslog

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

```

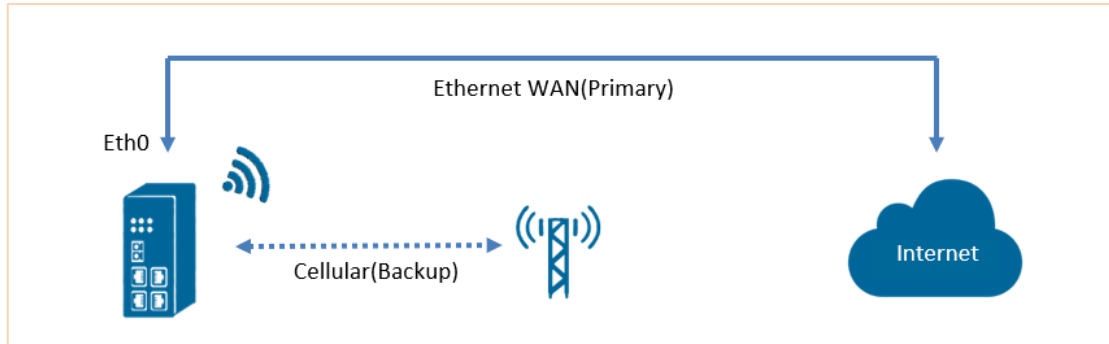
=====
Jun 12 08:00:27 casecomms daemon.err udhcpc[1575]: lease of 10.44.201.229 obtained, lease
time 7200
Jun 12 08:00:27 casecomms user.debug udhcpc: dhcpc get configuration of wwan1
Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: connection of wwan1 is
connected
Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: setup active link wwan1
Jun 12 08:00:27 casecomms user.debug connection_manager[1115]: start ICMP
detecting(wwan1->8.8.8.8/114.114.114.114)
Jul 29 11:18:40 casecomms user.debug modem[1185]: +CGREG: 2,1,"2508","6016C02",7
Jul 29 11:18:40 casecomms user.debug modem[1185]: OK
Jul 29 11:18:40 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (1/3)
Jul 29 11:18:43 casecomms user.debug connection_manager[1115]: timer proc status = 2
Jul 29 11:18:43 casecomms user.debug connection_manager[1115]: start ICMP
detecting(wwan1->8.8.8.8/114.114.114.114)
Jul 29 11:18:49 casecomms user.debug connection_manager[1115]: connection_manager
proc_icmp_detection
Jul 29 11:18:49 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (2/3)
Jul 29 11:18:50 casecomms user.debug modem[1185]: OK
Jul 29 11:18:52 casecomms user.debug connection_manager[1115]: start ICMP
detecting(wwan1->8.8.8.8/114.114.114.114)
Jul 29 11:18:55 casecomms user.daemon.info urandom_seed[1338]: Seed saved (/etc/urandom.seed)
Jul 29 11:18:58 casecomms user.debug connection_manager[1115]: WWAN1 ICMP detecting failed (3/3)
Jul 29 11:18:59 casecomms user.debug modem[1185]: link wwan1 disconnected
Jul 29 11:18:59 casecomms user.daemon.err udhcpc[1593]: entering released state
Jul 29 11:18:59 casecomms user.debug connection_manager[1115]: SIM switch from SIM1 to
SIM2, reload modem with SIM2
Jul 29 11:18:59 casecomms user.debug connection_manager[1115]: II wwan2
modem[1185]: modemd exit
Jul 29 11:19:09 casecomms user.debug modem[2360]: modem init with SIM2
Jul 29 11:19:41 casecomms daemon.err udhcpc[3000]: lease of 10.148.236.23 obtained, lease
time 7200

```


7.2 Link Back Up WAN to Cellular

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

Testing Topology



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

Eth0 Configuration

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

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



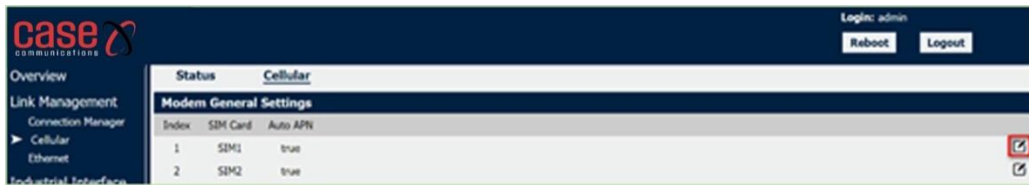
Step 3: Specify the interface and set it as **WAN**, Click **Save**.

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

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

Cellular Configuration

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



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

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

Link Backup Strategy Configuration

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



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



Connection Settings

General Settings

Priority

1

Enable

☒

Connection Type

WAN

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

case communications

Overview

Link Management

Connection Manager

Cellular

Ethernet

Status

Connection

General Settings

| Priority | Enable | Connection Type | Description |
|----------|--------|-----------------|-------------|
| 1 | true | WAN | |

Connection Settings

General Settings

Priority

2

Enable

☒

Connection Type

WWAN1

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

Testing

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

| | |
|-----------------------------|-------------|
| Section Seven | 6944 Manual |
| Configuring Resilient Links | Rev 2.8 |

Internet Status

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

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

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

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

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

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

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

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

Checking the 6944 Syslog

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

```

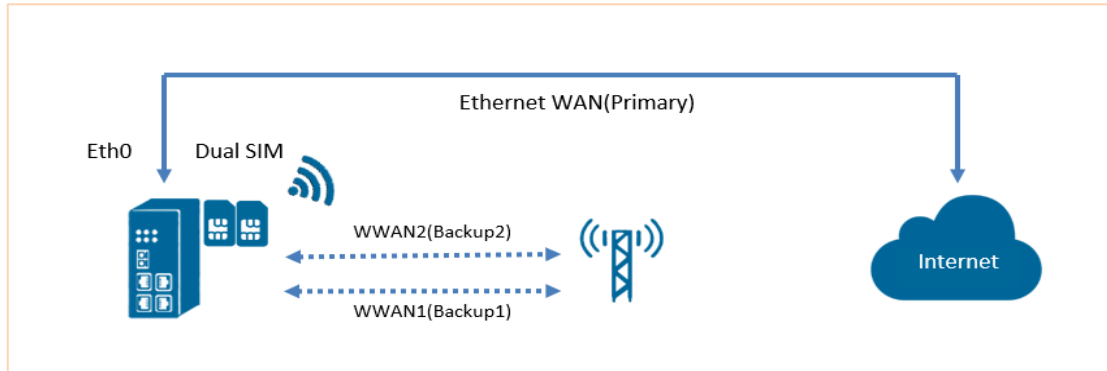
Jun 12 08:00:04 casecomms syslog.info syslogd started: BusyBox v1.25.1
Jun 12 08:00:07 casecomms user.debug connection_manager[1148]: setup active link wan
Jun 12 08:00:07 casecomms user.debug connection_manager[1148]: start ICMP detecting(wan->8.8.8.8/114.114.114.114)
Jun 12 08:00:08 casecomms user.debug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

```

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

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

Testing Topology

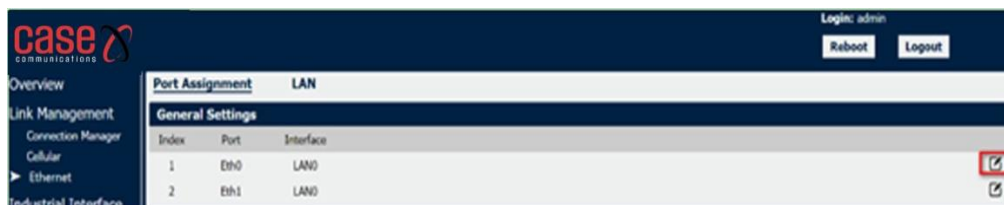


- Specify Eth0 as the Primary WAN interface and wwan1 as the secondary backup interface, and wwan2 as third backup interface.
- If the 6944 detects the primary WAN is down, it will switch to wwan1 (Wireless WAN 1) to provide an instant network connection.
- If the 6944 detects both WAN and wwan1 is down,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

Configuring Ethernet 0

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

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



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

Port Settings

General Settings

Index

1

Port

Eth0

Interface

WAN

Save

Close

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

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

Cellular Configuration

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

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

Link Backup Strategy Configuration

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

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

Connection Settings

General Settings

Priority

1

Enable

☒

Connection Type

WAN

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

case communications

Login: admin

Reboot

Logout

Overview

Link Management

Connection Manager

Cellular

Ethernet

Status

Connection

General Settings

| Priority | Enable | Connection Type | Description |
|----------|--------|-----------------|-------------|
| 1 | true | WAN | |

Connection Settings

General Settings

Priority

2

Enable

☒

Connection Type

WWAN1

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

case communications

Login: admin

Reboot

Logout

Overview

Link Management

Connection Manager

Cellular

Ethernet

Status

Connection

General Settings

| Priority | Enable | Connection Type | Description |
|----------|--------|-----------------|-------------|
| 1 | true | WAN | |
| 2 | true | WWAN1 | |

| | |
|-----------------------------|-------------|
| Section Seven | 6944 Manual |
| Configuring Resilient Links | Rev 2.8 |

Connection Settings

General Settings

Priority

3

Enable

☒

Connection Type

WWAN2

Description

ICMP Detection Settings

Enable

☒

Primary Server

8.8.8.8

Secondary Server

114.114.114.114

Interval

300

?

Retry Interval

5

?

Timeout

3

?

Retry Times

3

?

Save

Close

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

Testing

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

Internet Status

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

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

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

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

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

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

| | |
|-----------------------------|-------------|
| Section Seven | 6944 Manual |
| Configuring Resilient Links | Rev 2.8 |

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

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

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

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

Checking the Syslog

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

```

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

```


8 Network Security

8.1. Firewall and ACL

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

The screenshot shows a web interface for configuring ACLs. At the top, there are three tabs: 'ACL', 'Port Mapping', and 'DMZ'. The 'ACL' tab is selected. Below the tabs, there is a 'General Settings' section with a 'Default Policy' dropdown menu set to 'Accept'. Below that is an 'ACL rule Settings' section with a table header containing columns: Index, Description, Protocol, Source Address, Source Port, Destination Address, and Destination Port. A plus sign icon is visible at the end of the header row.

Router Configuration

Firewall->ACL

- Default Policy**

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

- Access Control List.**

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

The screenshot shows a dialog box titled 'ACL Settings'. It has a 'General Settings' tab. The form contains the following fields: 'Index' (text box with '1'), 'Description' (text box), 'Protocol' (dropdown menu with 'All'), 'Source Address' (text box with a help icon), and 'Destination Address' (text box with a help icon). At the bottom right, there are 'Save' and 'Close' buttons.

Firewall->ACL

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

Port Mapping Settings

Port Mapping rule Settings

| | | |
|----------------|----------------------------------|---|
| Index | <input type="text" value="1"/> | |
| Description | <input type="text"/> | |
| Protocol | <input type="text" value="All"/> | ? |
| Remote Address | <input type="text"/> | ? |
| Remote Port | <input type="text"/> | ? |
| Local Address | <input type="text"/> | ? |
| Local Port | <input type="text"/> | ? |

Firewall->Port Mapping

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

ACL
Port Mapping
DMZ

General Settings

| | | |
|------------------|--|---|
| Enable | <input checked="" type="checkbox"/> | |
| Remote Address | <input type="text" value="0.0.0.0/0"/> | ? |
| DMZ Host Address | <input type="text"/> | |

Firewall->DMZ

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

8.2. AN028-Configuring SSH with a Public Key

Router Configuration

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

The first screenshot shows the 'SSH' tab in the 'General Settings' section. The 'SSH Port' is set to 22, 'Allow Password Authentication' is checked, and the 'Public Key' field is empty.

The second screenshot shows the 'SSH' tab in the 'Remote Access Settings' section. The 'Remote SSH Access' checkbox is checked, along with 'Remote HTTP Access', 'Remote HTTPS Access', and 'Remote Telnet Access'.

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

Public/Private Key Generated

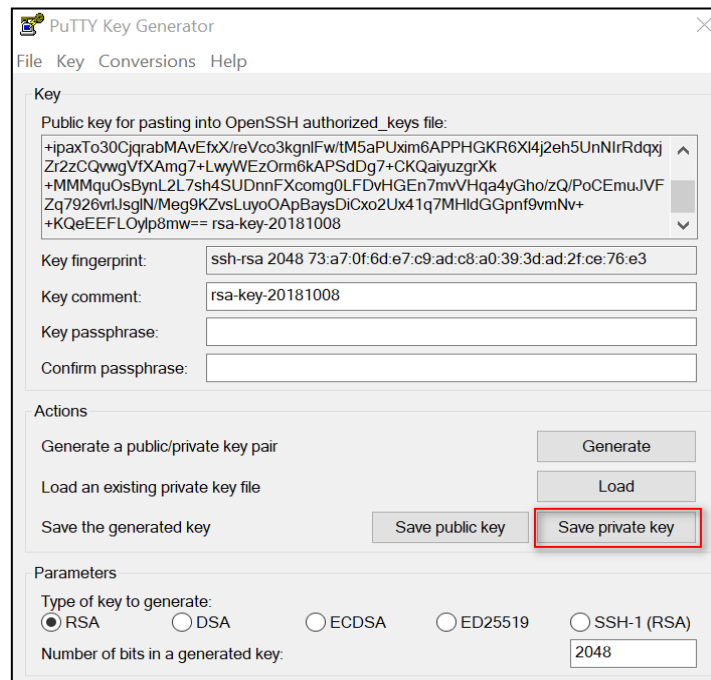
Step 1: Run the software “puttygen.exe” to build the public key, as shown below:

The PuTTY Key Generator window shows the 'Actions' section with the 'Generate' button highlighted. The 'Parameters' section shows 'Type of key to generate' set to RSA and 'Number of bits in a generated key' set to 2048.

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

The screenshot shows the 'SSH' tab in the 'General Settings' section. The 'SSH Port' is 22, 'Allow Password Authentication' is checked, and the 'Public Key' field now contains the string 'ssh-rsa AAAAB3NzaC1yc2EAAAQ...'. The 'Public Key' field is highlighted with a red box.

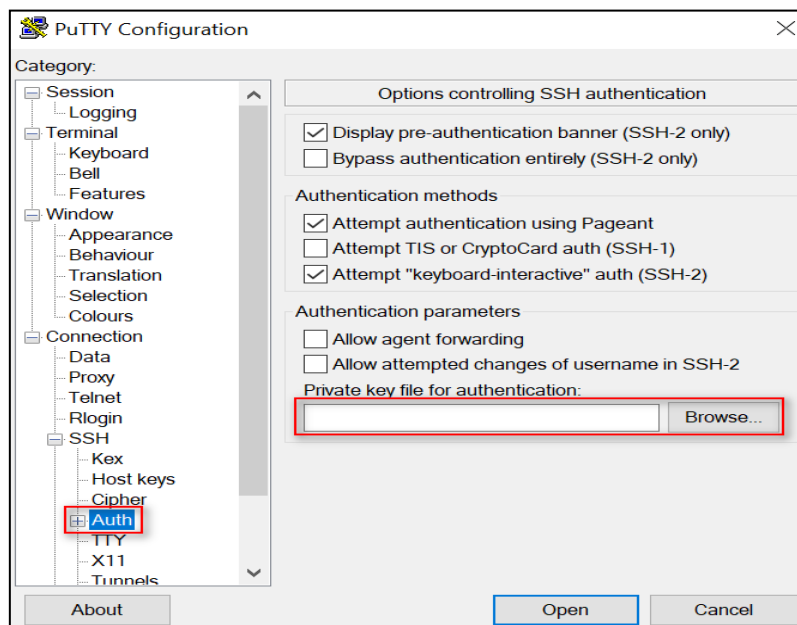
Step 3: Save the Private Key, as shown below:



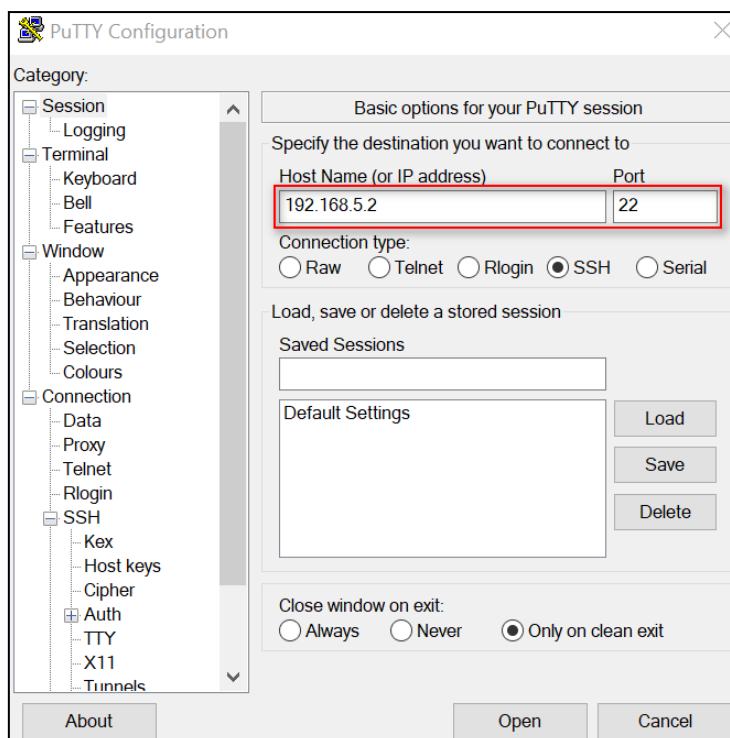
Note: we now need to import the private key to the SSH tool, so that it can provide SSH to the router successfully.

Testing SSH

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



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



Step 3: Test successful.



This page left blank intentionally

9 Routing

9.1. Static Routing

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

Please refer current route table as below.

| 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 type="text" value="1"/> |
| Description | <input type="text"/> |
| IP Address | <input type="text"/> |
| Netmask | <input type="text"/> |
| Gateway | <input type="text"/> |
| Interface | <input type="text"/> ? |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

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.

```

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#

```

| | |
|--------------|-------------|
| Section Nine | 6944 Manual |
| Routing | Rev 2.8 |

Step 2: Checking the 6944 Routing table 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 | 192.168.5.0 | 255.255.255.0 | 192.168.111.200 | 20 | wan |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

Testing

Step 1: Ping from the CISCO router 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#
```

Step 2: Test successful.

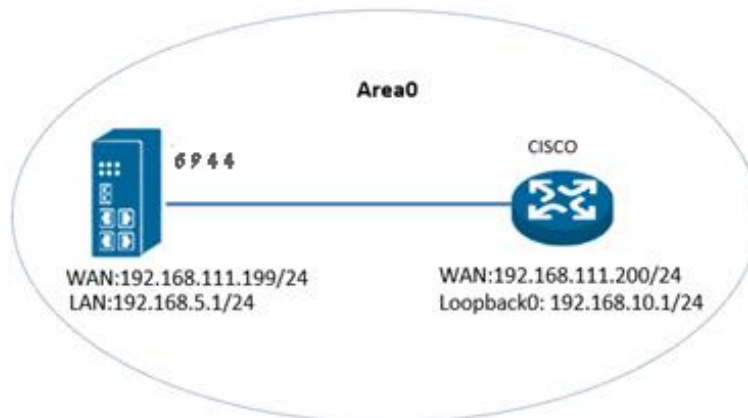
9.2. Dynamic Routing Using RIP

Introduction.

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

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

Dynamic Routing Topology



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

Configuration

CISCO_Configuration

```
CISCO7200#show running-config
Building configuration...
Current configuration : 1165 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO7200
!
boot-start-marker
boot-end-marker
!
no aaa new-model
no ip icmp rate-limit unreachable
ip cef
!
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
 log config
 hidekeys
!
ip tcp synwait-time 5
!
interface Loopback0
 ip address 192.168.10.1 255.255.255.0
!
```

```
interface FastEthernet0/0
 ip address 192.168.111.200 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 no ip address
 shutdown
 duplex auto
 speed auto
!
router rip
 version 2
 network 192.168.10.0
 network 192.168.111.0
 no auto-summary
!
line con 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line aux 0
 exec-timeout 0 0
 privilege level 15
 logging synchronous
 stopbits 1
line vty 0 4
 login
!
!
end
CISCO7200#
```

6944 Configuration

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

Step 2:
Click
Save>Apply

Check the Routing Tables

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

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

Gateway of last resort is not set

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

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

| 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 | 192.168.5.0 | 255.255.255.0 | 192.168.111.200 | 20 | wan |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

Testing

Step 1: Ping from CISCO to 6944

Step 2: Test successful.

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

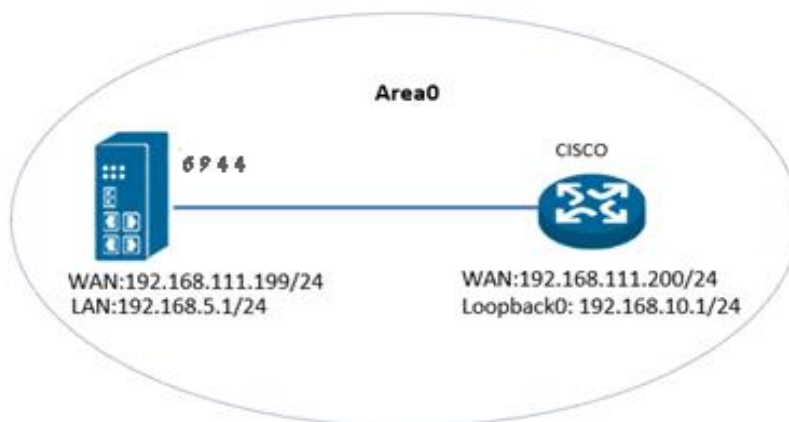
9.3. Dynamic Routing Using OSPF

Introduction.

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

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

Dynamic Routing Topology



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

Configuration

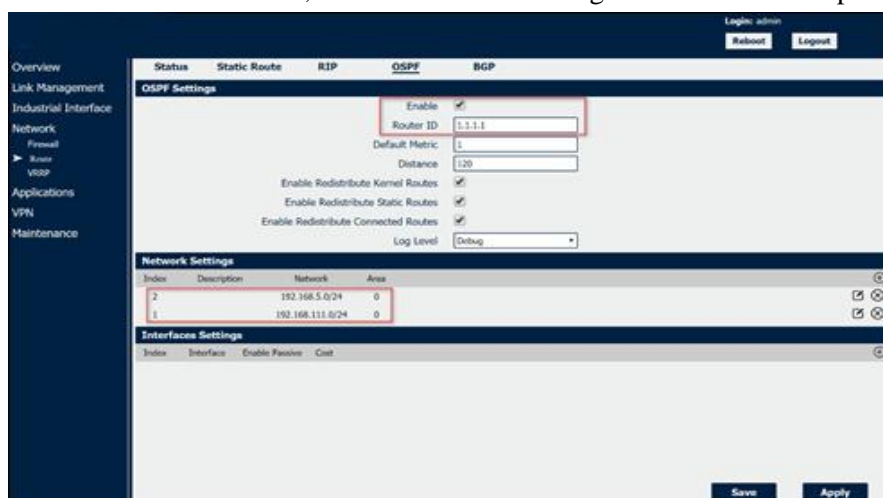
CISCO 7200 OSPF Configuration

```
CISCO7200#show running-config
Building configuration...
Current configuration : 1218 bytes
!
upgrade fpd auto
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname CISCO7200
!
boot-start-marker
boot-end-marker
no ip domain lookup
ip auth-proxy max-nodata-conns 3
ip admission max-nodata-conns 3
!
multilink bundle-name authenticated
!
archive
log config
  hidekeys
!
ip tcp synwait-time 5
!
interface Loopback0
  ip address 192.168.10.1 255.255.255.0
!
interface FastEthernet0/0
  ip address 192.168.111.200 255.255.255.0
  duplex auto
  speed auto
```

```
!
interface FastEthernet0/1
  no ip address
  shutdown
  duplex auto
  speed auto
!
router ospf 110
  router-id 2.2.2.2
  log-adjacency-changes
  network 192.168.10.0 0.0.0.255 area 0
  network 192.168.111.0 0.0.0.255 area 0
!
ip forward-protocol nd
no ip http server
no ip http secure-server
!
line con 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line aux 0
  exec-timeout 0 0
  privilege level 15
  logging synchronous
  stopbits 1
line vty 0 4
  login
!
end
CISCO7200
```

6944 OSPF Configuration

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



Step 2: Click Save>Apply.

| | |
|--------------|-------------|
| Section Nine | 6944 Manual |
| Routing | Rev 2.8 |

Checking the Routing Tables

Check the Cisco 7200 routing table for reference

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

Gateway of last resort is not set

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

Check the 6944 routing table for reference.

| | | | | | |
|----------------------|-------------------------|---------------|-----------------|-----------------|------------------|
| Overview | Status | Static Route | RIP | OSPF | BGP |
| Link Management | Route Table Information | | | | |
| Industrial Interface | Index | Destination | Netmask | Gateway | Metric Interface |
| Network | 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.11 | 0 wan |
| Firewall | 2 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 lan0 |
| Router | 3 | 192.168.10.1 | 255.255.255.255 | 192.168.111.200 | 20 wan |
| VRRP | 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 wan |

Testing

Ping from CISCO to the 6944

Test Successful

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

9.4. Dynamic Routing Using BGP

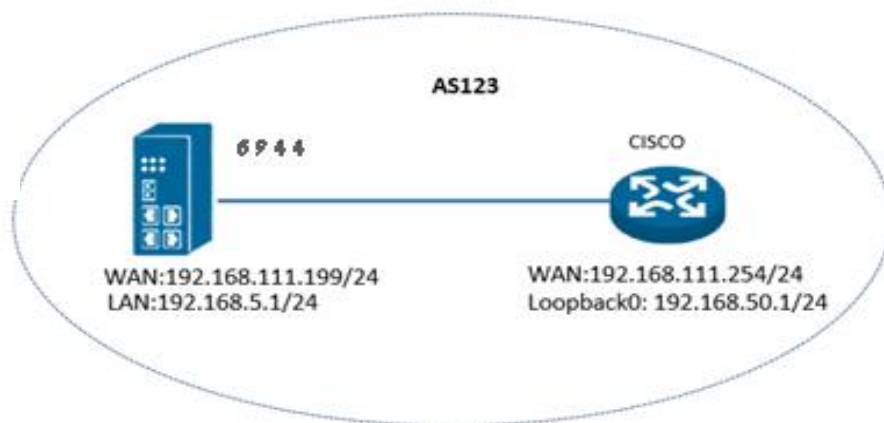
Introduction

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

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

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

Topology



| | |
|--------------|-------------|
| Section Nine | 6944 Manual |
| Routing | Rev 2.8 |

Configuration

Cisco 7200 Configuration.

```

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

```

Configuration Continued

```

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

```


6944 BGP Configuration

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

Step 2: Click Save>Apply.

Checking the Routing Tables

Step 1: Check the 7200 Routing Table for reference

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

Gateway of last resort is not set

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

Step 2: Checking the 6944 Routing table for reference

| 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 | 192.168.50.0 | 255.255.255.0 | 192.168.111.200 | 20 | wan |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

Testing

Ping from the CISCO router to the 6944 Router:

Test Successful

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

10 V.R.R.P

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

Configuration Options

VRRP

VRRP Network Settings

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

Network->VRRP

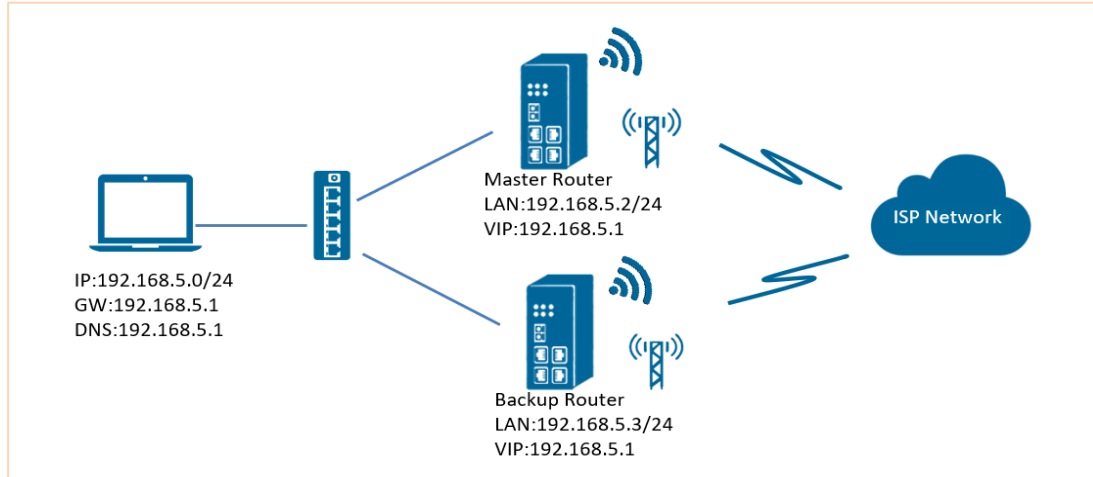
- **Enable**
Select this box will enable VRRP.
- **Interface**
Select the interface of Virtual Router.
- **Virtual Router ID**
User-defined Virtual Router ID. Range: 1-255.
- **Authentication Type**
Select the authentication type for VRRP.
- **Priority**
Enter the VRRP priority range is 1-254 (a bigger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

10.1. Configuring VRRP between Two 6944 Routers

Overview

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

Testing Topology



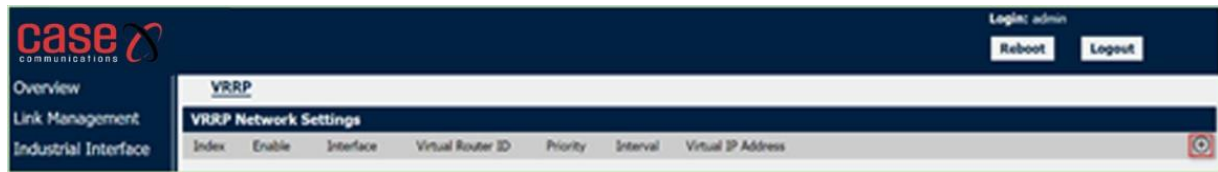
- The 6944 runs as VRRP Master router and Backup router and connects to the Internet via a SIM card.
- A PC connects to the Internet via the Master 6944 router under normal running Conditions.
- If the Master 6944 router goes down, the PC will switchover to Backup 6944 router to access the Internet.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

Configuring the Master 6944

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

| LAN Settings | |
|-------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Interface | LAN0 |
| IP Address | 192.168.5.2 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |
| DHCP Settings | |
| Enable | <input checked="" type="checkbox"/> |
| Mode | Server |
| IP Pool Start | 192.168.5.4 |
| IP Pool End | 192.168.5.10 |
| Netmask | 255.255.255.0 |
| Lease Time | 120 |
| Gateway | 192.168.5.1 |
| Primary DNS | 192.168.5.1 |
| Secondary DNS | |
| WINS Server | |
| <div>Save Close</div> | |

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



Step 3: Configure VRRP as shown below:

VRRP

VRRP Network Settings

| | |
|---------------------|--|
| Index | <input type="text" value="1"/> |
| Enable | <input checked="" type="checkbox"/> |
| Interface | <input type="text" value="LAN0"/> |
| Virtual Router ID | <input type="text" value="1"/> |
| Authentication Type | <input type="text" value="None"/> ? |
| Priority | <input type="text" value="120"/> |
| Interval | <input type="text" value="1"/> |
| Virtual IP Address | <input type="text" value="192.168.5.1"/> |

Step 4: Click Save>Apply.

Configuring the Backup Router

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

LAN Settings

General Settings

| | |
|------------|--|
| Index | <input type="text" value="1"/> |
| Interface | <input type="text" value="LAN0"/> |
| IP Address | <input type="text" value="192.168.5.3"/> |
| 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="192.168.5.11"/> |
| IP Pool End | <input type="text" value="192.168.5.20"/> |
| Netmask | <input type="text" value="255.255.255.0"/> |
| Lease Time | <input type="text" value="120"/> |
| Gateway | <input type="text" value="192.168.5.1"/> |
| Primary DNS | <input type="text" value="192.168.5.1"/> |
| Secondary DNS | <input type="text" value=""/> |
| WINS Server | <input type="text" value=""/> |

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



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

VRRP

VRRP Network Settings

Index: 1

Enable: ☒

Interface: LAN0

Virtual Router ID: 1

Authentication Type: None

Priority: 100

Interval: 1

Virtual IP Address: 192.168.5.1

Save Close

PC Configuration

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

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 5 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 5 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

| | |
|-------------|-------------|
| Section Ten | 6944 Manual |
| VRRP | Rev 2.8 |

Testing VRRP between 6944's

Now the PCs communicate with the Internet via Master Router;

```

Administrator Command prompt – tracert 8.8.8.8

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

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

C:\Users \ Administrator tracert 8.8.8.8

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

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

```

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

```

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

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

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

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops
  0  1 ms    *      1 ms    192.168.5.3
  1  220 ms  227 ms  238 ms  10.241.157.57
  2
  3

```

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

```

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

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=327ms TTL=41
Reply from 8.8.8.8: bytes=32 time=110ms TTL=41
Reply from 8.8.8.8: bytes=32 time=60ms TTL=41
Reply from 8.8.8.8: bytes=32 time=105ms TTL=41

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 60ms, Maximum = 327ms, Average = 150ms

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0  1 ms    1 ms    1 ms    192.168.5.2
  1  *      *      *      Request timed out.
  2
  3

```

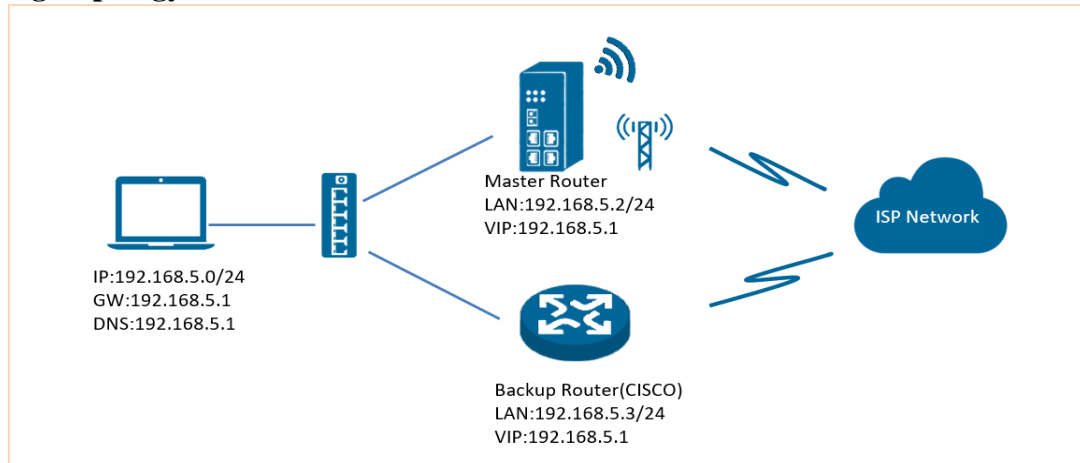
Test Successful

10.2. Configuring VRRP Between 6944 and Cisco Routers

Overview

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

Testing Topology



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

Configuration

Master Router Configuration

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

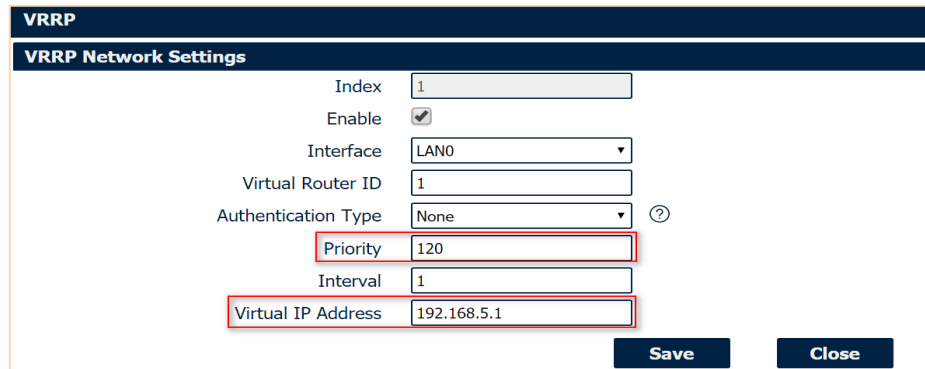
| LAN Settings | |
|-------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Interface | LAN0 |
| IP Address | 192.168.5.2 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |
| DHCP Settings | |
| Enable | <input checked="" type="checkbox"/> |
| Mode | Server |
| IP Pool Start | 192.168.5.4 |
| IP Pool End | 192.168.5.10 |
| Netmask | 255.255.255.0 |
| Lease Time | 120 |
| Gateway | 192.168.5.1 |
| Primary DNS | 192.168.5.1 |
| Secondary DNS | |
| WINS Server | |
| <div>Save Close</div> | |

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

| VRRP | |
|----------------------|-----------------------|
| Overview | VRRP Network Settings |
| Link Management | |
| Industrial Interface | |
| Index | Enable |
| Interface | Virtual Router ID |
| Priority | Interval |
| Virtual IP Address | |

| | |
|-------------|-------------|
| Section Ten | 6944 Manual |
| VRRP | Rev 2.8 |

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



Backup Router (CISCO) Configuration

The configuration on CISCO router as shown below

```

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

```

PC Configuration

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

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 5 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 5 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Testing VRRP Between the 6944 and Cisco

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

```
Administrator Command prompt – tracert 8.8.8.8

C:\Users\Administrator ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40

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

C:\Users\Administrator tracert 8.8.8.8

Tracing route to google public dns-a-google.com [8.8.8.8]
over a maximum of 30 hops:
  0  0ms  0ms  0ms  (192.168.5.2)
  1  85ms  89ms  130ms  logon (172.29.5.17)
  2  *
  3  *
```

```
Administrator Command prompt – tracert 8.8.8.8

C:\Users\Administrator ping 8.8.8.8
Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40
Reply from 8.8.8.8: bytes=32 time=16ms TTL=40

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

C:\Users\Administrator tracert 8.8.8.8

Tracing route to google public dns-a-google.com [8.8.8.8]
over a maximum of 30 hops:
  0  0ms  0ms  0ms  (192.168.5.3)
  1  230ms  227ms  130ms  logon (10.241.157.57)
  2  *
  3  *
```

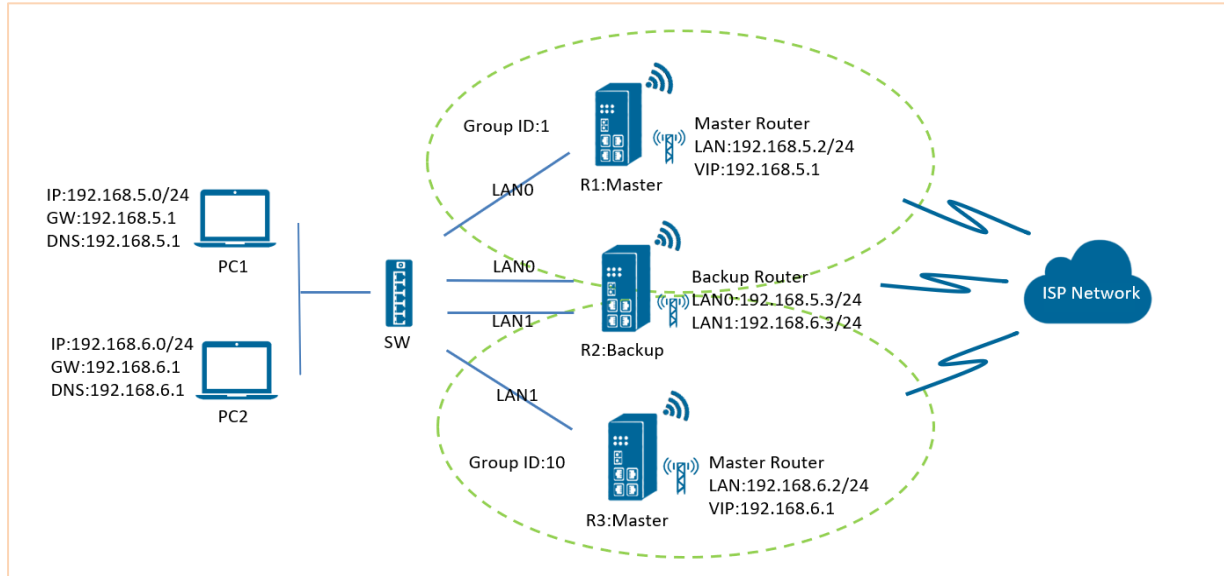
1. Remove the Ethernet cable between the 6944 master router and the Switch, the PC will access the Internet via the Cisco Backup Router.
2. Replace the Ethernet cable, the PC will then access the Internet via the 6944 Master Router.

10.3. VRRP Between Multiple 6944 Routers

Overview

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

Testing Topology

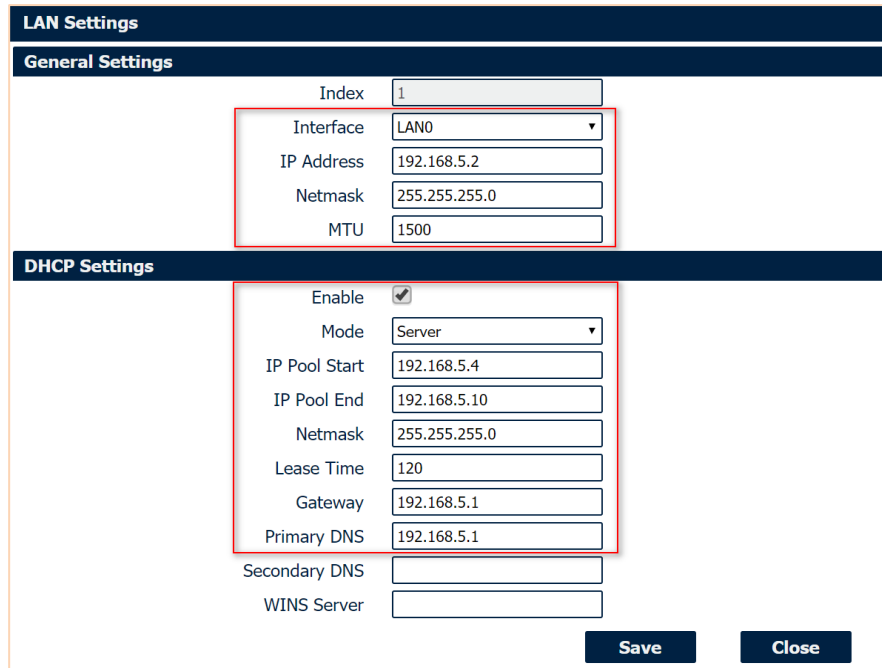


- 6944 R1 and 6944 R3 run as 6944 VRRP Master routers.
- 6944 R2 runs as a VRRP Backup router.
- Both of the 6944 routers connect to Internet with their SIM cards.
- 6944 R1 establishes VRRP with 6944 R2 via its LAN0 interface.
- 6944 R3 establish VRRP with R2 via its LAN1 interface.
- PC1 communicates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

Configuration

R1 Master Router Configuration

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



LAN Settings

General Settings

| | |
|------------|---------------|
| Index | 1 |
| Interface | LAN0 |
| IP Address | 192.168.5.2 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |

DHCP Settings

| | |
|---------------|-------------------------------------|
| Enable | <input checked="" type="checkbox"/> |
| Mode | Server |
| IP Pool Start | 192.168.5.4 |
| IP Pool End | 192.168.5.10 |
| Netmask | 255.255.255.0 |
| Lease Time | 120 |
| Gateway | 192.168.5.1 |
| Primary DNS | 192.168.5.1 |
| Secondary DNS | |
| WINS Server | |

Save **Close**

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



case communications

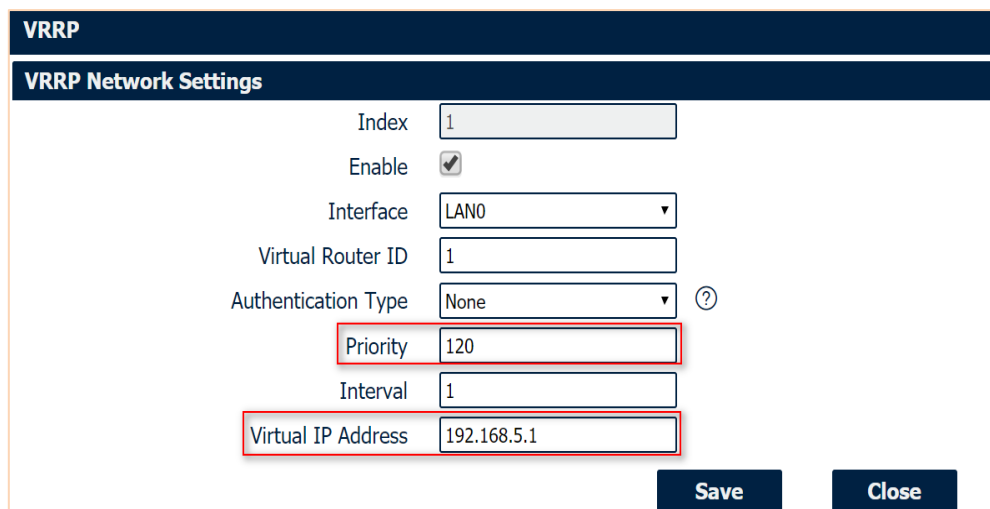
Log in: admin **Reboot** **Logout**

VRRP

VRRP Network Settings

| Index | Enable | Interface | Virtual Router ID | Priority | Interval | Virtual IP Address |
|-------|--------|-----------|-------------------|----------|----------|--------------------|
|-------|--------|-----------|-------------------|----------|----------|--------------------|

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



VRRP

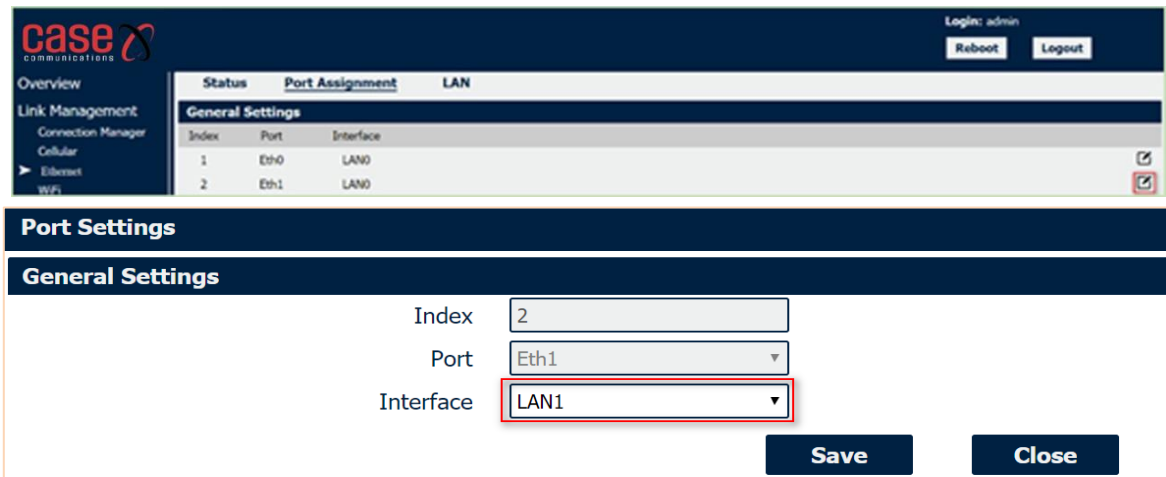
VRRP Network Settings

| | |
|---------------------|-------------------------------------|
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Interface | LAN0 |
| Virtual Router ID | 1 |
| Authentication Type | None |
| Priority | 120 |
| Interval | 1 |
| Virtual IP Address | 192.168.5.1 |

Save **Close**

R3 Master Router Configuration

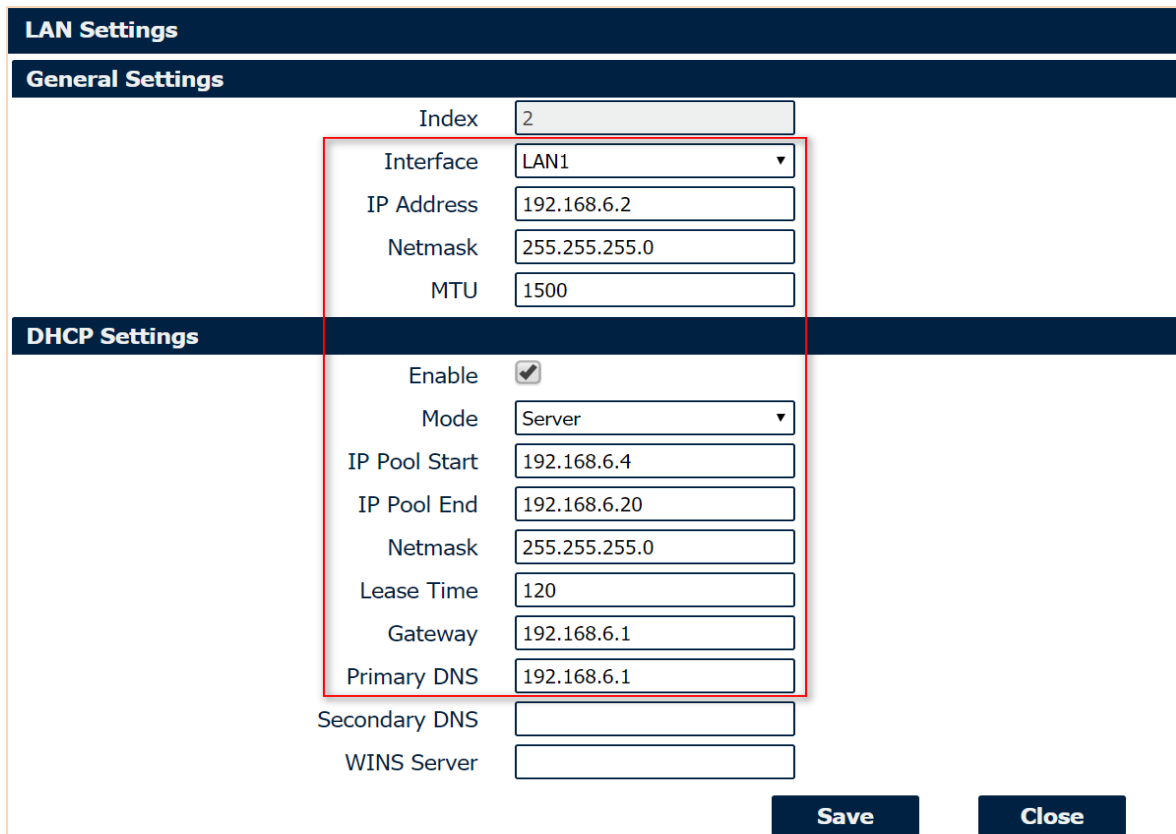
Step 1: Go to Link Management>Ethernet>Port Assignment, click Index2 to assign the LAN1 to ETH1, click Save>Apply.



| Status | Port Assignment | LAN |
|-------------------------|-----------------|-----------|
| General Settings | | |
| Index | Port | Interface |
| 1 | Eth0 | LAN0 |
| 2 | Eth1 | LAN0 |

| | |
|----------------------------------|------|
| Port Settings | |
| General Settings | |
| Index | 2 |
| Port | Eth1 |
| Interface | LAN1 |
| <div>Save</div> <div>Close</div> | |

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



| LAN Settings | |
|----------------------------------|-------------------------------------|
| General Settings | |
| Index | 2 |
| Interface | LAN1 |
| IP Address | 192.168.6.2 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |
| DHCP Settings | |
| Enable | <input checked="" type="checkbox"/> |
| Mode | Server |
| IP Pool Start | 192.168.6.4 |
| IP Pool End | 192.168.6.20 |
| Netmask | 255.255.255.0 |
| Lease Time | 120 |
| Gateway | 192.168.6.1 |
| Primary DNS | 192.168.6.1 |
| Secondary DNS | |
| WINS Server | |
| <div>Save</div> <div>Close</div> | |

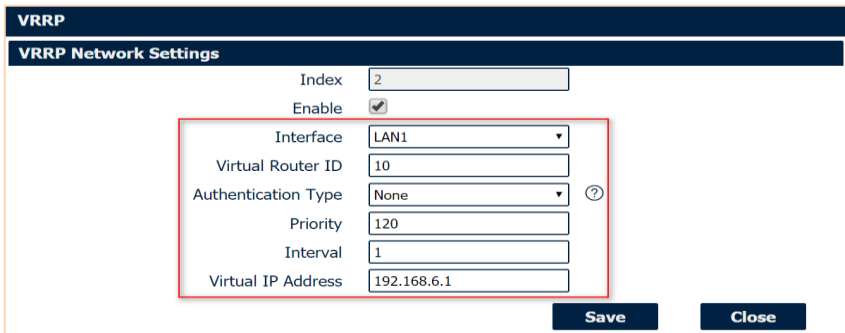
Step 3: Go to Network>VRRP>VRRP, Click the Edit button of VRRP, as shown below



| VRRP | | | | | | |
|-----------------------|--------|-----------|-------------------|----------|----------|--------------------|
| VRRP Network Settings | | | | | | |
| Index | Enable | Interface | Virtual Router ID | Priority | Interval | Virtual IP Address |
| <div>Edit</div> | | | | | | |

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

R2 Backup

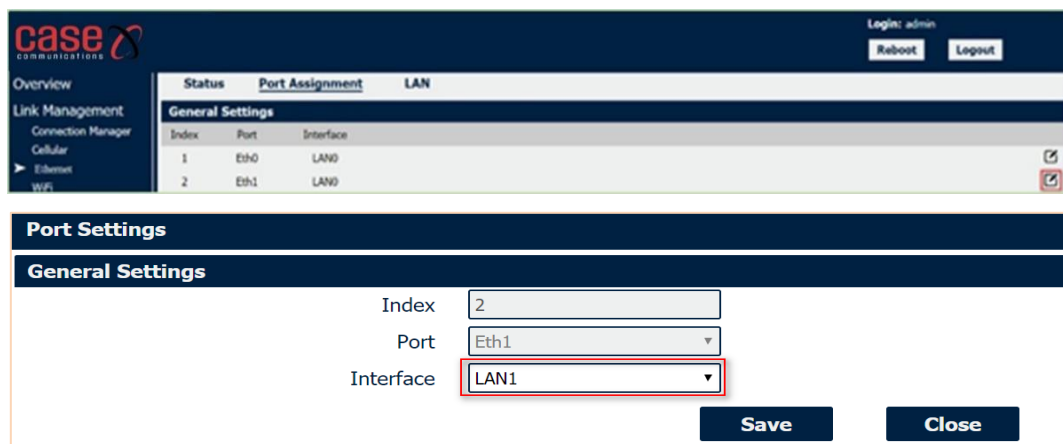


The VRRP Network Settings form shows the following configuration: Index 2, Enable checked, Interface LAN1, Virtual Router ID 10, Authentication Type None, Priority 120, Interval 1, and Virtual IP Address 192.168.6.1. The fields are highlighted with a red box.

Router

Configuration

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

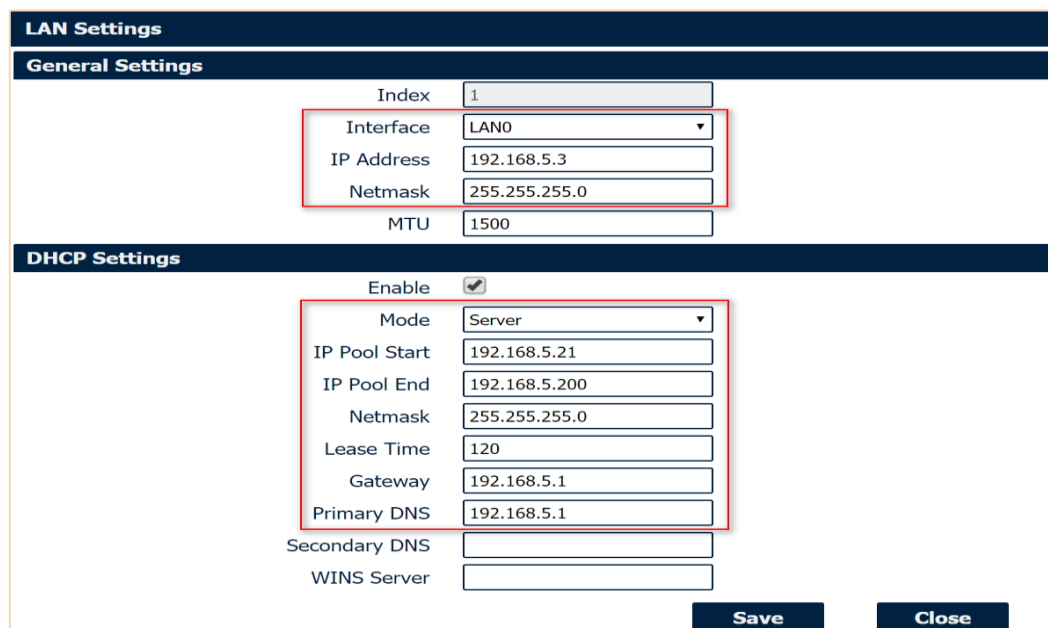


The Port Assignment table shows the following configuration:

| Status | Port Assignment | LAN |
|------------------|-----------------|-----------|
| General Settings | | |
| Index | Port | Interface |
| 1 | Eth0 | LAN0 |
| 2 | Eth1 | LAN0 |

The Port Settings form shows the following configuration: Index 2, Port Eth1, and Interface LAN1. The fields are highlighted with a red box.

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



The LAN Settings form shows the following configuration:

General Settings

| | |
|------------|---------------|
| Index | 1 |
| Interface | LAN0 |
| IP Address | 192.168.5.3 |
| Netmask | 255.255.255.0 |
| MTU | 1500 |

DHCP Settings

| | |
|---------------|---------------|
| Enable | checked |
| Mode | Server |
| IP Pool Start | 192.168.5.21 |
| IP Pool End | 192.168.5.200 |
| Netmask | 255.255.255.0 |
| Lease Time | 120 |
| Gateway | 192.168.5.1 |
| Primary DNS | 192.168.5.1 |
| Secondary DNS | |
| WINS Server | |

| | |
|-------------|-------------|
| Section Ten | 6944 Manual |
| VRRP | Rev 2.8 |

LAN Settings

General Settings

Index2

InterfaceLAN1
IP Address192.168.6.3
Netmask255.255.255.0
MTU1500

DHCP Settings

Enable☒

ModeServer
IP Pool Start192.168.6.21
IP Pool End192.168.5.200
Netmask255.255.255.0
Lease Time120
Gateway192.168.6.1
Primary DNS192.168.6.1
Secondary DNS
WINS Server

SaveClose

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

case communications

Login: admin
Reboot
Logout

Overview

Link Management

Industrial Interface

VRRP

VRRP Network Settings

IndexEnableInterfaceVirtual Router IDPriorityIntervalVirtual IP Address

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

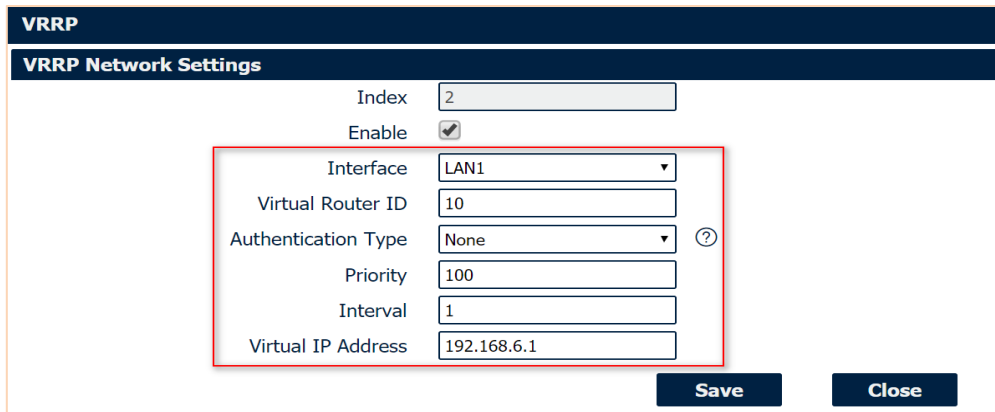
VRRP

VRRP Network Settings

Index1
Enable☒

InterfaceLAN0
Virtual Router ID1
Authentication TypeNone
Priority100
Interval1
Virtual IP Address192.168.5.1

SaveClose



VRRP

VRRP Network Settings

Index: 2

Enable: ☒

Interface: LAN1

Virtual Router ID: 10

Authentication Type: None

Priority: 100

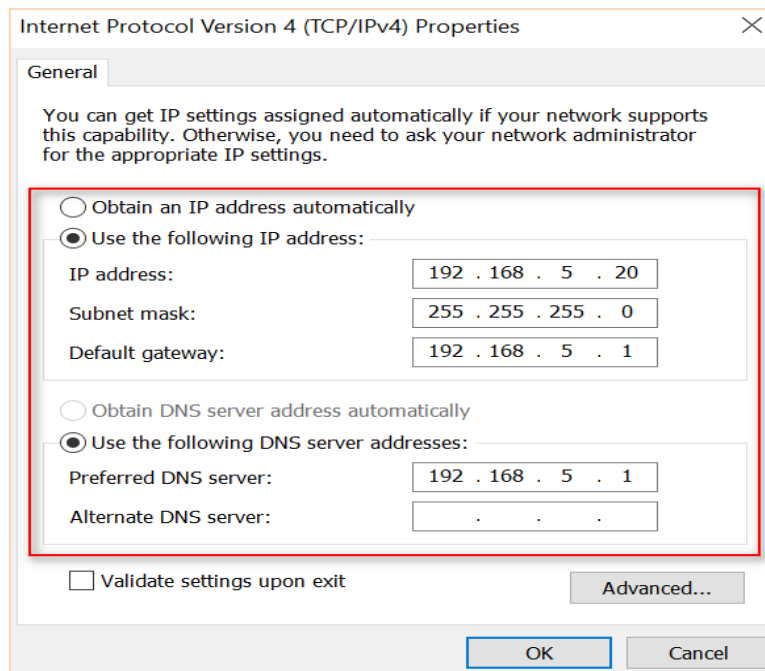
Interval: 1

Virtual IP Address: 192.168.6.1

Save Close

PC Configuration

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 5 . 20

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 5 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 5 . 1

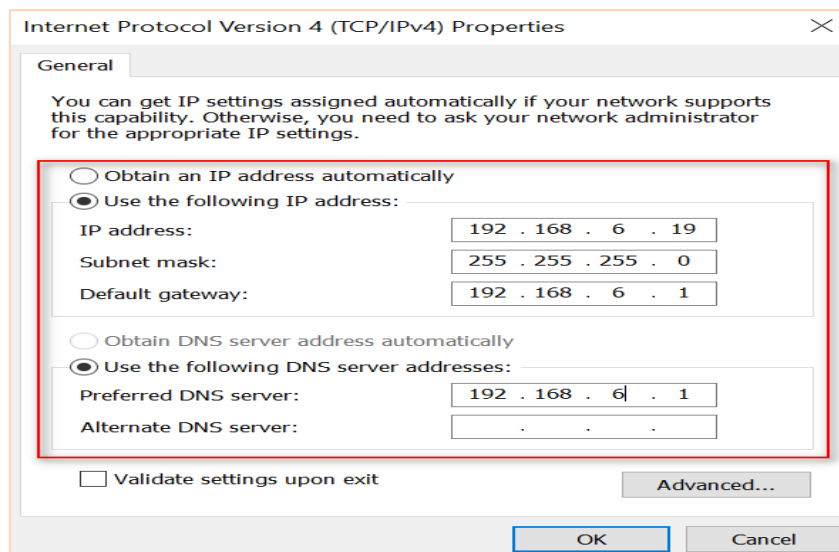
Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 6 . 19

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 6 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 6 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

| | |
|-------------|-------------|
| Section Ten | 6944 Manual |
| VRRP | Rev 2.8 |

Testing VRRP between multiple 6944's

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

```

C:\Users\Administrator>ping 8.8.8.8

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

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

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0  1 ms    1 ms    1 ms  navigatework.router [192.168.5.2]
  1  85 ms   89 ms   130 ms  bogon [172.29.5.17]
  2  *

```

```

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

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

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

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops
  0  1 ms    *      1 ms  192.168.5.3
  1  220 ms  227 ms  238 ms  10.241.157.57
  2  *

```

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

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

A Reply to your ping shows the link is successful.

```

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

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

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

C:\Users\Administrator>tracert 8.8.8.8

Tracing route to google-public-dns-a.google.com [8.8.8.8]
over a maximum of 30 hops:
  0  1 ms    1 ms    1 ms  [192.168.5.2]
  1  85 ms   89 ms   130 ms  bogon [172.29.5.17]
  2  *

```

This page left blank intentionally

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

11 VPN (Virtual Private Networks)

11.1. OpenVPN Introduction

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

| Status | OpenVPN | X.509 Certificate | | | |
|---------------------|---------|-------------------|--------|--------|------------|
| 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

1

Enable

☒

Description

Mode

Client

Protocol

UDP

Connection Type

TUN

Server Address

Server Port

1194

Authentication Method

X.509

?

Encryption Type

BF-CBC

Renegotiate Interval

3600

Keepalive Interval

20

Keepalive Timeout

60

Fragment

0

?

Private Key Password

Output Verbosity Level

3

Advanced Settings

Enable NAT

☐

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

VPN > Open VPN

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

Advanced Settings

Enable NAT

Enable PKCS#12

Enable X.509 Attribute nsCertType

Enable HMAC Firewall

Enable Compression LZ0

Additional Configurations

?

Save

Close

VPN->OpenVPN->Advanced Settings

- **Enable NAT** - Check this box to enable NAT, the source IP of host behind router will be disguised before accessing the remote end.
- **Enable PKCS#12** - It is an exchange of digital certificate encryption standard, used to describe personal identity information.
- **Enable X.509 Attribute nsCertType** - Require that peer certificate was signed with an explicit nsCertType designation of "server".
- **Enable Compression LZ0** - Compress the data.
- **Additional Configurations** - Enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.

| | |
|-----------------------|--------------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

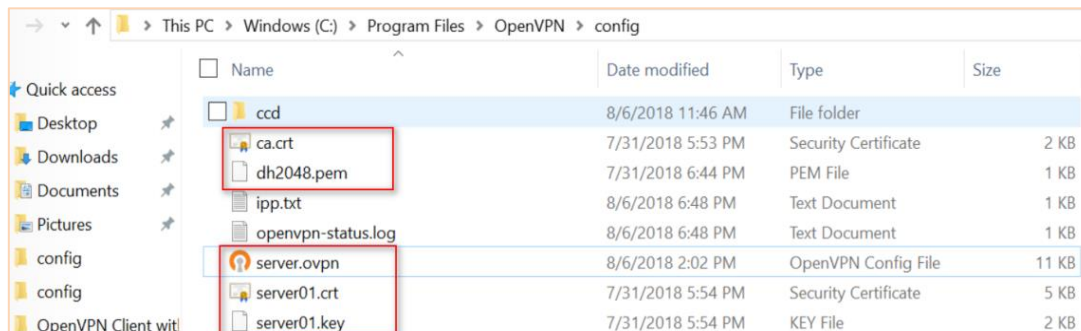
| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

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

Configuration

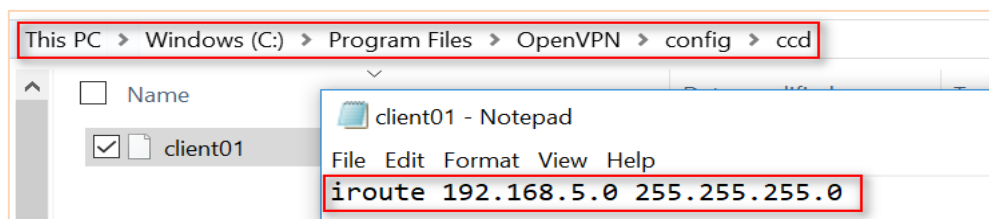
Step 1 - Install OpenVPN software on your PC and copy the related certifications and configuration as shown below:



Note: a) Download OpenVPN software from: <https://openvpn.net/>

b) Install and run OpenVPN software with **administrator authority**.

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



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

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

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

ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

Configure the Client

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

OpenVPN Settings

General Settings

Index

1

Enable

☒

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

☐

Enable PKCS#12

☐

Enable X.509 Attribute nsCertType

☐

Enable HMAC Firewall

☐

Enable Compression LZ0

☒

Additional Configurations

Save

Close

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

Overview

Link Management

Industrial Interface

Network

Applications

VPN

OpenVPN

Maintenance

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 |
|-------|------------|-----------|-------------------------|
| 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.

Overview

Link Management

Industrial Interface

Network

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

IPv4 Route Table

Active Routes:

| Network | Destination | Netmask | Gateway | Interface | Metric |
|-----------------|-----------------|-----------------|---------------|----------------|--------|
| 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 192.168.10.1 | 192.168.10.10 | 291 |
| 0.0.0.0 | 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 | 255.255.255.0 | 10.8.0.2 | 10.8.0.1 | 35 |
| 10.8.0.0 | 255.255.255.252 | 255.255.255.252 | On-link | 10.8.0.1 | 291 |
| 10.8.0.1 | 255.255.255.255 | 255.255.255.255 | On-link | 10.8.0.1 | 291 |
| 10.8.0.3 | 255.255.255.255 | 255.255.255.255 | On-link | 10.8.0.1 | 291 |
| 127.0.0.0 | 255.0.0.0 | 255.0.0.0 | On-link | 127.0.0.1 | 331 |
| 127.0.0.1 | 255.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 127.255.255.255 | 255.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 192.168.5.0 | 255.255.255.0 | 255.255.255.0 | 10.8.0.2 | 10.8.0.1 | 35 |
| 192.168.10.0 | 255.255.255.0 | 255.255.255.0 | On-link | 192.168.10.10 | 291 |
| 192.168.10.10 | 255.255.255.255 | 255.255.255.255 | On-link | 192.168.10.10 | 291 |
| 192.168.10.255 | 255.255.255.255 | 255.255.255.255 | On-link | 192.168.10.10 | 291 |

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

Route Table Information

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

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

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

C:\Users\Administrator>ping 192.168.5.1

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

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

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

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

Ping Traceroute

Ping Settings

Host Address: 192.168.10.10
Ping Count: 5
Local IP Address:

PING 192.168.10.10 (192.168.10.10): 56 data bytes
64 bytes from 192.168.10.10: seq=0 ttl=127 time=2.740 ms
64 bytes from 192.168.10.10: seq=1 ttl=127 time=2.413 ms
64 bytes from 192.168.10.10: seq=2 ttl=127 time=3.849 ms
64 bytes from 192.168.10.10: seq=3 ttl=127 time=3.481 ms

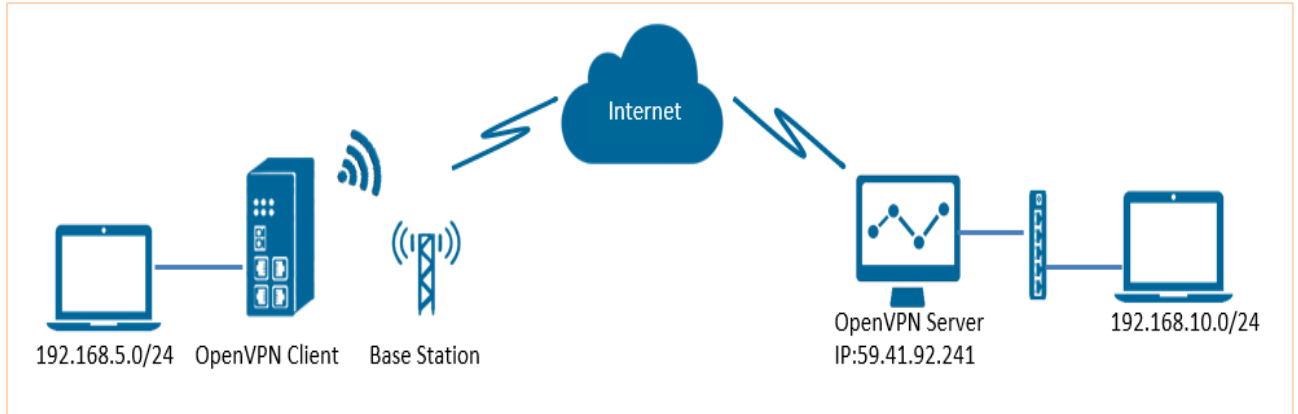
| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Introduction

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

Testing Topology



Configuration

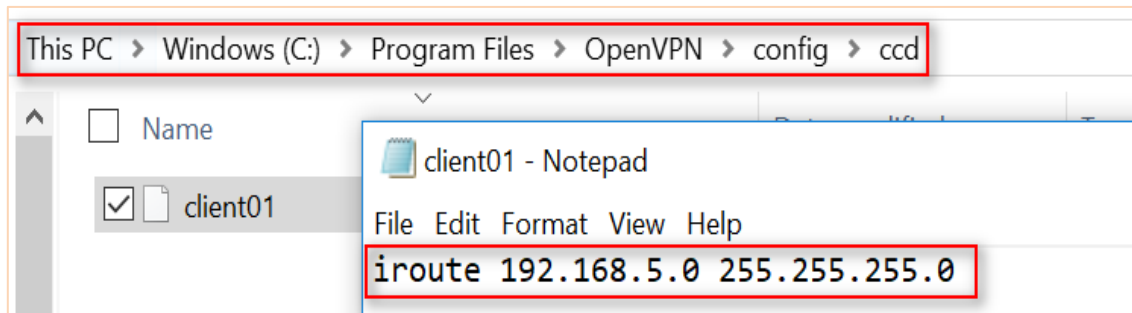
Server Configuration

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

PC > Windows (C) > Program Files > Open VPN > Config

| | |
|--------------------|----------------------|
| ccd | File Folder |
| Ca.crt | Security Certificate |
| Dh2048.pem | PEM File |
| Ipp.txt | Text Document |
| Openvpn-status.log | Text document |
| Server.ovpn | Open VPN Config File |
| Server01.crt | Security Certificate |
| Server01.key | Key File |

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



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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

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

ifconfig-pool-persist ipp.txt
push "route 192.168.10.0 255.255.255.0"
client-config-dir ccd
route 192.168.5.0 255.255.255.0
keepalive 10 120
cipher BF-CBC
comp-lzo
max-clients 100
persist-key
persist-tun
status openvpn-status.log
verb 3
```

6944 Client Configuration

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

The screenshot shows the 'OpenVPN Settings' window. The 'General Settings' tab is active, displaying various configuration fields. The 'Index' is set to 1, 'Enable' is checked, and 'Mode' is set to 'Client'. The 'Protocol' is 'UDP' and 'Connection Type' is 'TUN'. The 'Server Address' is '59.41.92.241' and 'Server Port' is '1194'. The 'Authentication Method' is 'X.509', 'Encryption Type' is 'BF-CBC', 'Renegotiate Interval' is '3600', 'Keepalive Interval' is '20', 'Keepalive Timeout' is '60', 'Fragment' is '1500', 'Private Key Password' is '123456', and 'Output Verbosity Level' is '3'. The 'Advanced Settings' tab is also visible, showing options like 'Enable NAT', 'Enable PKCS#12', 'Enable X.509 Attribute nsCertType', 'Enable HMAC Firewall', and 'Enable Compression LZ0' (checked). There are 'Save' and 'Close' buttons at the bottom right.

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

The screenshot shows the 'X.509 Certificate Import' interface. It has a sidebar with navigation links: Overview, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance. The main area is titled 'X.509 Certificate Import' and shows a 'Connection Index' of 1. Below this, there are several 'Choose File' buttons for importing certificates and keys: 'CA Certificate', 'Local Certificate File', 'Local Private Key', 'HMAC firewall Key', 'Pre-shared Key', and 'PKCS#12 Certificate'. A table titled 'X.509 Certificate Files' lists the imported files:

| Index | File Name | File Size | Date Modified |
|-------|------------|-----------|-------------------------|
| 1 | ca.crt | 1188 | Mon Aug 6 14:03:26 2018 |
| 2 | client.crt | 4382 | Mon Aug 6 14:03:33 2018 |
| 3 | client.key | 1834 | Mon Aug 6 14:03:38 2018 |

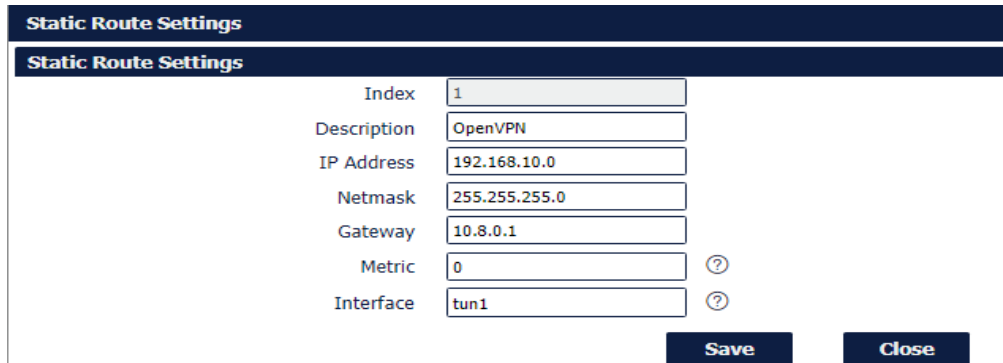
| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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



| OpenVPN Information | | | | | |
|---------------------|--------|-------------|-----------|----------|------------|
| Index | Enable | Description | Status | Uptime | Virtual IP |
| 1 | true | OpenVPN | Connected | 00:00:24 | 10.8.0.6 |

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



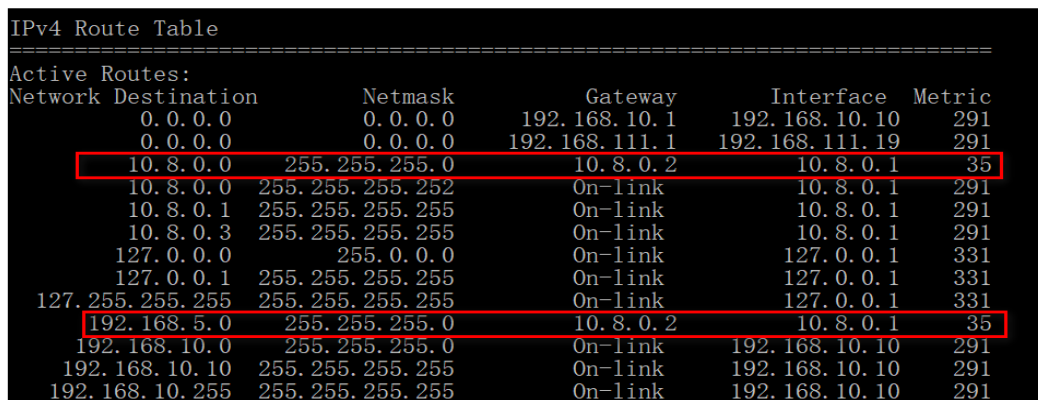
| Static Route Settings | |
|-----------------------|---------------|
| Index | 1 |
| Description | OpenVPN |
| IP Address | 192.168.10.0 |
| Netmask | 255.255.255.0 |
| Gateway | 10.8.0.1 |
| Metric | 0 |
| Interface | tun1 |

Save Close

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

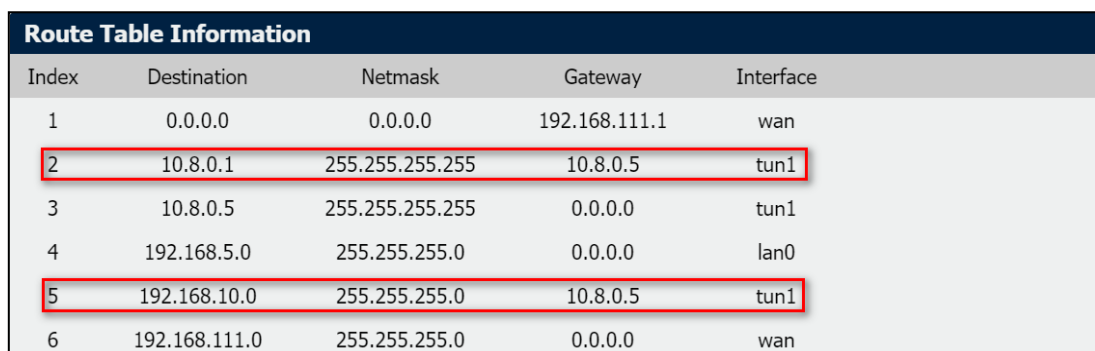
Checking the Routing Table on the Open VPN Server

Check the Routing Table on the OpenVPN Server for reference.



| Network | Destination | Netmask | Gateway | Interface | Metric |
|-----------------|-----------------|-----------------|---------------|----------------|--------|
| 0.0.0.0 | 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 | 0.0.0.0 | 192.168.111.1 | 192.168.111.19 | 291 |
| 10.8.0.0 | 255.255.255.0 | 255.255.255.0 | 10.8.0.2 | 10.8.0.1 | 35 |
| 10.8.0.0 | 255.255.255.252 | 255.255.255.252 | On-link | 10.8.0.1 | 291 |
| 10.8.0.1 | 255.255.255.255 | 255.255.255.255 | On-link | 10.8.0.1 | 291 |
| 10.8.0.3 | 255.255.255.255 | 255.255.255.255 | On-link | 10.8.0.1 | 291 |
| 127.0.0.0 | 255.0.0.0 | 255.0.0.0 | On-link | 127.0.0.1 | 331 |
| 127.0.0.1 | 255.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 127.255.255.255 | 255.255.255.255 | 255.255.255.255 | On-link | 127.0.0.1 | 331 |
| 192.168.5.0 | 255.255.255.0 | 255.255.255.0 | 10.8.0.2 | 10.8.0.1 | 35 |
| 192.168.10.0 | 255.255.255.0 | 255.255.255.0 | On-link | 192.168.10.10 | 291 |
| 192.168.10.10 | 255.255.255.255 | 255.255.255.255 | On-link | 192.168.10.10 | 291 |
| 192.168.10.255 | 255.255.255.255 | 255.255.255.255 | On-link | 192.168.10.10 | 291 |

Check the Routing Table on the OpenVPN Client for reference.



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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Setting NAT

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



Advanced Settings

Enable NAT ☐

Enable PKCS#12 ☐

Enable X.509 Attribute nsCertType ☐

Enable HMAC Firewall ☐

Enable Compression LZ0 ☐

Additional Configurations ?

Testing the VPN

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

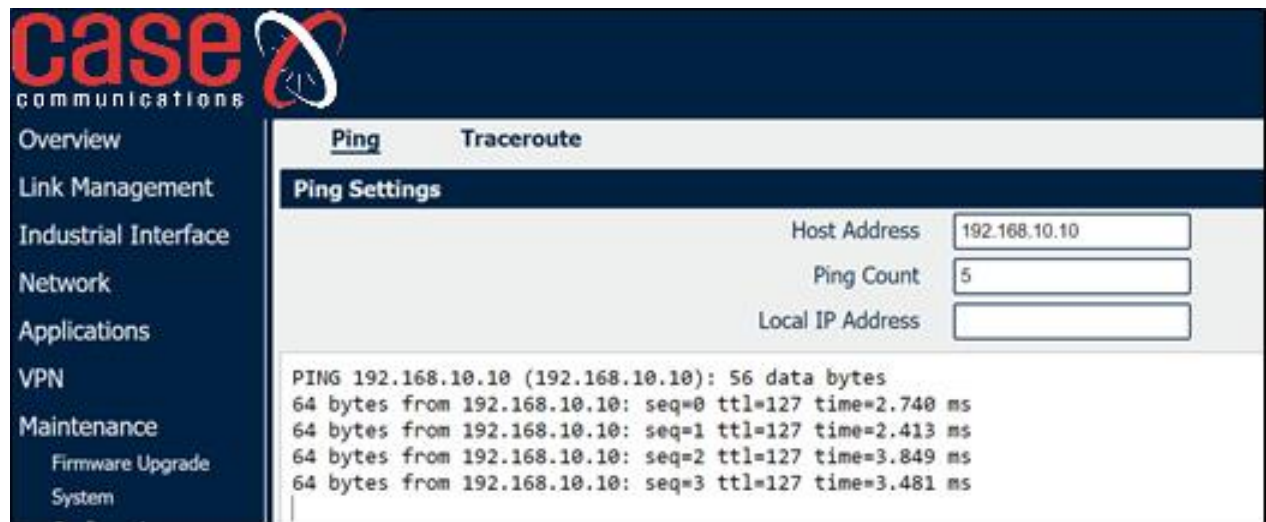
```
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>ping 192.168.5.1

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

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

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



case communications

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

Ping Traceroute

Ping Settings

Host Address: 192.168.10.10

Ping Count: 5

Local IP Address:

PING 192.168.10.10 (192.168.10.10): 56 data bytes

64 bytes from 192.168.10.10: seq=0 ttl=127 time=2.740 ms

64 bytes from 192.168.10.10: seq=1 ttl=127 time=2.413 ms

64 bytes from 192.168.10.10: seq=2 ttl=127 time=3.849 ms

64 bytes from 192.168.10.10: seq=3 ttl=127 time=3.481 ms

Test successful.

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Introduction

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

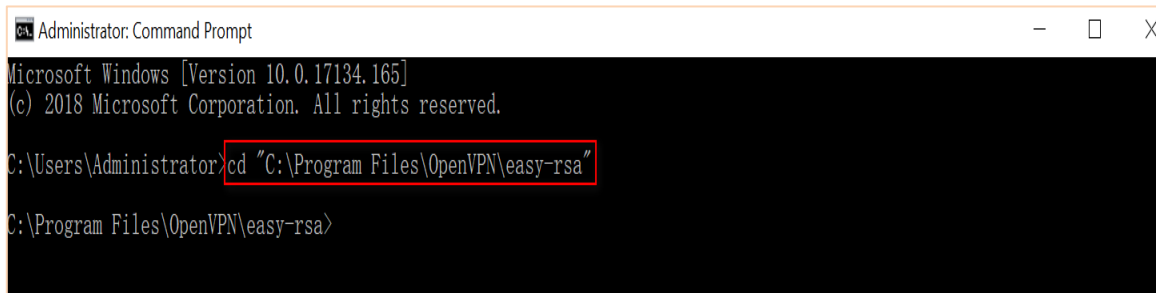
Configuration

Installing OpenVPN Software

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

Generating Certificates

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

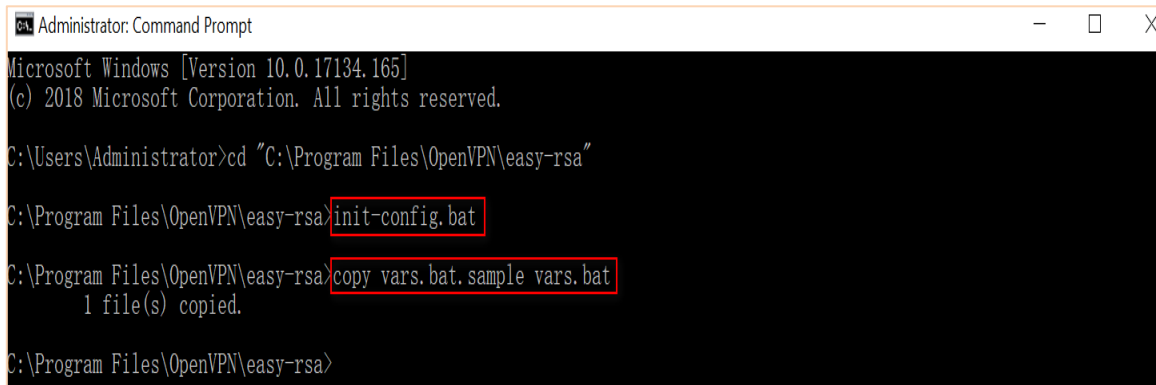


```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.17134.165]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

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

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



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

C:\Users\Administrator>cd "C:\Program Files\OpenVPN\easy-rsa"

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

C:\Program Files\OpenVPN\easy-rsa>copy vars.bat.sample vars.bat
1 file(s) copied.

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

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

Note: The parameters enter without any space between them.

```

1 @echo off
2 rem Edit this variable to point to
3 rem the openssl.cnf file included
4 rem with easy-rsa.
5
6 rem Automatically set PATH to openssl.exe
7 FOR /F "tokens=2*" %%a IN ('REG QUERY "HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"
8
9 rem Alternatively define the PATH to openssl.exe manually
10 rem set "PATH=%PATH%;C:\Program Files\OpenVPN\bin"
11
12 set HOME=%ProgramFiles%\OpenVPN\easy-rsa
13 set KEY_CONFIG=openssl-1.0.0.cnf
14
15 rem Edit this variable to point to
16 rem your soon-to-be-created key
17 rem directory.
18 rem
19 rem WARNING: clean-all will do
20 rem a rm -rf on this directory
21 rem so make sure you define
22 rem it correctly!
23 set KEY_DIR=keys
24
25 rem Increase this if you
26 rem are paranoid. This will slow
27 rem down TLS negotiation performance
28 rem as well as the one-time DH parms
29 rem generation process.
30 set DH_KEY_SIZE=2048
31
32 rem Private key size
33 set KEY_SIZE=4096
34
35 rem These are the default values for fields
36 rem which will be placed in the certificate.
37 rem Change these to reflect your site.
38 rem Don't leave any of these parms blank.
39
40 set KEY_COUNTRY=CN
41 set KEY_PROVINCE=GD
42 set KEY_CITY=Guangzhou
43 set KEY_ORG=OpenVPN
44 set KEY_EMAIL=mail@navigatoworx.domain
45 set KEY_CN=OpenVPN
46 set KEY_NAME=OpenVPN
47 set KEY_OU=OpenVPN
48 set PKCS11_MODULE_PATH=changeme
49 set PKCS11_PIN=1234
50

```

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

```

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

```

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

```

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

```

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

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

```

C:\Program Files\OpenVPN\easy-rsa> build-key-server.bat server01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.....**
writing new private key to 'keys\server01.key'

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [ ]:
State or Province Name (full name) [ ]:
Locality Name (eg, city) [ ]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]: server01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

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

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

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

```

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

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

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

```

Administrator: Command Prompt
C:\Program Files\OpenVPN\easy-rsa> build-key-pass.bat client01
WARNING: can't open config file: /etc/ssl/openssl.cnf
Generating a 4096 bit RSA private key
.....**
writing new private key to 'keys\client01.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase: ← Setup Private Key Password

You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value.
If you enter '.', the field will be left blank.

-----
Country Name (2 letter code) [ ]:
State or Province Name (full name) [ ]:
Locality Name (eg, city) [Guangzhou]:
Organization Name (eg, company) [OpenVPN]:
Organizational Unit Name (eg, section) [OpenVPN]:
Common Name (eg, your name or your server's hostname) [OpenVPN]: client01
Name [OpenVPN]:
Email Address [mail@navigateworx.domain]:

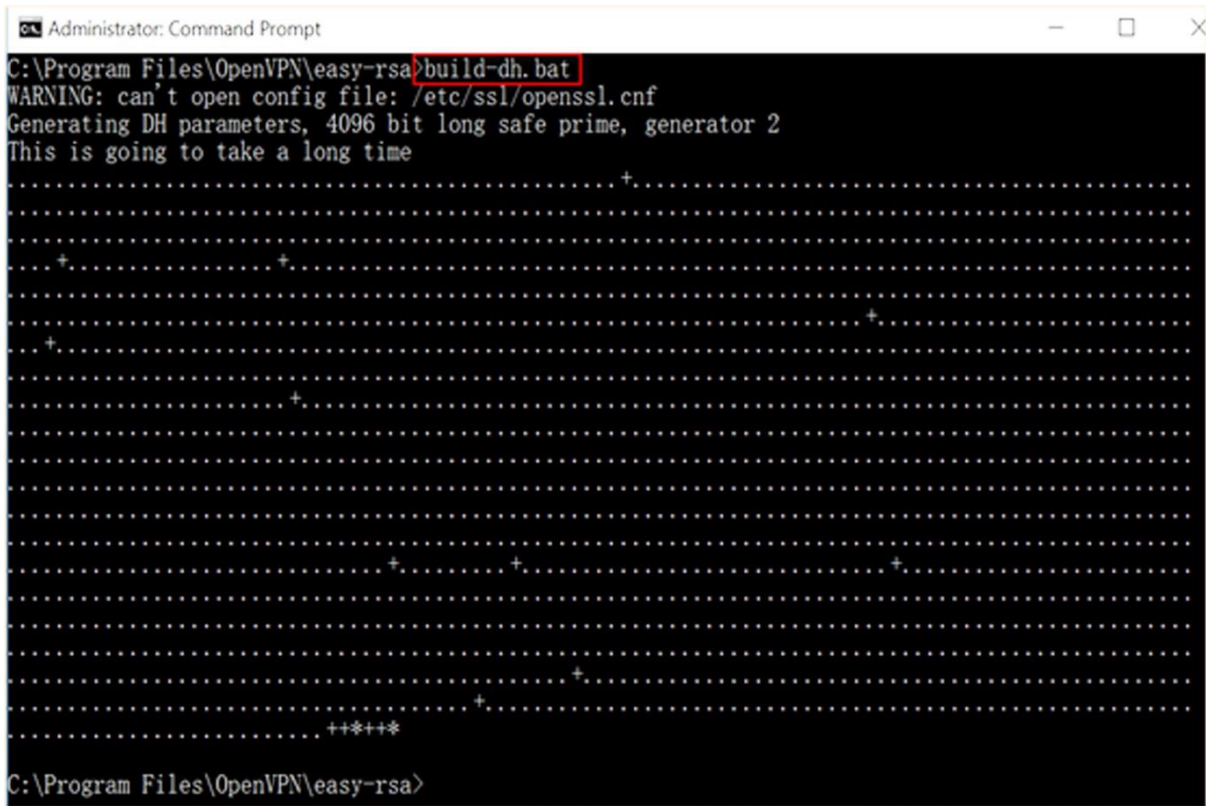
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password [ ]:
An optional company name [ ]:
WARNING: can't open config file: /etc/ssl/openssl.cnf
Using configuration from openssl-1.0.0.cnf
Check that the request matches the signature
Signature ok
The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

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

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

```

Step 8. Generate Diffie Hellman parameters.



This PC > Windows (C:) > Program Files > OpenVPN > easy-rsa > keys

| Name | Date modified | Type | Size |
|----------------|-------------------|----------------------|------|
| 01.pem | 9/14/2018 7:55 PM | PEM File | 8 KB |
| 02.pem | 9/14/2018 8:05 PM | PEM File | 8 KB |
| ca.crt | 9/14/2018 7:48 PM | Security Certificate | 3 KB |
| ca.key | 9/14/2018 7:48 PM | KEY File | 4 KB |
| client01.crt | 9/14/2018 8:05 PM | Security Certificate | 8 KB |
| client01.csr | 9/14/2018 8:05 PM | CSR File | 2 KB |
| client01.key | 9/14/2018 8:05 PM | KEY File | 4 KB |
| dh4096.pem | 9/14/2018 8:15 PM | PEM File | 1 KB |
| index.txt | 9/14/2018 8:05 PM | Text Document | 1 KB |
| index.txt.attr | 9/14/2018 8:05 PM | ATTR File | 1 KB |
| serial | 9/14/2018 8:05 PM | File | 1 KB |
| server01.crt | 9/14/2018 7:55 PM | Security Certificate | 8 KB |
| server01.csr | 9/14/2018 7:54 PM | CSR File | 2 KB |
| server01.key | 9/14/2018 7:54 PM | KEY File | 4 KB |

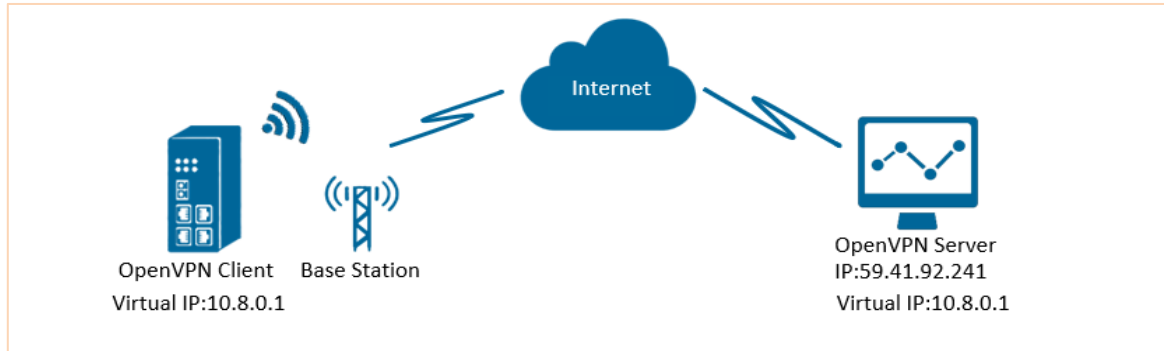
| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Overview

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

Testing Topology

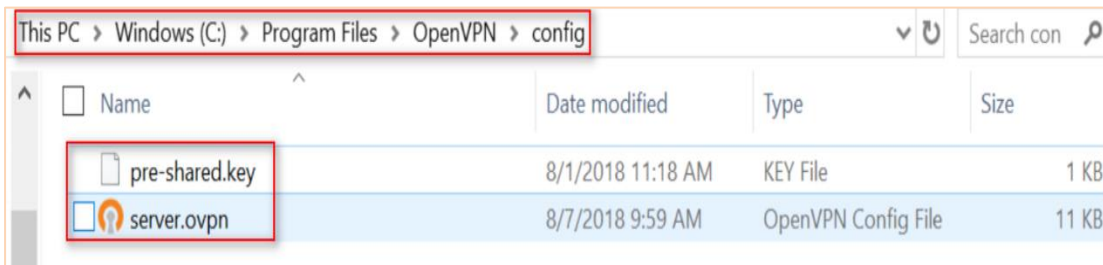


- The 6944 runs as an OpenVPN Client on an IP Network capable of pinging an IP OpenVPN server successfully.
- A PC runs as an OpenVPN Server with a **static** public IP address and opens a specified listening port for OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, allowing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

Configuring an Open VPN Client with a pre-shared key

Server Configuration

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



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

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

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

Client Configuration

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

Step 2. Click Save>Apply.

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

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

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Static Route Settings

Static Route Settings

Index

1

Description

OpenVPN

IP Address

192.168.10.0

Netmask

255.255.255.0

Gateway

10.8.0.1

Metric

0

Interface

tun1

Save

Close

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

Step7: Click Save>Apply

Checking the Routing Table

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

```
IPv4 Route Table
=====
Active Routes:
Network Destination        Netmask          Gateway          Interface        Metric
0.0.0.0                  0.0.0.0          192.168.111.1    192.168.111.19   291
0.0.0.0                  0.0.0.0          192.168.10.1     192.168.10.10    291
10.8.0.0                255.255.255.252   On-link          10.8.0.1         291
10.8.0.1                255.255.255.255   On-link          10.8.0.1         291
10.8.0.3                255.255.255.255   On-link          10.8.0.1         291
127.0.0.0                255.0.0.0         On-link          127.0.0.1        331
192.168.0.0              255.255.255.0     On-link          192.168.0.1      291
```

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

| Route Table Information | | | | |
|-------------------------|---------------|-----------------|---------------|-----------|
| Index | Destination | Netmask | Gateway | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | wan |
| 2 | 10.8.0.1 | 255.255.255.255 | 0.0.0.0 | tun1 |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | wan |

Testing the Open VPN with a Pre-Shared Key

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

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

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

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

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

case

communications

Overview

Link Management

Industrial Interface

Network

Applications

VPN

Maintenance

Firmware Upgrade

System

Configuration

Debug Tools

Ping

Traceroute

Ping Settings

Host Address

10.8.0.1

Ping Count

5

Local IP Address

PING 10.8.0.1 (10.8.0.1): 56 data bytes

64 bytes from 10.8.0.1: seq=0 ttl=128 time=3.077 ms

64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.567 ms

64 bytes from 10.8.0.1: seq=2 ttl=128 time=3.259 ms

64 bytes from 10.8.0.1: seq=3 ttl=128 time=2.571 ms

64 bytes from 10.8.0.1: seq=4 ttl=128 time=3.347 ms

10.8.0.1 ping statistics ---

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

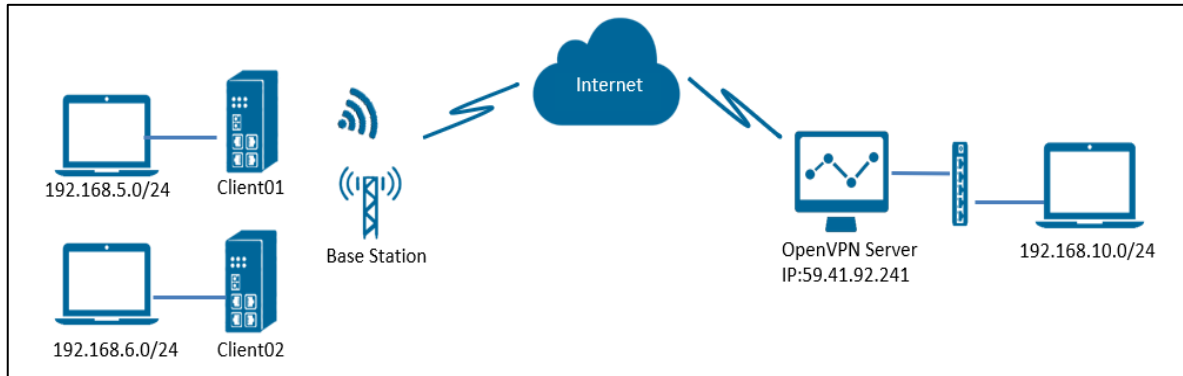
round-trip min/avg/max = 2.571/3.164/3.567 ms

11.6. AN008-Open VPN Client with Username and Password

Overview

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

Testing Topology

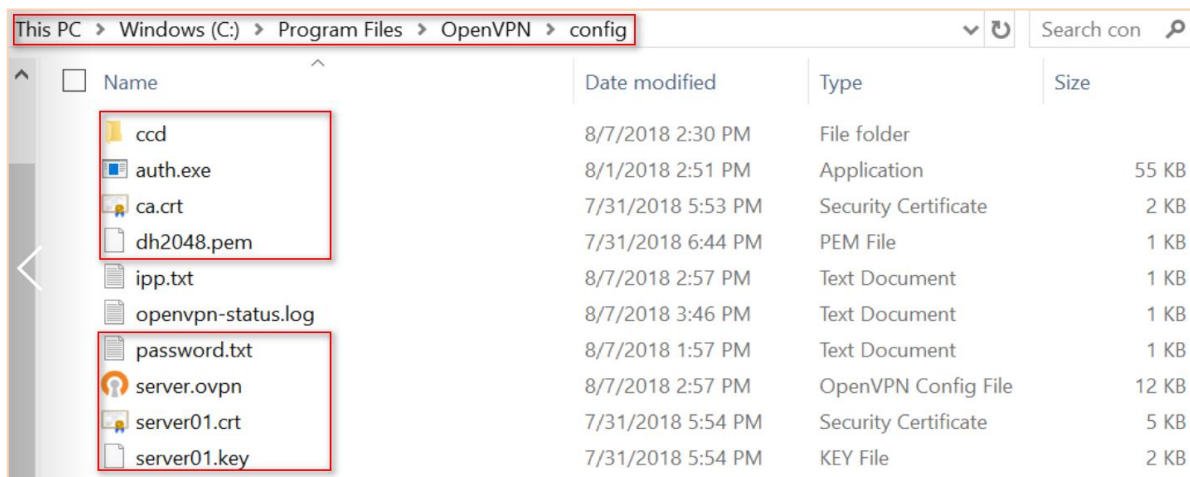


- Two 6944s run as OpenVPN Clients, Client01 and Client02 on an IP network, which can ping an OpenVPN server IP successfully.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified port for listening for the OpenVPN.
- The OpenVPN tunnel is established between the Server and the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

Configuration

Server Configuration

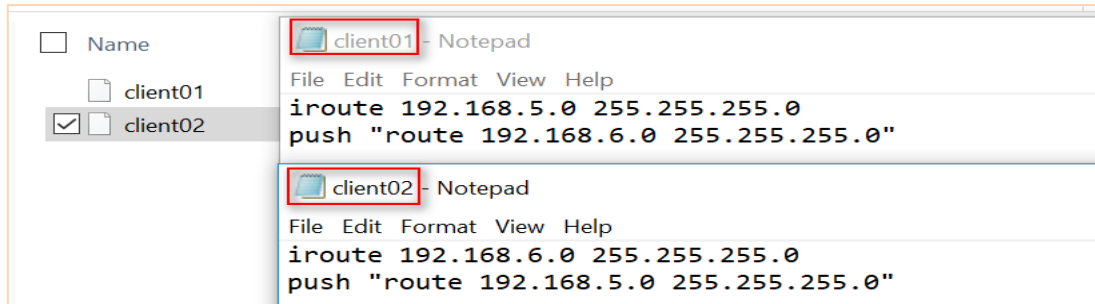
Step1. Install OpenVPN software on your PC and copy the related certificates and configuration to the PC as shown below:



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

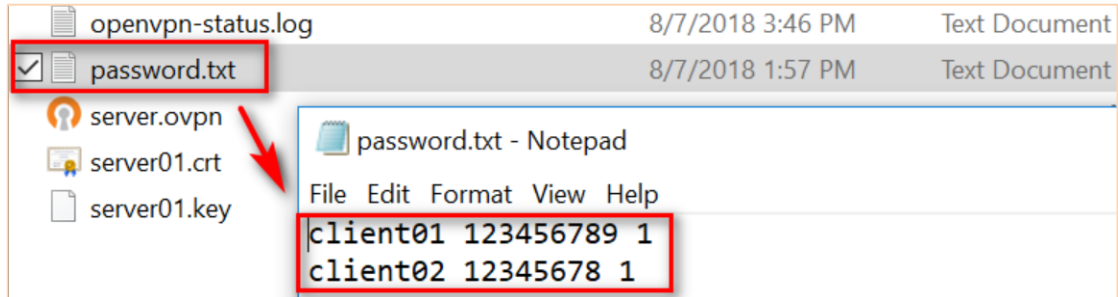
Step 2. Add a “ccd” folder, and create a new notepad, rename it without a suffix, configure as shown below:

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |



Note: client01 and client02 are the common name.

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



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

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

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Client01 Configuration

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

OpenVPN Settings

General Settings

Index: 1

Enable: ☒

Description:

Mode: Client

Protocol: UDP

Connection Type: TUN

Server Address: 59.41.92.241

Server Port: 1194

Authentication Method: Password

Encryption Type: BF-CBC

Username: client01

Password: 123456789

Renegotiate Interval: 3600

Keepalive Interval: 20

Keepalive Timeout: 60

Fragment: 1500

Output Verbosity Level: 3

Advanced Settings

Enable NAT: ☒

Enable HMAC Firewall: ☐

Enable Compression LZ0: ☒

Additional Configurations:

Save Close

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

case
communications

Overview
Link Management
Industrial Interface
Network
Applications
VPN
OpenVPN
Maintenance

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 |
|-------|-----------|-----------|-------------------------|
| 1 | ca.crt | 1188 | Tue Aug 7 14:17:06 2018 |

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

case
communications

Overview
Link Management
Industrial Interface
Network

Status OpenVPN X.509 Certificate

OpenVPN Information

| Index | Enable | Description | Status | Uptime | Virtual IP |
|-------|--------|-------------|-----------|----------|------------|
| 1 | true | 12 | Connected | 00:22:10 | 10.8.0.6 |

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

| Static Route Settings | |
|-----------------------|---------------|
| Index | 1 |
| Description | OpenVPN |
| IP Address | 192.168.10.0 |
| Netmask | 255.255.255.0 |
| Gateway | 10.8.0.1 |
| Metric | 0 |
| Interface | tun1 |
| <div>Save Close</div> | |

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

Client02 Configuration

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

| 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 | Password |
| Encryption Type | BF-CBC |
| Username | client02 |
| Password | 12345678 |
| Renegotiate Interval | 3600 |
| Keepalive Interval | 20 |
| Keepalive Timeout | 60 |
| Fragment | 1500 |
| Output Verbosity Level | 3 |
| Advanced Settings | |
| Enable NAT | <input checked="" type="checkbox"/> |
| Enable HMAC Firewall | <input type="checkbox"/> |
| Enable Compression LZ0 | <input checked="" type="checkbox"/> |
| Additional Configurations | |
| <div>Save Close</div> | |

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

| case communications | |
|-------------------------|---|
| Overview | Status OpenVPN X.509 Certificate |
| Link Management | X.509 Certificate Import |
| Industrial Interface | Connection Index 1 |
| Network | CA Certificate Choose File No file chosen |
| Applications | Local Certificate File Choose File No file chosen |
| VPN | Local Private Key Choose File No file chosen |
| OpenVPN | HMAC firewall Key Choose File No file chosen |
| Maintenance | 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 Tue Aug 7 14:17:06 2018 |

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |



Overview

Link Management

Industrial Interface

Network

Status

OpenVPN

X.509 Certificate

OpenVPN Information

| Index | Enable | Description | Status | Uptime | Virtual IP |
|-------|--------|-------------|-----------|----------|------------|
| 1 | true | user-pass | Connected | 00:13:00 | 10.8.0.10 |

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

| Static Route Settings | |
|-----------------------|---------------|
| Index | 1 |
| Description | OpenVPN |
| IP Address | 192.168.10.0 |
| Netmask | 255.255.255.0 |
| Gateway | 10.8.0.1 |
| Metric | 0 |
| Interface | tun1 |
| <div>Save Close</div> | |

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

Checking the Routing Tables

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

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

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

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

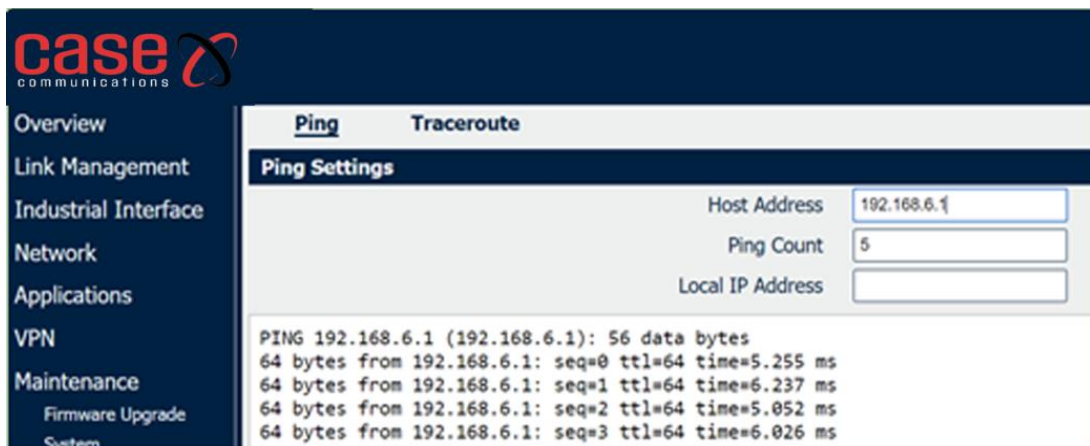
Step 3: Check the Routing Table on Client02 for reference.

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Testing

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



The screenshot shows the Case Communications web interface. On the left is a navigation menu with options: Overview, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance (with sub-options Firmware Upgrade and System). The main content area has tabs for 'Ping' and 'Traceroute'. The 'Ping' tab is active, showing 'Ping Settings' with fields for 'Host Address' (192.168.6.1), 'Ping Count' (5), and 'Local IP Address'. Below the settings, the ping results are displayed:

```

PING 192.168.6.1 (192.168.6.1): 56 data bytes
64 bytes from 192.168.6.1: seq=0 ttl=64 time=5.255 ms
64 bytes from 192.168.6.1: seq=1 ttl=64 time=6.237 ms
64 bytes from 192.168.6.1: seq=2 ttl=64 time=5.052 ms
64 bytes from 192.168.6.1: seq=3 ttl=64 time=6.026 ms
  
```

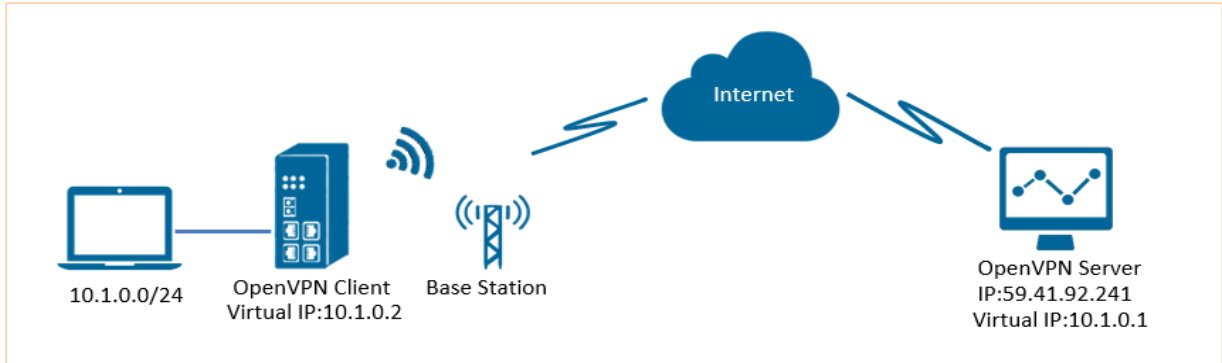
Step 2 and 3: Repeat the Ping test from Client 02 to client 01

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

Overview

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

Testing Topology

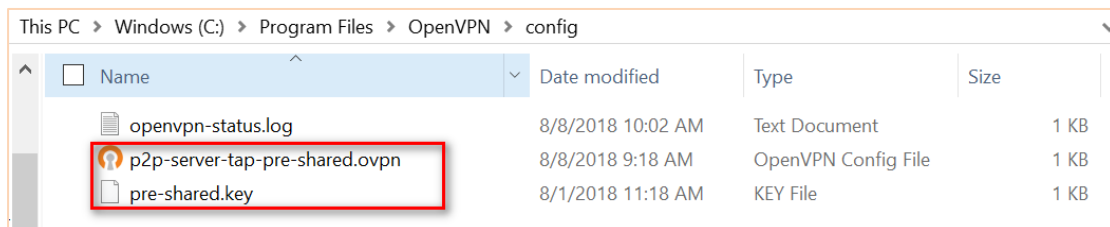


- The 6944 runs as an OpenVPN Client which can ping the OpenVPN IP servers.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified port a listening for an OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, the virtual IP can PING each other successfully.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

Configuration

Server Configuration

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



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

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

```

mode p2p
port 1194
proto udp
dev tap
# tap
ifconfig 10.1.0.1 255.255.255.0
keepalive 20 120
persist-key

persist-tun
secret pre-shared.key # None TLS Mode
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
  
```


| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Client Configuration

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

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

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

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

| Index | Enable | Description | Status | Uptime | Virtual IP |
|-------|--------|-------------|-----------|----------|------------|
| 1 | true | | Connected | 00:15:58 | 10.1.0.2 |

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Static Route Settings

Static Route Settings

| | |
|-------------|-----------------|
| Index | 1 |
| Description | OpenVPN |
| IP Address | 59.41.92.241 |
| Netmask | 255.255.255.255 |
| Gateway | 10.1.0.1 |
| Metric | 0 |
| Interface | tun1 |

Save Close

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

Step 7: Click Save>Apply

Routing Table

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

IPv4 Route Table

```
=====
```

Active Routes:

| Network | Destination | Netmask | Gateway | Interface | Metric |
|---------|-------------|-----------------|---------------|----------------|--------|
| | 0.0.0.0 | 0.0.0.0 | 192.168.10.1 | 192.168.10.10 | 291 |
| | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | 192.168.111.19 | 291 |
| | 10.1.0.0 | 255.255.255.0 | On-link | 10.1.0.1 | 291 |
| | 10.1.0.1 | 255.255.255.255 | On-link | 10.1.0.1 | 291 |
| | 10.1.0.255 | 255.255.255.255 | On-link | 10.1.0.1 | 291 |
| | 127.0.0.0 | 255.0.0.0 | On-link | 127.0.0.1 | 331 |

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

| Route Table Information | | | | |
|-------------------------|---------------|---------------|---------------|-----------|
| Index | Destination | Netmask | Gateway | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | wan |
| 2 | 10.1.0.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | wan |

Testing

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

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

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

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

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

Step 3: Receive the Ping Reply to for success.

11.8. AN010- OpenVPN Client_with_TAP_under_P2P_mode

Overview

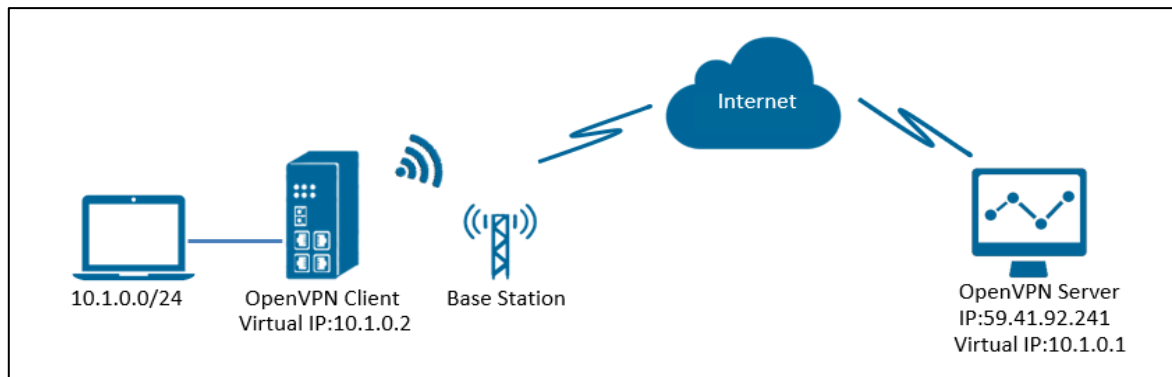
This document contains information regarding the configuration and use of a 6944 Industrial router running OpenVPN with TAP running under P2P mode,

Software Version

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

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

Testing Topology

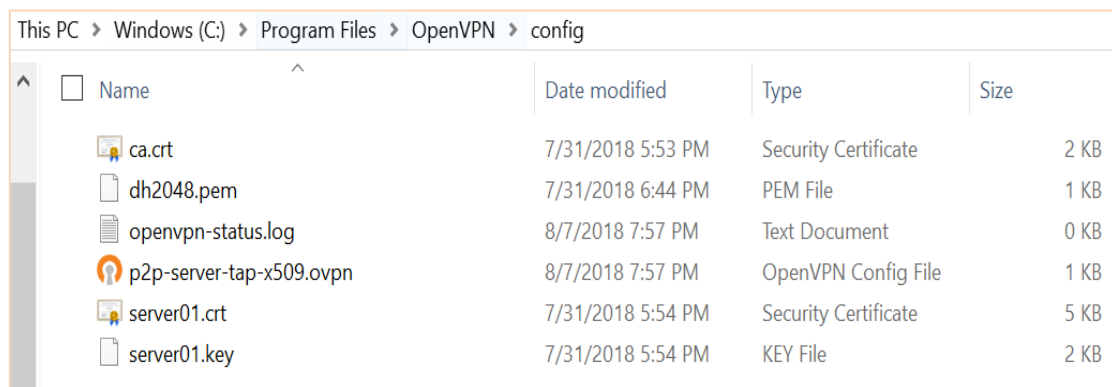


- The 6944 runs as an OpenVPN Client with any kind of IP, which can ping an OpenVPN IP server successfully.
- A PC runs as an OpenVPN Server with a static public IP and opens a specified a port listening for an OpenVPN.
- An OpenVPN tunnel is established between the Server and Client, the virtual IP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

Configuration

Server Configuration

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



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

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

```

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

```

Router Configuration

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

The screenshot shows the 'OpenVPN Settings' window with two tabs: 'General Settings' and 'Advanced Settings'.

General Settings:

- Index: 1
- Enable: ☒
- Description: 1
- Mode: P2P
- Protocol: UDP
- Connection Type: TAP
- Server Address: 59.41.92.241
- Server Port: 1194
- Authentication Method: X.509
- Encryption Type: BF-CBC
- Local IP Address: 10.1.0.2
- Local Netmask: 255.255.255.0
- TAP Bridge: LAN0
- Renegotiate Interval: 3600
- Keepalive Interval: 20
- Keepalive Timeout: 60
- Fragment: 1500
- Private Key Password: 123456
- Output Verbosity Level: 3

Advanced Settings:

- Enable NAT: ☒
- Enable PKCS#12: ☐
- Enable X.509 Attribute nsCertType: ☐
- Enable HMAC Firewall: ☐
- Enable Compression LZ0: ☒
- Additional Configurations:

Buttons: Save, Close

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

| Index | File Name | File Size | Date Modified |
|-------|------------|-----------|-------------------------|
| 1 | ca.crt | 1188 | Tue Aug 7 17:39:32 2018 |
| 2 | client.crt | 4382 | Tue Aug 7 17:39:43 2018 |
| 3 | client.key | 1834 | Tue Aug 7 17:39:48 2018 |

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

| Index | Enable | Description | Status | Uptime | Virtual IP |
|-------|--------|-------------|-----------|----------|------------|
| 1 | true | 1 | Connected | 00:16:51 | 10.1.0.2 |

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

| | |
|-------------|-----------------|
| Index | 1 |
| Description | OpenVPN |
| IP Address | 59.41.92.241 |
| Netmask | 255.255.255.255 |
| Gateway | 10.1.0.1 |
| Metric | 0 |
| Interface | tun1 |

Save **Close**

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Routing Table

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

IPv4 Route Table

```
=====
```

Active Routes:

| Network | Destination | Netmask | Gateway | Interface | Metric |
|---------|-------------|-----------------|---------------|----------------|--------|
| | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | 192.168.111.19 | 291 |
| | 0.0.0.0 | 0.0.0.0 | 192.168.10.1 | 192.168.10.10 | 291 |
| | 10.1.0.0 | 255.255.255.0 | On-link | 10.1.0.1 | 291 |
| | 10.1.0.1 | 255.255.255.255 | On-link | 10.1.0.1 | 291 |
| | 10.1.0.255 | 255.255.255.255 | On-link | 10.1.0.1 | 291 |

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

| Route Table Information | | | | |
|-------------------------|---------------|---------------|---------------|-----------|
| Index | Destination | Netmask | Gateway | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | wan |
| 2 | 10.1.0.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | wan |

Testing

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

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

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

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

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

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

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

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

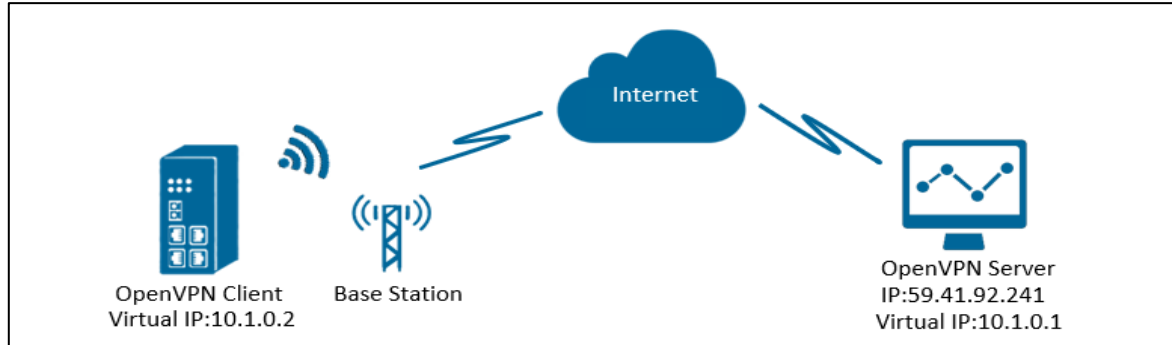
Step 3: Test successfully.

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

Overview

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

Testing Topology

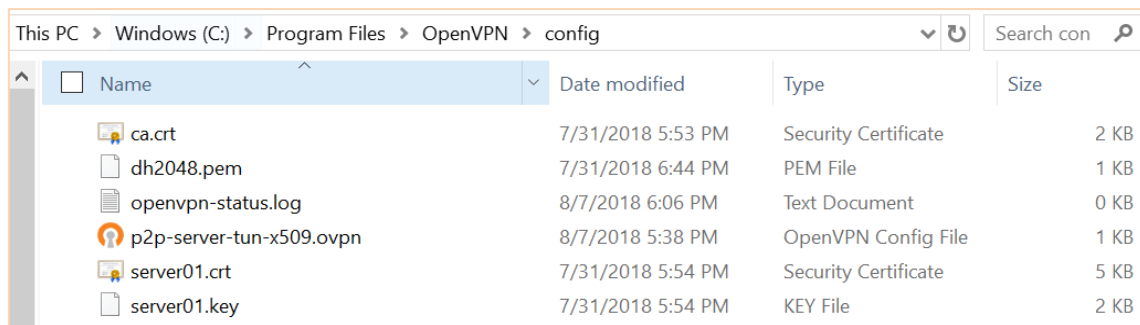


- The 6944 runs as an OpenVPN Client with any kind of IP, which can ping an OpenVPN IP server successfully.
- A PC runs as an OpenVPN Server with a static public IP address and opens a specific listening port for an OpenVPN.
- If the OpenVPN tunnel is established between the Server and Client, the virtual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

Configuration

Server Configuration

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



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

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

```

mode p2p
port 1194
proto udp
dev tun
# tun
ifconfig 10.8.0.1 10.8.0.2
keepalive 20 120

persist-key
persist-tun
tls-server
ca ca.crt
cert server01.crt
key server01.key
dh dh2048.pem

#tls-auth ta.key 0
cipher BF-CBC
comp-lzo
status openvpn-status.log
verb 3
tun-mtu 1500
fragment 1500
  
```

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Router Configuration

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

Step 2: Click Save>Apply.

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

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

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Static Route Settings

Static Route Settings

Index

1

Description

OpenVPN

IP Address

59.41.92.241

Netmask

255.255.255.255

Gateway

10.1.0.1

Metric

0

?

Interface

tun1

?

Save

Close

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

Step 7: Click Save>Apply

Checking the Routing Table

Step 1: Check the Routing Table on your PC

```

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

Step 2: Check the Routing Table on router

| Route Table Information | | | | |
|-------------------------|---------------|-----------------|---------------|-----------|
| Index | Destination | Netmask | Gateway | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | wan |
| 2 | 10.8.0.1 | 255.255.255.255 | 0.0.0.0 | tun1 |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | lan0 |
| 4 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | wan |

Step 3: Test Successful

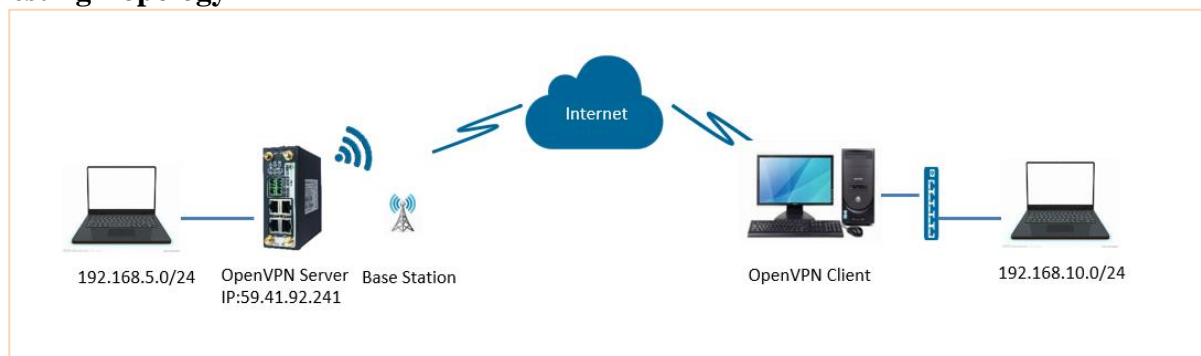
| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Overview

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

Testing Topology



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

Configuration

Server Configuration

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

| OpenVPN Settings | |
|---------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | OpenVPN |
| Mode | Server |
| Protocol | UDP |
| Connection Type | TUN |
| Max Clients | 5 |
| Authentication Method | X.509 |
| Encryption Type | AES-256-CBC |
| Local IP Address | |
| Local Port | 1194 |
| Topology | Subnet |
| Subnet | 10.8.0.0 |
| Subnet Netmask | 255.255.255.0 |
| Renegotiate Interval | 3600 |
| Keepalive Interval | 10 |
| Keepalive Timeout | 120 |
| Fragment | 0 |
| Private Key Password | 123456 |
| Output Verbosity Level | 3 |
| Advanced Settings | |
| Enable NAT | <input checked="" type="checkbox"/> |
| Enable Default Gateway | <input type="checkbox"/> |
| Enable PKCS#12 | <input type="checkbox"/> |
| Enable CRL | <input type="checkbox"/> |
| Enable Client to Client | <input type="checkbox"/> |
| Enable Duplicate CN | <input type="checkbox"/> |
| Enable IP Persist | <input type="checkbox"/> |
| Enable HMAC Firewall | <input type="checkbox"/> |
| Enable Compression LZ0 | <input checked="" type="checkbox"/> |
| Additional Configurations | |

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

Route Settings

Route Management

| Index | Enable | Route | Push Route |
|-------|-------------------------------------|-----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | 192.168.10.0/24 | 192.168.5.0/24 |

☐ Enable Duplicate CN
☐ Enable IP Persist
☐ Enable HMAC Firewall
☒ Enable Compression LZ0
 Additional Configurations ?

Save **Close**

Route Management

| Index | Enable | Route | Push Route | |
|-------|--------|-------|------------|---|
| | | | | + |

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

Client Settings

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route |
|-------|-------------------------------------|-------------|-------------------|-----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | client01 | | 192.168.10.0/24 | 192.168.5.0/24 |

☒ Enable Compression LZ0
 Additional Configurations ?

Save **Close**

Route Management

| Index | Enable | Route | Push Route | |
|-------|--------|-----------------|----------------|-----|
| 1 | true | 192.168.10.0/24 | 192.168.5.0/24 | ✎ ✕ |

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route | |
|-------|--------|-------------|-------------------|----------------|------------|---|
| | | | | | | + |

Step 4: After that, click Save>Apply.

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

Status OpenVPN X.509 Certificate

X.509 Certificate Import

OpenVPN Mode: Server

CA Certificate: Choose File No file chosen **ca.crt**

Local Certificate File: Choose File No file chosen **xx.crt**

Local Private Key: Choose File No file chosen **xx.key**

DH File: Choose File No file chosen **dh.pem**

HMAC Firewall Key: Choose File No file chosen

PKCS#12 Certificate: Choose File No file chosen

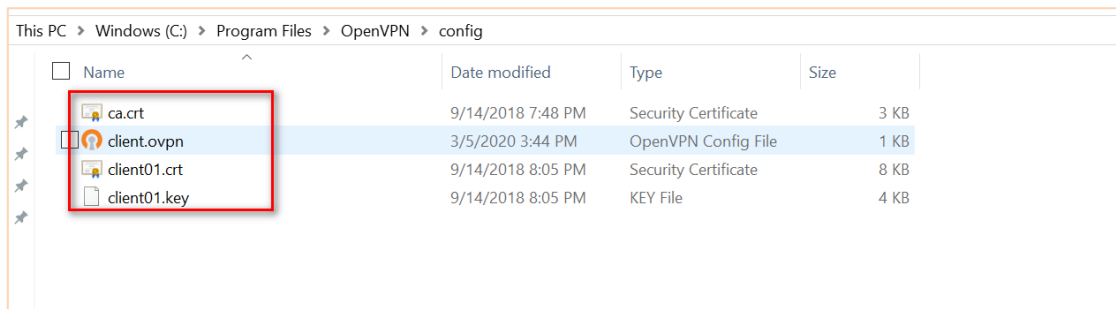
CRL File: Choose File No file chosen

X.509 Certificate Files

| Index | File Name | File Size | Date Modified |
|-------|------------|-----------|-------------------------|
| 1 | ca.crt | 2399 | Thu Mar 5 08:40:08 2020 |
| 2 | dh.pem | 769 | Thu Mar 5 08:40:45 2020 |
| 3 | server.crt | 8192 | Thu Mar 5 08:40:16 2020 |
| 4 | server.key | 3272 | Thu Mar 5 08:40:23 2020 |

Client Configuration

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



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

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

```

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

Routing Table

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

Status

Static Route

Route Table Information

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

Step 2: Route Table on OpenVPN Client for reference.

Select Administrator: Command Prompt

Active Routes:

| Network | Destination | Netmask | Gateway | Interface | Metric |
|-----------------|-----------------|----------|---------------|---------------|--------|
| 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 192.168.10.1 | 192.168.10.10 | 291 |
| 0.0.0.0 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | 192.168.111.4 | 35 |
| 10.8.0.0 | 255.255.255.0 | 0n-link | 10.8.0.2 | 291 | |
| 10.8.0.2 | 255.255.255.255 | 0n-link | 10.8.0.2 | 291 | |
| 10.8.0.255 | 255.255.255.255 | 0n-link | 10.8.0.2 | 291 | |
| 127.0.0.0 | 255.0.0.0 | 0n-link | 127.0.0.1 | 331 | |
| 127.0.0.1 | 255.255.255.255 | 0n-link | 127.0.0.1 | 331 | |
| 127.255.255.255 | 255.255.255.255 | 0n-link | 127.0.0.1 | 331 | |
| 192.168.5.0 | 255.255.255.0 | 10.8.0.1 | 10.8.0.2 | 35 | |
| 192.168.10.0 | 255.255.255.0 | 0n-link | 192.168.10.10 | 291 | |
| 192.168.10.10 | 255.255.255.255 | 0n-link | 192.168.10.10 | 291 | |

Testing


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

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

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

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

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



Overview

Link Management

Industrial Interface

Network

Applications

VPN

Maintenance

Firmware Upgrade

System

Ping Traceroute

Ping Settings

Host Address

Ping Count

Local IP Address

PING 10.8.0.1 (10.8.0.1): 56 data bytes

64 bytes from 10.8.0.1: seq=0 ttl=128 time=2.788 ms

64 bytes from 10.8.0.1: seq=1 ttl=128 time=3.141 ms

64 bytes from 10.8.0.1: seq=2 ttl=128 time=4.433 ms

64 bytes from 10.8.0.1: seq=3 ttl=128 time=3.103 ms

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

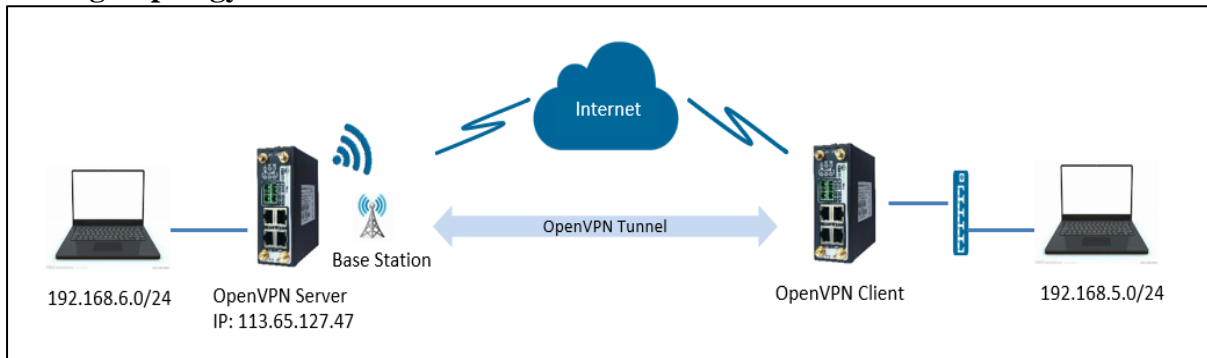
Overview

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

Compatibility

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

Testing Topology



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

Configuration

Server Configuration

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

| OpenVPN Settings | |
|---------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | |
| Mode | Server |
| Protocol | UDP |
| Connection Type | TUN |
| Max Clients | 5 |
| Authentication Method | X.509 |
| Encryption Type | BF-CBC |
| Local IP Address | |
| Local Port | 1194 |
| Topology | Subnet |
| Subnet | 10.8.0.0 |
| Subnet Netmask | 255.255.255.0 |
| Renegotiate Interval | 3600 |
| Keepalive Interval | 20 |
| Keepalive Timeout | 60 |
| Fragment | 1500 |
| Private Key Password | |
| Output Verbosity Level | 3 |
| Advanced Settings | |
| Enable NAT | <input checked="" type="checkbox"/> |
| Enable Default Gateway | <input type="checkbox"/> |
| Enable PKCS#12 | <input type="checkbox"/> |
| Enable CRL | <input type="checkbox"/> |
| Enable Client to Client | <input checked="" type="checkbox"/> |
| Enable Duplicate CN | <input type="checkbox"/> |
| Enable IP Persist | <input type="checkbox"/> |
| Enable HMAC Firewall | <input type="checkbox"/> |
| Enable Compression LZ0 | <input checked="" type="checkbox"/> |
| Additional Configurations | |

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

Route Settings

Route Management

| Index | Enable | Route | Push Route |
|-------|-------------------------------------|----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | 192.168.5.0/24 | 192.168.6.0/24 |

Save Close

Enable Duplicate CN ☐
 Enable IP Persist ☐
 Enable HMAC Firewall ☐
 Enable Compression LZ0 ☒
 Additional Configurations

Route Management

| Index | Enable | Route | Push Route |
|-------|--------|----------------|----------------|
| 1 | true | 192.168.5.0/24 | 192.168.6.0/24 |

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

Client Settings

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route |
|-------|-------------------------------------|-------------|-------------------|----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | client06 | | 192.168.5.0/24 | 192.168.6.0/24 |

Save Close

Enable HMAC Firewall ☐
 Enable Compression LZ0 ☒
 Additional Configurations

Route Management

| Index | Enable | Route | Push Route |
|-------|--------|----------------|----------------|
| 1 | true | 192.168.5.0/24 | 192.168.6.0/24 |

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route |
|-------|--------|-------------|-------------------|----------------|----------------|
| 1 | true | client06 | | 192.168.5.0/24 | 192.168.6.0/24 |

Step 4: After that, click Save>Apply.

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

X.509 Certificate Import

OpenVPN Mode: Server

CA Certificate: Choose File No file chosen ca.crt

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

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

DH File: Choose File No file chosen dh.pem

HMAC Firewall Key: Choose File No file chosen

PKCS#12 Certificate: Choose File No file chosen

CRL File: Choose File No file chosen

X.509 Certificate Files

| Index | File Name | File Size | Date Modified |
|-------|------------|-----------|-------------------------|
| 1 | ca.crt | 2399 | Thu Mar 5 08:40:08 2020 |
| 2 | dh.pem | 769 | Thu Mar 5 08:40:45 2020 |
| 3 | server.crt | 8192 | Thu Mar 5 08:40:16 2020 |
| 4 | server.key | 3272 | Thu Mar 5 08:40:23 2020 |

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Client Configuration

Step 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: ☒
Description: 1
Mode: Client
Protocol: UDP
Connection Type: TUN
Server Address: 113.65.127.47
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:
Output Verbosity Level: 3

Advanced Settings

Enable NAT: ☒
Enable PKCS#12: ☐
Enable X.509 Attribute nsCertType: ☐
Enable HMAC Firewall: ☐
Enable Compression LZ0: ☒
Additional Configurations:

SaveClose

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

StatusOpenVPNX.509 CertificateConfiguration Files

X.509 Certificate Import

OpenVPN Mode: Client
Connection Index: 1
CA Certificate: Choose File No file chosen ca.crt
Local Certificate File: Choose File No file chosen xx.crt
Local Private Key: Choose File No file chosen xx.key
HMAC Firewall Key: Choose File No file chosen
Pre-shared Key: Choose File No file chosen
PKCS#12 Certificate: Choose File No file chosen
User-Password File: Choose File No file chosen
Private Key Password File: Choose File No file chosen

X.509 Certificate Files

| Index | File Name | File Size | Date Modified |
|-------|------------|-----------|--------------------------|
| 1 | ca.crt | 1188 | Mon Dec 14 13:49:11 2020 |
| 2 | client.crt | 4382 | Mon Dec 14 13:49:24 2020 |
| 3 | client.key | 1704 | Mon Dec 14 13:49:31 2020 |

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

Overview

Link Management

Industrial Interface

Network

Applications

VPN

OpenVPN

Status

OpenVPN

X.509 Certificate

Configuration Files

OpenVPN Information

| Index | Enable | Description | Mode | Status | Uptime | Local Virtual IP |
|-------|--------|-------------|--------|-----------|----------|------------------|
| 1 | true | | Client | Connected | 00:33:14 | 10.8.0.2 |

OpenVPN Server Status

| Index | Common Name | Status | Uptime | Remote Virtual IP | Remote IP | Remote Port |
|-------|-------------|--------|--------|-------------------|-----------|-------------|
|-------|-------------|--------|--------|-------------------|-----------|-------------|

Routing Tables

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

Status

Static Route

Route Table Information

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

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

| Status | Static Route | RIP | OSPF | BGP | |
|-------------------------|---------------|-----------------|---------------|--------|-----------|
| Route Table Information | | | | | |
| Index | Destination | Netmask | Gateway | Metric | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 10.152.127.41 | 100 | wwan1 |
| 2 | 10.8.0.0 | 255.255.255.0 | 0.0.0.0 | 0 | tun1 |
| 3 | 10.152.127.40 | 255.255.255.252 | 0.0.0.0 | 0 | wwan1 |
| 4 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 5 | 192.168.6.0 | 255.255.255.0 | 10.8.0.1 | 0 | tun1 |

Testing

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

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

Step 3: Test successfully.

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

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

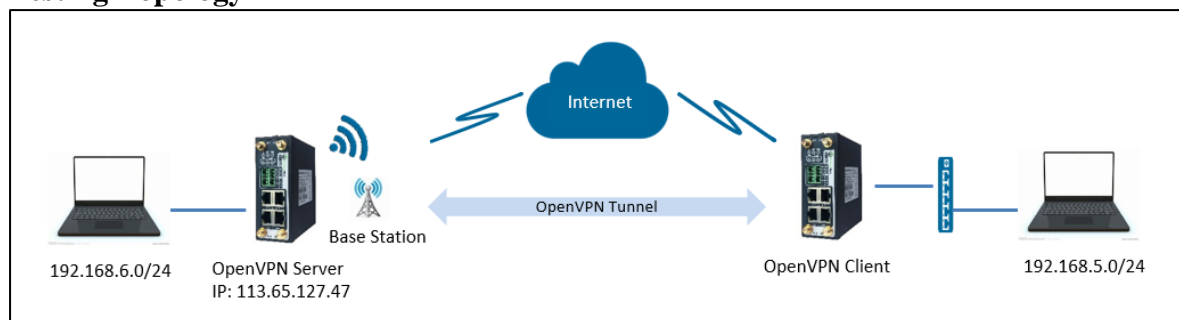
Overview

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

Software Version

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

Testing Topology



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

Configuration

Server Configuration

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

| OpenVPN Settings | |
|---------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | |
| Mode | Server |
| Protocol | UDP |
| Connection Type | TUN |
| Max Clients | 5 |
| Authentication Method | Password |
| Encryption Type | BF-CBC |
| Local IP Address | |
| Local Port | 1194 |
| Topology | Subnet |
| Subnet | 10.8.0.0 |
| Subnet Netmask | 255.255.255.0 |
| Renegotiate Interval | 3600 |
| Keepalive Interval | 20 |
| Keepalive Timeout | 60 |
| Fragment | 1500 |
| Output Verbosity Level | 3 |
| Advanced Settings | |
| Enable NAT | <input checked="" type="checkbox"/> |
| Enable Default Gateway | <input type="checkbox"/> |
| Enable Client to Client | <input checked="" type="checkbox"/> |
| Enable Duplicate CN | <input type="checkbox"/> |
| Enable IP Persist | <input type="checkbox"/> |
| Enable HMAC Firewall | <input type="checkbox"/> |
| Enable Compression LZ0 | <input checked="" type="checkbox"/> |
| Additional Configurations | |

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

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Route Settings

Route Management

| Index | Enable | Route | Push Route |
|-------|-------------------------------------|----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | 192.168.5.0/24 | 192.168.6.0/24 |

Save Close

Enable Client to Client ☒
 Enable Duplicate CN ☐
 Enable IP Persist ☐
 Enable HMAC Firewall ☐
 Enable Compression LZ0 ☒
 Additional Configurations

Route Management

| Index | Enable | Route | Push Route |
|-------|--------|-------|------------|
| | | | |

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

Client Settings

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route |
|-------|-------------------------------------|-------------|-------------------|----------------|----------------|
| 1 | <input checked="" type="checkbox"/> | client011 | | 192.168.5.0/24 | 192.168.6.0/24 |

Additional Configurations

Save Close

Route Management

| Index | Enable | Route | Push Route |
|-------|--------|----------------|----------------|
| 1 | true | 192.168.5.0/24 | 192.168.6.0/24 |

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route |
|-------|--------|-------------|-------------------|----------------|------------|
| | | | | | |

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

Client Password Settings

Client Password Management

Index
Enable ☒
Username
Password

Save

Close

Enable HMAC Firewall ☐
Enable Compression LZ0 ☒
Additional Configurations

Route Management

| Index | Enable | Route | Push Route | |
|-------|--------|----------------|----------------|--|
| 1 | true | 192.168.5.0/24 | 192.168.6.0/24 | |

Client Settings

| Index | Enable | Common Name | Client IP Address | Internal Route | Push Route | |
|-------|--------|-------------|-------------------|----------------|----------------|--|
| 1 | true | client011 | | 192.168.5.0/24 | 192.168.6.0/24 | |

Client Password Management

| Index | Enable | Username | Password | |
|-------|--------|----------|----------|--|
| | | | | |

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

Status

OpenVPN

X.509 Certificate

X.509 Certificate Import

OpenVPN Mode
CA Certificate No file chosen **ca.crt**
Local Certificate File No file chosen **xx.crt**
Local Private Key No file chosen **xx.key**
DH File No file chosen **dh.pem**
HMAC Firewall Key No file chosen
PKCS#12 Certificate No file chosen
CRL File No file chosen

X.509 Certificate Files

| Index | File Name | File Size | Date Modified | |
|-------|------------|-----------|-------------------------|--|
| 1 | ca.crt | 2399 | Thu Mar 5 08:40:08 2020 | |
| 2 | dh.pem | 769 | Thu Mar 5 08:40:45 2020 | |
| 3 | server.crt | 8192 | Thu Mar 5 08:40:16 2020 | |
| 4 | server.key | 3272 | Thu Mar 5 08:40:23 2020 | |

Step 6: Click Apply.

| | |
|----------------|-------------|
| Section Eleven | 6944 Manual |
| Open VPN | Rev 2.8 |

Client Configuration

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

OpenVPN Settings

General Settings

Index
Enable ☒
Description
Mode
Protocol
Connection Type
Server Address
Server Port
Authentication Method
Encryption Type
Username
Password
Renegotiate Interval
Keepalive Interval
Keepalive Timeout
Fragment
Output Verbosity Level

Advanced Settings

Enable NAT ☒
Enable HMAC Firewall ☐
Enable Compression LZ0 ☒
Additional Configurations

Save

Close

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

Status

OpenVPN

X.509 Certificate

Configuration Files

X.509 Certificate Import

OpenVPN Mode
Connection Index
CA Certificate No file chosen **ca.crt**
Local Certificate File No file chosen
Local Private Key No file chosen
HMAC Firewall Key No file chosen
Pre-shared Key No file chosen
PKCS#12 Certificate No file chosen
User-Password File No file chosen
Private Key Password File No file chosen

X.509 Certificate Files

| Index | File Name | File Size | Date Modified |
|-------|-----------|-----------|--------------------------|
| 1 | ca.crt | 1188 | Mon Dec 14 13:49:11 2020 |

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

Overview

Link Management

Industrial Interface

Network

Applications

VPN

OpenVPN

Status

OpenVPN

X.509 Certificate

Configuration Files

OpenVPN Information

| Index | Enable | Description | Mode | Status | Uptime | Local Virtual IP |
|-------|--------|-------------|--------|-----------|----------|------------------|
| 1 | true | | Client | Connected | 00:21:38 | 10.8.0.2 |

OpenVPN Server Status

| Index | Common Name | Status | Uptime | Remote Virtual IP | Remote IP | Remote Port |
|-------|-------------|--------|--------|-------------------|-----------|-------------|
|-------|-------------|--------|--------|-------------------|-----------|-------------|

Checking the Routing Table

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

Status

Static Route

Route Table Information

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

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

| Status | Static Route | RIP | OSPF | BGP | |
|-------------------------|---------------|-----------------|---------------|--------|-----------|
| Route Table Information | | | | | |
| Index | Destination | Netmask | Gateway | Metric | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 10.152.127.41 | 100 | wwan1 |
| 2 | 10.8.0.0 | 255.255.255.0 | 0.0.0.0 | 0 | tun1 |
| 3 | 10.152.127.40 | 255.255.255.252 | 0.0.0.0 | 0 | wwan1 |
| 4 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 5 | 192.168.6.0 | 255.255.255.0 | 10.8.0.1 | 0 | tun1 |

Testing

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

| Ping | Traceroute | AT Debug |
|--|-------------|----------|
| Ping Settings | | |
| Host Address | 192.168.6.2 | |
| Ping Count | 5 | |
| Local IP Address | 192.168.5.1 | |
| PING 192.168.6.2 (192.168.6.2) from 192.168.5.1: 56 data bytes 64 bytes from 192.168.6.2: seq=0 ttl=63 time=45.031 ms 64 bytes from 192.168.6.2: seq=1 ttl=63 time=52.755 ms 64 bytes from 192.168.6.2: seq=2 ttl=63 time=39.448 ms 64 bytes from 192.168.6.2: seq=3 ttl=63 time=44.184 ms 64 bytes from 192.168.6.2: seq=4 ttl=63 time=43.928 ms --- 192.168.6.2 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 39.448/45.069/52.755 ms | | |

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

| Ping | Traceroute | AT Debug |
|--|-------------|----------|
| Ping Settings | | |
| Host Address | 192.168.5.2 | |
| Ping Count | 5 | |
| Local IP Address | 192.168.6.1 | |
| PING 192.168.5.2 (192.168.5.2) from 192.168.6.1: 56 data bytes 64 bytes from 192.168.5.2: seq=0 ttl=63 time=34.432 ms 64 bytes from 192.168.5.2: seq=1 ttl=63 time=44.027 ms 64 bytes from 192.168.5.2: seq=2 ttl=63 time=38.660 ms 64 bytes from 192.168.5.2: seq=3 ttl=63 time=44.314 ms 64 bytes from 192.168.5.2: seq=4 ttl=63 time=54.063 ms --- 192.168.5.2 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 34.432/43.099/54.063 ms | | |

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

12 IP SEC

12.1. IP Sec Overview

Overview

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

Basic Configuration

Go to VPN> IP Sec

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

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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 the sub-mask if the network beyond the local LAN will be sending packets through the tunnel.
NOTE: The Remote subnet and Local subnet addresses must not overlap!
- **Local Pre-shared Key** - Enter the pre-shared key which match the remote endpoint.
- **Local ID Type** - The local endpoint's identification. The identifier can be a host name or an IP address.
- **Xauth Identity** - Enter Xauth identity after “Pre-shared Key and Xauth” on authentication Method is enabled.
- **Xauth Password** - Enter Xauth password “Pre-shared Key and Xauth” on authentication Method is enabled.
- **Remote Subnet** - Enter an IP address with mask if encrypted packets are also destined for the specified network that is beyond the Remote IP Address.
NOTE: The Remote subnet and Local subnet addresses must not overlap!
- **Remote ID Type** - The authentication address of the remote endpoint.

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

| IKE Proposal Settings | |
|-----------------------|--------------------|
| Encryption algorithm | AES-256 ▼ |
| Hash Algorithm | SHA2 256 ▼ |
| Diffie-Hellman group | Group5(modp1536) ▼ |
| Lifetime | 1440 |

| ESP Proposal Settings | |
|-----------------------|--------------------|
| Encryption algorithm | AES-256 ▼ |
| Hash Algorithm | SHA2 256 ▼ |
| Diffie-Hellman group | Group5(modp1536) ▼ |
| Lifetime | 60 |

| Advanced Settings | |
|---------------------------|------|
| DPD Interval | 30 ? |
| DPD Timeout | 90 ? |
| Additional Configurations | ? |

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 ‘;’.

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

Overview

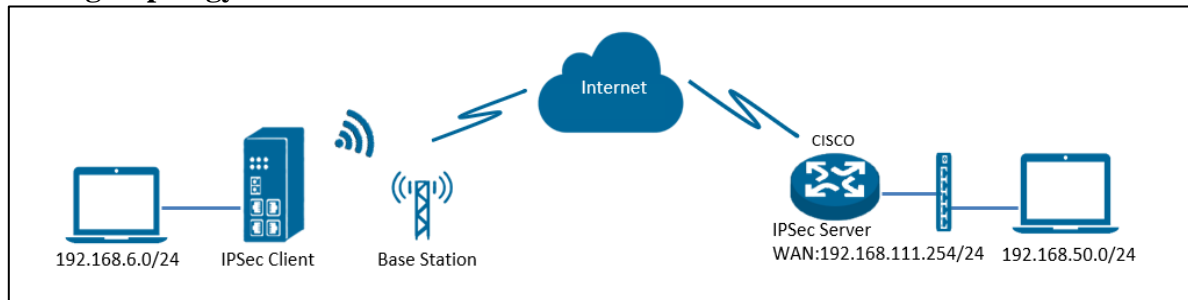
This document contains information regarding the configuration of a 6944 Industrial router running IP Sec with a pre-shared key to a Cisco router.

Software Version

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

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

Testing Topology



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

Configuration

Server Configuration

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

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

| Section Twelve | 6944 Manual |
|----------------|-------------|
| IP Sec | Rev 2.8 |

```
ip address 192.168.111.254 255.255.255.0
ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
speed auto
no mop enabled
crypto map SMAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 192.168.111.1
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
end
cisco2811#
```


Client Configuration (on 6944)

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

| IPSec Settings | |
|---------------------------|-------------------------------------|
| General Settings | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | IPsec_Pre-shared Key |
| Remote Gateway | 192.168.111.254 |
| IKE Version | IKEv1 |
| Connection Type | Tunnel |
| Negotiation Mode | Main |
| Authentication Method | Pre-shared Key |
| Local Subnet | 192.168.6.0/24 |
| Local Pre-shared Key | cisco |
| Local ID Type | IPv4 Address |
| Remote Subnet | 192.168.50.0/24 |
| Remote ID Type | IPv4 Address |
| IKE Proposal Settings | |
| Encryption algorithm | AES-256 |
| Hash Algorithm | MD5 |
| Diffie-Hellman group | Group5(modp1536) |
| Lifetime | 1440 |
| ESP Proposal Settings | |
| Encryption algorithm | 3DES |
| Hash Algorithm | MD5 |
| Diffie-Hellman group | Group5(modp1536) |
| Lifetime | 60 |
| Advanced Settings | |
| DPD Interval | 30 ? |
| DPD Timeout | 90 ? |
| Additional Configurations | ? |
| <div>Save Close</div> | |

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

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

| | | | | | |
|--|--------------------------|----------------------|-------------|----------|--------|
|  Overview Link Management Industrial Interface Network | Status IPSec | | | | |
| | IPSec Information | | | | |
| | Index | Enable | Description | Status | Uptime |
| 1 | true | IPsec_Pre-shared Key | Connected | 00:22:06 | |

Testing

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

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

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

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

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

Overview

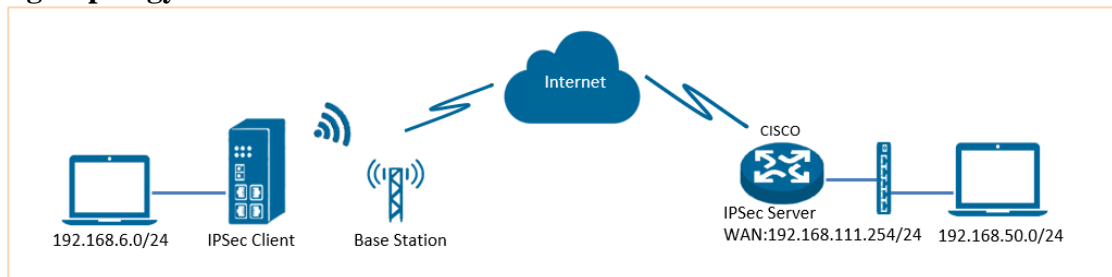
This document contains information regarding a 6944 running IP Sec and FQDN to a Cisco router

Software Version

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

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

Testing Topology



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

Configuration

Server Configuration

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

```
=====
cisco2811#show running-config
Building configuration...
version 12.4
hostname cisco2811
!
logging message-counter syslog
enable secret 5
$1$tW/d$UQQ3Xh06n.2HHFeAVIgXJ.
!
no aaa new-model
ip cef
!
ip name-server 192.168.111.1
ip address-pool local
multilink bundle-name authenticated
!
username cisco password 0 cisco
archive
 log config
  hidekeys
!
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 5
crypto isakmp key 6 cisco hostname 6944

crypto isakmp identity hostname
!
crypto isakmp peer address 0.0.0.0
 set aggressive-mode password cisco
 set aggressive-mode client-endpoint fqdn
6944
!
crypto ipsec transform-set 6944 esp-3des esp-
md5-hmac
!
crypto dynamic-map DYN 10
 set transform-set 6944
 set pfs group5
 match address 101
 reverse-route
!
crypto map SMAP 10 ipsec-isakmp dynamic
DYN
!
track 1 interface FastEthernet0/0 line-protocol
!
interface Loopback0
 ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
 ip address 192.168.111.254 255.255.255.0
 ip nat outside
```

| Section Twelve | 6944 Manual |
|----------------|-------------|
| IP Sec | Rev 2.8 |

```
ip nat enable
ip virtual-reassembly
duplex full
speed auto
no mop enabled
crypto map SMAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
ip forward-protocol nd
```

```
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
snmp-server community public RO
!
end
cisco2811#
```

Client Configuration

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

| IPSec Settings | |
|--|-------------------------------------|
| General Settings | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | IPsec_Pre-shared Key |
| Remote Gateway | 192.168.111.254 |
| IKE Version | IKEv1 |
| Connection Type | Tunnel |
| Negotiation Mode | Aggressive |
| Authentication Method | Pre-shared Key |
| Local Subnet | 192.168.6.0/24 |
| Local Pre-shared Key | cisco |
| Local ID Type | FQDN |
| Local ID | NR500 |
| Remote Subnet | 192.168.50.0/24 |
| Remote ID Type | FQDN |
| Remote ID | cisco2811 |
| IKE Proposal Settings | |
| Encryption algorithm | AES-256 |
| Hash Algorithm | MD5 |
| Diffie-Hellman group | Group5(modp1536) |
| Lifetime | 1440 |
| ESP Proposal Settings | |
| Encryption algorithm | 3DES |
| Hash Algorithm | MD5 |
| Diffie-Hellman group | Group5(modp1536) |
| Lifetime | 60 |
| Advanced Settings | |
| DPD Interval | 30 |
| DPD Timeout | 90 |
| Additional Configurations | |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

Step 2: Click Save>Apply.

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

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

Testing

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

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

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

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

Step 3: Test successful.

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

Overview

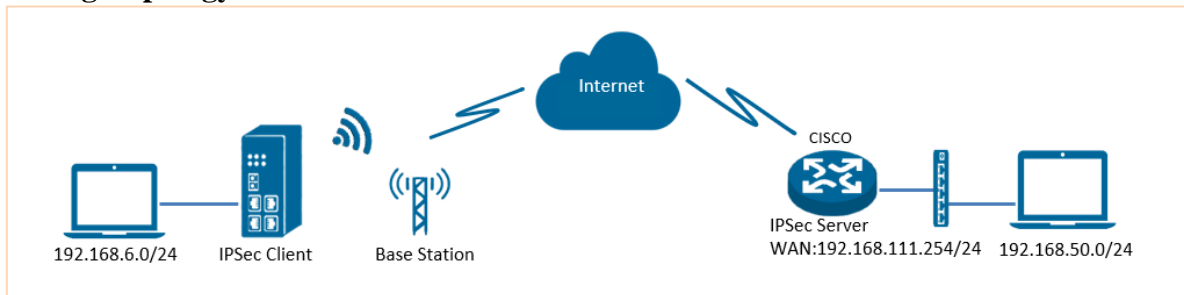
This document contains information regarding configuring a 6944 running IP Sec with a Pre-Shared Key to a Cisco router.

Software Version

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

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

Testing Topology



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

Configuration

Server Configuration

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

```

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

```


| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

```

interface FastEthernet0/0
ip address 192.168.111.254 255.255.255.0
ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
speed auto
no mop enabled
crypto map MAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!

```

```

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
!!
line con 0
line vty 5 15
exec-timeout 5 2
end

```

Client Configuration

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

IPSec Settings

General Settings

Index: 1

Enable: ☒

Description: IPsec_Pre-shared Key

Remote Gateway: 192.168.111.254

IKE Version: IKEv1

Connection Type: Tunnel

Negotiation Mode: Main

Authentication Method: Pre-shared Key and Xauth

Local Subnet: 192.168.6.0/24

Local Pre-shared Key: cisco

Local ID Type: IPv4 Address

Xauth Identity: cisco

Xauth Password: cisco

Remote Subnet: 192.168.50.0/24

Remote ID Type: IPv4 Address

IKE Proposal Settings

Encryption algorithm: AES-256

Hash Algorithm: MD5

Diffie-Hellman group: Group5(modp1536)

Lifetime: 1440

ESP Proposal Settings

Encryption algorithm: 3DES

Hash Algorithm: MD5

Diffie-Hellman group: Group5(modp1536)

Lifetime: 60

Advanced Settings

DPD Interval: 30

DPD Timeout: 90

Additional Configurations:

Save Close

2. Click Save>Apply.

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

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

Testing

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

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

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

| Ping Settings | |
|------------------|--------------|
| Host Address | 192.168.50.1 |
| Ping Count | 5 |
| Local IP Address | 192.168.6.1 |

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

Step 4: Test successful.

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

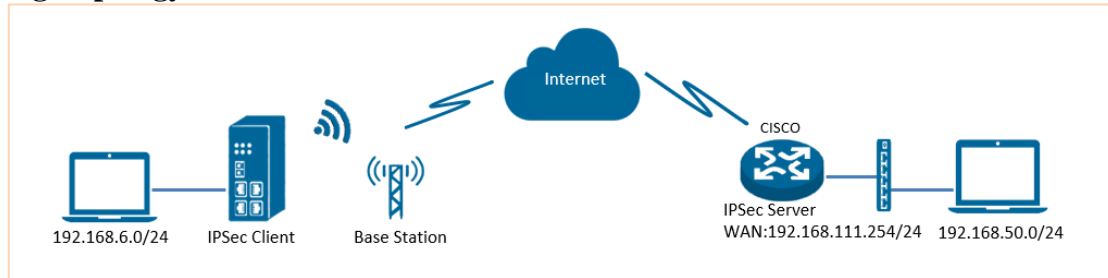
Overview

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

Software Versions

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

Testing Topology



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

Configuration

Server Configuration

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

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

```

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

```

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

```

!
interface FastEthernet0/0
ip address 192.168.111.254 255.255.255.0
ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
no mop enabled
crypto map MAP
!
interface FastEthernet0/1
ip address 192.168.5.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto

ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 192.168.111.1
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
ip access-list extended VPN
permit ip 192.168.50.0 0.0.0.255 192.168.6.0
0.0.0.255
!
access-list 10 permit 192.168.5.0 0.0.0.255
access-list 101 permit ip 192.168.50.0
0.0.0.255 192.168.6.0 0.0.0.255
line con 0
line vty 5 15
end

```

Client Configuration

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

IPSec Settings

General Settings

Index

1

Enable

☒

Description

IPsec_Pre-shared Key

Remote Gateway

192.168.111.254

IKE Version

IKEv1

Connection Type

Tunnel

Negotiation Mode

Aggressive

Authentication Method

Pre-shared Key and Xauth

Local Subnet

192.168.6.0/24

Local Pre-shared Key

cisco

Local ID Type

FQDN

Local ID

NR500

Xauth Identity

cisco

Xauth Password

cisco

Remote Subnet

192.168.50.0/24

Remote ID Type

FQDN

Remote ID

cisco2811

IKE Proposal Settings

Encryption algorithm

AES-256

Hash Algorithm

MD5

Diffie-Hellman group

Group5(modp1536)

Lifetime

1440

ESP Proposal Settings

Encryption algorithm

3DES

Hash Algorithm

MD5

Diffie-Hellman group

Group5(modp1536)

Lifetime

60

Advanced Settings

DPD Interval

30

DPD Timeout

90

Additional Configurations

Save

Close

| | |
|----------------|-------------|
| Section Twelve | 6944 Manual |
| IP Sec | Rev 2.8 |

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

| IPSec Information | | | | |
|-------------------|--------|-------------|-----------|----------|
| Index | Enable | Description | Status | Uptime |
| 1 | true | IPsec_FQDN | Connected | 00:00:00 |

Testing

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

```
cisco2811#ping 192.168.6.1 source 192.168.50.1 repeat 100

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

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

| Ping Settings | |
|------------------|--------------|
| Host Address | 192.168.50.1 |
| Ping Count | 5 |
| Local IP Address | 192.168.6.1 |

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

Step 3: Test successful.

This page left blank intentionally.

| | |
|-----------------------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Generic Routing Encapsulation | Rev 2.8 |

13 GRE Generic Routing Encapsulation

Overview

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

Checking the 6944 GRE Status

– Go to Status>GRE

| Status | | GRE | | |
|-----------------|--------|-------------|------|--------|
| GRE Information | | | | |
| Index | Enable | Description | Mode | Status |
| | | | | |

VPN->GRE->Status

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

| 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"/> |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

VPN->GRE

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

| | |
|-----------------------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Generic Routing Encapsulation | Rev 2.8 |

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

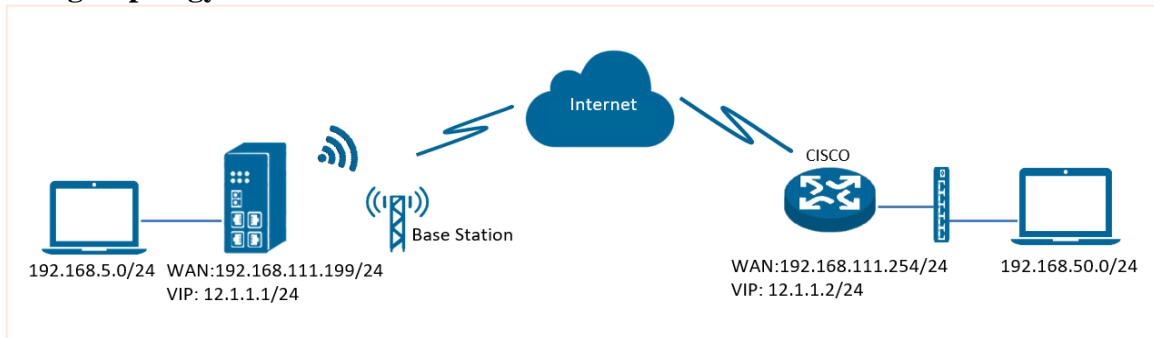
Overview

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

6944 Software Version

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

Testing Topology



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

Configuration

6944 Configuration

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



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

| GRE Settings | |
|--|-------------------------------------|
| GRE Information | |
| Index | 1 |
| Enable | <input checked="" type="checkbox"/> |
| Description | GRE TEST |
| Remote Gateway | 192.168.111.254 |
| Local Virtual IP | 12.1.1.1 |
| Local Virtual Netmask | 255.255.255.0 |
| Tunnel key | 123456 ? |
| Enable NAT | <input checked="" type="checkbox"/> |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

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



Configure the static route settings as shown below

| | |
|-----------------------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Generic Routing Encapsulation | Rev 2.8 |

Static Route Settings

Route Table Information

| | |
|-------------|---------------|
| Index | 1 |
| Description | GRE ROUTE |
| IP Address | 192.168.50.0 |
| Netmask | 255.255.255.0 |
| Gateway | |
| Interface | gretun1 |

?

Save

Close

Configuring the CISCO Router

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

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

| | |
|------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

Testing

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

The screenshot shows the Case Communications web interface. On the left is a navigation menu with options: Overview, Link Management, Industrial Interface, Network, Applications, VPN, and Maintenance (with sub-options: Upgrade, System, Configuration, and a 'Doing Tools' link). The main content area is titled 'Ping Traceroute'. Under 'Ping Settings', the 'Host Address' is set to '12.1.1.2', 'Ping Count' is '5', and 'Local IP Address' is empty. Below the settings, the ping results are displayed: 'PING 12.1.1.2 (12.1.1.2): 56 data bytes' followed by five lines of results showing 64 bytes from 12.1.1.2 with sequence numbers 0 through 4 and round-trip times ranging from 2.066 ms to 2.127 ms. At the bottom, a summary states: '--- 12.1.1.2 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 2.066/2.089/2.127 ms'.

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

The screenshot shows the Case Communications web interface with the 'Host Address' set to '192.168.50.1'. The ping results show: 'PING 192.168.50.1 (192.168.50.1): 56 data bytes' followed by five lines of results showing 64 bytes from 192.168.50.1 with sequence numbers 0 through 4 and round-trip times ranging from 2.104 ms to 2.198 ms. The summary at the bottom states: '--- 192.168.50.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 2.104/2.142/2.198 ms'.

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

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

Step 4: Test successful

| | |
|------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

13.2. AN056- GRE VPN Redundancy to Cisco Router

Overview

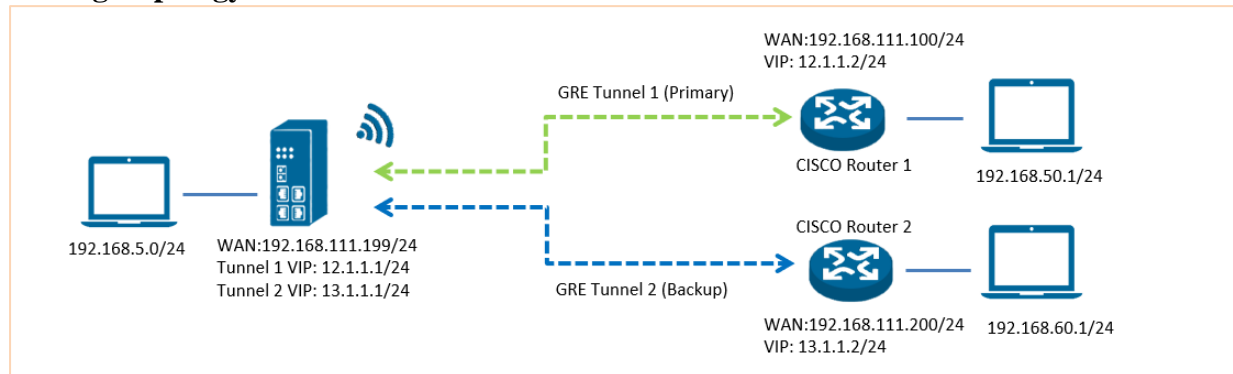
This document contains information regarding the configuration and use of GRE VPN redundancy between a 6944 router and CISCO router.

Software Compatibility

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

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

Testing Topology



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

Configuration

6944Router Configuration

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



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

The screenshot shows the 'GRE Settings' configuration form. The 'General Settings' section includes the following fields: 'Index' (1), 'Enable' (checked), 'Description' (GRE Tunnel 1), 'Mode' (Layer 3), 'Remote Gateway' (192.168.111.100), 'Local Virtual IP' (12.1.1.1), 'Local Virtual Netmask' (255.255.255.0), 'Tunnel key' (*****), 'Enable NAT' (checked), and 'Enable Default Route' (unchecked). The 'Advanced Settings' section includes the 'Binding Interface' field. The 'Save' and 'Close' buttons are at the bottom right.

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

| | |
|------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

GRE Settings

General Settings

| | |
|-----------------------|-----------------|
| Index | 2 |
| Enable | Tick |
| Mode | Layer 3 |
| Remote Gateway | 192.168.111.200 |
| Local Virtual IP | 13.1.1.1 |
| Local Virtual Netmask | 255.255.255.0 |
| Tunnel Key | ***** |
| Enable NAT | Tick |
| Enable Default Route | Leave Un-ticked |

Advanced Settings

Advanced Settings

| | |
|-------------------|-----------------|
| Binding Interface | Leave Un-ticked |
|-------------------|-----------------|

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

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

| Static Route Settings | |
|-----------------------|---------------------------|
| Index | 1 |
| Description | Tunnel 1 to remote subnet |
| IP Address | 192.168.50.0 |
| Netmask | 255.255.255.0 |
| Gateway | |
| Metric | 0 |
| Interface | gretun1 |
| <div>Save Close</div> | |

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

| Static Route Settings | |
|-----------------------|---------------------------|
| Index | 2 |
| Description | Tunnel 2 to remote subnet |
| IP Address | 192.168.60.0 |
| Netmask | 255.255.255.0 |
| Gateway | |
| Metric | 0 |
| Interface | gretun2 |
| <div>Save Close</div> | |

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

| Status | Static Route | | | | |
|-------------------------|---------------|---------------|---------------|--------|-----------|
| Route Table Information | | | | | |
| Index | Destination | Netmask | Gateway | Metric | Interface |
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.1 | 100 | wan |
| 2 | 12.1.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | gretun1 |
| 3 | 13.1.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | gretun2 |
| 4 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 5 | 192.168.50.0 | 255.255.255.0 | 0.0.0.0 | 0 | gretun1 |
| 6 | 192.168.60.0 | 255.255.255.0 | 0.0.0.0 | 0 | gretun2 |
| 7 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

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

| Overview | Status | VPN Redundancy |
|----------------------|---|----------------|
| Link Management | General Settings | |
| Industrial Interface | <div> <div>Enable</div> <div>VPN Type GRE</div> <div>Switch Mode Primary</div> <div>Primary VPN Index 1</div> <div>Enable Verbose Log</div> </div> | |
| Network | ICMP Detection Settings | |
| Applications | <div> <div>Connection 1 Remote Virtual IP 12.1.1.2</div> <div>Connection 2 Remote Virtual IP 13.1.1.2</div> <div>Connection 3 Remote Virtual IP</div> <div>Connection 4 Remote Virtual IP</div> <div>Connection 5 Remote Virtual IP</div> <div>Interval 30</div> <div>Retry Interval 5</div> <div>Timeout 3</div> <div>Retry Times 3</div> </div> | |
| VPN | | |
| OpenVPN | | |
| IPSec | | |
| GRE | | |
| VPN Redundancy | | |
| Maintenance | | |

Step 9: Click Save > Apply

| | |
|------------------|-------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

CISCO Router 1 and CISCO Router 2 Configuration

CISCO Router 1 Configuration

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

```

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

```

CISCO Router 2 Configuration

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

```

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

```

| | |
|-------------------------|--------------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

Testing

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

| Status VPN Redundancy | |
|-----------------------|------------------------|
| Enable | True |
| VPN Type | Gre |
| Primary VPN Status | Connection 1 Connected |
| Secondary VPN Status | Connection 2 Standby |

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

| Ping | Traceroute | AT Debug | Sniffer |
|--|--------------|----------|---------|
| Ping Settings | | | |
| Host Address | 192.168.50.1 | | |
| Ping Count | 5 | | |
| Local IP Address | | | |
| PING 192.168.50.1 (192.168.50.1): 56 data bytes 64 bytes from 192.168.50.1: seq=0 ttl=255 time=27.286 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=23.112 ms 64 bytes from 192.168.50.1: seq=2 ttl=255 time=24.963 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=23.224 ms 64 bytes from 192.168.50.1: seq=4 ttl=255 time=22.390 ms --- 192.168.50.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 22.390/24.195/27.286 ms | | | |

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

| Ping | Traceroute | AT Debug | Sniffer |
|--|--------------|----------|---------|
| Ping Settings | | | |
| Host Address | 192.168.60.1 | | |
| Ping Count | 5 | | |
| Local IP Address | | | |
| PING 192.168.60.1 (192.168.60.1): 56 data bytes --- 192.168.60.1 ping statistics --- 5 packets transmitted, 0 packets received, 100% packet loss | | | |

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

| Status VPN Redundancy | |
|------------------------------|---------------------------|
| VPN Redundancy Status | |
| Enable | True |
| VPN Type | Gre |
| Primary VPN Status | Connection 1 Disconnected |
| Secondary VPN Status | Connection 2 Connected |

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

| | |
|-------------------------|--------------------|
| Section Thirteen | 6944 Manual |
| GRE Tunnelling | Rev 2.8 |

| Ping | Traceroute | AT Debug | Sniffer |
|---|------------|--------------|---------|
| Ping Settings | | | |
| Host Address | | 192.168.60.1 | |
| Ping Count | | 5 | |
| Local IP Address | | | |
| <p>PING 192.168.60.1 (192.168.60.1): 56 data bytes 64 bytes from 192.168.60.1: seq=0 ttl=255 time=14.550 ms 64 bytes from 192.168.60.1: seq=1 ttl=255 time=26.281 ms 64 bytes from 192.168.60.1: seq=2 ttl=255 time=28.431 ms 64 bytes from 192.168.60.1: seq=3 ttl=255 time=29.668 ms 64 bytes from 192.168.60.1: seq=4 ttl=255 time=22.890 ms</p> <p>--- 192.168.60.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 14.550/24.364/29.668 ms</p> | | | |

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

| Ping | Traceroute | AT Debug | Sniffer |
|---|------------|--------------|---------|
| Ping Settings | | | |
| Host Address | | 192.168.50.1 | |
| Ping Count | | 5 | |
| Local IP Address | | | |
| <p>PING 192.168.50.1 (192.168.50.1): 56 data bytes</p> <p>--- 192.168.50.1 ping statistics --- 5 packets transmitted, 0 packets received, 100% packet loss</p> | | | |

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

| Status | VPN Redundancy |
|------------------------------|------------------------|
| VPN Redundancy Status | |
| Enable | True |
| VPN Type | Gre |
| Primary VPN Status | Connection 1 Connected |
| Secondary VPN Status | Connection 2 Standby |

| Ping | Traceroute | AT Debug | Sniffer |
|---|------------|--------------|---------|
| Ping Settings | | | |
| Host Address | | 192.168.50.1 | |
| Ping Count | | 5 | |
| Local IP Address | | | |
| <p>PING 192.168.50.1 (192.168.50.1): 56 data bytes 64 bytes from 192.168.50.1: seq=0 ttl=255 time=27.286 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=23.112 ms 64 bytes from 192.168.50.1: seq=2 ttl=255 time=24.963 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=23.224 ms 64 bytes from 192.168.50.1: seq=4 ttl=255 time=22.390 ms</p> <p>--- 192.168.50.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 22.390/24.195/27.286 ms</p> | | | |

Step 8: Test successful.

This page left blank intentionally

14 Layer Two Tunneling Protocol (L2TP)

14.1. AN044_L2TP_between_two_6944_Routers

Overview

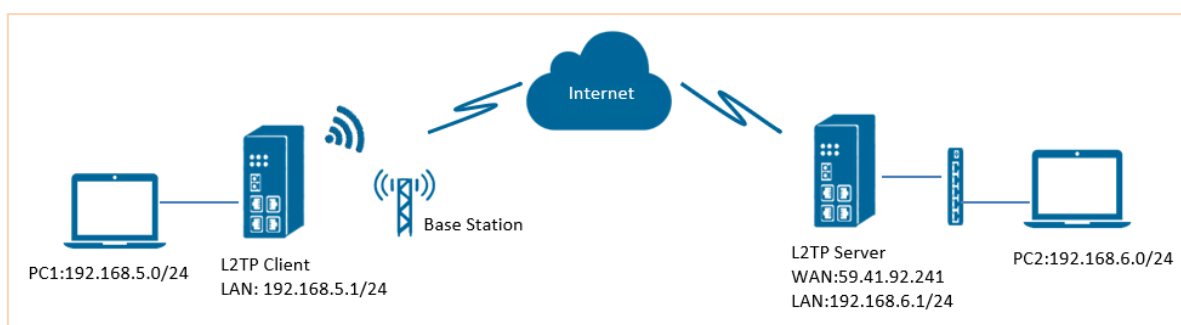
This document contains information regarding configuring an L2TP VPN between two 6944 routers.

Version

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

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

Testing Topology



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

Configuration

L2TP Server Configuration

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

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

The screenshot shows the 'L2TP Server' configuration page. The left sidebar contains a menu with 'Overview', 'Link Management', 'Industrial Interface', 'Network', 'Applications', 'VPN' (with sub-items: OpenVPN, IPsec, GRE, DMVPN, L2TP), and 'Maintenance'. The main content area has tabs for 'Status', 'L2TP Server', and 'L2TP Client'. The 'L2TP Server' tab is active, showing three sections: 'L2TP Settings', 'PPP Settings', and 'Advanced Settings'. In 'L2TP Settings', 'Enable' is checked, 'Local Port' is 1701, 'Challenge Secrets' is empty, 'Local IP' is 172.16.1.1, 'Start IP' is 172.16.1.2, 'End IP' is 172.16.1.254, and 'Enable Debug' is checked. In 'PPP Settings', 'Authentication' is CHAP, 'Username' is L2TPTEST, 'Password' is pass, 'MTU' is 1500, and 'Enable Debug' is checked. In 'Advanced Settings', 'Binding Interface' is empty, 'Enable Over IPsec' is unchecked, and 'Enable NAT' is checked. 'Save' and 'Apply' buttons are at the bottom right.

Click Save > Apply

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

The screenshot shows the 'Static Route' configuration page. The left sidebar is the same as the previous screenshot. The main content area has tabs for 'Status' and 'Static Route'. The 'Static Route' tab is active, showing a table with one entry (Index 1, Description L2TP, IP Address 192.168.5.0, Netmask 255.255.255.0, Gateway empty, Interface ppp0). Below the table is a 'Static Route Settings' dialog box with 'Route Table Information' fields: Index (1), Description (L2TP), IP Address (192.168.5.0), Netmask (255.255.255.0), Gateway (empty), and Interface (ppp0). 'Save' and 'Close' buttons are at the bottom right of the dialog.

L2TP Client Configuration

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

The screenshot shows the 'L2TP Client' configuration page. The left sidebar is the same. The main content area has tabs for 'Status' and 'L2TP Settings'. The 'L2TP Settings' tab is active, showing a table with one entry (Index 1, Description L2TP, Server Address 59.41.92.241, Server Port 1701, Challenge Secrets empty, Redial Timeout 20). Below the table is a 'L2TP Settings' dialog box with 'PPP Settings' fields: Authentication (CHAP), Username (L2TPTEST), Password (pass), Static Local IP (172.16.1.2), MTU (1500), and 'Enable Debug' (checked). In 'Advanced Settings', 'Binding Interface' is empty, 'Enable NAT' is checked, and 'Enable Default Route' is unchecked. 'Save' and 'Close' buttons are at the bottom of the dialog. A 'Save' and 'Apply' button are also visible on the right side of the main content area.

| | |
|----------------------------------|-------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

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

Testing

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

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

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

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

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

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

| | |
|----------------------------------|-------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

14.2. AN045-L2TP Server to Windows Operating System

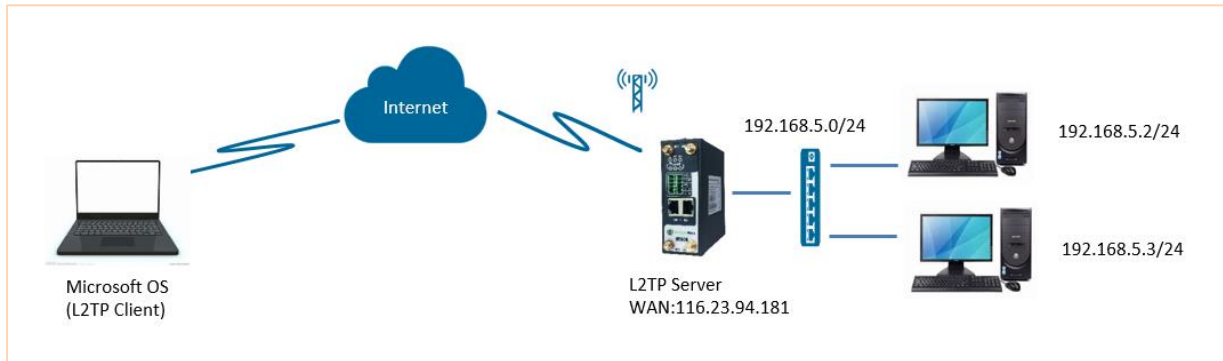
Overview

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

Software Compatibility

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

Testing Topology



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

Configuration

L2TP Server Configuration

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

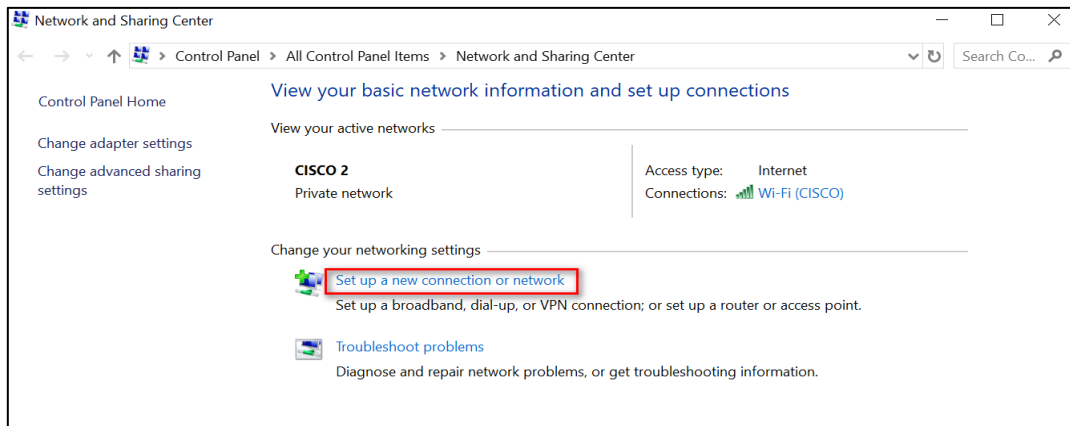
The screenshot shows the 'LAN Settings' configuration window. The 'General Settings' section includes fields for Index (1), Interface (LAN0), IP Address (192.168.5.1), Netmask (255.255.255.0), and MTU (1500). The 'DHCP Settings' section has 'Enable' checked, 'Mode' set to 'Server', 'IP Pool Start' (192.168.5.2), 'IP Pool End' (192.168.5.200), 'Netmask' (255.255.255.0), 'Lease Time' (120), and empty fields for Gateway, Primary DNS, Secondary DNS, and WINS Server. 'Save' and 'Close' buttons are at the bottom right of the window. The background shows the 'Link Management' menu with 'Ethernet' selected.

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

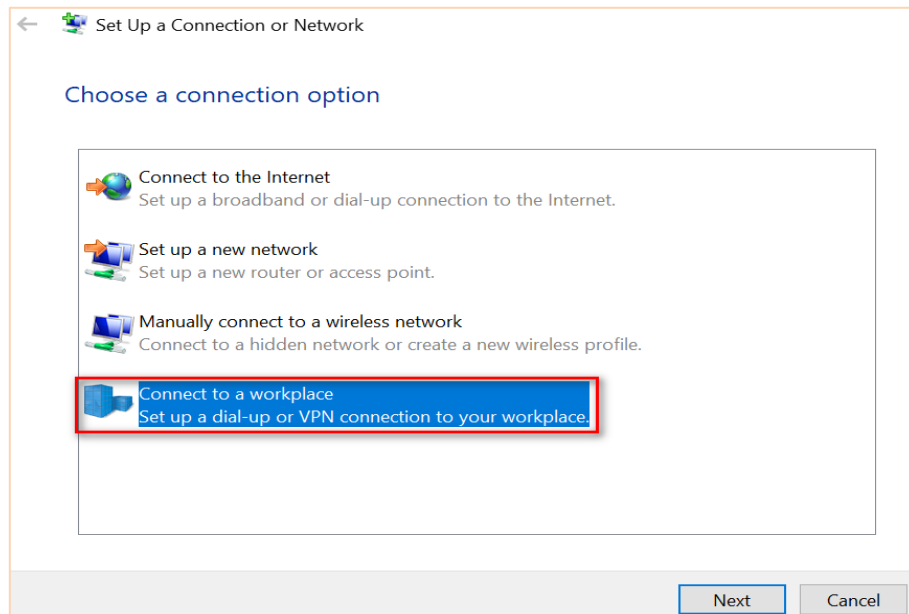
| | |
|---|--------------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

L2TP Client Configuration

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

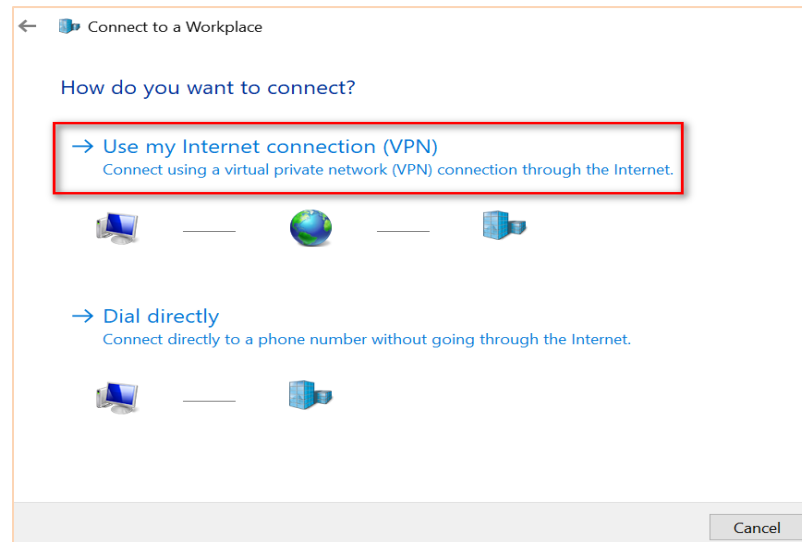


Step 2: Choose “Connect to a workplace” and click “Next”:

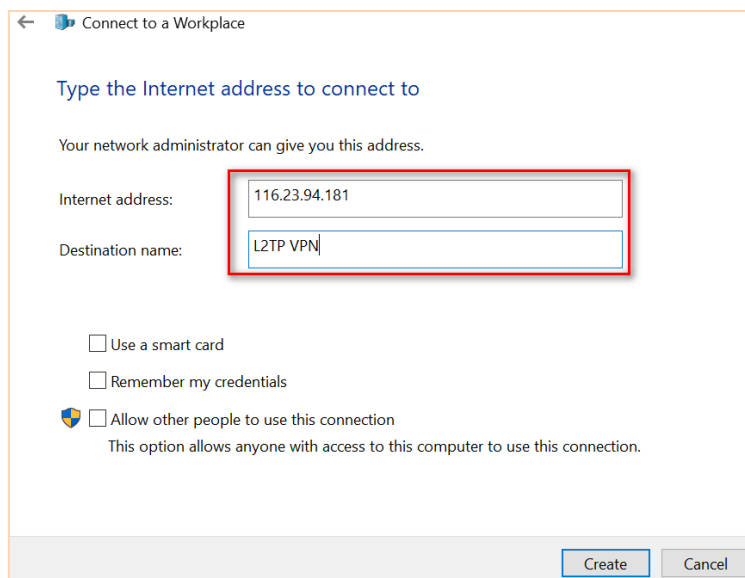


Step 3: Click “Use my Internet connection (VPN).”

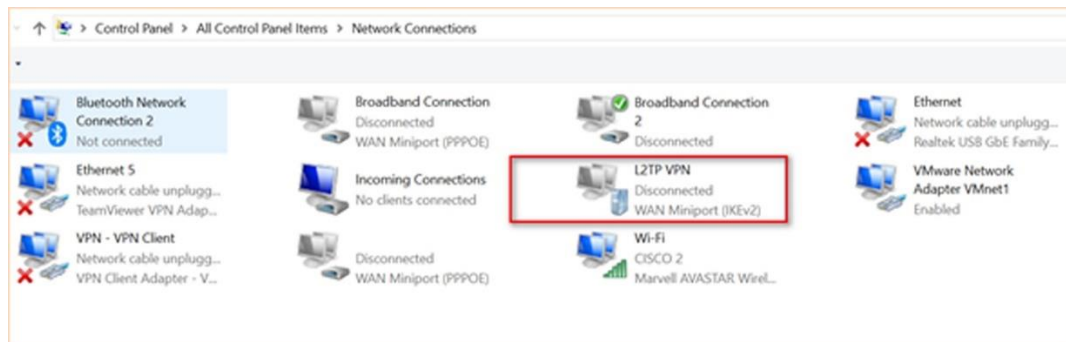
| | |
|---|--------------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |



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

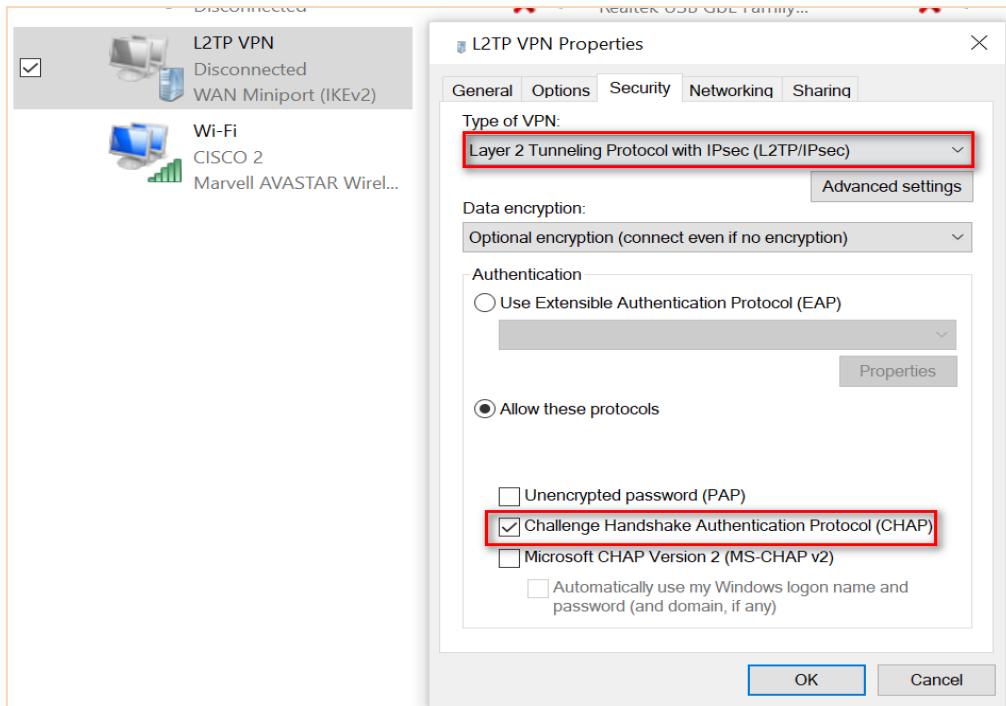


Step 5: After that, create an L2TP connection, as shown below:

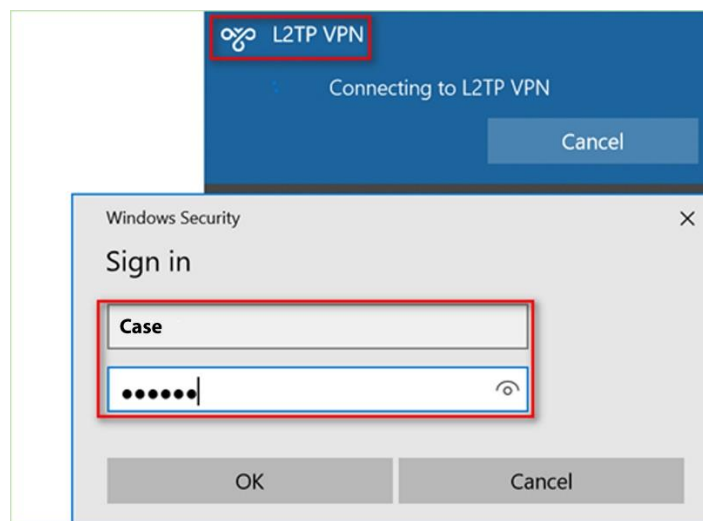


Step 6: Right Click “L2TP VPN”, and choose “Properties”, go to “Security” and specify the Type of VPN and Authentication, as shown below:

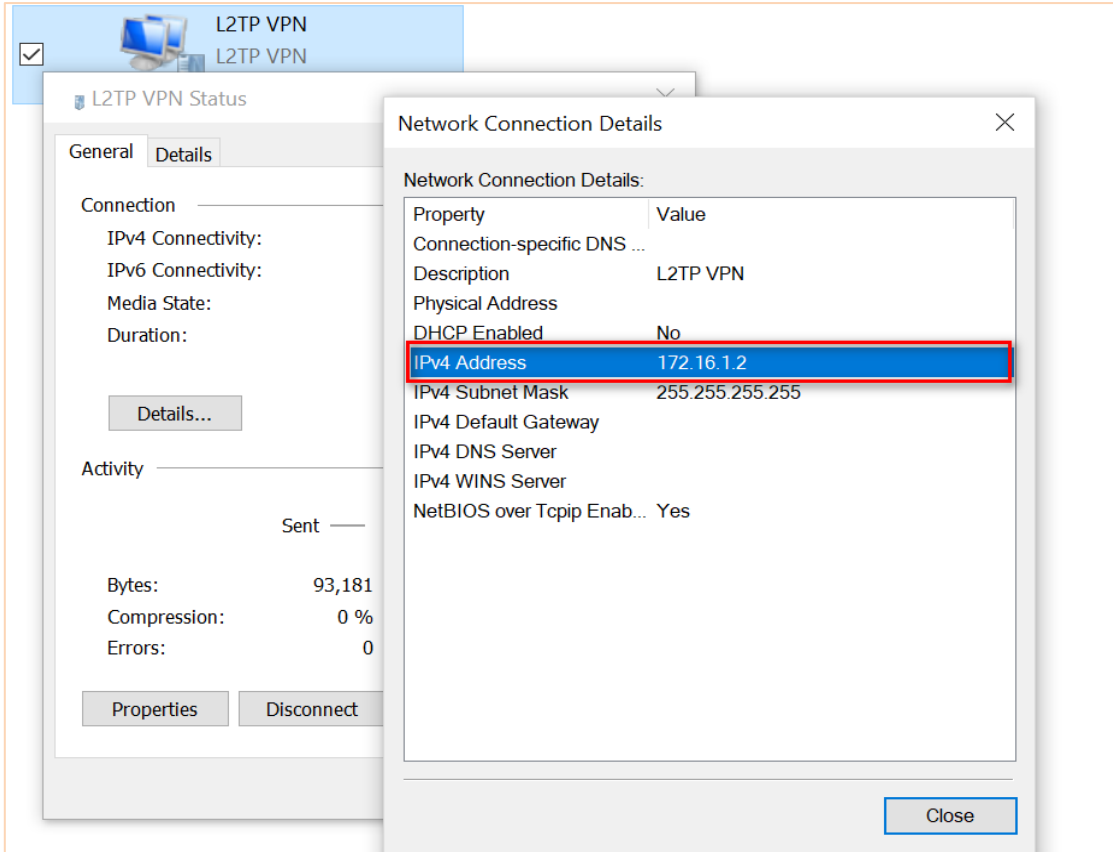
| | |
|---|--------------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |



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



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



Testing

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

```
C:\Users \ Administrator ping 192.168.5.1

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

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

| | |
|----------------------------------|-------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

14.3. AN046 - 6944 L2TP Client to Cisco L2TP Server

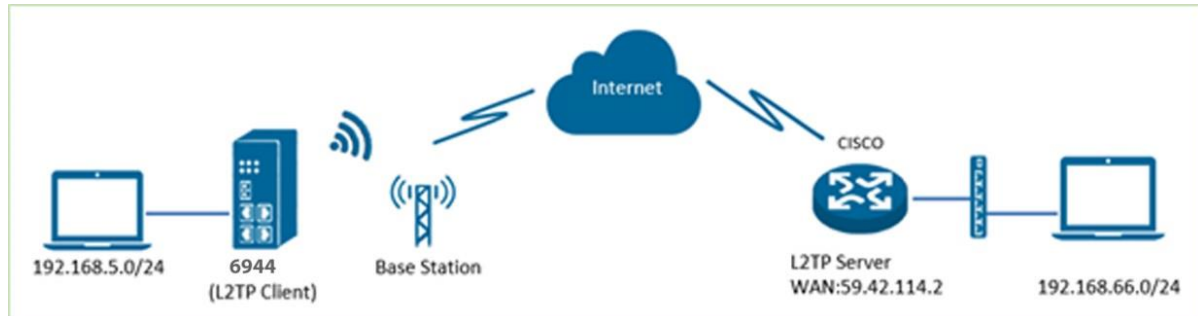
Overview

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

Software Compatibility

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

Testing Topology



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

Configuration

L2TP Server Configuration

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

```

cisco2811#show run
Building configuration...
Current configuration : 5447 bytes
version 12.4
ip cef
ip dhcp excluded-address 10.10.10.1
ip dhcp pool ABC
    network 10.10.10.0 255.255.255.0
    default-router 10.10.10.1
ip name-server 8.8.8.8
ip name-server 202.96.128.166
ip address-pool local!
vpdn enable
vpdn-group l2tp
! Default L2TP VPDN group
accept-dialin
protocol l2tp
virtual-template 1
l2tp tunnel password 0 123456
username l2tp password 0 l2tp
interface Loopback2
ip address 192.168.66.1 255.255.255.0
!
interface FastEthernet0/0
bandwidth 640
no ip address
ip nat outside

ip nat enable
ip virtual-reassembly
duplex full
speed auto
pppoe enable group global
pppoe-client dial-pool-number 1
no cdp enable
no mop enabled
!
interface FastEthernet0/1
ip address 10.10.10.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
no cdp enable
!
interface Virtual-Template1
ip address 10.5.5.1 255.255.255.0
peer default ip address pool l2tp
keepalive 20 3
ppp authentication ms-chap-v2
!
interface Dialer1
bandwidth 640
ip address negotiated

```

| | |
|----------------------------------|-------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

```
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip tcp adjust-mss 1452
no ip mroute-cache
dialer pool 1
dialer idle-timeout 0
dialer hold-queue 100
dialer persistent
dialer-group 1
no cdp enable
```

```
ppp authentication pap chap callin
ppp pap sent-username
020xxxxxxxxxx@163.gd password 0
XVGZW
crypto map SMAP
!
ip local pool l2tp 10.5.5.2 10.5.5.200
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 192.168.5.0 255.255.255.0 10.5.5.2
access-list 10 permit 10.10.10.0 0.0.0.255
cisco2811#
```

L2TP Client Configuration

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

Click **Save > Apply**

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

| | |
|----------------------------------|-------------|
| Section Fourteen | 6944 Manual |
| L2TP Layer 2 Tunnelling Protocol | Rev 2.8 |

Testing

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

| Status | L2TP Server | L2TP Client | | | | |
|--------------------|-------------|-------------|-----------|-----------|---------------|----------|
| L2TP Server Status | | | | | | |
| Index | Status | Remote IP | Interface | Uptime | | |
| L2TP Client Status | | | | | | |
| Index | Description | Status | Local IP | Remote IP | Interface | Uptime |
| 1 | | Connected | 10.5.5.2 | 10.5.5.1 | l2tp_client_1 | 00:34:57 |

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

| Overview | Ping | Traceroute | AT Debug |
|----------------------|---|------------------|--------------|
| Link Management | Ping Settings | | |
| Industrial Interface | | Host Address | 192.168.66.1 |
| Network | | Ping Count | 5 |
| Applications | | Local IP Address | 192.168.5.1 |
| VPN | PING 192.168.66.1 (192.168.66.1) from 192.168.5.1: 56 data bytes 64 bytes from 192.168.66.1: seq=0 ttl=255 time=45.784 ms 64 bytes from 192.168.66.1: seq=1 ttl=255 time=41.710 ms 64 bytes from 192.168.66.1: seq=2 ttl=255 time=45.168 ms 64 bytes from 192.168.66.1: seq=3 ttl=255 time=39.965 ms 64 bytes from 192.168.66.1: seq=4 ttl=255 time=102.676 ms --- 192.168.66.1 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 39.965/55.060/102.676 ms | | |
| Maintenance | | | |
| Upgrade | | | |
| Software | | | |
| System | | | |
| Configuration | | | |
| ▶ Debug Tools | | | |

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

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

Step 4: Test is successful

This page left blank intentionally.

15 Point to Point Tunneling Protocol (PPTP)

15.1. AN 051 PPTP Client to CISCO Server

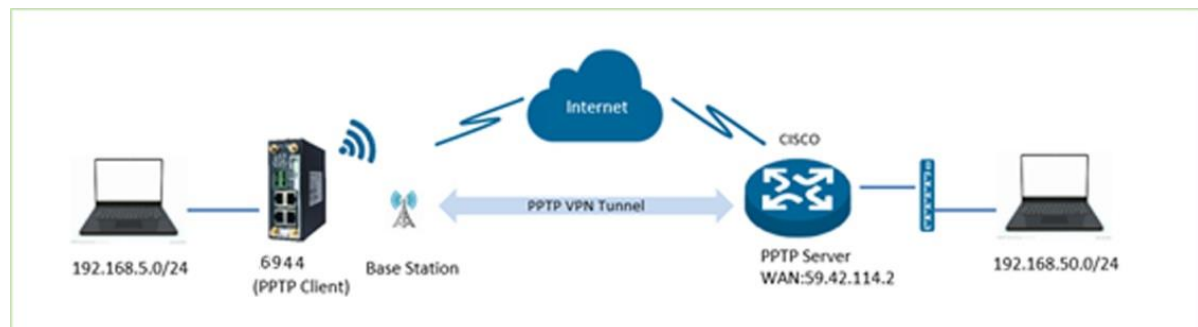
Overview

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

Software Compatibility

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

Testing Topology



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

Configuration

PPTP Server Configuration

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

```

cisco2811#show run
Building configuration...
Current configuration : 5611 bytes
!
version 12.4
hostname cisco2811
ip dhcp excluded-address 10.10.10.1
ip dhcp pool ABC
    network 10.10.10.0 255.255.255.0
    default-router 10.10.10.1
ip name-server 8.8.8.8
ip name-server 202.96.128.166
ip address-pool local
no ipv6 cef
vpdn enable
!
vpdn-group 2
! Default PPTP VPDN group
accept-dialin
protocol pptp
virtual-template 2
!
vpdn-group PPPOE

request-dialin
protocol pppoe
!
username pptp password 0 pptp
archive
!
interface Loopback0
ip address 192.168.50.1 255.255.255.0
!
interface FastEthernet0/0
bandwidth 640
no ip address
ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
speed auto
pppoe enable group global
pppoe-client dial-pool-number 1
no cdp enable
no mop enabled
!
interface FastEthernet0/1

```

| | |
|---|-------------|
| Section Fifteen | 6944 Manual |
| PPTP Point to Point Tunnelling Protocol | Rev 2.8 |

```
ip address 10.10.10.1 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
no cdp enable
!
```

```
interface Virtual-Template2
ip address 10.6.6.1 255.255.255.0
ip nat inside
ip virtual-reassembly
peer default ip address pool pptp
ppp encrypt mppe auto
ppp authentication ms-chap-v2
!
```

```
interface Dialer1
bandwidth 640
ip address negotiated
ip mtu 1492
ip nat outside
ip virtual-reassembly
encapsulation ppp
ip tcp adjust-mss 1452
no ip mroute-cache
```

```
dialer pool 1
dialer idle-timeout 0
dialer hold-queue 100
dialer persistent
dialer-group 1
no cdp enable
ppp authentication pap chap callin
ppp pap sent-username
0203XXXXXXXXXX@163.gd password 0
FSOXXXXXX
crypto map SMAP
!
ip local pool pptp 10.6.6.2 10.6.6.200
ip forward-protocol nd
ip route 0.0.0.0 0.0.0.0 Dialer1
ip route 192.168.5.0 255.255.255.0 10.6.6.2
!
ip nat inside source list 11 interface Dialer1
overload
!
access-list 11 permit 10.6.6.0 0.0.0.255
snmp-server community public RO
!
cisco2811#
```

PPTP Client Configuration

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

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

| | |
|---|-------------|
| Section Fifteen | 6944 Manual |
| PPTP Point to Point Tunnelling Protocol | Rev 2.8 |

Testing

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

| Status | PPTP Server | PPTP Client | | | | |
|--------------------|-------------|-------------|-----------|-----------|---------------|----------|
| PPTP Server Status | | | | | | |
| Index | Status | Remote IP | Interface | Uptime | | |
| PPTP Client Status | | | | | | |
| Index | Description | Status | Local IP | Remote IP | Interface | Uptime |
| 1 | | Connected | 10.6.6.2 | 10.6.6.1 | pptp_client_1 | 01:21:54 |

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

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

```
cisco2811#ping 192.168.5.1 source 192.168.50.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.5.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.50.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 32/48/68 ms
cisco2811#
```

15.2. AN052 6944 PPTP Server to Windows PC

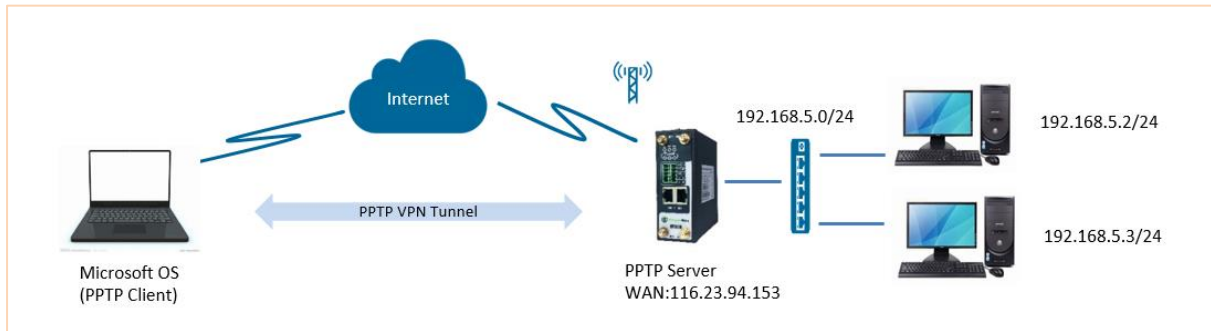
Overview

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

Software Compatibility

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

Testing Topology



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

Configuration

PPTP Server Configuration

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

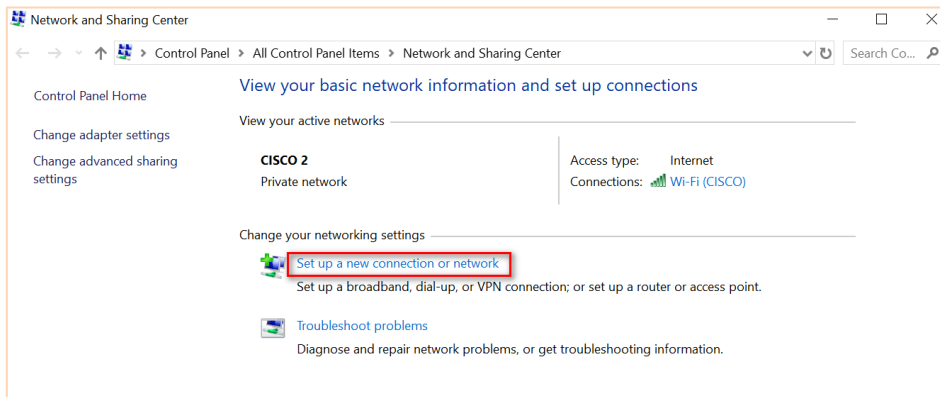
The screenshot shows the 'LAN Settings' configuration page in the 6944 web interface. The left sidebar contains navigation links: Overview, Link Management, Connection Manager, Cellular, Ethernet, WiFi, Industrial Interface, Network, Applications, VPN, and Maintenance. The main content area is titled 'LAN Settings' and includes a 'General Settings' section with fields for Index (1), Interface (LAN0), IP Address (192.168.5.1), Netmask (255.255.255.0), and MTU (1500). Below this is a 'DHCP Settings' section with fields for Enable (checked), Mode (Server), IP Pool Start (192.168.5.2), IP Pool End (192.168.5.200), Netmask (255.255.255.0), Lease Time (120), Gateway, Primary DNS, Secondary DNS, and WINS Server. At the bottom right, there are 'Save' and 'Close' buttons. At the very bottom of the page, there are 'Save' and 'Apply' buttons.

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

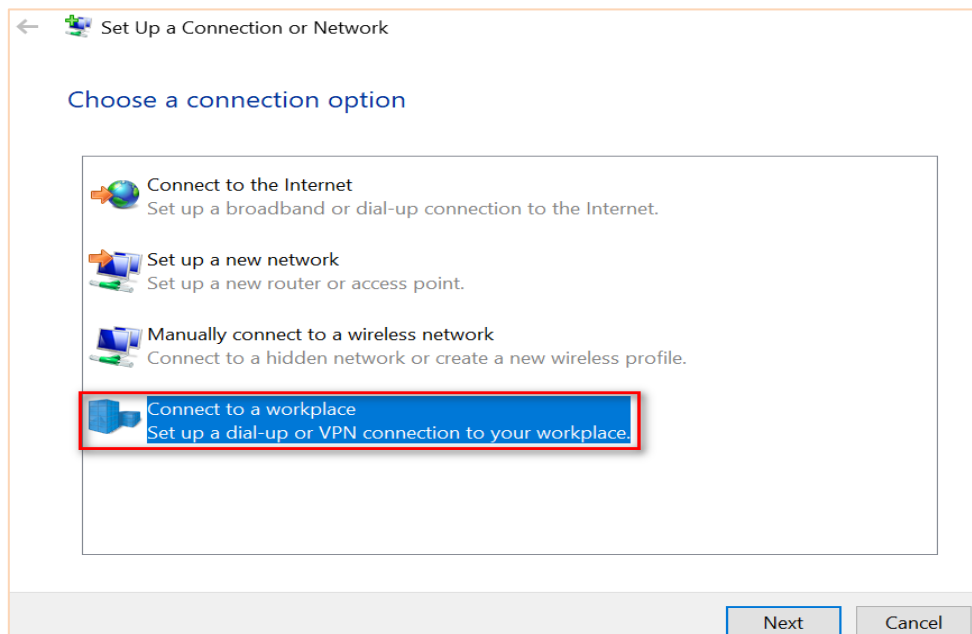
The screenshot shows a configuration interface for PPTP. On the left is a navigation menu with options: Overview, Link Management, Industrial Interface, Network, Applications, VPN, OpenVPN, IPsec, GRE, DMVPN, L2TP, PPTP (highlighted), and Maintenance. The main area has tabs for Status, PPTP Server, and PPTP Client. The PPTP Client tab is active, showing three sections: PPTP Settings, PPP Settings, and Advanced Settings. PPTP Settings includes 'Enable' (checked), 'Local IP' (192.168.168.1), 'Start IP' (192.168.168.2), 'End IP' (192.168.168.200), and 'Enable Debug' (checked). PPP Settings includes 'Authentication' (CHAP), 'Username' (nwtest), 'Password' (nwtest), 'MTU' (1500), and 'Enable Debug' (checked). Advanced Settings includes 'Binding Interface' (empty) and 'Enable NAT' (checked). 'Save' and 'Apply' buttons are at the bottom right.

PPTP Client Configuration

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

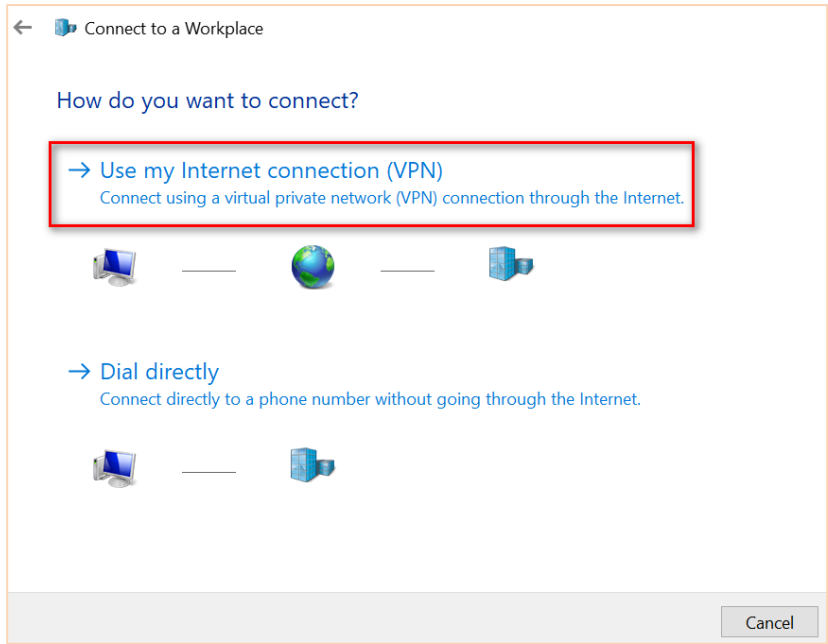


Step 2: Choose “Connect to a workplace” and click “Next”:

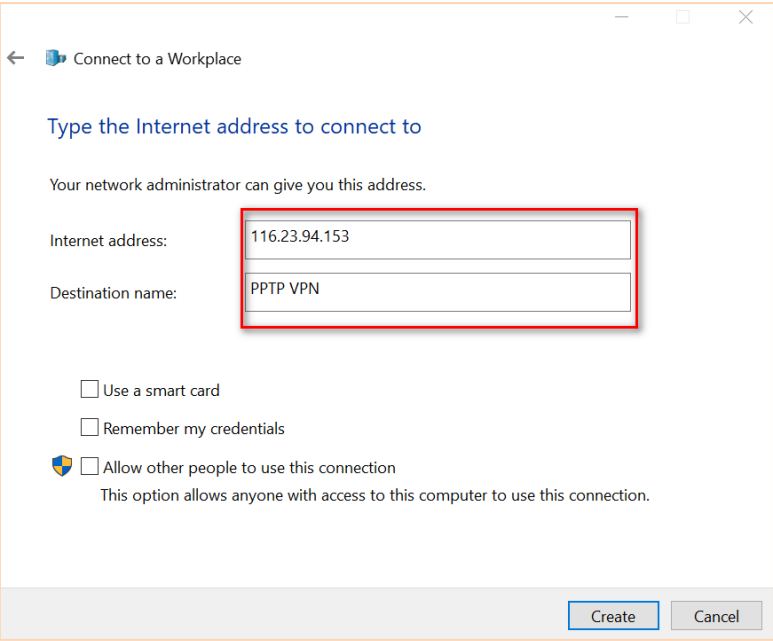


Step 3: Click “Use my Internet connection (VPN).”

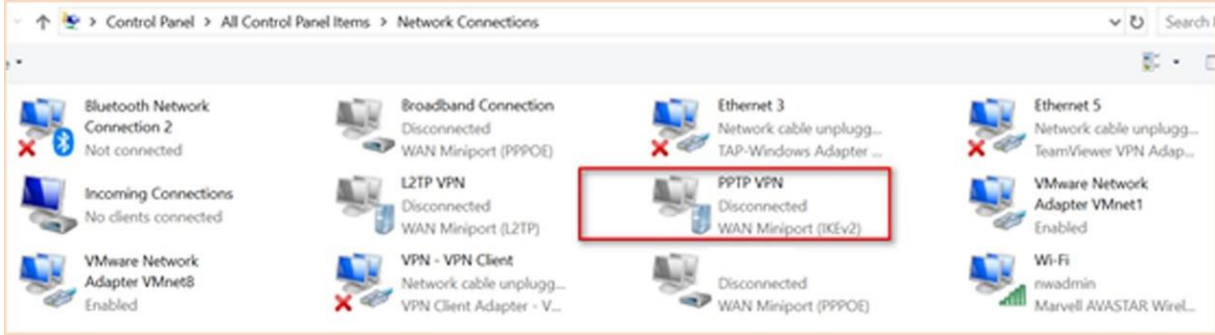
| | |
|--|--------------------|
| Section Fifteen | 6944 Manual |
| PPTP Point to Point Tunnelling Protocol | Rev 2.8 |



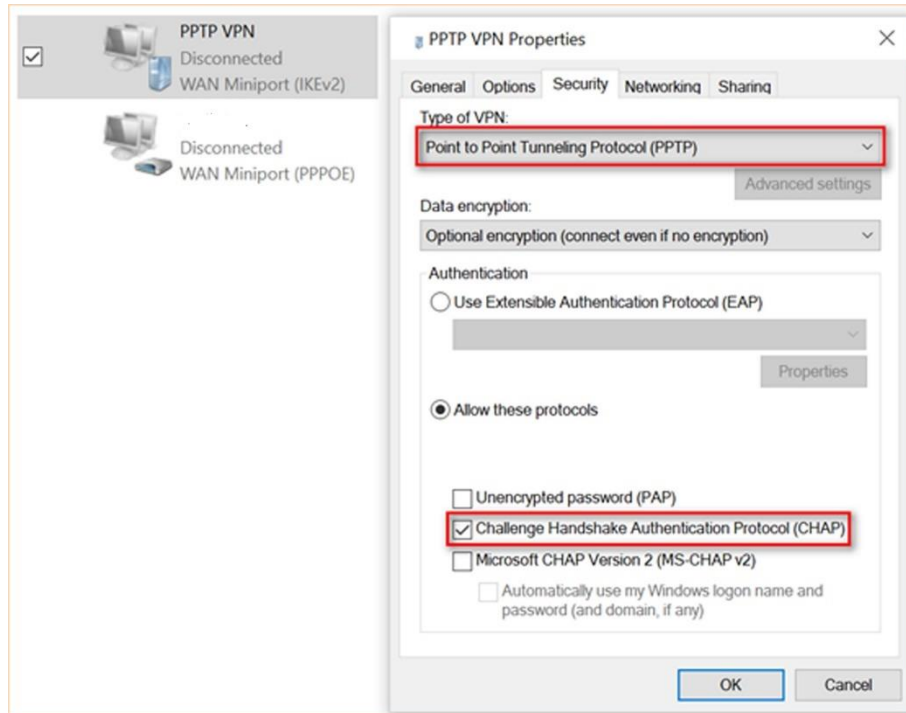
Step 4: Enter the PPTP Server IP address and Destination name, click “Create”.



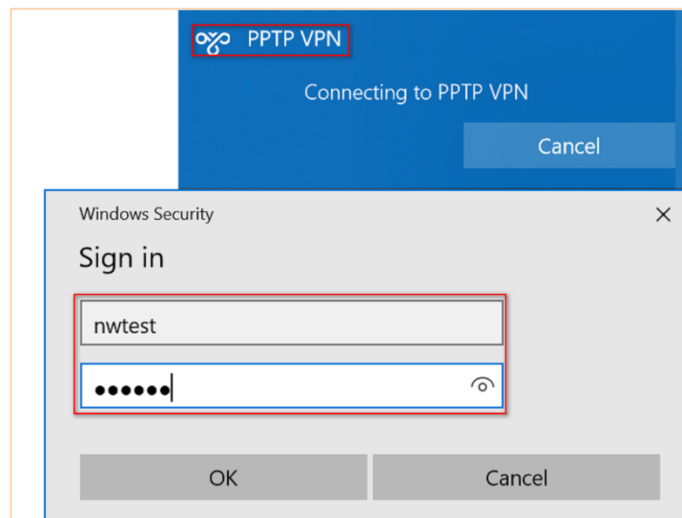
Step 5: After that, we create a PPTP connection, as shown below:



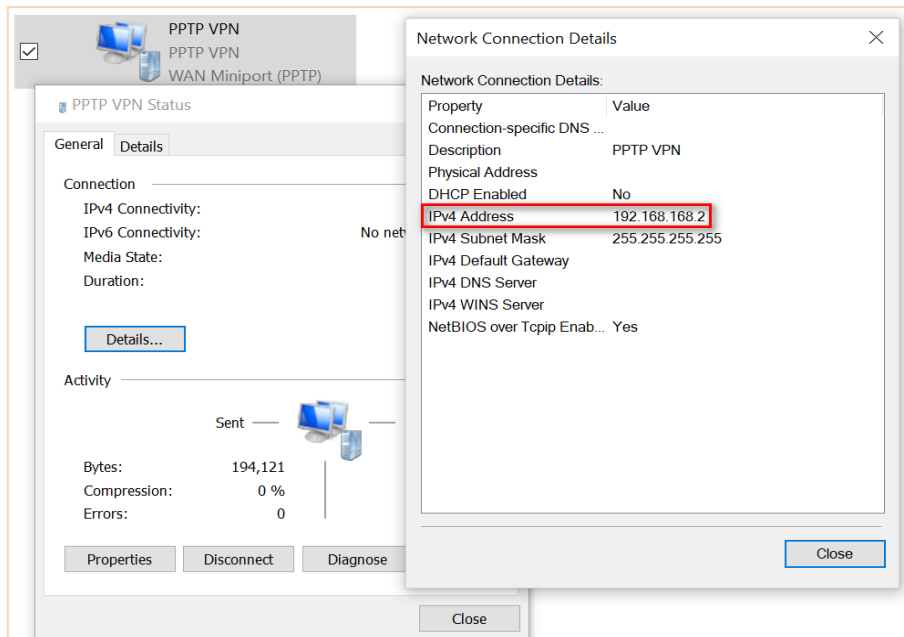
| | |
|---|-------------|
| Section Fifteen | 6944 Manual |
| PPTP Point to Point Tunnelling Protocol | Rev 2.8 |



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



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



Testing

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

Overview

Link Management

Industrial Interface

Network

Applications

VPN

OpenVPN

IPSec

GRE

DMVPN

L2TP

PPTP

Status

PPTP Server

PPTP Client

PPTP Server Status

| Index | Status | Remote IP | Interface | Uptime |
|-------|-----------|---------------|-----------|----------|
| 1 | Connected | 192.168.168.3 | ppp1 | 00:08:49 |

PPTP Client Status

| Index | Description | Status | Local IP | Remote IP | Interface | Uptime |
|-------|-------------|--------|----------|-----------|-----------|--------|
|-------|-------------|--------|----------|-----------|-----------|--------|

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

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

Pinging 192.168.5.1. with 32 bytes of data

Reply from 192.168.5.1: bytes=32 time=13ms TTL=64

Reply from 192.168.5.1: bytes=32 time=1ms TTL=64

Reply from 192.168.5.1: bytes=32 time=1ms TTL=64

Reply from 192.168.5.1: bytes=32 time=4ms TTL=64

Ping statistics for 192.168.5.1

Packets: sent = 4, Received = 4, Lost=0 (0% loss)

Approximate round trip times in milli-seconds

Minimum = 1ms, Maximum = 13ms, Average = 4ms

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

16 Configuring DMVPN on the 6944

16.1. AN029 Configuring DMVPN with RIP to a Cisco Router

Introduction

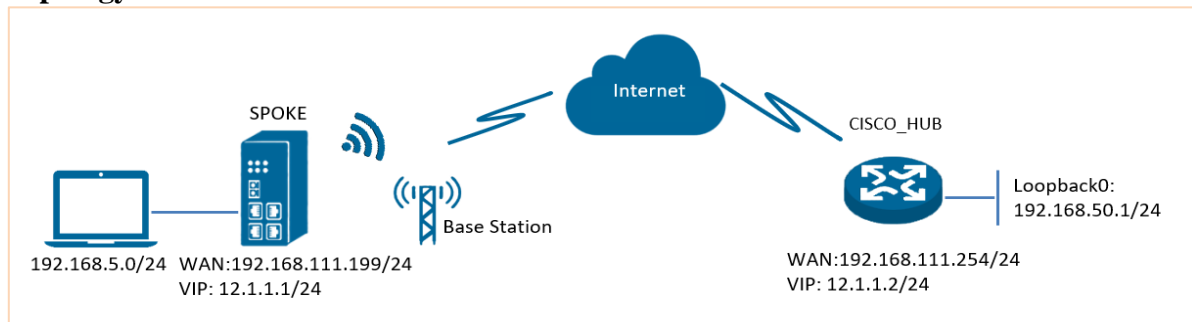
This document contains information explaining how to configure and use DMVPN with RIP on the Case Communications 6944 to a Cisco router. Software Versions

Software Compatibility

This feature requires the addition of Dynamic Routing software.

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

Topology



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

Configuration

CISCO Hub Configuration

Step 1: The configuration of CISCO as shown below:

```

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

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

ip address 192.168.111.254 255.255.255.0

ip nat outside
ip nat enable
ip virtual-reassembly
duplex full
speed auto
no mop enabled
!

interface FastEthernet0/1
ip address 192.168.6.3 255.255.255.0

ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!

router rip

Spoke Configuration

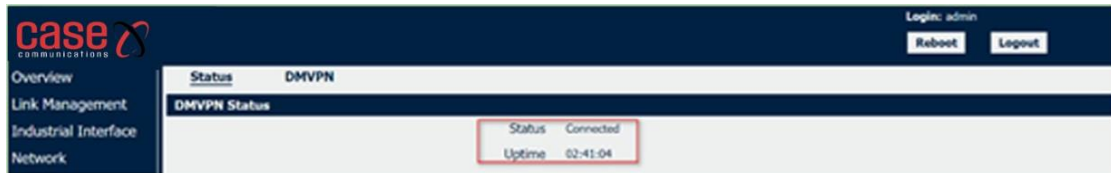
Step 1: Go to **VPN>DMVPN**, enable DMVPN and configure DMVPN as shown below.

Step 2: Click Save>Apply.

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

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

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |



Check the Cisco Routing Table

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

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

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

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

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

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

Testing

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

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

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

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

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

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

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

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

16.2. AN030-Configuring DMVPN with OSPF

Introduction

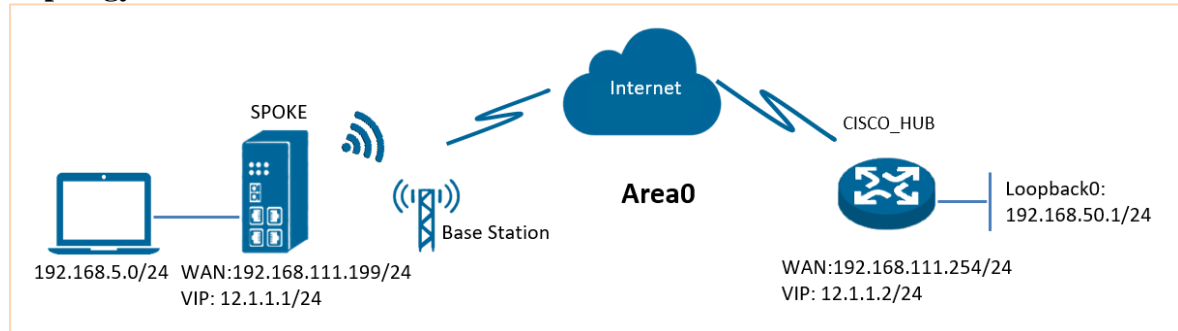
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running OSPF

6944 Software Versions

This feature requires the addition of Dynamic Routing software.

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

Topology



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

Configuration

CISCO Configuration

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

```

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

```

| | |
|------------------------|--------------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

```
ip virtual-reassembly
duplex full
speed auto
no mop enabled
!
```

```
interface FastEthernet0/1
ip address 192.168.6.3 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!
```

```
router ospf 1
router-id 9.9.9.9
```

Spoke Configuration

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

Step 2. Click Save>Apply.

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

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

Interfaces Settings

Index Interface Enable Passive Cost

Interface Settings

Index: 1

Interface: dmvptun

Enable Passive: ☐

Authentication Mode: None

Network Type: Non-Broadcast

Cost: 1

Priority: 1

Hello Interval: 30

Retransmit Interval: 5

Dead Interval: 120

Save Close

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

case communications

Login: admin Reboot Logout

Overview Link Management Industrial Interface Network

Status DMVPN

DMVPN Status

Status: Connected

Uptime: 02:41:04

Check the Routing Tables

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

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

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

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

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

case communications

Login: admin Reboot Logout

Overview Link Management Industrial Interface Network

Status Static Route RIP OSPF BGP

Route Table Information

| Index | Destination | Netmask | Gateway | Metric | Interface |
|-------|---------------|-----------------|----------------|--------|-----------|
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.11 | 0 | wan |
| 2 | 12.1.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | dmvptun |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 4 | 192.168.50.1 | 255.255.255.255 | 12.1.1.2 | 20 | dmvptun |
| 5 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

Testing

Step 1: Enable a CMD Ping from the end device of the 6944 SPOKE to the subnet on the CISCO HUB.

```

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

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

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

C:\Users\Administrator>

```

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

```

cisco2811#ping 192.168.5.2 source 192.168.50.1

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

```

Step 3: Test successful.

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

16.3. AN031 - Configuring DMVPN with BGP to a Cisco Router

Introduction

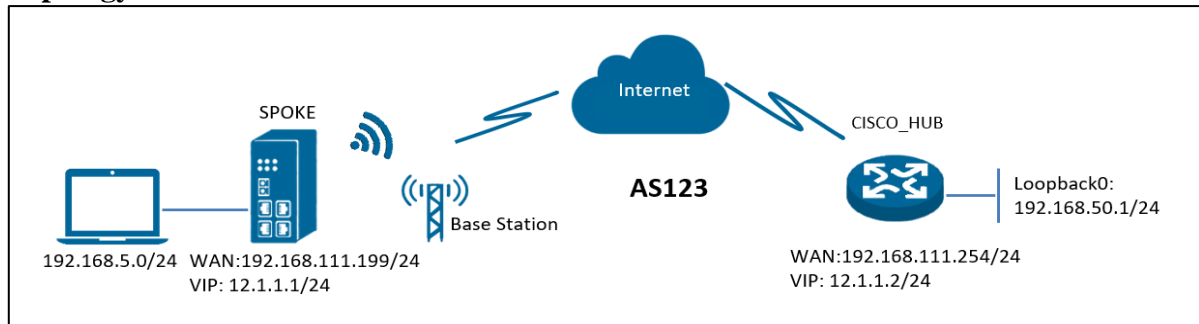
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running BGP

Software Compatibility

This applications requires the addition of Dynamic Routing software.

| Release Date | Doc. Version | Firmware Version | Software Version | Change Description |
|--------------|--------------|--------------------------|---|--------------------|
| 7/12/2018 | V1.1 | Devel (baba6c2) or newer | DR: V1.0.1 (642848) DMVPN: V1.0.1(42ccf3e) | First release |

Topology



- The 6944 runs as a DMVPN spoke with an IP device, which can ping the DMVPN hub.
- The CISCO router runs as DMVPN hub and has a static public IP Address.
- A tunnel is established between the 6944 spoke and Cisco hub, the subnets can PING each other.
- Both the 6944 and CISCO Router run BGP within a same AS123.

Configuration

CISCO Configuration

Step 1: Configure the CISCO router as shown below:

```

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

```


| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |

```

no mop enabled
!
interface FastEthernet0/1
ip address 192.168.6.3 255.255.255.0
ip nat inside
ip nat enable
ip virtual-reassembly
duplex auto
speed auto
!
router bgp 123
no synchronization
bgp router-id 2.2.2.2
bgp log-neighbor-changes

```

```

network 192.168.50.0
neighbor 12.1.1.1 remote-as 123
no auto-summary
ip forward-protocol nd
no ip http server
no ip http secure-server
!
ip nat inside source list 10 interface
FastEthernet0/0 overload
!
access-list 10 permit 192.168.6.0 0.0.0.255
snmp-server community public RO
cisco2811#

```

Spoke Configuration

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

Step 2: Go to **Network>Route>BGP**, enable BGP and configure BGP as shown below

Step 3: A Route has connected to the CISCO HUB. Go to **VPN>DMVPN>Status** to check the connection

| | |
|-----------------|-------------|
| Section Sixteen | 6944 Manual |
| DMVPN | Rev 2.8 |



Routing Tables

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

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

Gateway of last resort is 192.168.111.1 to network 0.0.0.0

C    192.168.88.0/24 is directly connected, Loopback3
C    192.168.111.0/24 is directly connected, FastEthernet0/0
C    172.16.0.0/24 is subnetted, 2 subnets
C      172.16.1.0 is directly connected, Loopback1
C      172.16.2.0 is directly connected, Loopback2
B    192.168.5.0/24 [200/0] via 12.1.1.3, 00:03:14
C    10.0.0.0/24 is subnetted, 1 subnets
C      10.1.1.0 is directly connected, Loopback100
C    12.0.0.0/24 is subnetted, 1 subnets
C      12.1.1.0 is directly connected, Tunnel1
C    192.168.50.0/24 is directly connected, Loopback0
S*   0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#
```

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

| Index | Destination | Netmask | Gateway | Metric | Interface |
|-------|---------------|---------------|----------------|--------|-----------|
| 1 | 0.0.0.0 | 0.0.0.0 | 192.168.111.11 | 0 | wan |
| 2 | 12.1.1.0 | 255.255.255.0 | 0.0.0.0 | 0 | dmvpnrtun |
| 3 | 192.168.5.0 | 255.255.255.0 | 0.0.0.0 | 0 | lan0 |
| 4 | 192.168.50.0 | 255.255.255.0 | 12.1.1.2 | 20 | dmvpnrtun |
| 5 | 192.168.111.0 | 255.255.255.0 | 0.0.0.0 | 0 | wan |

Testing

Step 1: Send a Ping from the device on the 6944 SPOKE to the subnet of CISCO HUB.

```
C:\>\Users\Administrator>Ping 192.168.50.1
Pinging 192.168.50.1 with 32 bytes of data:
Reply from 192.168.50.1 bytes=32 time= 4ms TTL=254
Reply from 192.168.50.1 bytes=32 time= 4ms TTL=254
Reply from 192.168.50.1 bytes=32 time=4ms TTL=254
Reply from 192.168.50.1 bytes=32 time=4ms TTL=254
```

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

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

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

| | |
|-------------------|-------------|
| Section Seventeen | 6944 Manual |
| IP Pass Through | Rev 2.8 |

17 IP Pass through

Overview

IP Pass through mode, disables NAT and routing and passes the WAN IP address from the WAN interface to the device connected on the local Interface. It is used instead of Network Address Translation (NAT) in order to make the router "transparent" in the communication process.

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.

This page left blank intentionally

18 Industrial Interface.

18.1. Industrial Interface Overview on the 6944

The Industrial page contains tabs for making configuration settings to the Serial RS232 and RS485, Digital input and output. Select Serial & Digital IO from the main navigation menu to navigate to this page.

Serial Connection

Review the status of serial connection.

| 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 |
| 2 | false | COM2 | 115200 | 8 | 1 | None |

Serial->Connection

- **Enable** - Displays status of current serial function.
- **Port** - Displays the serial type of COM port.
- **Baud Rate** - Displays the serial port baud rate.
- **Data Bits** - Displays the serial port Data Bits.
- **Stop Bits** - Displays the serial port Stop Bits.
- **Parity** - Displays the serial port parity.

| Connection Settings | |
|----------------------------------|--------------------------|
| Serial Connection Settings | |
| Index | 1 |
| Enable | <input type="checkbox"/> |
| Port | COM1 |
| Baud Rate | 115200 |
| Data Bits | 8 |
| Stop Bits | 1 |
| Parity | None |
| Transmission Settings | |
| Transmission Method | Transparent |
| MTU | 1024 |
| Protocol | TCP Client |
| Remote IP Address | |
| Remote Port | 2000 |
| <div>Save</div> <div>Close</div> | |

| | |
|----------------------|-------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

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 | Transparent ▼ |
| MTU | 1024 ⓘ |
| Protocol | TCP Server ▼ |
| Local IP Address | |
| Local Port | 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 | Transparent ▼ |
| MTU | 1024 ⓘ |
| Protocol | UDP ▼ |
| Local IP Address | |
| Local Port | 2000 |
| Remote IP Address | |
| Remote Port | 2000 |

| | |
|----------------------|-------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

- **Local IP Address** - Enter the IP Address of the local endpoint.
- **Local Port** - The port number assigned to the serial IP port on which communications will take place.
- **Remote IP Address** - Enter the IP address of the remote server.
- **Remote Port** - Enter the port number of the remote server.

Digital IO

This section allows you to set the Digital IO parameters. The Digital input can be used for triggering an alarm, and Digital output or could be used for controlling a slave device by digital signal. You could review the status of Digital IO as below.

| Status | Digital IO | | |
|----------------------------|------------|-------------|-----------|
| Digital Input Information | | | |
| Index | Enable | Logic Level | Status |
| 1 | false | High | Alarm OFF |
| 2 | false | High | Alarm OFF |
| Digital Output Information | | | |
| Index | Enable | Logic Level | Status |
| 1 | false | Low | Alarm OFF |
| 2 | false | Low | Alarm OFF |

Digital IO->Status

- **Enable** - Displays status of current digital IO function.
- **Logic Level** - Displays the electrical level of digital IO port.
- **Status** - Displays the alarm status of digital IO port.

| Digital Input | |
|--|----------------------------------|
| Digital Input Settings | |
| Index | <input type="text" value="1"/> |
| Enable | <input type="checkbox"/> |
| Alarm ON Mode | <input type="text" value="Low"/> |
| Alarm ON Content | <input type="text"/> |
| Alarm OFF Content | <input type="text"/> |
| <input type="button" value="Save"/> <input type="button" value="Close"/> | |

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.

| | |
|-----------------------------|--------------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

Digital Output

Digital Output Settings

Index

Enable ☐

Alarm Source

Alarm ON Action

Alarm OFF Action

Digital IO->Digital Output

- Enable**
Check this box to enable digital output function.
- Alarm Source**
Select from “Digital Input1”, “Digital Input2” or “SMS”, Digital output triggers the related action when there is alarm comes from Digital Input or SMS.
- Alarm ON Action**
Select from “High”, “Low” or “Pulse”. High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.
- Alarm OFF Action**
Initiates when alarm disappeared. Select from “High”, “Low” or “Pulse”. High means high electrical level output. Low means low electrical level output. Pulse will generate a square wave as specified in the pulse mode parameters when triggered.
- Pulse Width**
This parameter is available when select “Pulse” as “Alarm ON Action/Alarm OFF Action”. The selected digital output channel will generate a square wave as specified in the pulse mode parameters.

18.2. AN004 Transparent Mode with TCP Client on RS232

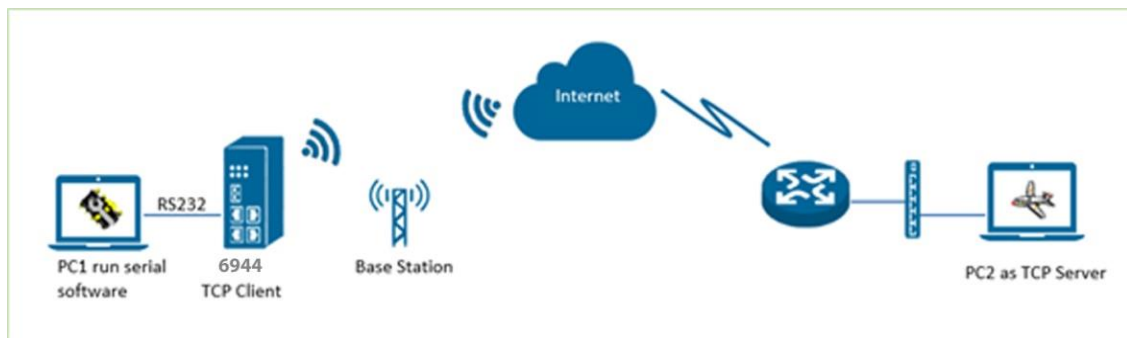
Overview

This document contains information on how to configure and use RS232 Transparent Mode with a TCP Client.

Software Version - This feature works with standard software

| Release Date | Doc. Version | Firmware Version | Additional sw | Change Description |
|--------------|--------------|---------------------|---------------|--------------------|
| 3.8.2018 | V1.1 | V1.1.1.4 (0c0c09fa) | Std Software | First released |

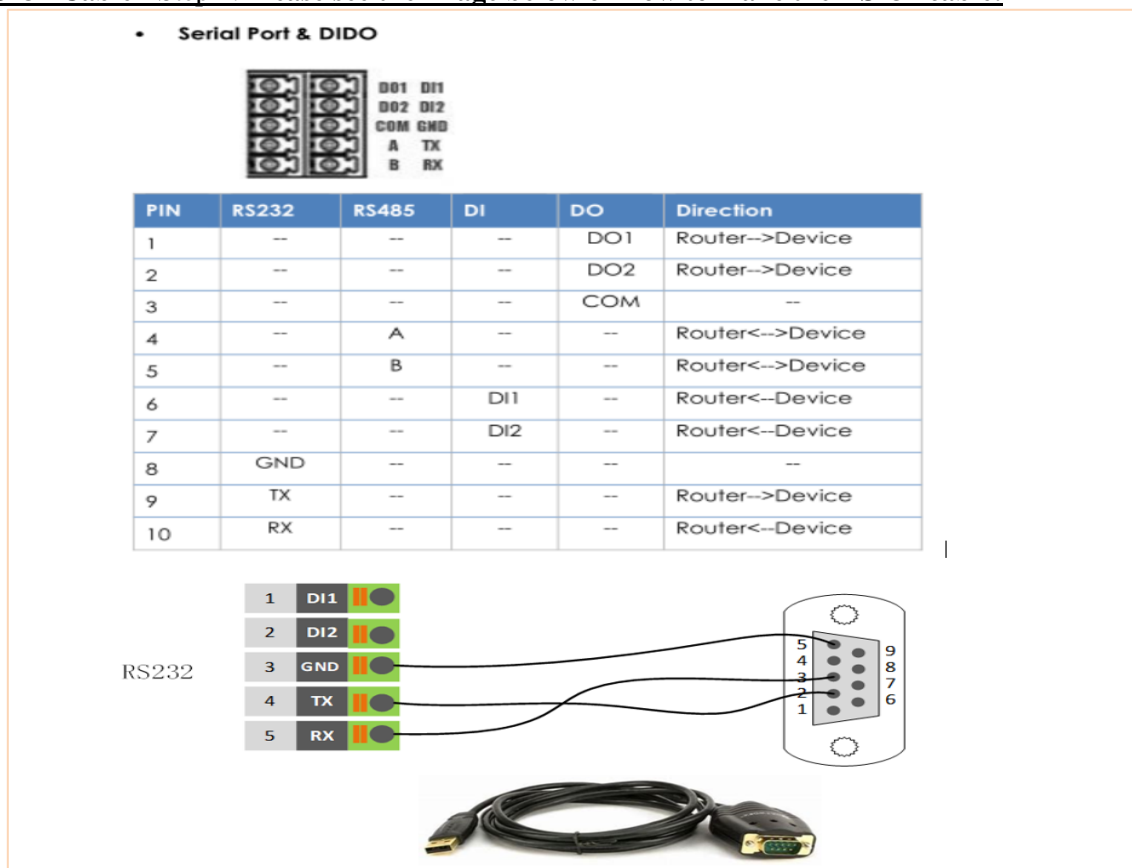
Testing Topology



- The 6944 runs as a TCP Client and connects to the Internet via its SIM card.
- PC1 simulates as a serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server side through 6944 in TCP transparent mode.
- PC2 runs as a TCP server getting its Public Static IP address from the Internet. PC2 enables TCP software, such as TCPUDPDbg. TCPUDPDbg allowing it to receive the data from TCP Client side.

Configuration

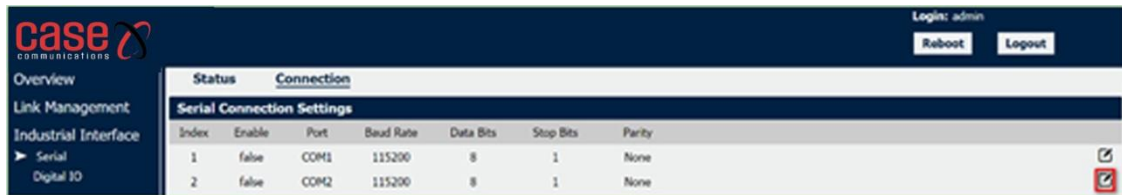
RS232 Cable - Step 1: Please see the image below on how to make the RS232 cable:



Configuration

RS232 Configuration

Step1. Go to Link **Industrial Interface>Serial>Connection>Index 2**, Click the **Edit** button of COM2.



Step 1: Enable the RS232 setting, select the Protocol as “TCP Client” and enter the Server IP address and Server Port. **Click Save > Apply.**

Connection Settings

Serial Connection Settings

Index: 2
 Enable: ☒
 Port: COM2
 Baud Rate: 115200
 Data Bits: 8
 Stop Bits: 1
 Parity: None

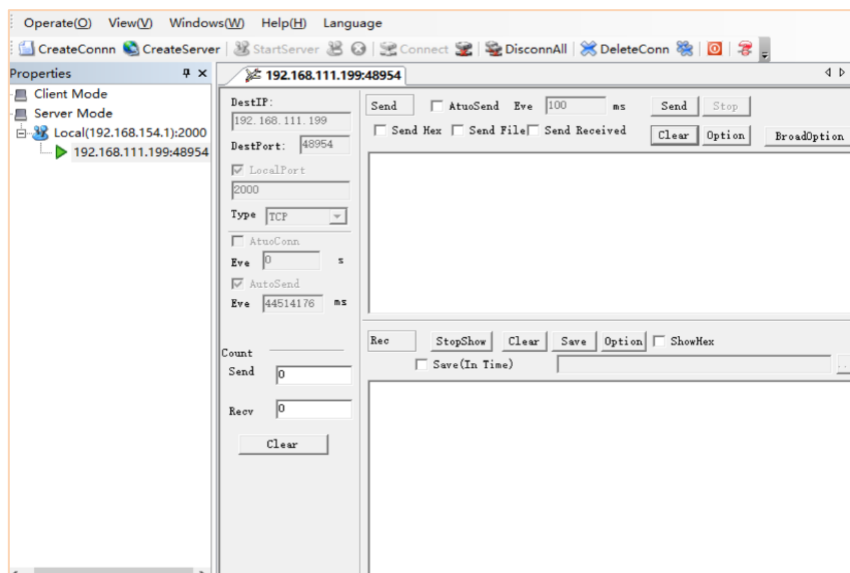
Transmission Settings

Transmission Method: Transparent
 MTU: 1024
 Protocol: TCP Client
 Remote IP Address: 113.65.230.194
 Remote Port: 2000

Buttons: Save, Close

TCP Server Configuration

Step 1. Run the TCP Software “TCPUDPDbg” on server PC2, the 6944 will connect to the TCP Server automatically.



Step 2: Go to **Industrial Interface>Serial>Status>Serial Information>Index2**, it will show the connection status.

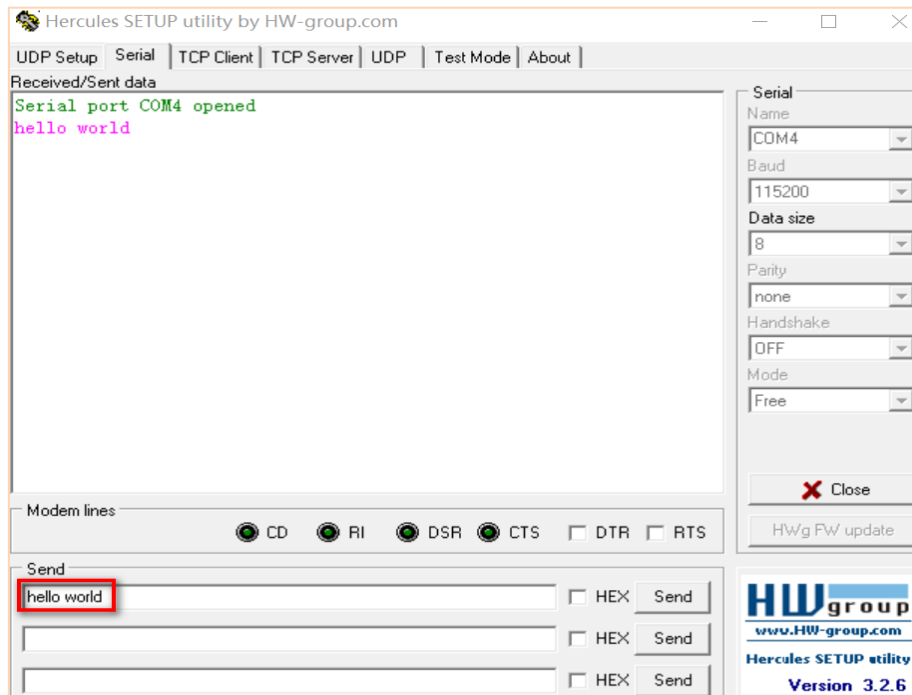


The screenshot shows the 'Industrial Interface' section of the Case Communications web application. A table titled 'Serial Information' displays the status of two serial connections. The first connection (Index 1) is disabled and disconnected. The second connection (Index 2) is enabled and connected, with the 'Connected' status highlighted by a red box.

| Index | Enable | Serial Type | Transmission Method | Protocol | Connection Status |
|-------|--------|-------------|---------------------|------------|-------------------|
| 1 | false | RS485 | Transparent | TCP Client | Disconnected |
| 2 | true | RS322 | Transparent | TCP Client | Connected |

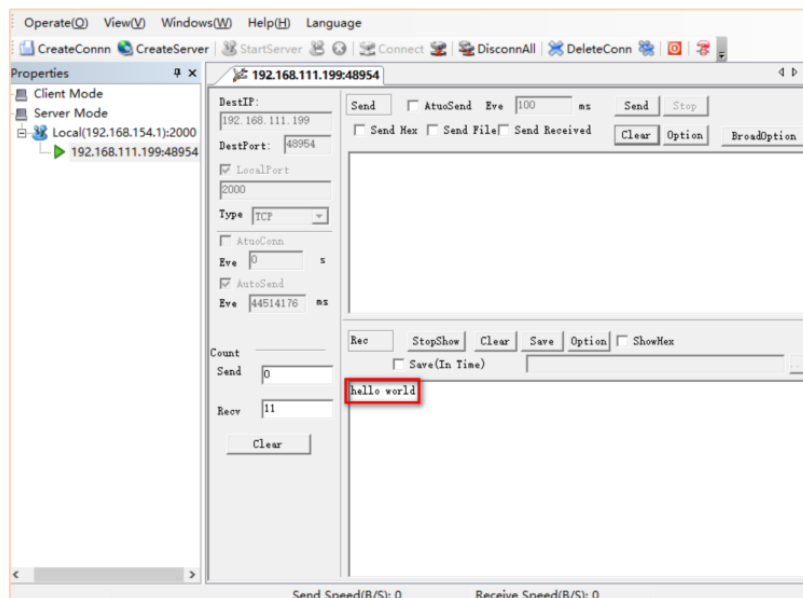
Testing

Step 1: Run the serial software "Hercules" on PC1, send the data "hello world".



Step 2: Test Result

Step 3: TCP Server side can receive the data "hello world"



| | |
|----------------------|-------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

18.3. AN005 RS485 Transparent Mode

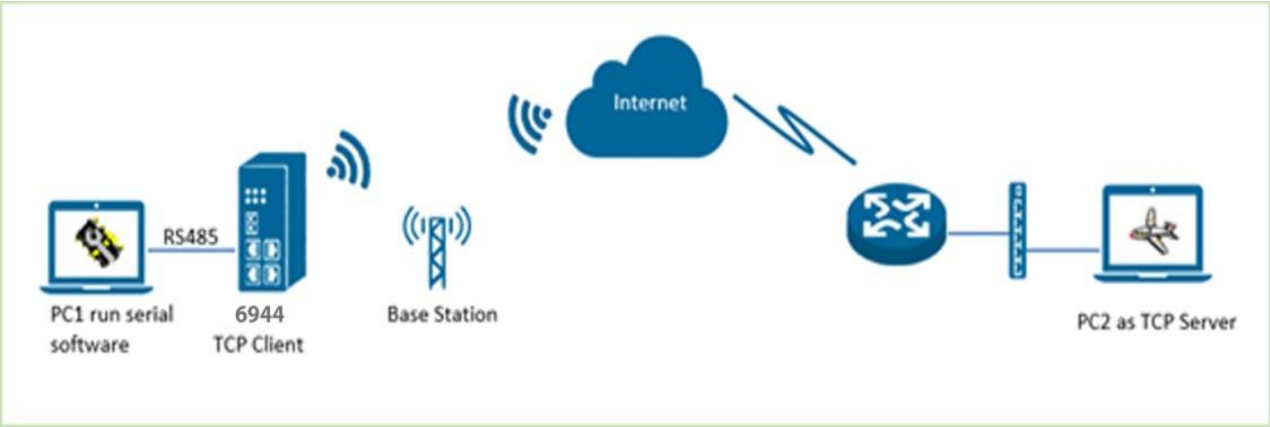
Overview

This document contains information regarding the configuration of RS485 in Transparent Mode with using a TCP Client on the 6944.

Software Version

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 3.8.2018 | V1.0.0 | V1.1.4 (0c0c9fa) | Std Software | First released |

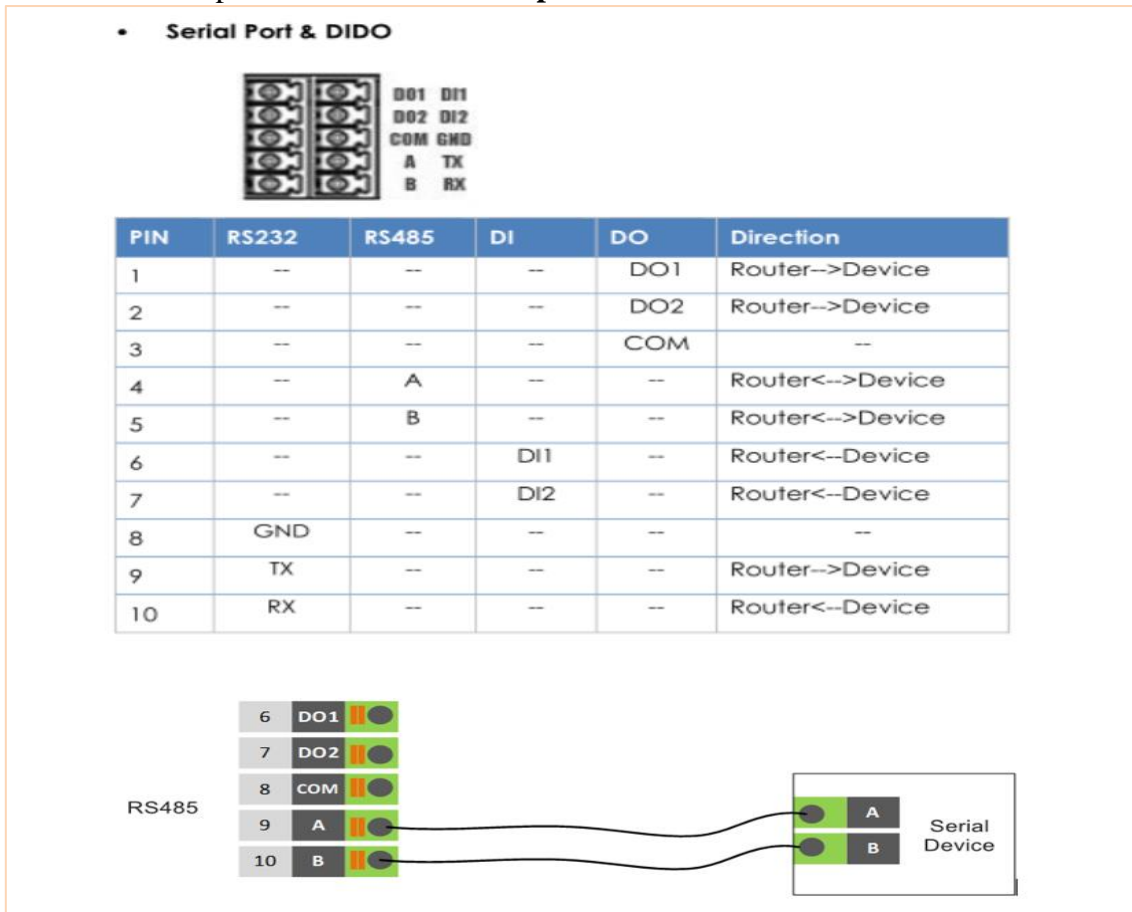
Testing Topology



- The 6944 runs as a TCP Client and connect to the Internet with a SIM card.
- PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server through the 6944 with TCP transparent mode.
- PC2 runs as a TCP server and connected to the Internet via a Public Static IP address. PC2 enable TCP software, such as TCPUDPDbg. TCPUDPDbg allowing it to receive the data from TCP Client side.

Configuration

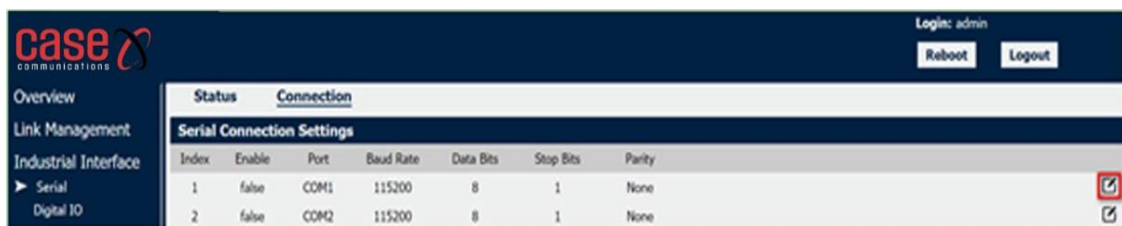
RS485 Cable - Step1. Please follow below picture to make the RS485 cable:



Configuration

RS485 Configuration

Step1. Go to Link **Industrial Interface>Serial>Connection>Index 1**, Click the **Edit** button of COM1.



Step 2: Enable the RS485 setting, select Protocol as “TCP Client” and enter the Server IP address and Server Port. **Click Save > Apply**

| | |
|-----------------------------|--------------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

Connection Settings

Serial Connection Settings

Index
Enable ☒
Port
Baud Rate
Data Bits
Stop Bits
Parity

Transmission Settings

Transmission Method
MTU
Protocol
Remote IP Address
Remote Port

TCP Server Configuration

Step1.Run TCP Software “TCPUDPDbg” on server PC2, the 6944 will connect to the TCP Server automatically.

Step 2. Go to **Industrial Interface>Serial>Status>Serial Information>Index1**, to show the connection status.

casecommunications

Overview

Link Management

Industrial Interface

Serial

Digital IO

Status

Connection

Serial Information

| Index | Enable | Serial Type | Transmission Method | Protocol | Connection Status |
|-------|--------|-------------|---------------------|------------|-------------------|
| 1 | true | RS485 | Transparent | TCP Client | Connected |
| 2 | false | RS232 | Transparent | TCP Client | Disconnected |

Login: admin

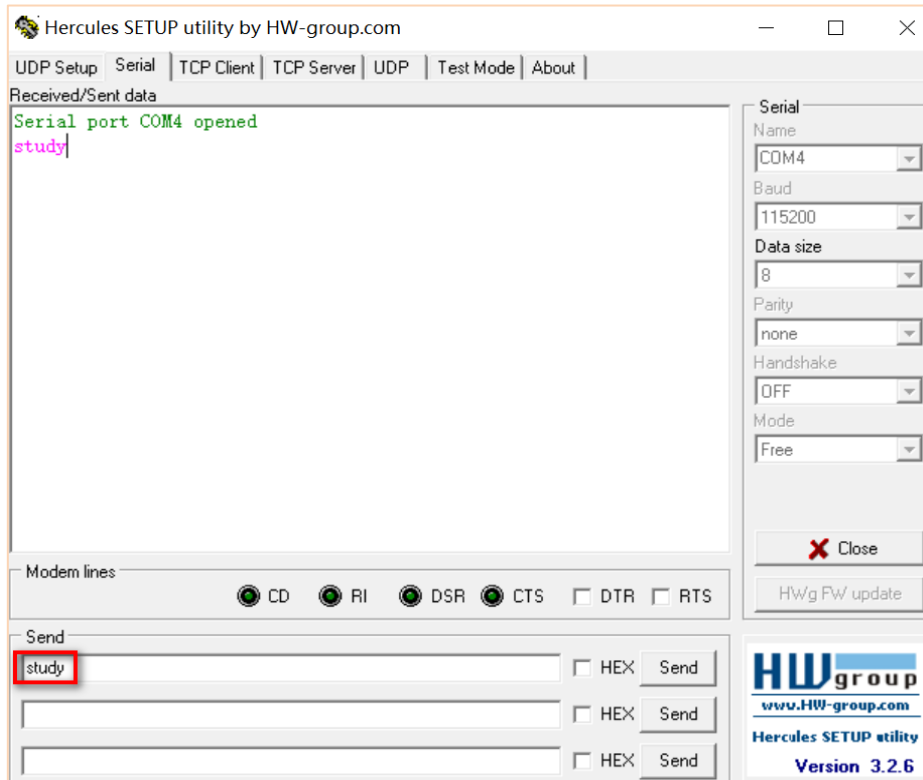
Reboot

Logout

| | |
|----------------------|-------------|
| Section Eighteen | 6944 Manual |
| Industrial Interface | Rev 2.8 |

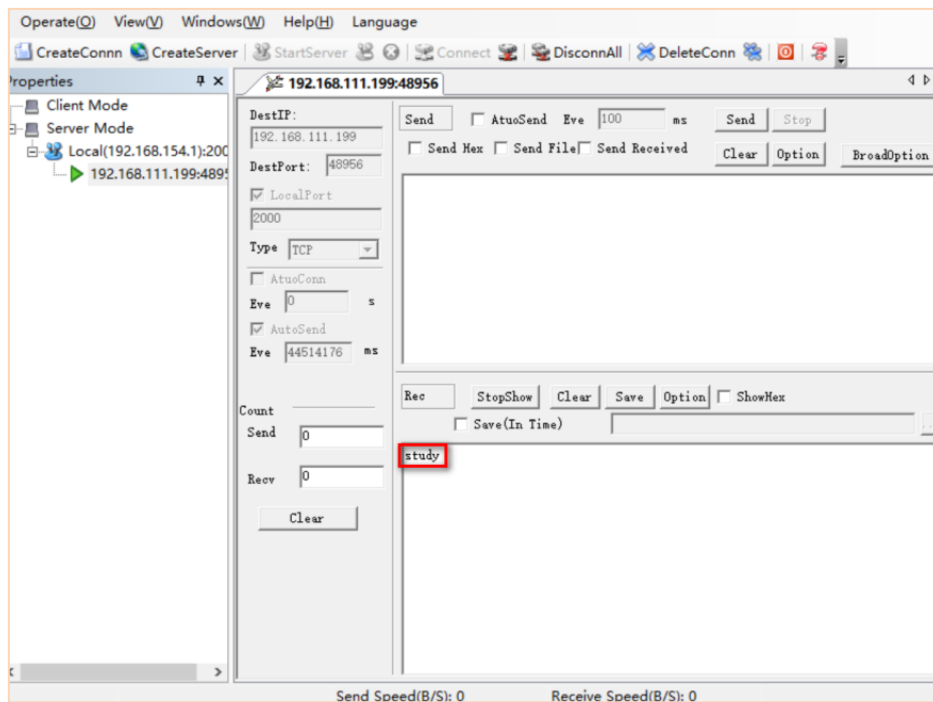
Testing

Step1. Run the serial software as an example using the word "Hercules" on PC1, send the data, for example the word "study".



Test Results

Step1. Ensure the TCP Server side can receive the data "study"

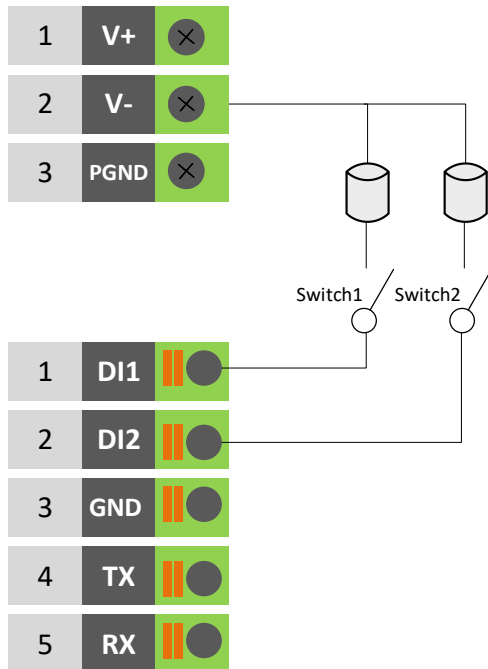


This page left blank intentionally

19. Digital I / O Ports

19.1. Digital Input Port

Typical Application Diagram



DI ELECTRICAL CHARACTERISTICS

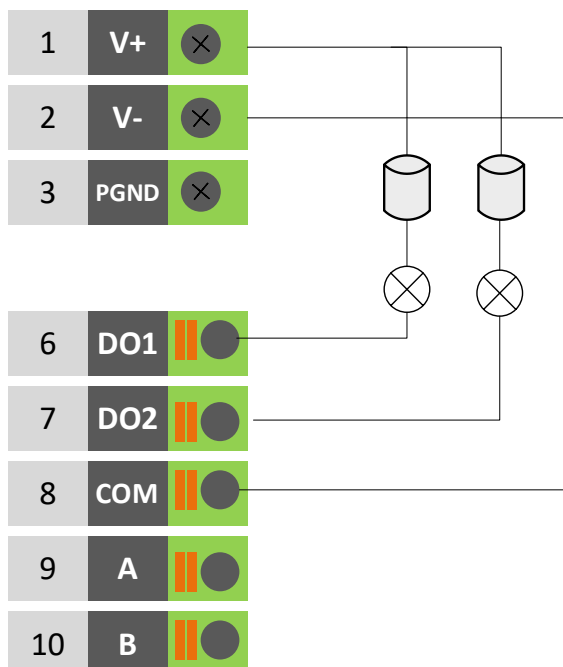
1. Galvanic isolation;
2. Over-Voltage Protection: 36 VDC
3. Over-Current Protection: 100mA per channel @ 25°C

Dry Contact Typical Application

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

19.2. Digital Output

Typical Application Diagram



DO ELECTRICAL CHARACTERISTICS

1. Galvanic isolation;
2. Over-Voltage Protection: 36 VDC
3. Over-Current Protection: 50mA per channel @ 25°C

Wet Contact Typical Application

DO Logic LOW: Switch ON(Led ON)
DO Logic HIGH: Switch OFF(Led OFF)

This page left blank intentionally

| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

20 MODBUS

20.1 MODBUS Slave

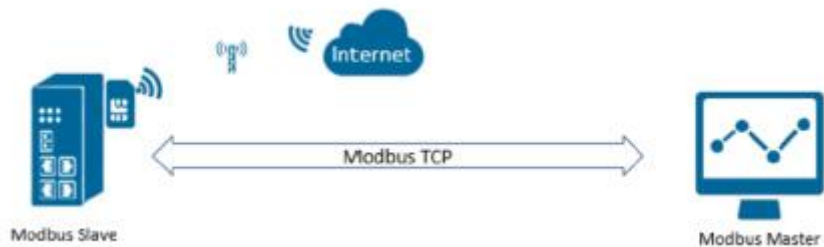
Overview

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

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Change Description |
|--------------|--------------|------------------|--------------------|
| 18.7.2019 | V1.2.1 | V1.1.0 (ADcaac4) | First release |

Topology



The 6944 router runs as Modbus Slave with a static public IP address with a SIM card.

The Modbus Master connects to the 6944 router (Modbus Slave) via a TCP connection.

The Modbus Master reads the status of the Digital IO and controls the DO.

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

Digital Input - Output Register Table

| Index | Item | Function | Address (Decimal) | Qty | Values |
|-------|------------------|----------------------|-------------------|-----|-------------------------------------|
| 1 | Digital Input 1 | 02 Input Status | 13800 | 1 | 00 – Low 01 - High |
| 2 | Digital Input 2 | 02 Input Status | 13801 | 1 | 00 – Low 01 - High |
| 3 | Digital Output 1 | 01 Coil Status | 13802 | 2 | 00 - Low 01 – High 02 - Pulse |
| 4 | Digital Output 2 | 01 Coil Status | 13804 | 2 | 00 - Low 01 – High 02 - Pulse |
| 5 | DO1 Pulse Width | 03 Holding Registers | 13806 | 1 | Default:500(ms) range:1~1000 |
| 6 | DO2 Pulse Width | 03 Holding Registers | 13807 | 1 | Default:500(ms) range:1~1000 |

| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

Example Read Di Status

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity |
|--------|----------------|-------------|-------------|----------|---------------|-------------|----------|
| Tx | 01.90 | 00.00 | 00.06 | 01 | 02 | 35E8 | 00.01 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Byte Length | Value |
| Rx | 01.90 | 00.00 | 00.04 | 01 | 02 | 01 | 01 |

Example Read Do Status

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity |
|--------|----------------|-------------|-------------|----------|---------------|-------------|----------|
| Tx | 04.81 | 00.00 | 00.06 | 01 | 01 | 35EA | 00.02 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Byte Length | Value |
| Rx | 04.81 | 00.00 | 00.04 | 01 | 01 | 01 | 02 |

Example: Control Do-Output Pulse

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity | Byte Length | Value |
|--------|----------------|-------------|-------------|----------|---------------|---------|----------|-------------|-------|
| Tx | 07.29 | 00.00 | 00.08 | 01 | 0F | 35EA | 00.02 | 01 | 02 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity | | |
| Rx | 07.29 | 00.00 | 00.06 | 01 | 0F | 35EA | 00.02 | | |

Cellular 6944 Series, Cellular / Ethernet / Wi-Fi / Serial / DI/O

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

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Value |
|--------|----------------|-------------|-------------|----------|---------------|---------|-------|
| Tx | 07.2C | 00.00 | 00.06 | 01 | 06 | 35EE | 01 F4 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Value |
| Rx | 07.2C | 00.00 | 00.06 | 01 | 06 | 35EE | 01 F4 |

Configuration

6944 Configuration

Step 1 Go to **Application>Modbus Slave**, enable the Modbus Slave feature as shown below:

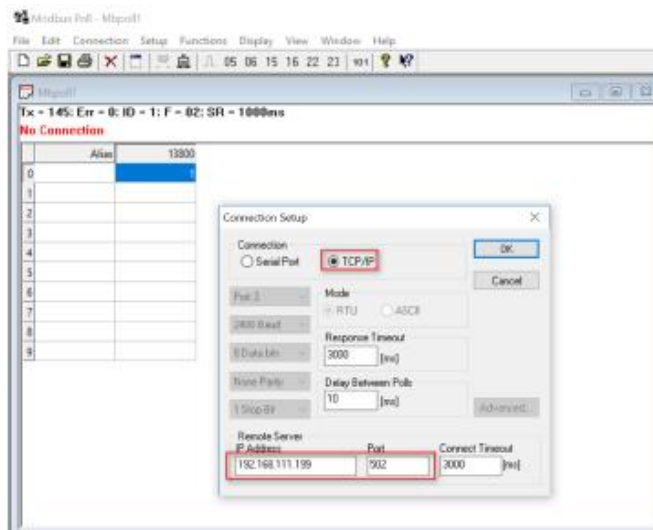
The screenshot shows the 'Modbus Slave' configuration window. On the left is a navigation menu with options: Overview, Link Management, Industrial Interface, Network, Applications, DNS, SMS, Schedule Editor, Modbus Slave (selected), VPN, and Maintenance. The main area is titled 'Status: Modbus Slave' and 'General Settings'. It contains a form with the following fields: 'Enable' (checked), 'Protocol' (TCP/IP), 'Slave ID' (1), 'Local IP' (empty), and 'Local Port' (502). At the bottom right are 'Save' and 'Apply' buttons.

Step 2 Click **Save > Apply**

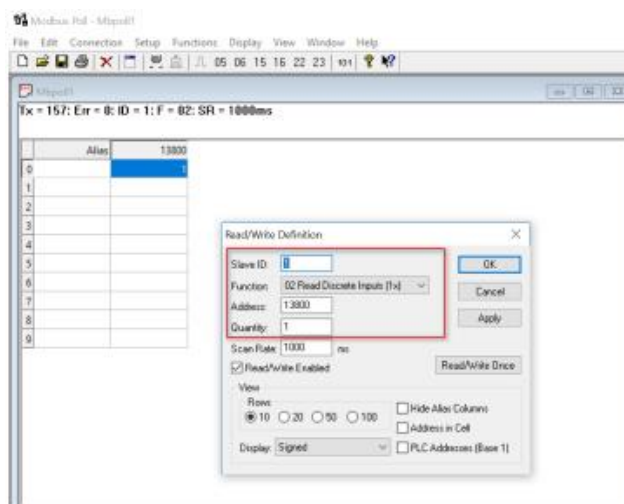
Testing

Read Digital Input Status

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

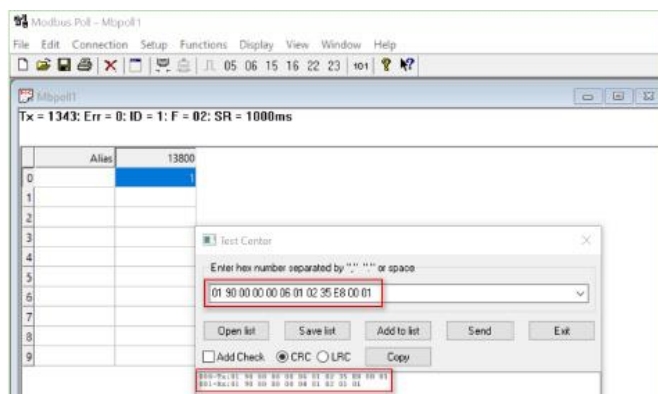


(Path: Setup> Read/ Write Definition)



Send the command to read the status of DI 1

(Path: Functions>Test Centre)



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

| | |
|-----------------------|--------------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

Read Digital Output Status

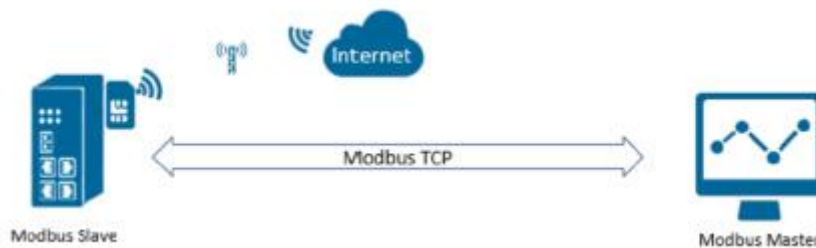
Set the Function Code to “01”, Address 13802 and the quantity is set to “2”.

Path: Setup>Read / Write Definition

Control Digital Output

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

Topology



1. The 6944 router runs as a Modbus Slave with a static public IP address with a SIM card.
2. Modbus Master connects to the 6944 router (Modbus Slave) via a TCP connection.
3. The Modbus Master reads the status of Digital IO and control DO.

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

Digital I/O Register Table

| Index | Item | Function | Address (Decimal) | Qty | Values |
|-------|------------------|----------------------|-------------------|-----|-------------------------------------|
| 1 | Digital Input 1 | 02 Input Status | 13800 | 1 | 00 – Low 01 - High |
| 2 | Digital Input 2 | 02 Input Status | 13801 | 1 | 00 – Low 01 - High |
| 3 | Digital Output 1 | 01 Coil Status | 13802 | 2 | 00 - Low 01 – High 02 - Pulse |
| 4 | Digital Output 2 | 01 Coil Status | 13804 | 2 | 00 - Low 01 – High 02 - Pulse |
| 5 | DO1 Pulse Width | 03 Holding Registers | 13806 | 1 | Default:500(ms) range:1~1000 |
| 6 | DO2 Pulse Width | 03 Holding Registers | 13807 | 1 | Default:500(ms) range:1~1000 |

Example Read Di Status

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity |
|--------|----------------|-------------|-------------|----------|---------------|-------------|----------|
| Tx | 01.90 | 00.00 | 00.06 | 01 | 02 | 35E8 | 00.01 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Byte Length | Value |
| Rx | 01.90 | 00.00 | 00.04 | 01 | 02 | 01 | 01 |

| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

Example Read Do Status

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity |
|--------|----------------|-------------|-------------|----------|---------------|-------------|----------|
| Tx | 04.81 | 00.00 | 00.06 | 01 | 01 | 35EA | 00.02 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Byte Length | Value |
| Rx | 04.81 | 00.00 | 00.04 | 01 | 01 | 01 | 02 |

Example: Control Do-Output Pulse

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity | Byte Length | Value |
|--------|----------------|-------------|-------------|----------|---------------|---------|----------|-------------|-------|
| Tx | 07.29 | 00.00 | 00.08 | 01 | 0F | 35EA | 00.02 | 01 | 02 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Quantity | | |
| Rx | 07.29 | 00.00 | 00.06 | 01 | 0F | 35EA | 00.02 | | |

Cellular 6944 Series, Cellular / Ethernet / Wi-Fi / Serial / DI/O

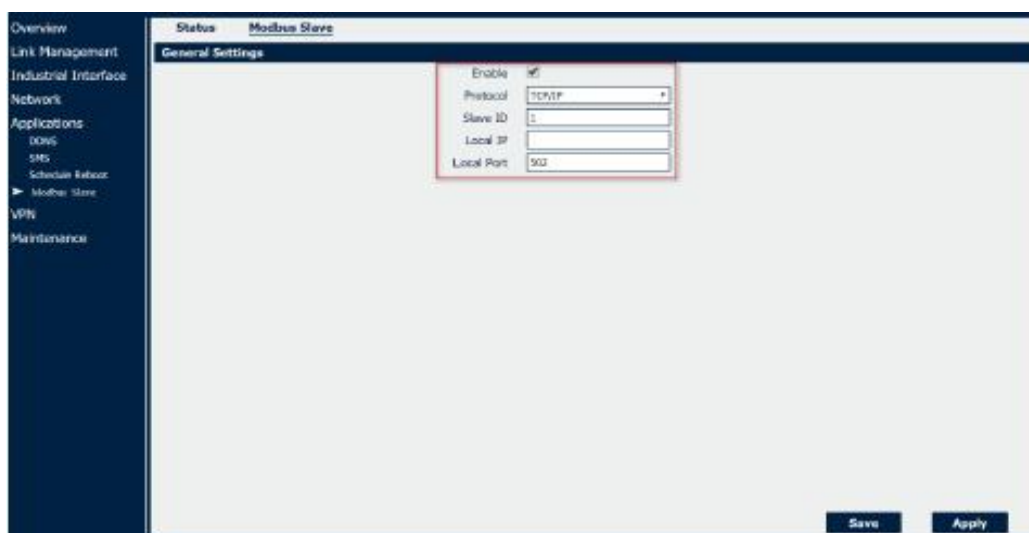
Example: Modify the width of the output pulse—500ms (The current output pulse to modify the width

| Master | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Value |
|--------|----------------|-------------|-------------|----------|---------------|---------|-------|
| Tx | 07.2C | 00.00 | 00.06 | 01 | 06 | 35EE | 01 F4 |
| Slave | Transaction ID | Protocol ID | Data Length | Slave Id | Function Code | Address | Value |
| Rx | 07.2C | 00.00 | 00.06 | 01 | 06 | 35EE | 01 F4 |

Configuration

6944 Configuration

Step 1. Go to **Application>Modbus Slave**, enable the Modbus Slave feature as shown below:

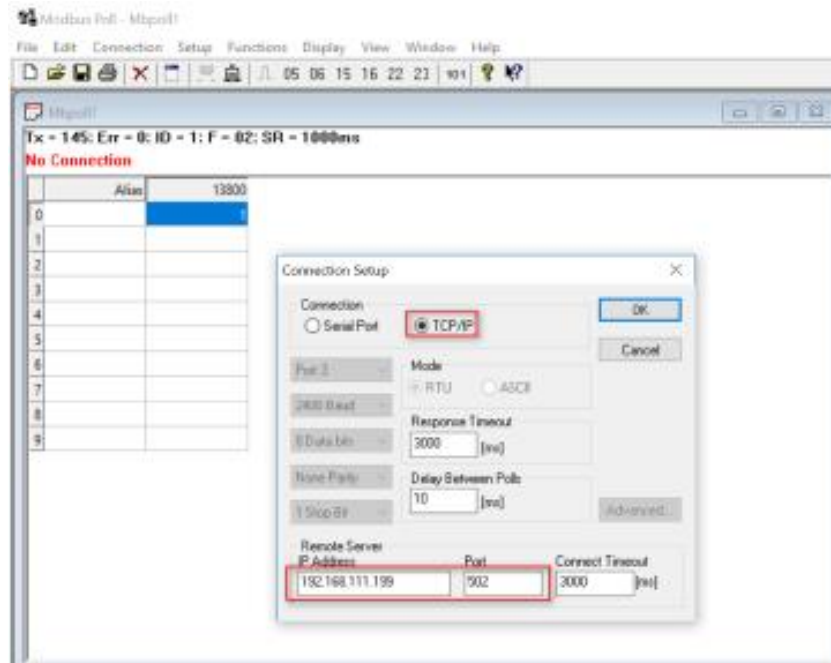


Step2. Click **Save > Apply**

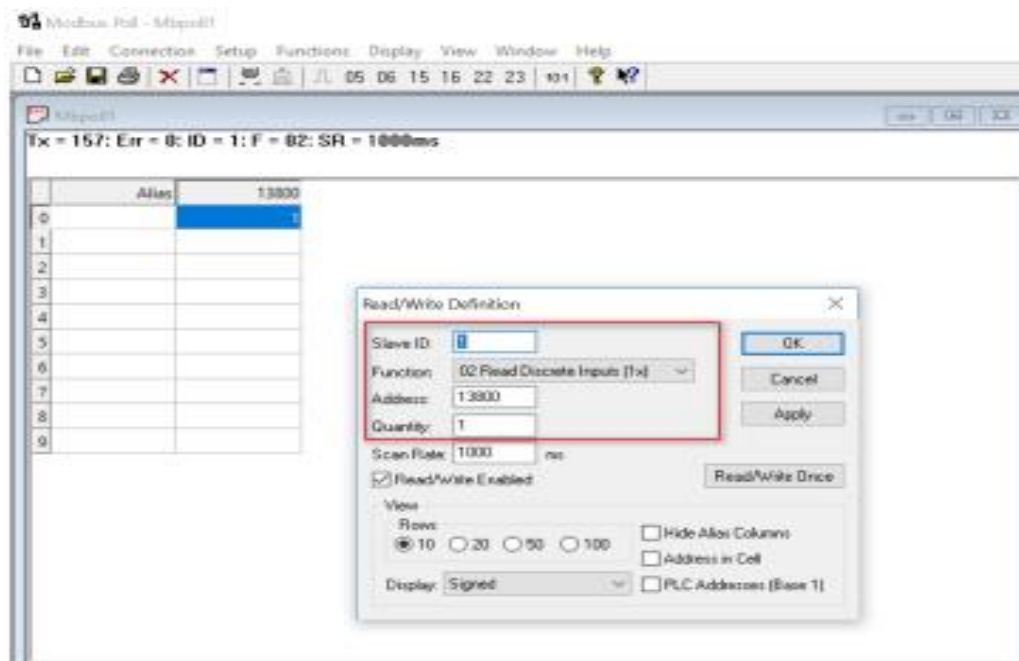
Testing

Read Digital Input Status

Step 1. Run the software “MODBUS Poll” to connect to the 6944 (MODBUS Slave) as shown below (Path Connection > Connect)



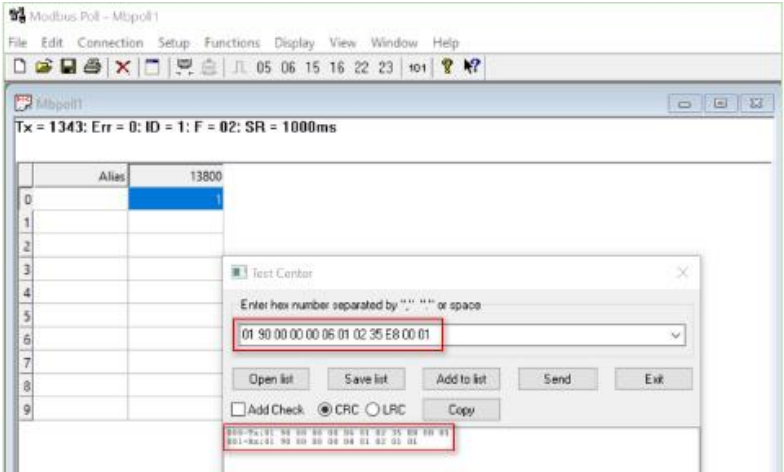
(Path: Setup> Read/ Write Definition)



Step 2. Send the command to read the status of DI 1

(Path: Functions>Test Centre)

| | |
|-----------------------|--------------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |



The reply Value is “00”, DO1 status is “Low”. Then the test is successful.

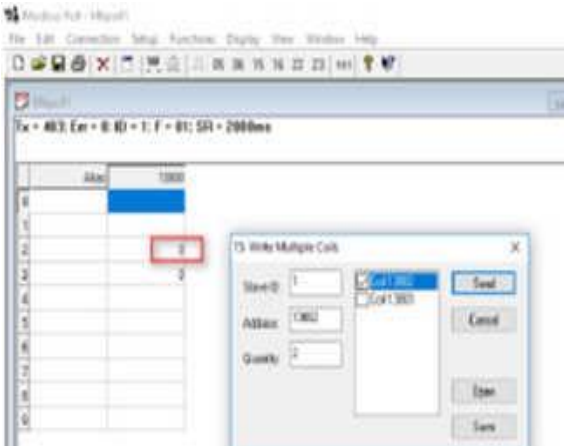
Read Digital Output Status

1. Set the Function Code to “01”, Address 13802 and the quantity is set to “2”.
Path: Setup>Read / Write Definition

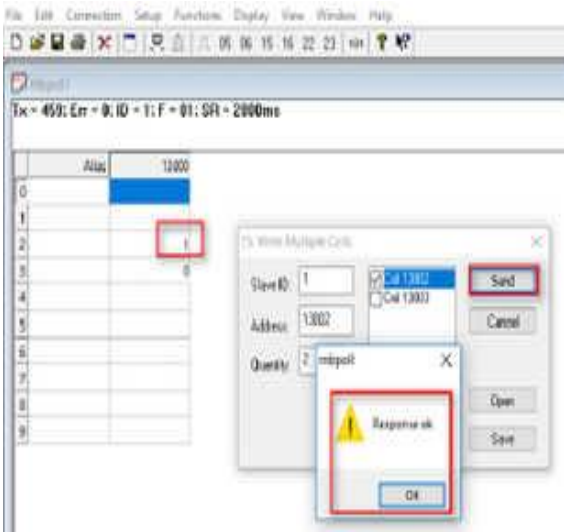
Control Digital Output

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

Test Successful



Test Successful



20.2 MODBUS Master

Introduction

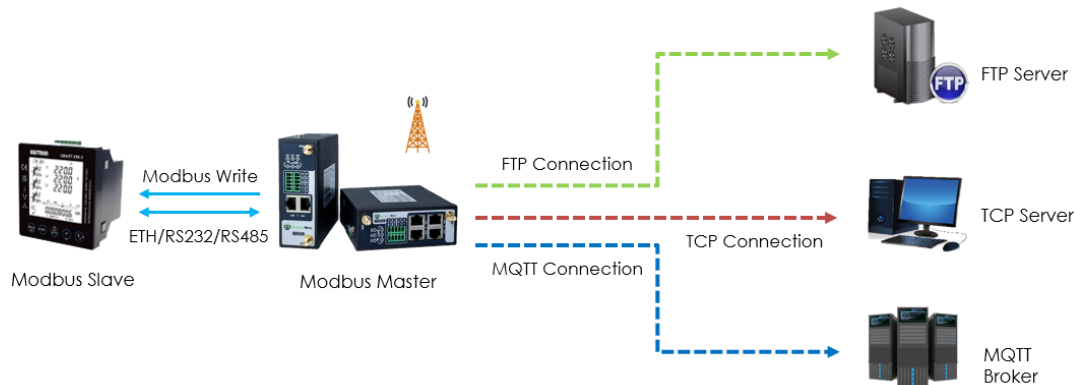
This section of the manual relates to the software for the MODBUS Master on the 6944 router. It requires the 6944 to be running the MODBUS Master software, which is version V1.0.0 written in Feb 2020

Software Compatibility

Updates between document versions are cumulative. Therefore, the latest document will include all the contents from the previous versions.

| Release Date | Doc. Version | Firmware Version | Change Description |
|--------------|--------------|------------------|--------------------|
| 2020/02/18 | V1.0.0 | V1.2.0(e958360) | MODBUS Master |

Topology



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

The 6944 router polls the MODBUS data from the MODBUS slave and sends to the remote management center via TCP, FTP or MQTT protocol.

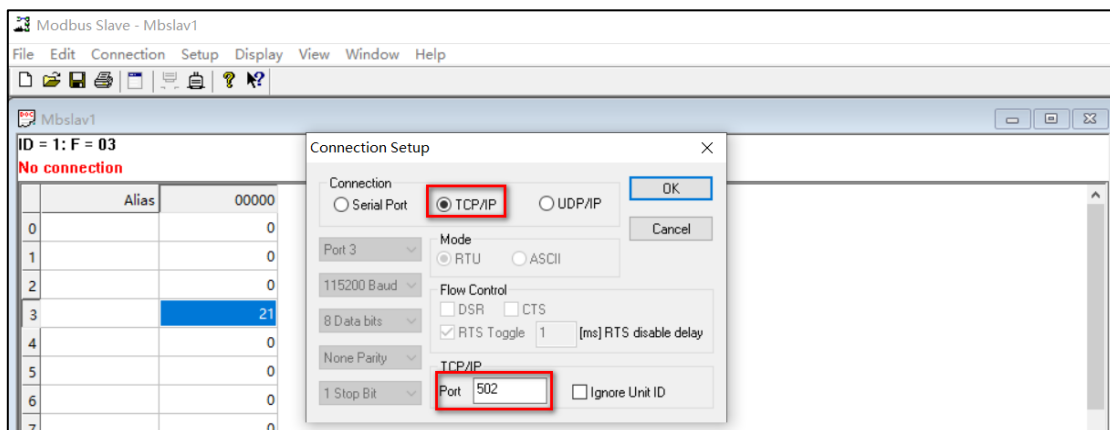
The 6944 as Modbus Master and writes to the register values or coil to Modbus Slave.

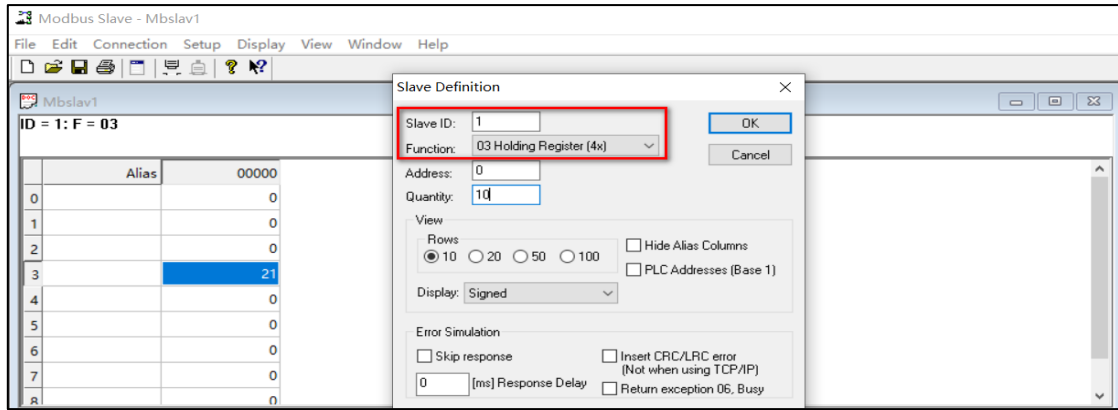
Note: For this Application Note, we will set the Connection Type as “TCP” as an example, which means that the 6944(Modbus Master) will connect to the Modbus Slave and read the value via the Ethernet port. This also works with the Serial Port (RS232/RS485).

Transport via TCP

Configuration of Modbus Slave

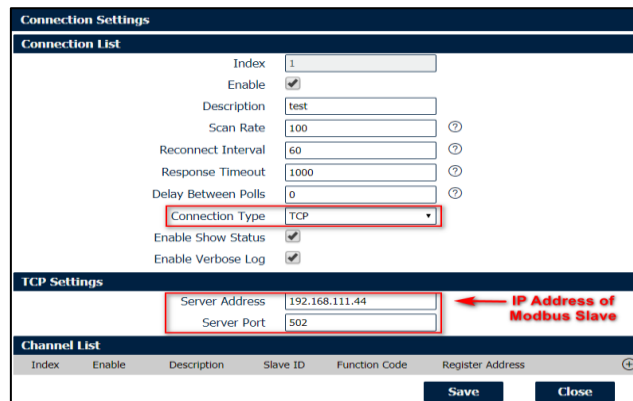
Here we use “Modbus Slave” software to simulate the end device (Modbus Slave device), and the TCP Port: 502, Slave ID: 1, Function Code: 03-Holding-Register, as shown in the image below:





Configuration of the Modbus Poll

Step 1 Go to **Application>Modbus Master>Modbus Poll**, add a “Connection List” and specify the “Connection Type” as “TCP”, specify the “TCP Setting” to connect to the Modbus Slave, like below:



Step 2 Click Save>Apply.

Step 3 Enable “Channel List”, and specify the Slave ID as “1”.

Step 4 Select Function Code as “03-Holding -Register”, Register Address to “3”, then it will poll the value from register address 3 of the Modbus Slave:

Step 5 Click Save>Save>Apply.

(Note: This is a secondary list, it needs to be double clicked to save)

Step 6 Go to **Application>Modbus Master>Status** to check the router has read the value from Modbus Slave successfully.

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

Save Close

Overview

Link Management

Industrial Interface

Network

Applications

DDNS

SMS

Schedule Reboot

GPS

Modbus Master

Modbus Transport

Status

Modbus Poll

Modbus Alarm

Modbus Write

Channel Status

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

Configuring Modbus Transport

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable “Connection List”, and specify the TCP server IP address and port to send the data to the remote TCP server.

Step 2 The Data Format can be defined accordingly or left as default.

Step 3 Enable the “Modbus Channel”, and the Modbus Master will select the value to send to the remote TCP server from Modbus Slave.

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
Enable ☒

2

Connection Index ?

Filter Items

Slave ID ?

Save

Close

Reconnect Interval ?
Connection Timeout ?
Enable Verbose Log ☒

Transport Data Settings

Data Location ?
Data Format ?
Line Break ☒

Modbus Channel

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

1

+

Save

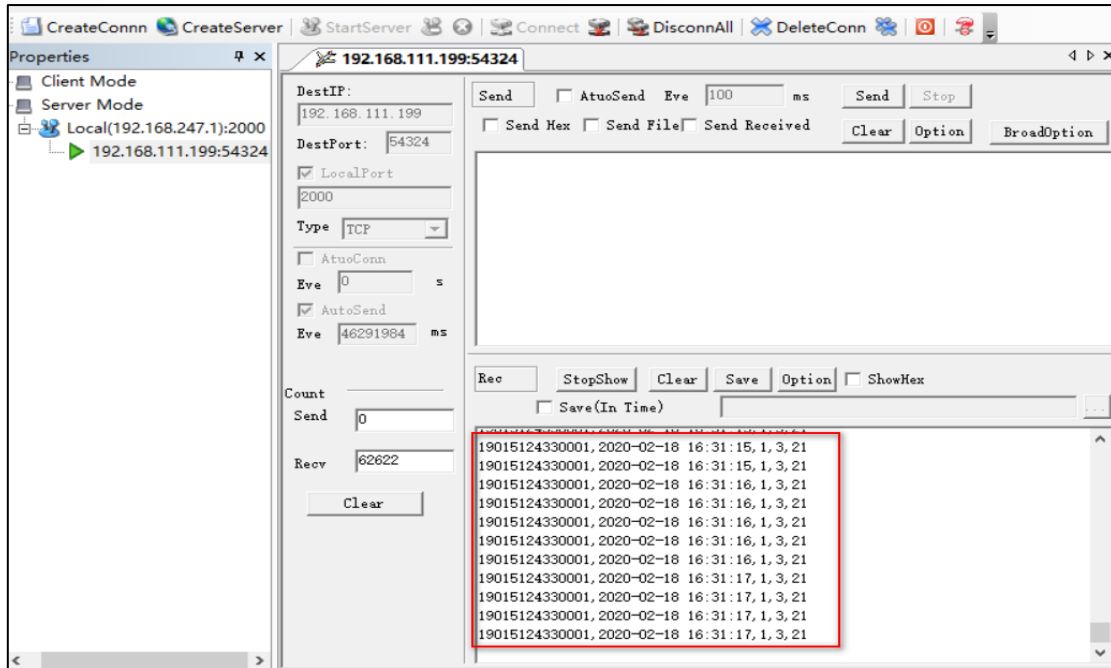
Close

Step 4 Click Save>Save>Apply.

Step 5 Go to **Application>Modbus Transport>Status**, the 6944(Modbus Mater) has connected to the remote server successfully via the TCP protocol.

| <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 |

The remote TCP Server received the data successfully.



Transport via FTP

Please refer to the section on “Configuring the Modbus Slave” and “Configuring the Modbus Poll” to finish the configuration.

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable “Connection List”, and specify the FTP server IP address, port, username and password to send the data to remote FTP server.

Step 2 The File Name and Data Format could be defined accordingly or set it as default.

Step 3 Enable “Modbus Channel”, and the Modbus Master will select the value to send to the remote FTP server from Modbus Slave.

Channel Settings

Modbus Channel

Index: 1

Enable: ☒

Connection Index: 1

Filter Items: Slave ID

Slave ID: 1

Save Close

Try To Send: 3

Enable Verbose Log: ☒

Transport Data Settings

Data Location: NULL

Add CSV File Title: ☒

File Name: \$SERIAL_NUMBER_\$DATE.csv

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

Step 4 Click Save>Save>Apply.

Step 5 Go to **Application>Modbus Transport>Status**, the 6944(Modbus Mater) has connected to the remote server successfully via the FTP protocol.

| 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.

| FTP SERVER FOLDER | | | | |
|--|-----------------|---------------------|------|--|
| 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 | |

Transport via MQTT

Please refer to the “Configuration for the Modbus Slave” and “Configuration of the Modbus Poll” to complete the configuration

Step 1 Go to **Application>Modbus Transport>Modbus Transport**, enable “Connection List”, and specify the MQTT Broker IP address, port, username and password to Publish the Topic with Modbus data to remote MQTT Broker.

Step 2 The Data Format can be defined or left as default.

Step 3 Enable “Modbus Channel”, define the “Topic” to publish to MQTT Broker with Modbus data.

Step 4 Click Save>Save>Apply.

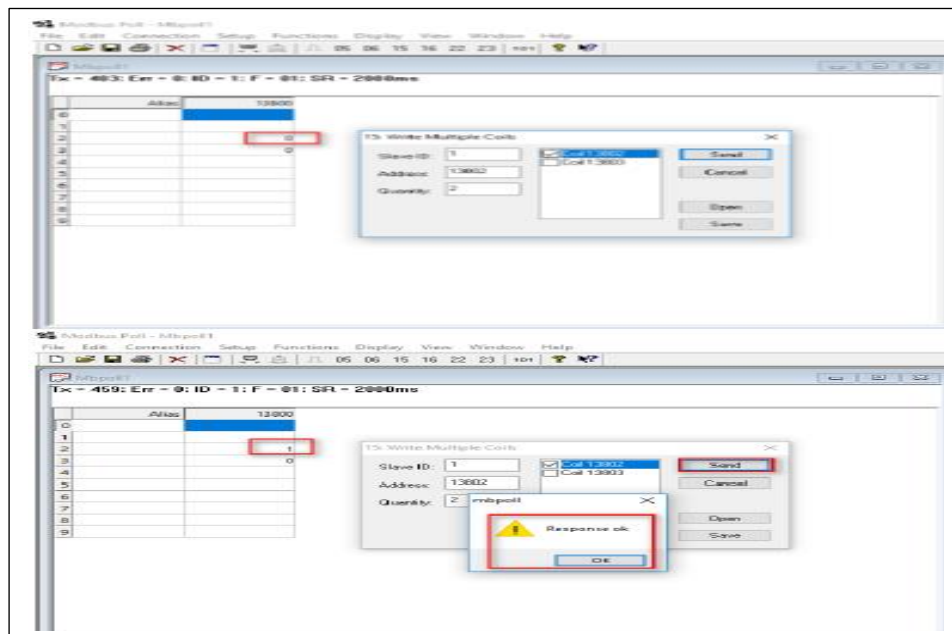
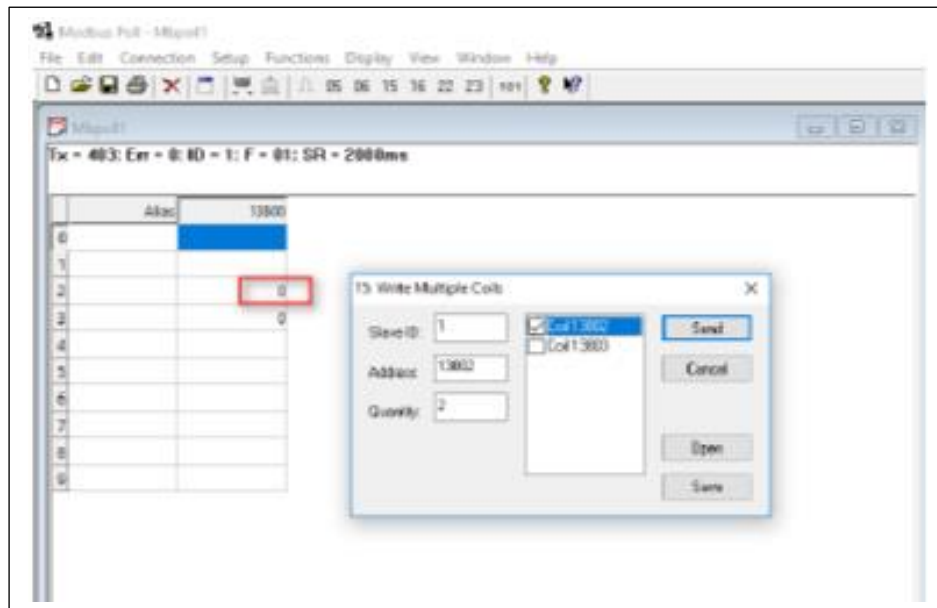
| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

Step 5 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 |

Step 6 Run the MQTT Client (MQTT Subscriber), to subscribe the topic just published to MQTT broker with MODBUS data. Then you should be able to retrieve the MODBUS data successfully.

Step 7 Test Successful



Control Digital Output

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

Test Successful

| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

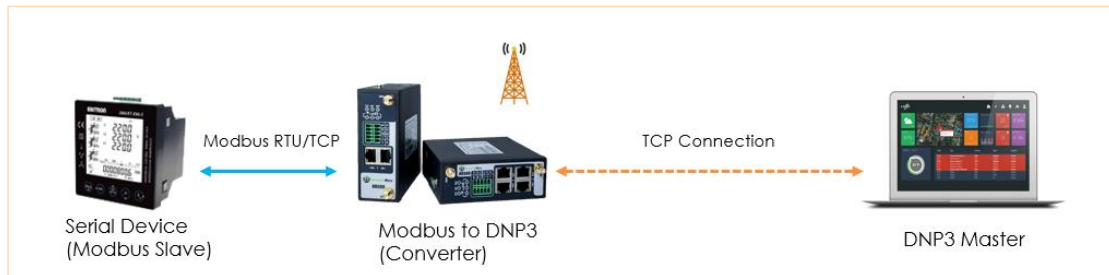
20.3 MODBUS to DNP3

This document contains information regarding the configuration and use of Modbus to DNP3 software on the 6944.

Software versions

| Release Date | Doc. Version | Firmware Version | Additional software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 2020/07/17 | V1.0.0 | V1.1.4(0c0c9fa) | Please contact Case | First released |

Testing Topology



- A 6944 Router runs as a Modbus to DNP3 converter, it acts as a Modbus Master and DNP3 Outstation.
- A serial device supports Modbus protocol and acts as a Modbus Slave. It connects to the 6944 router via its serial port or Ethernet port.
- The 6944 router polls the Modbus data from the end device (Modbus Slave), then sends the data to the remote DNP3 Master.

Configuration

Configuring the 6944

Step 1 Go to **Applications>Modbus To DNP3>Modbus Master**, specify the serial settings to make the router connect to the Modbus Slave via RS232 interface:

The screenshot shows the 'Modbus Master' configuration window. The 'Connection Settings' tab is selected. Under 'Connection List', there is one entry with Index 1, which is enabled. The 'Connection Type' is set to 'RS232'. In the 'Serial Settings' section, the 'Baud Rate' is 115200, 'Parity' is None, 'Data Bits' is 8, and 'Stop Bits' is 1. The 'Channel List' at the bottom is empty.

Step 2 Go to **Applications>Modbus To DNP3>Modbus Master>Channel List**, specify the Modbus Master settings and the DNP3 data type:

Modbus Master DNP3 Outstation

Connection Settings

Connection List

| Index | Enable | Description | Scan Rate | Reconnect Interval | Response Timeout | Delay Between Polls | Connection Type | Enable Show Status | Enable Verbose Log |
|-------|-------------------------------------|-------------|-----------|--------------------|------------------|---------------------|-----------------|-------------------------------------|--------------------------|
| 1 | <input checked="" type="checkbox"/> | | 1000 | 60 | 1000 | 0 | RS232 | <input checked="" type="checkbox"/> | <input type="checkbox"/> |

Serial Settings

Baud Rate: 115200
Parity: None
Data Bits: 8
Stop Bits: 1

Channel List

| Index | Enable | Description | Slave ID | Function Code | Register Address |
|-------|--------|-------------|----------|---------------|------------------|
| | | | | | |

Save Close Save Apply

Channel Settings

Enable: ☒
Description:
Slave ID: 1
Function Code: 03-Holding-Register
Register Address: 0
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

DNP3 Outstation Settings

Data Type: Counter Input
Class: 2
Enable Timestamp: ☒

Save Close

Step 3 Go to **Applications>Modbus To DNP3>DNP3 Outstation**, specify the DNP3 outstation settings as shown below:

Modbus Master DNP3 Outstation

DNP3 Outstation Settings

Enable: ☒
Local IP: 0.0.0.0
Local Port: 20000
Link Address: 1024
Master Link Address: 1
Enable Unsolicited: ☒

Data Settings

Data Location: FLASH
Send Interval: 60
Number of Sent: 5000

Advanced Settings

Server Accept Mode: Close New
Keepalive Timeout: 0
Enable Verbose Log: ☐

Save Apply

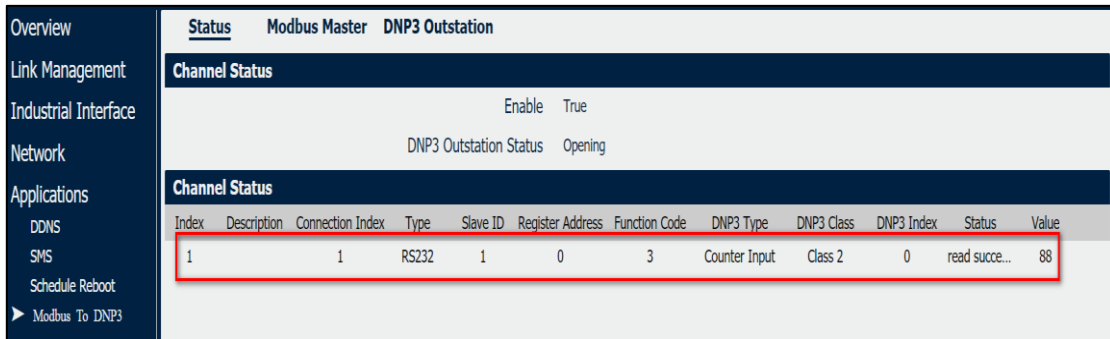
Step 4 Click **Save>Apply**.

Configuration of MODBUS Slave

Step 1 Set Slave ID as “1”; Function Code as “03”, and the value “88” on Register “0”:



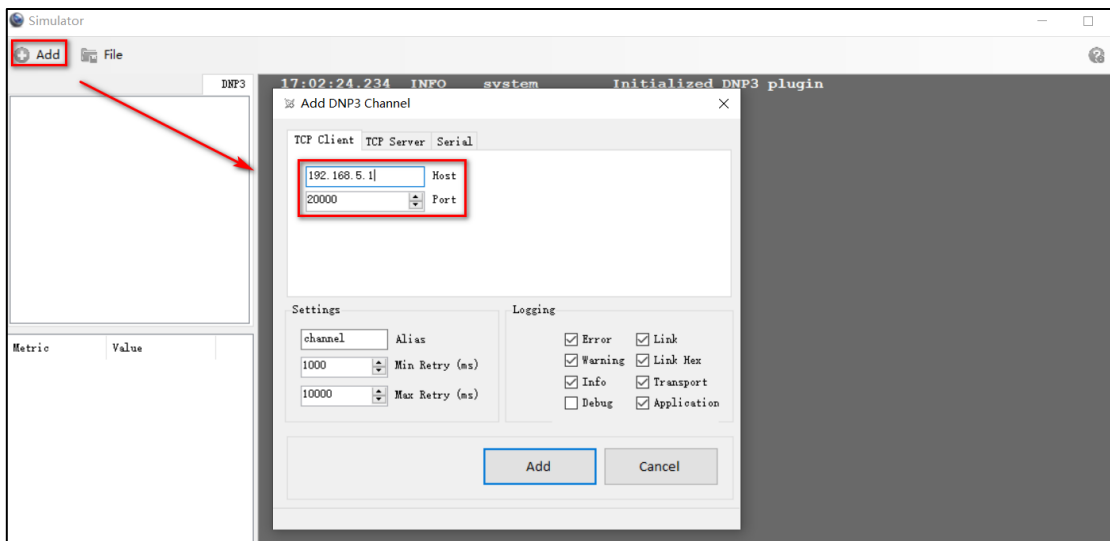
Step 2 Check that the 6944 has polled and retrieved data from the Modbus Slave successfully:



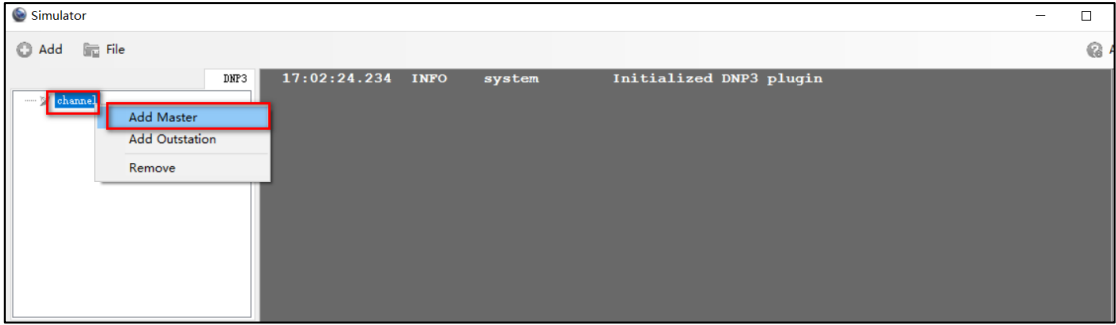
Testing

Use the DNP3 Simulator “OpenDNP3” to do the testing.

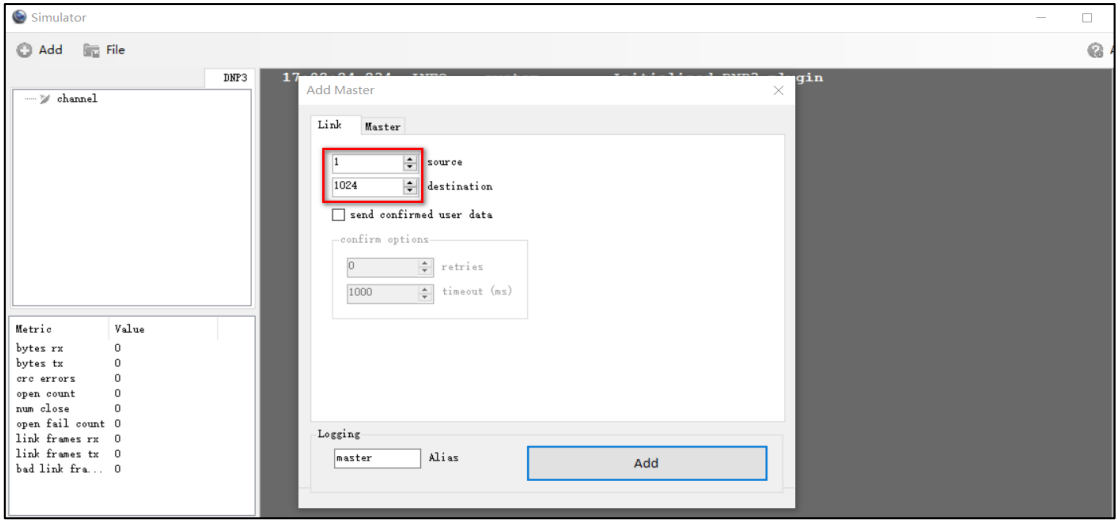
Step 1 Run DNP3 simulator and enter the IP Address and Port to make it connect to the 6944 (DNP3 Outstation):



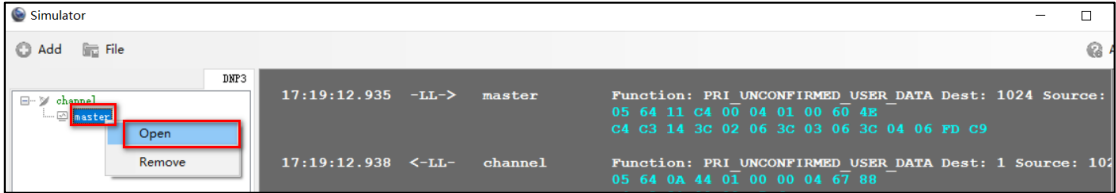
Step 2 Right Click “channel”, and Add Master:



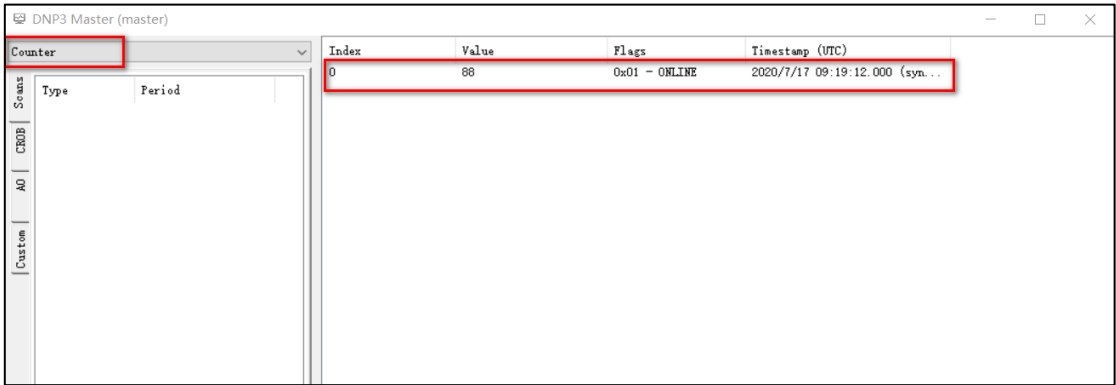
Step 3 Specify the address on the DNP3 Master, to make it match the settings on the 6944 (DNP3 Outstation):



Step 4 Right Click “Master” and open it:



Step 5 Select the data type as “Counter”, then you can see the data has been sent to the DNP3 Master from the 6944(DNP3 Outstation) successfully:



Step 6 Test successful.

| | |
|----------------|-------------|
| Section Twenty | 6944 Manual |
| MODBUS | Rev 2.8 |

20.4 AN053 IEC 101 to IEC 104

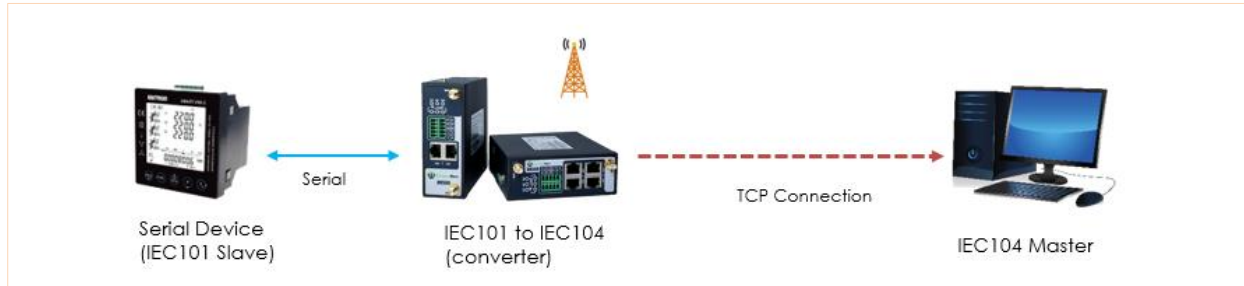
Overview.

This document contains information regarding the configuration and use of IEC101 to IEC104.

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 2020/07/17 | V1.0.0 | V1.1.4(0c0c9fa) | (e9b6cfe) | First released |

Topology



- The 6944 Router runs as an IEC101 to IEC104 converter.
- A serial device supports the IEC101 protocol and acts as slave connected to the 6944 router via a serial port.
- The IEC104 master connects to the 6944 router via TCP and requests data from the slave. After that, the slave will send the data to the master as requested.

Configuration

Configuring the 6944

Step 1 Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC101 configuration, like below:

IEC101 To IEC104 Connection Settings

Index: 1

Enable: ☒

Description:

Enable Verbose Log: ☒

IEC101 COM Settings

COM Type: RS232

Baud Rate: 9600

Data Bits: 8

Stop Bits: 1

Parity: None

IEC101 Settings

Cyclic Interval: 1000

Number Of Retries: 3

Link Address: 1

Link Address Length: 1

Cause Of Transmission Length: 1

Common Address Length: 1

Information Object Address Length: 2

Buttons: Save, Close, Save, Apply

Step 2 Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC104 configuration, as shown below:

Step 3 Click Save>Apply.

Configuring an IEC101 Simulator

Step 1 Specify the serial settings on the IEC101 simulator, and make it the same as the 6944 router serial settings:

Step 2 Specify the simulator works as the Slave Station:

Step 3 Specify the IEC101 Serial Port settings on the IEC101 simulator, to make it the same as the 6944 as shown above.

Step 4 Save and start to connect.

Configuring an IEC104 Simulator

Step 1 Enable the IEC104 simulator and configure it as a Master Station:

Step 2 Specify the settings on the IEC104 simulator, to make all the settings the same as the 6944 IEC104 setting, then connect to the 6944 via a TCP connection:

Step 3 Save and start to connect IEC104 Master to IEC101 Slave:

| IEC101 To IEC104 Status | | | | | | |
|-------------------------|--------|----------|--------------------------|----------------|-------------|--------------------------|
| Index | Enable | COM Type | IEC101 Connection Status | Client IP | Client Port | IEC104 Connection Status |
| 1 | true | RS232 | Connected | 192.168.111.19 | 50548 | Connected |

Step 4 Connected successfully

Testing

IEC104 Master requests data from the IEC101 Slave

IEC104 Master receives data from the IEC101 Slave

This page left blank intentionally

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

21. AT Commands

21.1. AT Over IP

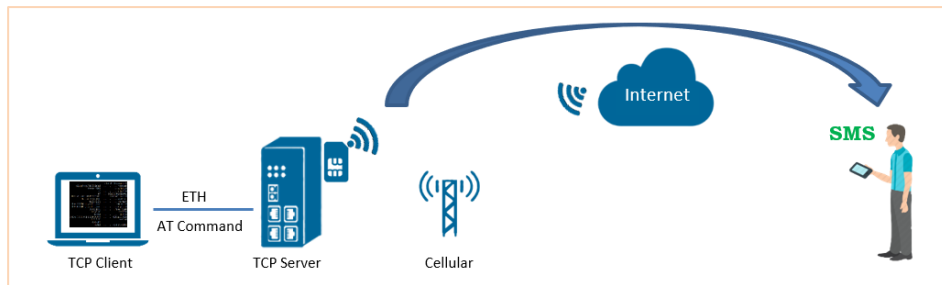
Overview

This document contains information regarding configuring the 6944 to run AT Over IP

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|-------------------|-------------------------------|--------------------|
| 4.7.2019 | V1.1 | V1.1.4 (0c0c09fa) | AT over IP 1.0.1 (42ccf3e) | First release |

Topology



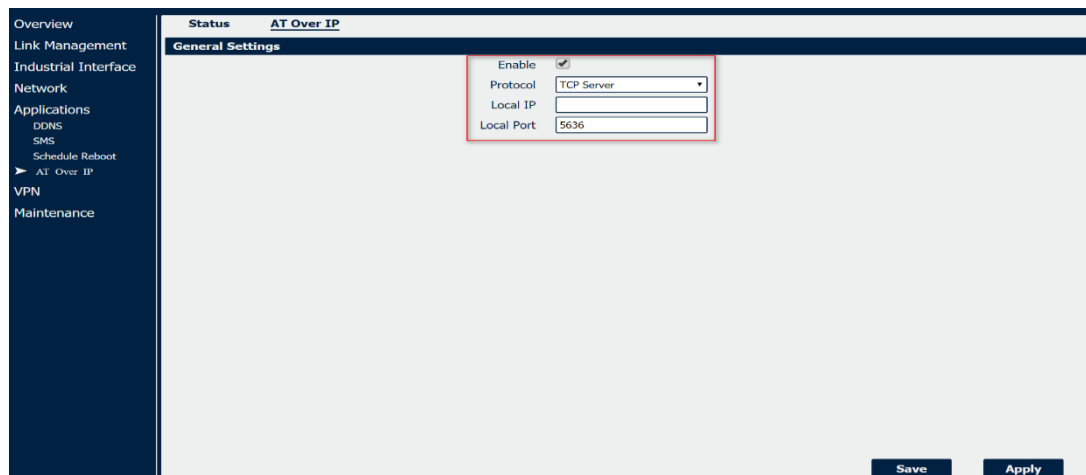
- The 6944 runs as a TCP Server and connects to the Internet via its SIM card.
- The PC runs as a TCP Client and connects to the 6944 via an Ethernet cable.
- The PC sends an AT Command to control the module on the 6944 to take some action.

Note: This application note will show how to use the AT Command via a TCP connection to control the module to send PDU mode SMS message

Configuration

6944 Configuration

Step 1 Go to **Application>AT Over IP**, enable AT Over IP feature like below:



Step 2 Click **Save>Apply**.

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

Testing

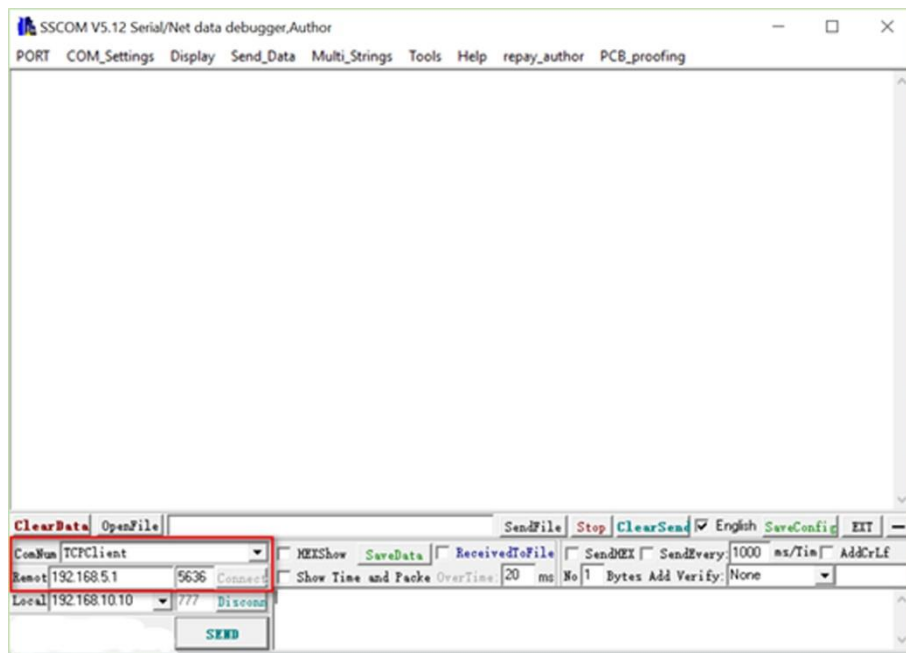
Send the message “TEST” to the mobile phone under PDU mode as an example message.

yy AT Commands and Content that needs to be sent one by one to the router.

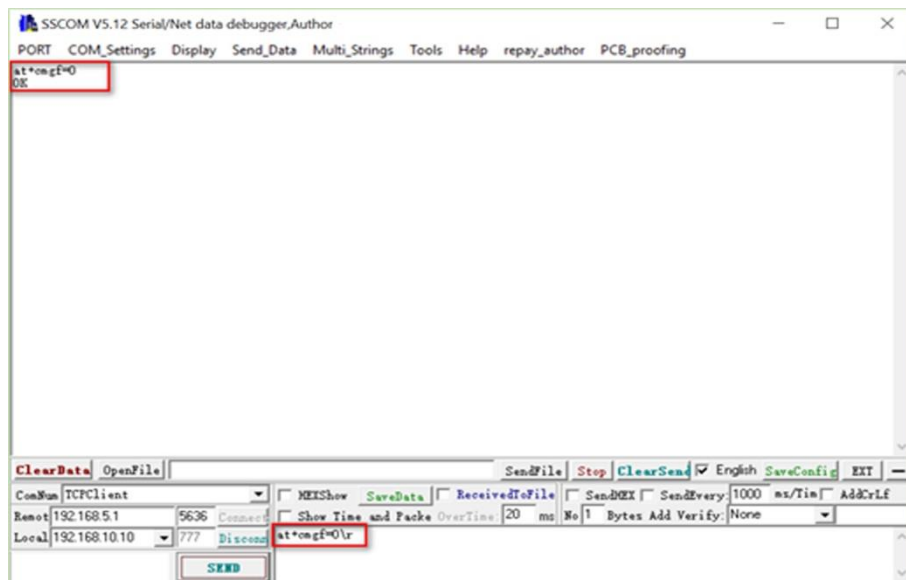
- at+cmgf=0\r
- at+cmgs=17\r
- 0001000BA15119852081F0000004D4E2940A
- 1a

Note: “\r” selects the keyboard “Enter”; Option “c” for the content to be sent under PDU mode; Option “d” is the end code to be sent with HEX.

Step 1 Run SSCOM software as a TCP client and connect the 6944 router (TCP Server), as shown below.

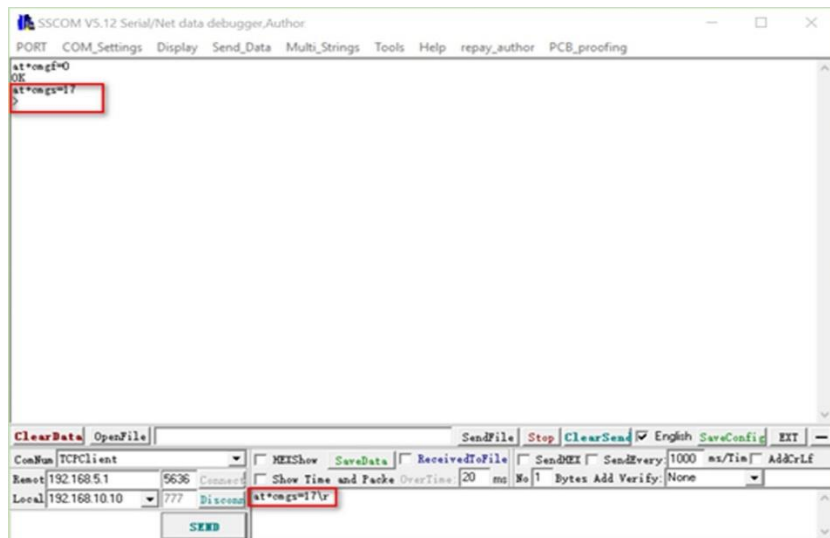


Step 2 Send the AT command “at+cmgf=0\r” to make sure it’s under PDU mode.

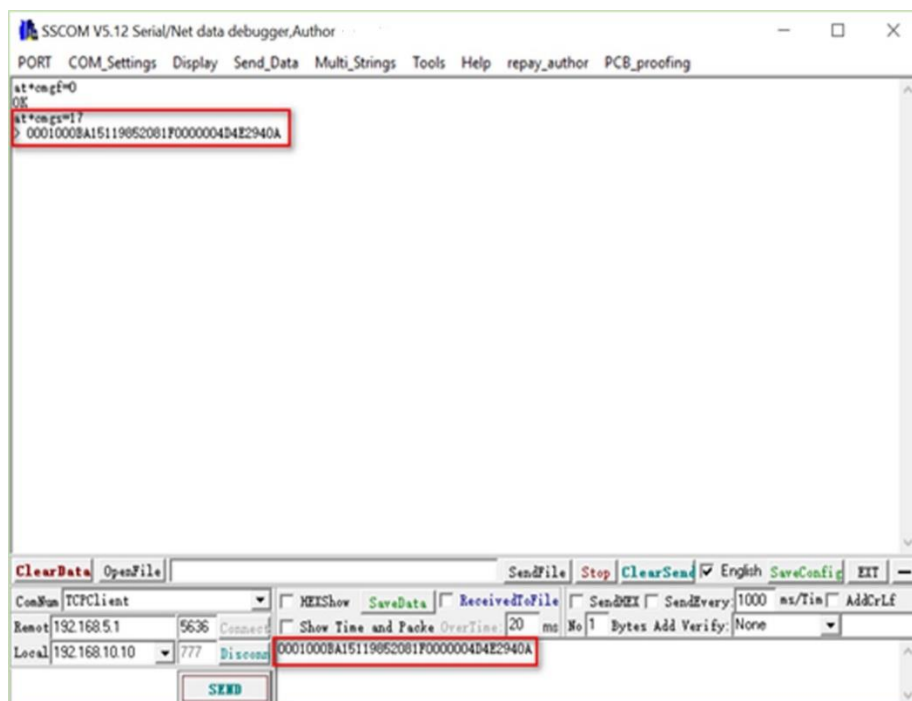


Step 3 Send the AT command “at+cmgs=17\r” to start to sending the content.

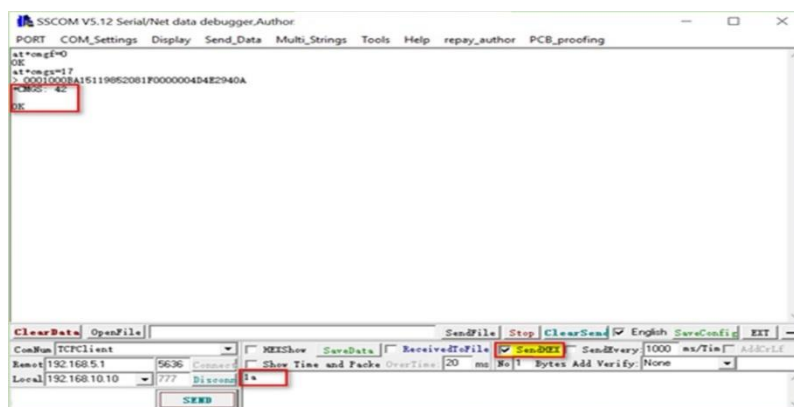
| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |



Step 4 Send the content.

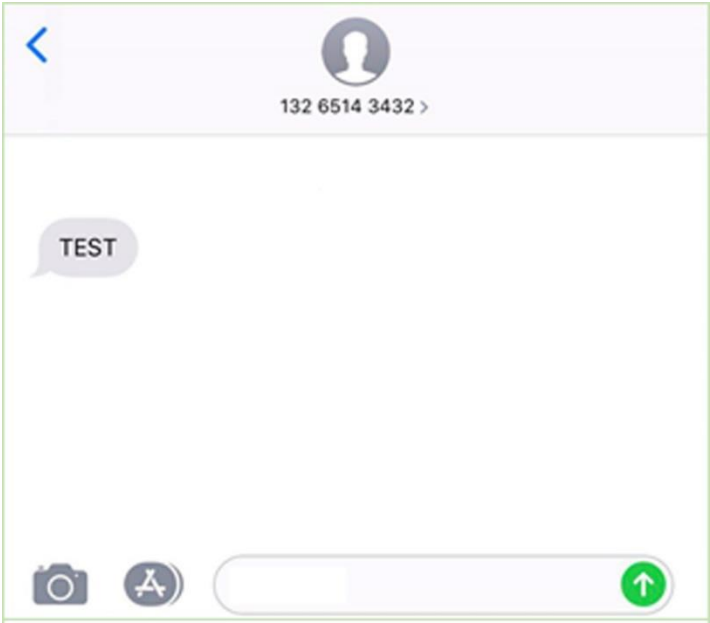


Step 5 Send the ending code “1a” in HEX, if you get the reply “OK” it means the SMS has been successfully sent.



Step 6 Test successful, the mobile phone has received the SMS message.

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |



| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

21.2. AT Over Telnet

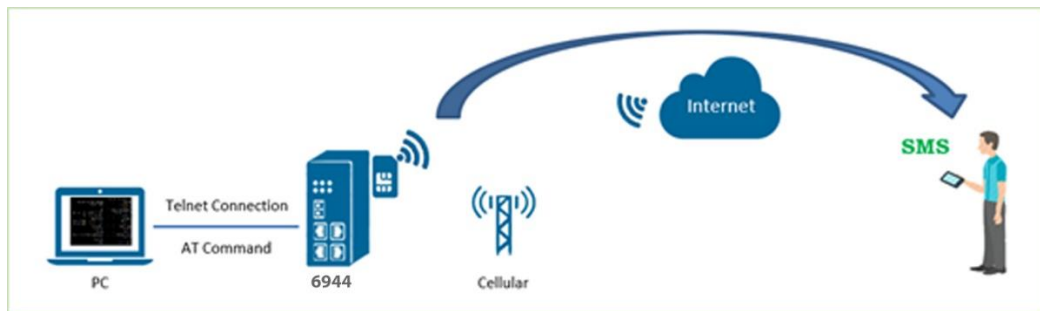
Overview

This document contains information regarding the configuration and use of AT over Telnet.

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 18.7.2019 | V1.1 | V1.1.4 () | 1.0.1 (42ccf3e) | First release |

Testing Topology

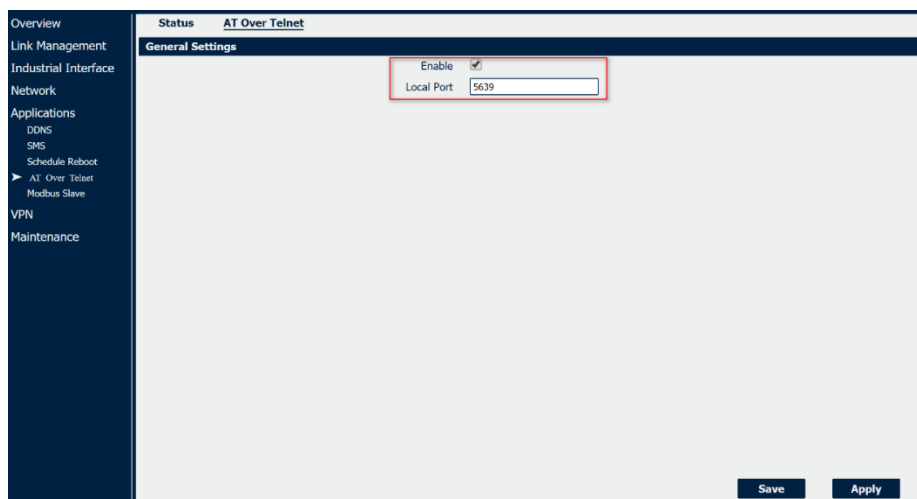


- The 6944 connects to the Internet via its SIM card.
- The PC connect to the 6944 via an ethernet cable using the Telnet protocol.
- The PC sends an AT Command to control the module in the 6944 to undertake an action.

Note: This application note will show how to use the AT Command to control module to send a text mode SMS message.

Configuration

Step 1 Go to **Application>AT Over Telnet**, enable AT Over Telnet feature like below:



Step 2 Click Save>Apply.

Testing

As a test send the content “TEST” to the mobile phone in text mode. We have shown the AT Command required to be sent to the 6944 router, with one command at a time.

```
at+cmgf=1
```

```
at+cmgs="15915802180"
```

```
>TEST
```

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

Note: After entering the content “TEST”, please press the keyboard “Ctrl+z” to send the SMS.

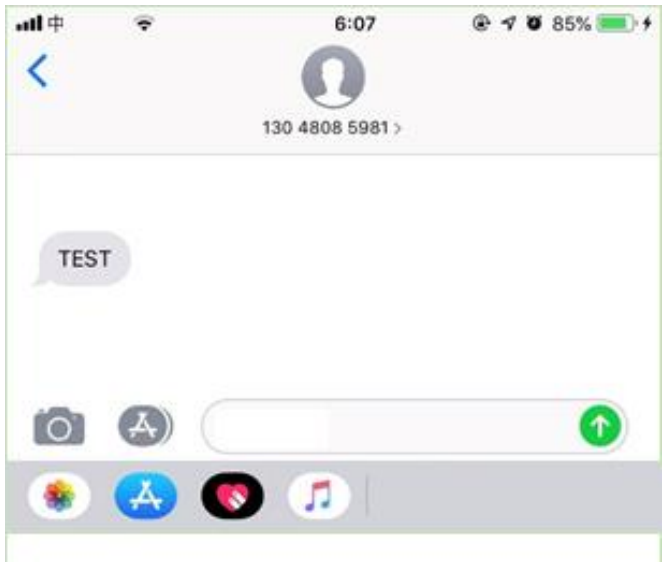
Step 1 Run the “putty” software and telnet to the router, enter the AT command to trigger the 6944 module to send the SMS as shown below:

```

192.168.5.1 – PuTTY
At
ERROR
At
OK
At+cmgf=1
OK
At+cmgs= 078875277882
>TEST
+CMGS: 237
OK

```

Step 2 The Mobile phone receives the SMS with content “TEST”:



Step 3 Test successfully.

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

21.3. AT Over COM

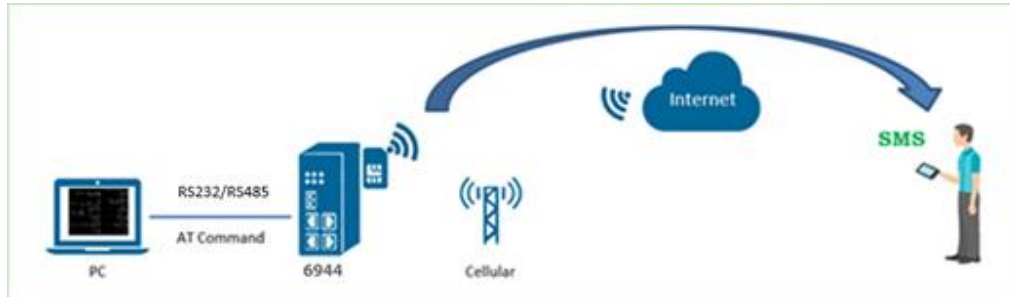
Overview

This document contains information regarding the configuration and use of AT Over Com

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 18.7.2019 | V1.1 | V1.1.4 (0c0c9fa) | 1.0.1 (42ccf3e) | First release |

Testing Topology



- The 6944 connects to the Internet via its SIM card.
- A PC connects to the 6944 via its serial port (RS232 or RS485).
- The PC sends an AT Command to control the 6944 to produce an action.

Note: This application note will show how to send the AT Command via RS232 interface to control the 6944 module to send an SMS message.

Configuration

6944 Configuration

Step 1 Go to **Application>AT Over COM**, enable AT Over COM as shown below

Overview
Link Management
Industrial Interface
Network
Applications
 DNS
 SMS
 Schedule Reboot
 AT Over IP
 ▶ **AT Over COM**
 AT Over Telnet
 Modbus Slave
VPN
Maintenance

Status **AT Over COM**

General Settings

Enable ☒

COM type

Baud Rate

Data Bits

Stop Bits

Parity

Save **Apply**

Step 2 Click **Save>Apply**.

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

Testing

Step 1 Send the content “HELLO” to the mobile phone using text mode to test.

Below is the AT Command and content need to be sent one by one to the router.

a) at+cmgf=1\r

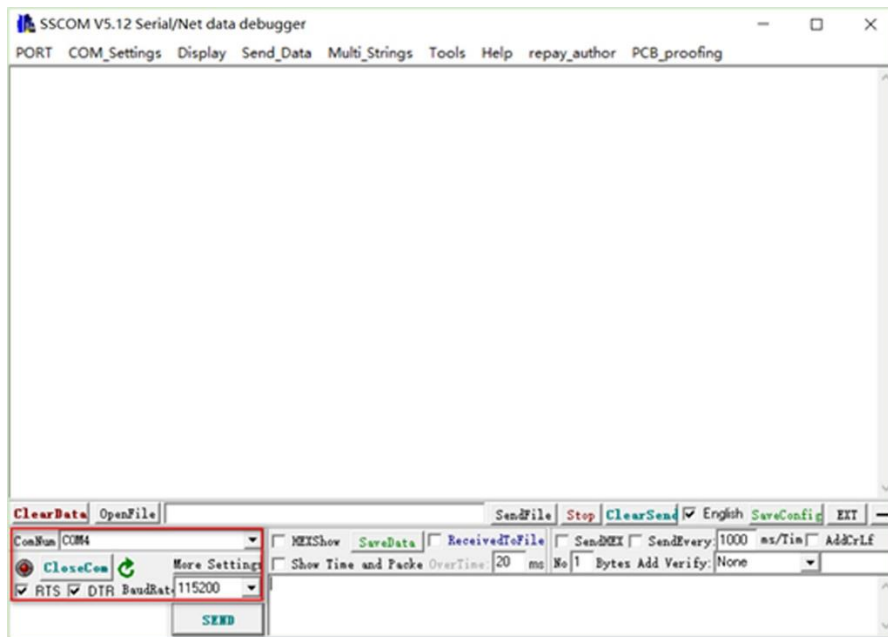
b) at+cmgs=15915802180\r

c) HELLO

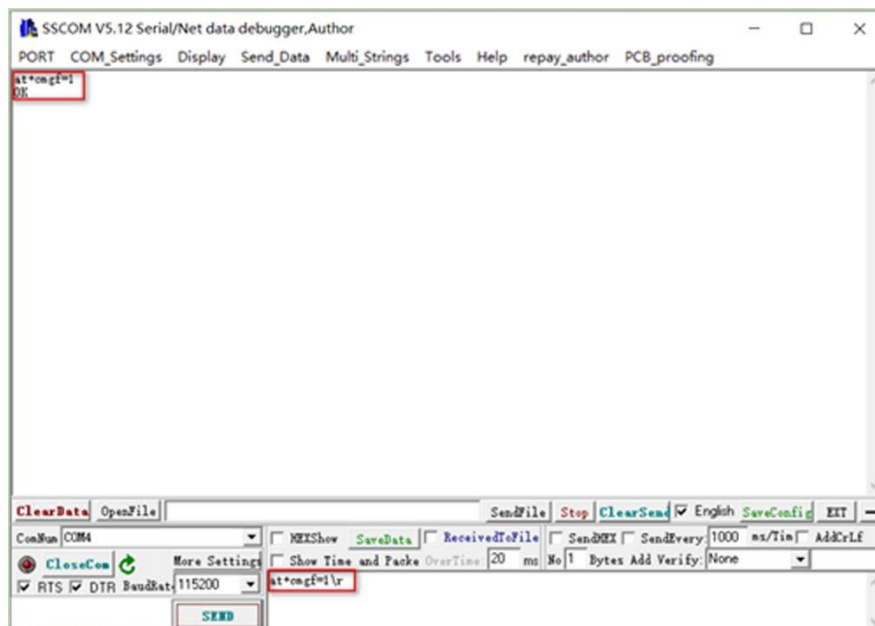
d) 1a

Note: “\r” means the keyboard “Enter”; Option “c” is the content to be sent under text mode; Option “d” is the end code to be sent with HEX.

Step 2 Run SSCOM software and connect the 6944 router via its serial port, as shown below:

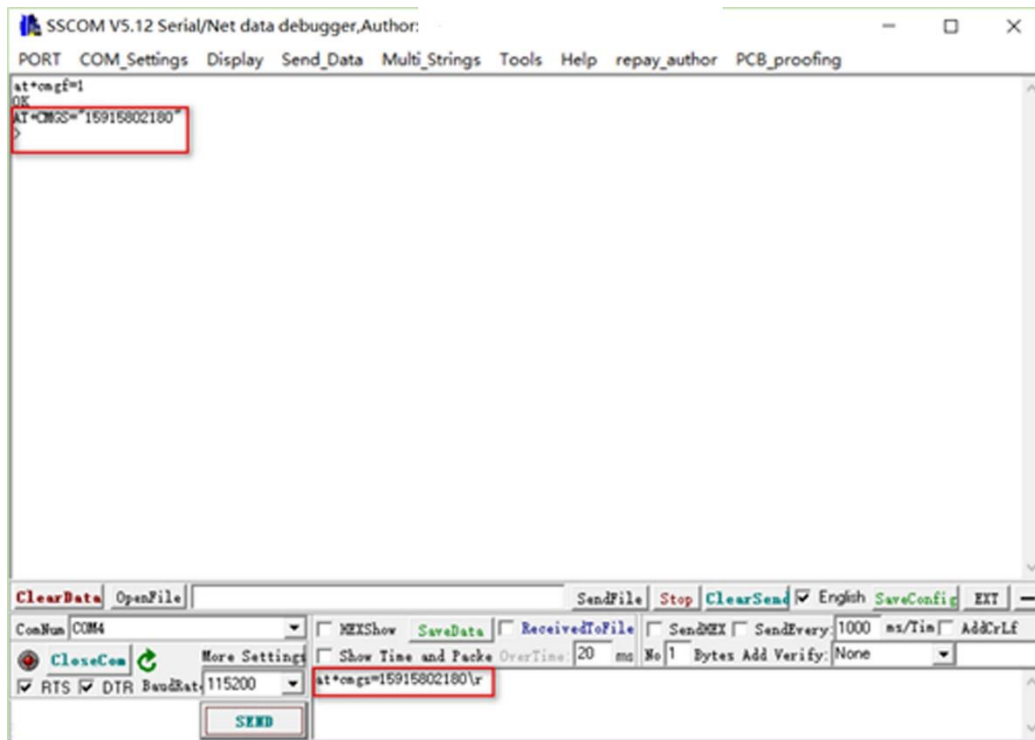


Step 3 Send the AT command “at+cmgf=1\r” in TEXT mode

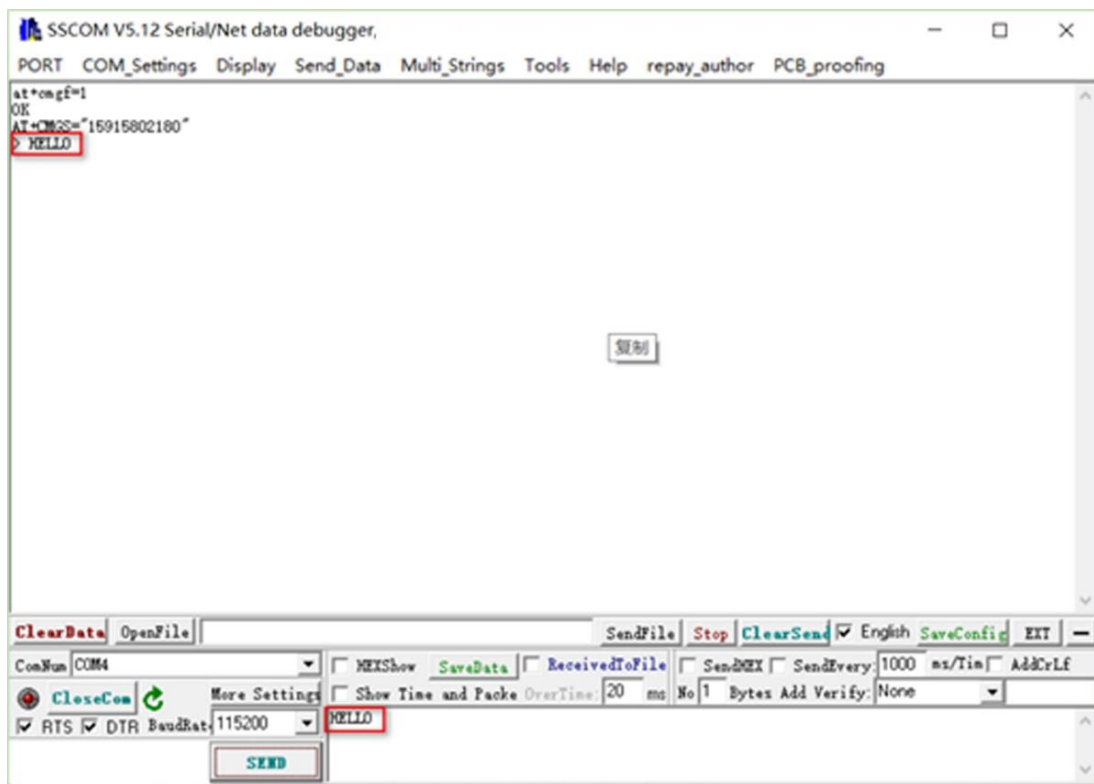


| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |

Step 4 Send the AT command “at+cmgs=15915802180\r” to start to send the content to the designated phone number.

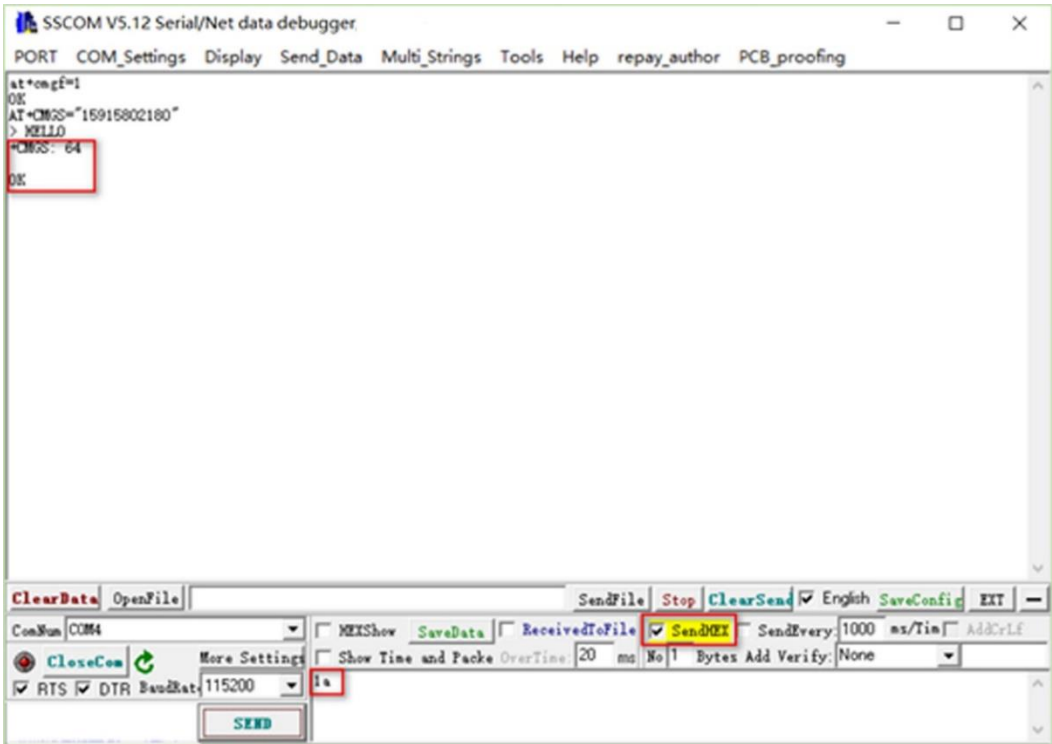


Step 5 Send the message “HELLO”.

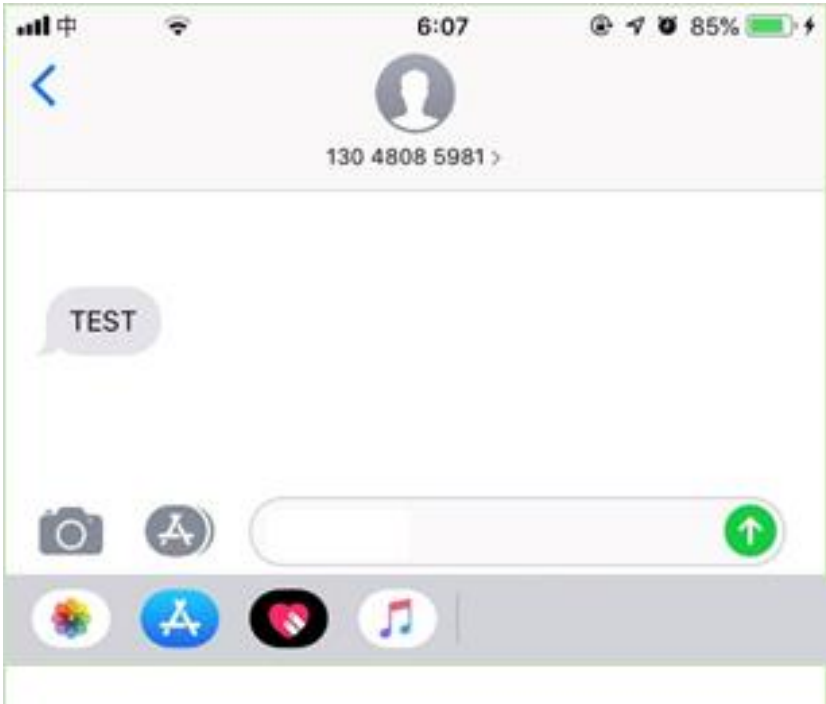


Step 6 Send the ending code “1a” with HEX. The reply “OK” means the SMS was sent successfully.

| | |
|----------------------|-------------|
| Section Twenty - One | 6944 Manual |
| AT Commands | Rev 2.8 |



Step 7 When the test is successful, the mobile phone will receive the SMS message.



| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

22. SMS Commands

SMS allows a user to send an SMS to monitor or control the 6944 router or get the operational status of the router. Using a Text or SMS allows the network manager to use the CLI to control the 6944

Application->SMS

- **Enable** - Select this box to enable SMS feature.
- **Authentication Type** - Specify the authentication mode for SMS, optional for “None” and “Password”.
- **Description** - Enter the description of the Phone Book
- **Phone Number** - Enter the special phone number and only allow this phone number to send an SMS to the 6944 router
The SMS Gateway sends SMS messages by using a valid syntax from the serial device or ethernet device.

Phone Number Settings

Allow Phone Book

| | |
|--------------|---|
| Index | 1 |
| Description | |
| Phone Number | |

Save

Close

Using SMS to control the Digital Input / Output

We can send the SMS message to control the Digital Output ON or OFF. Please kindly check below SMS command

admin\$admin\$doctl\$DO 1/2 ON
admin\$admin\$doctl\$DO 1/2 OFF

"1" means Digital Output 1

"2" means Digital Output 2

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

Application->SMS>Gateway

- **Enable** - Check the box will enable SMS gateway.
- **Authentication Type** - Specify the authentication mode for SMS, optional for “None” and “Password”.
- **SMS Source** - Specify SMS source to receive valid syntax, optional for “Serial Port” and “HTTP(S) GET/POST”.
- **Serial Port** - Select the serial port from COM1 or COM2.
- **Baud Rate** - Select the serial port baud rate. Supported values are 300, 600, 1200, 2400, 4800, 9600, 19200, 38400, 57600, or 115200.
- **Data Bits** - Select the values from 7 or 8.
- **Stop Bits** - Select the values from 1 or 2.
- **Parity** - Select values from none, even, odd.

SMS Notification feature allow to send SMS notification to the pre-setting phone number when some of router status changed.

| Notification Channel Settings | |
|----------------------------------|--------------------------|
| Index | 1 |
| Description | |
| Phone Number | |
| Startup Notify | <input type="checkbox"/> |
| Reboot Notify | <input type="checkbox"/> |
| NTP Update Notify | <input type="checkbox"/> |
| LAN Port Status Notify | <input type="checkbox"/> |
| WAN Port Status Notify | <input type="checkbox"/> |
| WWAN Port Status Notify | <input type="checkbox"/> |
| Active Link Status Notify | <input type="checkbox"/> |
| Digital Input Status Notify | <input type="checkbox"/> |
| Digital Output Status Notify | <input type="checkbox"/> |
| IPSec Connection Status Notify | <input type="checkbox"/> |
| Openvpn Connection Status Notify | <input type="checkbox"/> |

Save
Close

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

Application->SMS>Notification

- Index - **Display the index of the notification channel, maximum is 10.**
- Description - **Add the description for notification channel.**
- Phone Number - **Pre-setting phone number to receive the notification**
- Startup Notify - **Send SMS notification to the pre-setting phone number when system startup.**
- Reboot Notify - **Send SMS notification to the pre-setting phone number when system reboot.**
- NTP Update Notify - **Send SMS notification to the pre-setting phone number when NTP update successfully.**
- LAN Port Status Notify - **Send SMS notification to the pre-setting phone number when LAN port status changed.**
- WAN Port Status Notify - **Send SMS notification to the pre-setting phone number when WAN port status changed.**
- WWAN Port Status Notify - **Send SMS notification to the pre-setting phone number when WWAN port status changed.**
- Active Link Status Notify - **Send SMS notification to the pre-setting phone number when active link status changed.**
- Digital Input Status Notify - **Send SMS notification to the pre-setting phone number when DI status changed.**
- Digital Output Status Notify - **Send SMS notification to the pre-setting phone number when DO status changed.**
- IPSec Connection Status Notify - **Send SMS notification to the pre-setting phone number when IPSec connection status changed.**
- OpenVPN Connection Status Notify - **Send SMS notification to the pre-setting phone number when OpenVPN Connection Status changed.**

Schedule Reboot

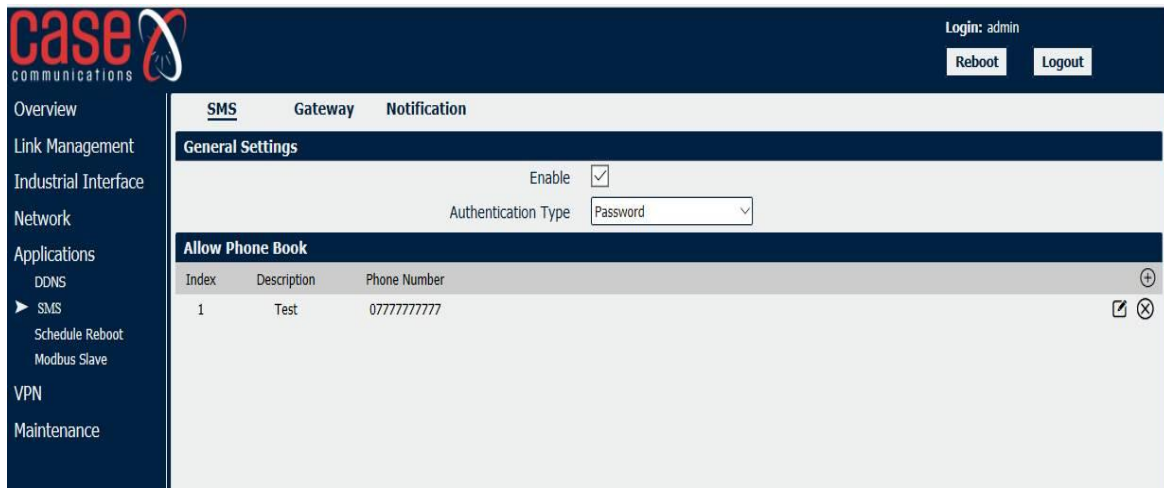
Schedule reboot allows the user to define a time for 6944 router reboot itself.

Application->Schedule Reboot

- **Enable** - Select this box to enable schedule reboot feature.
- **Time to Reboot** - Enter the time of each day to reboot device. Format: HH (00-23): MM (00-59).
- **Day to Reboot** - Enter the day of each month to reboot device. 0 means every day.

Sending SMS commands to control the 6944

It's possible to monitor and send commands to the 6944 Router using an SMS / text messages. To do this it's necessary to send commands using the CLI on the 6944 (Command Line Interface). Go to the Applications SMS. By default the SMS Control Function is enabled.



Under General Settings are the following options:

User Name and Password: Forces the manager to enter a user name and password (recommended)

User Name and Password: None – allows the manager to connect without using a user name and password.

Allow Phone Book: This option only allows the 6944 to send and receive SMS messages from numbers in its internal directory.

SMS Commands

Authentication Type: Password

1. Admin\$admin\$enable\$version // send an SMS to check the firmware version

- The first “admin” means the router username;
- The second “admin” means the router password;
- “Enable” means to send the CLI Command used in “enable mode”.
- “version” is the CLI command under enable mode

2. Admin\$admin\$config\$set syslog level info // send SMS to set router syslog to info level

- The first “admin” means the router username;
- The second “admin” means the router password;
- “Config” means to send the CLI Command of “config mode”.
- “set syslog level info” is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, like below:

1. admin\$admin\$enable\$version;show active link //

- Send SMS to check firmware version and link information together.

2. admin\$admin\$config\$set syslog location ram;set syslog level info //

- Send SMS to set syslog location and syslog level.

3. admin\$admin\$enable\$reboot

- This option reboots the 6944

Authentication Type: None (i.e. only using the 6944 telephone directory for security)

1. enable\$version

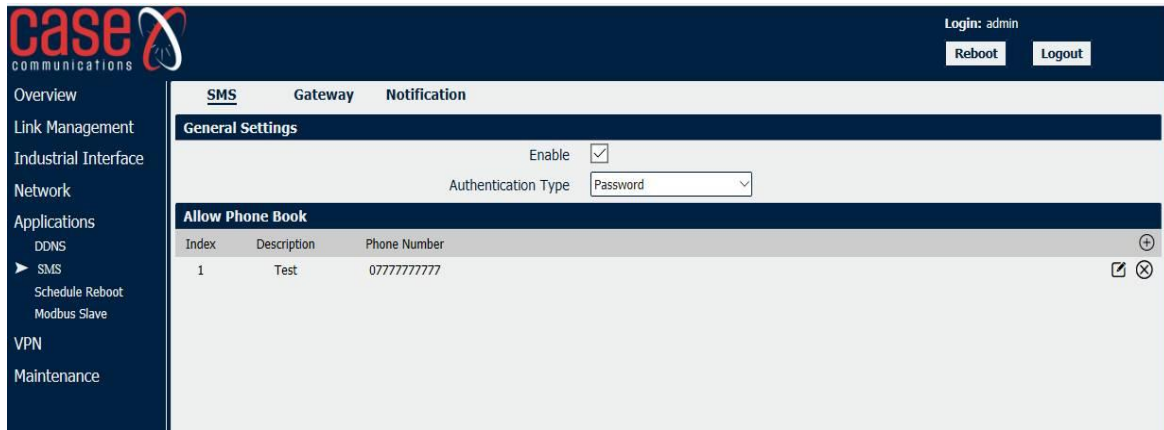
2. config\$set syslog level info

3. enable\$version;show active_link

4. config\$set syslog location ram;set syslog level info

22.1. SMS Control

Go to the Applications SMS. By default the SMS Control Function is enabled.



Under General Settings you have the following options:

User Name and Password: Force the manager to enter a user name and password (recommended)

User Name and Password: None – allows the manager to connect without using a user name and password.

Allow Phone Book: This option only allows the 6944 to send and receive SMS messages from numbers in its internal directory.

SMS Commands

Authentication Type: Password

1. admin\$admin\$enable\$version // send an SMS to check the firmware version

- The first “admin” means the router username;
- The second “admin” means the router password;
- “enable” means to send the CLI Command used in “enable mode”.
- “version” is the CLI command under enable mode

2. admin\$admin\$config\$set syslog level info // send SMS to set router syslog to info level

- The first “admin” means the router username;
- The second “admin” means the router password;
- “config” means to send the CLI Command of “config mode”.
- “set syslog level info” is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, as shown below

admin\$admin\$enable\$version;show active_link //

- send SMS to check firmware version and link information together.
admin\$admin\$config\$set syslog location ram;set syslog level info //
- send SMS to set syslog location and syslog level.
admin\$admin\$enable\$reboot
- This option reboots the 6944

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

Authentication Type: None (i.e. only using the 6944 telephone directory for security)

1. enable\$version
2. config\$set syslog level info
3. enable\$version;show active_link
4. config\$set syslog location ram;set syslog level info

CLI Command

Step 1: Telnet to the router to check the CLI command under “enable mode” or “config mode”.

6944.router login: admin

```
> ← Enable Mode (You are now in enable mode)
>
< Config
config# ← You're now in configuration mode
config#
```

Step 2 When you have connected to the router using telnet, it pops up with the character

“>”,

This means that the router is now in “enable mode” and you can then go into configure mode

Step 3 Using the CLI Command enter “config”, then the router will go into “config mode”

Step 4 Enter the “?” or keyboard “Tab”, then we can see the command options using the CLI as shown below

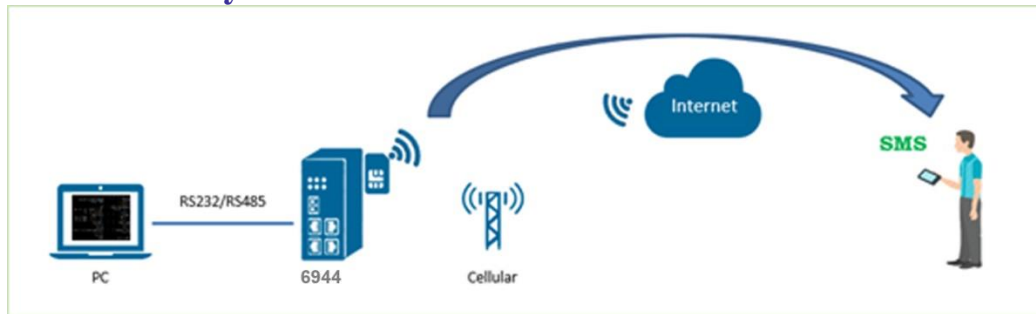
>

| | |
|-------------------|--|
| config | Change to the configuration mode |
| exit | Exit this CLI Session |
| help | Display and Overview of the options available using CLI syntax |
| ping | Send a Ping to a device |
| reboot | Reboot the 6944 router |
| show | Show the running configuration or running status |
| telnet | Telnet to a client |
| traceroute | Traceroute |
| upgrade | Upgrade the firmware |
| version | Display the 6944's current version of software |

Step 5 For example to reboot the 6944 enter (admin\$admin\$enable\$reboot)



22.2 SMS Gateway



- The 6944 connects to Internet via its SIM card.
- The PC connects to the 6944 via a serial port (RS232 or RS485).
- The PC sends the special command via its serial port to the 6944 and triggers the 6944 to send the SMS to the receiver.

Note: This Application Note will show the example when the router receives the special command from the RS232 Port. This can also work on the RS485 Port.

6944 Configuration

Step 1 Go to **Application>SMS>Gateway**, enable SMS Gateway feature like below:

| Overview | SMS | Gateway | Notification |
|----------------------|--|-------------------------------------|--------------|
| Link Management | General Settings | | |
| Industrial Interface | Enable <input checked="" type="checkbox"/> | | |
| Network | Authentication Type <input type="text" value="Password"/> | | |
| Applications | SMS Source <input type="text" value="Serial Port"/> | | |
| DDNS | Serial Port Settings | | |
| ► SMS | Serial Port | <input type="text" value="COM2"/> | |
| Schedule Reboot | Baud Rate | <input type="text" value="115200"/> | |
| GPS | Data Bits | <input type="text" value="8"/> | |
| SNMP | Stop Bits | <input type="text" value="1"/> | |
| DMPC | Parity | <input type="text" value="None"/> | |
| VPN | <input type="button" value="Save"/> <input type="button" value="Apply"/> | | |
| Maintenance | | | |

Step 2: Click Save>Apply.

Testing

Send a message (in our example it is “**hello**”) to the mobile phone.

Here are the commands that needs to be sent to the router via RS232 Port.

a) `sms_send&admin&admin&15915802180&Text_To_Send`

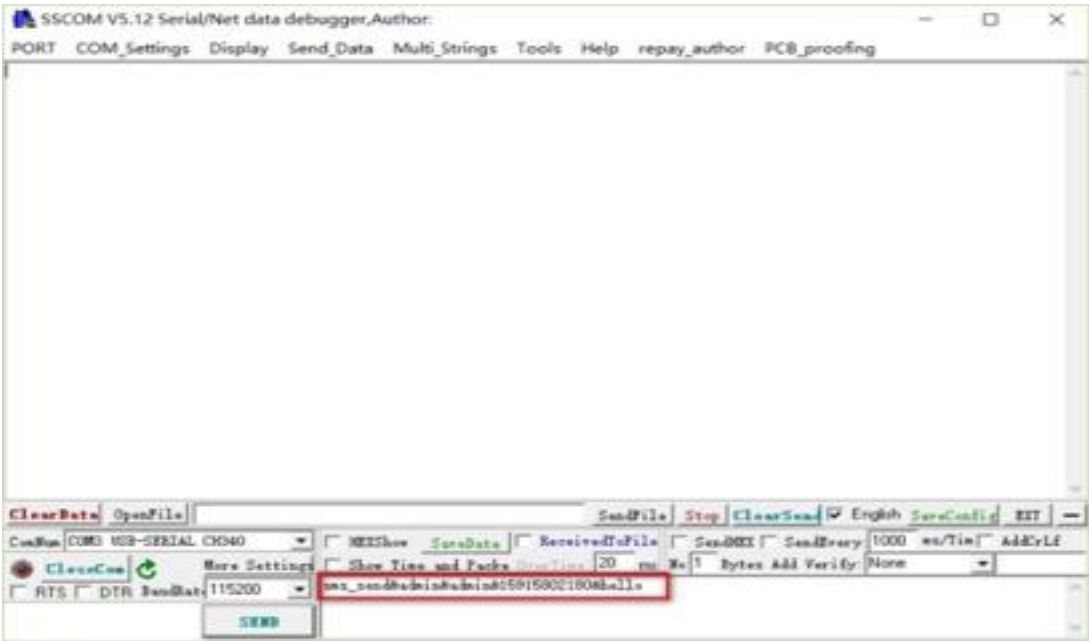
b) `1a` // it is the ending code and need to be sent with “HEX”

Here is the explanation of the command “a”:

`sms_send&username&password &phone number&SMS content`

Step 1 Run the SSCOM software and connect the 6944 router via serial port, as below:

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

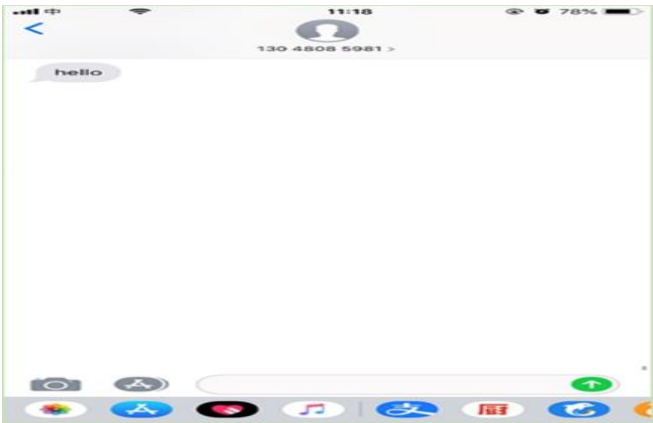


Step 2 Send the SMS with the content “**hello**” to a receiver phone number for example. **15915802180**”.

Step 3 Send the ending code “**1a**” with “**HEX**”:



Step 4. If the test is successful, the mobile phone will receive the SMS message.



22.3 SMS Notification

Overview

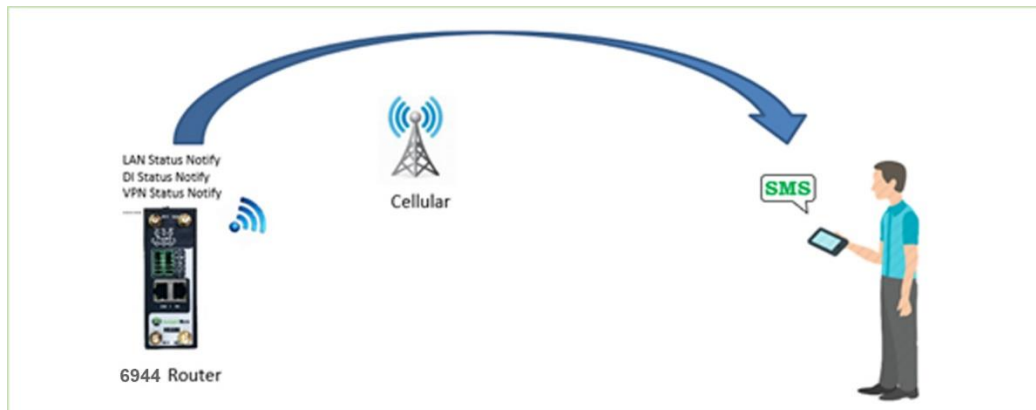
This document contains information regarding configuring the SMS Notification from the 6944 to a mobile device.

Software Version

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

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 3.9.2020 | V1.1 | V1.1.4 | Std Software | First release |

Topology



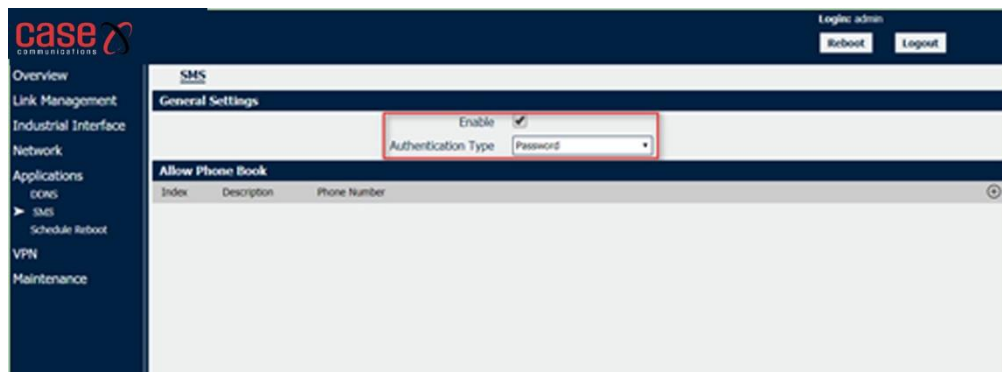
- The 6944 router connects to the Internet successfully via its SIM card.
- An engineer sends the SMS to the router with a Special SMS Command to control the 6944 router restart or configure the 6944 router.

Note:

Special SMS Command means the router CLI Command. The engineer will send SMS message with the CLI Command to control or monitor the router.

6944 Router Configuration

Step 1. Go to **Applications>SMS**, SMS control (the function) is enabled by default.



Authentication Type:

Password: SMS command with router username and password

None: SMS command without router username and password

Allow Phone Book:

The router only receives the SMS message from phone numbers listed in the phone book

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

SMS Command

Authentication Type: Password

1. **admin\$admin\$enable\$version** // send SMS to check the firmware version

The first “admin” means the router username; the second “admin” means the router password; “enable” means to send the CLI Command of “enable mode”. “Version” is the CLI command under enable mode

2. **admin\$admin\$config\$set syslog level info** //send SMS to set router syslog to info level

The first “admin” means the router username; the second “admin” means the router password; “config” means to send the CLI Command of “config mode”. “Set syslog level info” is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, like below:

1. **admin\$admin\$enable\$version;show active_link** //send SMS to check firmware version and link information together.

2. **admin\$admin\$config\$set syslog location ram;set syslog level info** // send SMS to set syslog location and syslog level.

Authentication Type: None

1. **enable\$version**

2. **config\$set syslog level info**

3. **enable\$version;show active_link**

4. **config\$set syslog location ram;set syslog level info**

CLI Command

Step 1 Telnet to the router to check the CLI command under “enable mode” or “config mode”.

```

casecomms router login: admin n
Password:
> ← Enable Mode
>
> config
config # ← Config Mode
config #
config #

```

When you have connected to the router using telnet the following prompt appears “>”, this means that the router is in “enable mode”

When you enter the CLI command “config”, then the router will go into “config mode”

Step 2 Enter the “?” or keyboard “Tab”, then we can see CLI commands as shown below:

| | |
|----------------------|-------------|
| Section Twenty - Two | 6944 Manual |
| SMS Commands | Rev 2.8 |

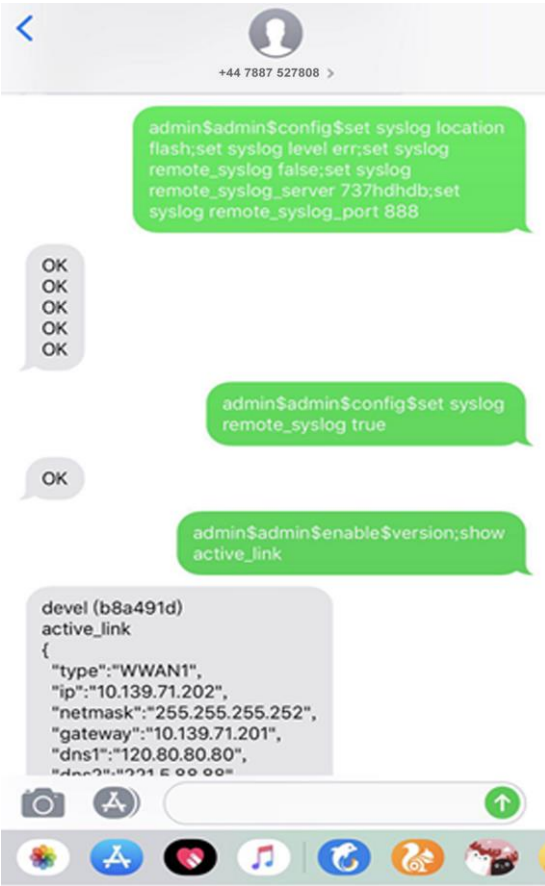
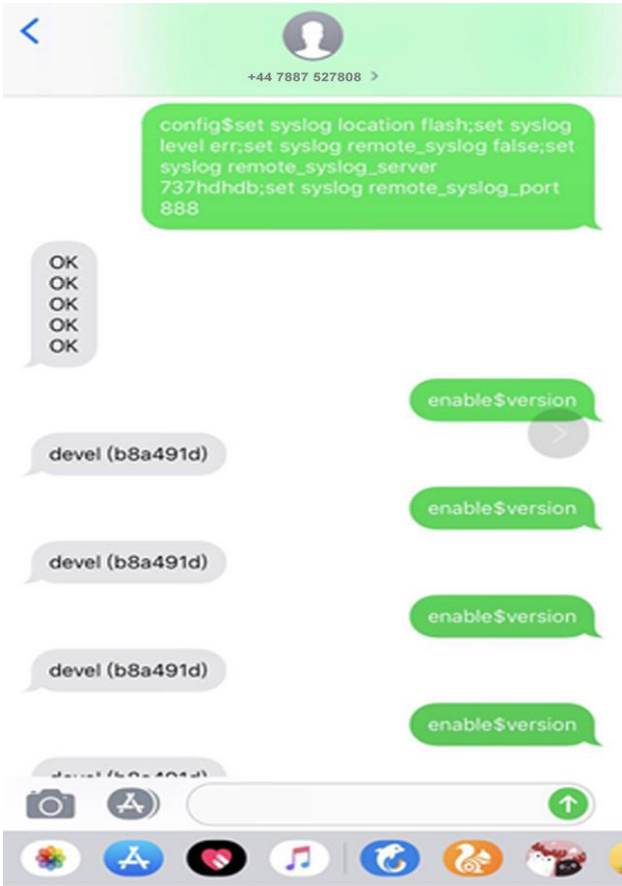
```

>
config      Change to the configuration mode
exit        Exit this CLI session
help        Display an overview of the CLI syntax
ping        Ping
reboot      Reboot system
show        Show running configuration or running status
telnet      Telnet Client
traceroute  TraceRoute
upgrade     Upgrade firmware
version     Show firmware version
>

```

Testing

Step 1: Below test result for reference.

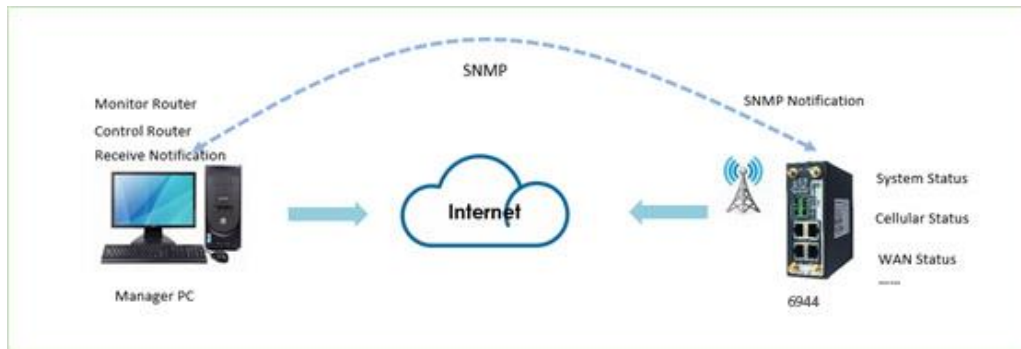


This page left blank intentionally

| | |
|------------------------|-------------|
| Section Twenty - Three | 6944 Manual |
| SNMP | Rev 2.8 |

23. SNMP

23.1. Testing Topology



Criteria of the SNMP test

- The 6944 Manager PC can access the 6944 router using SNMP Protocol.
- The Manager PC can obtain the 6944 operational status, and control the 6944 router and receive SNMP notifications from 6944 router.

Note: For this Application Note, the Intranet was used to test the SNMP instead of the Cellular WAN. The 6944 Manager PC is connected to the LAN port of 6944. The IP address of Manager PC is set to: 192.168.5.19 / 24. The IP address of 6944 LAN port is: 192.168.5.1 / 24.

Software Compatibility

| Release Date | Doc. Version | Firmware Version | Additional Software | Change Description |
|--------------|--------------|------------------|---------------------|--------------------|
| 4.3.2020 | V1.0 | V1.1.4 | V1.1.3(e335ec6) | First release |

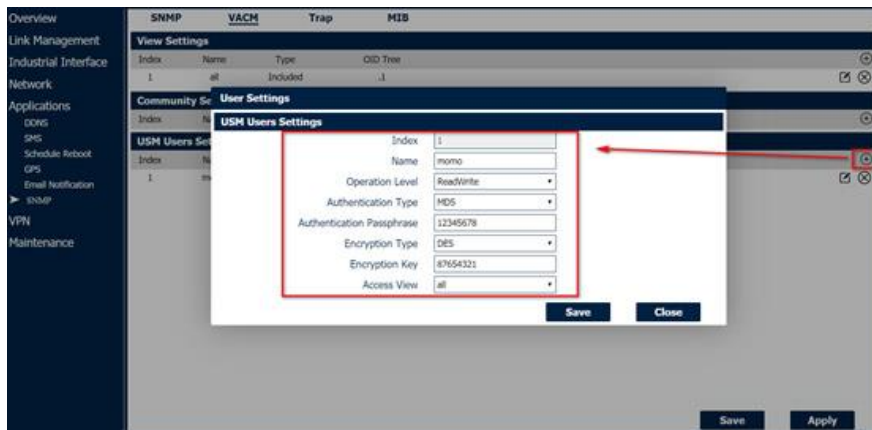
Configuration

Configuration of the 6944 Router

Step 1 Go to **Applications>SNMP>SNMP**, enable SNMP and set the configuration as below:

Step 2 Click **Save>Apply**.

Step 3 Go to **Applications>SNMP>VACM**, Set the configuration in “**View Settings**” to default. For “**USM Users Settings**”, please configure the page as shown below:



Step 4 Click ‘Save > Apply’

Step 5. Go to “**Applications>SNMP>Trap**”, enable SNMP Trap configuration, and the “Notification Host” should be the IP address of the PC running the SNMP management tool, as shown below.



Step 6. Then set the “LAN Notify” as an example, when the LAN Port status is changed, the SNMP management tool will receive the event alarm.

Go to “**Applications>SNMP>Trap>Events Settings**”, configuration as shown below.

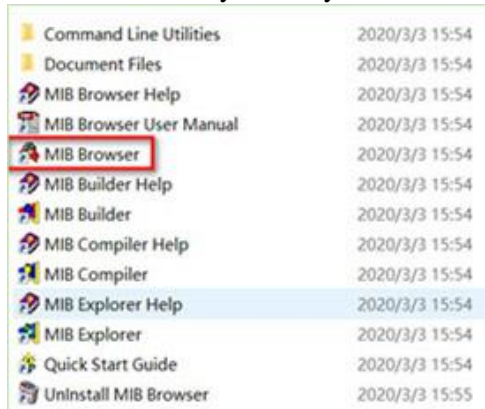


Step 8 Click Save>Apply

23.2. Configuring an SNMP Management Tool

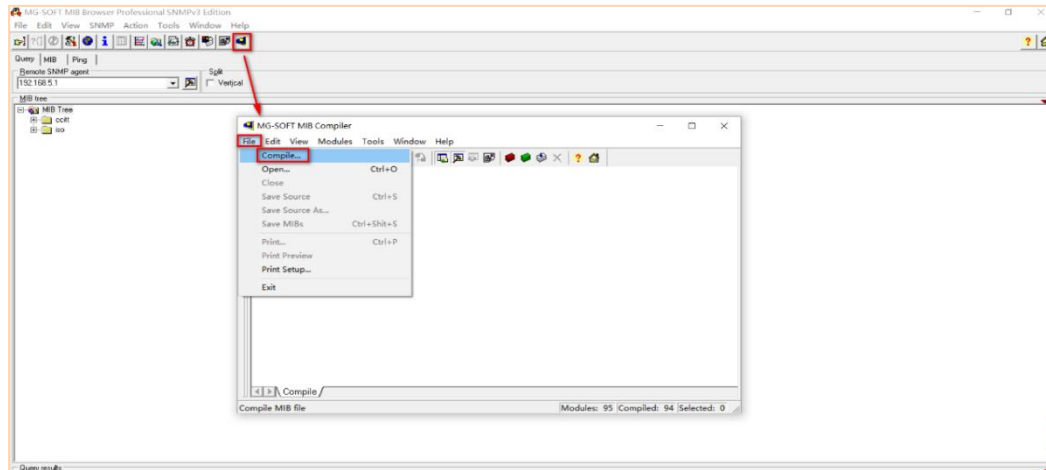
Step 1 - If you don’t have an SNMP Management system (such as CaseView) it is possible to use other software such as “MG MIB Browser” as a management tool.

Once installed on your PC you should see the following screen

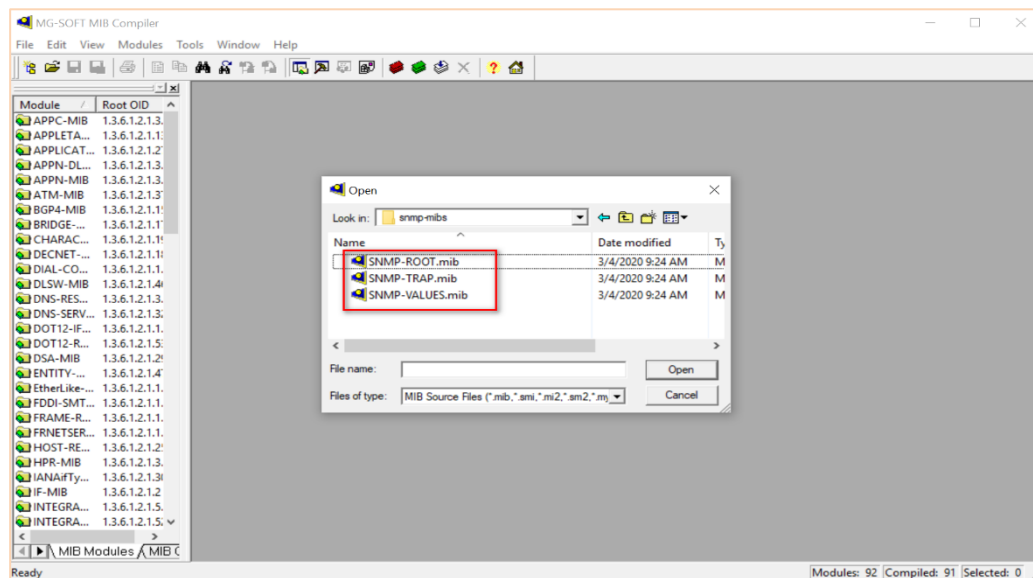


***Note:** After unzipping the “MG MibBrowser” package, install all the files into an “unzip” folder.*

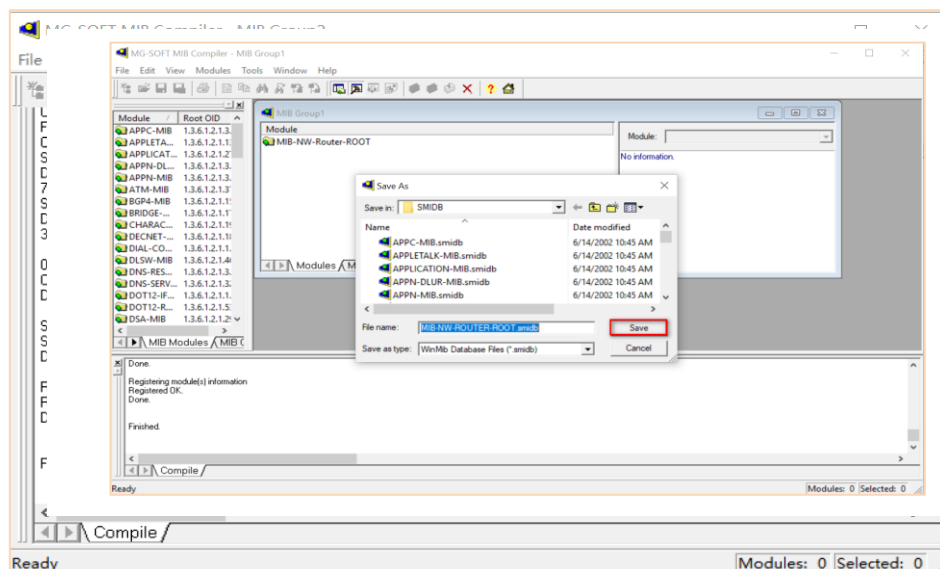
Step 2 Open MibBrowser and run the MIB Compiler as shown below:



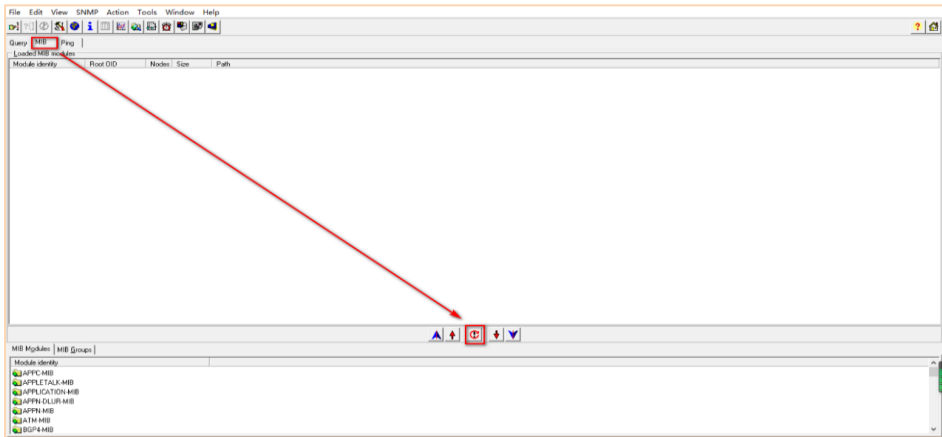
Step 3 Compile the MIB files “SNMP-ROOT.mib”, ”SNMP-TRAP.mib” and “SNMP-VALUES.mib” one by one:



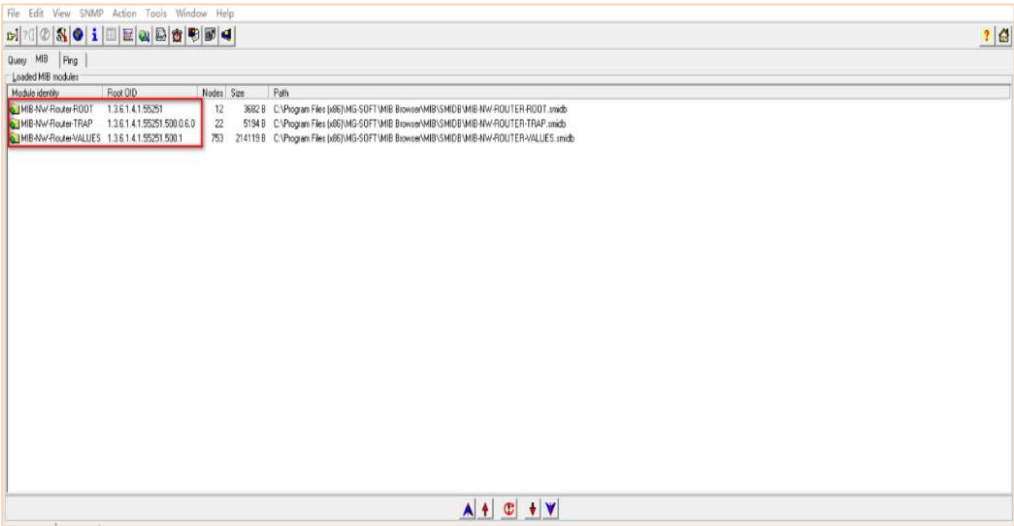
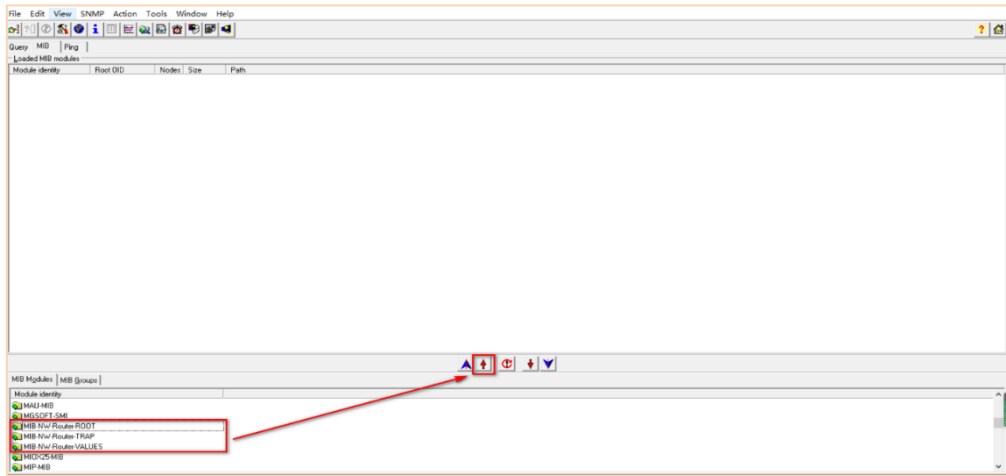
Step 3 : Save the Compiled File as default path, as shown below:



Step 5: After saving the compiled file, refresh the MIB Module:

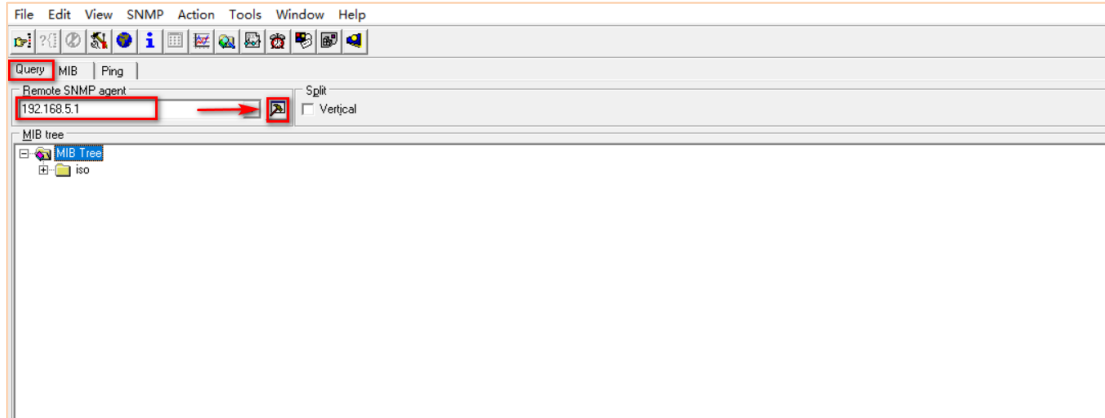


Step 6: Then check the MIB files and load them:

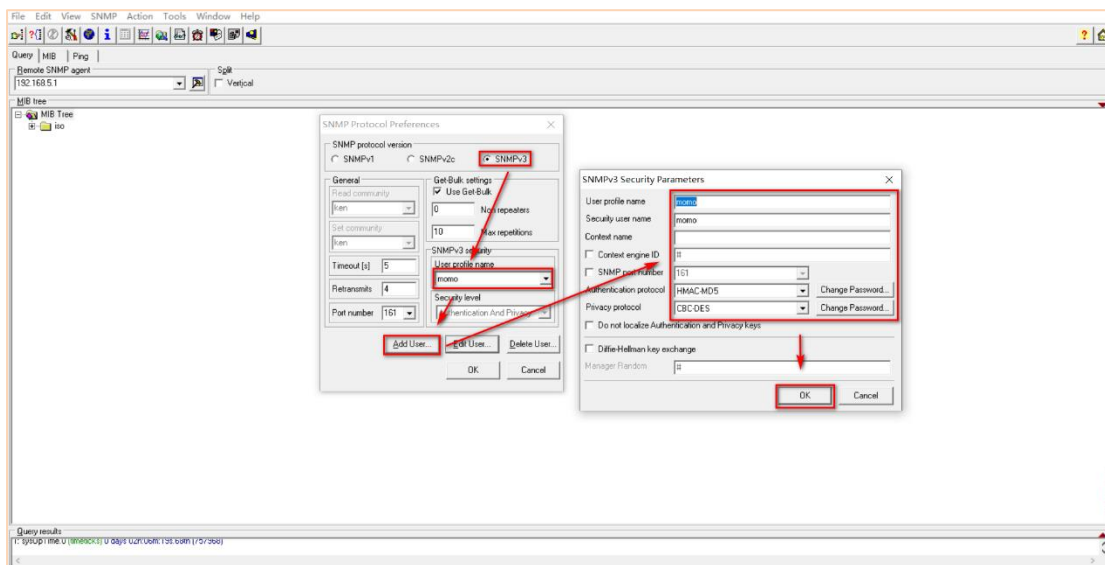


The MIB Files have been loaded

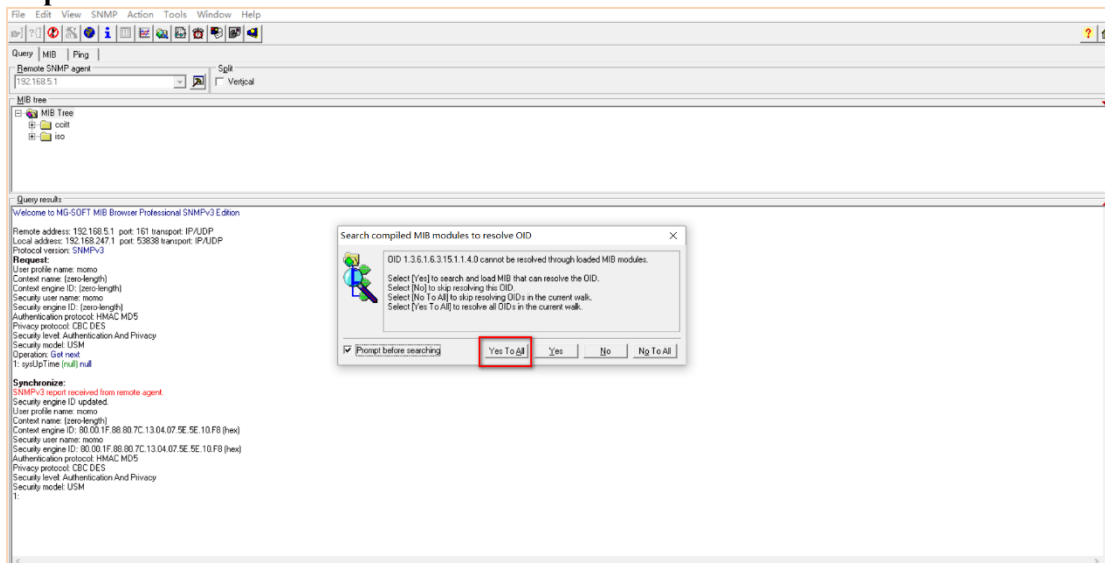
Step 7: Enter the IP address of 6944 router the management tool to the 6944



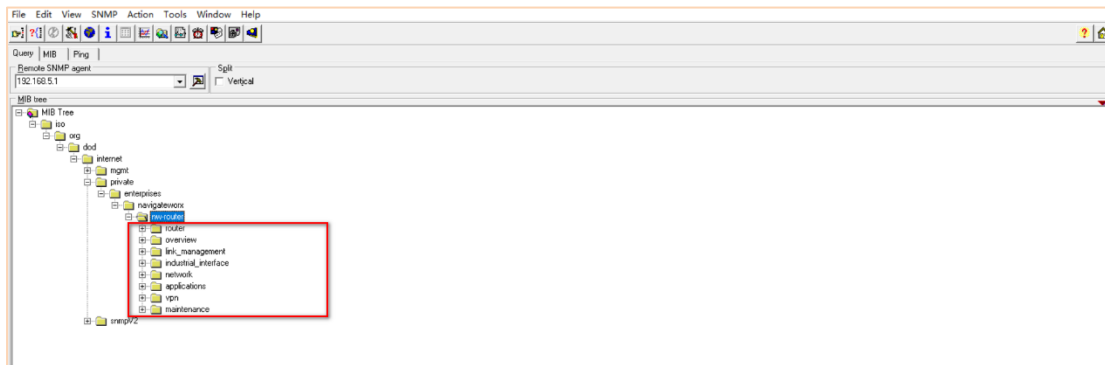
Step 8: Enter the SNMPv3, parameters such Name and the Authentication and so on, as shown below:



Step 9: Click “Yes To All”:



Step 10: We should now see the menu on the 6944 router:

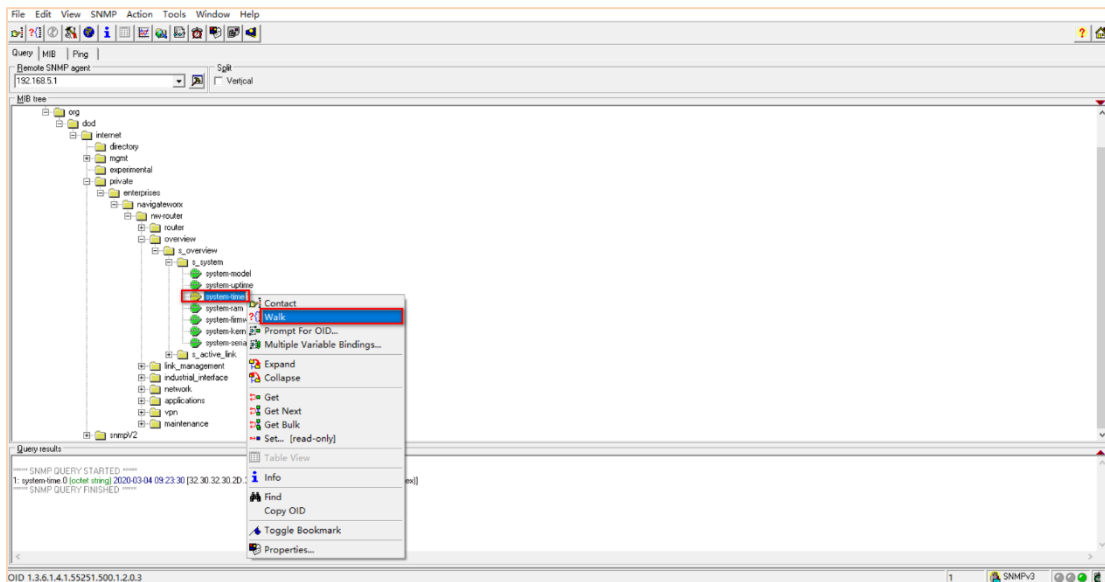


23.3. Testing SNMP

Monitor the Running Status Of The Router

Here we check the “system time” and check the “firmware version” as an example.

Step 1: Go to the “system-time” and Right Click, then click “Walk”:



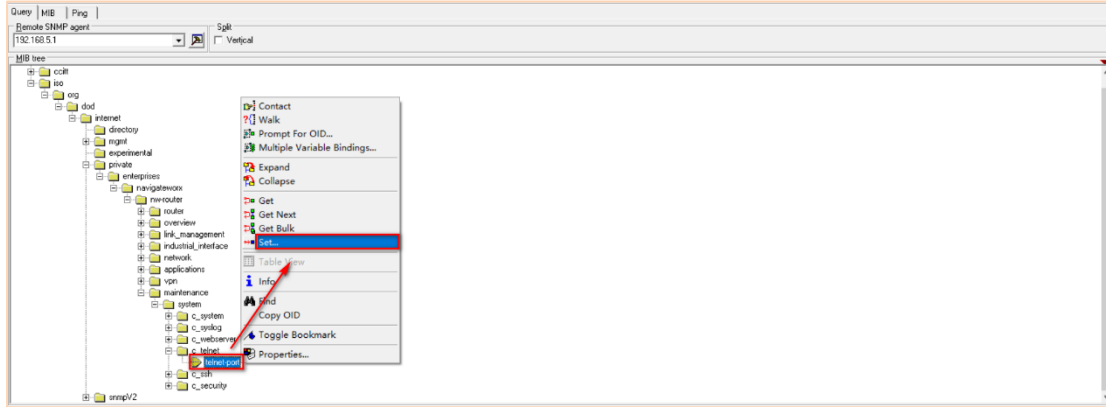
Step 2: Get the System Time of the router:



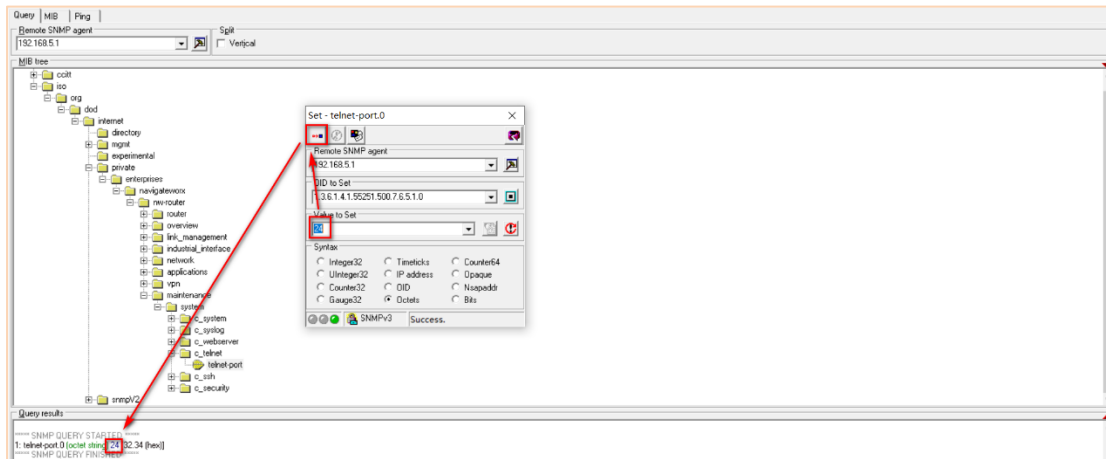
Controlling the 6944 Router

To demonstrate control of the router as an example change the Telnet Port of the 6944 router, then Save, then Apply.

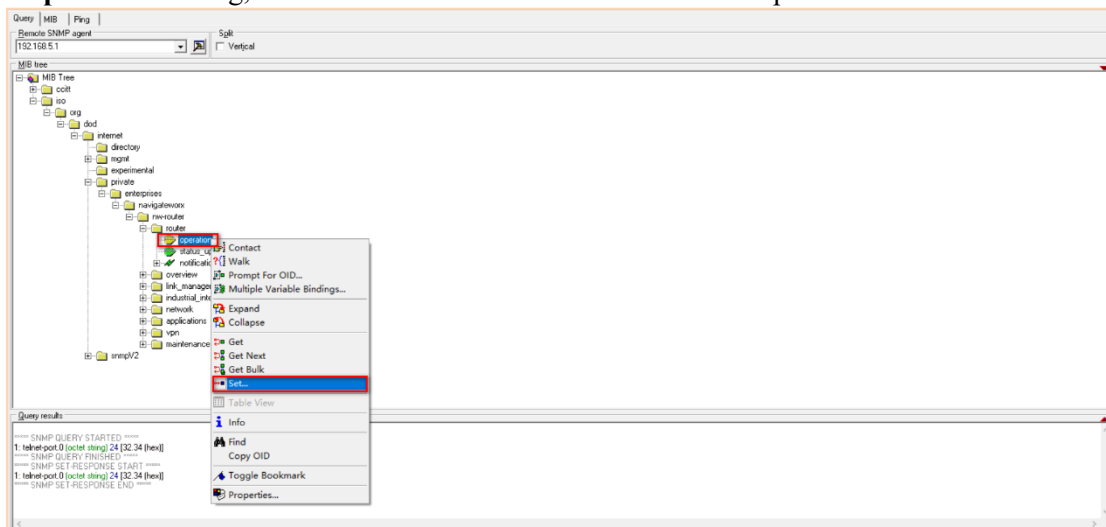
Step 1: Go to the “Telnet” Option, Right Click, then Click “Set”:

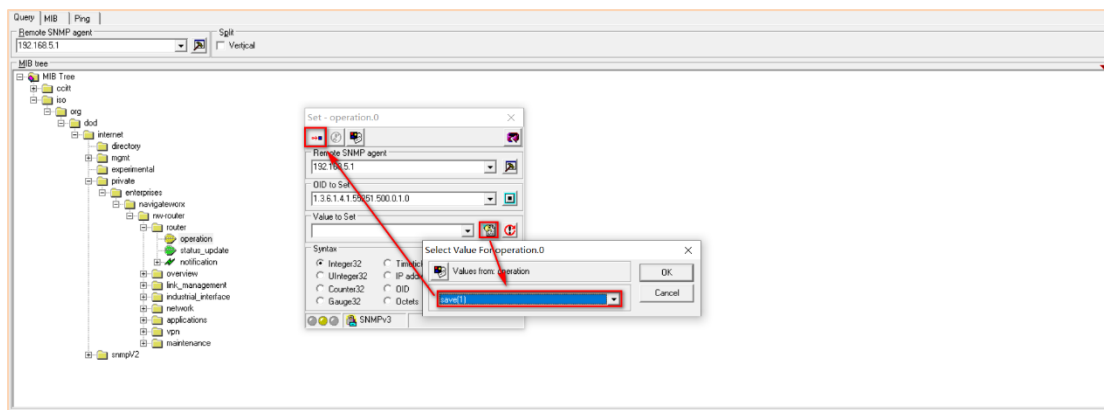


Step 2: Set the Telnet port to 24.

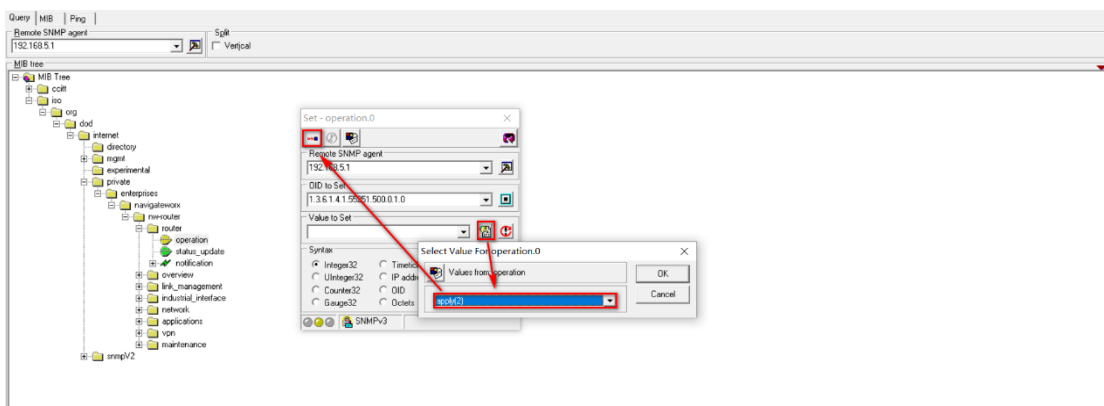


Step 3: After setting, the Port it needs to be saved. Go to “Save Operation” and save it:





Step 4: Now select “Apply”:



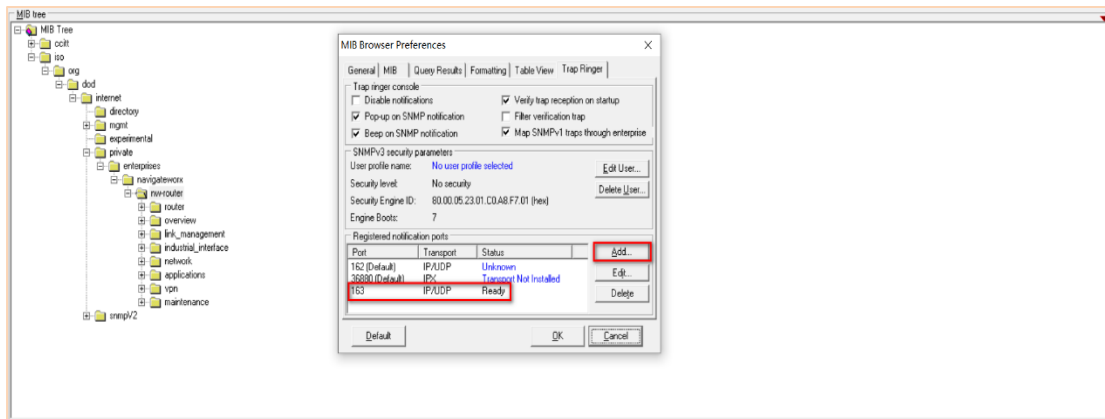
Step 5: Log in to the router and the Tenet Port had been changed to “24”:



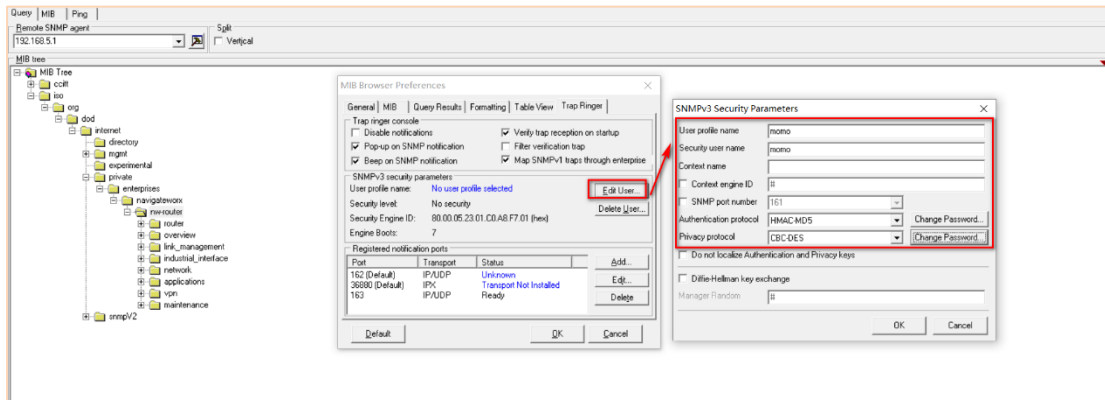
Step 6: The test is successful, now put Telnet port back to 23.

SNMP Trap Notification

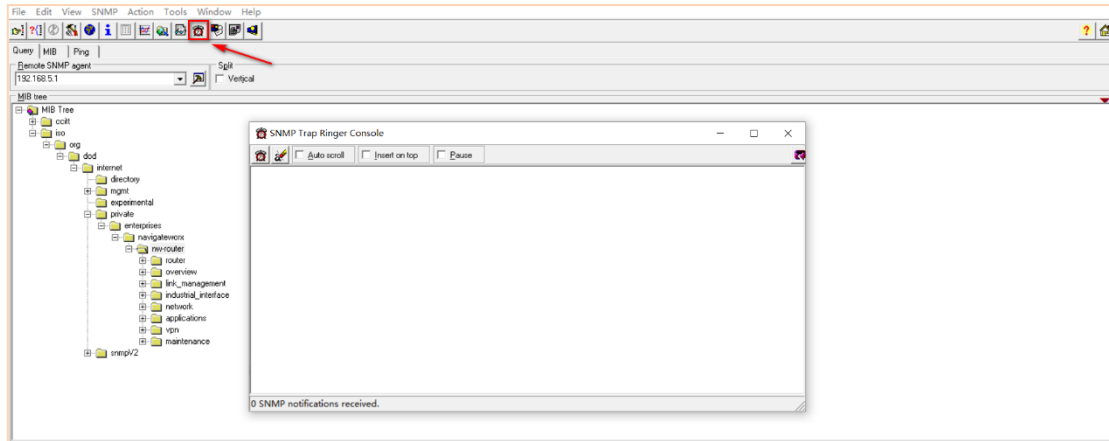
For this SNMP Trap test we use UDP port 163, as shown below



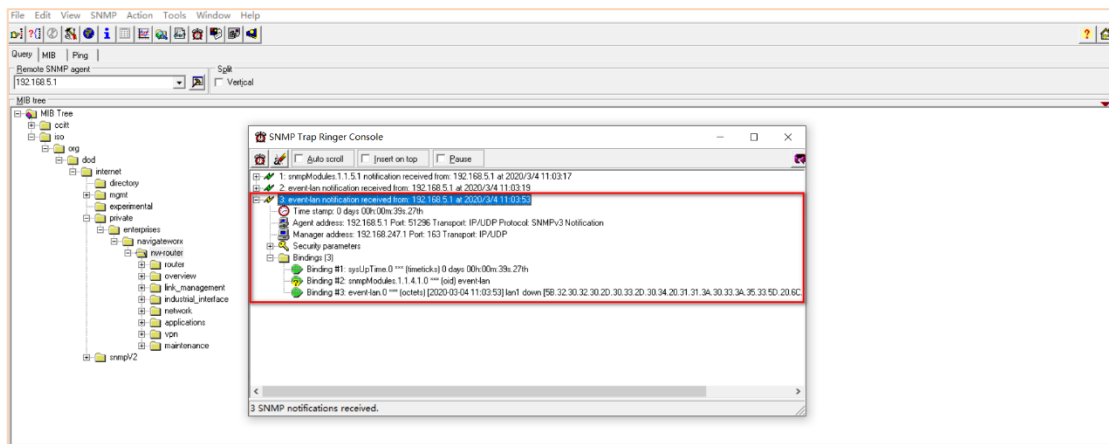
Add User and click “OK”:



Open the SNMP Trap Ringer Console:



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



Test successful.

24. TR069 management platform



- The 6944 router connects to the TR069 management platform.
- The 6944 management platform can do the monitoring or control the router. For example, control the router restart, reset the router to factory default setting, upgrade the firmware/APPs/configuration, syslog upload, NTP configured, check the cellular, active link and NTP status.

Note: This Application Note TR069 has been tested with the “XACS” TR069 management platform.

Configuration

Configuration TR069 on the 6944

Step 1 Go to **Applications>TR069**, specify the settings to make the router connect to TR069 management platform:

The screenshot shows the TR069 configuration page. The left sidebar contains navigation options: Overview, Link Management, Industrial Interface, Network, Applications (selected), VPN, and Maintenance. The main content area is titled "TR069" and contains three sections:

- Local Settings:** Includes checkboxes for "Enable" (checked), "Local Port" (7547), "Authentication" (Digest), "Username", "Password", and "Log Level" (Info).
- ACS Settings:** Includes a "URL" field (http://192.168.111.19/acs), "Username", "Password", "Enable Periodic" (checked), "Periodic Interval" (1800), and "Http 100 Continue Enable" (unchecked).
- Manufacturer Info:** Includes "Manufacturer" (Navigateworx) and "Manufacturer OUI" (FFFFFF).

At the bottom right, there are "Save" and "Apply" buttons.

Note: During the test without authentication on both the 6944 (CPE) and the TR069 Management Platform (XACS), there is no need to set the username and password.

Step 2 Login to the XACS, on the homepage we can see the router has connected to the platform successfully:

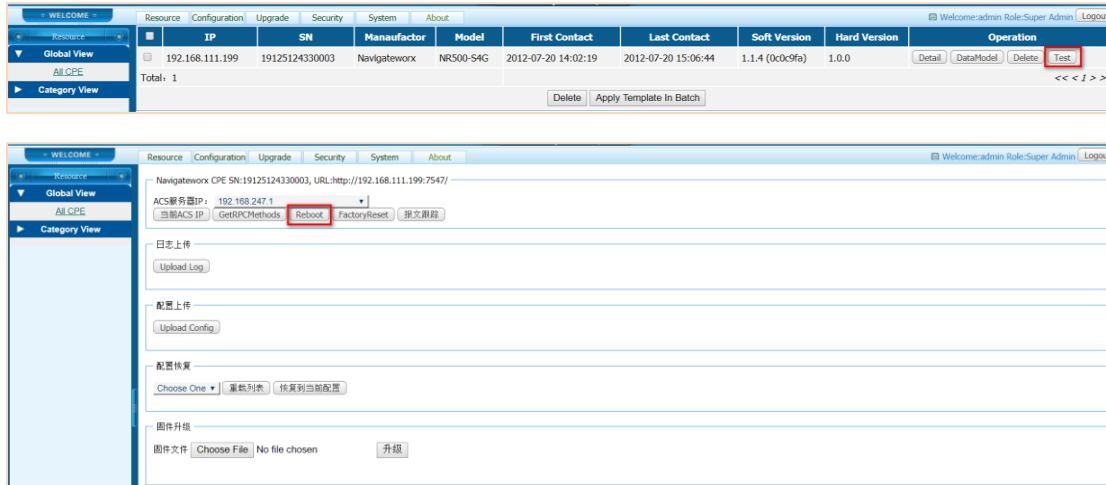
| Resource | IP | SN | Manufacturer | Model | First Contact | Last Contact | Soft Version | Hard Version | Operation |
|---------------|-----------------|----------------|--------------|-----------|---------------------|---------------------|-----------------|--------------|------------------------------|
| Global View | 192.168.111.199 | 19125124330003 | Navigateworx | NR500-S4G | 2012-07-20 14:02:19 | 2012-07-20 14:36:44 | 1.1.4 (0c0c9fa) | 1.0.0 | Detail DataModel Delete Test |
| Category View | Total: 1 | | | | | | | | |

At the bottom of the table, there are buttons for "Delete" and "Apply Template In Batch".

Control and Monitoring the 6944

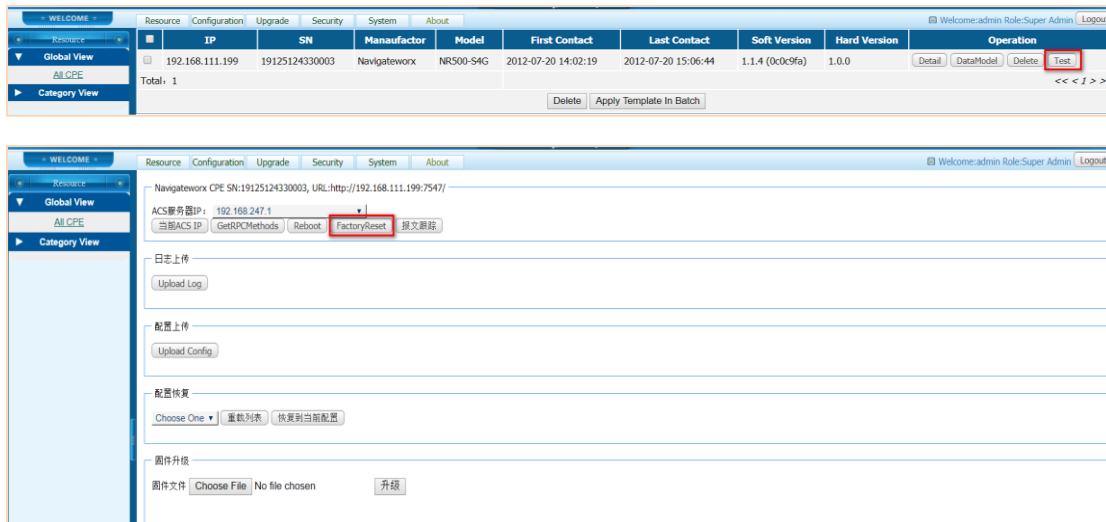
Reboot

Login to the platform and go to **Resource>Test>Reboot**, the router will reboot when click the “Reboot” button:



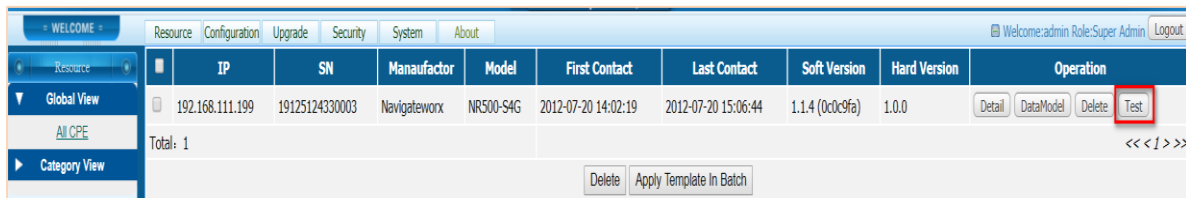
Factory Reset

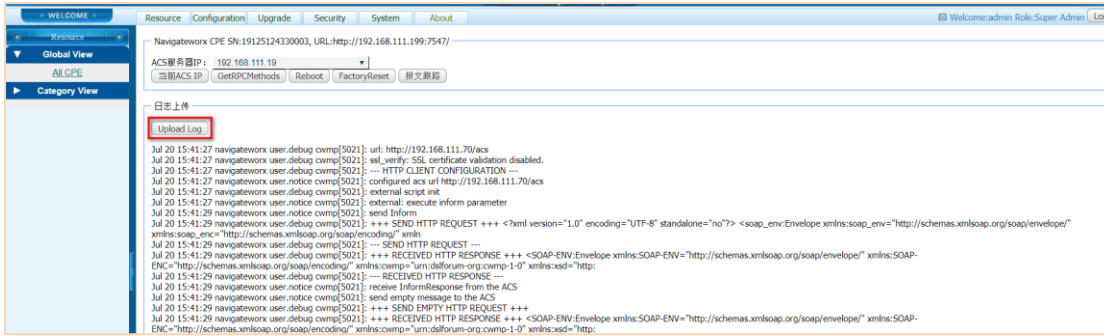
Login to the platform and go to **Resource>Test>FactoryReset**, the router will reset when click the “Factory Reset” button:



Syslog Upload

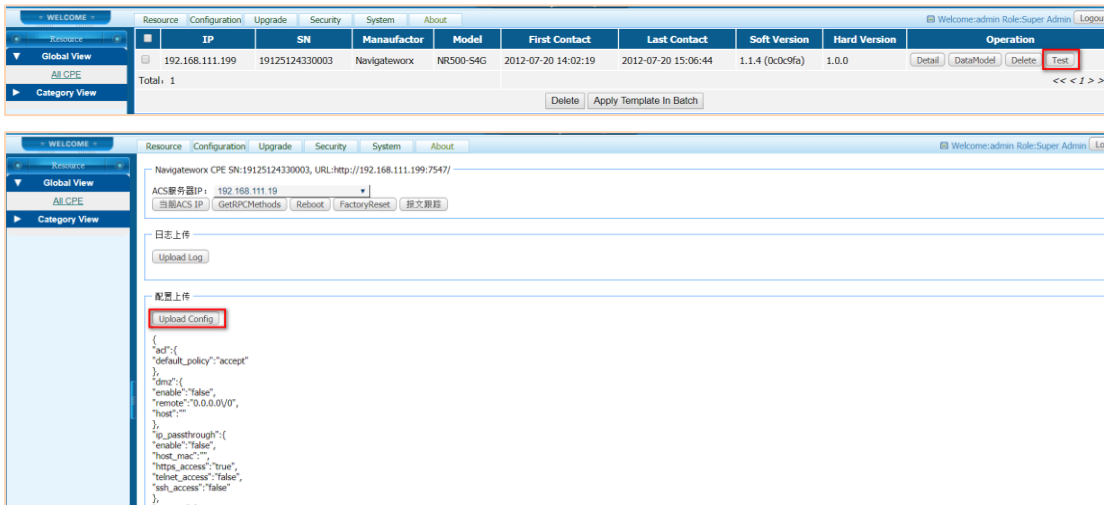
Login to the platform and go to **Resource>Test>Upload Log**, the router’s syslog will display on the TR069 management platform:





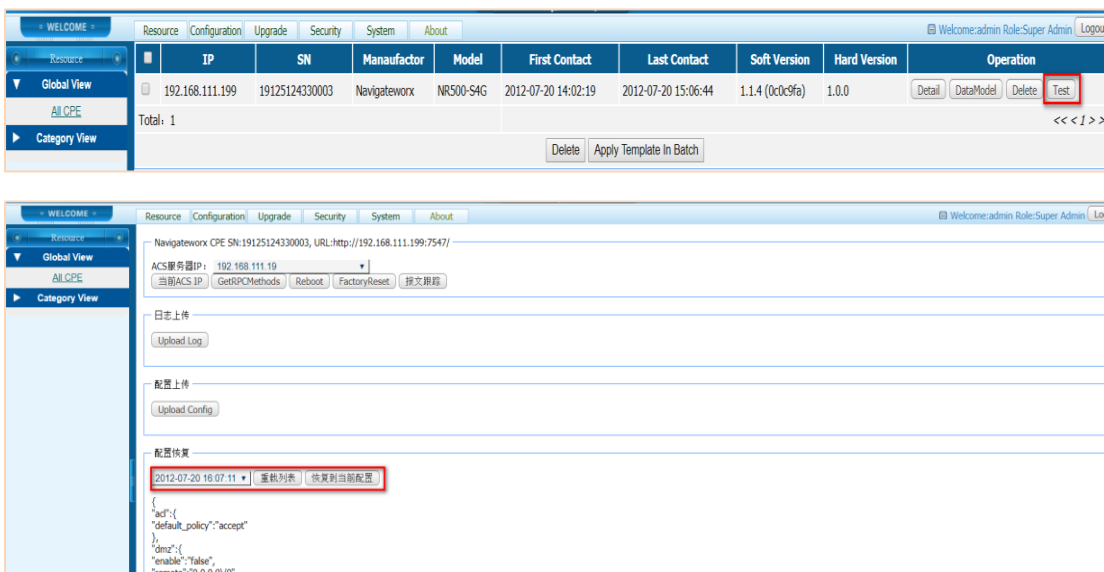
Config Upload

Login to the platform and go to **Resource>Test>Upload Config**, the router's config will display on the TR069 management platform:



Config Update

From the TR069 management platform, we can update the 6944 router. Follow the steps below and we can upload a configuration to the platform, or we can put the config file to the "uploads" installation folder, then go to **Resource>Test>Config Reset**, to download the configuration to the router:



Firmware/APP Upgrade

Login to the platform and go to **Resource>Test>Firmware Upgrade**, choose the firmware or APP file and upgrade to the router:

The screenshot shows the 'Firmware Upgrade' page. At the top, there's a table of devices. The 'Test' button is highlighted in the 'Operation' column. Below the table, there's a section for 'Firmware Upgrade' with a 'Choose File' button and an 'Upgrade' button.

NTP Operation

Login to the platform and go to **Resource>DataModel>.Time**, we can configure NTP parameters and check the NTP status. Check the local time:

The screenshot shows the 'NTP Operation' page. The left sidebar has a tree view with 'CurrentLocalTime' selected. The main area displays the configuration for 'CurrentLocalTime'. The 'GetParameterValues' button is highlighted.

Check the time zone:

The screenshot shows the 'NTP Operation' page. The left sidebar has a tree view with 'LocalTimeZone' selected. The main area displays the configuration for 'LocalTimeZone'. The 'GetParameterValues' button is highlighted.

Specify the NTP server1 address:

The screenshot shows the 'NTP Operation' page. The left sidebar has a tree view with 'NTPServer1' selected. The main area displays the configuration for 'NTPServer1'. The 'SetParameterValues' button is highlighted.

Specify the time zone:

The screenshot shows the 'LocalTimeZone' configuration page. The 'LocalTimeZone' parameter is highlighted in the left sidebar. The main area shows the configuration for 'LocalTimeZone' with a value of '+8:00' and an 'OK' button.

Active Link and Cellular Status

From the TR069 management platform we can check the active link and cellular status.

Step 1 Login to the platform and go to **Configuration>Create new template**, to create the template for active link and cellular:

The screenshot shows the 'Create new template' form. The 'Name' field is highlighted with a red box.

Step 2 After that, add the template parameters for active link and cellular:

The screenshot shows the 'Templates' list. The 'ActiveLink' and 'Cellular' templates are listed. The 'Modify' button for 'ActiveLink' is highlighted with a red box.

Step 3 Template Parameters for ActiveLink:

The screenshot shows the 'Template Property' and 'Template Parameter' sections for the 'ActiveLink' template. The 'Template Parameter' section shows a list of parameters with their names, types, and values. A red box highlights the parameters, and a red arrow points to the 'Add Parameter' button.

| Name | Type | Value |
|---|--------|-------|
| InternetGatewayDevice.ActiveLink.LinkType | string | WAN |
| InternetGatewayDevice.ActiveLink.IP | string | 1 |
| InternetGatewayDevice.ActiveLink.Netmask | string | 1 |
| InternetGatewayDevice.ActiveLink.Gateway | string | 1 |
| InternetGatewayDevice.ActiveLink.PrimaryDNSServer | string | 1 |
| InternetGatewayDevice.ActiveLink.SecondaryDNSServer | string | 1 |

Step 4 Template Parameters for Cellular:

| Name | Type | Value |
|---|--------|-------|
| InternetGatewayDevice.Cellular.1.CSQ | int | 1 |
| InternetGatewayDevice.Cellular.1.IMEI | string | 1 |
| InternetGatewayDevice.Cellular.1.Registration | string | 1 |
| InternetGatewayDevice.Cellular.1.Operator | string | 1 |
| InternetGatewayDevice.Cellular.1.NetworkType | int | 1 |
| InternetGatewayDevice.Cellular.1.PLMNID | int | 1 |
| InternetGatewayDevice.Cellular.1.LocalAreaCode | int | 1 |
| InternetGatewayDevice.Cellular.1.CellID | int | 1 |
| InternetGatewayDevice.Cellular.1.IMSI | string | 1 |
| InternetGatewayDevice.Cellular.1.TXBytes | string | 1 |
| InternetGatewayDevice.Cellular.1.RXBytes | string | 1 |
| InternetGatewayDevice.Cellular.1.ModemFirmwareVersion | string | 1 |

| Name | Type | Value |
|---|--------|-------|
| InternetGatewayDevice.Cellular.1.CSQ | int | 1 |
| InternetGatewayDevice.Cellular.1.IMEI | string | 1 |
| InternetGatewayDevice.Cellular.1.Registration | string | 1 |
| InternetGatewayDevice.Cellular.1.Operator | string | 1 |
| InternetGatewayDevice.Cellular.1.NetwokType | int | 1 |
| InternetGatewayDevice.Cellular.1.PLMNID | int | 1 |
| InternetGatewayDevice.Cellular.1.LocalAreaCode | int | 1 |
| InternetGatewayDevice.Cellular.1.CellID | int | 1 |
| InternetGatewayDevice.Cellular.1.IMSI | string | 1 |
| InternetGatewayDevice.Cellular.1.TXBytes | string | 1 |
| InternetGatewayDevice.Cellular.1.RXBytes | string | 1 |
| InternetGatewayDevice.Cellular.1.ModemFirmwareVersion | string | 1 |

Step 5 After creating the template, go to **Resource>DataModel**, click any one of the templates, and copy the Template Parameters to the “Path”

Step 6 Click “OK” then we can get the related value. Here we see the “IP address” as an example:

| Name | Value |
|-------------------------------------|-----------------|
| InternetGatewayDevice.ActiveLink.IP | 192.168.111.199 |

| | |
|---------------------|-------------|
| Section Twenty-Five | 6944 Manual |
| Maintenance | Rev 2.8 |

25. Maintenance

When newer versions of the 6944, firmware become available, the user can manually update the unit by uploading a software package to the unit.

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

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

25.1. Upgrade via Uboot

Step 1. Connected to the router with console cable, then reboot the router, when “booting” to “0”, please hit any key on the keyboard to make the router go into u-boot mode.

```
*****
                        6944 U-Boot 1.0.0.
                      Build id: 2018 – 08 – 20
*****

Board:      6944 Standard
CPU:        MIPS 74KC
RAM:        64MD DDR1 16-Bit CL3-3-3-8
FLASH:      16MB Winbon w2SQ128
MAC:        00:03:7F:09:08:AD (Fixed)
Clocks:     CPU / RAM/AMB/ SPI/REF
            550 / 400 / 200 / 25 / 25Mhz

Hit any key to stop booting  0
```

Step 2 Run the command “**printenv**” to check the info and setup the server IP on the PC accordingly.

```
6944 > printenv
bootargs=board=nr500s console=ttyS0,115200 mtdparts=spi0.0:128k(u-boot),128k(board),8192
bootcmd=bootm 0x9F040000
bootdelay=1
baudrate=115200
ipaddr=192.168.111.200
serverip=192.168.111.101
autoload=no
hostname=u-boot-nr500s
bootfile=firmware.bin
loadaddr=0x80800000
ncport=6666
lsdk_kernel=1
uboot_name=u-boot.bin
uboot_addr=0x9F000000
uboot_size=0x1EC00
uub-if ping $serverip; then tftp $loadaddr $uboot_name && if test $filesize -le $uboot
$uboot_size && echo DONE! U-Boot upgraded!; else echo ERROR! File is too big!; fi; else
fw_addr=0x9F040000
ufw-if ping $serverip; then tftp $loadaddr $bootfile && erase $fw_addr + $filesize && cp
o ERROR! $serverip is not reachable!; fi (fixed)
stdin=serial
stdout=serial
stderr=serial
ethaddr=00:03:7F:09:08:AD
ethact=eth0
Environment size: 995/4092 bytes
```

Step 3 Set a correct IP address on your PC:

| | |
|----------------------------|--------------------|
| Section Twenty-Five | 6944 Manual |
| Maintenance | Rev 2.8 |

Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

☐ Obtain an IP address automatically

☒ Use the following IP address:

IP address: 192 . 168 . 111 . 101

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 111 . 1

☐ Obtain DNS server address automatically

☒ Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 111 . 1

Alternate DNS server: . . .

☐ Validate settings upon exit

Advanced...

OK Cancel

Step 4 Put the firmware and TFTP software in the same folder, and rename the firmware as “**firmware.bin**”, then run the TFTP software.

UBOOT UPGRADE

Name

firmware.bin

tftp32.exe

Tftpd32 by Ph. Jounin

Current Directory C:\Users\Administrator\Desktop\UJC Browse

Server interfaces ::1 Software L Show Dir

Tftp Server Tftp Client DHCP server Syslog server DNS server

peer file start time progress

About Settings Help

| | |
|---------------------|-------------|
| Section Twenty-Five | 6944 Manual |
| Maintenance | Rev 2.8 |

Step 5 Run the command “**run ufw**” to start the firmware upgrade.

```
6944 > run ufw
Link down: eth0
Ethernet mode (duplex/speed): 1/1000 Mbps
Using eth1 device

Ping OK, host 192.168.111.101 is alive!

TFTP from IP: 192.168.111.101
  Our IP: 192.168.111.200
  Filename: firmware.bin
  Using: eth1
  Load address: 0x80800000

  Loading: #####
           #####
           #####
           #####
           #####
           #####
           #####
           #####
```

Step 6 Check firmware upgraded successfully

```
TFTP transfer complete!

Bytes transferred: 5831984 (0x58fd30)
Erase FLASH from 0x9F040000 to 0x9F5CFFFF in bank #1
Erasing: #####
          #####
          #####

Erased sectors: 89

Copying to FLASH...
Writing at address: 0x9F040000

Done!

DONE! Firmware upgraded!
```

25.2. Scheduled Reboot

Run the command “**reset**” to reboot the router.

Case Communications Ltd

Unit 12E Norths Estate

Old Oxford Road

Piddington

High Wycombe

Bucks HP14 3BE

+44 (0) 1494 880 240

www.casecomms.com

admin@case.uk.com