

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 Noti		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: <u>support@case.uk.com</u> Web: <u>www.casecomms.com</u>



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.	PR	ODUCT 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	INS	STALLATION	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	AC	CESSING 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	BA	SIC 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	Lin	ık 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	2. RADIUS Configuration	5-14
6	Wi-	Fi	6-1
	6.1	Wi-Fi Access Point	6-1
	6.1.	Configuring the Wi-Fi Access Point	6-1
	6.1.2	2. Configuring the Wi-Fi Access Point	6-3
	6.1.3	3. Wireless Access Configuration Example	6-3
7	Con	onfiguring Resilient Links	
	7.1	1 AN001 Dual SIM Configuration	
	7.2	Link Back Up WAN to Cellular	7-4
	7.3	AN003 - 3 Link back up WAN, WWAN1 & WWAN 2	7-8
8	Net	work Security	8-1
	8.1.	Firewall and ACL	8-1
	8.2.	AN028-Configuring SSH with a Public Key	8-3
9	Rou	~	9-1
	9.1.	Static Routing	9-1
		Dynamic Routing Using RIP	9-2
		Dynamic Routing Using OSPF	9-4
	9.4.	Dynamic Routing Using BGP	9-6
10	V.R.		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		V (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. 11.7.	AN008-Open VPN Client with Username and Password AN009-Open VPN Client Running TAP Pre-shared key P2P Mode	11-18 11-24
	11.7.	AN010- Open VPN Client_with_TAP_under_P2P_mode	11-24
	11.8 11.9.	AN010- Open VPN Chent_whit_TAF_undet_F2F_mode AN011-OpenVPN with TUN and X.509 certificate P2P Mode	11-27
		AN050-6944 as an Open VPN Server with X.509 Certificate	11-34
		AN57-Open VPN between 6944 routers with X.509 Certificate.	11-34
		AN058-Open VPN using passwords between two 6944's	11-30
12	IIII2.		12-1
14	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		E Generic Routing Encapsulation	13-1
	13.2.	AN056- GRE VPN Redundancy to Cisco Router	13-5



14	La	yer 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	Po	int 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	Co	onfiguring 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	In	dustrial 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.	Digita	al I / O Ports	19- 1
	19.1	Digital Input Port	19-1
	19.2.	Digital Output	19-1
20	Μ	ODBUS	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	A	Г 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.	SN	AS Commands	22-1
	22.1.	SMS Control	22-5
	22.2	SMS Gateway	22-7
	22.3	SMS Notification	22-9
23	SN	MP	23-1
24.	TI	R069 management platform	24-1
25.	M	aintenance	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

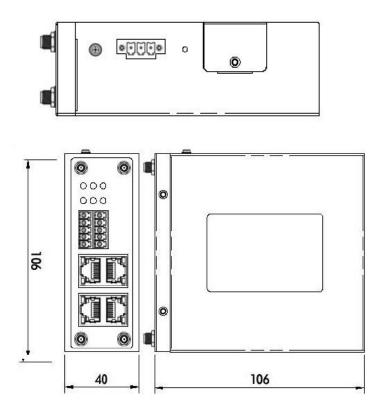
Environmental

- 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)

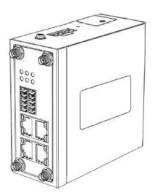


1.5. Packaging Checklist

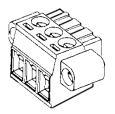
The 6944 series Router includes the parts shown in below, please verify your components. **NOTE:** if any of the below items is missing or damaged, please contact your sales representative.

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



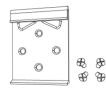
• 1 x 3-pin 3.5 mm male terminal block with lock for power supply



- 1 x Ethernet cable



• 35mm Din-rail mounting kit



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



• 1 x Quick Start Guide



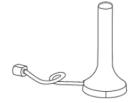
Optional Accessories (sold separately)

• 3G/4G cellular antenna

Stubby antenna

Magnet antenna







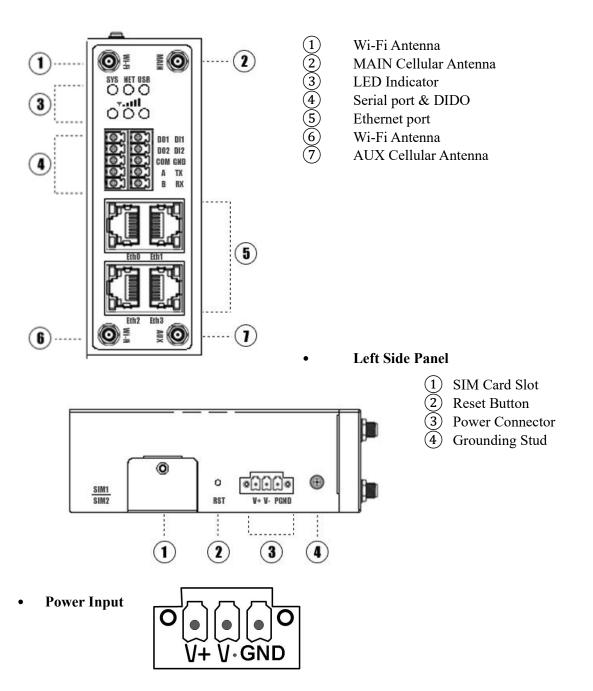
Rev 2.8

This page left blank intentionally



2 INSTALLATION

- 2.1. Product Overview
- Front Panel



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



2.2. LED Indicators

Name	Color	Status	Description
		Slow Blinking (500ms duration)	Operating normally
SYS NET USR: SIM USR: Wi-Fi Signal Strength Indicator	Green	Fast Blinking	The 6944 is initialising
		Off	Power is off
		On	Registering to Highest priority network service (depend on Radio, e.g. Radio support LTE as Highest priority network).
NET	Green	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
		On	The 6944 is trying cellular connection with SIM1
USR: SIM	Green	Fast Blinking (250ms duration)	The 6944 is trying cellular connection with SIM2
		Off	No SIM detected
		On	Wi-Fi is enabled but without data transmission
USK: W1-F1	Green	Blinking	Wi-Fi is enabled and data transmission
		Off	Wi-Fi is disable or initialize failed
Signal Strength		On, 3 LED light up	Signal strength (21-31) is high
Indicator		On, 2 LED light up	Signal strength (11-20) is medium
	Green	On, 1 LED light up	Signal strength (1-10) is low
T.11		Off	No signal

2.3. Ethernet Port Indicator

Name	Status	Description		
Link indicator	On Blinking	Connection is established 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		А			Router<>Device			
5		В			Router<>Device			
6			DI1		Router <device< th=""></device<>			
7			DI2		Router <device< th=""></device<>			
8	GND							
9	TX				Router>Device			
10	RX				Router <device< th=""></device<>			



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

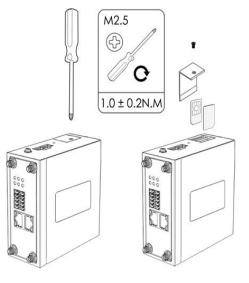
2.5. Reset Button

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

2.6. Insert SIM card

• Insert / Remove SIM card

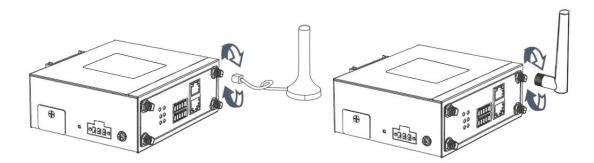
- 1. Make sure the power is disconnected.
- 2. Use a Phillips-head screwdriver to remove SIM slot cover.
- 3. Insert the SIM card(s) into the SIM sockets.
- 4. Replace the SIM slot cover.





2.7. Installing the Antenna

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

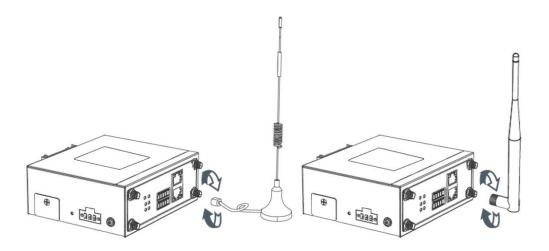


NOTE: The 6944 router supports dual antennas with MAIN and AUX connectors. The MAIN connector is for receiving and transmitting data. The AUX connector is for enhancing the signal strength, and should be used with the MAIN Antenna.

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

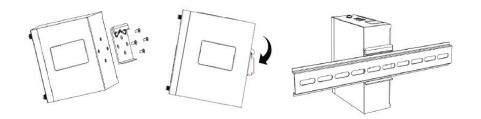
Please follow the picture below to install the Wi-Fi antenna in the right position before testing.

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



2.8. DIN-Rail Mounting

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



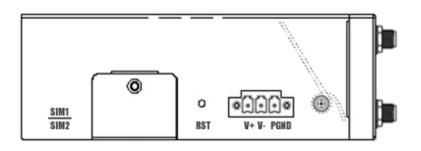




2.9. Protective Grounding Installation

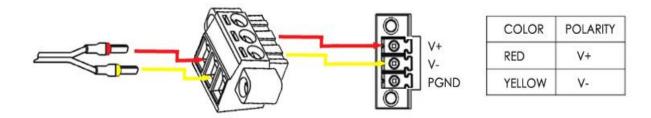
- 1. Remove the grounding nut.
- 2. Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.

NOTE: Strongly recommended the router to be grounded when deployed



2.10. Power Supply Installation

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



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.



Rev 2.8

This page left blank intentionally



Accessing the web configuration

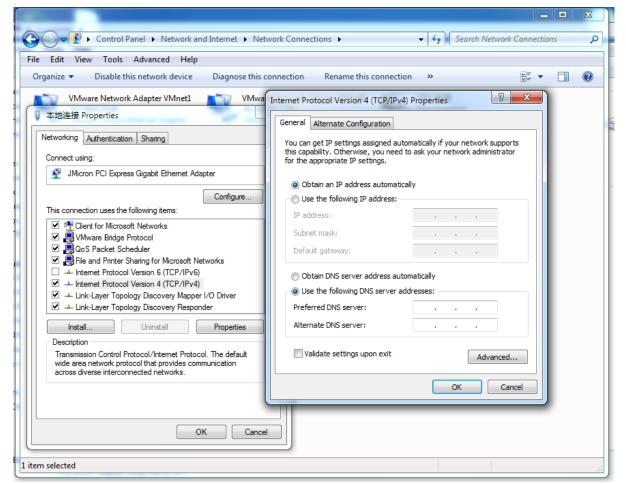
3. **ACCESSING THE WEB CONFIGURATION**

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



Accessing the web configuration

Control Panel > Network and Internet > Network File Edit View Tools Advanced Help	rk Connections 🕨	✓ 4y Search Network	Connections
	10 D 111 11		
Organize Disable this network device Diagnose this control of the device Diagnose the	nection Rename this connection	n »>	₩= ▼ 1 0
VMware Network Adapter VMnet1 VMwa In 章 本地连接 Properties Networking Authentication Sharing Connect using: 愛 JMicron PCI Express Gigabit Ethemet Adapter Configure This connection uses the following items:	ternet Protocol Version 4 (TCP/IPv4) General You can get IP settings assigned auto this capability. Otherwise, you need t for the appropriate IP settings. Obtain an IP address automatica Obtain an IP address automatica IP address:	matically if your network suppor o ask your network administrator	
Generation Microsoft Networks Generation Microsoft Networks Generation Strain for Microsoft Networks Anternet Protocol Version 6 (TCP/IPv6) Anternet Protocol Version 4 (TCP/IPv4) Anternet Protocol Version 4 (TCP/IPv	Subnet mask: Default gateway: Obtain DNS server address autor Outse the following DNS server address autor Preferred DNS server:	· · · · · · · · · · · · · · · · · · ·	
Install Uninstall Properties Description Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.	Alternate DNS server:	Advanced.	
OK Cancel		OK Can	

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.



admin

Image: Straight of the st



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.

	_			0			10					
-	3	Router Web UI		× + ~							-	٥
\leftarrow	\rightarrow	0 G	0 1	92.168.5.1/index.html					☆	Zţ≡	h	ß
	Com							Login: admin Reboot	Logo	out		
	Over		Ĩ	Status								1
		verview /slog		System Information								
		Managemer	.+		Device Mod	lel	6944					L
		strial Interfa			System Uptin	ne	00:06:22					L
			ace		System Tin	ne	2019-07-30 17:39:59					L
	Netv				RAM Usa	ge	24M Free/18M Shared/64M Total					L
		ications			Firmware Version	on	1.1.0 (2d7248a)					L
	VPN				Kernel Versi	on	4.4.92					L
	Main	tenance			Serial Numb	er	19075144330006					L
				Active Link Information								
					Link Ty	pe						L
					IP Addre	SS						L
					Netma	sk						L
					Gatew	ay						L
					Primary DNS Serv	er						L
					Secondary DNS Serv	er						L
												L
												L
												L

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.

Reboot Logout

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

Save Apply

• Close: exit without changing the configuration on current page.

Close

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



Basic Browser Configuration

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.

		Login: admin	
	S	Reboot	Logout
verview	Syslog Events		
Overview Syslog	Syslog Information		
ink Management	Jul 30 17:34:00 casecomms syslog.info syslogd started: BusyBox v1.25.1 Jul 30 17:34:05 casecomms daemon.info dnsmasg[1738]: started. version 2.78 cachesize 150		
ndustrial Interface	Jul 30 17:34:05 casecomms daemon.info dnsmasq[1738]: compile time options: no-IPv6 GNU-getopt no-DBus no-i180 no-conntrack no-ipset no-auth no-DNSSEC no-ID loop-detect inotify	n no-IDN DHCP no-DH	CPv6 no-Lua TFTP
letwork	Jul 30 17:34:05 casecomms daemon.info dnsmasq-dhop[1738]: DHCP, IP range 192.168.5.2 - 192.168.5.200, lease t Jul 30 17:34:05 casecomms daemon.info dnsmasq-dhop[1738]: DHCP, sockets bound exclusively to interface lan0	time 2h	
pplications	Jul 30 17:34:05 casecomms daemon.warn dnsmasq[1738]: no servers found in /etc/resolv.conf, will retry		
'PN	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		
laintenance	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[17/39]. 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?		



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



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	
Connection Type	WWAN1 V
Description	
ICMP Detection Settings	
Enable	
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interval	300 ⑦
Retry Interval	5 ⑦
Timeout	3
Retry Times	3
	Save Close



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.

Statu	us (Cellular							
Cellula	r Informat								
Index	Modem	Registration	CSQ	Operator	Netwok Type	IMEI	IMSI	TX Bytes	RX Bytes
1	EC25	Registered	31 (-51dBm)	vodafone	LTE	861107038049871	460015956236598	2992	2748
				Index	1				
				Modem	EC25				
			R	egistration	Registered				
				CSQ	31 (-51d8m)				
				Operator	vodafone				
			Ne	twok Type	LTE				
				IMEI	861107038049871				
				PLMN ID	46001				
			Local	Area Code	2508				
				Cell ID	6016C02				
				IMSI	460015956236598				
				TX Bytes	2992				
				RX Bytes	2748				
			Moden	n Firmware	EC25EFAR06A01M4G				



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.

Stat	us	<u>Cellular</u>	
Moder	n General	Settings	
Index	SIM Card	Auto APN	
1	SIM1	true	ß
2	SIM2	true	ß

Cel	lular
•	SIM Card - Displays the SIM card support on this unit.
•	Auto APN - Displays the Enable status of auto APN function.
SIN	1 Card Settings
•	SIM Card - Displays the current SIM card settings
•	Auto APN - Check this box enable auto checking the Access Point Name provided by the carrier.
•	Dial Number - Enter the dial number of the carrier.
•	Authentication Type - Authentication method used by the carrier. Possible selections are Auto, PAP, CHAP.
•	PIN Cod - Enter a 4-8 characters PIN code to unlock the SIM.
•	Monthly Data Limitation - Enter the data total amount for SIM card, SIM card switchover when data reach limitation.
•	Override Primary DNS - Enter the primary DNS server will override the automatically obtained DNS.
•	Network Type - Select the mode of operation of the cell module (Auto, 4G Firstly, 4G Only, etc.).
•	Use All Bands - Check this box to enable all bands selection or choose specified bands.



SIM Card Settings	
Modem General Settings	
Index	1
SIM Card	SIM1 v
Auto APN	
Dial Number	*99#
Authentication Type	Auto 🔻
PIN Code	
Monthly Data Limitation	0 ⑦
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

				Logint admin Reboot Logout	
Overview	Stat	tus	Cellular		
Link Management	Moder	n General	Settings		
Connection Manager	Index	SIM Card	Auto APN		_
 Cellular Ethernet WFi 	1 2	SIM1 SIM2	true true		Ø

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

Link Management

em General Settings					
	Index	1			
	SIM Card	SIM1	Ψ.		
	Auto APN				
	APN	internet			
U	Isername	Vodafone			
	Password				
Authentical	tion Type	Auto	•		
	PIN Code			0	
Monthly Data L	imitation	0		0	
Monthly B	liling Day	1		0	
Override Prin	nary DNS				
Override Second	dary DNS				
em Network Settings					
Network Type		Auto	•		
Use All Bands		•			

Step 3: Click Save>Apply.

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

				Logist admin Reboot Logout
Overview	Sta	tus	Cellular	
Link Management	Mode	m General	Settings	
Connection Manager	Index	SIM Card	Auto APN	
> Cellular	1	SIM1	true	ß
Ethernet WE	2	SIM2	true	8 8

Step 5: Setup the parameters of WWAN1 as below:

Connection Settings						
Connection Information						
Priority	1					
Enable						
Connection Type	WWAN1 •	\bigcirc				
Description						
ICMP Detection Settings						
Enable						
Primary Server	8.8.8.8					
Secondary Server	114.114.114.114					
Interval	300	\bigcirc				
Retry Interval	5	\bigcirc				
Timeout	3	0				
Retry Times	3	0				
		Save Close				

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

Stat	us	Port Assignme	ent WA	N LAN	VLAN			
Ethernet Port Information								
Index	Name	Status						
1	ETH0	Up						
2	ETH1	Up						
3	ETH2	Up						
4	ETH3	Up						
Interfa	ice Info	rmation						
Index	Name	MAC Addre	SS					
1	wan							
2	lan0	A8:3F:A1:E0:A	A2:FA					
DHCP I	Lease Ta	ıble						
Index	MAC	Address	IP Address	Lease Expires	Hostname			
1	30:59:b7	:16:3b:66 19	2.168.111.40	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	1
Port	Eth0 v
Interface	WAN v
	Save 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 Sett	ings	1			
		Conne	ection Type	DHCP	
Advanced Se	ttings				
		1	NAT Enable		
			MTU	1500	
		Override Pr	rimary DNS		
		Override Seco	ndary DNS		



5.3.2. Configuring an Ethernet LAN port

Ethernet->LAN

- Interface Select the configurate LAN port of this subnet.
- IP Address Enter LAN IP address for this interface.
- Netmask Enter subnet mask for this subnet.
- MTU

Maximum Transmission Unit, maximum packet size allowed to be transmitted. Should be left as default value of 1500 in most cases.

- Enable Check this box to enable DHCP feature on current LAN port.
- Mode Select the DHCP working mode from "Server" or "Relay".
- **Relay Server** Enter the IP address of DHCP relay server.

• IP Pool Start

External LAN devices connected to this unit will be assigned IP address in this range when DHCP is enabled. This is the beginning of the pool of IP addresses.

• **IP Pool End -** This is the end of the pool of IP addresses.

• Netmask

Subnet mask of the IP address obtained by DHCP clients from DHCP server.

- Lease Time The lease time of the IP address obtained by DHCP clients from DHCP server.
- **Gateway** The gateway address obtained by DHCP clients from DHCP server.
- **Primary DNS** Primary DNS server address obtained by DHCP clients from DHCP server.
- Secondary DNS Secondary DNS server address obtained by DHCP clients from DHCP server.
- WINS Server Windows Internet Naming Service obtained by DHCP clients from DHCP server.

5.3.3. Configuring and Ethernet WAN Port

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

Ethernet->WAN

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



Status	Port Assignment	WAN	LAN	VLAN	
General Set	ttings				
		Con	nection Type	Static IP	۲
			IP Address		
			Netmask		
			Gateway		
			Primary DNS		
		Se	econdary DNS		
Status	Port Assignment	WAN	LAN	VLAN	
General Set	ttings		ļ		
		Con	nection Type	PPPoE	٠
		Authen	tication Type	Auto	•
			Username		
			Password		

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.

Statu	ıs Port	Assignment	WAN	LAN	VLAN	
Genera	Settings					
Index	Interface	IP Address	Netmask			(
1	LAN0	192.168.5.1	255.255.255.0			⊠ ⊗
Multipl	e IP Setting	5				
Index	Interface	IP Address	Netmask			(

Ethernet->LAN

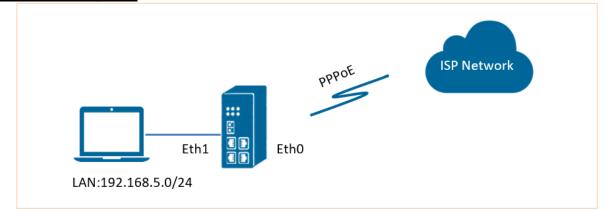
- Interface Displays current name of LAN subnet.
- IP Address Displays LAN IP address of this subnet.
- Netmask Displays subnet mask for this subnet.



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]

5.3.4. AN021 – Configuring PPPoE Configuration Topology



Save

Close

- 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.

				Login: admin Reboot	Logout
Overview	Port Ass	ignment	LAN		
Link Management	General	Settings			
Connection Manager	Index	Port	Interface		
Cellular	1	Eth0	LAND		[
 Ethenet W/i 	2	Eth1	LANO		(
Industrial Interface	3	Eth2	LAND		1
the set	4	Eth3	LANO		

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

casen				Login: admin Rebost	Logout
Communications	Port Ass	ignment	LAN		
Link Management	General	Settings			
Connection Manager	Index	Port	Interface		
Cellular	1	Eth0	LAND		
 Ethenet W/i 	2	Eth1	LANO		
Industrial Interface	3	Eth2	LAND		
Notwork	4	Eth3	LAND		

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 v
		Authentication Type	Auto
		Username	GZHZFTTH@16900.gd
		Password	16900
Advanced Settings			
		NAT Enable	
		MTU	1500
		Override Primary DNS	
	Ov	erride Secondary DNS	

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:

					Login: admin Reboot	Logout
Overview	Port Assig	Port Settings				
Link Management	General S	General Settings				
Connection Manager Cellular	Index	Index	1			
► Libernet	1	Port	Eth0 *			ß
WiFi	2	Interface	WAN •			ß
Industrial Interface	3		Save	Close		ß
Network	4					ß



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	0	
		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
Gateway	10.8.128.1
Primary DNS Server	116.116.116
Secondary DNS Server	221.5.88.88

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

Overview	Ping	Traceroute			
Link Management	Ping Setting	gs			
Industrial Interface			Host Address	8.8.8.8	
Network			Ping Count	5	
Applications			Local IP Address		
VPN		(8.8.8.8): 56 data by			
Maintenance Upgrade System Configuration Debug Teols	64 bytes from 64 bytes from 64 bytes from 8.8.8.8 pin 5 packets tra	n 8.8.8.8: seq=0 ttl= n 8.8.8.8: seq=1 ttl= n 8.8.8.8: seq=3 ttl= n 8.8.8: seq=4 ttl= ng statistics nsmitted, 4 packets r in/avg/max = 20.962	39 time=21.083 ms 39 time=20.962 ms 39 time=21.033 ms eceived, 20% packet loss		

Step 3. Test successful.

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

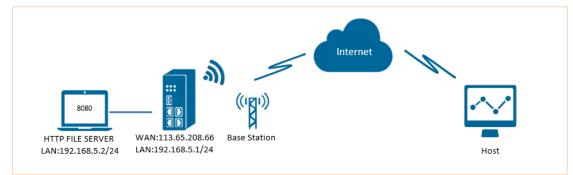
Trunk Settings	
VLAN Trunk Settings	
Index	1
Interface	LAN0 •
VID	10
IP Address	
Netmask	
	Save Close

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.

Ethernet	Network Connection Det	tails ×
Network 110 Realtak LISB GbE Eamily	Network Connection Detail	s:
Wi-Fi Not connected Marvell AVASTAR Wirel	Property Connection-specific DNS Description Physical Address DHCP Enabled IPv4 Address IPv4 Subnet Mask Lease Obtained Lease Obtained Lease Obtained IPv4 Default Gateway IPv4 DHCP Server IPv4 DHCP Server	Value
	IPv4 WINS Server NetBIOS over Topip Enab Link-local IPv6 Address IPv6 Default Gateway IPv6 DNS Server	



Step 2. Enable HTTP FILE SERVER on the PC.

🚔 HFS ~ HTTP File Server 2.3m			Build 300	_		×
🔄 Menu 📅 Port: 8080 👥 You	are in Easy mode					
Popen in browser http://192.168.5.	2:8080/			📄 Сор	y to clipb	oard
Virtual File System			Log			
A / Port Mapping Test Port Mapp						
🔋 IP address		File	Status	Speed	Time	P
Out: 0.0 KB/s In: 0.0 KB/s						

Port Mapping Configuration

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

verview	Port Mapping Settings Port Mapping rule Settings	
dustrial Interface twork Firewall Route plications N	Protocol Remote Address Remote Port	1 Port Mapping All
intenance		8080 ⑦ Save Close

Testing

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

🚔 HFS / 🛛 🗙 🗌				
$\leftarrow \rightarrow \mathbf{C}$ 🗅 113.65.208.66:8080				
Login	Name .extension	Size	Timestamp	Hits
└────────────────────────────────────	Port Mapping Test	folder	9/15/2018 10:33:27 AM	0
Home 1 folders, 0 files, 0 Bytes				
Search go				

Step 2: Test successful

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



5.6 RADIUS Authentication (IEEE 802.1x)

RADIUS - IEEE 802.1x

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

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

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

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

5.6.1 How RADIUS Works on the 6944

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

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

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

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

5.6.2 RADIUS Configuration

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

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



IEEE 802.1X Authenticator Settings						
Enable						
Reauthentication Period	3600 ⑦					
Use PAE Group Address						
Authentication Server Settings						
Radius Server Address						
Radius Server Port	1812					
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.



Rev 2.8

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.

Sta	tus	Basic	WiFi AP		
WiFi S	tatus				
				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
Assoc	iated Sta	tion			
Index	MAC A	Address	Signal	Station Na	ame
1	30:59:b7	:16:3b:66	-55 dBm	KEN-COMPI	UTER
2	98:10:e8	:67:dd:35	-64 dBm	iPhone	2
Sta	tus	Basic	WiFi AP		
Basic	Settings				
				Running Mode	AP •
				Country Code	UK
		Wi-I	Fi->Basic		

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

5.7Configuring the Wi-Fi Access Point

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

Status	Basic	WiFi AP		
WiFi AP Setti	ngs			
		Enable		
		SSID	wifi-a-p	
		Enable Broadcast SSID		
		Security Mode	WPA PSK 🔹	
		WPA Type	Auto 🔻	
		Encryption Type	Auto 🔻	
		Password		0
Advanced Se	ttings			
		Channel	Auto 🔻	
		Wireless Mode	802.11bgn 🔻	
		Channel Width	40 MHz 🔹	
		Beacon TX Rate HT MCS Index	Auto 🔻	0
		TX Power	High 🔻	
		Beacon Interval	100	
		DTIM Period	100	
		Max Client Support	64	
		Enable Short GI		
		Enable AP Isolate		



Wi-Fi Configuration

Wi-Fi->Wi-Fi AP

- Enable Select this box to enable the Wireless interface.
- SSID

The SSID is the name of the wireless local network. Devices connecting to the 6944 router WiFi access will identify the Access Point by this SSID.

• Enable Broadcast SSID

When the checkbox is not checked, SSID broadcast is disabled, other wireless devices cannot find the SSID, and users have to enter the SSID manually to access to the wireless network.

- Security Mode Select security mode from "None", "WEP" or "WPA PSK".
- WPA Type Select WPA Type from "Auto", "WPA" and "WPA2".

• Encryption Type

Select the encryption method. Options are "Auto", "TKIP", or "CCMP". Because these options depend on the authentication method selected, some options will not be available.

- **Password** Enter the pre-shared key of WEP/WPA encryption.
- Channel

Select the Wi-Fi channel the module will transmit on. If there are other Wi-Fi devices in the area the 6944 router should be set to a different channel than the other access points. Channels available for selection depend on the selected Band.

• Wireless Mode

Select the Wi-Fi 802.11 mode: B, G, or N. Available selections depend on the selected Band.

• Channel Width

Select the width of the Wi-Fi channel. 20 MHz will limit the channel to 20 MHz wide; 20/40 MHz will enable the use of a 40 MHz wide channel when available.

• Beacon TX Rate HT MCS Index

Modulation and Coding Scheme, The MCS modulation coding table is a representation proposed by 802.11n to characterize the communication rate of the WLAN. The MCS takes the factors affecting the communication rate as the columns of the table and uses the MCS index as a row to form a rate table.

• TX power

Select the transmission power for the AP from "High", "Medium" and "Low".

Beacon Interval

Enter the interval of time in which the router AP broadcasts a beacon which is used for wireless network authentication.

• DTIM Period

Enter the delivery traffic indication message period and the router AP will multicast the data according to this period.

• Max Client Support

Enter the maximum number of clients to access when the router is configured as AP.

• Enable Short GI

Check this box to enable Short GI (guard interval), Short GI is a blank time between two symbols, providing a long buffer time for signal delay.

• Enable AP Isolate

Check this box to enable AP isolate, the route will isolate all connected wireless devices.



5.8Configuring the Wi-Fi Access Point

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

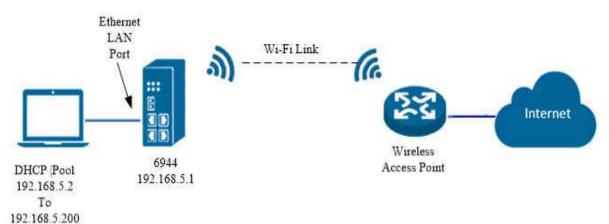
Status	Basic	WiFi Client	
WiFi Client Se	ttings		
		Enable	
		Connect to Hidden SSID	
		SSID	
		Password	
IP Address Se	ttings		
		Connection Type	DHCP

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

5.9Wireless Access Configuration Example

Testing Topology





Configuring Wi-Fi

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

Status	Basic	WiFi Client	
WiFi Client Set	tings		
		Enable	
		Connect to Hidden SSID	
		SSID	
		Password	
IP Address Set	tings		
		Connection Type	Static IP
		IP Address	
		Netmask	
		Gateway	
		Primary DNS	
		Secondary DNS	

Overview	Status	Basic	WiFi Client		
Link Management	Basic Settings				
Connection Manager				Running Mode	Client 🗸
Cellular				Country Code	UK
Ethernet				country cour	
▶ 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 Se	ettings		
Connection Manager			Enable	
Cellular Ethernet			Connect to Hidden SSID	
► WiFi			SSID	Case_Guest_Engineering
Industrial Interface			Password	••••••
Network	IP Address Se	ettings		
Applications			Connection Type	DHCP 🗸

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 Ethernet			ESSID	Case_Guest_Engineering
► WiFi			Current Channel	6
Industrial Interface			Signal	-56 dBm
Network			TX Power	20 dBm



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	✓	
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	
 Connection Manager Collector 	Priority	Priority	1
Cellular Ethernet	1	Enable	
WiFi	2	Connection Type	WLAN 🗸 🕐
Industrial Interface		Description	WLAN
Network		NAT Enable	✓
Applications		ICMP Detection Settings	
VPN		Enable	✓
Maintenance		Primary Server	8.8.8.8
		Secondary Server	114.114.114.114
		Interval	300
		Retry Interval	5 ⑦
		Timeout	3 (?)
		Retry Times	3

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

Step 4: Give it a description.

Step 5: Edit the ICMP Detection Settings as required.

Step 6: Click on Save and then Apply.



General Settings

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

Overview	Status	con	nection	
Link Management	General	Settings		
Connection Manager	Priority	Enable	Connection Type	Description
Cellular	1	true	WLAN	WLAN
Ethernet	2	false	WWAN2	
WiFi	2	Taise	WWAN2	

Checking WAN Status

Click Status to view the WAN status.

Overview	Stat	us C	onnection			
Link Management	Conne	ction Info	rmation			
 Connection Manager 	Index	Туре	Status	IP Address	Netmask	Gateway
Cellular Ethernet	1	WLAN	Connected	192.168.2.13	255.255.255.0	192.168.2.1

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.

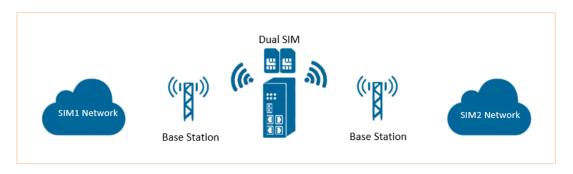


7 Configuring Resilient Links

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.

					Logist admin Roboot Lagaut
Overview	Status	Con	nection		
Link Management	General	Settings			
 Connection Manager 	Priority	Enable	Connection Type	Description	•
Gilder	1	tue	WHANI		20
Ethernet Industrial Interface	2	the	WIIIAN2		8

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	www.www.www.www.www.www.www.www.www.ww
Description	
ICMP Detection Settings	
Enable	. 🗹
Primary Server	8.8.8.8
Secondary Server	114.114.114.114
Interva	300 ⑦
Retry Interva	5 ⑦
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 T
Description	
ICMP Detection Settings	
Enable	
Primary Server	8.8.8
Secondary Server	114.114.114.114
Interval	300 ⑦
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.

Overview	Stat	us C	onnection				
Link Management	Conne	ction Info	mation				
 Connection Manager 	Index	Type	Status	IP Address	Netmask	Gateway	
Cellular Ethernet	1	WWAN1	Connected	10.148.30.147	255.255.255.248	10.148.30.148	
Industrial Interface	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.

Link Type WWAN2 IP Address 10.148.236.23 Netmask 255.255.250 Gateway 10.148.236.24	Active Link Information	
Netmask 255.255.240	Link Type	WWAN2
	IP Address	10.148.236.23
Gateway 10.148.236.24	Netmask	255.255.255.240
	Gateway	10.148.236.24

Overview	Stat	tus Co	onnection			
Link Management	Conne	ction Infor	mation			
 Connection Manager 	Index	Type	Status	IP Address	Netmask	Gateway
Cellular Ethernet	1	WWAN1	Disconnected			
Industrial Interface	2	WWAN2	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->8.8.8/114.114.114.114)

```
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

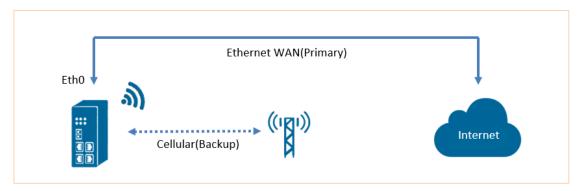
Jul 29 11:19:41 casecomms daemon.err udhcpc[3000]: lease of 10.148.236.23 obtained, lease time 7200



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.

				Lopins admin Reboot Lopsut	
Overview	Port Ass	ignment	LAN		
Link Management	General	Settings			
Connection Manager	Index	Port	Interface		
Cellular	1	Eth0	LAN0		2
 Ethernet Industrial Interface 	2	Eth1	LAND		2

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 of the WAN port to make sure the 6944connects to Internet.

					Reboot	Logout
Overview	Port Assignment WAN	LAN				
Link Management	General Settings					i
Connection Manager		Connection Type	Static IP ·	1		
Cellular Ethernet		Ip Address	192.168.111.111			
Industrial Interface		Netmask	255.255.255.0			
		Gateway	192.168.111.1			
Network		Primary DNS	192.168.111.1			
Applications		Secondary DNS	\$.5.0.5			
VPN	Advanced Settings					
Maintenance		NAT Enable	2			
		MTU	1500			
		Override Primary DNS				
		Override Secondary DNS				

Step 5: Click Save>Apply.



Cellular Configuration

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

				Legin: admin Reboot	Logout	
Overview	Stat	turs	Cellular			
Link Management	Moder	n General	Settings			
Connection Manager	Index	SIM Card	Auto APN			
 Cellular 	1	SIMI	true			
Ethernet Inclustrial Interface	2	SIM2	true			Ø

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

SIM Card Settings	
Modem General Settings	
Index	1
SIM Card	SIM1 v
Auto APN	
APN	internet
Username	
Password	
Authentication Type	Auto 🔻
PIN Code	0
Monthly Data Limitation	0 ⑦
Monthly Bliling Day	1 ⑦
Override Primary DNS	
Override Secondary DNS	
Modem Network Settings	
Network Type	Auto 🔻
Use All Bands	
	Save Close

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**.

						Login: admin Reboot	Logout
Overview	Status	Con	nection				
Link Management	General	Settings					
 Connection Manager 	Priority	Enable	Connection Type	Description			
Cellular	1	true	WWAN1				C
Ethernet	2	true	WWAN2				C

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

00000					Login: admin	N
					Reboot	Logout
Overview	Status	Con	nection			
Link Management			F 2			
Connection Manager	Priority	Enable	Connection Type	Description		<u></u>



Connection Settings		
General Settings		
	Priority	1
	Enable	
	Connection Type	WAN 🔻
	Description	
ICMP Detection Setting	js	
	Enable	
	Primary Server	8.8.8.8
9	Secondary Server	114.114.114
	Interval	300 ⑦
	Retry Interval	5 ⑦
	Timeout	3
L L	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.**

0000								Login: admin	
								Reboot	Logout
iew	Status	Con	nection						
lanagement	General S	ettings							
nnection Manager ular	Priority	Enable	Connection Type	Descript	tion				C
ernet	1	true	WAN						e
Connectio	on Setti	ngs							
General S	Settings	;							
			P	riority	2				
			E	nable					
			Connection	Type	WWAN1	Ţ			
				ription		_			
		o		ption					
ICMP Det	tection	Settin					_		
				nable					
			Primary S	Server	8.8.8.8				
			Secondary S	Server	114.114.114.114				
			In	iterval	300	(?		
			Retry In	iterval	5	(?		
				neout	3		?		
			Retry	limes	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



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 Typ	e WWAN1
IP Addres	s 10.162.9.151
Netmas	k 255.255.255.240
Gatewa	y 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



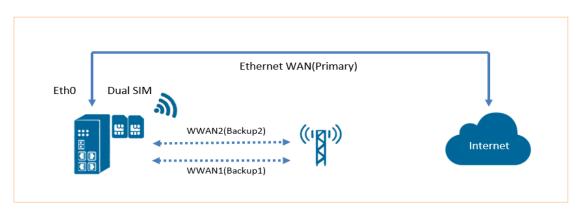
Configuring Resilient Links

Rev 2.8

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.

				Logis: admin Reboot	Logout
Overview	Port Ass	ignment	LAN		
Link Management	General	Settings			
Connection Manager	Index	Port	Interface		
Cellular	1	Eth0	LANO		12
 Ethernet Industrial Interface 	2	Eth1	LANO		2

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

Port Settings				
General Settings				
Inde	ex 1			
Po	rt Eth0	▼		
Interfac	ce 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.



Configuring Resilient Links

		Login: admin Reboot Logout
Overview	Port Assignment WAN LAN	
Link Management	General Settings	
Connection Manager	Connection T	pe Static IP •
Cellular Ethernet	Ip Addr	192.168.111.111
Industrial Interface	Netm	isk 255.255.255.0
	Gatev	ay 192.168.111.1
Network	Primary D	NS 192.108.111.1
Applications	Secondary D	NS 8.8.8
VPN	Advanced Settings	
Maintenance	NAT Ena	ble 🕑
	м	TU 1500
	Override Primary D	NS
	Override Secondary D	NS

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.

odem General Settings	
Index	1
SIM Card	SIM1 v
Auto APN	
APN	internet
Username	
Password	
Authentication Type	Auto
PIN Code	
Monthly Data Limitation	0 ⑦
Monthly Bliling Day	1 ⑦
Override Primary DNS	
Override Secondary DNS	
odem Network Settings	
Network Type	Auto 🔻
Use All Bands	

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**.

						Login: admin Reboot	Logout
Overview	Status	Con	nection				
Link Management	General S	Settings					
 Connection Manager 	Priority	Enable	Connection Type	Description			۲
Cellular	1	true	WWAN1				20
Ethernet Texturation Interface	2	true	WWAN2				12 N 12 N 12 N

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

						Reboot	Logout	
Overview	Status	Con	nection					
Link Management	General S	Settings						
 Connection Manager Gellular 	Priority	Enable	Connection Type	Description				0



Connection Settings			
General Settings			
	Priority	1	
	Enable		
C	Connection Type	WAN	•
_	Description]
ICMP Detection Settings			
	Enable		
	Primary Server	8.8.8.8	
Se	econdary Server	114.114.114.114	
	Interval	300	0
	Retry Interval	5	0
	Timeout	3	0
	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**

00000								Lo	igin: admin		
									Reboot	Logout	
Overview	Status	Con	inection								
Link Management	General S	Settings									
 Connection Manager 	Priority	Enable	Connection Type	Descrip	tion						0
Cellular Ethernet	1	true	WAN								ß⊗
Connecti	on Setti	ings									
General	Settings	5									
			Pric	ority	2						
			En	able							
			Connection T	уре	WWAN1	•					
			Descrip	tion							
ICMP De	tection	Settin	gs								
			En	able							
			Primary Se	rver	8.8.8.8		- 1				
			Secondary Se	rver	114 114 114 114		- 1				

?

?

 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

300

5

Interval

Retry Interval

					Legin: admin Reboot Logout
Overview	Status	Con	nection		
Link Management	General	Settings			
Connection Manager	Priority	Enable	Connection Type	Description	0
Cellular	1	true	WAN		2 S
Ethernet	2	true	WWANI		8 N



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
Interval	300 ⑦
Retry Interval	5 ⑦
Timeout	3 ⑦
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 Typ	e WWAN1
IP Addres	s 10.162.9.151
Netmas	k 255.255.255.240
Gatewa	y 10.162.9.152

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



Configuring	Resilient	Links
-------------	-----------	-------

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->8.8.8/114.114.114.114)

Jun 12 08:00:23 casecomms user.debug connection_manager[1126]: connection_manager proc_icmp_detection Jun 12 08:00:23 casecomms user.debug connection_manager[1126]: WAN ICMP detecting failed (3/3)

Jun 12 08:00:23 casecomms user.debug connection_manager[1126]:

Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: started, v1.25.1

Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: sending discover

Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: sending select for 10.169.103.152

Jun 12 08:00:28 casecomms daemon.err udhcpc[1955]: lease of 10.169.103.152 obtained, lease time 7200

Jun 12 08:00:29 casecomms user.debug udhcpc: dhcpc get configuration of wwan1

Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: connection_manager proc_connected

Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: connection_manager proc_icmp_detection Jun 12 08:00:29 casecomms user.debug connection_manager[1126]: WWAN1 ICMP detecting success



Network Security

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.

	ACL	Port Mapping	DMZ				
Gene	eral Settings						
			Default Policy	Accept	¥		
ACL	rule Setting	s					
Inde	x Des	cription Protoco	Source Address	Source Port	Destination Address	Destination Port	\oplus

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.

ACL Settings	
General Settings	
Index	1
Description	
Protocol	All
Source Address	
Destination Address	
	Save Close

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	1
Description	
Protocol	All v
Remote Address	
Remote Port	Ø
Local Address	
Local Port	
	Save Close

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 <u>DMZ</u>	
General Settings	
Enabl	e 🖉
Remote Addres	s 0.0.0.0/0 ⑦
DMZ Host Addres	s

- 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.

								Login: admin Reboot	Logout
Overview	General	Accounts	Syslog	Web Server	Telnet	SSH	Security		
Link Management	General Setti	ngs							
Industrial Interface				SSH Port	22				
Network			Allow Passwor	rd Authentication					
Applications				Public Key					
								Login: admin Reboot	Logout
Overview	General	Accounts	Syslog	Web Server	Telnet	SSH	Security		
Link Management	Remote Acce	ss Settings							
Industrial Interface					8				
Network				te HTTPS Access					
Applications				ote Teinet Access					
VPN			Re	mote SSH 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:

PuTTY Key Generator		×
		~
File Key Conversions Help		
Кеу		
No key.		
Actions Generate a public/private key pair	ſ	Generate
Generate a public/private key pair	L	Generate
Load an existing private key file		Load
Save the generated key	 Save public key	Save private key
Parameters		
Type of key to generate:	O ED25519	◯ SSH-1 (RSA)
Number of bits in a generated key:		2048

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

								Login: admin Reboot Logout
Overview	General	Accounts	Syslog	Web Server	Teinet	SSH	Security	
Link Management	General Setti	ings						
Industrial Interface				SSH Port	22			
Network			Allow Passwo	rd Authentication	8			
Applications				Public Key	ssh-rsa AAA837	kwClyc2644		



Network Security

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

PuTTY Key Generato	or		×						
File Key Conversions	Help								
Key									
Public key for pasting in	ito OpenSSH authorize	d_keys file:							
Zr2zCQvwgVfXAmg7+	LwyWEzOrm6kAPSdD								
+MMMquOsBynL2L7sh4SUDnnFXcomg0LFDvHGEn7mvVHqa4yGho/zQ/PoCEmuJVF Zq7926vrlJsglN/Meg9KZvsLuyoOApBaysDiCxo2Ux41q7MHldGGpnf9vmNv+									
+KQeEEFLOylp8mw==	rsa-key-20181008		×						
Key fingerprint:	Key fingerprint: ssh-rsa 2048 73:a7:0f:6d:e7:c9:ad:c8:a0:39:3d:ad:2f:ce:76:e3								
Key comment:	Key comment: rsa-key-20181008								
Key passphrase:									
Confirm passphrase:									
Actions									
Generate a public/priva	te key pair		Generate						
Load an existing private	key file		Load						
Save the generated key	1	Save public key	Save private key						
Parameters									
Type of key to generate	e: DSA OECDS	SA () ED25519	◯ SSH-1 (RSA)						
Number of bits in a gen	erated key:		2048						

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:

聲 PuTTY Configurati	on	×					
Category:							
	^	Options controlling SSH authentication					
Logging Terminal Keyboard		Display pre-authentication banner (SSH-2 only) Bypass authentication entirely (SSH-2 only)					
- Bell Features Window - Appearance - Behaviour - Translation		Authentication methods					
		Attempt authentication using Pageant Attempt TIS or CryptoCard auth (SSH-1) Attempt "keyboard-interactive" auth (SSH-2)					
Colours		Authentication parameters					
Connection Data Proxy		Allow agent forwarding Allow attempted changes of username in SSH-2 Private key file for authentication:					
Telnet Rlogin SSH Kex		Browse					
- Host keys							
-X11 Tunnels	\sim						
About		Open Cancel					

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



Rev 2.8

🛃 PuTTY Configurat	tion			×
Category:				
Session Logging Terminal Keyboard Bell Features Window Appearance Behaviour	^	Basic options Specify the destination Host Name (or IP addr 192.168.5.2 Connection type: Raw Telnet Load, save or delete a s		
 Translation Selection Colours Connection Data Proxy Telnet Rlogin SSH Kex 		Saved Sessions Default Settings		Load Save Delete
- Host keys - Cipher ⊕ Auth - TTY - X11 - Tunnels	~	Close window on exit: Always Neve	er Only on 	clean exit
About			Open	Cancel

Step 3: Test successful.

192.168.5.2 - Putty	-	Х
Login as: admin Authenticating with public Key "rsa-key-20181008"		



Rev 2.8



This page left blank intentionally



Rev 2.8

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 R	oute			
Route Ta	ble Informati	on			
Index	Destination	Netmask	Gateway	Metric	Interface
1	192.168.5.0	255.255.255.0	0.0.0	0	lan0
Route	e->Route	Table Informa	ntion		

- **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	1		
Description			
IP Address			
Netmask			
Gateway			
Interface		0	
		Save	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#



Step 2: Checking the 6944 Routing table for reference

							Reboot	Logout
Overview	Statu	Static Route	RIP	OSPF	BG			
Link Management	Route T	able Information						
Industrial Interface	Index	Destination	Netroak	Gateway	Hetric	Interface		
Network	1	0.0.0.0	0.0.0.0	192.198.111.11	0	wan		
Frend	2	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0		
Resta	5	192.168.50.0	255.255.255.0	192.168.111.200	20	-wan		
VRRP	4	192.168.111.0	255.255.255.0	0.0.0.0	0	and the		

Testing

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

CISC07200#ping 192.168.5.1		
Type escape sequence to abort. Sending 5, 100-byte ICMP Echos to !!!!! Success rate is 100 percent (5/5) CISCO7200#		

Step 2: Test successful.

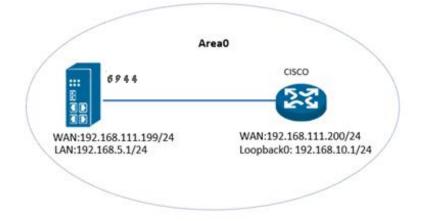
9.2. Dynamic Routing Using RIP

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	First release
			Software V1.0.1 642848	

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.



Section Nine

Routing

Rev 2.8

Configuration CISCO Configuration

CISCO7200#show running-config interface FastEthernet0/0 Building configuration... ip address 192.168.111.200 255.255.255.0 Current configuration : 1165 bytes duplex auto speed auto upgrade fpd auto 1 interface FastEthernet0/1 version 12.4 service timestamps debug datetime msec no ip address service timestamps log datetime msec shutdown no service password-encryption duplex auto speed auto 1 hostname CISCO7200 ! router rip version 2 boot-start-marker boot-end-marker network 192.168.10.0 network 192.168.111.0 1 no aaa new-model no auto-summary no ip icmp rate-limit unreachable ! ip cef line con 0 exec-timeout 0 0 no ip domain lookup privilege level 15 ip auth-proxy max-nodata-conns 3 logging synchronous ip admission max-nodata-conns 3 stopbits 1 line aux 0 multilink bundle-name authenticated exec-timeout 0 0 ١ privilege level 15 logging synchronous archive stopbits 1 log config hidekeys line vty 04 login 1 ip tcp synwait-time 5 ! ! interface Loopback0 end ip address 192.168.10.1 255.255.255.0 CISCO7200# ١

6944 Configuration

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

ase	Status	Static Rou		OSPF	BGP		Reboot	Logout	
rview			te <u>RIP</u>	USPF	BOP				
	RIP Setting	6		Enable	8				
strial Interface				Version	RIPv2				
xk wal				Neighbor	RUP92				
-				Default Metric					G4 A
9				Distance	120				Step 2:
ations				Update Interval	30				Click
				Timeout					CIICK
tenance			-		180				Save>App
				bage Collect Time	120	•			Save>np
				ute Kernel Routes	8				
				sute Static Routes	8				
		Er	while Redistribute (8				
				Log Level	Debug	·			
	Network Se								
	Index D	Nescription	Network					•	
	2		192.168.5.0/24					88	
	1		192.358.111.0/24					88	
	Interfaces 1								
	Index Into	erface Enable	Passive Split-horiz	10m				\odot	



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 CISCO/200#

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

case a								Reboot	Logeut
Overview	Status	Static Route	RIP	OSPF	BG	Р			
Link Management	Route Ta	able Information							
Industrial Interface	Index	Destination	Netmask	Gateway	Metric	Interface			
Vetwork	1	0.0.0.0	0.0.0.0	192.168.111.11	0	wan			
Frenal	2	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0			
Ente	3	192.168.10.0	255.255.255.0	192.168.111.200	20	wan			
VRRP	4	192.168.111.0	255.255.255.0	0.0.0.0	0	wan			
Applications									

Testing

Step 1: Ping from CISCO to 6944

Step 2: Test successful.

CISC07200#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/ CISCO7200#	max =	8/18/36 ms

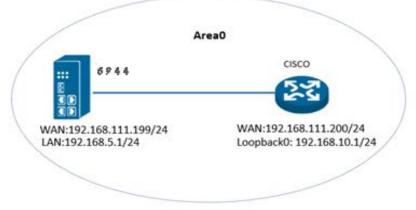
9.3. Dynamic Routing Using OSPF

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 ١ Building configuration... Current configuration : 1218 bytes upgrade fpd auto version 12.4 service timestamps debug datetime msec ١ 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 ۱ multilink bundle-name authenticated archive log config hidekeys ١ 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 end 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 00 privilege level 15 logging synchronous stopbits 1 line vty 04 login CISCO7200

6944 OSPF Configuration

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

						Logist adm	a second s
						Reboot	Logout
w	Status	Static Route	RIP	OSPF	BGP		
anagement	OSPF Settin	gs.					
al Interface				Enable	8		
K				Router ID	1.1.1.1		
				Default Metric	4		
				Distance	120		
ions		En	able Redistribu	te Kernel Routes	8		
~~~		Er	nable Redistribs	ute Static Routes	8		
ance		Enable	Redistribute C	onnected Routes	8		
warkce				Log Level	Dribug *		
1	Network Se	ttings		100			
1	- and a second s		Network	Area			
	2		1368.5.0/24	0			Ø
	1		168.111.0/24	0			ß
	Interfaces S						
	Index Inte	orface Enable Passio	en Cent				





#### **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 NI - 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
<pre>C 192.168.111.0/24 is directly connected, FastEthernet0/0 C 192.168.10.0/24 is directly connected, Loopback0 0 192.168.5.0/24 [110/11] via 192.168.111.199, 00:17:32, FastEthernet0/0 CISCO7200#</pre>

Check the 6944 routing table for reference.

							Login: admin Reboot Logout
Overview	Statu	static Ro	ute RIP	OSPF	BG	P	
Link Management	Route T	able Informatio	a				
Industrial Interface	Index	Destination	Netmask	Gabeway	Metric	Interface	
Network	1	0.0.0.0	0.0.0.0	192.168.111.11	0	wan	
Freval	2	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0	
> Roste	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	
111.1	192.168.5.1, timeout is 2 seconds: round-trip min/avg/max = 4/344/988 ms

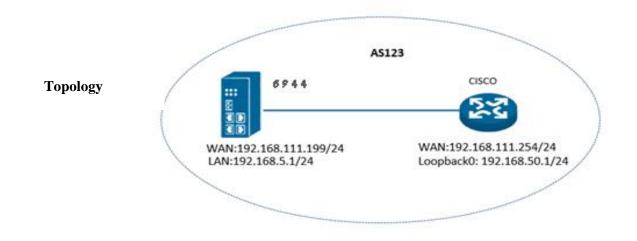
# 9.4. Dynamic Routing Using BGP

#### 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

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



### 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 ١ hostname CISCO7200 1 boot-start-marker boot-end-marker 1 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 ۱ multilink bundle-name authenticated archive log config hidekeys ip tcp synwait-time 5 interface Loopback0 ip address 192.168.50.1 255.255.255.0 interface FastEthernet0/0 ip address 192.168.111.254 255.255.255.0 #

duplex auto speed auto 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

**Configuration Continued** 



#### 6944 BGP Configuration

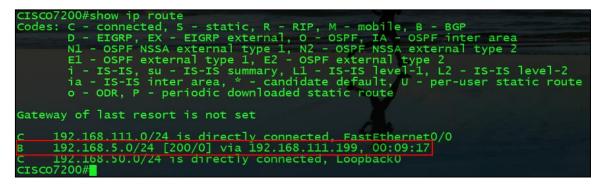
Step 1: Go to Network>Route>BGP, enable BGP and configure BGP as below picture.



Step 2: Click Save>Apply.

#### Checking the Routing Tables

Step 1: Check the 7200 Routing Table for reference



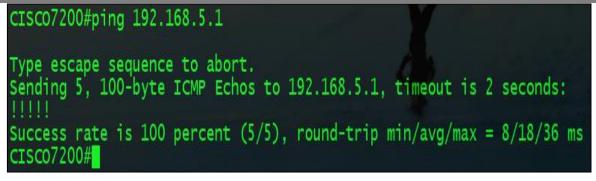
Step 2: Checking the 6944 Routing table for reference

							Legini admin Roboot	Logeut
Overview	Status	Static Route	RIP	OSPF	BG	2		-
Link Management	Route Ta	ble Information						
Industrial Interface	Index	Destination	Netreak	Gateway	Hetric	Interface		
Network	1	0.0.0.0	0.0.0.0	192.198.111.11	0	wan		
Frewal	2	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0		
► Reals	þ	192.168.50.0	255.255.255.0	192-168.111.200	20	wan		
VRRP	4	192.168.111.0	255.255.255.0	0.0.0.0	0	anget.		

#### Testing

Ping from the CISCO router to the 6944 Router:

Test Successful







# 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.

onfiguration Options			
VRRP			
VRRP Network Settings			
Index	1		
Enable			
Interface	LANO	•	
Virtual Router ID	1		
Authentication Type	None	• ?	
Priority	100		
Interval	1		
Virtual IP Address			
		Save	Close
		Jure	

- 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.

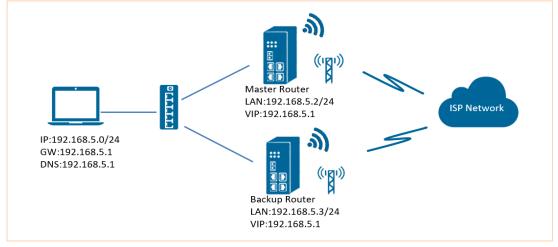


# **10.1.** Configuring VRRP between Two 6944 Routers

#### 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 T
	IP Address	192.168.5.2
	Netmask	255.255.255.0
	MTU	1500
DHCP Settings		
	Enable	
	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 VRRP Edit button, as shown below.



								Legin: admin Reboot Legout
Overview	VRF	RP.						
Link Management	VRRP	Network S	Settings					
Industrial Interface	Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address	0

Step 3: Configure VRRP as shown below:

VRRP	
VRRP Network Settings	
Index	1
Enable	
Interface	LAN0 •
Virtual Router ID	1
Authentication Type	None •
Priority	120
Interval	1
Virtual IP Address	192.168.5.1
	Save Close

**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	1
Interface	LAN0 T
IP Address	192.168.5.3
Netmask	255.255.255.0
MTU	1500
DHCP Settings	
Enable	
Mode	Server 🔻
IP Pool Start	192.168.5.11
IP Pool End	192.168.5.20
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 VRRP Edit button as shown below:



								Login: admin Reboot	Logout	
Overview	VRF	RP.								
Link Management	VRRP	Network S	Settings							
Industrial Interface	Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address			0

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	$\times$			
General					
You can get IP settings assigned autom this capability. Otherwise, you need to for the appropriate IP settings.					
Obtain an IP address automaticall	у				
Use the following IP address:		-1			
IP address:	192 . 168 . 5 . 20				
Subnet mask:	255 . 255 . 255 . 0				
Default gateway:	192.168.5.1				
Obtain DNS server address autom	atically				
Use the following DNS server add	resses:	-1			
Preferred DNS server:	192.168.5.1				
Alternate DNS server:					
Validate settings upon exit Advanced					
	OK Cance	<u>!</u>			



Section Ten

#### **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							
1.1ms1ms(192.168.5.2)2.85ms89ms130mslogon (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	-	$\times$
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 <mark>\tracert 8.8.8.8</mark>		
Tracing route to 8.8.8.8 over a maximum of 30 hops		
1 1 ms * 1 ms 192.168.5.3 2 220 ms 227 ms 238 ms 10.241.157.57 3		

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

11 Ad	Invisionation: C	ommand Pror	npt - tracer	1 8888	
		istrator) istrator		8, 8, 8	
Reply Reply Reply	from 8,8 from 8.8 from 8.8	.8.8: byte .8.8: byte	es=32 ti es=32 ti es=32 ti	of data: ime=327ms TTL=41 ime=110ms TTL=41 ime=60ms TTL=41 ime=105ms TTL=41	Test Successful
P	ackets: S ximate ro	und trip	Received times in	d = 4. Lost = 0 (0% loss), n milli-seconds: 327ms, Average = 150ms	i est duccessiui
C:\Us	ers\Admin	istrator	tracert	8.8.8.8	
		to google of 30 ho		-dns-a.google.com [8.8.8.8]	
12	1 ms	1 ms	1 ms	[192.168.5.2] Request timed out.	

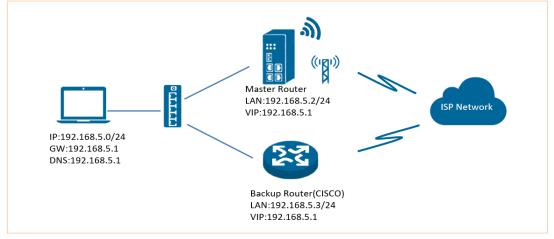


# **10.2.** Configuring VRRP Between 6944 and Cisco Routers

#### 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	
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 of								Legist admin Reboot	Logout	
Overview	VRF	P								
Link Management	VRRP	VRRP Network Settings								
Industrial Interface	Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address		0	



____

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

VRRP		
VRRP Network Settings		
Index	1	
Enable		
Interface	LAN0 •	
Virtual Router ID	1	
Authentication Type	None 🔻	0
Priority	120	
Interval	1	
Virtual IP Address	192.168.5.1	
		Save Close

#### **Backup Router (CISCO) Configuration**

The configuration on CISCO router as shown below

cisco2811# interface FastEthernet0/0 cisco2811#show run Building configuration... ip nat outside Current configuration : 3316 bytes ip nat enable 1 version 12.4 duplex full speed auto service timestamps debug datetime msec service timestamps log datetime msec no mop enabled no service password-encryption crypto map MAP hostname cisco2811 1 boot-start-marker ip nat inside boot-end-marker ip nat enable 1 logging message-counter syslog duplex auto enable secret 5 speed auto \$1\$tw/d\$UQQ3Xh06n.2HHFeAVIgXJ. no aaa new-model ip name-server 192.168.111.1 ip address-pool local no ipv6 cef no ip http server 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 end cisco2811# ۱

ip address 192.168.111.254 255.255.255.0 ip virtual-reassembly interface FastEthernet0/1 ip address 192.168.5.3 255.255.255.0 ip virtual-reassembly 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 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



#### **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	$\times$					
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	/						
Ose 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 automa	atically						
Use the following DNS server addr	esses:						
Preferred DNS server:	192 . 168 . 5 . 1						
Alternate DNS server:							
Validate settings upon exit	Advanced						
	OK Cano	el					

#### 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-16m s TTL=40
Reply from 8.8.8.8: bytes=32 time-16m s TTL=40
Reply from 8.8.8.8: bytes=32 time-16m s TTL=40
Ping statistics for 8.8.8.8:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip tim es 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
                        1ms (192.168.5.2)
    1. 1ms
               1ms
   2. 85ms 89ms 130ms logon (172.29.5.17)
   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.

```
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-16m s TTL=40
Reply from 8.8.8.8: bytes=32 time-16m s TTL=40
Reply from 8.8.8.8: bytes=32 time-16m s TTL=40
Ping statistics for 8.8.8.8:
Packets: sent = 4, Received = 4, Lost=0 (0% loss)
Approximate round trip tim es 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
              *
                        1ms (192.168.5.3)
       lms
   2 230ms 227ms 130ms logon (10.241.157.57)
    3
```

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



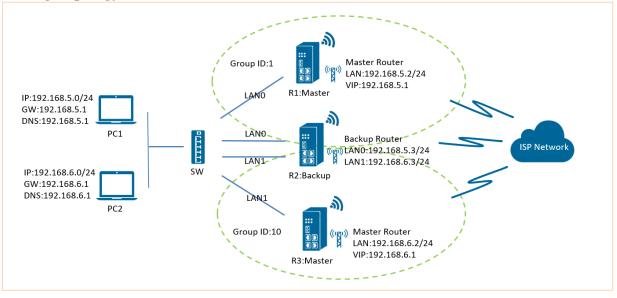


#### 10.3. **VRRP Between Multiple 6944 Routers**

#### **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

**<u>R1 Master Router Configuration</u>** 

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

General Settings			
	Index	1	
[	Interface	LANO	•
	IP Address	192.168.5.2	
	Netmask	255.255.255.0	
	MTU	1500	
DHCP Settings			
	Enable		
	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		

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

case of								Kepint admin Reboot Logout	
Overview	V	RRP							
Link Management	VRRP	Network S	ettings						
Industrial Interface	Index	Enable	Interface	Vetual Router ID	Piority	Interval	Virtual IP Address		0

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

VRRP			
VRRP Network Settings			
Index	1		
Enable			
Interface	LAN0 •		
Virtual Router ID	1		
Authentication Type	None 🔻	?	
Priority	120		
Interval	1		
Virtual IP Address	192.168.5.1		
		Save	Close



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

					Login: admin Reboot Log	pout
Overview	Status	Por	t Assignment	LAN		
Link Management	General	Settings				
Connection Manager Cellular	Index	Port	Interface			
► Ebernet	1	Etho	LANO			2 2
W5	2	Eth1	LANO			
Port Setting	5					
General Sett	ings					
				Index	2	
				Port	Eth1 v	
			Int	erface	LAN1 •	
					Save Clos	e

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

LAN Settings			
General Settings			
_	Index	2	_
	Interface	LAN1 •	1
	IP Address	192.168.6.2	
	Netmask	255.255.255.0	
	MTU	1500	
DHCP Settings			
	Enable		
	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	
Sec	condary DNS		
	WINS Server		
Stop 2. Co to Notworks VD			Save

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

								Logia; admin Reboot	Logout	
Overview	VRF	<u>s</u> p								
Link Management	VRRP	VRRP Network Settings								
Industrial Interface	Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address		٥	



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

	VRRP									
<u>R2 Backup</u>	VRRP Network Settings									
	Index 2									
	Enable 🗹									
D' Dooluun	Interface LAN1 🔻	Doutor								
K2 Dackup	Virtual Router ID 10	<u>Router</u>								
	Authentication Type None 🔻 🧿									
	Priority 120									
	Interval 1									
	Virtual IP Address 192.168.6.1									
	Save Close									

#### **Configuration**

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

					Legint admin Reboot Legent	
Overview	Status	Por	t Assignment	LAN		
Link Management	General Se	ettings				
Connection Manager Cellular	Index	Port	Interface			
► Ehmet		EthO	LANO			ß
W5	2	Eth1	LAND			
Port Setting General Set						
				Index	2	
				Port	Eth1 🔻	
			Int	erface	LAN1 •	
					Save Close	

**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

LAN Settings				
General Settings				
_	Index	1		
	Interface	LAN0	•	
	IP Address	192.168.5.3		
L	Netmask	255.255.255.0		
	MTU	1500		
DHCP Settings				
_	Enable			
	Mode	Server	•	1
	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		
Sec	condary DNS			
,	WINS Server			
				Save



**Rev 2.8** 

General Settings			
5	Index	2	
	Interface	LAN1	•
	IP Address	192.168.6.3	
	Netmask	255.255.255.0	
	MTU	1500	
DHCP Settings			
	Enable		
	Mode	Server	•
	IP Pool Start	192.168.6.21	
	IP Pool End	192.168.5.200	
	Netmask	255.255.255.0	
	Lease Time	120	
	Gateway	192.168.6.1	
	Primary DNS	192.168.6.1	
S	econdary DNS		
	WINS Server		

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

								Login: admin Reboot	Logout	
Overview	VR	P								
Link Management	VRRP	Network S	Settings							
Industrial Interface	Index	Enable	Interface	Virtual Router ID	Priority	Interval	Virtual IP Address			0

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

VRRP		
VRRP Network Set	tings	
	Index	1
	Enable	
	Interface	LAN0 T
	Virtual Router ID	1
	Authentication Type	None 🔻 🕐
	Priority	100
	Interval	1
	Virtual IP Address	192.168.5.1
		Save Close



**Rev 2.8** 

VRRP			
VRRP Network Set	tings		
	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	$\times$
General		
You can get IP settings assigned autom this capability. Otherwise, you need to a 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 automa	atically	
Use the following DNS server addr	esses:	-1
Preferred DNS server:	192.168.5.1	
Alternate DNS server:	· · ·	
Validate settings upon exit	Advanced	
	OK Cance	el

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 autom this capability. Otherwise, you need to for the appropriate IP settings.	
Obtain an IP address automatical	y
• 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 autom	atically
-• Use the following DNS server add	resses:
Preferred DNS server:	192 . 168 . 6 . 1
Alternate DNS server:	· · ·
Validate settings upon exit	Advanced
	OK Cancel



the stress during have not support the address of

**Rev 2.8** 

#### **Testing VRRP between multiple 6944's**

	States of the Line and the	ands. while come
Test on PC1: - Make sure	C:\Users\Administrator	ping 8.8.8.8
PC1 can communicate with Internet via the 6944 Master Router	Reply from 8,8,8,8; by Reply from 8,8,8,8; by	2 bytes of data: tes=32 time=98mm TTL=60 tes=32 time=52mm TTL=40 tes=32 time=58mm TTL=40 tes=32 time=51mm TTL=40
	Approximate round trip	8.8.5: Received = 4. Lost = 0 (0% loss), times in milli-seconds: ximum = 98ms, Average = 64ms
	C:\Users\Administrator	tracert 8.8.8.8
	Tracing route to googl over a maximum of 30 h	e-public-dns-m.google.com [8.8.8.8] ops:
	1 1 ms 1 ms 2 85 mi 89 mi 3	1 mm navigateworx.router [192.168.5.2] 130 mm bogon [172.29.5.17]
Administrator: Command Prompt - tracert 8.8 C:\Users\Administrator\pping 8.8.8.		
Pinging 8.8.8.8 with 32 bytes of a Reply from 8.8.8.8: bytes=32 time= Reply from 8.8.8.8: bytes=32 time= Reply from 8.8.8.8: bytes=32 time= Reply from 8.8.8.8: bytes=32 time= Reply from 8.8.8.8: bytes=32 time=	lata: 53ns TTL=40 71ns TTL=40 59ns TTL=40	Remove the Ethernet cable between the 6944 Master
Ping statistics for 8.8.8.8; Packets: Sent = 4, Received = Approximate round trip times in mi Minimum = 53ms, Maximum = 71ms	lli-seconds:	router and Switch. PC1 will access the Internet via the 6944 Backup Router
C:\Users\Administrator\tracert 8.8	. 8. 8	
Tracing route to 8.8.8.8 over a ma	ximum of 30 hops	
	2. 168. 5. 3 9. 241. 157. 57	

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

A Reply to your ping shows the link is successful.





**Rev 2.8** 

This page left blank intentionally



# 11 VPN (Virtual Private Networks)

## **11.1. OpenVPN Introduction**

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

State	us	OpenVPN X.509	Certificate				
OpenVP	N Informat	ion					
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 ⑦
Private Key Password	
Output Verbosity Level	3
Advanced Settings	
Enable NAT	





#### **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-topoint 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		2		
		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 LZO Compress the data. •
- Additional Configurations Enter some other options of OpenVPN in this field. Each . expression can be separated by a ';'.



**Open VPN** 

Status	Open\	/PN <u>X</u>	.509 Certificate		
X.509 Ce	rtificate Imp	ort			
			Connection Index	1	
			CA Certificate	Choose File No file chosen	٢
			Local Certificate File	Choose File No file chosen	\$
			Local Private Key	Choose File No file chosen	ۍ
			HMAC firewall Key	Choose File No file chosen	٢
			Pre-shared Key	Choose File No file chosen	ۍ 📃
			PKCS#12 Certificate	Choose File No file chosen	٢
X.509 Ce	rtificate 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



# 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:

Quick access	Name	Date modified	Туре	Size
Desktop *	Ccd	8/6/2018 11:46 AM	File folder	
Downloads	Ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KE
	dh2048.pem	7/31/2018 6:44 PM	PEM File	1 K
🗎 Documents 🛛 🖈	ipp.txt	8/6/2018 6:48 PM	Text Document	1 KI
E Pictures 📌	openvpn-status.log	8/6/2018 6:48 PM	Text Document	1 KI
config	n server.ovpn	8/6/2018 2:02 PM	OpenVPN Config File	11 KI
config	server01.crt	7/31/2018 5:54 PM	Security Certificate	5 K
OpenVPN Client wit	server01.key	7/31/2018 5:54 PM	KEY File	2 K

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

This	s PC > Windows (C:) >	Program Files > OpenVPN > config > ccd
~	Name	×
Name		🥘 client01 - Notepad
	client01	File Edit Format View Help
		iroute 192.168.5.0 255.255.255.0

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

#### **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

**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 •	0
Encryption Type	BF-CBC •	
Renegotiate Interval	3600	
Keepalive Interval	20	
Keepalive Timeout	60	
Fragment	1500	0
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		0
		Save Close

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

	68						Login; admin Reboot	Logeut
Overview	Status	s Open	VPN X.5	09 Certificate				
Link Management	X.509 Ce	rtificate Imp	sort		88			
Industrial Interface				Connection Index	[ ·			
etwork.				CA Certificate	Choose File No Se chosen	5		
oplications				Local Certificate File	Choose File No file chosen	3		
/PN				Local Private Key	Choose File No file chosen	3		
<ul> <li>OperVPN</li> </ul>				HMAC finewall Key	Choose File. No file chosen	3		
faintenance				Pre-shared Key	Choose File, No No choose	4		
				PKCS#12 Certificate	Choose File. No file chosen	<u>د</u>		
	X.509 Ce	rtificate File	1					
	Index	File Name	File Size	Date Modified				
	1	ca.ot	1188	Mon Aug 6 14:03:26 2018				8
	2	client.ot	4382	Mon Aug 6 14:02:33 2008				8
	2	client.key	1834	Mon Aug 6 14:03:38 2008				8

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

	1					
Overview	Stat	us	OpenVPN	X.509 Certificate		
Link Management	OpenV	PN Info	mation			
Industrial Interface	Index	Enable	Description	n Status	Uptime	Virtual IP
Network	1	true		Connected	00:00:24	10.8.0.6

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



**Open VPN** 

ctive Routes:				
etwork Destination	n Netmask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.10.1	192.168.10.10	291
0. 0. 0. 0	0. 0. 0. 0	192. 168. 111. 1	192. 168. 111. 19	291
10. 8. 0. 0	255. 255. 255. 0	10.8.0.2	10.8.0.1	35
10. 8. 0. 0	255. 255. 255. 252	On-link	10.8.0.1	291
10.8.0.1	255. 255. 255. 255	On-link	10.8.0.1	291
10.8.0.3	255. 255. 255. 255	On-link	10.8.0.1	291
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331
127.0.0.1	255. 255. 255. 255	On-link	127.0.0.1	331
127. 255. 255. 255	255, 255, 255, 255	On-link	127.0.0.1	331
192. 168. 5. 0	255. 255. 255. 0	10.8.0.2	10.8.0.1	35
192.168.10.0	255. 255. 255. 0	On-link	192.168.10.10	291
192.168.10.10	255. 255. 255. 255	On-link	192.168.10.10	291
192. 168. 10. 255	255. 255. 255. 255	On-link	192.168.10.10	291

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

Route T	able Informatio	n		
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=3ms 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	Ping	Traceroute			
Link Management	Ping Settings				
Industrial Interface			Host Add	iress 192.168	.10.10
Network			Ping C	ount 5	
Applications			Local IP Add	iress	
VPN	PING 192.168	.10.10 (192.168.10.	10): 56 data byte	s	
Maintenance Firmware Upgrade System	64 bytes from 64 bytes from	n 192.168.10.10: se n 192.168.10.10: se n 192.168.10.10: se n 192.168.10.10: se	q=1 ttl=127 time= q=2 ttl=127 time=	2.413 ms 3.849 ms	

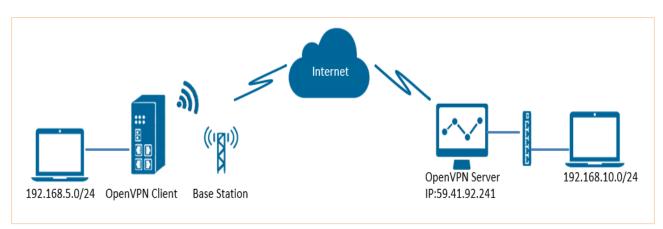


# 11.3. AN006 – 6944 Open VPN Client with X.509 Certificate.

#### 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

This	This PC > Windows (C:) > Program Files > OpenVPN > config > ccd						
~							
	Name	🧊 client01 - Notepad					
	✓ ☐ client01	File Edit Format View Help					
		iroute 192.168.5.0 255.255.255.0					

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



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

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

penVPN 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	• 0	
Encryption Type	BF-CBC	•	
Renegotiate Interval	3600		
Keepalive Interval	20		
Keepalive Timeout	60		
Fragment	1500	0	
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	<ul> <li>Image: A start of the start of</li></ul>		
Additional Configurations		0	
		Save	Close

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

								Login: admin Reboot	Logout	
Overview	Status	OpenV	PN X.	09 Certificate						
Link Management	X.509 Ce	rtificate Impo	ort							
Industrial Interface				Connection Index	1	•				
Network				CA Certificate	Choose File No file chose		5			
Applications				Local Certificate File	Choose File No file chose	n .	۵			
VPN				Local Private Key	Choose File No file chose	٥	٢			
► OpenVPN				HMAC frewall Key	Choose File No file chose	·	ۍ			
Maintenance				Pre-shared Key	Choose File No file chose		٢			
				PKCS#12 Certificate	Choose File No file chose	6	٢			
	X.509 Ce	rtificate Files								
	Index	File Name	File Size	Date Modified						
	1	ca.ot	1188	Mon Aug 6 14:03:26 2018						$\otimes$
	2	client.ort	4382	Mon Aug 6 14:03:33 2008						$\otimes$
	>	client.key	1834	Mon Aug 6 14:03:38 2008						$\otimes$



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

Overview	Stat	us	OpenVPN	X.509 Certificate		
Link Management	OpenV	PN Infor	mation			
Industrial Interface	Index	Enable	Descriptio	n Status	Uptime	Virtual IP
Network	1	true		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		
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	0
Interface	tun1	0
		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.

IPv4 Route Table				
Active Routes:				
Network Destination	n Netmask	Gateway	Interface	Metric
0. 0. 0. 0	0.0.0.0	192.168.10.1	192.168.10.10	291
0. 0. 0. 0	0.0.0.0	192.168.111.1	192.168.111.19	291
10. 8. 0. 0	$255.\ 255.\ 255.\ 0$	10.8.0.2	$10.\ 8.\ 0.\ 1$	35
10. 8. 0. 0	255. 255. 255. 252	On-link	$10.\ 8.\ 0.\ 1$	291
10. 8. 0. 1	255. 255. 255. 255	On-link	10. 8. 0. 1	291
10.8.0.3	255. 255. 255. 255	On-link	10.8.0.1	291
$127.\ 0.\ 0.\ 0$	255.0.0.0	On-link	127.0.0.1	331
127. 0. 0. 1	255. 255. 255. 255	On-link	127.0.0.1	331
127. 255. 255. 255	255. 255. 255. 255	On-link	127.0.0.1	331
192.168.5.0	$255.\ 255.\ 255.\ 0$	10.8.0.2	$10.\ 8.\ 0.\ 1$	35
$192.\ 168.\ 10.\ 0$	$255.\ 255.\ 255.\ 0$	On-link	192.168.10.10	291
192. 168. 10. 10	255. 255. 255. 255	On-link	192. 168. 10. 10	291
192.168.10.255	255.255.255.255	On-link	192.168.10.10	291

Check the Routing Table on the OpenVPN Client for reference.

Route 1	able Informatio	on		
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
Open VPN

#### 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.

<b>Case</b>	$\sim$	
Overview	Ping Traceroute	
Link Management	Ping Settings	
Industrial Interface	Host Address 192.168.10.10	
Network	Ping Count 5	
Applications	Local IP Address	
VPN	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	
Maintenance Firmware Upgrade System	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.



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

#### Introduction

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

#### Configuration

#### Installing OpenVPN Software

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

#### **Generating Certificates**

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



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

Administrator: Command Prompt -	Х
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 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.

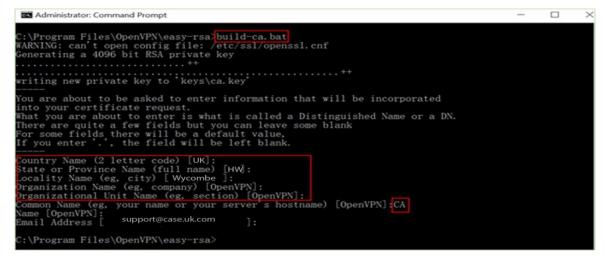


-1	0 1	
1	@echo off	
2	rem Edit this variable to point to	
3	rem the openssl.cnf file included	
4	rem with easy-rsa.	
5	-	
6	rem Automatically set PATH to openssl.e	X0
7		
	FOR /F "tokens=2*" <a "<="" ("reg="" in="" query="" td=""><td>HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"</td></a>	HKEY_LOCAL_MACHINE\SOFTWARE\OpenVPN"') DO set "PATH=%PATH%;%%b\bin"
8		
9	rem Alternatively define the PATH to op	enssl.exe manually
10	rem set "PATH=%PATH%;C:\Program Files\C	penVPN\bin"
11		
12	set HOME=%ProgramFiles%\OpenVPN\easy-rs	a
13	set KEY CONFIG=openssl-1.0.0.cnf	
14	Sec NEI_CONFIG=OpenSSI 1.0.0.CHI	
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	
	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		
31	set DH_KEY_SIZE=2048	
32	rem Private key size	
33	set KEY_SIZE=4096	
34		
35	rem These are the default values for fi	elds
36	rem which will be placed in the certifi	cate.
37	rem Change these to reflect your site.	
38	rem Don't leave any of these parms blan	k.
39		
40	set KEY COUNTRY=CN	
41	set KEY_PROVINCE=GD	
42	<pre>set KEY_CITY=Guangzhou</pre>	
43	set KEY_ORG=OpenVPN	
44	<pre>set KEY_EMAIL=mail@navigateworx.domain</pre>	
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.



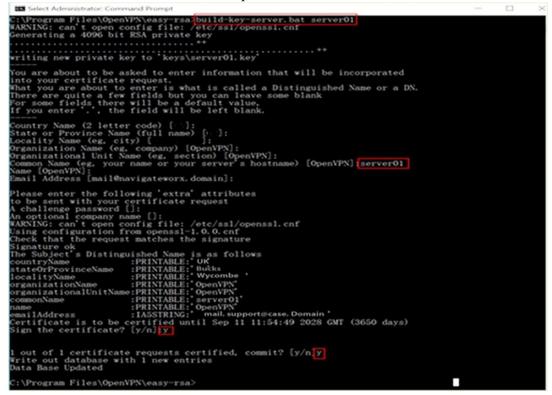
**Step 5** - The command (**build-ca.bat**) will build the certificate authority(CA) certificate and the private key by invoking the interactive openssl command.





*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.



*Note:* <u>server01</u> 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	- 0	>
C:\Program Files\OpenVP\\easy-rsa\build-key-pass.bat clientO WARNING: can't open config file: /etc/ssl/openssl.cnf Generating a 4096 bit RSA private key 	Private Key Password	
You are about to be asked to enter information that will be into your certificate request. What you are about to enter is what is called a Distinguishe 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) [OpenV Name [OpenVPN]; Email Address [mail@navigateworx.domain];	PN] [clientOl]	
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: UK localityName : PRINTABLE: High Wycombe organizationName : PRINTABLE: OpenVPN' commonName : PRINTABLE: OpenVPN' commonNam	T (3650 days)	
l 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:* <u>*client01*</u> in "build-key-pass.bat client01" is the file name of the certificate(the name of public key and private key). Always use a unique common name for each client.

Step 8. Generate Diffie Hellman parameters.

C Administrator: Command Prompt	-	×
C:\Program Files\OpenVPN\easy-rsa\build-dh.bat WARNING: can't open config file: /etc/ssl/openssl.cnf Generating DH parameters, 4096 bit long safe prime, generator 2 This is going to take a long time +		
+		•••
+		
·····		•••
		 •••
	• • • • • •	•••
++.		 
+		•••
+		
++*+*		
C:\Program Files\OpenVPN\easy-rsa>		

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

This P	C > Windows (C:) > Program Files	; > OpenVPN > easy-rsa > keys		✓ U Sea
[	Name	<ul> <li>Date modified</li> </ul>	Туре	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
r	📮 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
าร	client01.csr	9/14/2018 8:05 PM	CSR File	2 KB
sh	Client01.key	9/14/2018 8:05 PM	KEY File	4 KB
	🗋 dh4096.pem	9/14/2018 8:15 PM	PEM File	1 KB
at	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

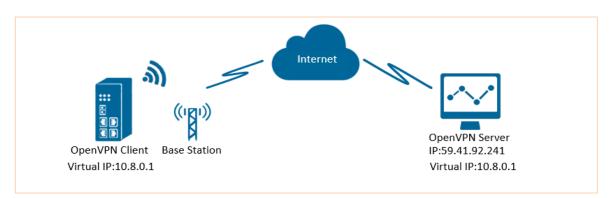


# 11.5. AN007-Configuring an Open -VPN Client with a Pre-shared Key

#### 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 <u>static</u> 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:

This PC > Windows (C:) > Program Files > OpenVP	N > config	~ U	Search con 👂
↑ Name	Date modified	Туре	Size
pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB
server.ovpn	8/7/2018 9:59 AM	OpenVPN Config File	11 KB

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.



OpenVPN Settings	
General Settings	
Index	1
Enable	
Description	
Mode	P2P •
Protocol	UDP •
Connection Type	TUN 🔻
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC V
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
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	0
	Save Close

#### Step 2. Click Save>Apply.

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

Overview	Status	OpenV	PN X.5	09 Certificate			
Link Management	X.509 Ce	rtificate Impo	rt				
Industrial Interface				Connection Index	1	•	
Network				CA Certificate	Choose File	No file chosen	ి
Applications				Local Certificate File	Choose File	No file chosen	త
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	3
				PKCS#12 Certificate	Choose File	No file chosen	త
	X.509 Ce	rtificate Files					
	Index	File Name	File Size	Date Modified			
	1	pre-shared.key	636	Tue Aug 7 09:57:59 2018			

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

Overview	Stat	us	OpenVPN	X.509 Certificate			
Link Management	OpenV	PN Infor	mation				
Industrial Interface	Index	Enable	Description	n Status	Uptime	Virtual IP	
Network	1	true		Connected	00:00:10	10.8.0.2	

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



**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	0	
Interface	tun1	0	

**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	n Netmask	Gateway	Interface	Metric
0. 0. 0. 0	0. 0. 0. 0	192. 168. 111. 1	192. 168. 111. 19	291
0. 0. 0. 0	0. 0. 0. 0	192, 168, 10, 1	192.168.10.10	291
10.8.0.0	255. 255. 255. 252	On-link	10. 8. 0. 1	291
10.8.0.1	255. 255. 255. 255	On-link	10.8.0.1	291
10.8.0.3	$255.\ 255.\ 255.\ 255$	On-link	10.8.0.1	291
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331

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

Route T	able Informatio	n		
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	0.0.00	tun1
3	192.168.5.0	255.255.255.0	0.0.00	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.

Overview	Ping	Traceroute	
Link Management	Ping Setting	15	
Industrial Interface		Host Address	10.8.0.1
Network		Ping Count	5
Applications		Local IP Address	
VPN		.1 (10.8.0.1): 56 data bytes	
Maintenance Firmware Upgrade System Configuration	64 bytes fr 64 bytes fr 64 bytes fr 64 bytes fr	om 10.8.0.1: seq=0 ttl=128 time=3.077 ms om 10.8.0.1: seq=1 ttl=128 time=3.567 ms om 10.8.0.1: seq=2 ttl=128 time=3.259 ms om 10.8.0.1: seq=3 ttl=128 time=2.571 ms om 10.8.0.1: seq=4 ttl=128 time=3.347 ms	
<ul> <li>Debug Tools</li> </ul>	5 packets t	<pre>l ping statistics ransmitted, 5 packets received, 0% packet min/avg/max = 2.571/3.164/3.567 ms</pre>	loss

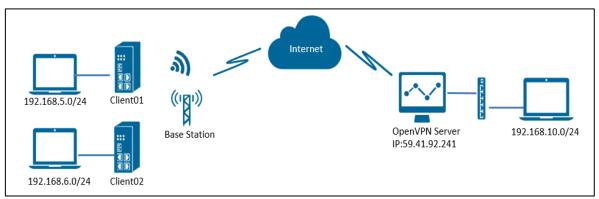


# 11.6. AN008-Open VPN Client with Username and Password

### 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:

This P	C 👂 Windows (C:) 👂 Progra	m Files » OpenVPN » config	ٽ ~	Search con 🔎
<b>^</b> [	Name ^	Date modified	Туре	Size
	尾 ccd	8/7/2018 2:30 PM	File folder	
	auth.exe	8/1/2018 2:51 PM	Application	55 KB
	🙀 ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB
	dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB
$\leq$	ipp.txt	8/7/2018 2:57 PM	Text Document	1 KB
	openvpn-status.log	8/7/2018 3:46 PM	Text Document	1 KB
	password.txt	8/7/2018 1:57 PM	Text Document	1 KB
	n server.ovpn	8/7/2018 2:57 PM	OpenVPN Config File	12 KB
	server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB
	server01.key	7/31/2018 5:54 PM	KEY File	2 KB

Note: a) Download OpenVPN software with: <a href="https://openvpn.net/">https://openvpn.net/</a>

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** 

**Open VPN** 

Name	File Edit Format View Help
client01	iroute 192.168.5.0 255.255.255.0 push "route 192.168.6.0 255.255.255.0"
	Client02 - Notepad File Edit Format View Help
	iroute 192.168.6.0 255.255.255.0 push "route 192.168.5.0 255.255.255.0"

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

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

openvpn-status.ld	og 8	/7/2018 3:46 PM	Text Document
✓  password.txt	8	/7/2018 1:57 PM	Text Document
<ul> <li>♀ server.ovpn</li> <li>♀ server01.crt</li> <li>☐ server01.key</li> </ul>	password.txt - Notepad File Edit Format View Help client01 123456789 1 client02 12345678 1		

*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



Step 1. Go to VPN>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 V
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 7							
Overview	Status	Open	VPN X.5	09 Certificate			
Unk Management	X.509 Ce	rtificate Imp	ort				
Industrial Interface				Connection Index	1	•	
Network				CA Certificate	Choose File	No file chosen	4
Applications				Local Certificate File	Choose File	No file chosen	ٹ
VPN				Local Private Key	Choose File	No file chosen	4
OperVPN				HMAC firewall Key	Choose File	No file chosen	3
Maintenance				Pre-shared Key	Choose File	No file chosen	4
				PKCS#12 Certificate	Choose File	No file chosen	3
	X.509 Ce	stificate File	3				
	Index	File Name	File Size	Date Modified			
	1	ca.crt	1183	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.

Overview	Stat	us	OpenVPN	X.509 Certificate		
Link Management	OpenV	PN Info	rmation			
Industrial Interface	Index	Enable	Descriptio	n Status	Uptime	Virtual IP
Network	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.



**Open VPN** 

**Rev 2.8** 

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

**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	
Description	
Mode	Client •
Protocol	UDP •
Connection Type	TUN 🔻
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Password •
Encryption Type	BF-CBC V
Username	client02
Password	12345678
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500 ⑦
Output Verbosity Level	3
Advanced Settings	
Enable NAT	
Enable HMAC Firewall	
Enable Compression LZ0	
Additional Configurations	0
	Save Close

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

Overview	Status	Open	VPN X.5	09 Certificate			
Link Management	X.509 Cer	rtificate Imp	ort				
Industrial Interface				Connection Index	1	•	
Network				CA Certificate	Choose File	No file chosen	ి
Applications				Local Certificate File	Choose File	No file chosen	ۍ 📄
VPN				Local Private Key	Choose File	No file chosen	3
► OpmVPN				HMAC firewall Key	Choose File	No file chosen	3
Maintenance				Pre-shared Key	Choose File	No file chosen	3
				PKCS#12 Certificate	Choose File	No file chosen	3
	X.509 Ce	rtificate File					
	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.



**Rev 2.8** 

casex						
Overview	Stat	us	OpenVPN	X.509 Certificate		
Link Management	OpenV	PN Info	mation			
Industrial Interface	Index	Enable	Descriptio	on Status	Uptime	Virtual IP
Network	1	true	user-pas	s 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		
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	0
Interface	tun1	0
		Save Close

**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 Destinatio	n 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
109 109 10 10	ALL ALL ALL ALL	0 - 1 - 1	100 100 10 10	901

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

Route T	able Informatio	on		
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	tun1
4	192.168.5.0	255.255.255.0	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	0.0.00	wan

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



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

<u>Testing</u> Step 1: Ping from Client01 to Client02 and check the result as shown below:

Overview	Ping	Traceroute	
Link Management	Ping Setting	S	
Industrial Interface		Host Address	192.168.6.1
Network		Ping Count	5
Applications		Local IP Address	
VPN		8.6.1 (192.168.6.1): 56 data bytes	
Maintenance		om 192.168.6.1: seq=0 ttl=64 time=5.255 ms om 192.168.6.1: seq=1 ttl=64 time=6.237 ms	
Firmware Upgrade Swstem		om 192.168.6.1: seq=2 ttl=64 time=5.052 ms om 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

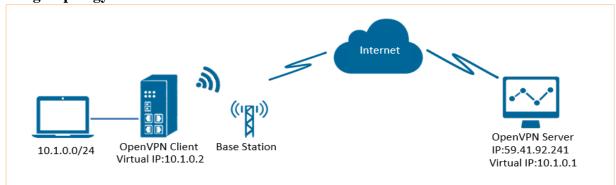


## 11.7. AN009-Open VPN Client Running TAP Pre-shared key P2P Mode

### 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:

Th	is PC > Windows (C:) > Program Files > OpenVPN	> config		~
^	Name ^	<ul> <li>Date modified</li> </ul>	Туре	Size
	openvpn-status.log	8/8/2018 10:02 AM	Text Document	1 KB
		8/8/2018 9:18 AM	OpenVPN Config File	1 KB
	pre-shared.key	8/1/2018 11:18 AM	KEY File	1 KB

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



#### **Client Configuration**

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

OpenVPN Settings	
General Settings	
Index	1
Enable	
Description	
Mode	P2P •
Protocol	UDP 🔻
Connection Type	TAP 🔻
Server Address	59.41.92.241
Server Port	1194
Authentication Method	Pre-shared Key
Encryption Type	BF-CBC •
Local IP Address	10.1.0.2
Local Netmask	255.255.255.0
TAP Bridge	LAN0 V
Renegotiate Interval	3600
Keepalive Interval	20
Keepalive Timeout	60
Fragment	1500 ⑦
Output Verbosity Level	3
Advanced Settings	
Enable NAT	
Enable HMAC Firewall	
Enable Compression LZ0	
Additional Configurations	
	Save Close
	Save

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

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

Overview	Statu	s OpenV	PN <u>X.5</u>	09 Certificate			
Link Management	X.509 C	ertificate Impo	ort				
Industrial Interface				Connection Index	1	•	
Network				CA Certificate	Choose File	No file chosen	<b></b>
Applications				Local Certificate File	Choose File	No file chosen	3
VPN				Local Private Key	Choose File	No file chosen	3
<ul> <li>OpenVPN</li> </ul>				HMAC firewall Key	Choose File	No file chosen	3
IPSec				Pre-shared Key	Choose File	No file chosen	3
Maintenance				PKCS#12 Certificate	Choose File	No file chosen	3
	X.509 C	ertificate Files	N.				
	Index	File Name	File Size	Date Modified			
	1	pre-shared.key	636	Wed Aug 8 09:22:45 2018			

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

Overview	Stat	us	OpenVPN	X.509 Certifie	cate	
Link Management	OpenV	PN Infor	mation			
Industrial Interface	Index	Enable	Descripti	ion Status	Uptime	Virtual IP
Network	1	true		Connect	ed 00:15:58	10.1.0.2

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



**Open VPN** 

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	0	
		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 2	$255.\ 255.\ 255.\ 255$	On-link	$10.\ 1.\ 0.\ 1$	291
10. 1. 0. 255 2	$255.\ 255.\ 255.\ 255$	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	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

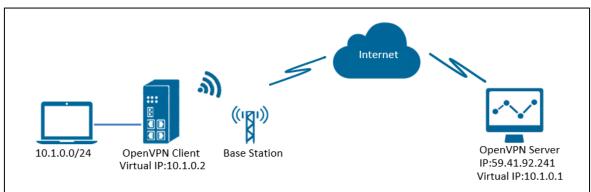
This document contains information regarding the configuration and use of a 6944 Industrial router running OpenVPN with TAP running under P2P mode,

#### **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:

This PC > Windows (C:) > Program Files > OpenVPN > config					
^ □ Name	Date modified	Туре	Size		
📮 ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KB		
🗋 dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KB		
openvpn-status.log	8/7/2018 7:57 PM	Text Document	0 KB		
ρ2p-server-tap-x509.ovpn	8/7/2018 7:57 PM	OpenVPN Config File	1 KB		
🙀 server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KB		
server01.key	7/31/2018 5:54 PM	KEY File	2 KB		

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

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



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

#### **Router Configuration**

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

OpenVPN 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 T
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	
	Save Close

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



**Open VPN** 

**Rev 2.8** 

Overview	Status	Open	VPN X.5	09 Certificate		
Link Management	X.509 Cert	ificate Imp	ort			
Industrial Interface				Connection Index	1	
Network				CA Certificate	Choose File No file chosen	3
Applications				Local Certificate File	Choose File No file chosen	- 4
VPN				Local Private Key	Choose File No file chosen	3
<ul> <li>OpenVPN</li> </ul>				HMAC firewall Key	Choose File No file chosen	3
1PSec				Pre-shared Key	Choose File No file chosen	3
Maintenance				PKCS#12 Certificate	Choose File No file chosen	4
	X.509 Cert	ificate File				
	Index	File Name	File Size	Date Modified		
	1	ca.crt	1188	Tue Aug 7 17:39:32 2018		
	2	client.ort	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.

Overview	Stat	us	OpenVPN	X.5	09 Certificate		
Link Management	OpenV	PN Info	mation				
Industrial Interface	Index	Enable	Descripti	on	Status	Uptime	Virtual IP
Network	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.

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	0
Interface	tun1	0
		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** 



#### **Routing Table**

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

IPv4 Route Tabl	e 			
Active Routes:				
Network Destina	tion 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. 2	55 255. 255. 255. 255	On-link	10. 1. 0. 1	291

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

Route 1	Table Informatio	n		
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	0.0.00	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

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 = <u>0ms</u>
```

Step 3: Test successfully.

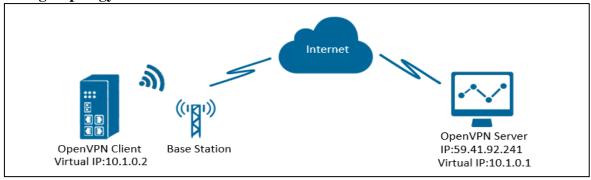


## 11.9. AN011-OpenVPN with TUN and X.509 certificate P2P Mode

#### Overview

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

#### **Testing Topology**



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

## Configuration

#### Server Configuration

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

This P	C > Windows (C:) > Program Files > OpenVPN	↓ > config	v ت	Search con 🔎
^	Name	✓ Date modified	Туре	Size
	📮 ca.crt	7/31/2018 5:53 PM	Security Certificate	2 KE
	dh2048.pem	7/31/2018 6:44 PM	PEM File	1 KE
	openvpn-status.log	8/7/2018 6:06 PM	Text Document	0 KE
	🕥 p2p-server-tun-x509.ovpn	8/7/2018 5:38 PM	OpenVPN Config File	1 KE
	🙀 server01.crt	7/31/2018 5:54 PM	Security Certificate	5 KI
	server01.key	7/31/2018 5:54 PM	KEY File	2 Ki

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

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

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



**Open VPN** 

#### **Router 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	
Mode	P2P •
Protocol	UDP •
Connection Type	TUN
Server Address	59.41.92.241
Server Port	1194
Authentication Method	×.509 • ⑦
Encryption Type	BF-CBC V
Local IP Address	10.8.0.2
Remote IP Address	10.8.0.1
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 2:** Click Save>Apply.

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

Overview	Status	Open	VPN X.S	509 Certificate		
Link Management	X.509 Ce	rtificate Imp	ort			
Industrial Interface				Connection Index	1 •	
Network				CA Certificate	Choose File No file chosen	3
Applications				Local Certificate File	Choose File No file chosen	ٹ 📃
VPN				Local Private Key	Choose File No file chosen	3
<ul> <li>Opm/VPN</li> </ul>				HMAC firewall Key	Choose File No file chosen	3
1PSec				Pre-shared Key	Choose File No file chosen	ۍ 🗧
Maintenance				PKCS#12 Certificate	Choose File No file chosen	ٹ ا
	X.509 Ce	rtificate File	5			
	Index	File Name	File Size	Date Modified		
	1	ca.crt	1188	Tue Aug 7 17:39:32 2018		
	2	client.ort	4382	Tue Aug 7 17:39:43 2018		
	3	client.key	1834	Tue Aug 7 17:39:48 2018		

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

Overview	Stat	us	OpenVPN	X.50	9 Certificate		
Link Management	OpenV	PN Info	mation				
Industrial Interface	Index	Enable	Descripti	ion	Status	Uptime	Virtual IP
Network	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.



Open VPN

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	0	
Interface	tun1	0	
		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

<u>Checking the Routing Table</u> Step 1: Check the Routing Table on your PC

IPv4 Route Table				
Active Routes:				
Network Destination	n 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



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

Step 3: Test Successful



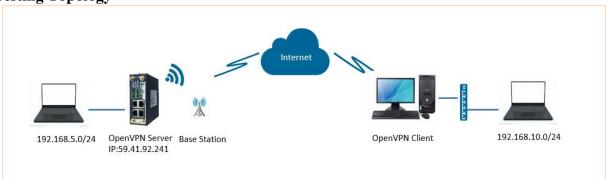
## 11.10.

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

#### Overview

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

#### **Testing Topology**



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

#### Configuration

#### Server Configuration

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

OpenVPN Settings		
General Settings		
Index	1	
Enable	<b>*</b>	
Description	OpenVPN	
Mode	Server •	
Protocol	UDP •	
Connection Type	TUN •	
Max Clients	5	
Authentication Method	X.509 •	0
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	0
Fragment	0	0
Private Key Password	123456	
Output Verbosity Level	3	
Advanced Settings		
Enable NAT	Image: A start and a start and a start a st	
Enable Default Gateway		
Enable PKCS#12		
Enable CRL		
Enable Client to Client		
Enable Duplicate CN		
Enable IP Persist		
Enable HMAC Firewall		
Enable Compression LZ0	<ul> <li>Image: A start of the start of</li></ul>	
Additional Configurations		0

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



Route Settings				
Route Management				
	Index	1		
	Enable		_	
	Route	192.168.10.0/24		
	Push Route	192.168.5.0/24		
			Save	Close
Enable Duplicate CN			<	
Enal	Enable IP Persist		$\mathbf{i}$	
Enable HMAC Firewall				
Enable Compression LZ0				
Additional Configurations			] ⑦	$\mathbf{i}$
Route Management				
Index Enable R	oute	Push Route		Ð

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

Client Se	Client Settings						
Client Se	ttings						
		I	index	1			
		E	nable			_	
		Common N	Name	client01			
		Client IP Ad	dress				
		Internal F	Route	192.168.10	.0/24	] ⑦	
		Push F	Route	192.168.5.0	)/24	0	
	Addit	tional Configura	tions		<u> </u>	0	
						Save	Close
	Enab	e Compression	LZ0			<u> </u>	
	Additi	onal Configurat	ions			0	
Route Ma	anagement						
Index	Enable	Route		Push Route			÷
1	true	192.168.10.0/24	1	92.168.5.0/24			
Client Se	ttings						
Index	Enable	Common Name	Client I	P Address	Internal Route	Push Rou	te 🕀

Step 4: After that, click Save>Apply.

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



**Open VPN** 

Status	Open	VPN <u>X.5</u>	09 Certificate		
X.509 Ce	rtificate Imp	ort			
			OpenVPN Mode	e Server •	
			CA Certificate	Choose File No file chosen ca.crt	
			Local Certificate File	Choose File No file chosen XXX.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 Ce	rtificate Files	s			
Index	File Name	File Size	Date Modified		
1	ca.crt	2399	Thu Mar 5 08:40:08 2020		$\otimes$
2	dh.pem	769	Thu Mar 5 08:40:45 2020		$\otimes$
3	server.crt	8192	Thu Mar 5 08:40:16 2020		$\otimes$
4	server.key	3272	Thu Mar 5 08:40:23 2020		$\otimes$

#### **Client Configuration**

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

g/14/2018 7:48 PM         Security Certificate         3 KB           ca.crt         3/5/2020 3:44 PM         OpenVPN Config File         1 KB           client.ovpn         3/5/2020 3:44 PM         OpenVPN Config File         1 KB           client01.crt         9/14/2018 8:05 PM         Security Certificate         8 KB           client01.key         9/14/2018 8:05 PM         KEY File         4 KB	Name	Date modified	Туре	Size
Glient01.crt         9/14/2018 8:05 PM         Security Certificate         8 KB	📮 ca.crt	9/14/2018 7:48 PM	Security Certificate	3 KB
	Client.ovpn	3/5/2020 3:44 PM	OpenVPN Config File	1 KB
<b>client01.key</b> 9/14/2018 8:05 PM KEY File 4 KB	🔄 client01.crt	9/14/2018 8:05 PM	Security Certificate	8 KB
	client01.key	9/14/2018 8:05 PM	KEY File	4 KB

_____

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

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.

Statu	s Static Ro	ute			
Route T	able Informatio	n			
Index	Destination	Netmask	Gateway	Metric	Interface
1	0.0.0.0	0.0.00	192.168.111.1	0	wan
2	10.8.0.0	255.255.255.0	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	0.0.00	0	wan

Step 2: Route Table on OpenVPN Client for reference.

🔤 Select Administrator: C	🖾 Select Administrator: Command Prompt					
Active Routes:						
Network Destinatio	n Netmask	Gateway	Interface	Metric		
0. 0. 0. 0	0.0.0.0	192.168.10.1	192. 168. 10. 10	291		
0. 0. 0. 0	0. 0. 0. 0	192. 168. 111. 1	192. 168. 111. 4	35		
10.8.0.0	255.255.255.0	On-link	10.8.0.2	291		
10.8.0.2	255. 255. 255. 255	On-link	10.8.0.2	291		
10. 8. 0. 255	255. 255. 255. 255	On-link	10.8.0.2	291		
127.0.0.0	255.0.0.0	On-link	127.0.0.1	331		
127.0.0.1	255. 255. 255. 255	On-link	127.0.0.1	331		
127. <u>255. 255. 255</u>	255. 255. 255. 255	On-link	127.0.0.1	331		
192. 168. 5. 0	255.255.255.0	$10.\ 8.\ 0.\ 1$	10.8.0.2	35		
192.168.10.0	255.255.255.0	On-link	192.168.10.10	291		
192.168.10.10	255. 255. 255. 255	On-link	192. 168. 10. 10	291		

#### **Testing**

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

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

Pinging 10.8.0.2 with 32 bytes of data:

Reply from 10.8.0.2: bytes=32 time=2ms TTL=64

Reply from 10.8.0.2: bytes=32 time=3ms TTL=64

Reply from 10.8.0.2: bytes=32 time=2ms 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	Ping	Traceroute				
Link Management	Ping Settings					
Industrial Interface		Host Address	10.8.0.1			
Network		Ping Count	5			
Applications		Local IP Address				
VPN		1 (10.8.0.1): 56 data bytes				
Maintenance		m 10.8.0.1: seq=0 ttl=128 time=2.788 ms m 10.8.0.1: seq=1 ttl=128 time=3.141 ms				
Firmware Upgrade System		m 10.8.0.1: seq=2 ttl=128 time=4.433 ms m 10.8.0.1: seq=3 ttl=128 time=3.103 ms				

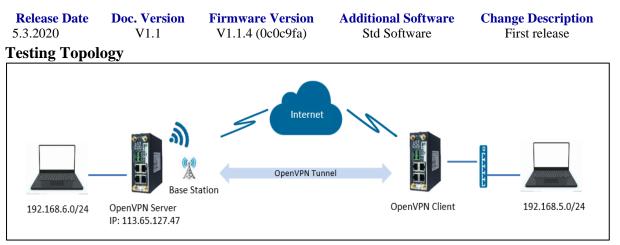


## 11.11. AN57-Open VPN between 6944 routers with X.509Certificate.

#### Overview

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

#### Compatibility



- 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	<b>~</b>	
Description		
Mode	Server ~	
Protocol	UDP ~	
Connection Type	TUN ~	
Max Clients	5	
Authentication Method	X.509 ~	0
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	0
Fragment	1500	0
Private Key Password		
Output Verbosity Level	3	
Advanced Settings		
Enable NAT		
Enable Default Gateway		
Enable PKCS#12		
Enable CRL		
Enable Client to Client	<b>~</b>	
Enable Duplicate CN		
Enable IP Persist		
Enable HMAC Firewall		
Enable Compression LZ0		
Additional Configurations		$\bigcirc$



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

Route Settings		
Route Management		
	Index	1
	Enable	<u> </u>
	Route	192.168.5.0/24
	Push Route	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 🕀

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

Client Se	ttings				
Client Se	ettings				
		Index	1		
		Enable		_	
		Common Name	client06		
		Client IP Address			
		Internal Route	192.168.5.0/24	0	
		Push Route	192.168.6.0/24	0	
	Add	litional Configurations		0	
				Save	Close
	-				
	Enal	ole Compression LZ0			
	Addi	tional Configurations			
Route Ma	anagement	t			
Index	Enable	Route	Push Route		$\oplus$
1	true	192.168.5.0/24	192.168.6.0/24		
Client Se	ettings				
Index	Enable	Common Name Clien	t IP Address Internal Route	Push Route	$\oplus$

**Step 4:** After that, click Save>Apply.

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

Status	Open\	/PN <u>X.5</u>	09 Certificate		
X.509 Ce	rtificate Imp	ort			
			OpenVPN Mode	e 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	e 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 Ce	rtificate Files	;			
Index	File Name	File Size	Date Modified		
1	ca.crt	2399	Thu Mar 5 08:40:08 2020		$\otimes$
2	dh.pem	769	Thu Mar 5 08:40:45 2020		$\otimes$
3	server.crt	8192	Thu Mar 5 08:40:16 2020		$\otimes$
4	server.key	3272	Thu Mar 5 08:40:23 2020		$\otimes$



#### **Client Configuration**

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

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 ~	• ⑦
Encryption Type	BF-CBC	-
Renegotiate Interval	3600	]
Keepalive Interval	20	]
Keepalive Timeout	60	0
Fragment	1500	0
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		0

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

Status	Open	VPN <u>X.5</u>	09 Certificate	Configura	tion Files					
X.509 Ce	rtificate Imp	ort								
			Open	VPN Mode	Client	~				
			Connec	ction Index	1	~				
			CA	Certificate	Choose File	No file chosen	ca.crt	٢		
			Local Cert	tificate File	Choose File	No file chosen	xx.crt	\$		
			Local F	Private Key	Choose File	No file chosen	xx.key	٢		
	HMAC Firewall Key				Choose File	No file chosen		٢		
			Pre-s	shared Key	Choose File	No file chosen		٢		
			PKCS#12	Certificate	Choose File	No file chosen		٢		
			User-Pas	ssword File	Choose File	No file chosen		٢		
			Private Key Pas	ssword File	Choose File	No file chosen		٢		
X.509 Ce	rtificate Files	5						_		
Index	File Name	File Size	Date Modi	ified						
1	ca.crt	1188	Mon Dec 14 13:4	19:11 2020						$\otimes$
2	client.crt	4382	Mon Dec 14 13:4	19:24 2020						$\otimes$
3	client.key	1704	Mon Dec 14 13:4	49:31 2020						$\otimes$

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



Section Eleven

**Open VPN** 

**Rev 2.8** 

Overview	Stat	us	OpenVPN	X.509	Certifica	ate Con	figuratior	n Files				
Link Management	OpenV	OpenVPN Information										
Industrial Interface	Index	Enable	Descriptio	on	Mode	Statu	IS	Uptime	Local Virtual IP			
Network	1	true			Client	Connec	ted	00:33:14	10.8.0.2			
Applications	OpenV	OpenVPN Server Status										
VPN	Index	Commo	n Name	Status		Uptime	Remote	Virtual IP	Remote IP	Remote Port		
▶ OpenVPN												

#### **Routing Tables**

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

Status	Static Ro	oute					
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.

s Static Ro	ute RIP	OSPF	BGP	)
able Informatio	n			
Destination	Netmask	Gateway	Metric	Interface
0.0.00	0.0.0.0	10.152.127.41	100	wwan1
10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
10.152.127.40	255.255.255.252	0.0.00	0	wwan1
192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
192.168.6.0	255.255.255.0	10.8.0.1	0	tun1
	able Information Destination 0.0.0.0 10.8.0.0 10.152.127.40 192.168.5.0	Information           Destination         Netmask           0.0.0.0         0.0.0.0           10.8.0.0         255.255.255.0           10.152.127.40         255.255.255.252           192.168.5.0         255.255.255.0	Information         Netmask         Gateway           Destination         0.0.0.0         10.152.127.41           10.8.0.0         255.255.255.0         0.0.0.0           10.152.127.40         255.255.255.252         0.0.0.0           192.168.5.0         255.255.255.0         0.0.0.0	Able Information         Netmask         Gateway         Metric           0.0.0.0         0.0.0.0         10.152.127.41         100           10.8.0.0         255.255.255.0         0.0.0.0         0           10.152.127.40         255.255.255.255.0         0.0.0.0         0           102.168.5.0         255.255.255.0         0.0.0.0         0

## Testing

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

**Step 3:** Test successfully.



192.168.5.0/24

## **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 Ver	rsion			
Release Date	Doc. Version	Firmware	Additional Software	Change Description
14.12.2020	V1.1	V1.1.4 (0c0c9fa)	Standard Software	First release
Testing Topo	logy			
	ு வி	Inter	net	
_		OpenVPN Station	Tunnel	

# 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.

OpenVPN Client

• An OpenVPN tunnel is established between the Server and the Client, the subnet can PING each other successfully

#### Configuration

192.168.6.0/24

#### Server Configuration

OpenVPN Server

IP: 113.65.127.47

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

enVPN Settings			
eneral Settings			
Index	1		
Enable			
Description			
Mode	Server	~	
Protocol	UDP	~	
Connection Type	TUN	~	
Max Clients	5		
Authentication Method	Password	~	0
Encryption Type	BF-CBC	~	
Local IP Address			
Local Port	1194		
Topology	Subnet	~	
Subnet	10.8.0.0	1	
Subnet Netmask	255.255.255.0		
Renegotiate Interval	3600		
Keepalive Interval	20		
Keepalive Timeout	60	_	0
Fragment	1500		0
	3		
Output Verbosity Level	3		
vanced Settings			
Enable NAT			
Enable Default Gateway			
Enable Client to Client			
Enable Duplicate CN			
Enable IP Persist			
Enable HMAC Firewall			
Enable Compression LZ0			
Additional Configurations			0

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



**Rev 2.8** 

Route Setti	ngs				
Route Mana	agement				
		Index	1	]	
		Enable		_	
		Route	192.168.5.0/24	]	
		Push Route	192.168.6.0/24	]	
				Save	Close
		Duplicate CN			
		able IP Persist		< No. 100	
		HMAC Firewall			
	Enable Cor	mpression LZ0			
	Additional (	Configurations		?	
Route Mana	agement				
Index	Enable	Route	Push Route		Ð

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

Client Se	ettings								
Client Se	ettings								
Index				1		]			
		Er	nable	<ul> <li>Image: A start of the start of</li></ul>					
		Common N	lame	client011					
		Client IP Add	dress			]			
		Internal R	loute	192.168.5.	0/24	] ⑦			
		Push R	loute	192.168.6.	0/24	] ⑦			
	Add	litional Configura	tions			] ⑦			
						Save		Close	
Koute Ma	anagemen	C							
Index	Enable	Route		Push Route				$\oplus$	)
1	true	192.168.5.0/24	19	92.168.6.0/2	4			$\boxtimes$	)
Client Se	ettings								
Index	Enable	Common Name	Client I	P Address	Internal Route	Pu	ish Route	Œ	)

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



**Open VPN** 

Client Pa	ssword Se	ettings						
Client Pa	assword M	anagement						
		I	[ndex	1		]		
		E	nable			_		
		User	name	client011		] ⑦		
		Pass	sword	test01		]		
						Save	С	lose
			wall		1			
	Ena	able Compression	LZ0	<b>~</b>				
	Add	litional Configurat	ions			?		
Route M	anagemen	ıt						
Index	Enable	Route		Push Route				$(\neq)$
1	true	192.168.5.0/24	19	92.168.6.0/24				$\boxtimes$
Client Se	ettings							
Index	Enable	Common Name	Client I	P Address	Internal Route	Push Ro	ute	$\oplus$
1	true	client011			192.168.5.0/24	192.168.6	.0/24	$\boxtimes$
Client Pa	assword M	anagement						
Index	Enable	Username	Pas	sword				Ð

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

Status	Open	VPN <u>X.</u>	509 Certificate		
X.509 Ce	rtificate Imp	ort			
			OpenVPN Mode	Server •	
			CA Certificate	Choose File No file chosen ca.crt	
			Local Certificate File	Choose File No file chosen XXX.crt	
			Local Private Key	Choose File No file chosen XXX.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 Ce	rtificate Files	S			
Index	File Name	File Size	Date Modified		
1	ca.crt	2399	Thu Mar 5 08:40:08 2020		$\otimes$
2	dh.pem	769	Thu Mar 5 08:40:45 2020		$\otimes$
3	server.crt	8192	Thu Mar 5 08:40:16 2020		$\otimes$
4	server.key	3272	Thu Mar 5 08:40:23 2020		$\otimes$

Step 6: Click Apply.



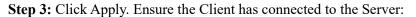
#### **Client Configuration**

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

General Settings		
Index	1	
Enable		
Description		]
Mode	Client 🗸	]
Protocol	UDP ~	]
Connection Type	TUN 🗸	]
Server Address	113.65.127.47	]
Server Port	1194	]
Authentication Method	Password ~	] ⑦
Encryption Type	BF-CBC 🗸	]
Username	client011	]
Password	test01	]
Renegotiate Interval	3600	]
Keepalive Interval	20	]
Keepalive Timeout	60	] ⑦
Fragment	1500	] ⑦
Output Verbosity Level	3	]
Advanced Settings		
Enable NAT		
Enable HMAC Firewall		
Enable Compression LZ0		
Additional Configurations		] ⑦
		Save Close

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

Status	OpenVP	N <u>X.5</u>	09 Certificate	Configura	tion Files					
.509 Certif	icate Impor	t								
			Open	VPN Mode	Client	~				
			Connec	tion Index	1	~				
			CA	Certificate	Choose File	No file chosen	ca.crt	٢		
			Local Cert	tificate File	Choose File	No file chosen		٢		
			Local F	Private Key	Choose File	No file chosen		٢		
			HMAC F	rewall Key	Choose File	No file chosen		٢		
			Pre-s	shared Key	Choose File	No file chosen		٢		
			PKCS#12	Certificate	Choose File	No file chosen		٢		
			User-Pas	sword File	Choose File	No file chosen		٢		
			Private Key Pas	sword File	Choose File	No file chosen		٢		
.509 Certif	icate Files									
Index F	ile Name	File Size	Date Modi	fied						
1	ca.crt	1188	Mon Dec 14 13:4	9:11 2020						



Overview	Stat	us	OpenVPN	X.509	Certifica	te Config	juration Files			
Link Management	OpenV	'PN Infor	mation							
Industrial Interface	Index	Enable	Descriptio	on	Mode	Status	Uptime	Local Virtual IP		
Network	1	true			Client	Connected	d 00:21:38	10.8.0.2		
Applications	OpenV	PN Serve	er Status							
VPN	Index	Commo	n Name	Status	ι	lptime	Remote Virtual IP	Remote IP	Remote Port	
▶ OpenVPN										



#### **Checking the Routing Table**

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

Status	s Static Ro	oute			
Route Ta	able Informatio	n			
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.

5	Status	Static Rout	ie RIP	OSPF	BGP	
Ro	oute Tal	ble Information				
Ind	dex	Destination	Netmask	Gateway	Metric	Interface
1	1	0.0.0.0	0.0.0.0	10.152.127.41	100	wwan1
2	2	10.8.0.0	255.255.255.0	0.0.0.0	0	tun1
3	3	10.152.127.40	255.255.255.252	0.0.0.0	0	wwan1
4	4	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
5	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 Setting	IS				
			Host Address	192.168.5.2	
			Ping Count	5	
		Loc	al IP Address	192.168.6.1	
64 bytes from 64 bytes from 64 bytes from 64 bytes from 64 bytes from 192.168.5. 5 packets tran	5.5.2 (192.168.5.2) 192.168.5.2: seq= 192.168.5.2: seq= 192.168.5.2: seq= 192.168.5.2: seq= 192.168.5.2: seq= 192.168.5.2: seq= 2 ping statistics nsmitted, 5 packets n/avg/max = 34.43	0 ttl=63 time=34. 1 ttl=63 time=44. 2 ttl=63 time=38. 3 ttl=63 time=44. 4 ttl=63 time=54. received, 0% pac	432 ms 027 ms 660 ms 314 ms 063 ms ket loss		



## 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

Stat	us	IPSec				
IPSec 1	Informati	on				
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	
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 🔹



#### VPN->IPSec

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

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

**Transport:** In transport mode, only the payload of the IP packet is usually encrypted or authenticated. The routing is intact, since the IP header is neither modified nor encrypted.

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



Section Twelve

IP Sec

IKE Proposal Settings			
Encryption algorithm	AES-256	•	
Hash Algorithm	SHA2 256	•	
Diffie-Hellman group	Group5(modp1536)	•	
Lifetime	1440		- 11
ESP Proposal Settings			
Encryption algorithm	AES-256	•	
Hash Algorithm	SHA2 256	•	
Diffie-Hellman group	Group5(modp1536)	•	
Lifetime	60		
Advanced Settings			
DPD Interval	30	0	
DPD Timeout	90	0	
Additional Configurations		0	
		Save Close	-

#### VPN->IPSec

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



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

#### Overview

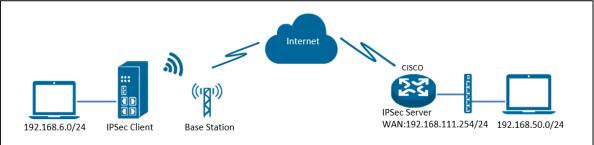
This document contains information regarding the configuration of a 6944 Industrial router running IP Sec with a pre-shared key to a Cisco router.

#### **Software Version**

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

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

#### **Testing Topology**



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

#### Configuration

#### **Server Configuration**

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

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

ISEN	Section	Twelve	6944 Manual	
nications	IPS	Sec	Rev 2.8	
ip nat outside ip nat enable ip virtual-reasse duplex full speed auto no mop enabled crypto map SM. ! interface FastEth	AP hernet0/1 .68.5.1 255.255.255.0 mbly	ip route 0.0.0.0 0.0.0.0 19 no ip http server no ip http secure-server ! ip nat inside source list 10 FastEthernet0/0 overload ! ip access-list extended VF permit ip 192.168.50.0 0. 0.0.0.255 ! access-list 10 permit 192. access-list 101 permit ip 1 0.0.0.255 192.168.6.0 0.0 snmp-server community p end cisco2811#	) interface PN 0.0.255 192.168.6.0 168.5.0 0.0.0.255 92.168.50.0 .0.255	

<u>Client Configuration (on 6944)</u> 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		
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	0
DPD Timeout	90	0
Additional Configurations		0
		Save Close

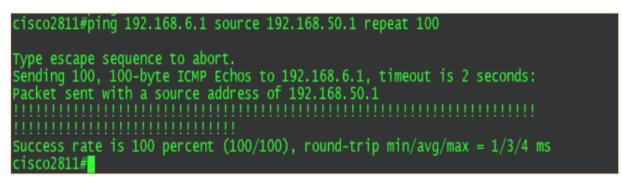
**Step 3:** Check to see if the IP-Sec tunnel has connected successfully. Go to **VPN>IPSec>Status** to check the connection status.



Overview	Stat	us	IPSec		
Link Management	IPSec 2	Informat	ion		
Industrial Interface	Index	Enable	Description	Status	Uptime
Network	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



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



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

#### Overview

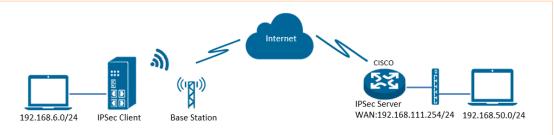
This document contains information regarding a 6944 running IP Sec and FQDN to a Cisco router

#### **Software Version**

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

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

	Section Twelve IP Sec	
unications		
ip nat enable ip virtual-reassembly duplex full speed auto	ip route 0.0.0.0 0.0.0 ip nat inside source FastEthernet0/0 ove	list 10 interface
no mop enabled crypto map SMAP !	ip access-list extend permit ip 192.168.5 0.0.0.255	ed VPN 0.0 0.0.0.255 192.168.6.0
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	! access-list 10 permir access-list 101 perm 0.0.0.255 192.168.6 snmp-server commu ! end cisco2811#	.0 0.0.0.255

#### **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		
Description	IPsec_Pre-shared Key	
Remote Gateway	192.168.111.254	
IKE Version	IKEv1	•
Connection Type	Tunnel	•
Negotiation Mode	Aggressive	v
Authentication Method	Pre-shared Key	•
Local Subnet	192.168.6.0/24	
Local Pre-shared Key	cisco	
Local ID Type	FQDN	•
Local ID	NR500	0
Remote Subnet	192.168.50.0/24	
Remote ID Type	FQDN	T
Remote ID	cisco2811	0
IKE Proposal Settings		
Encryption algorithm	AES-256	T
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	0
DPD Timeout	90	0
Additional Configurations		0
		Save Close

Step 2: Click Save>Apply.

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

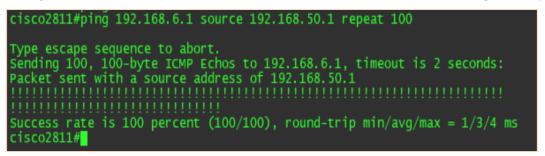


**IP Sec** 

Overview	Stat	us	IPSec			
Link Management	IPSec 1	Informat	tion			
Industrial Interface	Index	Enable	Description	Status	Uptime	
Network	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.



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

Overview	Ping	Traceroute	
Link Management	Ping Setting	gs	
Industrial Interface		Host Address	192.168.50.1
Network		Ping Count	5
Applications		Local IP Address	192.168.6.1
VPN		58.50.1 (192.168.50.1) from 192.168.6.1: 56 rom 192.168.50.1: seq=0 ttl=255 time=1.607 r	
Maintenance	64 bytes fr	om 192.168.50.1: seq=1 ttl=255 time=1.854 r	ms
Firmware Upgrade Sustem		rom 192.168.50.1: seq=2 ttl=255 time=1.510 r rom 192.168.50.1: seq=3 ttl=255 time=1.514 r	

Step 3: Test successful.



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

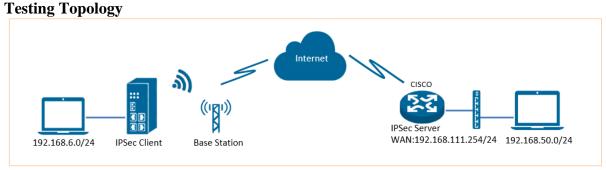
#### Overview

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

#### **Software Version**

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

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



- 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	encr aes 256
version 12.4	hash md5
hostname cisco2811	authentication pre-share
!	group 5
enable secret 5	crypto isakmp key 6 cisco address 0.0.0.0
\$1\$tw/d\$UQQ3Xh06n.2HHFeAVIgXJ.	0.0.0.0
aaa new-model	!
aaa authentication login LOGIN local	crypto ipsec transform-set 6944 esp-3des
!	md5-hmac
aaa session-id common	!
dot11 syslog	crypto dynamic-map DYN 10
ip source-route	set transform-set 6944
1	set pfs group5
ip cef	match address 101
ip domain name cisco.com	reverse-route
ip name-server 192.168.111.1	!
ip address-pool local	crypto map MAP client authentication list
no ipv6 cef	LOGIN
!	crypto map MAP 10 ipsec-isakmp dynam
username cisco password 0 cisco	DYN
archive	!
log config	track 1 interface FastEthernet0/0 line-prot
hidekeys	interface Loopback0
!	ip address 192.168.50.1 255.255.255.0
crypto isakmp policy 10	!
51 11 5	

CASex	Section	6944 Manual		
communications	IP	Sec	Rev 2.8	
ip nat outside ip nat enable ip virtual-reasse duplex full speed auto no mop enabled crypto map MA ! interface FastEth	168.111.254 255.255.255.0 embly l P hernet0/1 168.5.1 255.255.255.0	ip forward-protocol nd ip route 0.0.00 0.0.00 19 ip nat inside source list 10 FastEthernet0/0 overload ! ip access-list extended VF permit ip 192.168.50.0 0. 0.0.0.255 ! access-list 10 permit 192. access-list 101 permit ip 1 0.0.0.255 192.168.6.0 0.0 !! line con 0 line vty 5 15 exec-timeout 5 2 end	9 interface PN 0.0.255 192.168.6.0 168.5.0 0.0.0.255 92.168.50.0	

#### **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 ⑦
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.



**IP Sec** 

Overview	Stat	us	IPSec			
Link Management	IPSec	Informat	tion			
Industrial Interface	Index	Enable	Description	Status	Uptime	
Network	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.

Overview	Ping	Traceroute	
Link Management	Ping Settin	gs	
Industrial Interface		Host Address	192.168.50.1
Network		Ping Count	5
Applications		Local IP Address	192.168.6.1
VPN		68.50.1 (192.168.50.1) from 192.168.6.1: 56 rom 192.168.50.1: seq=0 ttl=255 time=1.607 r	
Maintenance	64 bytes fi	rom 192.168.50.1: seq=1 ttl=255 time=1.854 r	ms
Firmware Upgrade System		rom 192.168.50.1: seq=2 ttl=255 time=1.510 r rom 192.168.50.1: seq=3 ttl=255 time=1.514 r	

Step 4: Test successful.



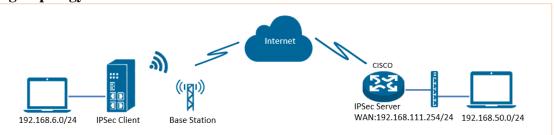
# 12.5. AN015 - IP Sec with a Pre-shared Key to Cisco Router

#### Overview

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

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

Sex	Section	6944 Manual			
ications (	IP	Sec	<b>Rev 2.8</b>		
! interface FastEth ip address 192.1 ip nat outside ip nat enable ip virtual-reassen duplex full no mop enabled crypto map MAI !	58.111.254 255.255.255.0 nbly	ip forward-protocol nd ip route 0.0.0.0 0.0.0.0 19 ip nat inside source list 10 FastEthernet0/0 overload ! ip access-list extended VF permit ip 192.168.50.0 0. 0.0.0.255 !	) interface PN		
interface FastEth ip address 192.1 ip nat inside ip nat enable ip virtual-reasser duplex auto	68.5.1 255.255.255.0	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			

<u>Client Configuration</u> 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 V		
Local Subnet	192.168.6.0/24		
Local Pre-shared Key	cisco		
Local ID Type	FQDN •		
Local ID	NR500	0	
Xauth Identity	cisco		
Xauth Password	cisco		
Remote Subnet	192.168.50.0/24		
Remote ID Type	FQDN V		
Remote ID	cisco2811	0	
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



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

Overview	Stat	us	IPSec			
Link Management	IPSec	Informati	on			
Industrial Interface	Index	Enable	Description	Status	Uptime	
Network	1	true	IPsec_FQDN	Connected	00:00:00	

<u>Testing</u> 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	Traceroute	
Ping Setting	gs	
	Host Address	192.168.50.1
	Ping Count	5
	Local IP Address	192.168.6.1
64 bytes fr 64 bytes fr	rom 192.168.50.1: seq=1 ttl=255 time=1.854 ; rom 192.168.50.1: seq=2 ttl=255 time=1.510 ;	ms
	PING 192.10 64 bytes fi 64 bytes fi 64 bytes fi	Ping Settings Host Address Ping Count

Step 3: Test successful.



**Rev 2.8** 

This page left blank intentionally.



#### 13 **GRE Generic Routing Encapsulation**

#### **Overview**

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

#### **Checking the 6944 GRE Status**

- Go to	Status	>GRE					
Status		GRE					
GRE Info	rmation						
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. ٠

GRE Settings			
GRE Information			
Index	1	]	
Enable			
Description		]	
Mode	Layer 3 🔹	]	
Remote Gateway		]	
Local Virtual IP		]	
Local Virtual Netmask	255.255.255.252	]	
Tunnel key		] ⑦	
Enable NAT			
		Save	Close

#### VPN->GRE

KL/	
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".
<b>Remote Gatew</b>	ay Enter the remote IP address of the Peer GRE tunnel.
Local Virtual I	<b>P</b> Enter the local tunnel IP address of the GRE tunnel.
Local Virtual N	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 Interfa	ce Specify the bridge interface to work in Layer 2 mode.



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

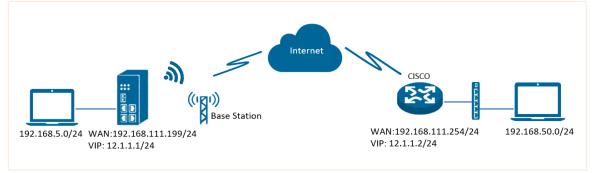
#### Overview

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

#### 6944 Software Version

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

#### **Testing Topology**



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

#### Configuration

#### 6944 Configuration

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

					Login: admin		
					Reboot	Logout	
tus (	GRE						
al Settings							
Enable	Description	Remote Gateway	Local Vinual IP				$\odot$
	al Settings	al Settings	al Settings	al Settings	tus <u>GRE</u> ral Settiops	tus <u>GRE</u> ral Settings	tus <u>GRE</u> ral Settings

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

GRE Settings			
GRE Information			
Index	1		
Enable			
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			
		Save	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.

							Login: admin Reboot Lopout
Overview	Status	Route	1				
Link Management	Static Ro	oute Settings					
Industrial Interface	Index	Description	IP Address	Netmask	Gateway	Interface	•
Network							

Configure the static route settings as shown below



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 ⑦
	Save Close

#### **Configuring the CISCO Router**

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

cisco2811# duplex auto cisco2811#SHOW RUNning-config speed auto Building configuration... ip route 192.168.5.0 255.255.255.0 12.1.1.1 version 12.4 no ip http server no ip http secure-server 1 hostname cisco2811 ip name-server 192.168.111.1 ip nat inside source list 10 interface FastEthernet0/0 overload ip address-pool local no ipv6 cef 1 access-list 10 permit 192.168.5.0 0.0.0.255 1 username cisco password 0 cisco ! username admin password 0 admin end 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



#### Testing

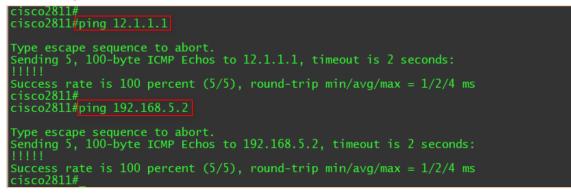
**Step1:** Ping the virtual IP address from the 6944 to the Cisco router.

		Leginc admin Reboot Logout
Overview	Ping Traceroute	
Link Management	Ping Settings	
Industrial Interface	Host Address 12.1.1.2	
Network	Ping Count 5	
Applications	Local IP Address	
VPN	PING 12.1.1.2 (12.1.1.2): 56 data bytes	
Maintenance Upgrade System Configuration	64 bytes from 12.1.1.2: seq=0 UE+255 time=2.127 ms 64 bytes from 12.1.1.2: seq=1 tti=255 time=2.087 ms 64 bytes from 12.1.1.2: seq=2 tti=255 time=2.084 ms 64 bytes from 12.1.1.2: seq=3 tti=255 time=2.081 ms 64 bytes from 12.1.1.2: seq=4 tti=255 time=2.066 ms	
<ul> <li>Doing Tools</li> </ul>	<ul> <li>12.1.1.2 ping statistics ···</li> <li>S packets transmitted, S packets received, 0% packet loss round-trip min/avg/max = 2.066/2.089/2.127 ms</li> </ul>	

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

000000		Login: admin	
		Reboot	Logout
Overview	Ping Traceroute		
Link Management	Ping Settings		
Industrial Interface	Host Address 292.166.50.1		
Network	Ping Count 5		
Applications	Local IP Address		
VPN	PING 192.168.50.1 (192.168.50.1): 56 data bytes		
Maintenance	64 bytes from 192.168.50.1: seq=0 ttl=255 time=2.198 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=2.134 ms		
Upgrade System	64 bytes from 192.168.50.1: seq=2 ttl=255 time=2.143 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=2.134 ms		
Configuration	64 bytes from 192.168.50.1: seq=4 ttl=255 time=2.104 ms		
<ul> <li>Debug Tools</li> </ul>	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



Step 4: Test successful



# **13.2.** AN056- GRE VPN Redundancy to Cisco Router

#### Overview

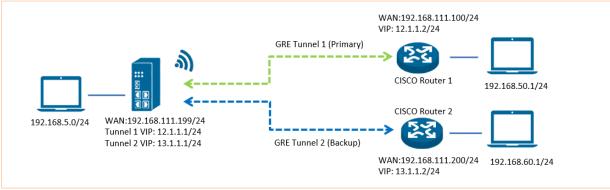
This document contains information regarding the configuration and use of GRE VPN redundancy between a 6944 router and CISCO router.

#### **Software Compatibility**

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

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

#### **Testing Topology**



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

#### Configuration

#### **6944Router Configuration**

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

						Logint admin Reboot Logout
Overview	Status		GRE			
Link Management	General S	Settings				
Industrial Interface	Index	Enable	Description	Remote Gateway	Local Virtual IP	

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

GRE Settings		
General Settings		
Index	1	
Enable		
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		0
Enable NAT		
Enable Default Route		
Advanced Settings		
Binding Interface		0
		Save Close

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



GRE Settings	
General Settings	
Index	2
Enable	Tick
Mode	Layer 3
Remote Gateway	192.168.111.200
Local Virtual IP	13.1.1.1
Local Virtual Netmask	255.255.255.0
Tunnel Key	****
Enable NAT	Tick
Enable Default Route	Leave Un-ticked
Advanced Settings	
Advanced Settings	
<b>Binding Interface</b>	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		
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	0
Interface	gretun1	
		Save Close

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

Static Route Settings			
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	0	
Interface	gretun2	?	
		Save	Close

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

<u>Status</u>	Static Rout	te				
Route Table Information						
Index	Destination	Netmask	Gateway	Metric	Interface	
1	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	gretun1	
3	13.1.1.0	255.255.255.0	0.0.0	0	gretun2	
4	192.168.5.0	255.255.255.0	0.0.00	0	lan0	
5	192.168.50.0	255.255.255.0	0.0.0	0	gretun1	
6	192.168.60.0	255.255.255.0	0.0.0	0	gretun2	
7 1	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 Sett	tings			
Industrial Interface			Enable	<b>*</b>	
Network			VPN Type	GRE •	
Applications			Switch Mode	Primary •	]
VPN			Primary VPN Index	1 *	
OpenVPN			Enable Verbose Log	<b>*</b>	
IPSec	ICMP Detect	tion Settings			
GRE VPN Redundancy		Connectio	n 1 Remote Virtual IP	12.1.1.2	
Maintenance		Connectio	n 2 Remote Virtual IP	13.1.1.2	
		Connectio	n 3 Remote Virtual IP		
		Connectio	n 4 Remote Virtual IP		]
		Connectio	n 5 Remote Virtual IP		]
			Interval	30	0
			Retry Interval	5	0
			Timeout	3	] 💿
			Retry Times	3	0

Step 9: Click Save > Apply



**Section Thirteen** 

**GRE Tunnelling** 

**Rev 2.8** 

## CISCO Router 1 and CISCO Router 2 Configuration

CISCO Router 1 Configuration	<b><u>CISCO Router 2 Configuration</u></b>
<b>Step 1:</b> Telnet to the cisco route and configure cisco router 1	<b>Step1.</b> Telnet to the cisco router and configure cisco
GRE VPN as shown below:	router 2 GRE VPN as shown below:
cisco2811#	airca 2011#
cisco2811#SHOW RUNning-config	cisco2811#
Building configuration	cisco2811#SHOW RUNning-config
version 12.4	Building configuration
!	version 12.4
hostname cisco2811	
ip name-server 192.168.111.1	hostname cisco2811
ip address-pool local	ip name-server 192.168.111.1
no ipv6 cef	ip address-pool local
	no ipv6 cef
username cisco password 0 cisco	
username admin password 0 admin	username cisco password 0 cisco
archive	username admin password 0 admin
log config	archive
hidekeys	log config
!	hidekeys
interface Loopback0	
ip address 192.168.50.1 255.255.255.0	interface Loopback0
-r	ip address 192.168.60.1 255.255.255.0
interface Tunnel1	
ip address 12.1.1.2 255.255.255.0	interface Tunnel1
tunnel source 192.168.111.100	ip address 13.1.1.2 255.255.255.0
tunnel destination 192.168.111.199	tunnel source 192.168.111.200
tunnel key 123456	tunnel destination 192.168.111.199
· ·	tunnel key 123456
interface FastEthernet0/0	
ip address 192.168.111.100 255.255.255.0	interface FastEthernet0/0
ip nat outside	ip address 192.168.111.200 255.255.255.0
ip nat enable	ip nat outside
ip virtual-reassembly	ip nat enable
duplex full	ip virtual-reassembly
speed auto	duplex full
no mop enabled	speed auto
interface FastEthernet0/1	no mop enabled
ip address 192.168.0.1 255.255.255.0	interface FastEthernet0/1
ip nat inside	ip address 192.168.0.1 255.255.255.0
ip nat enable	ip nat inside
ip virtual-reassembly	ip nat enable
duplex auto	ip virtual-reassembly
speed auto	duplex auto
ip route 192.168.5.0 255.255.255.0 12.1.1.1	speed auto
no ip http server	ip route 192.168.5.0 255.255.255.0 13.1.1.1
no ip http secure-server	no ip http server
	no ip http secure-server
ip nat inside source list 10 interface FastEthernet0/0 overload	!
	ip nat inside source list 10 interface FastEthernet0/0
access-list 10 permit 192.168.5.0 0.0.0.255	overload
!	!
end	access-list 10 permit 192.168.5.0 0.0.0.255
	!
	- end



#### Testing

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

Status	VPN Redundancy		
VPN Redund	lancy Status		
		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	in the second	
F	Host Address 192.168.50.1	
	Ping Count 5	
Loca	al 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=2: 64 bytes from 192.168.50.1: seq=1 ttl=255 time=2: 64 bytes from 192.168.50.1: seq=3 ttl=255 time=2: 64 bytes from 192.168.50.1: seq=3 ttl=255 time=2: 64 bytes from 192.168.50.1: seq=4 ttl=255 time=2:	3.112 ms 44.963 ms 3.224 ms	
192.168.50.1 ping statistics 5 packets transmitted, 5 packets received, 0% packer round-trip min/avg/max = 22.390/24.195/27.286 m		

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 Setting	5			
			Host Address	192.168.60.1
			Ping Count	5
		L	ocal IP Address	
PING 192.168.				
192.168.60 5 packets trans				

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

Status	VPN Redundancy						
VPN Redund	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.



<u>Ping</u>	Traceroute	AT Debug	Sniffer		
Ping Setting	s				
			Host Address	192.168.60.1	
			Ping Count	5	
		L	ocal IP Address.		
64 bytes from 64 bytes from 64 bytes from 64 bytes from	.60.1 (192.168.60. 192.168.60.1: sec 192.168.60.1: sec 192.168.60.1: sec 192.168.60.1: sec 192.168.60.1: sec	1=0 ttl=255 time 1=1 ttl=255 time 1=2 ttl=255 time 1=3 ttl=255 time	=14.550 ms =26.281 ms =28.431 ms =29.668 ms		
5 packets tran	).1 ping statistics - Ismitted, 5 packets I/avg/max = 14.55	received, 0% pa			

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 Setting	5			
			Host Address	192.168.50.1
			Ping Count	5
		L	ocal IP Address	
PING 192.168.	50.1 (192.168.50.	1): 56 data byte	S	
	.1 ping statistics smitted, 0 packets		packet loss	

**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 Setting	S		
			Host Address
			Ping Count
		l	ocal IP Address
64 bytes from 64 bytes from 64 bytes from 64 bytes from 64 bytes from	50.1 (192.168.50) 192.168.50.1: sec 192.168.50.1: sec 192.168.50.1: sec 192.168.50.1: sec 192.168.50.1: sec	q=0 ttl=255 time q=1 ttl=255 time q=2 ttl=255 time q=3 ttl=255 time q=4 ttl=255 time	=27.286 ms =23.112 ms =24.963 ms =23.224 ms
5 packets tran	).1 ping statistics - smitted, 5 packets /avg/max = 22.39	s received, 0% p	

Step 8: Test successful.



**Rev 2.8** 

This page left blank intentionally



# 14Layer Two Tunneling Protocol (L2TP)

## 14.1. AN044_L2TP_between_two_6944_Routers

### Overview

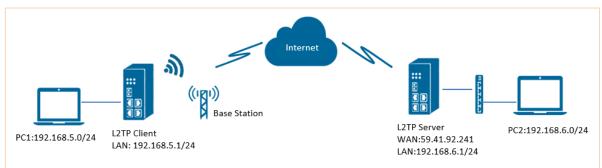
This document contains information regarding configuring an L2TP VPN between two 6944 routers.

#### 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	<b>Firmware Version</b>	Additional Software	Change Description
24.9.2018	V1.1	V1.1.4 (0c0c09fa)	L2TP_1.0.1 (e9b6efe)	First release

#### **Testing Topology**

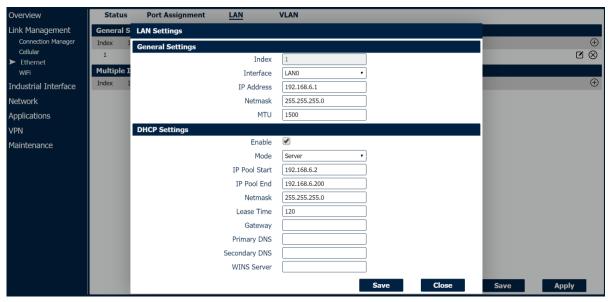


- One 6944 runs as an L2TP server and connects to the Internet using a Sim card with a Fixed Public IP Address.
- A second 6944 run as L2TP client with any type of SIM card which will allow a connection to the internet.
- An L2TP VPN tunnel is established between the two 6944 routers and the subnet PCs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



#### L2TP Layer 2 Tunnelling Protocol

Overview	Status	L2TP Server	L2TP Client				
Link Management	L2TP Setting	S					
Industrial Interface			Enable				
Network			Local Port	1701			
Applications			Challenge Secrets		0		
VPN			Local IP	172.16.1.1			
OpenVPN			Start IP	172.16.1.2			
IPSec			End IP	172.16.1.254			
GRE DMVPN			Enable Debug				
► L2TP	PPP Settings	;					
Maintenance			Authentication	CHAP •			
			Username	L2TPTEST			
			Password	pass			
			MTU	1500			
			Enable Debug				
	Advanced Se	ttings					
			Binding Interface		0		
			Enable Over IPsec				
			Enable NAT				
						Save	Apply

#### 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

Overview	Status	Static Rout	te				
Link Management	Static Ro	ute Settings					
Industrial Interface	Index	Description	IP Address	Netmasi	Gabeway	Interface	
Network	1	Static Route	Settings				
Frewal		Route Table	Information				
<ul> <li>Route</li> <li>VRP</li> </ul>				Index	1		
IP Passthrough			D	rescription	L2TP		
Applications			I	P Address	192.168.5.0		
VPN				Netmask	255.255.255.0		
Maintenance				Gateway			
				Interface	ppp0	0	
						Save	Close

#### **L2TP Client Configuration**

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

Overview	Status	L2TP Settings			
Link Management	L2TP Sett	Index	1	J	
Industrial Interface	Index	Enable			$\oplus$
Network	1	Description	L2TP		⊠ ⊗
Applications		Server Address	59.41.92.241		
VPN		Server Port	1701		
OpenVPN		Challenge Secrets		0	
IPSec		Redial Timeout	20		
GRE		PPP Settings			
► L2TP		Authentication	CHAP •		
Maintenance		Username	L2TPTEST		
		Password	pass		
		Static Local IP	172.16.1.2	]	
		MTU	1500	]	
		Enable Debug			
		Advanced Settings			
		Binding Interface		0	
		Enable NAT			
		Enable Default Route			
				Save Close	Save Apply



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

#### **Testing**

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

C:\Users \ Administrator>ping 192.168.6.2 Pinging 192.168.6.2. with 32 bytes of data Reply from 192.168.6.2: bytes=32 time<1ms TTL=128 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 Ping statistics for 192.168.5.2: Packets: sent = 4, Received = 4, Lost=0 (0% loss) Approximate round trip times in milli seconds Minimum = 64ms, Maximum = 87ms, Average = 77ms



# 14.2. AN045-L2TP Server to Windows Operating System

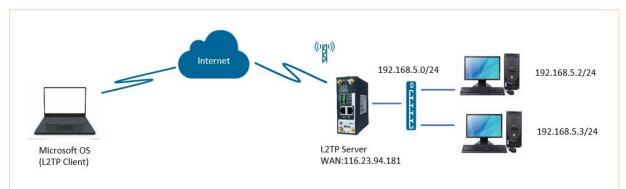
#### Overview

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

#### **Software Compatibility**

	-p			
<b>Release Date</b>	Doc. Version	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>
29.2.2020	V1.1	V1.1.4 (0c0c9fa)	V1.0.1 (e9b6efe)	First release

#### **Testing Topology**

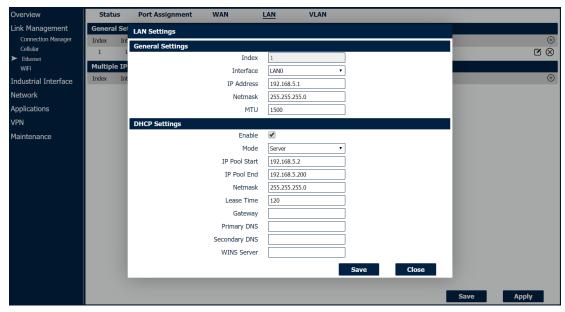


- The 6944 Router run as an L2TP server with a public IP address.
- A PC runs with a Microsoft Windows Operating system working as L2TP client.
- A L2TP VPN tunnel is established between the 6944 router and the PC, The PC can access the LAN devices behind the 6944 Router.

#### Configuration

#### **L2TP Server Configuration**

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



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



#### L2TP Layer 2 Tunnelling Protocol

Overview	Status	L2TP Server	L2TP Client		
Link Management	L2TP Setting	gs			
Industrial Interface			Enable	4	
Network			Challenge Secrets		] ③
Applications			Local IP	172.16.1.1	
VPN			Start IP	172.16.1.2	
OpenVPN			End IP	172.16.1.10	
IPSec GRE			Enable Debug		
DMVPN	PPP Setting	S			
► L2TP			Authentication	CHAP •	
рртр			Username	nwtest	
Maintenance			Password	nwtest	
			MTU	1500	]
			Enable Debug		
	Advanced Se	ettings			
			Binding Interface		] ③
			Enable Over IPsec		
			Enable NAT		
					Save Apply

#### **L2TP Client Configuration**

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

el > All Control Panel Items > Network a	and Sharing Center	v Ū	Search Co	
View your basic network info	rmation and set up connections			
View your active networks				
CISCO 2	Access type: Internet			
Private network	Connections: Wi-Fi (CISCO)			
		nt.		
Troubleshoot problems				
	View your basic network info View your active networks CISCO 2 Private network Change your networking settings Change your networking settings Set up a new connection or r Set up a broadband, dial-up, Troubleshoot problems	CISCO 2       Access type:       Internet         Private network       Connections:       If Wi-Fi (CISCO)         Change your networking settings       Set up a new connection or network       Set up a new connection or network         Set up a broadband, dial-up, or VPN connection; or set up a router or access point       Set up a new connection       Set up a new connection	View your basic network information and set up connections         View your active networks         CISCO 2         Private network         Access type:         Internet         Connections:         Wi-Fi (CISCO)         Change your networking settings         Set up a new connection or network         Set up a broadband, dial-up, or VPN connection; or set up a router or access point.         Troubleshoot problems	View your basic network information and set up connections         View your active networks         CISCO 2         Private network         Access type:         Internet         Connections:         Wi-Fi (CISCO)         Change your networking settings         Set up a new connection or network         Set up a new connection or network         Set up a broadband, dial-up, or VPN connection; or set up a router or access point.         Troubleshoot problems

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

~	🐲 Set Up a Connection or Network
	Choose a connection option
	Connect to the Internet Set up a broadband or dial-up connection to the Internet.
	Set up a new network Set up a new router or access point.
	Manually connect to a wireless network Connect to a hidden network or create a new wireless profile.
	Connect to a workplace Set up a dial-up or VPN connection to your workplace.
	Next Cancel

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



←	Description of the second s	
	How do you want to connect?	
	→ Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.	
	💌 — 🥥 — 🕪	
	→ Dial directly Connect directly to a phone number without going through the Internet.	
	ing ing	
		Cancel

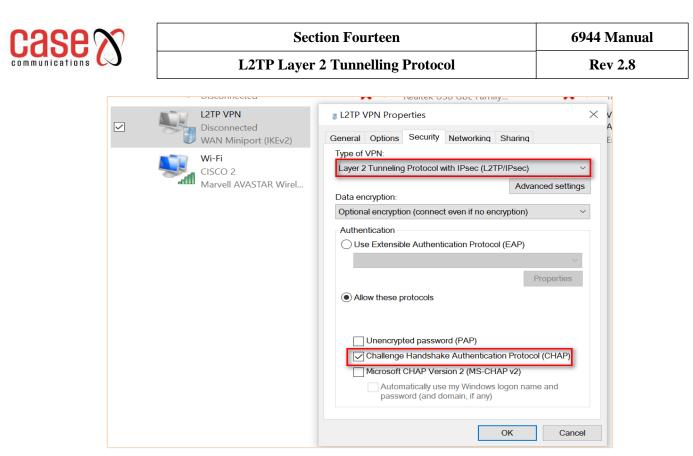
Step 4: Enter the L2TP Server IP address and Destination name, click "Create".

←	Connect to a Workpla	ce
	Type the Internet a	ddress to connect to
	Your network administrate	or can give you this address.
	Internet address:	116.23.94.181
	Destination name:	L2TP VPN
	Use a smart card	
	Remember my cre	dentials
	👎 🗌 Allow other peop	e to use this connection
	This option allows	anyone with access to this computer to use this connection.
		Create Cancel

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



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



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

	Connecting to L2	TP VPN Cancel	
Windows Security Sign in Case		_	

**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.



L2TP VPN Status	
Company I and a	Network Connection Details ×
General Details	Network Connection Details:
Connection	Property Value
IPv4 Connectivity:	Connection-specific DNS
IPv6 Connectivity:	Description L2TP VPN
Media State:	Physical Address
Duration:	DHCP Enabled No
	IPv4 Address 172.16.1.2
	IPv4 Subnet Mask 255.255.255
Details	IPv4 Default Gateway
Activity	IPv4 DNS Server
, identity	IPv4 WINS Server
Sent —	NetBIOS over Tcpip Enab Yes
Bytes: 93,181	
Compression: 0 %	
Errors: 0	
Properties Disconnect	1

#### **Testing**

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

C:\Users \ Administrator ping 192.168.5.1 Pinging 192.168.5.1. with 32 bytes of data Reply from 192.168.5.1: bytes=32 time-13ms TTL=64 Reply from 192.168.5.1: bytes=32 time-1ms TTL=64 Reply from 192.168.5.1: bytes=32 time-1ms TTL=64 Reply from 192.168.5.1: bytes=32 time-1ms TTL=64 Ping statistics for 192.168.5.1: Packets: sent = 4, Received = 4, Lost=0 (0% loss) Approximate round trip times in milli seconds Minimum = 1ms, Maximum = 13ms, Average = 4ms



# 14.3. AN046 - 6944 L2TP Client to Cisco L2TP Server

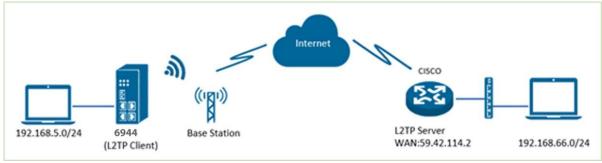
#### Overview

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

#### Software Compatibility

<b>Release Date</b>	Doc. Version	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>
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 ip nat enable Building configuration... ip virtual-reassembly Current configuration : 5447 bytes duplex full speed auto version 12.4 ip cef pppoe enable group global ip dhcp excluded-address 10.10.10.1 pppoe-client dial-pool-number 1 ip dhcp pool ABC no cdp enable network 10.10.10.0 255.255.255.0 no mop enabled default-router 10.10.10.1 ip name-server 8.8.8.8 interface FastEthernet0/1 ip name-server 202.96.128.166 ip address 10.10.10.1 255.255.255.0 ip address-pool local! ip nat inside vpdn enable ip nat enable vpdn-group l2tp ip virtual-reassembly ! Default L2TP VPDN group duplex auto accept-dialin speed auto protocol l2tp no cdp enable virtual-template 1 l2tp tunnel password 0 123456 interface Virtual-Template1 ip address 10.5.5.1 255.255.255.0 username l2tp password 0 l2tp interface Loopback2 peer default ip address pool l2tp ip address 192.168.66.1 255.255.255.0 keepalive 20 3 ppp authentication ms-chap-v2 ١ interface FastEthernet0/0 bandwidth 640 interface Dialer1 no ip address bandwidth 640 ip nat outside 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 020xxxxxxx@163.gd password 0 XVGZW crypto map SMAP ۱

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 0.0.0255 cisco2811#

#### **L2TP Client Configuration**

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

Overview	Status	L2TP Settings				
Link Management	L2TP Sett	Index	1		^	
Industrial Interface	Index	Enable	<b>v</b>			$\oplus$
Network	1	Description				$\boxtimes$
Applications		Server Address	59.42.114.2			
VPN		Challenge Secrets	123456	0		
OpenVPN		Redial Timeout	20			
IPSec GRE		PPP Settings				
DMVPN		Authentication	MSCHAP_V2 •			
► L2TP		MPPE	NONE •			
РРТР		Username	l2tp			
Maintenance		Password	l2tp			
		Static Local IP				
		MTU	1500			
		Enable Debug	<b>I</b>			
		Advanced Settings				
		Binding Interface		0		
		Enable NAT	4			
		Enable Default Route			*	
				Save Close	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

Status	Static Route	RIP	OSPI	F	BGP			
Static Ros	Static Route Settin	<b>9</b> 5						
Index	Route Table Inform	nation						-1
1			Index	1		]		
			Description			j		
			IP Address	192.168.66	.0	]		
			Netmask	255.255.25	5.0	]		
			Gateway			]		
			Interface	12tp_client_	1	] 💿		
						Save	Close	
	Static Ros	Static Rot Static Route Settin	Static Rot Static Route Settings	Static Rot Index 1 Route Table Information Index Description IP Address Netmask Gateway	Static Rot Static Route Settings Index I Route Table Information Index I Description IP Address I92.168.66 Netmask 255.255.25 Gateway	Static Rot Static Route Settings Index I Route Table Information I Description IP Address I92.168.66.0 Netmask 255.255.255.0 Gateway	Static Rot Static Route Settings Index I Route Table Information Index I Description IP Address I92.168.66.0 Netmask 255.255.255.0 Gateway Interface I2tp_client_1 ©	Static Rot       Static Route Settings         Index       Route Table Information         1       Index         1       Interface         1       Interface



#### **Testing**

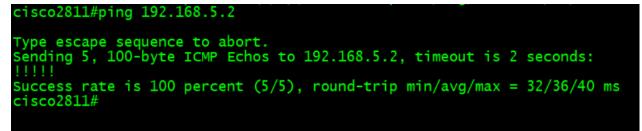
**Step 1:** The 6944 L2TP Client has connected the CISCO L2TP Server successfully. Go to **VPN>L2TP>Status**, to check the connection status.

Status	L2TP Server	L2TP Client				
L2TP Sei	rver Status					
Index	Status	Remote IP	Interface	Uptime		
L2TP Clie	ent 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 Maintenance Upgrade Software System Configuration Debug Tools	64 bytes from 64 bytes from 64 bytes from 64 bytes from 64 bytes from 192.168.66. 5 packets trans	192.168.66.1: sec 192.168.66.1: sec 192.168.66.1: sec 192.168.66.1: sec 192.168.66.1: sec 1 ping statistics - mitted, 5 packets	.1) from 192.168.5.1: 56 data by q=0 ttl=255 time=45.784 ms q=1 ttl=255 time=41.710 ms q=2 ttl=255 time=45.168 ms q=3 ttl=255 time=39.965 ms q=4 ttl=255 time=102.676 ms  s received, 0% packet loss 55/55.060/102.676 ms	rtes

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



Step 4: Test is successful



**Rev 2.8** 

This page left blank intentionally.



# 15 Point to Point Tunneling Protocol (PPTP)15.1. AN 051 PPTP Client to CISCO Server

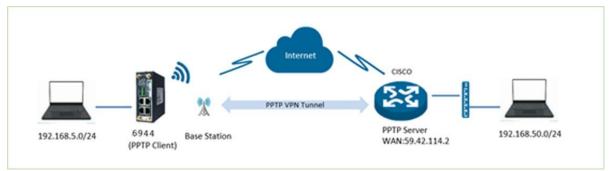
#### Overview

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

#### Software Compatibility

<b>Release Date</b>	Doc. Version	Firmware	Additional Software	<b>Change Description</b>
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	request-dialin
Building configuration	protocol pppoe
Current configuration : 5611 bytes	!
!	username pptp password 0 pptp
version 12.4	archive
hostname cisco2811	!
ip dhcp excluded-address 10.10.10.1	interface Loopback0
ip dhcp pool ABC	ip address 192.168.50.1 255.255.255.0
network 10.10.10.0 255.255.255.0	!
default-router 10.10.10.1	interface FastEthernet0/0
ip name-server 8.8.88	bandwidth 640
ip name-server 202.96.128.166	no ip address
ip address-pool local	ip nat outside
no ipv6 cef	ip nat enable
vpdn enable	ip virtual-reassembly
!	duplex full
vpdn-group 2	speed auto
! Default PPTP VPDN group	pppoe enable group global
accept-dialin	pppoe-client dial-pool-number 1
protocol pptp	no cdp enable
protocol pptp	no cdp enable
virtual-template 2	no mop enabled
!	!
vpdn-group PPPOE	interface FastEthernet0/1



<pre>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</pre>	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 0203XXXXXX @ 163.gd password 0 FSOXXXXXX crypto map SMAP ! <b>ip local pool pptp 10.6.6.2 10.6.6.200</b> ip forward-protocol nd ip route 0.0.0.0 0.0.0.0 Dialer1 <b>ip route 192.168.5.0 255.255.255.0 10.6.6.2</b> ! 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#
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

#### **<u>PPTP Client Configuration</u>**

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

Overview	Status	PPTP Settings				
Link Management	PPTP Set	PPTP Settings				
Industrial Interface	Index	Index	1			<b>(+)</b>
Network	1	Enable				$\boxtimes$
Applications		Description				
VPN		Server Address	59.42.114.2			
OpenVPN		PPP Settings				
IPSec GRE		Authentication	MSCHAP_v2 •			
DMVPN		MPPE	NONE •			
▶ РРТР		Username	pptp			
Maintenance		Password	pptp			
		Static Local IP	10.6.6.2			
		MTU	1500			
		Enable Debug				
		Advanced Settings				
		Binding Interface		0		
		Enable NAT				
		Enable Default Route				
				Save Close		
					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.



PPTP Point to Point Tunnelling Protocol

Overview	Status	Static Route			
Link Management	Static Ro	Static Route Settings			
Industrial Interface	Index	Route Table Information			
Network Firewall > Route VRSP IP Passtbrough Applications VPN		Index Description IP Address Netmask Gateway Interface	1 192.168.50.0 255.255.0	•	
Maintenance		stortade	pptp_client_1	Save	Close

#### 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.

Statu	IS PPTP Serve	er PPTP Client				
PPTP S	erver Status					
Index	Status	Remote IP	Interface	Uptime		
PPTP C	lient 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.

Overview	Ping Traceroute AT Debug							
Link Management	Ping Settings							
Industrial Interface	Host Address 192.168.50.1							
Network	Ping Count 5							
Applications	Local IP Address 192.168.5.1							
VPN	PING 192.168.50.1 (192.168.50.1) from 192.168.5.1: 56 data bytes							
Maintenance	64 bytes from 192.168.50.1: seq=0 ttl=255 time=49.351 ms 64 bytes from 192.168.50.1: seq=1 ttl=255 time=55.116 ms 64 bytes from 192.168.50.1: seq=2 ttl=255 time=53.829 ms 64 bytes from 192.168.50.1: seq=3 ttl=255 time=45.210 ms 64 bytes from 192.168.50.1: seq=4 ttl=255 time=52.693 ms							
Upgrade								
Software System								
Configuration	192.168.50.1 ping statistics							
<ul> <li>Debug Tools</li> </ul>	5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 45.210/51.239/55.116 ms							

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 Packet sent with a source address	192.168.5.1, timeout is of 192.168.50.1	2	seconds:
Success rate is 100 percent (5/5), cisco2811#	, round-trip min/avg/max	=	32/48/68 ms



# 15.2. AN052 6944 PPTP Server to Windows PC

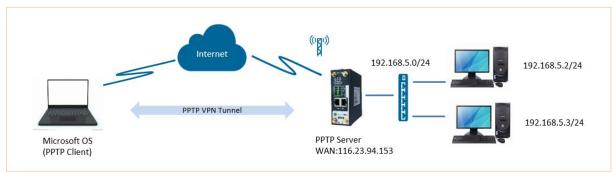
#### Overview

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

	Software	Com	patibi	lity
--	----------	-----	--------	------

soltware companying								
<b>Release Date</b>	Doc. Version	Firmware	Additional Software	<b>Change Description</b>				
17.3.2020	V1.1	V1.1.4(0c0c9fa)	PPTP_1.0.2 (6424848)	First release				

#### **Testing Topology**



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

#### Configuration

#### **<u>PPTP Server Configuration</u>**

**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** 

Overview	Status	Port Assignment WA	N <u>I</u>	AN VLAN				
Link Management	General Set	LAN Settings						
Connection Manager Cellular	Index Int	General Settings						(† (†
<ul> <li>Ethernet</li> <li>WiFi</li> </ul>	Multiple IP		Index Interface	1 LAN0	•		_	
Industrial Interface	Index Int		IP Address	192.168.5.1	<u>·</u>			÷
Network			Netmask	255.255.255.0				
Applications			MTU	1500				
VPN		DHCP Settings						
Maintenance			Enable	<b>v</b>				
			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					
		Se	condary DNS					
			WINS Server					
					Save	Close		
							Save	Apply

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



Overview	Status	PPTP Server	PPTP Client					
Link Management	PPTP Settin	gs						
Industrial Interface				Enable				
Network				Local IP	192.168.168.1	]		
Applications				Start IP	192.168.168.2	]		
VPN				End IP	192.168.168.200	]		
OpenVPN				Enable Debug				
IPSec	PPP Setting	s						
GRE DMVPN				Authentication	CHAP •	]		
L2TP				Username	nwtest	]		
► PPTP				Password	nwtest	]		
Maintenance				MTU	1500	]		
				Enable Debug				
	Advanced S	ettings						
			Bi	nding Interface		] @		
				Enable NAT				
							Save	Apply

#### **<u>PPTP Client Configuration</u>**

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

$ ightarrow ~ \uparrow 💐 > Control Pa$	anel 🔹 All Control Panel Items 🔹 Network a	nd Sharing Center	✓ ບ Search Co.	
Control Panel Home	View your basic network info			
Change adapter settings	View your active networks			
Change advanced sharing	CISCO 2	Access type: Internet		
settings	Private network	Connections: 📲 Wi-Fi (CISCC	))	
	Change your networking settings Set up a new connection or n Set up a broadband, dial-up,	etwork or VPN connection; or set up a router or access po	pint.	
	Troubleshoot problems			
		problems, or get troubleshooting information.		

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

<ul> <li>Set Up a Connection or Network</li> </ul>	
Choose a connection option	
Connect to the Internet Set up a broadband or dial-up connection to	the Internet.
Set up a new network	
Manually connect to a wireless network Connect to a hidden network or create a new	wireless profile.
Connect to a workplace Set up a dial-up or VPN connection to your v	vorkplace.
	Next Cancel

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

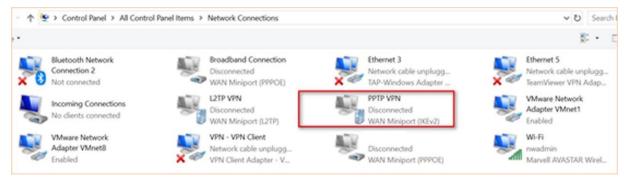


÷	Connect to a Workplace
	How do you want to connect?
	→ Use my Internet connection (VPN) Connect using a virtual private network (VPN) connection through the Internet.
	🧶 — 🎱 — 🕪
	→ Dial directly Connect directly to a phone number without going through the Internet.
	💐 — 🕪
	Cancel

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

		—		$\times$
← ● Connect to a Work	place			
Type the Interne	t address to connect to			
Your network adminis	rator can give you this address.			
Internet address:	116.23.94.153			
Destination name:	PPTP VPN			
Use a smart ca	rd			
🗌 Remember my	credentials			
👎 🗌 Allow other pe	ople to use this connection			
This option all	ows anyone with access to this computer to use this co	onnection.		
	[	Create	Car	icel

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





2	PPTP VPN Disconnected	PPTP VPN Properties
	WAN Miniport (IKEv2)	General Options Security Networking Sharing
	A	Type of VPN:
	Disconnected	Point to Point Tunneling Protocol (PPTP) ~
	WAN Miniport (PPPOE)	Advanced settings Data encryption:
		Optional encryption (connect even if no encryption) $\qquad \qquad \qquad$
		Authentication
		O Use Extensible Authentication Protocol (EAP)
		Properties     Allow these protocols
		Unencrypted password (PAP)
		Challenge Handshake Authentication Protocol (CHAP)
		Microsoft CHAP Version 2 (MS-CHAP v2)     Automatically use my Windows logon name and     password (and domain, if any)
		OK Cancel

**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

	NO PPTP V	ing to PP	TP VPN		
				Cancel	
Windows Sec	curity				×
Sign in					
nwtest		 			
•••••			$\diamond$		
	ОК		Cano	el	

**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.



### **PPTP** Point to Point Tunnelling Protocol

**Rev 2.8** 

PPTP VPN	Network Connection Details
WAN Miniport (PPTP)	Network Connection Details:
PPTP VPN Status	Property Value
General Details Connection IPv4 Connectivity: IPv6 Connectivity: No n Media State: Duration: Details	Connection-specific DNS Description PPTP VPN Physical Address DHCP Enabled No IPv4 Address 192.168.168.2 IPv4 Subnet Mask 255.255.255.255 IPv4 Default Gateway IPv4 DNS Server IPv4 WINS Server NetBIOS over Tcpip Enab Yes
Activity Sent — Sent — — — — — — — — — — — — — — — — — — —	-
Properties Disconnect Diagnose	Close
	Close

### **Testing**

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

Overview	Status	PPTP Ser	ver PPTP Client					
Link Management	PPTP Serv	ver Status						
Industrial Interface	Index	Status	Remote IP	Interface	Uptime			
Network	1	Connected	192.168.168.3	ppp1	00:08:49			
Applications	PPTP Clier	nt Status						
VPN	Index	Description	Status	Local IP	Remote IP	Interface	Uptime	
OpenVPN								
IPSec								
GRE								
DMVPN L2TP								
► PPTP								

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-4ms TTL=64 Ping statistics for 192.168.5.1 Packets: sent = 4, Received = 4, Lost=0 (0% loss) Approximate round trip times in milli-seconds Minimum = 1ms, Maximum = 13ms, Average = 4ms



# 16 Configuring DMVPN on the 6944

# **16.1.** AN029 Configuring DMVPN with RIP to a Cisco Router

# Introduction

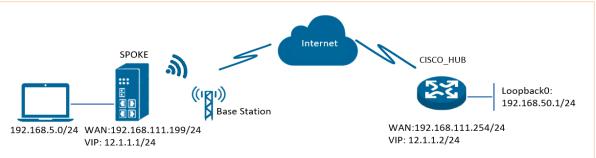
This document contains information explaining how to configure and use DMVPN with RIP on the Case Communications 6944 to a Cisco router. Software Versions

# Software Compatibility

This feature requires the addition of Dynamic Routing software.

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

# Topology



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

# Configuration

# **CISCO Hub Configuration**

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

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



**DMVPN** 

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

# router rip

# Spoke Configuration

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

Status	DMVPN			
NHRP Settings				
		Enable		
		Hub Address	192.168.111.254	]
		NHRP Mapping Address	12.1.1.2	] @
		NHRP Authentication Key	cisco	]
		NHRP Holdtime	120	]
mGRE Settings	;			
		mGRE Local Virtual IP	12.1.1.1	]
		mGRE Local Virtual Netmask	255.255.255.0	]
		mGRE Tunnel key	123456	] Ø
IPSec Settings				
		Negotiation Mode	Main 🔻	
		Local ID Type	None 🔻	
		IKE Encryption Algorithm	3DES 🔻	]
		IKE Hash Algorithm	MD5 •	]
		IKE Diffie-Hellman Group	Group2(modp1024)	
		Pre-shared Key	cisco	]
		ESP Encryption Algorithm	3DES 🔻	
		ESP Hash Algorithm	SHA1 •	]
		ESP Diffie-Hellman Group	None 🔻	
				Save Apply

### Step 2: Click Save>Apply.

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

Statu	s Static Route	RIP	OSPF	BGP	
RIP Set	tings				
			Enable	<b>A</b>	
			Version	RIPv2	•
			Neighbor		
			Default Metric	1	
			Distance	120	
			Update Interval	30	0
			Timeout	180	
		Garba	ige Collect Time	120	
	F	nable Redistribut		Image: A start and a start	
		Enable Redistribu		Image: A start of the start	
		le Redistribute Co			
	Endb		Log Level	Debug	•
Networl	c Settings		Log Lover	babag	
Index	Description	Network			$\oplus$
2		92.168.5.0/24			r 🕺
1		12.1.1.0/24			Ľ ×
Interfac	es Settings				
Index	Interface Enable Pas	sive Split-horizo	n		$\oplus$
	Endblo F do				
					Save Apply

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



**Rev 2.8** 

					1	Login: admin Reboot	Logout
Overview	Status	DMVPN					
Link Management	<b>DMVPN Status</b>						
Industrial Interface			Status	Connected			
Network			Uptime	02:41:04			

# **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-IŚ summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.111.1 to network 0.0.0.0
C 192.168.88.0/24 is directly connected, Loopback3
C 192.168.111.0/24 is directly connected, FastEthernet0/0
172.16.0.0/24 is subnetted, 2 subnets
c 172.16.1.0 is directly connected, Loopback1
C 172.16.2.0 is directly connected, Loopback2
R 192.168.5.0/24 [120/1] via 12.1.1.1, 00:00:17, Tunnel1
12.0.0.0/24 is subnetted, 1 subnets
C 12.1.1.0 is directly connected, Tunnel1
C 192.168.50.0/24 is directly connected, Loopback0
s* 0.0.0.0/0 [1/0] via 192.168.111.1

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

Overview	Status	Static Ro	ute RIP			
Link Management	Route Ta	ble Informatio	n			
Industrial Interface	Index	Destination	Netmask	Gateway	Metric	Interface
Network	1	0.0.0.0	0.0.0.0	192.168.111.1	0	wan
Firewall	2	12.1.1.0	255.255.255.0	0.0.0.0	0	dmvpntun
Route	3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0
VRRP	4	192.168.50.0	255.255.255.0	12.1.1.2	20	dmvpntun
pplications	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
Ping statistics for 192.168.50.1:
Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 4ms, Maximum = 4ms, Average = 4ms
C:\Users\Administrator>
```

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

```
cisco2811#ping 192.168.5.2 source 192.168.50.1

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.5.2, timeout is 2 seconds:

Packet sent with a source address of 192.168.50.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 4/4/8 ms

cisco2811#
```



# **16.2. AN030-Configuring DMVPN with OSPF**

# Introduction

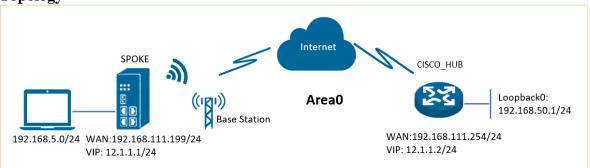
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running OSPF

# **6944 Software Versions**

This feature requires the addition of Dynamic Routing software.

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





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



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

# Spoke Configuration

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

Status	DMVPN					
NHRP Settings						
		Enable				
		Hub Address	192.168.111.254			
		NHRP Mapping Address	12.1.1.2	0		
		NHRP Authentication Key	cisco			
		NHRP Holdtime	120			
mGRE Settings						
		mGRE Local Virtual IP	12.1.1.1			
		mGRE Local Virtual Netmask	255.255.255.0			
		mGRE Tunnel key	123456	0		
IPSec Settings						
		Negotiation Mode	Main 🔹			
		Local ID Type	None •			
		IKE Encryption Algorithm	3DES 🔻			
		IKE Hash Algorithm	MD5 •			
		IKE Diffie-Hellman Group	Group2(modp1024)			
		Pre-shared Key	cisco			
		ESP Encryption Algorithm	3DES •			
		ESP Hash Algorithm	SHA1 •			
		ESP Diffie-Hellman Group	None •			
					Save	Apply

### Step 2. Click Save>Apply.

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

Status	s Static Rou	te RIP	OSPF	BGP	
OSPF Se	ttings				
			Enable		
			Router ID	1.1.1.1	
			Default Metric	1	
			Distance	120	
		Enable Redistribu	te Kernel Routes		
		Enable Redistribu	ute Static Routes		
	Er	nable Redistribute Co	onnected Routes	4	
			Log Level	Debug •	
Network	Settings				
Index	Description	Network	Area		$\oplus$
2		192.168.5.0/24	0		
1		12.1.1.0/24	0		
Interfac	es Settings				
Index	Interface Enable	Passive Cost			$\oplus$
					Save Apply

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



**Rev 2.8** 

Inter	aces Setting	js					
Index	Interface	Enable Passive	Cost				$\oplus$
	Interface	Settings					
	Interface	s Settings					
			Index	1			
			Interface	dmvpntun			
			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.

						Reboot	Logout
Overview	Status	DMVPN					
Link Management	<b>DMVPN Status</b>						
Industrial Interface			Status	Connected			
Network			Uptime	02:41:04			

<u>Check the Routing Tables</u> Step 1: Check the Routing Table on the CISCO HUB for reference.

cisco2811#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route
Gateway of last resort is 192.168.111.1 to network 0.0.0.0
C 192.168.88.0/24 is directly connected, Loopback3
C 192.168.111.0/24 is directly connected, FastEthernet0/0
172.16.0.0/24 is subnetted, 2 subnets
c 172.16.1.0 is directly connected, Loopback1
C172.16.2.0 is directly connected. Loopback2
o 192.168.5.0/24 [110/1010] via 12.1.1.3, 00:19:30, Tunnel1
10.0.0.0/24 is subnetted, 1 subnets
C 10.1.1.0 is directly connected, Loopback100
12.0.0.0/24 is subnetted, 1 subnets
c 12.1.1.0 is directly connected, Tunnel1
C 192.168.50.0/24 is directly connected, Loopback0
s* 0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#

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

							Legin: admin Reboot	Logout
Overview	Status	Static Rout	e RIP	OSPF	BG	P		
Link Management	Route Ta	ble Information						
Industrial Interface	Index	Destination	Netmask	Gatemay	Metric	Interface		
Network	1	0.0.0.0	0.0.0.0	192.168.111.11	0	wan		
Frewal	2	12.1.1.0	255.255.255.0	0.0.0.0	0	dmvpntun		
<ul> <li>Rosts</li> </ul>	3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0		
VERP	4	192.168.50.1	255 255 255 255	12.1.1.2	20	devontun		
Applications	5	192.168.111.0	255.255.255.0	0.0.0.0	0	wat		

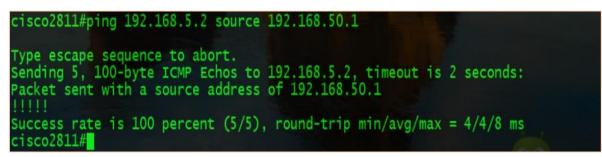


### **Testing**

**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.



Step 3: Test successful.



# **16.3.** AN031 - Configuring DMVPN with BGP to a Cisco Router

# Introduction

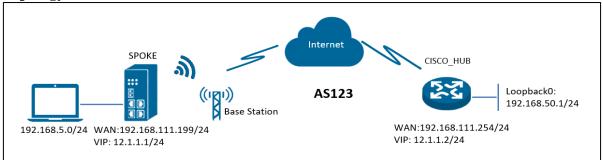
This document contains information explaining how to configure and use of DMVPN on a Case Communications 6944 router running BGP

# Software Compatibility

This applications requires the addition of Dynamic Routing software.

<b>Release Date</b>	Doc. Version	<b>Firmware Version</b>	Software Version	<b>Change Description</b>
7/12/2018	V1.1	Devel (baba6c2) or	DR:V1.0.1 (642848)	First release
		newer	DMVPN:V1.0.1(42ccf3e)	





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





**DMVPN** 

no mop enabled 1 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	<b>VPN</b>	>DMVPN	I. enable	DMVPN	and	configure	<b>DMVPN</b>	as shown	below
~					.,						

Status <u>DMVPN</u>	
NHRP Settings	
Enable	
Hub Address	192.168.111.254
NHRP Mapping Address	12.1.1.2 ⑦
NHRP Authentication Key	cisco
NHRP Holdtime	120
mGRE Settings	
mGRE Local Virtual IP	12.1.1.1
mGRE Local Virtual Netmask	255.255.255.0
mGRE Tunnel key	123456 ⑦
IPSec Settings	
Negotiation Mode	Main
Local ID Type	None
IKE Encryption Algorithm	3DES •
IKE Hash Algorithm	MD5 V
IKE Diffie-Hellman Group	Group2(modp1024)
Pre-shared Key	cisco
ESP Encryption Algorithm	3DES V
ESP Hash Algorithm	SHA1 •
ESP Diffie-Hellman Group	None •
	Save Apply

Step 2: Go to Network>Route>BGP, enable BGP and configure BGP as shown below

Stat	us Static R	oute RI	[P	OSPF	BGP			
BGP Se	ettings							
				Enable				
				AS Number	123			
				Router ID	1.1.1.1			
		Enable Re	distribute Ker	nel Routes				
		Enable Re	edistribute St	atic Routes				
		Enable Redistr	ibute Connec	ted Routes				
				Log Level	Debug 🔻			
Netwo	ork Settings							
Index	Description	Network						Ð
1		192.168.5.0	/24				<b>I</b> (	$\otimes$
Neighb	oors Settings							
Index	Neighbor Address	Remote AS	Next Hop S	elf				$\oplus$
1	12.1.1.2	123	false				<b>I</b> (	$\otimes$
						Sav	re Apply	

Step 3: A Route has connected to the CISCO HUB. Go to VPN>DMVPN>Status to check the connection



DMVPN

**Rev 2.8** 

						Reboot	Lopout
Status	DMVPN						
<b>DMVPN Status</b>							
		Status	Connected				
		Uptime	02:41:04				
		-	OMVPN Status Status	DMVPN Status Status Connected	DMVPN Status Status Connected	Status DMVPN ONVPN Status Status Connected	Status DMVPN OMVPN Status Status Connected

### **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
o - obk, r - per fourt downtoaded statter fourte
Gateway of last resort is 192.168.111.1 to network 0.0.0.0
Gateway of fast resolt is 192.108.111.1 to network 0.0.0.0
C 192.168.88.0/24 is directly connected, Loopback3
c 192.100.00.0/24 is directly connected, Loopbacks
C 192.168.111.0/24 is directly connected, FastEthernet0/0 172.16.0.0/24 is subnetted, 2 subnets
C 172.16.1.0 is directly connected, Loopback1 C 172.16.2.0 is directly connected, Loopback2
B 192.168.5.0/24 [200/0] via 12.1.1.3, 00:03:14
10.0.0/24 is subnetted, 1 subnets
C 10,1,1,0 is directly connected, Loopback100
12.0.0.0/24 is subnetted, 1 subnets
C 12.1.1.0 is directly connected, Tunnel1
C 192.168.50.0/24 is directly connected, Loopback0
s* 0.0.0.0/0 [1/0] via 192.168.111.1
cisco2811#

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

							Logint admin Reboot	Logout
Overview	Status	Static Route	RIP	OSPF	BG	P		
ink Management	Route Ta	ble Information						
ndustrial Interface	Index	Destination	Netmask	Gateway	Metric	Interface		
letwork.	1	0.0.0.0	0.0.0.0	192.168.111.11	0	wan		
Frenal	2	12.1.1.0	255.255.255.0	0.0.0.0	0	ómypréun		
Rode	3	192.168.5.0	255.255.255.0	0.0.0.0	0	lan0		
VRRP	4	192.168.50.0	255.255.255.0	12.1.1.2	20	ómypritun		
oplications	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 Packet sent with a source address !!!!!	192.168.5.2, timeout is 2 seconds: of 192.168.50.1
Success rate is 100 percent (5/5) cisco2811#	, round-trip min/avg/max = 4/4/8 ms



# 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 <u>Network Address</u> <u>Translation</u> (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.



**Rev 2.8** 

This page left blank intentionally



Industrial Interface

# **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.

Stat	us (	Connection	1			
Serial	Connecti	on Setting	s			
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		
Port	COM1 •	]
Baud Rate	115200 🔹	]
Data Bits	8 🔻	]
Stop Bits	1 •	]
Parity	None •	]
Transmission Settings		
Transmission Method	Transparent •	]
MTU	1024	] ⑦
Protocol	TCP Client •	]
Remote IP Address		
Remote Port	2000	]
		Save Close



### 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				



- 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		
	Digit	al Input Informatio	n
Index	Enable	Logic Level	Status
1	false	High	Alarm OFF
2	false	High	Alarm OFF
	Digita	l Output Information	on
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	1	]	
Enable			
Alarm ON Mode	Low •	]	
Alarm ON Content		]	
Alarm OFF Content		]	
		Save	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.



Digital Output	
Digital Output Settings	
Index	1
Enable	
Alarm Source	Digital Input 1
Alarm ON Action	High 🔹
Alarm OFF Action	Low •
	Save Close

## 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

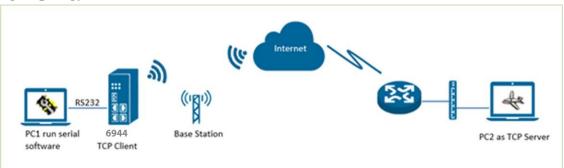
# Overview

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
Soliware		· I ms icature		stanuar u sortwart

Release Date	Doc. Version	<b>Firmware Version</b>	Additional sw	<b>Change Description</b>
3.8.2018	V1.1	V1.1.1.4 (0c0c09fa)	Std Software	First released

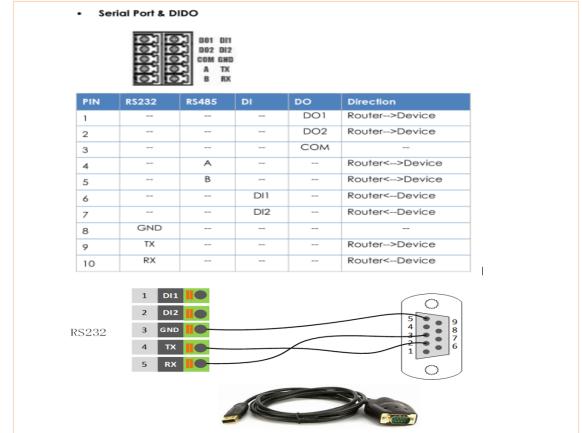
# **Testing Topology**



- 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.

									Reboot	Logout	
Overview	Stat	us	Connection								
Link Management	Serial	Connect	ion Settings								
Industrial Interface	Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity				
<ul> <li>Serial</li> </ul>	1	false	COMI	115200	8	1	None				ß
Digital 10	2	false	COM2	115200	8	1	None				2

**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	r				
В	aud Rate	115200	•				
	Data Bits	8	•				
	Stop Bits	1	•				
	Parity	None	•				
Transmission Settings							
Transmissio	n Method	Transparent	r				
	MTU	1024	) ?				
	Protocol	TCP Client					
Remote If	P Address	113.65.230.194					
Rer	note Port	2000	)				
				Save		Close	

### **TCP Server Configuration**

**Step 1.**Run the TCP Software "TCPUDPDbg" on server PC2, the 6944 will connect to the TCP Server automatically.

Operate(O) View(V) Window	
실 CreateConnn 🔊 CreateServe	r   🐰 StartServer 🛞 🔞   😤 Connect 🕃   🌺 DisconnAll   💥 DeleteConn 🎇   🔟   ಿ 🖕
Properties 7 ×	₩ 192.168.111.199:48954
E Client Mode Server Mode	DestIF:       Image: Send
< >	

Step 2: Go to Industrial Interface>Serial>Status>Serial Information>Index2, it will show the connection status.



							Login: admin Reboot	Logout
Overview	Stat	us C	onnection					
Link Management	Serial	Informatic	on .					
Industrial Interface	Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status		
<ul> <li>Serial</li> </ul>	1	false	R5485	Transparent	TCP Client	Disconnected		
Digital 10	2	true	R5232	Transparent	TOP Client	Connected		

<u>Testing</u> Step 1: Run the serial software "Hercules" on PC1, send the data "hello world".

😵 Hercules SETUP utility by HW-group.com		- [	
UDP Setup Serial TCP Client TCP Server UDP Test Mode Ab	out		
Received/Sent data		0	
Serial port COM4 opened		Serial —	
hello world			
		COM4	~
		Baud	
		115200	-
		Data size	
		8	~
		Parity	
		none	-
		Handshake	
		1	Ŧ
		Mode	
		Free	~
		×	Close
Modem lines			CIOSE
	🗆 DTR 🖂 RTS	HWg F\	√ update
Send	- 1		
hello world	☐ HEX Send	HIU	group
		www.HW-	
1	□ HEX Send	Hercules SE	<u> </u>
	HEX Send		ion 3.2.6
		Yers	JUIL 3.2.0

### Step 2: Test Result

Step 3: TCP Server side can receive the data "hello world"

Operate( <u>O</u> ) View( <u>V</u> ) Windo	ws(W) Help(H) Language 🛛 🗙
🔄 CreateConnn 🔕 CreateServe	er   🐰 StartServer 🛞 😡   😒 Connect 🐲   🌺 DisconnAll   💥 DeleteConn 🎇   🔯   💈 💂
Properties 4 ×	₩ 192.168.111.199:48954 4 ▷ ×
<ul> <li>☐ Client Mode</li> <li>☐ Server Mode</li> <li>☐ Server Mode</li> <li>☐ 2 Los(1/(92.168.154.1):2000</li> <li>☐ 192.168.111.199:48954</li> </ul>	DestIF:     Send     AtusSend     Eve     100     ns     Send     Stop       192.168.111.199     Send Mex     Sand File     Send Mex     Send Mex     Option     BroadDytion       V     LocalFort     100     Top     Top     Top     Top     Top       7     LocalFort     Send     Send Mex     Send File     Send Received     Clear     Option     BroadDytion       7     Tops TOP     Top     Top     Top     Top     Top     Top     Top       7     AtusConn     Eve     0     s     Send Kex     Send File     Send Send File       8     Count     Seve(In Time)     Seve(In Time)     Image: Send File     Send File     Send File       8     Clear     11     Send File     Send Option     ShowHex
	Send Speed(B/S): 0 Receive Speed(B/S): 0



# **18.3.** AN005 RS485 Transparent Mode

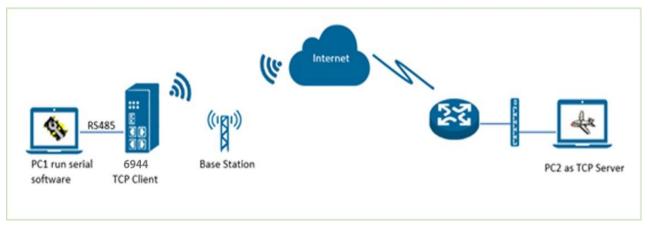
## Overview

This document contains information regarding the configuration of RS485 in Transparent Mode with using a TCP Client on the 6944.

# Software Version

<b>Release Date</b>	<b>Doc. Version</b>	<b>Firmware Version</b>	Additional Software	<b>Change Description</b>
3.8.2018	V1.0.0	V1.1.4 (0c0c9fa)	Std Software	First released

# Testing Topology

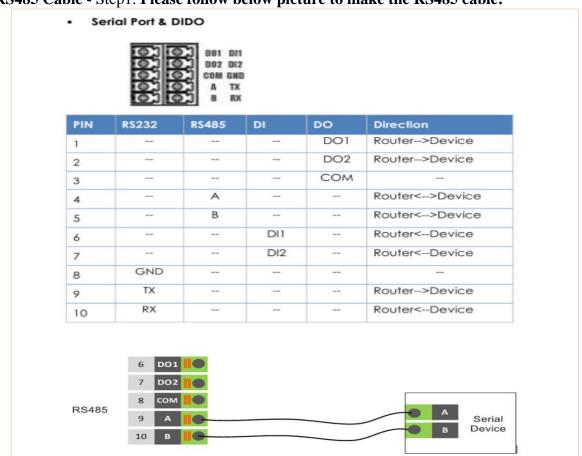


- The 6944 runs as a TCP Client and connect to the Internet with a SIM card.
- PC1 simulate as serial device and runs serial software, such as Hercules. Hercules will send the data to the TCP server through the 6944 with TCP transparent mode.
- PC2 runs as a TCP server and connected to the Internet via 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.

								Login: admin Reboot	Logout
Overview	Stat	us :	Connection						
Link Management	Serial	Connecti	on Settings	1					
Industrial Interface	Index	Enable	Port	Baud Rate	Data Bits	Stop Bits	Parity		
► Serial	1	false	COMI	115200	8	1	None		S S
Digital 10	2	false	COM2	115200	8	1	None		ß

**Step 2:** Enable the RS485 setting, select Protocol as "TCP Client" and enter the Server IP address and Server Port. **Click Save > Apply** 



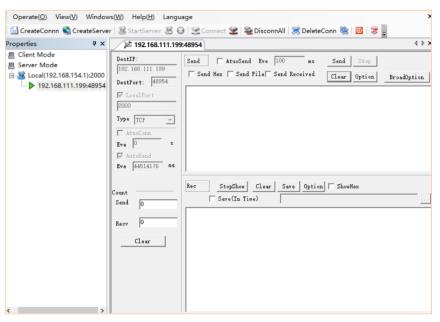
### **Industrial Interface**

**Rev 2.8** 

Connection Setting	gs		
Serial Connection	Settings		
	Index	1	]
	Enable		
	Port	COM1	Ŧ
	Baud Rate	115200	•
	Data Bits	8	•
	Stop Bits	1	•
	Parity	None	•
Transmission Sett	ings		
	Transmission Method	Transparent	•
	MTU	1024	0
	Protocol	TCP Client	- -
	Remote IP Address	113.65.230.194	
	Remote Port	2000	
			Save Close

### **TCP Server Configuration**

**Step1.**Run TCP Software "TCPUDPDbg" on server PC2, the 6944 will connect to the TCP Server automatically.



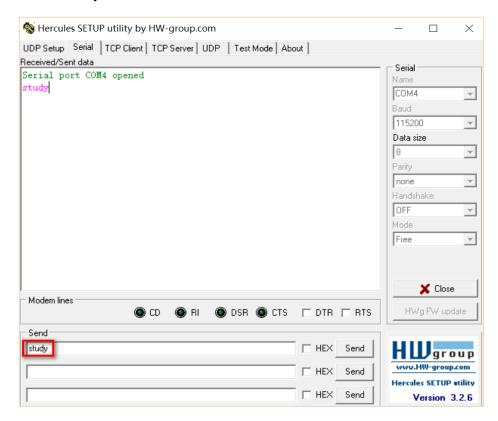
Step 2. Go to Industrial Interface>Serial>Status>Serial Information>Index1, to show the connection status.

Com								Login: adr Reboot	Logout
Oven	hew	Stat	WS .	Connection					
Link	Management	Serial	Informat	ion					/
Indus	trial Interface	Index	Enable	Serial Type	Transmission Method	Protocol	Connection Status		
► Se		1	true	R5485	Transparent	TOP Client	Connected		
Dig	pital 10	2	false	R5232	Transparent	TCP Client	Disconnected		



# **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"

Operate(O) View(V) Window	ws(W) Help(H) Language
실 CreateConnn 🔕 CreateServe	er   🐰 StartServer, 😤 😡   😤 Connect 🐲   🛬 DisconnAll   💥 DeleteConn 🎇   🔟   寒 💂
Properties 7 ×	₩ 192.168.111.199:48956
Client Mode	DestIP: [192.168.111.199] Send TAtuaSend Eve 100 ms Send Stop DestFort: 489956 F LocalPort 2000 Type TCP Y TAtuoConn Eve 0 Send Max Send File Send Received Clear Option BroadOption Eve 0 Send Base StopShow Clear Save Option ShowMax Count Send 0 Eve 0 Clear 0 Study Recv 0 Clear
	Send Speed(B/S): 0 Receive Speed(B/S): 0



**Rev 2.8** 

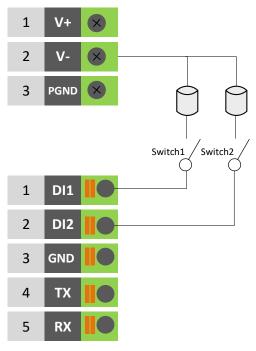
This page left blank intentionally



# **19.** Digital I / O Ports

# **19.1.** Digital Input Port

Typical Application Diagram



DI ELECTRICAL CHARACTERISTICS

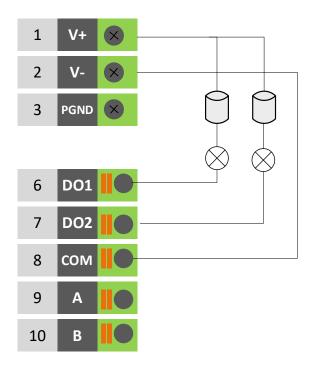
1. Galvanic isolation;

2. Over-Voltage Protection: 36 VDC

3. Over-Current Protection: 100mA per channel @  $25^{\circ}C$ 

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)



**Rev 2.8** 

This page left blank intentionally



# MODBUS

# 20.1 MODBUS Slave

# Overview

20

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

# Software Compatibility

Release Date	Doc. Version	<b>Firmware Version</b>	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	13806	1	Default:500(ms)
		Registers			range:1~1000
6	DO2 Pulse Width	03 Holding	13807	1	Default:500(ms)
		Registers			range:1~1000



### **Example Read Di Status**

Master	Transaction	Protocol	Data	Slave Id	Function	Address	Quantity
	ID	ID	Length		Code		
Tx	01.90	00.00	00.06	01	02	35E8	00.01
Slave	Transaction	Protocol	Data	Slave Id	Function	Byte	Value
	ID	ID	Length		Code	Length	
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	Protocol	Data	Slave Id	Function	Byte	Value
	ID	ID	Length		Code	Length	
Rx	04.81	00.00	00.04	01	01	01	02

## **Example: Control Do-Output Pulse**

Master	Transaction	Protocol	Data	Slave	Function	Address	Quantity	Byte	Value
	ID	ID	Length	Id	Code		-	Length	
Tx	07.29	00.00	00.08	01	0F	35EA	00.02	01	02
Slave	Transaction	Protocol	Data	Slave	Function	Address	Quantity		
	ID	ID	Length	Id	Code				
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	Protocol ID	Data	Slave	Function	Address	Value
	ID		Length	Id	Code		
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:

Nendew	Status	Modbus Slave					
nk Management	General Sett	tings					
dustrial Interface			Enable	1			
etwork			Protocol	TOMP			
plications			Slave ID	1:			
DONS			Local 37				
SMS Schedule Reborz			Local Port	907			
Mother Street							
N							
laintenance							
							-
						Save	Apply

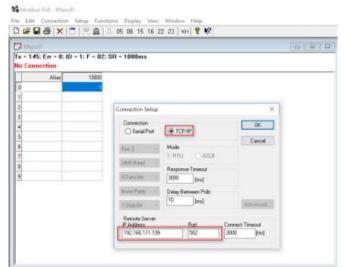
**Step 2 Click Save > Apply** 



### **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)

			(m) [
: Err = 0: ID	= 1: F = 82: S	R = 1000ms	
Allas	13830		
		Read/Write Definition	×
		Steve ID  Function 02 Read Discete Inputs (1%) Addess: 13800 Guarter, 1	te:
		Scan Rate 1000 ne Scan Rate Looked Read/Wite D	Inco
		Rows         □ Hide Allesi Columni           ● 10         20         50         0.100         □ Hide Allesi Columni           □ Address in Cell	

Send the command to read the status of DI 1 (Path: Functions>Test Centre)

and the second	🖳 🚖   IL 05 06 15 16 22 23   101   💡 🎀	
Thopelit	0	
= 1343: Err = 0: IC	) = 1: F = 02: SR = 1000ms	
Alies	13800	
Antes		
	Test Center X	1
	Enter hex number separated by "" "" or space	
	01 90 00 00 00 06 01 02 35 E8 00 01 v	
	Open list Save list Add to list Send Exit	

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



# **Read Digital Output Status**

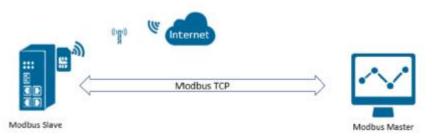
Set the Function Code to "01", Address 13802 and the quantity is set to "2".

Path: Setup>Read / Write Definition

# **Control Digital Output**

Go to Functions>15: WriteMultiple Coils, to change the DO state from "0" to "1".s

# Topology



- 1. The 6944 router runs as a Modbus Slave with a static public IP address with a SIM card.
- 2. Modbus Master connects to the 6944 router (Modbus Slave) via a TCP connection.
- 3. The Modbus Master reads the status of Digital IO and control DO.

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

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	03 Holding	13806	1	Default:500(ms)
	Width	Registers			range:1~1000
6	DO2 Pulse	03 Holding	13807	1	Default:500(ms)
	Width	Registers			range:1~1000

# Digital I/O Register Table

## **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	Protocol	Data	Slave Id	Function	Byte	Value
	ID	ID	Length		Code	Length	
Rx	01.90	00.00	00.04	01	02	01	01



MODBUS

## **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	Protocol	Data	Slave Id	Function	Byte	Value
	ID	ID	Length		Code	Length	
Rx	04.81	00.00	00.04	01	01	01	02

# **Example: Control Do-Output Pulse**

Master	Transaction	Protocol	Data	Slave	Function	Address	Quantity	Byte	Value
	ID	ID	Length	Id	Code		-	Length	
Tx	07.29	00.00	00.08	01	0F	35EA	00.02	01	02
Slave	Transaction	Protocol	Data	Slave	Function	Address	Quantity		
	ID	ID	Length	Id	Code		-		
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	Protocol	Data	Slave Id	Function	Address	Value
	ID	ID	Length		Code		
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:

Overview	Status 1	Modbus Slave				
Link Management	General Setting					
Industrial Interface			Enable			
Network			Pretocol	10P/1P		
Applications			Slave ID	1		
DONG SMS			Local IP			
Schedule Reborz			Local Port	903		
<ul> <li>Mother time</li> </ul>						
VPN						
Maintenance						
					Save	Apply
	1				2010	A A A A A

**Step2. Click Save > Apply** 



# <u>Testing</u> <u>Read Digital Input Status</u>

**Step 1**. Run the software "MODBUS Poll" to connect to the 6944 (MODBUS Slave) as shown below (Path Connection > Connect)

Err = 0: ID	- 1: F - 02::	SR - 1000ms				a
Alia	13800					
		Connection Setup Connection	(® TCP)	3	OK	×
		Part 1	Mode + RTU Response 3000	() ASCI	Car	
		Nore Party	Delay Be 10	(wa)		ed.
		Renote Server P Address 192,168,111,199		Part 502	Connect Tineout	0

(Path: Setup> Read/ Write Definition)

Err = 0: ID	- 1: F - 82: S	R = 1000ms	
Alias	13830		
		Read/Write Definition	×
		Slave ID 02 Fead Discele Inputs (1x) Addeese 13900	OK Cancel Apoly
		Guantly: 1 Scen Role: 1000 no Pl Read/wite Ended R	Read/Wide Drice
		Wese         Bows         □ Hide Allo           ❀ 10         20         50         100         □ Address	
		Display: Signed PLCAdd	Resources (Blase 1)

Step 2. Send the command to read the status of DI 1

(Path: Functions>Test Centre)



MODBUS

	🗂   樊 直   几 05 06 15 16 22 23   101   💡 🕅	
9 Mbpolit		0
	D = 1: F = 02: SR = 1000ms	
Alies	13800	
2	24	
	I Test Cerker	×
		×
1 m m	Enter hes number separated by "." "" or space	×
1 m m		×
	Enter her number separated by "" or space 01 90 00 00 06 01 02 35 E8 00 01	~
1 2 3 4 5 6 6 7 8 9	Enter her number separated by "" or space 01 90 00 00 06 01 02 35 E8 00 01	

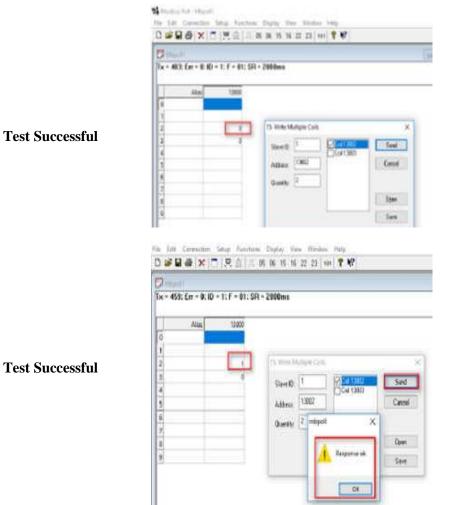
The reply Value is "00", DO1 status is "Low". Then the test is successful.

# **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





# 20.2 MODBUS Master

# Introduction

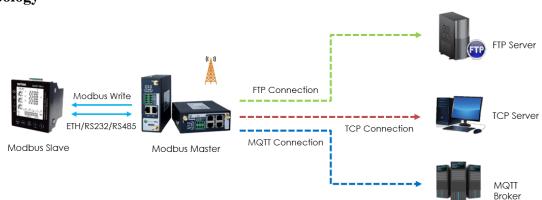
This section of the manual relates to the software for the MODBUS Master on the 6944 router. It requires the 6944 to be running the MODBUS Master software, which is version V.1.0.0 written in Feb 2020

# Software Compatibility

Updates between document versions are cumulative. Therefore, the latest document will include all the contents from the previous versions.

Release Date	Doc. Version	<b>Firmware Version</b>	<b>Change Description</b>
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:** 

📓 Modbus Slave - Mbslav1		
File Edit Connection Setup Display View Window Help		
🗒 Mbslav1		
ID = 1: F = 03	Connection Setup X	
No connection	Connection	
Alias 00000	O Serial Port	^
0 0	Cancel	
1 0	Port 3  O RTU O ASCII	
2 0	115200 Baud 💛 – Flow Control	
3 21	8 Data bits	
4 0	RTS Toggle 1 [ms] RTS disable delay	
5 0	None Parity V	
6 0	1 Stop Bit V Port 502 Ignore Unit ID	
7 0		



**MODBUS** 

**Rev 2.8** 

₽.X	Modbus Slave - M	bslav1		
			View Window	Help
D	🚔 🔒 🎒 🛅	🗒 📋 🤋 📢		
	Mbslav1		Sla	ave Definition X
ID	= 1: F = 03			Slave ID: 1 Cunction: 03 Holding Register (4x) Cancel
	Alias	00000	A	Address: 0
0		0	Q	Quantity: 10
1		0		View
2		0		Rows     □     Hide Alias Columns       ● 10     ○ 20     ○ 50     ○ 100
3		21		PLC Addresses (Base 1)
4		0		Display: Signed V
5		0		Error Simulation
6		0		Skip response Insert CRC/LRC error
7		0		(Not when using TCP/IP)     [ms] Response Delay
8		0		v v

### **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:

Connectio	n Setting	s				
Connectio	n List					
		Inc	lex 1			
		Enal	ble 🕑			
		Descripti	on test			
		Scan Ra	ate 100		0	
		Reconnect Inter	val 60		0	
		Response Time	out 1000	)	0	
		Delay Between Po	olls 0		0	
		Connection Ty	pe TCP		•	
		Enable Show Stat	tus 💌		_	
		Enable Verbose L	.og 🖉			
TCP Settir	igs					
		Server Addre	255 192.	168.111.44		Address of
		Server P	ort 502		M	odbus Slave
Channel L	ist					
Index	Enable	Description	Slave ID	Function Code	Register Address	0
					Save	Close

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.



Index       1         Enable       Image: Construction code         Description       test         Slave ID       1         Function Code       03-Holding-Register         Register Address       3         Data type       Uint16         Data type       Uint16         Data type       Uint16         Data Endian       AB         Plus       0         Subtract       0         Divisor       1         O       Multiplier         Multiplier       1         O       Shift Right Bits         O       O         Number Of Bits       16         Keep Decimal Places       0         O       O         Status       Modbus Alarm         Modbus Pol       Modbus Write         Index 1       1         TCP       1       3       read successed       21	Channel List				
Description       test         Slave ID       1         Function Code       03-Holding-Register         Register Address       3         Data type       Uint16         Data type       Uint16         Data type       Uint16         Data type       Uint16         Data type       0         O       O         Subtract       0         Divisor       1         O       O         Multiplier       1         Shift Right Bits       0         Number Of Bits       16         Keep Decimal Places       0         O       O         Statz       Modbus Alarm         Mutber Of Bits       0         O       O         Statz       Modbus Alarm         Modbus Poll       Modbus Alarm         Modbus Poll	Index	1			
Slave ID       1         Function Code       03-Holding-Register         Register Address       3         Data type       Uint16         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	Enable	1			
Function Code       03-Holding-Register         Register Address       3         Data type       Uint16         Data type       Uint16         Data type       Uint16         Data Endian       AB         Plus       0         Subtract       0         Divisor       1         O       O         Multiplier       1         Shift Right Bits       0         Number Of Bits       16         Keep Decimal Places       0         Save       Close	Description	test			
Register Address       3         Data type       Uint16         Data type       Uint16         Data Endian       AB         Plus       0         Subtract       0         Divisor       1         Divisor       1         Multiplier       1         Shift Right Bits       0         Number Of Bits       16         Keep Decimal Places       0         Status       Modbus Anam         Modbus Poll       Modbus Airm	Slave ID	1			
Data type       Uint16         Data Endian       AB         Plus       O         Subtract       O         Divisor       1         Divisor       1         Multiplier       1         Shift Right Bits       O         Number Of Bits       16         Keep Decimal Places       O         Status       Modbus Poll         Modbus Poll       Modbus Airm         Modbus Poll       Modbus Virte         Channel Status       Image Status         Index       Description       Connection Index         Type       Silve ID       Register Address       Function Code       Status       Value	Function Code	03-Holding-Register	• •		
Data Endian       AB         Plus       0         Subtract       0         Subtract       0         Divisor       1         O       0         Multiplier       1         Shift Right Bits       0         Number Of Bits       16         Keep Decimal Places       0         Status       Modbus Poil         Modbus Poil       Modbus Write         Channel Status       Index Desription         Index       Type       Save ID       Register Address       Function Code       Status       Value	Register Address	3			
Plus       O         Subtract       O         Divisor       1         Divisor       1         Multiplier       1         Shift Right Bits       O         Number Of Bits       16         Keep Decimal Places       O         Status       Modbus Poll         Modbus Poll       Modbus Alarm         Modbus Poll       Modbus Vrite         Channel Status       Inction Code         Status       Value	Data type	Uint16	•		
Subtract 0 0 0 Divisor 1 0 Multiplier 1 0 Shift Right Bits 0 0 Number Of Bits 16 0 Keep Decimal Places 0 0 Save Close	Data Endian	AB	•		
Divisor 1 ① Multiplier 1 ② Shift Right Bits 0 ③ Number Of Bits 16 ③ Keep Decimal Places 0 ③ Save Close Save Close	Plus	0		0	
Multiplier       1       ⑦         Shift Right Bits       0       ⑦         Number Of Bits       16       ⑦         Keep Decimal Places       0       ⑦         Save       Close         Status       Modbus Poll       Modbus Alarm         Modbus Poll       Modbus Alarm       Modbus Write         Channel Status       Index Description       Connection Index       Type         Save D       Register Address       Function Code       Status       Value	Subtract	0		?	
Shift Right Bits 0 ⑦ Number Of Bits 16 ⑦ Keep Decimal Places 0 ⑦ Save Close Save Close Status Modbus Poll Modbus Alarm Modbus Write Channel Status Index Description Connection Index Type Siave ID Register Address Function Code Status Value	Divisor	1		0	
Number Of Bits     16     ⑦       Keep Decimal Places     0     ⑦       Save     Close         Status     Modbus Poll     Modbus Alarm     Modbus Write         Channel Status       Index     Description     Correction Index     Type   Save Discription Correction Index Type Slave ID Register Address Function Code Status Value	Multiplier	1		?	
Keep Decimal Places       Image: Close         Save       Close         Status       Modbus Poll         Modbus Poll       Modbus Alarm         Modbus Poll       Modbus Write         Channel Status       Index         Index       Description         Correction Index       Type         Silve ID       Register Address         Function Code       Status         Value       Value	Shift Right Bits	0		0	
Status         Modbus Poll         Modbus Alarm         Modbus Write           Channel Status         Index         Description         Correction Index         Type         Slave ID         Register Address         Function Code         Status         Value	Number Of Bits	16		0	
<u>Status</u> Modbus Poll Modbus Alarm Modbus Write Channel Status Index Description Connection Index Type Siave ID Register Address Function Code Status Value	Keep Decimal Places	0		0	
<u>Status</u> Modbus Poll Modbus Alarm Modbus Write Channel Status Index Description Connection Index Type Slave ID Register Address Function Code Status Value				C	Class
Channel Status Index Description Connection Index Type Slave ID Register Address Function Code Status Value				Save	Close
Channel Status Index Description Connection Index Type Slave ID Register Address Function Code Status Value					
Index Description Connection Index Type Slave ID Register Address Function Code Status Value		is Write			
1 testi 1 TCP 1 3 3 read successed 21		lave ID Register Address	Function Code	Status	Value
	1 test1 1 TCP	1 3	3	read successed	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 ⑦
Connection Timeout	30 ⑦
Enable Verbose Log	
Transport Data Settings	
Data Location	NULL • ⑦
Data Format	\$SERIAL_NUMBER,\$DATE,\$S ③
Line Break	
Modbus Channel	
Index Enable Connection Index Filter I	tems Channel Index Slave ID Register Address $\oplus$
	Save Close



Channel Settings				
Modbus Channel				
	Index 1			
	Enable 🗹	)		
Conne	ction Index 1	•	?	
2	Filter Items	ave ID 🔹		
	Slave ID 1		0	
			Save	Close
Reconne		,	÷	
Connectio	on Timeout 30	)	?	
Enable V	erbose Log 🛛 🗹	)		
Transport Data Settings				
Da	ta Location 🛛 🛛 🔊	ULL 🔻	?	
D	ata Format 🛛 \$9	SERIAL_NUMBER,\$DATE,\$S	?	
	Line Break 🛛 🗹	)		<b>1</b>
Modbus Channel				
Index Enable Connection Ir	ndex Filter Items	Channel Index Slave 1	ID Register A	ddress
			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>Stat</u>	tus Mo	odbus Transpo	rt X.509 Cei	rtificate	
Conne	ction Statu	IS			
Index	Enable	Description	Protocol	Status	Uptime
1	true	TCP Setting	TCP Client	Connected	00:02:35

The remote TCP Server received the data successfully.



**MODBUS** 

**Rev 2.8** 

🔄 CreateConnn 🔕 CreateServe	🛛 🛞 StartServer 🛞 🐼   😪 Connect 🗝   🏖 DisconnAll   💥 DeleteConn 🎇   🔟   🕏 🍃
Properties 🛛 🕂 🗙	/≱ 192.168.111.199:54324 4 ▷
<ul> <li>Client Mode</li> <li>Server Mode</li> <li>Server Mode</li> <li>Local(192.168.247.1):2000</li> <li>192.168.111.199:54324</li> </ul>	DestIP:       Send AtuoSend Eve 100 ms       Send Stop         192.168.111.199       DestFort:       54324         Image: Send Point       Send Hex Image: Send File Send Received       Clear Option         192.168.111.199       DestFort:       54324         Image: Send Point       Send Hex Image: Send File Send Received       Clear Option         192.168.111.199       DestFort:       54324         Image: Send Point       Send Hex Image: Send File Send Received       Clear Option         192.1000       Type TCP       Image: Send File Send Received       Clear Option         192.1000       Type TCP       Image: Send File Send Received       Send Option         Image: Send Point Send File Send Received       Image: Send Option Send File Send Received       Send Option Send File Send Received         Count       Send Option       Senve (In Time)       Image: Send Send Send Send Send Send Send Send
<	Reov         62622           19015124330001, 2020-02-18 16:31:15, 1, 3, 21           19015124330001, 2020-02-18 16:31:15, 1, 3, 21           19015124330001, 2020-02-18 16:31:16, 1, 3, 21           19015124330001, 2020-02-18 16:31:16, 1, 3, 21           19015124330001, 2020-02-18 16:31:16, 1, 3, 21           19015124330001, 2020-02-18 16:31:16, 1, 3, 21           19015124330001, 2020-02-18 16:31:16, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21           19015124330001, 2020-02-18 16:31:17, 1, 3, 21

### 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.

Connection Settings Connection List				
	Index	1		
	Enable			
	Description	FTP Setting		
	Protocol	FTP •	1	
	Server Address	14.215.177.39		
	Server Port	21		
	Username	admin		
	Password	adminftp		
Cor	nnection Timeout	30	0	
	Try To Send	3	?	
Ena	able Verbose Log			
Transport Data Setting	js			
	Data Location	NULL	0	
F	Add CSV File Title			
	File Name	\$SERIAL_NUMBER_\$DATE.cs	?	
	Upload Interval	30	0	
	Data Format	\$SERIAL_NUMBER,\$DATE,\$S	0	
			Save	Close

**Step 3** Enable "Modbus Channel", and the Modbus Master will select the value to send to the remote FTP server from Modbus Slave.



MODBUS

Channel Settings		
Modbus Channel		
	Index	1
	Enable	
	Connection Index	1 ⑦
2	Filter Items	Slave ID 🔹
	Slave ID	1 ⑦
		Save Close
	Try To Send	3
E	nable Verbose Log	
Transport Data Setti	ngs	
	Data Location	NULL
	Add CSV File Title	
	File Name	\$SERIAL_NUMBER_\$DATE.cs
	Upload Interval	30 ⑦ 〔1
	Data Format	\$SERIAL_NUMBER,\$DATE,\$S ⑦
Modbus Channel		
Index Enable Cor	nnection Index Filter I	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.

Connection Status           Index         Enable         Description         Protocol         Status         Uptime           1         true         FTP Setting         FTP         Sent Successfully	<u>Stat</u>	tus M	Iodbus Transport	X.509 C	ertificate	
	Conne	ction Stat	tus			
1 true FTP Setting FTP Sent Successfully	Index	Enable	Description	Protocol	Status	Uptime
	1	true	FTP Setting	FTP	Sent Successfully	

### Remote FTP Server received the CSV file successfully.

Ì → 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
R	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.

Connection Settings			
	Enable		
	Description	MQTT Setting	
	Protocol	MQTT 🔻	
	Server Address	192.168.111.93	
	Server Port	1883	
	Enable SSL		
	Username	mo_test	
	Password	test123456	
	Client ID		0
	Subscribe Topic		0
	Keepalive	60	0
Re	econnect Interval	60	?
Cor	Connection Timeout		0
	Enable LWT		
En	able Verbose Log		
Transport Data Setting	JS		
	Data Location	NULL	0
	Data Format	\$SERIAL_NUMBER,\$DATE,\$S	0
			Save Close

Step 3 Enable "Modbus Channel", define the "Topic" to publish to MQTT Broker with Modbus data.

Channel Settings			
Modbus Channel			
	Index	1	
	Enable		_
	Publish Topic	test	
	Connection Index	1	• ?
2	Filter Items	Slave ID	·
	Slave ID	1	0
			Save Close
C	onnection Timeout	30	0
	Enable LWT		
E	nable Verbose Log		
Transport Data Settir	igs		
	Data Location	NULL	] ⑦
	Data Format	\$SERIAL_NUMBER,\$DATE,\$S	
	Line Break		<b>0</b>
Modbus Channel			
Index Enable Con	nection Index Filter It	tems Channel Index Slave	e ID Register Address 🕒 🚽
			Save Close

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



**Step 5** Go to **Application>Modbus Transport>Status**, The 6944(Modbus Mater) had connected to the remote MQTT broker successfully.

Stat	<u>us</u> M	lodbus Transport	X.509 Ce	ertificate		
Conne	ction Stat	us				
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

March				00
x = 403: Em = 0: 10	) = 1: F = 01: SR	- 2000ms		
Akas	33800			
2	0	15 Write Multiple Colti	×	
2	0	SeelD. 1. Contact	Sent	
4		L 100 1 3860	Cancal	
5			Concernant and	
7		Quevily: 2	And the second second	
			Dpen	
9			Sare	
		A.c.		
SE SX		B B 15 16 22 23   441   <b>5 17</b>		
- Bax	n 5   5   6   A 0 - 1: F - 61: 50			
- 403 Err - 0 1		t - 2000ms		(
- 403 Err - 0 1		1 - 2000ms	×	c
3 1444-145 (x = 403: Err + 0; 8		1- 2000ans	20 Savar	c
		1 - 2000me TS Write Multiple Colt Garanto 1 Addres 1300	00 Sant Crool Sans	c
- 403: Eer - 0: 0		1 - 2000me TS Write Multiple Colt Garanto 1 Addres 1300	Dpen	c
- 403: Err - 0: 1		1 - 2000me TS Write Multiple Colt Garanto 1 Addres 1300	Dpen	c
	0 - 1: F - 012 Set	1 - 2000me TS Write Multiple Colt Garanto 1 Addres 1300	Dpen	c
Marthan Pati - Milare		1 - 2000me TS Write Multiple Colt Garanto 1 Addres 1300	Dpen	
	53900 53900 0 0 0 0 0 0 0 0 0 0 0 0	- 2000me	Dpen	c
Adaptation Ford - Molecular Adaptation of the second seco	53900 53900 0 0 0 0 0 0 0 0 0 0 0 0	- 2000me	Dpen	
Adaptation Ford - Molecular Adaptation of the second seco	53900 53900 0 0 0 0 0 0 0 0 0 0 0 0	I - 2000me           I - 2000me           I - 2000me           I - 2000me	Jame Jame	
	D - 1: F - 41: SR 33900 0 0 0 0 0 0 0 0 0 0 0 0		Same Same	
	D - 1: F - 41: SR 33900 0 0 0 0 0 0 0 0 0 0 0 0	I - 2000mm           I - 2000mm           I - 2000mm           I - 2000mm           I - 2000mm		

### **Control Digital Output**

Go to **Functions>15: Write Multiple Coils**, to change the DO state from "0"to "1".s **Test Successful** 



# 20.3 MODBUS to DNP3

This document contains information regarding the configuration and use of Modbus to DNP3 software on the 6944.

# Software versions

Release Date	Doc. Version	Firmware Version	Additional software	Change Description	
2020/07/17	V1.0.0	V1.1.4(0c0c9fa)	Please contact Case	First released	

# **Testing Topology**



- A 6944 Router runs as a Modbus to DNP3 converter, it acts as a Modbus Master and DNP3 Outstation.
- A serial device supports Modbus protocol and acts as a Modbus Slave. It connects to the 6944 router via its serial port or Ethernet port.
- The 6944 router polls the Modbus data from the end device (Modbus Slave), then sends the data to the remote DNP3 Master.

# Configuration

### **Configuring the 6944**

**Step 1** Go to **Applications>Modbus To DNP3>Modbus Master**, specify the serial settings to make the router connect to the Modbus Slave via RS232 interface:

Overview	Status	Modbus Master	DNP3 Outstation					
Link Management	Connectio	Connection Settings						
Industrial Interface	Index	Connection List					dress Server Port	$\oplus$
Network			Index	1				
Applications			Enable					
DDNS			Description		]			
SMS			Scan Rate	1000	0			
Schedule Reboot Modbus To DNP3			Reconnect Interval	60	0			
VPN			Response Timeout	1000	0			
Maintenance		[	Delay Between Polls	0	0			
Maintenance			Connection Type	RS232 *	]			
		1	Enable Show Status					
		1	Enable Verbose Log					
		Serial Settings						
			Baud Rate	115200 •				
			Parity	None •	]			
			Data Bits	8 •	]			
			Stop Bits	1 *	]			
		Channel List						
		Index Enable	Description S	ave ID Function Code	Reaister Address	(+)		Analy
					Save	Close	Save	Apply

**Step 2** Go to **Applications>Modbus To DNP3>Modbus Master>Channel List**, specify the Modbus Master settings and the DNP3 data type:



**Rev 2.8** 

verview	Status			DNP3 Outstat	tion	_		-		_	_				
ink Management	Connectio	Connectio	on Settings	8							_				
ndustrial Interface	Connection	Connectio	on List									dress	Server Por		$( \mathbf{+} )$
	1			In	dex	1							502		$\boxtimes$
letwork	•			Ena	able	1							502		
pplications				Descript	tion										
DDNS SMS				Scan R	late	1000			0						
Sms Schedule Reboot				Reconnect Inter	rval	60			0						
Modbus To DNP3				Response Time	out	1000			0						
'PN				Delay Between P	olls	0			0						
laintenance				Connection T	уре	RS232		٠							
				Enable Show Sta	atus										
				Enable Verbose I	Log										
		Serial Set	tings												
				Baud R	late	115200		٠		1					
				Pa	rity	None		٠							
				Data I	Bits	8		٠							
				Stop I	Bits	1		•			<b>V</b>				
		Channel I	.ist									-			
		Index	Enable	Description	S	lave ID	Function Code		Register Address		$\oplus$	-			
									Save	Close		s	ave	App	y
															_

Channel Settings		
Enable		
Description		
Slave ID	1	
Function Code	03-Holding-Register	•
Register Address	0	
Data type	Uint16	•
Data Endian	AB	•
Plus	0	0
Subtract	0	0
Divisor	1	0
Multiplier	1	0
Shift Right Bits	0	0
Number Of Bits	16	0
Keep Decimal Places	0	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:

Overview	Status	Modbus Master	DNP3 Outstation		
Link Management	DNP3 Outsta	ation Settings			
Industrial Interface			Enable		_
Network			Local IP	0.0.0.0	
Applications			Local Port	20000	
DDNS			Link Address	1024	
SMS Schedule Reboot			Master Link Address	1	
<ul> <li>Modbus To DNP3</li> </ul>			Enable Unsolicited	<b>A</b>	
VPN	Data Setting	s			
Maintenance			Data Location	FLASH •	0
			Send Interval	60	0
			Number of Sent	5000	0
	Advanced Se	ettings			
			Server Accept Mode	Close New •	]
			Keepalive Timeout	0	0
			Enable Verbose Log		
					Save Apply
					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":

Modbus	Slave - Mbslave1							
File Edit	ile Edit Connection Setup Display View Window Help							
🗅 🛸 🖬								
🔛 Mbslave								
ID = 1: F =	03							
	Alias 00000							
0	88							
1	0							
2	0							
3	0							
4	0							

Step 2 Check that the 6944 has polled and retrieved data from the Modbus Slave successfully:

Overview	Stat	us Moo	dbus Master	DNP3 Out	station								
Link Management	Channe	el Status											
Industrial Interface					E	Enable True							
Network				DNP3 (	Outstation S	Status Opening							
Applications	Channe	el Status											
DDNS	Index	Description	Connection Index	х Туре	Slave ID	Register Address	Function Code	DNP3 Type	DNP3 Class	DNP3 Index	Status	Value	
SMS	1		1	RS232	1	0	3	Counter Input	Class 2	0	read succe	88	
Schedule Reboot	_											_	
► Modbus To DNP3													

### **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):

Simulator		- 0
🖸 Add 🛛 🔚 File		@ 4
DNF3	17:02:24.234     INFO     svstem     Initialized DNP3 plugin       Ø Add DNP3 Channel     ×       TCP Client     TCP Server     Serial       192.168.5.1     Host	
	20000 🛊 Port	
Metric Value	Settings     Logging       channel     Alias     Image: Front or state of the stat	
	Add Cancel	

Step 2 Right Click "channel", and Add Master:



Simulator					- 0
🔘 Add 📓	File				G
2 Chiunci	Add Master Add Outstation Remove	17:02:24.234	INFO system	Initialized DNP3 plugin	

Step 3 Specify the address on the DNP3 Master, to make it match the settings on the 6944 (DNP3 Outstation):

Simulator	_	
🗘 Add 🛛 🙀 File		6
	Add Master x Link Master x Link Master 1024 to source 1024 to sestination confirme options 0 to retries 1000 to timeout (ms) Logging master Alias Add	

Step 4 Right Click "Master" and open it:

Simulator					-	
🗘 Add 🛛 🔚 File						6
DNP3	17:19:12.935	-ll->	master	Function:         PRI UNCONFIRMED         USER         DATA         Dest:         1024           05         64         11         C4         00         04         01         00         60         4E	Sou:	rce:
Remove	17:19:12.938	<-TT-	channel	Function: PRI UNCONFIRMED USER DATA Dest: 1 Sc 05 64 0A 44 01 00 00 04 67 88	urce	: 102

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:

S.	DNP3 Master (r	master)					_	$\times$
Cou	nter	~	Index	Value	Flags	Timestamp (UTC)		
Scens	Туре	Period	0	88	0x01 - ONLINE	2020/7/17 09:19:12.000 (syn		
CROB								
A0								
Custom								

Step 6 Test successful.



# **20.4 AN053 IEC 101 to IEC 104**

### **Overview.**

This document contains information regarding the configuration and use of IEC101 to IEC104.

# **Software Compatibility**

Release Date	<b>Doc. Version</b>	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>
2020/07/17	V1.0.0	V1.1.4(0c0c9fa)	(e9b6efe)	First released

### Topology



- The 6944 Router runs as an IEC101 to IEC104 converter.
- A serial device supports the IEC101 protocol and acts as slave connected to the 6944 router via a serial port.
- The IEC104 master connects to the 6944 router via TCP and requests data from the slave. After that, the slave will send the data to the master as requested.

# Configuration Configuring the 6944

**Step 1** Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC101 configuration, like below:

Overview	Status	IEC101 To IEC104 Connection Settings					
Link Management	Connectio	Index	1			^	
Industrial Interface	Index E	Enable	<b>v</b>				$\oplus$
Network	1	Description					
Applications		Enable Verbose Log					
DDNS		IEC101 COM Settings					
SMS		COM Type	RS232 •				
Schedule Reboot FIEC101 To IEC104		Baud Rate	9600 •				
VPN		Data Bits	8 •				
Maintenance		Stop Bits	1 •				
Maintenance		Parity	None •				
		IEC101 Settings					
		Cyclic Interval	1000	0			
		Number Of Retries	3	0			
		Link Address	1				
		Link Address Length	1 •				
		Cause Of Transmission Length	1 •				
		Common Address Length	1 •				
		Information Object Address Length	2 *			-	
				Save	Close		
				ouve	ciose	Save	Apply

**Step 2** Go to **Applications>IEC101 To IEC104>Connection**, specify the IEC104 configuration, as shown below:



Local 1	IP 0.0.0.0			
nance Local Po	ort 2404			
IEC104 Settings				
T1 Timeo	ut 15	0		
T2 Timeo	ut 10	0		
T3 Timeo	ut 20	0		
	K 12	0		
	W 8	0		
Cause Of Transmission Lengt	th 2	•		
Common Address Lengt	th 2	•		
Information Object Address Lengt	th 3	•	Save	Apply

### 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:

Select Com Port	СОМ 3
Data rate	9600
Word Size	8
Parity	Even
Stop Bits	1

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:

Overview	Sta	tus	Connection				
Link Management	IEC10	1 To IE	C104 Status				
Industrial Interface	Index	Enable	СОМ Туре	IEC101 Connection Status	Client IP	Client Port	IEC104 Connection St
Network	1	true	RS232	Connected	192.168.111.19	50548	Connected
Applications							
DDNS							
SMS							
Schedule Reboot							
IEC101 To IEC104							

Step 4 Connected successfully

### **Testing**

IEC104 Master requests data from the IEC101 Slave

IEC104 Master receives data from the IEC101 Slave



**Rev 2.8** 

This page left blank intentionally



# 21. AT Commands

# 21.1. AT Over IP

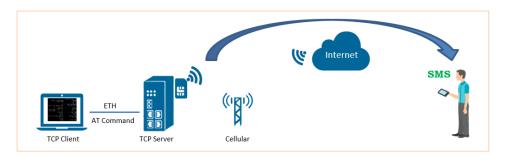
# Overview

This document contains information regarding configuring the 6944 to run AT Over IP

### Software Compatibility

Release Date	Doc. Version	<b>Firmware Version</b>	Additional Software	Change Description
4.7.2019	V1.1	V1.1.4 (0c0c09fa)	AT over IP	First release
			1.0.1 (42ccf3e)	

# 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:

Overview	Status	AT Over IP				
Link Management	General Settin	ngs				
Industrial Interface			Enable	1		
Network			Protocol	TCP Server		
Applications			Local IP			
DDNS			Local Port	5636		
SMS Schedule Reboot			-			
► AT Over IP						
VPN						
Maintenance						
					Save	Apply

**Step 2** Click Save>Apply.

# **Testing**

Send the message "TEST" to the mobile phone under PDU mode as an example message.

yy AT Commands and Content that needs to be sent one by one to the router.

- a.  $at+cmgf=0\r$
- b.  $at+cmgs=17\r$
- c. 0001000BA15119852081F0000004D4E2940A
- d. 1a

Note: "r" selects the keyboard "Enter"; Option "c" for the content to be sent under PDU mode; Option "d" is the end code to be sent with HEX.

**Step 1** Run SSCOM software as a TCP client and connect the 6944 router (TCP Server), as shown below.

ORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_author	PCB_proofing			
ar	Data OpenFile	1					SendFile S	top ClearSead 6	₹ English Sa	weConfi a	ETT
-	Data OpenFile							top ClearSend			
Nun	TCPClient						vedToFile 🖂 :	SendHEX   SendEv	ery: 1000 .	s/Tin∏	AddCrLf
Nun ot 1	TCPClient 92.168.5.1						vedToFile 🖂 :	the second secon	ery: 1000 .		AddCrLf
Nun ot 1	TCPClient	5636					vedToFile 🖂 :	SendHEX   SendEv	ery: 1000 .	s/Tin∏	AddCrLf

Step 2 Send the AT command "at+cmgf=0\r" to make sure it's under PDU mode.

SS SS	COM V5.12 Serial	/Net data	debugger,A	uthor					-		×
PORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_author	PCB_proofing			
at*ong OK	£=0										~
Clear	Bata OpenFile	1					Sendrile St	op ClearSend 🔽	English Save	Confiel	ст I —
	TCPClient		• •	True Save		Receiv		SendOEX   SendEve			
the later of the l	92.168.5.1	5636						Bytes Add Verif		-	
and the second se		777	Discond at*e	mgf=0\r				-			^
		-	XD CK								

**Step 3** Send the AT command "at+cmgs=17\r" to start to sending the content.



**AT Commands** 

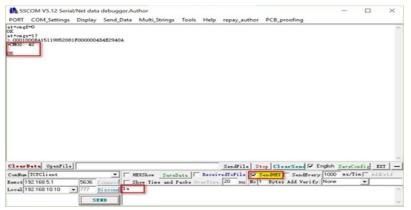
**Rev 2.8** 

SSI SSI	COM V5.12 Serial	/Net data	debugger,Au	uthor							×
PORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_autho	or F	CB_proofing		
t *ongi K t *ongs											
	OpenFile								ClearSend F En		
lenot 1	TCPClient 92.168.5.1	5636	searce I S	Show Time and 1					dHEI   SendEvery Bytes Add Verify:	/Tin T A	ddCrLf
ocal 1	92.168.10.10	777	iscons at*e	mgs=17\r							9

Step 4 Send the content.

	COM V5.12 Seri									-		×
ORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_author	PCB_proc	ofing			
*ces	£≈0											
+cng	s=17											
0001	0008A1511985208	51F0000004	D422940A									
	Baba (SurFi)	1					e		- 17 m	deb c		
-	Data OpenFile	•					Sendřile S	section and and the section of the s	_		management of a survey	
n N un	TCPClient			ISher Savel			edToFile 🖂	Sender [	SendEvery:	1000 ms/	management of a survey	_
80		5636	Connect I S	how Time and I	Packe Or	erTine	20 ms No	Sender [	SendEvery:	1000 ms/	management of a survey	
al dia	TCPClient	5636	Connect I S		Packe Or	erTine	20 ms No	Sender [	SendEvery:	1000 ms/	Tin T Ad	_

**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.



**Rev 2.8** 





# 21.2. AT Over Telnet

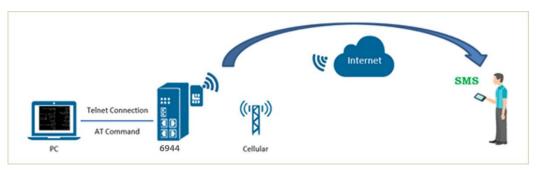
# Overview

This document contains information regarding the configuration and use of AT over Telnet.

# **Software Compatibility**

<b>Release Date</b>	<b>Doc. Version</b>	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>
18.7.2019	V1.1	V1.1.4 ()	1.0.1 (42ccf3e)	First release

# **Testing Topology**

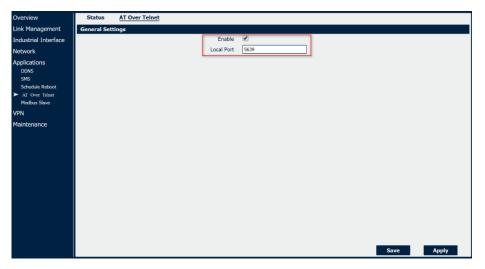


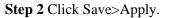
- The 6944 connects to the Internet via its SIM card.
- The PC connect to the 6944 via an ethernet cable using the Telnet protocol.
- The PC sends an AT Command to control the module in the 6944 to undertake an action.

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:





### **Testing**

As a test send the content "TEST" to the mobile phone in text mode. We have shown the AT Command required to be sent to the 6944 router, with one command at a time. at+cmgf=1

```
at+cmgs="15915802180"
```

>TEST



*Note: After entering the content "TEST", please press the keyboard "Ctrl+z" to send the SMS.* 

**Step 1** Run the "putty" software and telnet to the router, enter the AT command to trigger the 6944 module to send the SMS as shown below:

192.168.5.1 – PuTTY	
At	
ERROR	
At	
OK	_
At+cmgf=1	
OK	
At+cmgs= 078875277882	
>TEST	
+CMGS: 237	
OK	
	•

Step 2 The Mobile phone receives the SMS with content "TEST":



Step 3 Test successfully.





# 21.3. AT Over COM

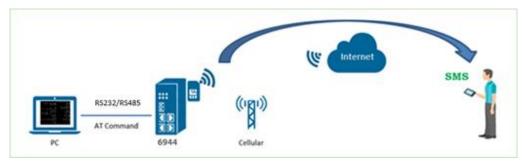
# Overview

This document contains information regarding the configuration and use of AT Over Com

### **Software Compatibility**

<b>Release Date</b>	<b>Doc. Version</b>	<b>Firmware Version</b>	Additional Software	<b>Change Description</b>							
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	Status	AT Over COM						
Link Management	General Set	tings						
Industrial Interface				Enable				
Network				COM type	RS232 •	-		
Applications			l l	Baud Rate	115200 •	•]		
DDNS				Data Bits	8 •	-		
SMS				Stop Bits	1 •	•		
Schedule Reboot AT Over IP				Parity	None •			
► AT Over COM								
AT Over Telnet								
Modbus Slave								
VPN								
Maintenance								
							Save	Apply
	-							

**Step 2** Click Save>Apply.



# **Testing**

**Step 1** Send the content "HELLO" to the mobile phone using text mode to test.

Below is the AT Command and content need to be sent one by one to the router.

a) at+cmgf=1r

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:

ORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_author	PCB_proofin	9		
						_					
arD	ata OpenFile						File Step Cl				
_	ata OpenFile			Show SaveData		eivedToF	ile 🗆 Sender	SendEvery	1000 ms/		
Nun				Show SaveData Time and Pack		eivedToF	ile 🗆 Sender	SendEvery	1000 ms/		
Nun Cl	COM4	More Sett				eivedToF	ile 🗆 Sender	SendEvery	1000 ms/	Tin A	

Step 3 Send the AT command "at+cmgf=1\r" in TEXT mode

SS SS	COM V5.12 Seria	l/Net data	a debugger, A	author					-	- 0	×
	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_auth	or PCB_proo	fing		
t*ongi K	-1										
						See	Wile Step	ClearSend F	English Su	veConfie	
lear	openFile							on case of case it.			EXT -
			▼ F HEXS	how SaveData	E Rece				_		
on Nun	COM4		tings T Show	Time and Pack		ivedIel	ile 🗆 Send	DEX   SendEve	ry:1000		
Condition		More Set		Time and Pack		ivedIel	ile 🗆 Send	DEX   SendEve	ry:1000	s/Tis	



**Step 4** Send the AT command "at+cmgs=15915802180\r" to start to send the content to the designated phone number.

SS SS	COM V5.12 Seria	l/Net data	debugger,A	uthor:					-		×
PORT	COM_Settings	Display	Send_Data	Multi_Strings	Tools	Help	repay_author	PCB_proofing			
at*ongf	=1										^
AT +CN 25	="15915802180"										
2											
											~
Clear	Data OpenFile					Sen	File Stop Cl	earSend 🔽 Englis	th SaveCo	onfiel E	xt   -
ConNun			· DEXS	how SaveData	E Rec			SendEvery: 10			
	oseCon 👌	More Sett						es Add Verify: No		-	
	DTR Baudka		+ at+ongs	=15915802180\r	1						~
It mis	in one ofference										
		SEND									~

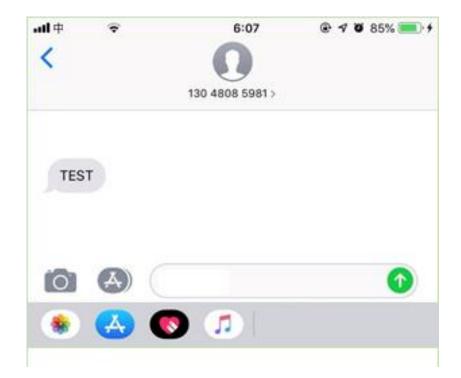
Step 5 Send the message "HELLO".

🏠 SSCOM V5.12 Serial/Net data debugger,	-	
PORT COM_Settings Display Send_Data Multi_Strings Tools Help repay_author PCB_proofing		
at *engf=1 OK T*CM22="15915802180" NELLO SUBJ		~
ClearData OpenFile Stop ClearSend V Englis	h	et al 1977   _
ConNun COM4		
	ne	V AGOLFLE
CloseCom C More Setting Show Time and Packe OverTime: [20 mg] No 1 Bytes Add Verify: Nor RTS V DTR BaudRat 115200 VELLO		^
SEED		~

Step 6 Send the ending code "1a" with HEX. The reply "OK" means the SMS was sent successfully.

case	$\mathbf{X}$			5	Section T	wenty	- One			6	944 Manua
mmunications					AT Co	mman	ds				<b>Rev 2.8</b>
	PORT COM				Multi_Strings	Tools H	Help rep	ay_author	PC8_proofing	- 0	×
	at +cmgf=1 OK AT +CMSS="15910 > NELLO +CMSS: 64	802180″									~
	pr.										
											~
	ClearData	)penFile		_					arSend 🔽 Engl		
	ConNun COM4								SendEvery 10 Add Verify: No		AddCrLE
	RTS DT			- 1.			1.1.1.1				^
		Г	SEND								

Step 7 When the test is successful, the mobile phone will receive the SMS message.





**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

SMS	Gatewa	ay Notification		
General	Settings			
		Enable	•	
		Authentication Type	Password •	
Allow Pl	none Book			
Index	Description	Phone Number		( )

#### 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
Notification Channel Settings		-	
Index	1		
Description			
Phone Number			
Startup Notify			
Reboot Notify			
NTP Update Notify			
LAN Port Status Notify			
WAN Port Status Notify			
WWAN Port Status Notify			
Active Link Status Notify			
Digital Input Status Notify			
Digital Output Status Notify			
IPSec Connection Status Notify			
Openvpn Connection Status Notify			
		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



### 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.

Index	1
Description	
Phone Number	
Startup Notify	
Reboot Notify	
NTP Update Notify	
LAN Port Status Notify	
WAN Port Status Notify	
WWAN Port Status Notify	
Active Link Status Notify	
Digital Input Status Notify	
Digital Output Status Notify	
IPSec Connection Status Notify	
Openvpn Connection Status Notify	

**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.

Schedule Reboot	
General Settings	
Enable	
Time to Reboot	00:00 ⑦
Day to Reboot	0 ⑦

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.



	S				Login: admin Reboot	Logout
Overview	SMS	Gateway	Notification			
Link Management	General	Settings				
Industrial Interface			Enable	$\checkmark$		
Network			Authentication Type	Password		
Applications	Allow Ph	one Book				
DDNS	Index	Description	Phone Number			$\oplus$
<ul> <li>SMS</li> <li>Schedule Reboot</li> <li>Modbus Slave</li> <li>VPN</li> <li>Maintenance</li> </ul>	1	Test	07777777777			⊠ ⊗

# **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.

Case 2	5				Login: admin Reboot	Logout
Overview	SMS	Gateway	Notification			
Link Management	General S	Settings		airean		
Industrial Interface			Enable			
Network			Authentication Type	Password V		
Applications	Allow Pho	one Book				
DDNS	Index	Description	Phone Number			$\oplus$
<ul> <li>SMS Schedule Reboot Modbus Slave</li> <li>VPN Maintenance</li> </ul>	1	Test	07777777777			⊻⊗

Under General Settings you have the following options:

User Name and Password: Force the manager to enter a user name and password (recommended)

**User Name and Password**: None – allows the manager to connect without using a user name and password.

Allow Phone Book: This option only allows the 6944 to send and receive SMS messages from numbers in its internal directory.

### **SMS Commands**

### **Authentication Type: Password**

1. admin\$admin\$enable\$version // send an SMS to check the firmware version

- *The first "admin" means the router username;*
- The second "admin" means the router password;
- "enable" means to send the CLI Command used in "enable mode".
- "version" is the CLI command under enable mode

2. admin\$admin\$config\$set syslog level info //send SMS to set router syslog to info level

- *The first "admin" means the router username;*
- The second "admin" means the router password;
- "config" means to send the CLI Command of "config mode".
- "set syslog level info" is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, as shown below

### admin\$admin\$enable\$version;show active_link //

- send SMS to check firmware version and link information together. admin\$admin\$config\$set syslog location ram;set syslog level info //
- send SMS to set syslog location and syslog level.
- admin\$admin\$enable\$reboot
- This option reboots the 6944



Authentication Type: None (i.e. only using the 6944 telephone directory for security)

- 1. enable\$version
- 2. config\$set syslog level info
- 3. enable\$version;show active_link
- 4. config\$set syslog location ram;set syslog level info

# **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</p>

config#

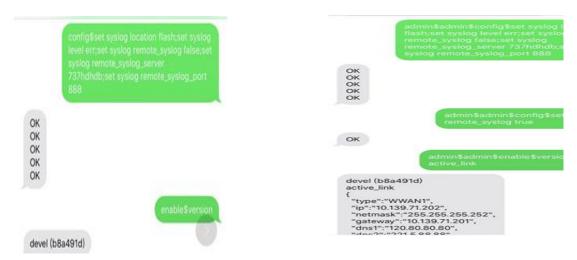
Step 2 When you have connected to the router using telnet, it pops up with the character

">",

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

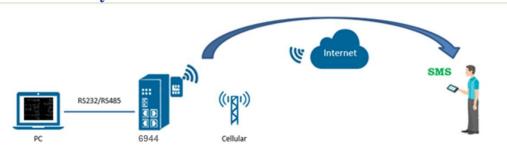
>

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	e 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 Sett	ings				
Industrial Interface			Enable			
Network			Authentication Type	Password •		
Applications			SMS Source	Serial Port •		
DDNS	Serial Port S	ettings				
<ul> <li>SMS</li> <li>Schedule Reboot</li> </ul>			Serial Port	COM2 •		
GPS			Baud Rate	115200 •		
SNMP			Data Bits	8 •		
DMPC			Stop Bits	1 •		
VPN			Parity	None •		
Maintenance						
					Save	Apply

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

### Testing

Send a message (in our example it is "**hello**") to the mobile phone. Here are the commands that needs to be sent to the router via RS232 Port.

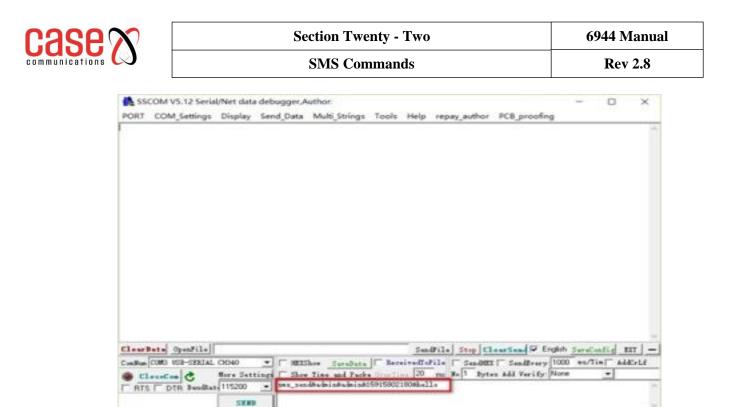
# a) sms_send&admin&admin&15915802180&Text_To_Send

b) 1a // it is the ending code and need to be sent with "HEX"

*Here is the explanation of the command "a":* 

sms_send&username&password &phone number&SMS content

Step 1 Run the SSCOM software and connect the 6944 router via serial port, as below:



Step 2 Send the SMS with the content "hello" to a receiver phone number for example. 15915802180".

Step 3 Send the ending code "1a" with "HEX":

A ssi	COM V5.12 Seria	d/Net data	debugger,						 	×
PORT	COM_Settings	Display	Send_Date	Multi_Strings	Tools	Helpi	repay_author	PC8_preading		_
OR										
										in the second
	Inta Cpenfile				1			Learling IP Engli		
	CORD WIR-CONTAL							Sandlenry 10		0.94
	DIR Busilia		a la	Tine and Pack		1.150	antimate abe	es Add Varify No	 -	_

Step 4. If the test is successful, the mobile phone will receive the SMS message.

	-	11:18		78%
<				
	1	30 4808 5981 >		
hello				
			183	



# 22.3 SMS Notification

# Overview

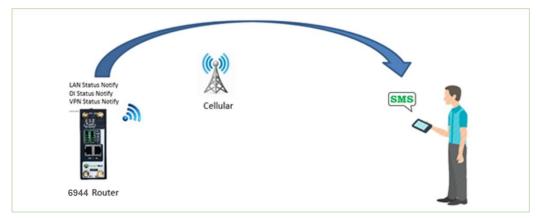
This document contains information regarding configuring the SMS Notification from the 6944 to a mobile device.

# **Software Version**

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

<b>Release Date</b>	Doc. Version	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>
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.

case 8							Reboot	Logout	
Overview	SMS								
Link Management	General	Settings							
Industrial Interface				Enable					
Network				Authentication Type	Password	•			
Applications		one Book							-
cons ► SMS	Index	Description	Phone Numbe	r					۲
Schedule Reboot									
Maintenance									

### Authentication Type:

**Password:** SMS command with router username and password **None:** SMS command without router username and password

### Allow Phone Book:

The router only receives the SMS message from phone numbers listed in the phone book



# **SMS Command**

### Authentication Type: Password

1. admin\$admin\$enable\$version // send SMS to check the firmware version

The first "admin" means the router username; the second "admin" means the router password; "enable" means to send the CLI Command of "enable mode". "Version" is the CLI command under enable mode

2. admin\$admin\$config\$set syslog level info //send SMS to set router syslog to info level

The first "admin" means the router username; the second "admin" means the router password; "config" means to send the CLI Command of "config mode". "Set syslog level info" is the CLI command under config mode

We also can send SMS with **multiple** CLI Commands, like below:

**1. admin\$admin\$enable\$version;show active_link** //send SMS to check firmware version and link information together.

**2.** admin\$admin\$config\$set syslog location ram;set syslog level info // send SMS to set syslog location and syslog level.

### **Authentication Type: None**

- 1. enable\$version
- 2. config\$set syslog level info
- 3. enable\$version;show active_link
- 4. config\$set syslog location ram;set syslog level info

### **CLI Command**

Step 1 Telnet to the router to check the CLI command under "enable mode" or "config mode".



When you have connected to the router using telnet the following prompt appears ">", this means that the router is in "enable mode"

When you enter the CLI command "config", then the router will go into "config mode"

Step 2 Enter the "?" or keyboard "Tab", then we can see CLI commands as shown below:



Section Twenty - Two

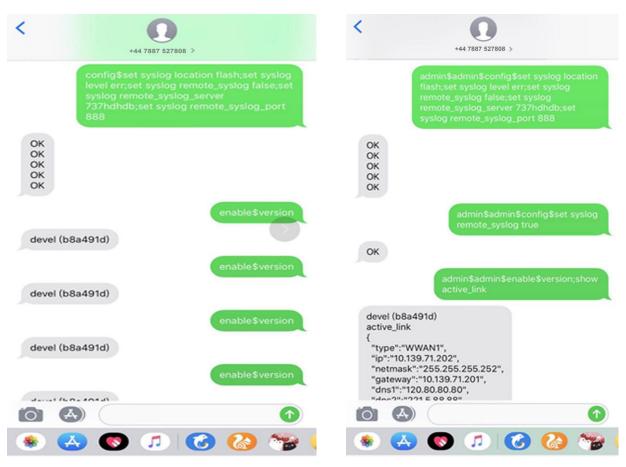
#### **SMS** Commands

**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	
version	Upgrade firmware Show firmware version
Verbron	

### **Testing**

**Step 1:** Below test result for reference.





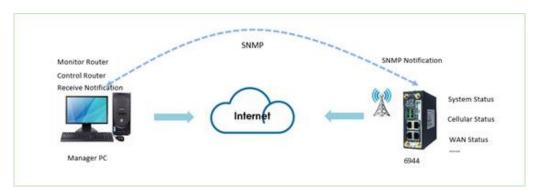
**Rev 2.8** 

This page left blank intentionally



#### 23. **SNMP** 23.1.

**Testing Topology** 



## Criteria of the SNMP test

- The 6944 Manager PC can access the 6944 router using SNMP Protocol.
- The Manager PC can obtain the 6944 operational status, and control the 6944 router and receive • SNMP notifications from 6944 router.

Note: For this Application Note, the Intranet was used to test the SNMP instead of the Cellular WAN. The 6944 Manager PC is connected to the LAN port of 6944. The IP address of Manager PC is set to: 192.168.5.19 / 24. The IP address of 6944 LAN port is: 192.168.5.1 / 24.

## **Software Compatibility**

<b>Release Date</b>	Doc. Version	<b>Firmware Version</b>	<b>Additional Software</b>	<b>Change Description</b>	
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:



Link Management Industrial Interface Nétvork k Applications Soriel State is record Prive State is record Prive State is record Prive Maintenance Name State is record State is reco	Overview	SNMP	VACM	Trap MI8				
Network     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1     1 <t< td=""><td>Link Management</td><td>View Setting</td><td>1</td><td></td><td></td><td></td><td></td><td></td></t<>	Link Management	View Setting	1					
Community Se     User Settings       Operations     Index       Consolutions     Index       State     Index       Consolutions     Index       State     Index       Consolutions     Index       Consolutions     Index       Consolutions     Index       State     Index       Consolutions     Index	Industrial Interface	Index	Nome T	rpe OID Tree				0
Specification     India     N     USH Users Settings       SPE     Schoole     Index     Index       Schoole     Index     Index     Index       PN     Authentication Passphrase     Index     Index       Adametrication     Index     Index     Index       Schoole     Index     Index     Index       Schoole     Index     Index     Index       PN     Authentication Passphrase     Index     Index       Address View	Vetwork	1		1.11 ( 1.1	_	_		R 🛛
State     State     Index I       Scholar Netox     Index I	oplications	Community S	User Setting	<b>9</b> .				
Schedule Reboxt United Team Un	DONS	Index	USM Users S	Settings		11.35		0
Oris     Index     Name     Index       Email Stationary     I     In     Operation Level     ReadWrite       Station     Interface     Authoritocolon     Id       VPN     Authoritocolon     Dess       Maintenance     Encryption Key     Id       Encryption Key     Id     Id		USM Users S		Index	12		-	
shole     Authentication Type     MD5     Authentication Pasighrave     Encryption Type     De5     Encryption Type     Encryption Key     R054321     Access View     al		1/des		Name	momo			
PN Authoritaning 12356778 tambonance Encryption Type Des • Encryption Key 87054323 Access View al •		1		Operation Level	ReadVinte			20
Saintonance Encryption Type DES   Encryption Key  Encryption Key Access View  #	► INMP			Authentication Type	MD5	•		
Encryption Key 87654321 Access View # •	VPN			Authentication Passphrase	12345678			
Access View at .	Maintenance			Encryption Type	DES	•		
				Encryption Key	87654321			
Save				Access View	al	•		
			1 13	Gentario de la composición de		Saus	Close	
		1.11						
							Sav	e Apply

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.

Overview	SNMP	VACM	Trap	MIB			
Link Management	General Setti	tings		a la secondad	and a second		
Industrial Interface				Enable	8		
Network				SNMP Version	SNMPv3	•	]
Applications			Ne	otification Host	192.168.5.19		]
DONS	4			Port Number	163		]
945				Username	momo	•	] 0
Schedule Reboot GPS	Events Settin	ngs					

**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.

Overview	SNMP	VACM	Trap	MIB				
ink Management	General Set	Event Settings						_
dustrial Interface		Events Settings				-		
letwork				Index	1			
oplications cons				Name	LAN Port			
96				Notify	2		-	
Schedule Reboot GPS	Events Set					Save	Close	
Email Notification	Indes	Norse	Notify					

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.

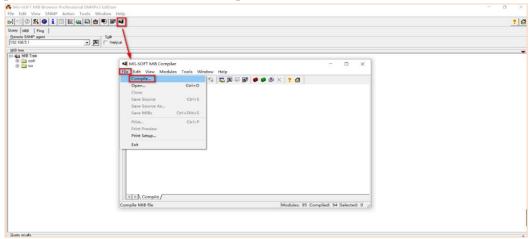
Once installed on your PC you should see the following screen

Command Line Utilities	2020/3/3 15:54
Document Files	2020/3/3 15:54
🔗 MIB Browser Help	2020/3/3 15:54
MIB Browser User Manual	2020/3/3 15:54
A MIB Browser	2020/3/3 15:54
🔊 MIB Builder Help	2020/3/3 15:54
煮 MIB Builder	2020/3/3 15:54
🔗 MIB Compiler Help	2020/3/3 15:54
🤾 MIB Compiler	2020/3/3 15:54
🔗 MIB Explorer Help	2020/3/3 15:54
🕺 MIB Explorer	2020/3/3 15:54
🖇 Quick Start Guide	2020/3/3 15:54
🗊 Uninstall MIB Browser	2020/3/3 15:55

*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**:

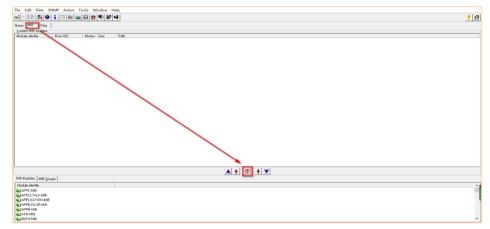
MG-SOFT MIB Compiler		– 🗆 X
File Edit View Modules Tools V	Nindow Help	
🖹 📽 🖬 🖬 🏼 🚳 🖿 🗛 🕯	🔐 🟗 🏗 🕅 🐼 🐼 🍁 🧇 🛠 ! ? 🛃	
B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B         B	Image: Second secon	
Ready	Modules	: 92 Compiled: 91 Selected: 0

**Step 3** : Save the Compiled File as default path, as shown below:

File	MG-SOFT MIB Compiler - MIB Group1		– 🗆 🗙
	File Edit View Modules Tools Window H	elp	
۲ <b>.</b>	1	😨 🕱 🐼 🥔 🕸 🗙 🥐 🍰	
	MIB Group1		
L F	Module / Root OID		
112	APPC-MIB 1.3.6.1.2.1.3.     Module     MIB-NW-Ro	Module:	
	APPLETA 1.3.6.1.2.1.1: MIB-NW-Ro APPLICAT 1.3.6.1.2.1.2		
S	APPDICAT 1.3.0.1.2.1.2	No information.	
C	APPN-MIB 1.3.6.1.2.1.3.		
7	ATM-MIB 1.3.6.1.2.1.3	Save As ×	
S	BGP4-MIB 1.3.6.1.2.1.1	Save in: SMIDB 🔹 🔶 🖆 📰 🕶	
Č	BRIDGE 1.3.6.1.2.1.1		
3	CHARAC 1.3.6.1.2.1.1!	Name Date modified	
J	DIAL-CO 1.3.6.1.2.1.1	APPC-MI8.smidb 6/14/2002 10:45 AM	
		APPLETALK-MIB.smidb 6/14/2002 10:45 AM	
0	DLSW-MIB 1.3.6.1.2.1.4		
11 C	DNS-SERV 1.3.6.1.2.1.3.	APPN-DLUR-MIB.smidb 6/14/2002 10:45 AM	
C	DOT12-IF 1.3.6.1.2.1.1.	APPN-MIB.smidb 6/14/2002 10:45 AM 🗸	
	DOT12-R 1.3.6.1.2.1.5	< >>	
S	S DSA-MIB 1.3.6.1.2.1.2" >	File name: MIB-NW-ROUTER-ROOT smdb Save	
ŝ	MIB Modules MIB C		
Ĕ		Save as type: WinMb Database Files (*.smidb) Cancel	
L.	Done.		^
F	Registering module(s) information		
	Registered DK. Done.		
F	Done.		
C	Finished.		
	Finished.		
			~
F	<		>
III.'	Compile		
	Ready		Modules: 0 Selected: 0 //
			-
1 N			



## **Step 5**: After saving the compiled file, refresh the MIB Module:



**Step 6**: Then check the MIB files and load them:

File Edit View SNMP Action Tools Window Help	
	? 🖨
Query HB   Ping	
Loaded HIB modules Module identity Root DID Nodes Size Path	
RE Moduler   MB Group	
Modale identity DI MULHUB	^
UNSOFT Store	
LINGGOT AND	
MIR NV Roder VALUES	
a MP 448	~
le Edit View SNMP Action Tools Window Help	
	? 6
uny MB Ping	
paded MB modules	
lodale identity Root OID Notes See Party	
IMB AVV Route R001         1.3.6.1.4.1.55251         12         3882.8         C.Vhogran Filer (JdE) MS SOFT WIE Browner/MB ISMOE WIE NW ROUTER R001.midb           IMB AVV Router TRAP         1.3.6.1.4.1.55251 500.0.6.0         22         5154.8         C.Vhogran Filer (JdE) MS SOFT WIE Browner/MB ISMOE WIE NW ROUTER TRAP. midb	
IMB AW Router TRAP         1.3.6.1.4.15551500.00.0         22         5134.0         C/Program File: (d6)/MG-SOFT WIB Browset/MB/SMDB/ME/MW/ROUTER TRAP.midb           IMB AW Router VALUES         1.3.6.1.4.15551500.00.0         25         5134.0         C/Program File: (d6)/MG-SOFT WIB Browset/MB/SMDB/ME/AW/ROUTER TRAP.midb           IMB AW Router VALUES         1.3.6.1.4.15551500.00.0         25         5134.0         C/Program File: (d6)/MG-SOFT WIB Browset/MB/SMDB/ME/AW/ROUTER TRAP.midb           IMB AW Router VALUES         1.3.6.1.4.15551500.00.0         25         5134.0         C/Program File: (d6)/MG-SOFT WIB Browset/MB/SMDB/ME/AW/ROUTER TRAP.midb           IMB AW Router VALUES         1.3.6.1.4.15551500.00.00         753         2141190         C/Program File: (d6)/MG-SOFT WIB Browset/MB/SMDB/ME/AW/ROUTER TRAP.midb	
THEOREM PROVINCE THE FORT OF THE PROPERTIES AND A THE PROVINCE AND A T	
<u>A</u> <u>+</u> <u>v</u>	

The MIB Files have been loaded



Step 7: Enter the IP address of 6944 router the management tool to the 6944

								$\boldsymbol{\omega}$		
File E	dit View	SNMP	Action	Tools	Windo	ow Help				
<b>6-1</b> ?{	0 🐒	0 i	III 🔛	🔬 🖾	1	8 🐼 🝕				
	MIB Pir									
192.16		nt	-			Split Vertical				
<u> </u>	e									
	MIB Tree								 	

Step 8: Enter the SNMPv3, parameters such Name and the Authentication and so on, as shown below:

File Edit View SNMP Action Tools Window Help			
e-i ?() (2) 🛼 🚳 i 💷 🔤 🤬 🖳 🏦 🐨 🗣			? 🚰
Query MIB Ping			
Bemote SNMP agent Split			
192.168.5.1 💌 🎦 🗆 Vertical			
MiB tree			-
E 🙀 MIB Tree B 🧰 📺 ito	SNMP Protocol Preferences		
200 C	SNMP protocol version		
	C SNMPv1 C SNMPv2c C SNMPv3		
	General Get-Bulk settings	SNMPv3 Security Parameters ×	
	Read community Vise Get-Bulk	User profile name	
	ken 0 No repeaters		
	Set community 10 Max repetitions	Security user name momo	
	SNMPv3 stranty		
	Timeout [s] 5 User profile name	Context engine ID #	
	momo	T SNMP contrumber 161	
	Retransmits 4 Security level	Authentication protocol HMAC-MD5  Change Password	
	Port number 161 - Whentication And Prive	Privacy protocol CBC-DES   Change Password	
		Do not localize Authenitication and Privacy keys	
	Add User Delete User	Diffie-Hellman key exchange	
	OK Cancel	Manager Random	
	·	OK. Cancel	
Query results (1: sysup rime u (menckis) u days uzn ubm; ras, barn (757368)			
c			0
1 s			>

## Step 9: Click "Yes To All":

File Edit View SNMP Action Tools Window Help		
nd 20 🐼 🐠 主 💷 😾 🤐 🤀 🐯 🚳 4		? 🔂
Query MIB Ping		
Bemote SNMP agent Split		
192.168.5.1		
MIB tree		-
En eggi MB Tree Friend cont En engli ino		
Query results		
Welcome to MG-SOFT MIB Browser Professional SNMPv3 Edition		^
Rende sedens: 152.186.5.1 port LF Langont (PAUP) Local addres: 152.186.5.1 port SS88 transport (PAUP) Protect vers: (SHPA) Use profer name mono Context name (mon-Berght) Context name (mon-Berght) Context name (mon-Berght) Security register). Exclosion Security register (Discover) Security register). Exclosion Security register (Discover) Security register). Security register Automation And Privacy Security register (Discover).	Search compiled MIB modules to resolve OID     X       OD 1.3.6.6.3.151.1.4 0 carvo be resolved though loaded MB modules.     Search (regit) to search and load MIB Part clame resolve the DD.       Search (regit) to search and load MIB Part clame resolve the DD.     Search (regit) to search and load MIB Part clame resolve the DD.       Search (regit) to search and load MIB Part clame resolve the MD.     Search (regit) to search and load MIB Part clame resolve the MD.       Search (regit) to search and load MIB Part clame resolve the MD.     Search (regit) to search and MD.       Search (regit) to search and load MIB Part clame resolve the MD.     Search (regit) to search and MD.       V Prompt before searching     Yes: To git _ Yes: MD.	
Synchronics: Security regime 10 robots Security regime 10 robots Cateform regime 10 robots Cateform regime 10 80 0.01 robots 07 13.04.07 555 251 0.158 (here) Security regime 10 80 0.01 F88 00 7C 13.04.07 555 251 0.158 (here) Authentication protocol: HAAC MOS Authentication protocol: HAAC MOS Prevery protocol: Cateform And Phinacy Security model: USM		Ŷ



Step 10: We should now see the menu on the 6944 router:

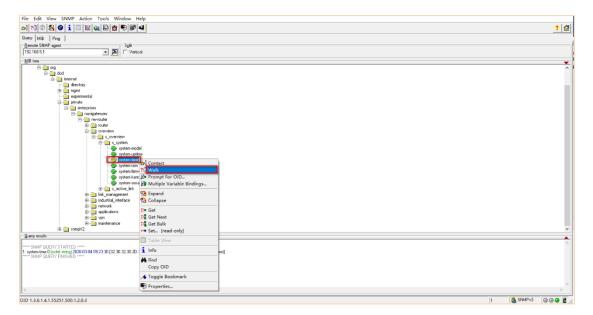
ile Edit View SNMP Action Tools Window Help	
	? 🛃
Welly Mills Pring	
Bende SNMP agent SIMP agent SIMP agent SIMP agent IS SIM □ Vertical	
MB bee	
MB Unes Graph MB Tree Graph MB Tre	
E org	
C internet	
E: I touter	
B- Can overview	
B ⊡ int _e paragement B ⊡ int _e paragement	
⊕applications	
B 😑 vpn	
B C maintenance	
13 <u>-</u> umpra	

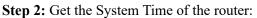
# 23.3. Testing SNMP

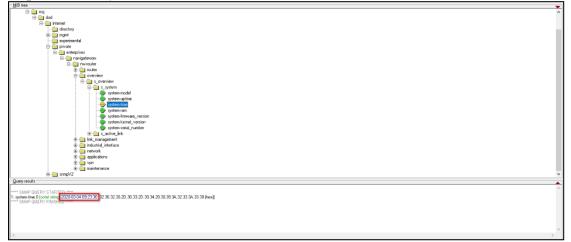
## Monitor the Running Status Of The Router

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":









# **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":

Query MIB Ping	
Bemote SNMP agent Split	
192.168.5.1 💌 🂌 🏳 Vertical	
MIB tree	_
Brude SUM part 22 CHS 11 Weice HB tree	
e 💼 iso	
🖻 🧰 org	
B dod Dri Contact	
r) waik	
gie Floringt for Old	
experimental	
e i private 😯 Expand	
enterprises	
navigatework	
Overview     Overview     Cat Bully	
Ink_management	
B applications	
🖲 🤤 vpn 🧯 Info	
i maintenance	
E gystem	
E _ c_sydog	
C teinet Properties	
teinet-pot	
E Cisth	
c_secuny	

## **Step 2**: Set the Telnet port to 24.

Query         Mail         Pring           Benned SNMP-Agend         Split           192:163.51         Split           Well toe         Veripcal	
Image: content of the second of the secon	
Start Fund	

Step 3: After setting, the Port it needs to be saved. Go to "Save Operation" and save it:

Query MIB Ping		
Bernote SNMP agent	SpR	
192.168.5.1 🔹 🔊	Vertical	
MIB tree		
E- 🔬 MIB Tree		X
E- Coit		
É- 🧰 iso		
ii-iii org ii-iii dod		
E- internet		
- directory		
E- ingmt		
- experimental		
⊟ mivate		
i i i i i i i i i i i i i i i i i i i		
E- C rw-router		
E- in router		
cperatio	Contact	
	2 Walk	
	Prompt For OID	
E- ink_manage	Multiple Variable Bindings	
⊞ industrial_ini	N	
network     end	C Expand	
e applications ⊕ vpn	Ta Collapse	
E- maintenance	🕫 💭 Get	
⊞- 📄 snmpV2	Cet Next	
	De Get Bulk	
	••• Set	
	III Table View	
Query results		
	1 Info	
THE SNMP QUERY STARTED THE	Find	
1: telnet-port.0 (octet string) 24 [32.34 (hex)]	Copy OID	
Amount SNMP SET-RESPONSE START And A Long A	🔸 Toggle Bookmark	
1: telnet-port.0 (octet string) 24 [32.34 [hex)]		
	Properties	1
		- v



Queey          Hit         Prog           Bender SNMP Synet         Splt           [10:168:51         Variped
Hencie SNMP sgint Sgint Sgint (12156) [ Varical
Later and the second se
MB bee
🗄 💫 MIB Tree
H cont
e indod
D private 000 to Sa
☐ artescies     [1.35.1.4.128c] 500.01.0     □
B network v value to Set
stutu update Syntax Select Value Foroperation.0 X
Br → molination ← Integer 32 ← Integer 52 ←
B ink_management C Constant22 C OID
B- industrial_interface
e network
🕀 🚞 applications 🖉 🖉 🖉 👔 SNMPy3
e 🚔 vpn
B minimum and mi
B 🔤 trimp/2

Step 4: Now select "Apply":

Query         MIB         Ping	
MB like MC lik	Set - operation 0 Request SNAP agent Set - operation 0 Request SNAP agent Set - operation 0 Set - opera

**Step 5:** Log in to the router and the Tenet Port had been changed to "24":

Overview	General	Accounts	Syslog	Web Server	Telnet	SSH	Security
Link Management	General Setti	ings					
Industrial Interface Network				Telnet Port	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

📭 ? 🕄 🖉 MIB Node Properties Ctrl+D		? 🚮
Query MIB Browser Preferences Ctrl+R		
Benote SN 19216851 V Toolbar		
MB tree		
MIB      Zoom Query Tab		<b>*</b>
e e iso		
⊡- <u></u> idod ⊡- <u>⊡</u> internet		
Grectory     Grectory     Grectory		
experimental		
enterprises		
E-Car Inversulter		
router     router     overview		
Briemennent Briemennent Briemennent		
retwork     retwork     retwork		
⊕ vpn ⊕ maintenance		
⊞- <u></u> snmpV2		
· · · · ·		
MIB tree		• i
- NIB Tree		•
E colt	MB Browser Preferences X	×
	General MIB Query Results Formatting Table View Trap Ringer	×
E ∰ MB Tree B ⊕ cott C ⊕ to C ⊕ to C ⊕ dod C ⊕ dod C ⊕ dod	General   MB   Query Results   Formating   Table View   Trap Ringer   Trap imper concide	×
E ⊕ 198 Tree F ⊕ ct E ⊕ to E ⊕ og C ⊕ og C ⊕ og F ⊕ dod C ⊕ og fermet G ⊕ fermet G ⊕ fermet G ⊕ fermet	General   HB   Query Results   Formatting   Table View Trap Finger   □ Trap ringer consule □ Disable indifications □ ♥ Very tage reception on statup ♥ Peryop on SMM Indification Trap □ ₱ Peryop on The week loss in tage □ ₱ Peryop on tage the period of	¥
E ⊕ Ha Free F ⊕ cct E ⊕ no E ⊕ no	General   MB   Query Results   Formatting   Table View Trap Finger   Trap inger controle □ Disable inclination □ Disable inclination □ Disable inclination □ Proper op 15MM inflication □ Flew revision thap □ SIMP rolification □ Map SIMP' I traps through enterprise	¥
B Constant of the set	General     MB     Query Results     Formating     Table View     Table Finger       To trade modification     To Verify the reception on startup       TP     Picepus on SMMP indication     The Remerciption to parameters       To Bible Product parameters     Map SMMP-11 traps through enterprise	¥
B ⊕ Ma Free B ⊕ a cot B ⊕ a co	General     MB     Query Results     Formating     Table View     Tab Finger       To brack motion     If you wanted to brack the second on an statup       IF Depug on SNMP notification     If Her verification tap       IF Depug on SNMP notification     If Her verification tap       IF Depug on SNMP notification     If Her verification tap       IF Depug on SNMP notification     If Mag SNMP/1 tags through enterprise       ONE of concept parameters     Use profile neame       Description     Description	¥
Image: Second	General     MB     Query Results     Formatting     Table View     Tab Pringer       To pay integr console     To bisable notifications     To bisable notifications     To bisable notification       TP     Popo on SMMP notification     To Har verification hap     The verification hap       TP     Exect on SMMP notification     To Map SMMP/1 traps through enterprise       SMMP/1 stoutly parameters     User prific selected     Edit User.	¥
Image: Section of the section of th	General     MB     Query Results     Formatting     Table View     Tab Pringer       To pay integr console     To Verify tap reception on statup       To Disable notifications     To Verify tap reception on statup       TP Report on SMMP notification     The verification tap       To Beep on SMMP notification     The verification tap       Statut Provide control     Map SMMP-1 taps through enterprise       Statut Provide control     Map SMMP-1 taps through enterprise       Security France     No socially       Security France     Beet Control       Security France     Beet Control       Deleter Lisen     Deleter Lisen	×
B: Guile MB Tree B: Guile MB Tree B: Guile A Tree B: G	General     MB     Query Results     Formating     Total Fringer       To trade reconcide     To trade reconcide     To trade reconcide       To trade reconcide     To Verify they reception on startup       TP trade reconcide     The Reconcidence     The Reconcidence       TP trade reconcidence     The Reconcidence     East Uses       TP trade reconcidence     The Reconcidence     East Uses       The Reconcidence     No reconcidence     East Uses       Security From ID     No reconcide     East Uses       Engine Boots:     7     To     To	
B: Guile MB Tree B: Guile MB Tree B: Guile MB Tree B: Guile Color B: Guile	General     MB     Query Results     Formating     Total Frager       To pice procession     Total Frager     Total Frager       To pice procession     Total Frager     Total Frager       Discled Procession     The Result Frager     Total Frager       Discled Procession     The Result Frager     East NMP of Color Frager       Discled Procession Procession     The Result Frager     East NMP of Color Frager       Security Frager ID     80000 55 20 10 C0AB F701 (Ped)     East Uter       Part     Trageopt     Status     East       Part     Trageopt     Status     East       Part     Trageopt     Uterson     East	¥
B G Hall Tree B G A HA	General     MB     Query Renatis     Total France       Totale root concide     FV     Velly top reception on statup       FD Diabel Problem Collidation     F New Year SMMP roblemation     F New Year SMMP roblemation       F Diabel Problematic Status     F May SMMP-11 tops through enterprise       F SNMP Architication     F May SMMP-11 tops through enterprise       F SNMP Architication     F May SMMP-11 tops through enterprise       Security Fred     No exactly Societ       Security Fred     No exactly Developed       Engine Boote:     7       Pagatiened roblemation parameter:     Target Tele Torget National       Fred     Target Status       Status     Edd.       TSQUE Orget JP     Edd.	Ţ
Contemporation     Contempo	General     MB     Query Results     Formatting     Table View     Tab Pinger       To bisable notifications     IF     Verify top reception on statup       IP     Popo on SNMP notification     IF     Her verification top       IP     Beep on SNMP notification     IF     Her verification top       IP     Beep on SNMP notification     IF     Mag SNMP/1 tops through enterprise       IP     Secure Fingle     No encortly     Mag SNMP/1 tops through enterprise       Secure Fingle     Do to scortly     Edd     Left       Secure Fingle Boots     7     Registeed rotification point     Bodd       Registeed rotification point     Tarseport Nature     Add       122     Default     PALIP     Unexcent Me Installed	Ţ
B G Hall Tree B G A HA	General     MB     Query Results     Formating     Totale View     Trap Finger       To trade motion     Totale View     Trap Finger       To trade motion     Trap Finger       Discled motion     Finger       Security Finger     No security       Security Finger     No security       Delete     Delete       Port     Trapport       Security Finger     Utation       Security Finger     Utation       Security Finger     No security       Delete     Delete	
Contemporation     Contempo	General     MB     Query Renatis     Total France       Totale root concide     FV     Velly top reception on statup       FD Diabel Problem Collidation     F New Year SMMP roblemation     F New Year SMMP roblemation       F Diabel Problematic Status     F May SMMP-11 tops through enterprise       F SNMP Architication     F May SMMP-11 tops through enterprise       F SNMP Architication     F May SMMP-11 tops through enterprise       Security Fred     No exactly Societ       Security Fred     No exactly Developed       Engine Boote:     7       Pagatiened roblemation parameter:     Target Tele Torget National       Fred     Target Status       Status     Edd.       TSQUE Orget JP     Edd.	
Degli MB Tree Degli MB Tree Degli Do Degli Do Degli Do Degli Do Degli Potental Degli Po	General     MB     Query Results     Formating     Total Program       To paid reconcide     Total Program     Total Program     Total Program       To paid reconcide     Total Program     Total Program     Total Program       To paid Program     Total Program     Total Program     Total Program       Total Program     Non and Program     Total Program     Edit Urec.       Security Program     No security     Delete Urec.       Program     No security     Delete Urec.       Program     Total Program     Edit Urec.       Security Program     No security     Delete Urec.       Program     Total Program     Edit       Program     No security     Delete Urec.       Program     Total Program     Edit       Program     Program     Urecone       152     Urecone     Edit       153     IPA/UPD     Resdor       153     IPA/UPD     Feedor       153     IPA/UPD     Feedor       153     IPA/UPD     Feedor	
Contemporation     Contempo	General     MB     Query Results     Formating     Total Program       To paid reconcide     Total Program     Total Program     Total Program       To paid reconcide     Total Program     Total Program     Total Program       To paid Program     Total Program     Total Program     Total Program       Total Program     Non and Program     Total Program     Edit Urec.       Security Program     No security     Delete Urec.       Program     No security     Delete Urec.       Program     Total Program     Edit Urec.       Security Program     No security     Delete Urec.       Program     Total Program     Edit       Program     No security     Delete Urec.       Program     Total Program     Edit       Program     Program     Urecone       152     Urecone     Edit       153     IPA/UPD     Resdor       153     IPA/UPD     Feedor       153     IPA/UPD     Feedor       153     IPA/UPD     Feedor	Ţ

#### Add User and click "OK":

Query         Mill         Ping           Bencies SNMP agent	•
definition     d	MB Browser Preferences     ×       General MB Guey Reads [ Femating ] Table Vew Txp Ringw     Finite concile       The index Concile     V Varity tap reception on statup       V Region 05 MMP rodication     Varity tap reception on statup       The end of SMMP rodication     Varity tap reception on statup       Security Parameters     ×       User großen and Numer profile sected     Ed User       Sacuty Fingel     Ed User       Sacuty Fingel     Baber       Profile Social point     Ed User       Fingeleet doctain point     Ed User       Fingeleet doctain point     Educet       Fingeleet doctain point     Educet

Open the SNMP Trap Ringer Console:



File Edit View SNMP Action Tools Window H	telp	
ri 🕄 🖉 🕵 🌒 i 🔟 😾 🔬 🔯 🐯 🗃	a ?	
Query MIB Ping		
Bemote SNMP agent Split		
192.168.5.1 Verig		
MIB tree		•
E- colt E- iso		
	📸 SNMP Trap Ringer Console – 🗆 🗙	
e io e org e dod	📸 🚀 🗋 Auto scroll 🔲 Insert on top 🗌 Pause	
internet		
😟 🧰 mgmt		
experimental		
enterprises		
i⊟ navigateworx i⊒ -tag nwrouter		
couter		
⊞- <u>n</u> overview ⊞- <u>n</u> link_management		
industrial_interface		
⊕ network ⊕ applications		
🕀 🚞 vpn		
maintenance		
iii- impV2		
	0 SNMP notifications received.	
	v simir nunicaturin tecenet.	

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

File Edit View SNMP Action Tools Window H	elp	
pi ?(] Ø 🐒 🜒 i 💷 🔛 🤬 🖶 🕱 🕬	4	? 🛃
Query MIB Ping		
Bemote SNMP agent Split		
192.168.5.1 💌 🎽 🗆 Vertja	al	
MIB tree		<b>•</b>
E-  MIB Tree		
🖻 🚞 iso	📸 SNMP Trap Ringer Console – 🗆 🗙	
i∃- i org ⊟- i od	👸 🍻 🗆 Auto scroll 🗆 Insert on top 🗆 Pause	
internet	E # 1: snmpModules.1.1.5.1 notification received from: 192.168.5.1 at 2020/3/4 11:03:17	
e increase in the increase increase in the increase inc	🗄 🛷 2. event-lan notification received from: 192.168.5.1 at 2020/3/4 11:03:19	
- in experimental	devention notification received from 192 168 51 at 2000/3/4 11:03:63     Devention notification received from 192 168 51 at 2000/3/4 11:03:63	
🖻 🧰 private	Agent address: 192.168.5.1 Port: 51296 Transport: IP/UDP Protocol: SNMPv3 Notification	
enterprises	- J Manager address: 192.168.247.1 Port: 163 Transport: IP/UDP	
E mwrouter	🗄 💐 Security parameters 🗄 🎒 Bindings (3)	
🗄 🧰 router	Bindings (3) Binding #1: sysUp Time.0 *** (timeticks) 0 days 00h:00m:39s.27th	
iæ- i overview iæ- i link_management	- 🙃 Binding #2: snmpModules:1.1.4.1.0 *** (oid) event-lan	
industrial_interface	👋 Binding #3: event-lan 0 **** (octets) [2020-03-04 11:03:53] lan1 down [58:32:30.32:30:20:30:33:20:30:34:20:31:31:34:30:33:34:35:33:5D:20.6C	
network		
applications		
⊕- 📴 vpn ⊕- 🧰 maintenance		
⊞- 🚞 snmpV2		
	< >	
	3 SNMP notifications received.	

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:

Overview	TR069	
Link Management	Local Settings	
Industrial Interface	Enable	
Network	Local Port	7547
Applications	Authentication	Digest
DDNS	Username	
SMS	Password	
Schedule Reboot TR069	Log Level	Info •
VPN	ACS Settings	
Maintenance	URL	http://192.168.111.19/acs
	Username	
	Password	
	Enable Periodic	✓
	Periodic Interval	1800
	Http 100 Continue Enable	
	Manufacturer Info	
	Manufacturer	Navigateworx
	Manufacturer OUI	FFFFE
		Save Apply

*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:

	- WELCOME -	Resource Configuration Upgrade Security System About 📾 Welcome:admin Role:Super Admin Log						Logout				
0	Resource		IP	SN	Manaufactor	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	
	AILCPE	Total	1 1								<< <	:1>>>
►	Category View	ggory View Delete 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:

= WELCOME =	Resource Configuration	Upgrade Security	System A	bout					S Welcome:admir	Role:Super Admin Logout		
C Resource O	IP IP	SN	Manaufactor	Model	First Contact	Last Contact	Soft Version	Hard Version	O	peration		
▼ Global View	192.168.111.199	19125124330003	Navigateworx	NR500-S4G	2012-07-20 14:02:19	2012-07-20 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel	Delete Test		
AILCPE	Total: 1									<< <1>>>		
<ul> <li>Category View</li> </ul>					Delete App	ly Template In Batch						
- WELCOME -	Resource Configuration	Upgrade Security	System	About					Welcome:admi	n Role:Super Admin Logout		
Resource	Navigateworx CPE SN:19	125124330003, URL:http	://192.168.111.199:7	547/								
Global View	ACS服务器IP: 192.168.		*									
All CPE	(当前ACS IP) GetRPCM	能ACS IP GetRPCMethods Reboxt FactoryReset										
Category view	一日志上传	日志上作										
	Upload Log											
	- 配置上传											
	Upload Config											
	- 配置恢复											
	Choose One ▼ 重载万	利表 恢复到当前配置										
	- 固件升级											
	固件文件 Choose File	No file chosen	升级									

## **Factory Reset**

Login to the platform and go to **Resource>Test>FactoryReset**, the router will reset when click the "Factory Reset" button:

= WELCOME =	Resource Configuration	Upgrade Security	System /	About					Welcome:admin Role:Super Admin Logout
O Resource O	IP IP	SN	Manaufactor	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 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel Delete Test
AILCPE	Total: 1								<< <1>>>
Category View					Delete App	ply Template In Batch			
- WELCOME -	Resource Configuration	Upgrade Security	System	About					Welcome:admin Role:Super Admin Logout
Resource	Navigateworx CPE SN:19	125124330003, URL:http	://192.168.111.199:7	547/					
▼ Global View	ACS服务器IP: 192.168.								
All CPE	当前ACS IP GetRPCM	1ethods Reboot Fac	ctoryReset 报文跟	踪					
Category View	一日志上传								
	Upload Log								
	Upioad Log								
	一配置上传								
	Upload Config								
	- 配置恢复								
	Choose One 🔻 重载万	表   恢复到当前配置							
	固件升级								
	固件文件 Choose File	No file chosen	升级						
		2							

## Syslog Upload

Login to the platform and go to **Resource>Test>Upload Log**, the router's syslog will display on the TR069 management platform:

	elcome =	Reso	ource Configuration	Upgrade Security	System At	out					🖨 Welcome:admin Role:Super A	dmin Logout
C R	Resource 🔘		IP	SN	Manaufactor	Model	First Contact	Last Contact	Soft Version	Hard Version	Operation	
▼ Glo	obal View		192.168.111.199	19125124330003	Navigateworx	NR500-S4G	2012-07-20 14:02:19	2012-07-20 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel Delete	Test
A	AII CPE	Total	: 1									<< <1>>>>
Cate;	egory View	Delete Apply Template In Batch										



* WELCOME *	Resource Configuration Upgrade Security System About B Welcometadmin Role:Super Admin Logg
	Navigateworx CPE SN:19125124330003, URL:http://192.168.111.199.7547/ ACS錄务習印: 192.168.111 19
Collegery vive	DBL#1         Ubbad Iop         Jul 21541:27 anglaterons user.debug comp(501]: ust.http://121.08.111.70/ucs         Jul 21541:27 anglaterons user.debug comp(502]: ust.http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: ust.http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: ust.http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: confaunct das unit http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: confaunct das unit http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: confaunct das unit http://122.08.11.07/ucs         Jul 21541:27 anglaterons user.debug comp(502]: betterails sept int         Jul 21541:27 anglaterons user.debug comp(502]: mits sept int         Jul 21541:27 anglaterons user.debug comp(502]:

## **Config Upload**

Login to the platform and go to **Resource>Test>Upload Config**, the router's config will display on the TR069 management platform:

	= WELCOME =	Resource Configuration	Upgrade Security	System	Vbout					Welcome:admin Role:Super	Admin Logout
0	Resource	IP IP	SN	Manaufactor	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 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel Delete	Test
	ALCPE	Total: 1									<< < 1 > >>
•	Category View					Delete App	ly Template In Batch				
L	- WELCOME -	Resource Configuration	Upgrade Securit	y System	About					G Welcome:admin Role:Su	er Admin Logo
0	Resource	- Navigateworx CPE SN:1	9125124330003, URL:ht	p://192.168.111.199	7547/						
•	Global View	ACS服务器IP: 192.168	8,111,19	*							
	AILCPE	当前ACS IP GetRPC	Methods Reboot	actoryReset 报文	見踪						
•	Category View	一日志上传									
		Upload Log									
		opioad Log									
		配置上传									
		Upload Config									
		( opioad coning )									
		ad":{ "default_policy":"accept"									
		<pre>deraulc_poilcy : accept }, "dmz":{</pre>									
		"enable":"false",									
		"remote":"0.0.0.0\/0", "host":""									
		}, "ip_passthrough":{									
		"enable":"false", "host_mac":"",									
		"https_access":"true", "telnet_access":"false",									
		"ssh_access":"false" },									

#### 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:

= WELCOME =	Resource Configuration	Upgrade Security	System A	bout					Welcome:admin Role:Super Admin Logout
C Resource O	I IP	SN	Manaufactor	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 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel Delete Test
<u>All CPE</u>	Total: 1								<<<1>>>>
Category View					Delete App	ly Template In Batch			
- WELCOME -	Resource Configuration	Upgrade Security	System	About					🖨 Welcome:admin Role:Super Admin Logo
C Resource O	- Navigateworx CPE SN:19	125124330003, URL:http	://192.168.111.199:7	/547/					
Global View <u>All CPE</u> Category View	ACS服务器IP: 192.168. 当前ACS IP GetRPCN		▼ ctoryReset	B.					
	日志上传								
	Upload Log								
	1 配置上传								
	Upload Config								
	- 配置恢复								
	2012-07-20 16:07:11 *	重裁列表(恢复到当前	前配置						
	{ "ad":{ "default_policy":"accept"								
	}, "dmz":{								
	"enable":"false", "remote":"0.0.0.0\/0",								



## 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:

= WELCOME =	Resource Configuration	Upgrade Security	System	About					Welcome:admin Role:Super Admin Logout			
C Resource O	IP IP	SN	Manaufactor	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 15:06:44	1.1.4 (0c0c9fa)	1.0.0	Detail DataModel Delete Test			
AILCPE	Total: 1								<< <1>>>>			
Category View					Delete App	ly Template In Batch						
= WELCOME =	1	and the second	1									
	Resource Configuration	Upgrade Security	System	About					Welcome:admin Role:Super Admin Logout			
C Resource O	Navigateworx CPE SN:19	125124330003, URL:http	://192.168.111.199:	7547/								
Global View     All CPE	ACS服务器IP: 192.168.		•									
Category View	当用ACS IP GetRPCM	当能ACS IP GetRPCMethods Reboot FactoryReset 报及服装										
	□ 日志上传											
	Upload Log											
	- 配置上传											
	Upload Config											
	配置恢复											
	Choose One ▼ 重载列	快复到当前配置										
	- 图件升级											
	图件文件 Choose File	No file chosen	升级									

#### **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:

= WELCOME =	Resource Configuration Upgrade Security	System About			🗟 Welcome:admin Role:Super Admin Logout
C Resource O	TR-098 T Expand Collapse	Name	CurrentLocalTime	Version	1.0
Global View	LANDeviceNumberOfEntries     MANDeviceNumberOfEntries	MinValue	-9223372036854775808	MaxValue	9223372036854775807
<u>All CPE</u>	⊕ 🛄 .Capabilities.	Length	2147483647	Writable	NO
Category View	DeviceInfo.	Description	The current date and time in the CPE抯 local time zone.		
	<ul> <li>DeviceConfig.</li> <li>DanagementServer.</li> </ul>	Path	InternetGatewayDevice.Time.CurrentLocalTime		
	🕀 😋 . Time. — 🗋 Enable	Туре	dateTime •	Operation	GetParameterValues v OK
	- Status	Value		Instance	
		Result	Name InternetGatewayDevice.Time.CurrentLocalTime	-	Value 2020-07-20T16:37:30
	INTPseve5     Current coalTime     Carent coalTime     LocalTimeZonethane     LocalTimeZonethane     Daylopticswingslast     Daylopticswingslast     Daylopticswingslast				

Check the time zone:

Resource	TR-098 T Expand Collapse	Name	LocaITImeZone	Version	1.0	
Global View	LANDeviceNumberOfEntries     WANDeviceNumberOfEntries	* MinValue	-9223372036854775808	MaxValue	9223372036854775807	
AILCPE	B- Capabilities.	Length	6	Writable	YES	
Category View	<ul> <li>DeviceInfo.</li> <li>DeviceConfig.</li> <li>DeviceConfig.</li> <li>DeviceConfig.</li> </ul>	Description			in the form: +hh:mm -hh:mm For example, this This parameter is OBSOLETED because the info	
	🖻 😋 .Time.	Path	InternetGatewayDevice Time LocalTimeZo	ine		
	- Status	Туре	string •	Operation	GetParameterValues • OK	
	- NTPServer2	Value		Instance		
	NTPServer3     NTPServer4	Result		Name		Value
	- NTPServer5	Result	InternetGatewayDevice.Time.LocalTimeZo			+8:00

Specify the NTP server1 address:

- WELCO	OME -	Resource Configuration Upgrade	Security	System About			Welcome:admin Role:Super Admin Logout
C Reco	ee (0)	TR-098 • Expand Collapse		Name	NTPServer1	Version	1.0
V Global			WANDeviceNumberOfEntries     Capabilities.	MinValue	-9223372036854775808	MaxValue	9223372036854775807
AILCI		Capabilities.			Length	64	Writable
Category	View	<ul> <li>DeviceInfo.</li> <li>DeviceConfig.</li> </ul>	Description	First NTP timeserver. Either a host name or IP address.			
		.managementServer.		Path	InternetGatewayDevice.Time.NTPServer1		
		Status		Туре	string	Operation	SetParameterValues • OK
			Value	pool.ntp.org	Instance		
			- 11	Result			



**TR069** 

Specify the time zone:

- WELCOME -	Resource Configuration Upgrade Security	System	About		🖬 Welcome:admin Role:Super Admin Logout
C Reserve C	TR-098 V Expand Collapse	Name	LocalTimeZone	Version	1.0
▼ Global View	.LANDeviceNumberOfEntries     .WANDeviceNumberOfEntries	MinValue	-9223372036854775808	MaxValue	9223372036854775807
AILCPE	B- Capabilities.	Length	6	Writable	YES
Category View	⊕DeviceInfo. ⊕DeviceConfig. ⊕ManagementServer.	Description			the form: +hh:mm -hh:mm For example, this will always be "-08:00" for his parameter is OBSOLETED because the information that it represents is fully
	⊖- 😋 .Time. ├── Enable	Path	InternetGatewayDevice.Time.LocalTimeZ	one	
	Status     NTPServer1	Туре	string	Operation	SetParameterValues   OK
	- 🗋 NTPServer2	Value	+8:00	Instance	
	NTPServer3     NTPServer4	Result	Response Result: 1 - The Object creation	has been validated and committed, but no	ot yet applied; Instance Number:
	- 🗋 NTPServer5				
	CurrentLocalTime				
	LocalTimeZoneName				

#### **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:

	= WELCOME =	Resource Configu	ration Upgrade Security Syst	em About	B Welcome:admin Role:Super Admin Logout
0	Configuration O	- Templates			
•	Templates				
	Template Manage		Name	Description	Operation
				Delete	
		Create new templ	ate		
		Name			
		Description			
				Apply	

Step 2 After that, add the template parameters for active link and cellular:

- WELCOME -	Resource Configuration L	Upgrade Security Sys	tem About			B Welcome:admin Role:Super Admin Logour
• Configuration •	- Templates					
▼ Templates						
Template Manage		Name	Description			Operation
	C ActiveLink		Active Link Status		Delete	dify
	Cellular		Cellular Info		Delete	dify
				Delete	_	

Step 3 Template Parameters for ActiveLink:

ate Manage	Name			
		ActiveLink		
	Description	Active Link Status		
		Apply		
	Template Parameter			
	•	Name	Туре	Value
	InternetGatewayDevice.ActiveLink.LinkType	string	WAN	
	InternetGatewayDevice.ActiveLink.IP		string	1
	InternetGatewayDevice.ActiveLink.Netmask		string	1
	InternetGatewayDevice.ActiveLink.Gateway		string	1
	InternetGatewayDevice.ActiveLink.PrimaryDNSSer	ver	string	1
	InternetGatewayDevice.ActiveLink.SecondaryDNS	Server	string	1
		Delete		
	Add Parameter			

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:



**Rev 2.8** 

	Appl	(		
Template Parameter				
•	Name		Туре	v
InternetGatewayDevice.Cellular.1.CSQ			int	1
InternetGatewayDevice.Cellular.1.IMEI			string	1
InternetGatewayDevice.Cellular.1.Registrati	n		string	1
InternetGatewayDevice.Cellular.1.Operator			string	1
InternetGatewayDevice.Cellular.1.NetwokTy	pe		int	1
InternetGatewayDevice.Cellular.1.PLMNID			int	1
InternetGatewayDevice.Cellular.1.LocalArea	Code		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.ModemFil	mwareVersion		string	1
	Delet	0		

Name	Туре	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:

= WELCOME =	Resource Configuration Upgrade Security	System About			Welcome:admin Role:Super Admin Logout	
O Resource O	TR-098  Expand Collapse	Name	.DeviceSummary	Version	1.1	
Global View	DeviceSummary	MinValue	-9223372036854775808	MaxValue	9223372036854775807	
ALCPE	- LANDeviceNumberOfEntries	Length	1024	Writable	NO	
<ul> <li>Category View</li> </ul>		Description	As defined in [3].			
	<ul> <li>Capabilities.</li> <li>DeviceInfo.</li> </ul>	Path	InternetGatewayDevice.ActiveLink.IP			
	<ul> <li>⊕- ☐ .DeviceConfig.</li> <li>⊕- ☐ .ManagementServer.</li> </ul>	Туре	string	Operation	GetParameterValues    OK	
	⊕ ¹ Time. ⊕ ¹ UserInterface.	Value		Instance		
	Image: Second	Result	Name InternetGatewayDevice.ActiveLink.IP		Value 192.168.111.199	
	⊕     QuarkHangement.       ⊕     J.McGnigSecurity.       ⊕     J.Projegostots.       ⊕     J.TaceRouteDiagnostics.       ⊕     QuarkBalagnostics.       ⊕     QuarkBalagnostics.       ⊕     Uplead Bagnostics.       ⊕     Uplead Bagnostics.       ⊕     QuarkBagnostics.       ⊕     Uplead Bagnostics.					



# 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 64MD DDR1 16-Bit CL3-3-3-8 RAM: 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	1521 reboots Restarting system
ncport=6666	
lsdk_kernel=1	
uboot_name=u-boot.bin	
uboot_addr=0x9F000000 uboot_size=0x1EC00	
uub-if ning Servering then tftph Sloadaddr	Suboot name A& if itset 1 Sfilesize an Suboo
Suboot size & echo DONE! U-Boot upgraded!	<pre>Suboot_name &amp;&amp; if itest.l \$filesize &lt;= \$uboo else echo ERROR! File is too big!; fi; else</pre>
fw_addr=0x9F040000	erse eens ennon: Pire is cos orgi, in erse
ufw=if ping Sserverip: then tftpb Sloadaddr	<pre>\$bootfile &amp;&amp; erase \$fw_addr +\$filesize &amp;&amp; cp</pre>
o ERROR! Sserverip is not reachable!; fi	
stdin-serial encode course while survey	
stdout=serial SS0/400/2007/25/25/0	
stderr=serial	
ethaddr=00:03:7F:09:08:AD of to stop boot mit to	
ethact=eth0 masses	
Environment cize: 005/4002 butes	
Environment size: 995/4092 bytes	

Step 3 Set a correct IP address on your PC:



**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 add	Iresses:						
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.

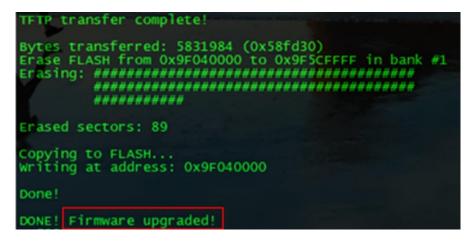
UBOOT UPGRADE		v ت
I Name I firmware.bin I I I I I I I I I I I I I I I I I I I	Iftpd32     py Ph. Jounin     —     X       Current Directory     C:\Users\Administrator\Desktop\UBC     Browse       Server interfaces     ::1     Software L     Show Dir       Tftp Server     Tftp Client     DHCP server     Syslog server     DNS server       peer     file     start time     progress       About     Settings     Help	Size 5,696 KB 230 KB



Step 5 Run the command "run ufw" to start the firmware upgrade.

Link do	t mode	h0 (duplex/speed): 1/1000 Mbps	
Ping Ok	, host	192.168.111.101 is alive!	
Fil	ename: Using:	192.168.111.101 192.168.111.200 firmware.bin eth1 0x80800000	
Lo	oading:		

Step 6 Check firmware upgraded successfully



# 25.2. Scheduled Reboot

Run the command "**reset**" to reboot the router.



**Rev 2.8** 

# **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