Case Communications

6402 Industrial Router

Manual

Revision 1.5

28.1.2022

Rev 1.5

Firmware Revision 08071200

This page left blank intentionally

Contents

Contents

Contents

Contents

Contents

Date	Revision	Firmware	Notes
28.1.2022	1.5	0CB0QO0.IA2_eA6.0CB0_08191000	Updated Field Bus Chapter 6 for new menus
			Updated Chapter 9 Services
			Added RADIUS and TACAS Server configuration

This page left blank intentionally

SECTION ONE

HARDWARE

Introduction

The Case Communications 6402 Router / Gateway is an Industrial ADSL Router, and Modbus Cellular Gateway for M2M (Machine-to-Machine) applications,

With a built-in 4G LTE and ADSL2+ module, you just need to insert a SIM card from a local mobile carrier to get access to the Internet. The redundant SIM and mobile/ADSL combo-WAN design provides a reliable WAN connection for critical applications. By using VPN tunnelling technology, remote sites easily become a part of your Intranet, and all data is transmitted over a secure (256-bit AES encryption) link.

To meet a variety of M2M application requirements the 6402 Industrial Router / Gateway includes VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for complex and demanding business and M2M (Machine-to-Machine) applications.

With its redundant design, dual 9-48 VDC power supplies, dual SIM cards and VRRP function makes the 6402 suitable for non-stop operation.

Main Features:

- Provide various and configurable WAN connection.
- Support dual SIMs for the redundant wireless WAN connection.
- Support ADSL2+ uplink connection ability.
- Provide Ethernet ports for comprehensive LAN connection and the LAN-1 port can be configured to be another WAN interface.
- VPN and NAT firewall to have powerful security.
- Supports local or remote management to monitor the network.
- Designed in a solid and easy-to-mount metal body for business and IoT environment to work with a variety M2M (Machine-to-Machine) applications.

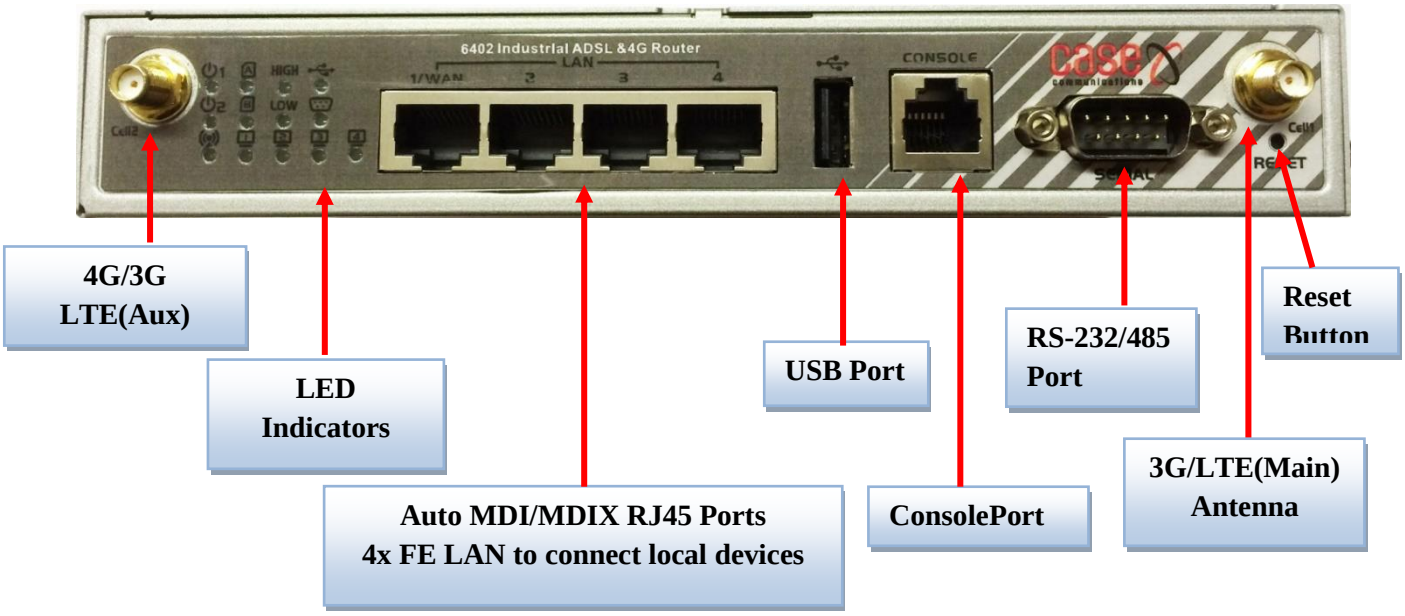
Before you install and use this product, please read this manual in detail to fully understand the features and functions of the 6402.

1.1. Packing List

Items	Description	Contents	Quantity
1	**6402 Industrial Router Modbus Cellular 6402**		1pcs
2	**Cellular Antenna**		2pcs
3	**Wi-Fi Antenna**		2pcs
4	**Power Adapter (DC 48V)** (*[1])		1pcs
5	**RJ45 Cable**		1pcs
6	**RJ11 Cable**		1pcs
7	**Console Cable**		1pcs
8	**CD (Manual)**		1pcs
9	**Mounting Bracket**		2pcs
10	**DIN-Rail Bracket**		1pcs

1.2. Hardware Configuration

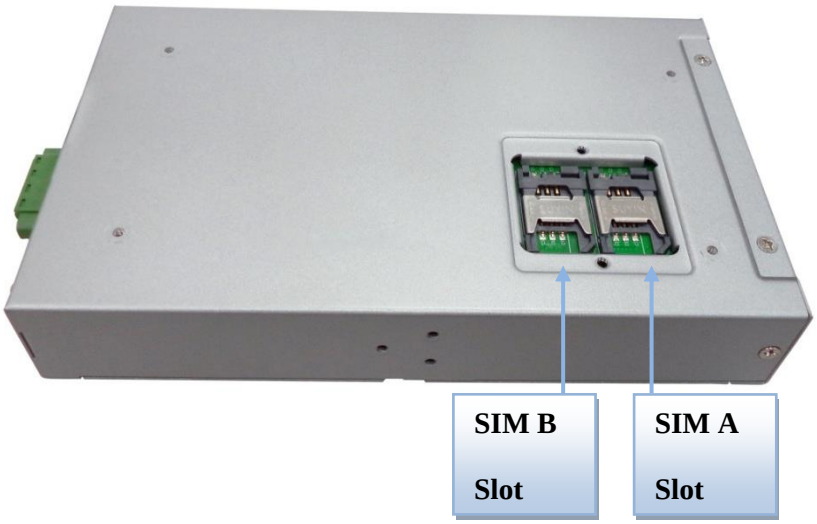
Front View



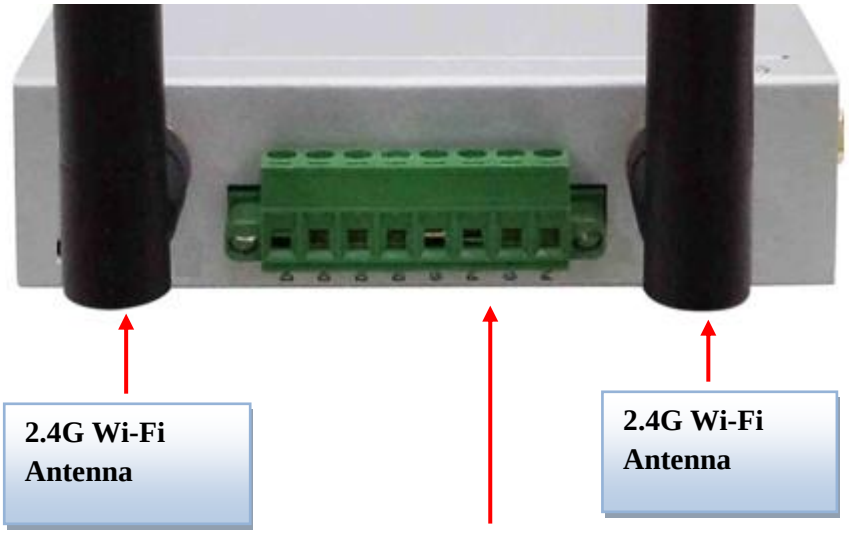
※Reset Button

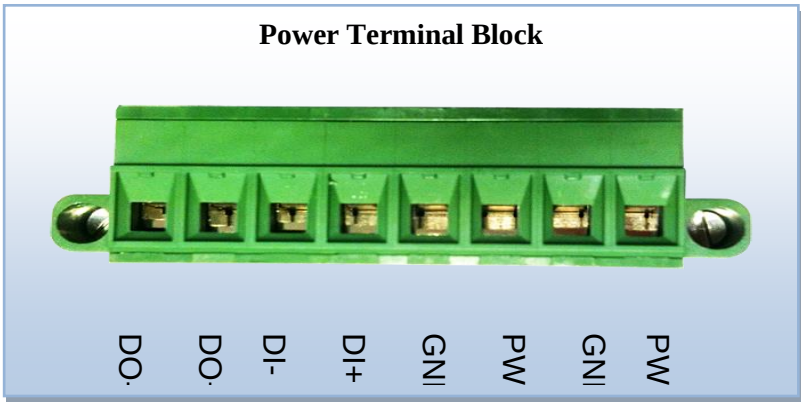
The RESET button provides users with a quick and easy way to restore the default setting. Press the RESET button continuously for 6 seconds, and then release it. The 6402 will restore to its factory default settings.

Bottom View

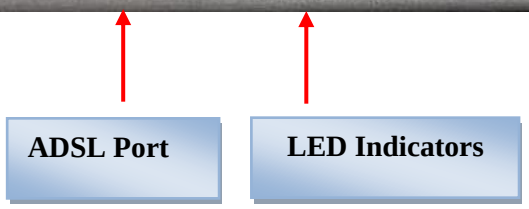


Left View



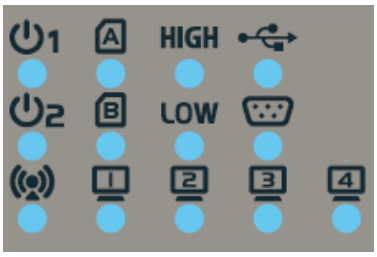


Right View

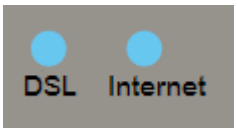


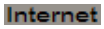
1.3. LED Indication

Front Panel



Right Panel



LED Icon	Indication	LED Colour	Description
	Power Source 1	Green	**Steady ON:**6402 is powered on by power source 1
	Power Source 2 (*[2])	Green	**Steady ON:**6402 is powered on by power source 2
	WLAN (Wi-Fi)	Green	**Steady ON:** Wireless radio is enabled **Flash:** Data packets are transferred **OFF:** Wireless radio is disabled
	SIM A	Green	**Steady ON:**SIM card A is used
	SIM B	Green	**Steady ON:**SIM card B is used
	LAN 1 ~ LAN 4	Green	**Steady ON:** The relevant Ethernet port has established a connection. **Flash:** Data packets are being transferred
	High 3G Signal	Green	**Steady ON:**3G has a strong signal strength
	Low 3G Signal	Green	**Steady ON:**3G has a weak signal strength
	USB	Green	**Steady ON:** If a USB device is attached
	Serial Port	Green	**Steady ON:** If a serial device is attached
	DSL	Green	**Steady ON:** Synchronization with the DSLAM is complete **Flash:** Attempting to synchronize with the DSLAM
	Internet	Green	**Steady ON:**A DSL Internet connection is established

2 If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. The LED of power source 2 will remain OFF in this condition.

1.4. Installation and maintenance

System Requirements

Network Requirements	• An Ethernet RJ45cable or DSL Line • 3G/4G cellular service subscription • IEEE 802.11n or 802.11b/g wireless clients • 10/100 Ethernet adapter on PC
Web-based Configuration Utility Requirements	**Computer with the following:** • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter **Browser Requirements:** • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

WARNING

Attention

- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product.
- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the product on a stable surface and avoid using this product and all accessories outdoors.

HOT SURFACE CAUTION

CAUTION:

The surface temperature for the metallic enclosure can be very high!

Especially after operating for a long time or installed in a closed cabinet without air conditioning support or ventilation, or in a high ambient temperature space.

DO NOT touch the hot surface with your fingers while servicing!!

1.5. Hardware Installation

This section describes how to install and configure the hardware

The6402 Industrial Router can be mounted on a wall, horizontal plane, or DIN Rail in a cabinet with the mounting accessories (brackets or DIN-rail kit). The mounting accessories are not attached to the 6402 when despatched from Case. Please screw the required wall-mount kits or DIN-rail bracket on to the 6402before use.

1.5.1 Insert the SIM Card

WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT THE 6402 IS NOT POWERED UP.

The SIM card slots are located at the bottom of 6402 Router housing. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After a SIM card has been fitted, replace the SIM card cover.

Step 1:

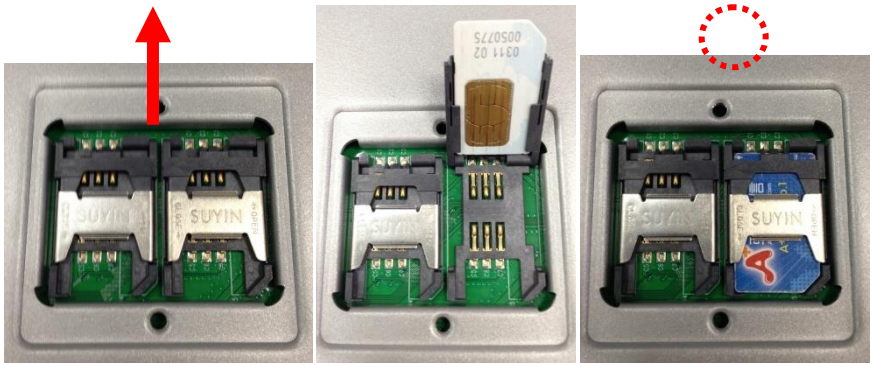
Follow red arrow to unlock SIM socket

Step 2:

Lift up SIM holder, and insert SIM card

Step 3:

Put back SIM holder, and follow red arrow to lock SIM socket

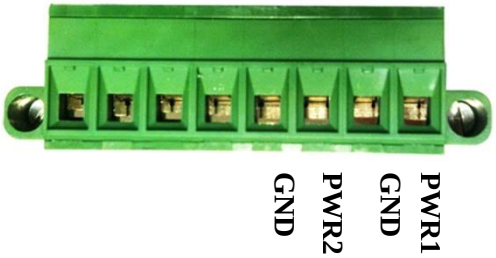


1.5.2 Connecting Power

The6402 Industrial Router can be powered by connecting a DC power source to the terminal block.

The 6402 Router supports dual 9 to 48VDC power inputs.

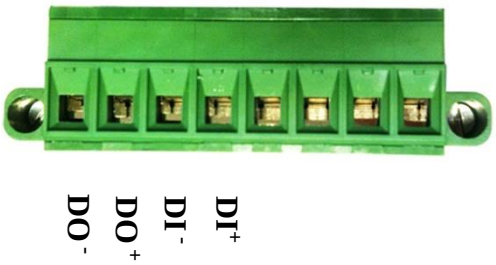
The following picture are the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



There is a DC converter and a DC48V power adapter in the package. Connect DC power to this terminal block.

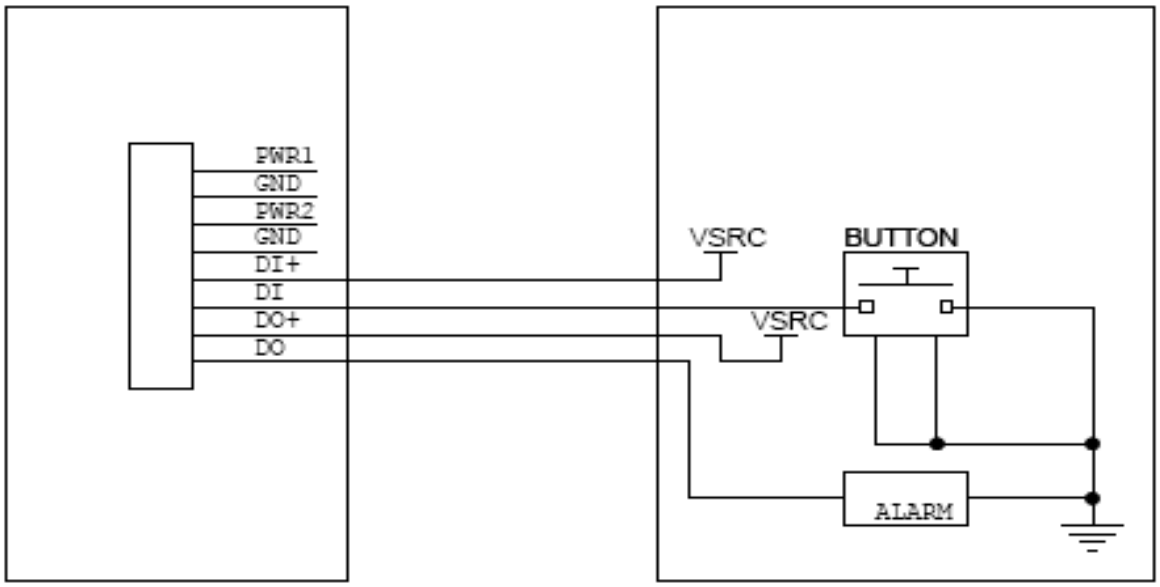
1.5.3 Connecting DI/DO Devices

The Green block contains the Digital Input (DI) and Digital Output (DO) ports together with power terminal block. Please refer to following specification to connect DI and DO devices.



Mode	Specification	
Digital Input	Trigger Voltage (high)	Logic level 1: 5V~30V
	Normal Voltage (low)	Logic level 0: 0V~2.0V
Digital Output	Voltage (Relay Mode)	Depends on external device maximum voltage is 30V
	Maximum Current	1A

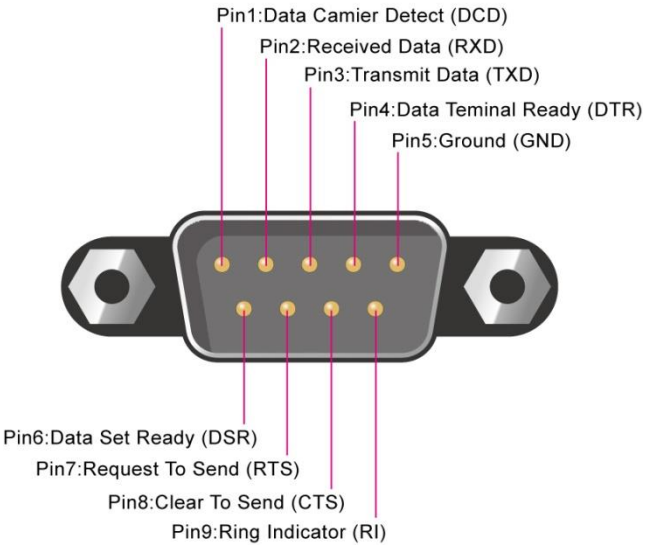
Example of Connection Diagram



1.5.4 Connecting Serial Devices

The 6402 Industrial Router provides one standard serial port DB-9 male connector. Connect the serial device to the unit DB-9 male port with the right pin assignments of RS-232/485 are shown as below.

RS232 Pinout



	Pin1	Pin2	Pin3	Pin4	Pin5	Pin6	Pin7	Pin8	Pin9
RS-232	DCD	RXD	TXD	DTR	GND	DSR	RTS	CTS	RI
RS-485			DATA+	DATA-	GND				

CHAPTER 2

GETTING STARTED

2.1 Connecting to the network or a host

The 6402 Industrial Router series provides 4x10/100Mbps RJ45 ports. It can auto detect the transmission speed and configure itself automatically.
Connect the Ethernet cable to the RJ45 ports of the 6402. Plug one end of an Ethernet cable into your computer's network port and the other end into one of 6402 Industrial Router LAN ports on the front panel. If you need to configure or troubleshoot the device, you may need to connect the 6402 directly to the host PC. In this way, you can also use the RJ45 Ethernet cable to connect the 6402 to the host PC's Ethernet port.

2.1.1. Setup by Configuring WEB GUI

You can browse the web GUI to configure the device, the default IP Address is

http://192.168.123.254

Figure 2.1 – Logon IP Address in Browser

You should then be presented with the following Logon Screen

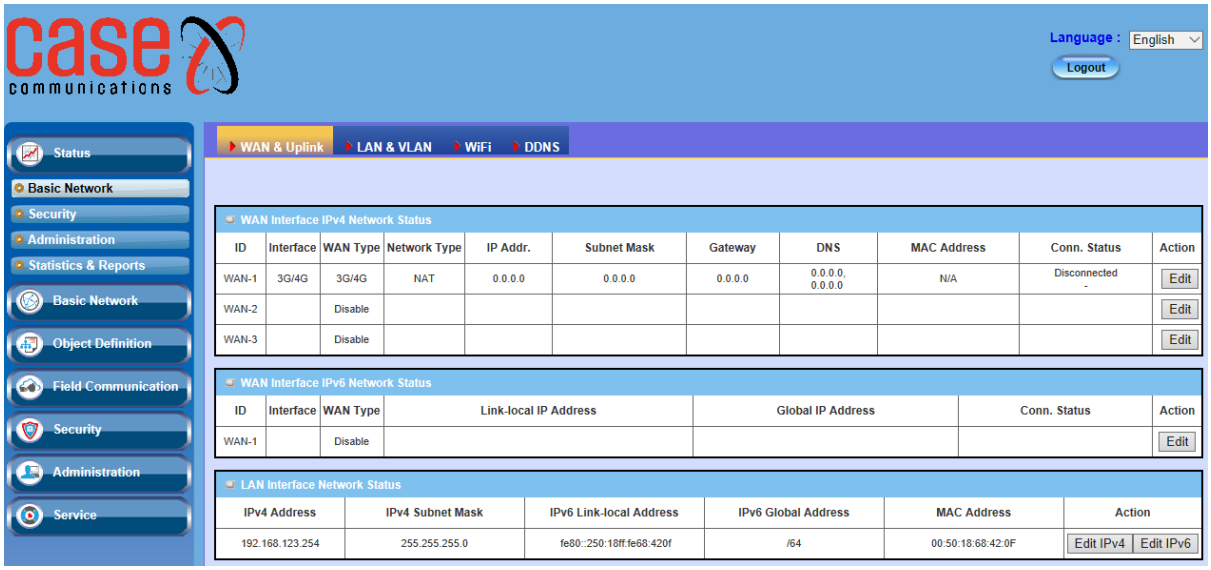
Figure 2.2 – Logon Screen

When you see the login page, enter the following username and password
Username **'admin'**

Password **'admin'**

Then click the **'Login'** button.
After logging on you will be presented with the following page and menu options

Figure 2.3 Initial Screen after Logging on



This manual is laid out in the same manner as the option shown, which are:

STATUS – Check the status of the following

Basic Network
Security
Administration
Statistics and Reports

BASIC NETWORK – Configure the following network parameters

WAN & Uplink
LAN & VLAN
Wi-Fi
IPv6
Port Forwarding
Routing
DNS & DDNS
QoS
Redundancy

OBJECT DEFINITION

Scheduling
Grouping
External Server
Certificate

FIELD COMMUNICATION

BUS Protocol
Data Logging

SECURITY

VPN
Firewall

ADMINISTRATION

Configure and Manage
System Operation
FTP
Diagnostic

SERVICE

Cellular Toolkit
Event Handling

This page left blank intentionally

SECTION 3

NETWORK STATUS

3.1 Network Status

3.1.1 WAN &Uplink

Go to Status> Basic Network > WAN & Uplink

3.1.1.1 IPv4 Network Status

The first section in the Status section is for the basic network settings, with the WAN Interface being the first table. This displays the WAN Interface Network Status as shown below:

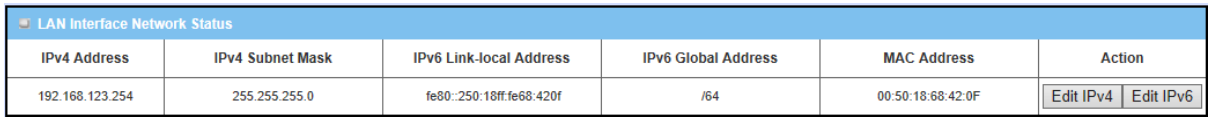
WAN interface IPv4 Network Status		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
WAN Type	N/A	Displays the method which public IP address is obtained from your ISP. Depending on the model purchased, it can be Static IP, Dynamic IP, PPPoE, PPTP, L2TP, 3G/4G.
Network Type	N/A	Displays whether the WAN uses NAT or is Routed.
IP Addr.	N/A	Displays the public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
Subnet Mask	N/A	Displays the Subnet Mask for public IP address obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
Gateway	N/A	Displays the WAN's default gateway, assigned by the ISP
DNS	N/A	Displays the IP address of DNS server obtained from your ISP for Internet connection. Default value is 0.0.0.0 if left un-configured.
MAC Address	N/A	Displays the MAC Address for your ISP to allow you for Internet access. Note: Not all ISP may require this field.
Conn. Status	N/A	Displays the connection status of the device to your ISP. Status are Connected or disconnected.
Action	N/A	This area provides functional buttons. **Renew** button allows user to force the device to request an IP address from the DHCP server. Note: **Renew** button is available when DHCP WAN Type is used and WAN connection is disconnected. **Release** button allows user to force the device to clear its IP address setting to disconnect from DHCP server. Note: **Release** button is available when DHCP WAN Type is used and WAN connection is connected. **Connect** button allows user to manually connect the device to the Internet. Note: Connect button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN& Uplink> Internet Setup**) and WAN connection status is disconnected. **Disconnect** button allows user to manually disconnect the device from the Internet. Note: **Connect** button is available when Connection Control in WAN Type setting is set to Connect Manually (Refer to **Edit** button in **Basic Network > WAN& Uplink> Internet Setup**) and WAN connection status is connected.

3.1.1.2 WAN interface IPv6 Network Status

The WAN interface IPv6 Network Status screen shows status information for IPv6 network.

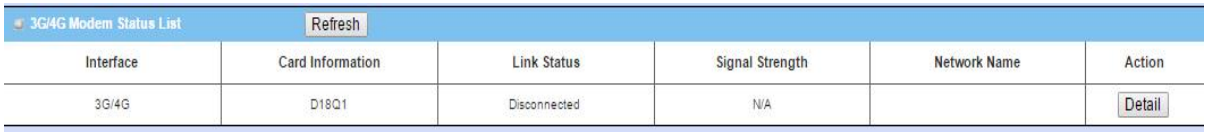
WAN interface IPv6 Network Status		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
WAN Type	N/A	Displays the method which public IP address is obtained from your ISP. WAN type setting can be changed from **Basic Network > IPv6 > Configuration**.
Link-local IP Address	N/A	Displays the LAN IPv6 Link-Local address.
Global IP Address	N/A	Displays the IPv6 global IP address assigned by your ISP for your Internet connection.
Conn. Status	N/A	Displays the connection status. The status can be connected, disconnected and connecting.
Action	N/A	This area provides functional buttons. **Edit Button** when pressed, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

3.1.1.3 LAN interface Network Status



LAN Interface Network Status		
Item	**Value setting**	**Description**
IPv4 Address	N/A	Displays the current IPv4 IP Address of the 6402 This is also the IP Address user use to access Router's Web-based Utility.
IPv4 Subnet Mask	N/A	Displays the current mask of the subnet.
IPv6 Link-local Address	N/A	Displays the current LAN IPv6 Link-Local address. This is also the IPv6 IP Address user use to access Router's Web-based Utility.
IPv6 Global Address	N/A	Displays the current IPv6 global IP address assigned by your ISP for your Internet connection.
MAC Address	N/A	Displays the MAC Address of the LAN. Assigned at manufacture of the router.
Action	N/A	This area provides functional buttons. **Edit IPv4 Button** when press, web-based utility will take you to the Ethernet LAN configuration page. (**Basic Network > LAN & VLAN > Ethernet LAN** tab). **Edit IPv6 Button** when press, web-based utility will take you to the IPv6 configuration page. (**Basic Network > IPv6 > Configuration**.)

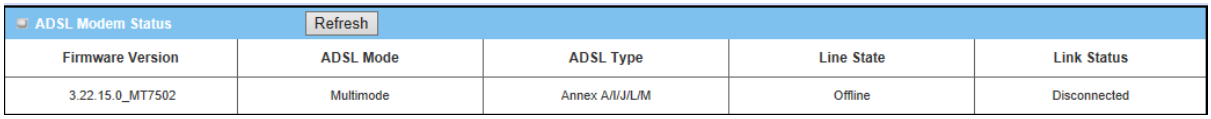
3.1.1.4 3G/4G Modem Status



3G/4G Modem Status List		
Item	**Value**	**Description**
Interface	N/A	Displays the type of WAN physical interface. Depending on the model you purchased, it can be 3G/4G and USB 3G/4G. Note: Some device model may support two 3G/4G modules. Their physical interface name will be **3G/4G-1** and **3G/4G-2**.
Card Information	N/A	Displays the vendor's 3G/4G modem model name.
Link Status	N/A	Displays the 3G/4G connection status. The status can be Connecting, Connected, Disconnecting, and Disconnected.
Signal Strength	N/A	Displays the 3G/4G wireless signal level.
Network Name	N/A	Displays the name of the service network carrier.
Refresh	N/A	Click the **Refresh** button to renew the information.
Action	N/A	This area provides functional buttons. **Detail** button when press, windows of detail information will appear. They are the Modem Information, SIM Status, and Service Information. Refer to next page for more.

3.1.1.5 ADSL Modem Status

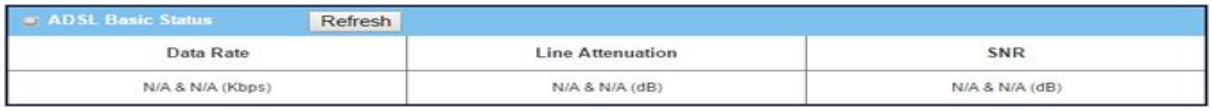
ADSL Modem Status screen shows status information for embedded ADSL modem.



ADSL Modem Status		
Item	**Value**	**Description**
Firmware Version	N/A	Displays the firmware version of the embedded ADSL modem.
ADSL Mode	N/A	Displays the operation mode of the embedded ADSL modem.
ADSL Type	N/A	Displays the supported protocol type of the embedded ADSL modem.
Line State	N/A	Displays the connection status of the ADSL line.
Link Status	N/A	Displays the link status of the ADSL WAN.

3.1.1.6 ADSL Basic Status

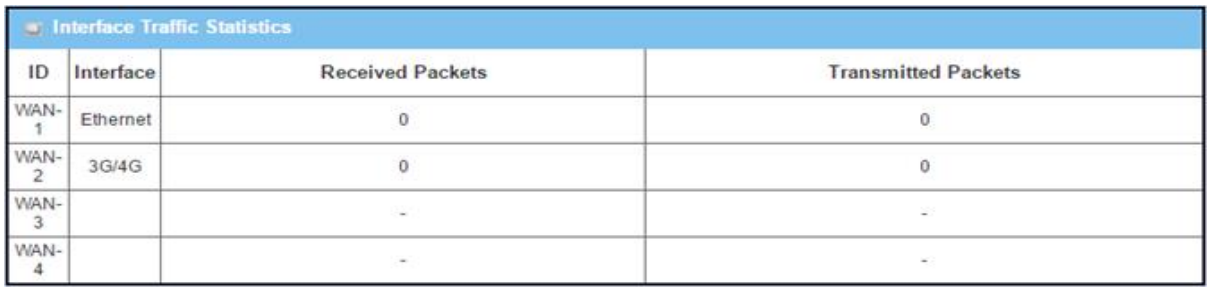
ADSL Basic Status screen shows some information for the embedded ADSL modem.



ADSL Basic Status		
Item	**Value setting**	**Description**
Data Rate	N/A	It displays the downstream / upstream data rate of the ADSL connection.
Line Attenuation	N/A	It displays the signal attenuation of the ADSL line.
SNR	N/A	It displays the signal SNR of the ADSL line.
Link Status	N/A	It displays the link status of the ADSL WAN.

3.1.1.7 Interface Traffic Statistics

The Interface Traffic Statistics screen displays the Interface's total transmitted packets.



Interface Traffic Statistics

ID	Interface	Received Packets	Transmitted Packets
WAN-1	Ethernet	0	0
WAN-2	3G/4G	0	0
WAN-3		-	-
WAN-4		-	-

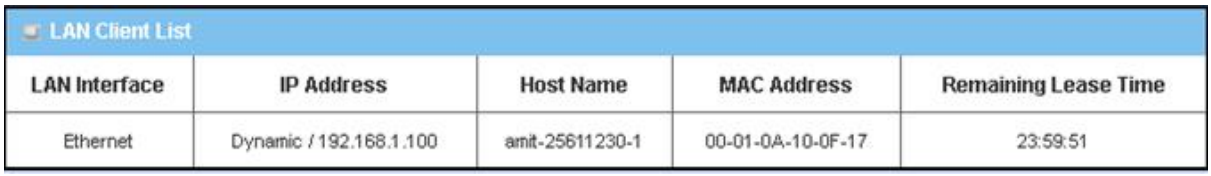
Interface Traffic Statistics		
Item	**Value setting**	**Description**
ID	N/A	Displays corresponding WAN interface WAN IDs.
Interface	N/A	Displays the type of WAN physical interface. Depending on the model purchased, it can be Ethernet, 3G/4G, USB 3G/4G.
Received Packets	N/A	Displays the downstream packets. It is reset when the device is rebooted.
Transmitted Packets	N/A	Displays the upstream packets. It is reset when the device is rebooted.

3.1.2 LAN & VLAN

Go to Status> Basic Network > LAN & VLAN

3.1.2.1 LAN Client List

The Client List shows you the LAN Interface, IP address, Host Name, MAC Address, and Remaining Lease Time of each device that is connected to this 6402.



LAN Client List

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.1.100	amit-25611230-1	00-01-0A-10-0F-17	23:59:51

LAN Client List		
Item	Value	Description
LAN Interface	N/A	Client record of LAN Interface. String Format.
IP Address	N/A	Client record of IP Address Type and the IP Address. Type is String Format and the IP Address is IPv4 Format.
Host Name	N/A	Client record of Host Name. String Format.
MAC Address	N/A	Client record of MAC Address. MAC Address Format.
Remaining Lease Time	N/A	Client record of Remaining Lease Time. Time Format.

3.1.3 Wi-Fi Status

The Wi-Fi Status window shows the overall statistics of Wi-Fi VAP entries.

Go to **Status> Basic Network > Wi-Fi** tab.

3.1.3.1 Wi-Fi Module One Virtual AP List

The Wi-Fi Virtual AP List shows all of the virtual AP information. The Edit button allows for quick configuration changes.

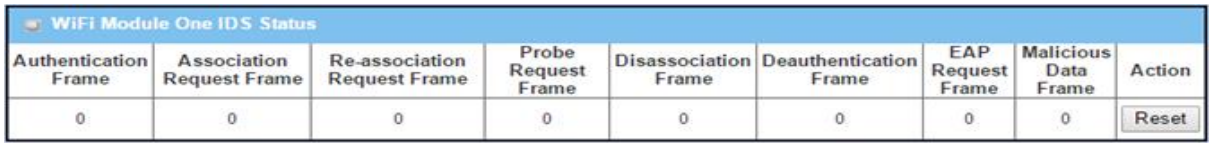
WiFi Module One Virtual AP List

Op. Band	ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.&Security	MAC Address	Action
2.4G	VAP-1	☑	WDS Hybrid	Staff_2.4G	Auto	b/g/n Mixed	Auto(None)	00:50:18:14:15:18	Edit QR Code
2.4G	VAP-2	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:10:15:18	Edit QR Code
2.4G	VAP-3	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:11:15:18	Edit QR Code
2.4G	VAP-4	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:12:15:18	Edit QR Code
2.4G	VAP-5	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:13:15:18	Edit QR Code
2.4G	VAP-6	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:14:15:18	Edit QR Code
2.4G	VAP-7	☐	WDS Hybrid	default	Auto	b/g/n Mixed	Auto(None)	02:50:18:15:15:18	Edit QR Code
2.4G	VAP-8	☑	WDS Hybrid	Guest_2.4G	Auto	b/g/n Mixed	Auto(None)	02:50:18:16:15:18	Edit QR Code

Wi-Fi Virtual AP List		
Item	**Value**	**Description**
Op. Band	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the ID of VAP.
Wi-Fi Enable	N/A	Displays whether the VAP wireless signal is enabled or disabled.
Op. Mode	N/A	The Wi-Fi Operation Mode of VAP. Depends of device model, modes are AP Router, WDS Only and WDS Hybrid, Universal Repeater and Client.
SSID	N/A	Displays the network ID of VAP.
Channel	N/A	Displays the wireless channel used.
Wi-Fi System	N/A	The Wi-Fi System of VAP.
Auth. & Security	N/A	Displays the authentication and encryption type used.
MAC Address	N/A	Displays MAC Address of VAP.
Action	N/A	Click the **Edit** button to make a quick access to the Wi-Fi configuration page. (**Basic Network > Wi-Fi > Configuration** tab) The **QR Code** button allow you to generate QR code for quick connect to the VAP by scanning the QR code.

3.1.3.2 Wi-Fi Module One IDS Status

The Wi-Fi Traffic Statistic shows all the received and transmitted packets on Wi-Fi network.



WiFi Module One IDS Status

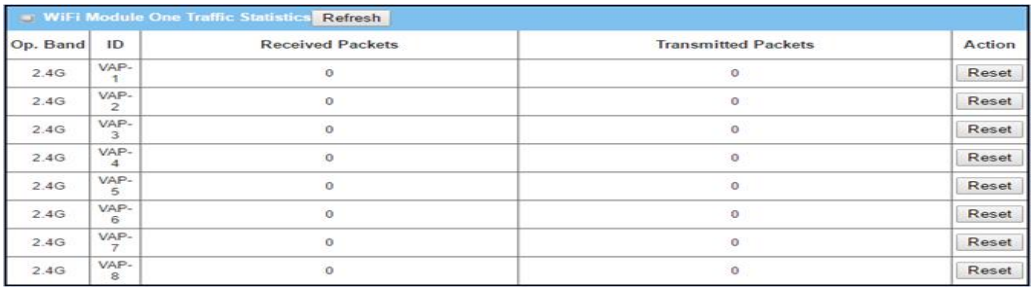
Authentication Frame	Association Request Frame	Re-association Request Frame	Probe Request Frame	Disassociation Frame	Deauthentication Frame	EAP Request Frame	Malicious Data Frame	Action
0	0	0	0	0	0	0	0	Reset

Wi -Fi IDS Status		
Item	**Value**	**Description**
Authentication Frame	N/A	Displays the receiving Authentication Frame count.
Association Request Frame	N/A	Displays the receiving Association Request Frame count.
Re-association Request Frame	N/A	Displays the receiving Re-association Request Frame count.
Probe Request Frame	N/A	Displays the receiving Probe Request Frame count.
Disassociation Frame	N/A	Displays the receiving Disassociation Frame count.
De authentication Frame	N/A	Displays the receiving De authentication Frame count.
EAP Request Frame	N/A	Displays the receiving EAP Request Frame count.
Malicious Data Frame	N/A	Displays the number of receiving unauthorized wireless packets.
Action	N/A	Click the **Reset** button to clear the entire statistic and reset counter to 0.

- **Ensure WIDS function is enabled**
- **Go to Basic Network > Wi-Fi > Advanced Configuration tab**
- **Note that the WIDS of 2.4G or 5G should be configured separately**

3.1.3.3 Wi-Fi Module One Traffic Statistics

The Wi-Fi Traffic Statistic shows all the received and transmitted packets on Wi-Fi network.



Wi-Fi Traffic Statistic		
Item	**Value**	**Description**
Op. Band	N/A	Displays the Wi-Fi Operation Band (2.4G or 5G) of VAP.
ID	N/A	Displays the VAP ID.
Received Packets	N/A	Displays the number of received packets.
Transmitted Packet	N/A	Displays the number of transmitted packets.
Action	N/A	Click the **Reset** button to clear individual VAP statistics.
Refresh Button	N/A	Click the **Refresh** button to update the entire VAP Traffic Statistic.

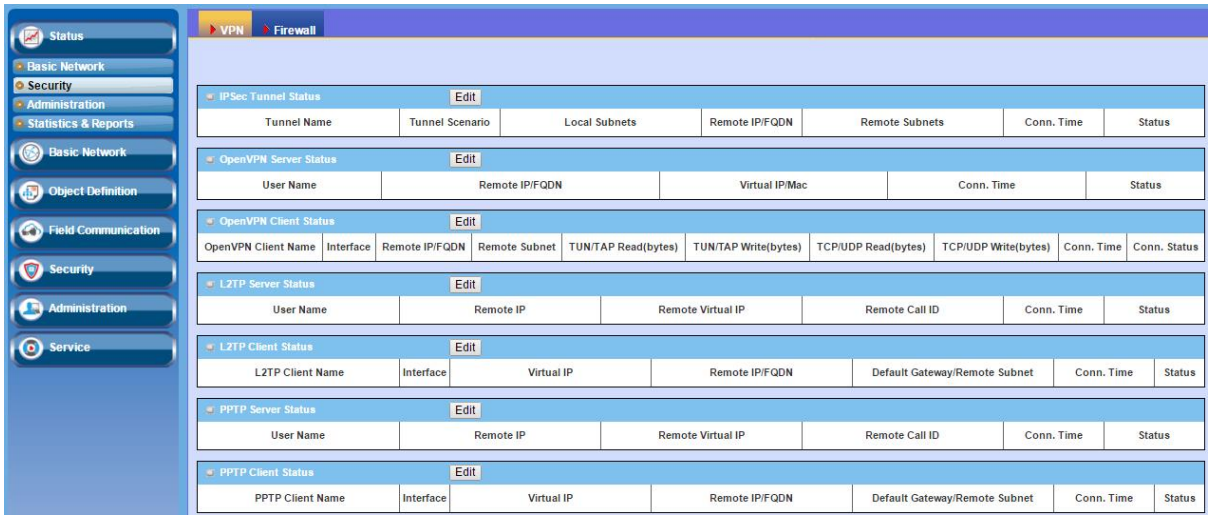
3.1.4 DDNS Status

The DDNS Status window shows the current DDNS service in use, the last update status, and the last update time to the DDNS service server.

Go to **Status> Basic Network > DDNS.**

DDNS Status		
Item	**Value Setting**	**Description**
Host Name	N/A	Displays the name you entered to identify DDNS service provider
Provider	N/A	Displays the DDNS server of DDNS service provider
Effective IP	N/A	Displays the public IP address of the device updated to the DDNS server
Last Update Status	N/A	Displays whether the last update of the device public IP address to the DDNS server has been successful (Ok) or failed (Fail).
Last Update Time	N/A	Displays time stamp of the last update of public IP address to the DDNS server.
Refresh button	N/A	The **refresh** button allows user to force the display to refresh information.

3.2 Security



3.2.1. VPN Status

The VPN Status window shows the overall VPN tunnel status.

From the menu on the left, select Status >Security >VPN Status.

3.2.1.1 IPSec Tunnel Status

IPSec Tunnel Status windows show the configuration for establishing IPSec VPN connection and current connection status.

IPSec Tunnel Status		
Item	**Value**	**Description**
Tunnel Name	N/A	Displays the Tunnel name that was entered during configuration
Tunnel Scenario	N/A	Displays the Tunnel Scenario specified.
Local Subnets	N/A	Displays the Local Subnets specified.
Remote IP/FQDN	N/A	Displays the Remote IP/FQDN specified.
Remote Subnets	N/A	Displays the Remote Subnets specified.
Conn. Time	N/A	Displays the connection time for the IPSec tunnel.
Status	N/A	Displays the Status of the VPN connection. The status displays are Connected, Disconnected, Wait for traffic, and Connecting.
Edit Button	N/A	Click on Edit Button to change IPSec setting, web-based utility will take you to the IPSec configuration page. (**Security> VPN > IPSec** tab)

3.2.1.2 Open VPN Status

OpenVPN Server Status		
Item	**Value**	**Description**
User Name	N/A	Displays the Client name that was entered during configuration
Remote IP/FQDN	N/A	Displays the public IP address (the WAN IP address) of the connected OpenVPN Client
Virtual IP/MAC	N/A	Displays the virtual IP/MAC address assigned to the connected OpenVPN client.
Conn. Time	N/A	Displays the connection time for the corresponding OpenVPN tunnel.
Status	N/A	Displays the connection status of the corresponding OpenVPNtunnel. The status can be Connected or Disconnected.

3.2.1.3 Open VPN Client Status

OpenVPN Client Status		
Item	**Value**	**Description**
OpenVPN Client Name	N/A	Displays the Client name entered during configuration.
Interface	N/A	Displays the WAN interface specified for the OpenVPN client connection.
Remote IP/FQDN	N/A	Displays the peer OpenVPNServer's Public IP address (the WAN IP address) or FQDN.
Remote Subnet	N/A	Displays the Remote Subnet specified.
TUN/TAP Read(bytes)	N/A	Displays the TUN/TAP Read Bytes of OpenVPN Client.
TUN/TAP Write(bytes)	N/A	Displays the TUN/TAP Write Bytes of OpenVPN Client.
TCP/UDP Read(bytes)	N/A	Displays the TCP/UDP Read Bytes of OpenVPN Client.
TCP/UDP Write(bytes)	N/A	Displays the TCP/UDP Write Bytes of OpenVPN Client. Connection
Conn. Time	N/A	Displays the connection time for the corresponding OpenVPN tunnel.
Conn. Status	N/A	Displays the connection status of the corresponding OpenVPN tunnel. The status can be Connected or Disconnected.

3.2.1.4 L2TP Server/Client Status

The LT2TP Server/Client Status shows the configuration for establishing LT2TP tunnel and current connection status

L2TP Server Status		
Item	**Value**	**Description**
User Name	N/A	Displays the login name entered during configuration of the connection.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected L2TP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected L2TP client.
Remote Call ID	N/A	Displays the L2TP client Call ID.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of each of the L2TP client connection. The status displays Connected, Disconnect, Connecting
Edit Button	N/A	Click on **Edit** Button to change L2TP server setting, web-based utility will take you to the L2TP server page. (**Security**> **VPN** > **L2TP** tab)

L2TP Client Status		
Item	**Value**	**Description**
Client Name	N/A	Displays Name for the L2TP Client specified.
Interface	N/A	Displays the WAN interface with which the 6402 will use to request PPTP tunnelling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of L2TP server.
Remote IP/FQDN	N/A	Displays the L2TP Server's Public IP address (the WAN IP address) or FQDN.
Default 6402/Remote Subnet	N/A	Displays the specified IP address of the 6402 device used to connect to the internet to connect to the L2TP server –the default 6402. Or other specified subnet if the default 6402 is not used to connect to the L2TP server –the remote subnet.
Conn. Time	N/A	Displays the connection time for the L2TP tunnel.
Status	N/A	Displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change L2TP client setting, web-based utility will take you to the L2TP client page. (**Security**> **VPN** > **L2TP** tab)

3.2.1.5 PPTP Server/Client Status

The PPTP Server/Client Status screen shows the configuration for establishing PPTP tunnel and current connection status.

PPTP Server Status		
Item	**Value**	**Description**
User Name	N/A	Displays the login name of the user entered during configuration.
Remote IP	N/A	Displays the public IP address (the WAN IP address) of the connected PPTP client.
Remote Virtual IP	N/A	Displays the IP address assigned to the connected PPTP client.
Remote Call ID	N/A	Displays the PPTP client Call ID.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of each of the PPTP client connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP server setting, web-based utility will take you to the PPTP server page. (**Security> VPN > PPTP** tab)

PPTP Client Status		
Item	**Value**	**Description**
Client Name	N/A	Displays Name for the PPTP Client specified.
Interface	N/A	Displays the WAN interface with which the 6402 will use to request PPTP tunnelling connection to the PPTP server.
Virtual IP	N/A	Displays the IP address assigned by Virtual IP server of PPTP server.
Remote IP/FQDN	N/A	Displays the PPTP Server's Public IP address (the WAN IP address) or FQDN.
Default 6402 / Remote Subnet	N/A	Displays the specified IP address of the 6402 device used to connect to the internet to connect to the PPTP server –the default 6402. Or other specified subnet if the default 6402 is not used to connect to the PPTP server –the remote subnet.
Conn. Time	N/A	Displays the connection time for the PPTP tunnel.
Status	N/A	Displays the Status of the VPN connection. The status displays Connected, Disconnect, and Connecting.
Edit Button	N/A	Click on **Edit** Button to change PPTP client setting, web-based utility will take you to the PPTP server page. (**Security> VPN > PPTP** tab)

3.2.2. Firewall Status

From the menu on the left, select Status >Security > Firewall Status Tab.

3.2.2.1 Packet Filter Status

Packet Filter Status		
Item	**Value**	**Description**
Activated Filter Rule	N/A	This is the Packet Filter Rule name.
Detected Contents	N/A	This is the logged packet information, including the source IP, destination IP, protocol, and destination port –the TCP or UDP. String format:Source IP to Destination IP: Destination Protocol (TCP or UDP)
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: *Ensure Packet Filter Log Alert is enabled. Refer to Security > Firewall > Packet Filter tab. Check Log Alert and save the setting.*

3.2.2.2 URL Blocking Status

URL Blocking Status		
Item	**Value setting**	**Description**
Activated Blocking Rule	N/A	This is the URL Blocking Rule name.
Blocked URL	N/A	This is the logged packet information.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

Note: Ensure URL Blocking Log Alert is enabled.

Refer to Security > Firewall > URL Blocking tab. Check Log Alert and save the setting

3.2.2.3 Web Content Filter Status

Web Content Filter Status		
Item	**Value**	**Description**
Activated Filter Rule	N/A	Logged packet of the rule name. String format.
Detected Contents	N/A	Logged packet of the filter rule. String format.
IP	N/A	Logged packet of the Source IP. IPv4 format.
Time	N/A	Logged packet of the Date Time. Date time format ("Month" "Day" "Hours":"Minutes":"Seconds")

***Note**: Ensure Web Content Filter Log Alert is enabled.*

*Refer to **Security > Firewall > Web Content Filter** tab. Check Log Alert and save the setting*

3.2.2.4 MAC Control Status

MAC Control Status		
Item	**Value**	**Description**
Activated Control Rule	N/A	This is the MAC Control Rule name.
Blocked MAC Addresses	N/A	This is the MAC address of the logged packet.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

***Note:** Ensure MAC Control Log Alert is enabled.*

Refer to Security > Firewall > MAC Control tab. Check Log Alert and save the setting.

3.2.2.5 Application Filters

Application Filters Status		
Item	**Value**	**Description**
Filtered Application Category	N/A	The name of the Application Category being blocked.
Filtered Application Name	N/A	The name of the Application being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

***Note:** Ensure Application Filter Log Alert is enabled.*

Refer to Security > Firewall > Application Filter tab. Check Log Alert and save the setting.

3.2.2.6 IPS Status (Intrusion Protection Support)

IPS Firewall Status		
Item	**Value**	**Description**
Detected Intrusion	N/A	This is the type of intrusion packets being blocked.
IP	N/A	The Source IP (IPv4) of the logged packet.
Time	N/A	The Date and Time stamp of the logged packet. Date & time format. ("Month" "Day" "Hours":"Minutes":"Seconds")

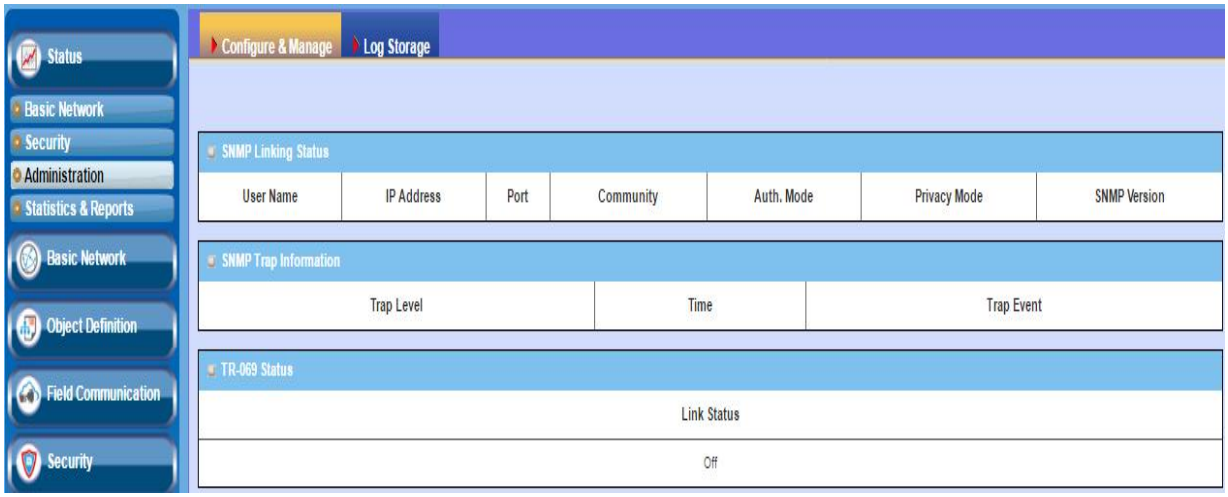
Note: Ensure IPS Log Alert is enabled.
Refer to Security> Firewall > IPS tab. Check Log Alert and save the setting.

3.2.2.7 Firewall Options Status

Firewall Options Status		
Item	**Value setting**	**Description**
Stealth Mode	N/A	Enable or Disable setting status of Stealth Mode on Firewall Options. String Format: Disable or Enable
SPI	N/A	Enable or Disable setting status of SPI on Firewall Options. String Format: Disable or Enable
Discard, Ping from WAN	N/A	Enable or Disable setting status of Discard Ping from WAN on Firewall Options. String Format: Disable or Enable
Remote Administrator Management	N/A	Enable or Disable setting status of Remote Administrator. If Remote Administrator is enabled, it shows the currently logged in administrator's source IP address and login user name and the login time. Format: IP: "Source IP", User Name: "Login User Name", Time: "Date time" Example: IP: 192.168.127.39, User Name: admin, Time: Mar 3 01:34:13

Note: *Ensure Firewall Options Log Alert is enabled.*
Refer to ***Security> Firewall > Options*** *tab. Check Log Alert and save the setting.*

3. 3 Administration



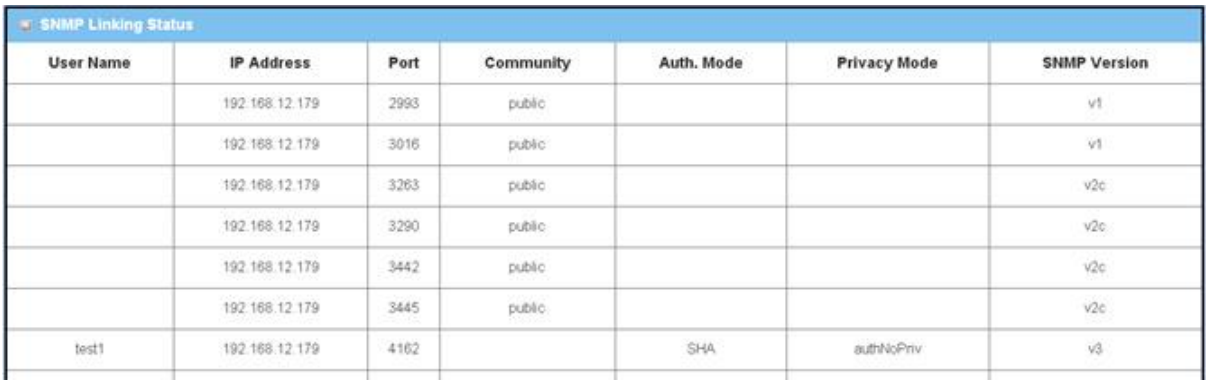
3.3.1 Configure & Manage Stats

From the menu on the left, select Status >Administration > Configure & Manage tab.

3.3.1.1 SNMP Linking Status

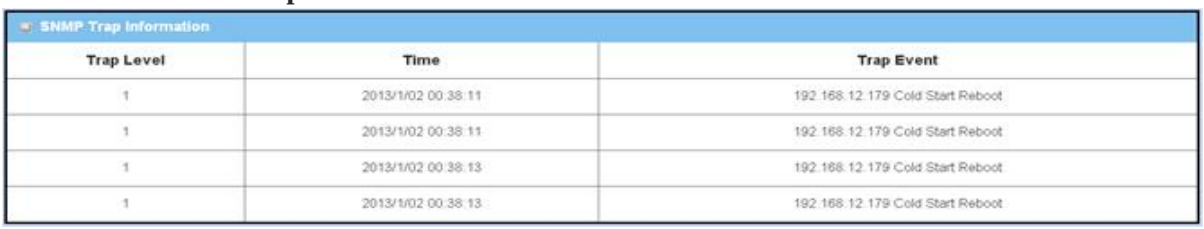
The SNMP Link Status screen shows the status of current active SNMP connections.

The Configure & Manage Status window shows the status for managing remote network devices.



SNMP Link Status		
Item	**Value**	**Description**
User Name	N/A	Displays the user name for authentication. This is only available for SNMP version 3.
IP Address	N/A	Displays the IP address of SNMP manager.
Port	N/A	Displays the port number used to maintain connection with the SNMP manager.
Community	N/A	Displays the community for SNMP version 1 or version 2c only.
Auth. Mode	N/A	Displays the authentication method for SNMP version 3 only.
Privacy Mode	N/A	Displays the privacy mode for version 3 only.
SNMP Version	N/A	Displays the SNMP Version employed.

3.3.1.2 SNMP Trap Information



SNMP Trap Information		
Item	**Value**	**Description**
Trap Level	N/A	Displays the trap level.
Time	N/A	Displays the timestamp of trap event.
Trap Event	N/A	Displays the IP address of the trap sender and event type.

3.3.1.3 TR-069 Status

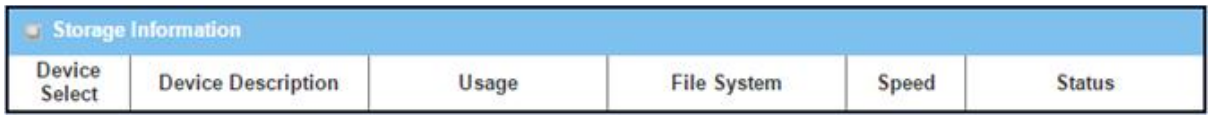
The TR-069 Status screen shows the current connection status with the TR-069 server.

TR-069 Status		
Item	**Value**	**Description**
Link Status	N/A	Displays the current connection status with the TR-068 server. The connection status is either On when the device is connected with the TR-069 server or Off when disconnected.

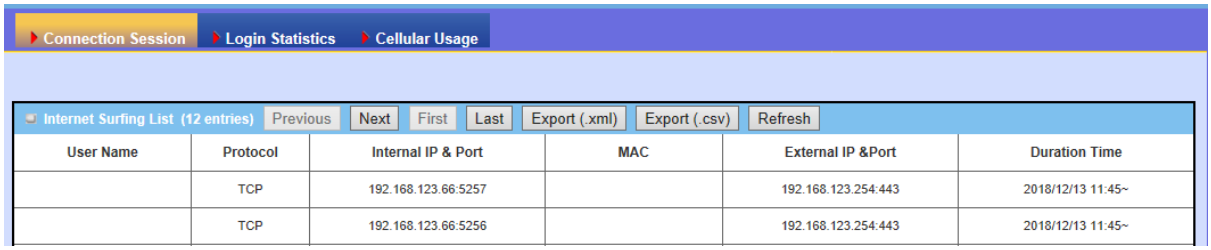
3.3.2 Log Storage Status

The Log Storage Status window shows the status for selected device storage.

From the menu on the left, select Status >Administration > Log Storage tab.



3. 4 Statistics and Reporting



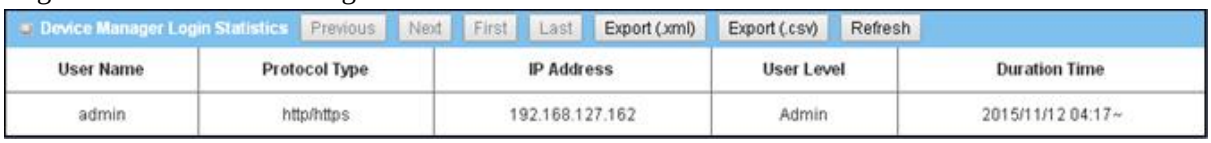
3.4.1 Connection Session

Internet Surfing Statistic		
Item	**Value**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of track list.
Next	N/A	Click the **Next** button; you will see the next page of track list.
First	N/A	Click the **First** button; you will see the first page of track list.
Last	N/A	Click the **Last** button; you will see the last page of track list.
Export (.xml)	N/A	Click the **Export (.xml)** button to export the list to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the list to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the list.

3.4.2. Login Statistics

Go to Status > Statistics & Reports >Login Statistics tab.

Login Statistics shows the login information

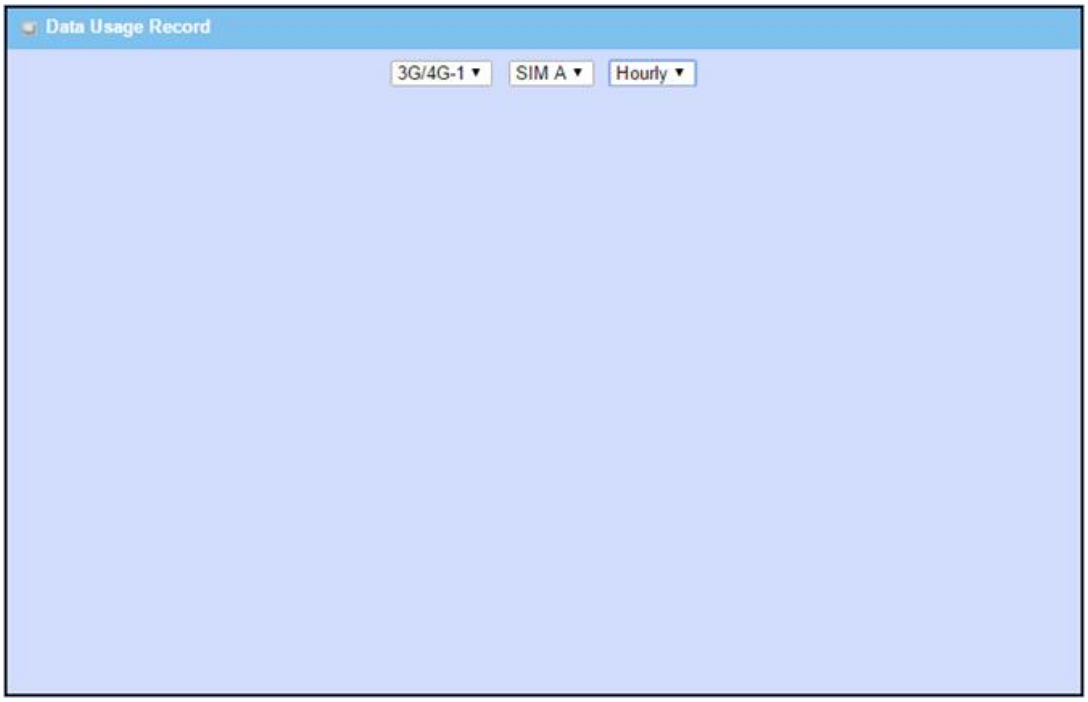


Device Manager Login Statistic		
Item	**Value**	**Description**
Previous	N/A	Click the **Previous** button; you will see the previous page of login statistics.
Next	N/A	Click the **Next** button; you will see the next page of login statistics
First	N/A	Click the **First** button; you will see the first page of login statistics
Last	N/A	Click the **Last** button; you will see the last page of login statistics
Export (.xml)	N/A	Click the **Export (.xml)** button to export the login statistics to xml file.
Export (.csv)	N/A	Click the **Export (.csv)** button to export the login statistics to csv file.
Refresh	N/A	Click the **Refresh** button to refresh the login statistics

3.4.3 Cellular Usage

Go to Status > Statistics & Reports > Cellular Usage tab.

Cellular Usage screen shows data usage statistics for the selected cellular interface. The cellular data usage can be accumulated per hour or per day.



SECTION 4

BASIC NETWORK

4.1 WAN & UPLINK - Configuring WAN Ports

4.1.1 Physical Interface

4.1.1.1 Introduction.

Basic Network>WAN & Uplink>Physical Interface> Physical Interface List

The Case Communications 6402 Router / Gateway provides one or more WAN interfaces allowing multiple paths out to the Internet.

The WAN Connection lets you specify the WAN Physical Interface, WAN Internet Setup and WAN Load Balancing to access the Internet.

For each **WAN Interface**, you must specify the following

1.Its physical interface first.

2. The configuration to allow it to connect to your ISP.

Physical Interface List

Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	ADSL	Always on	100 (Mbps) / 100 (Mbps)	Edit
WAN-2	3G/4G	Always on	150 (Mbps) / 150 (Mbps)	Edit
WAN-3	Ethernet	Failover	100 (Mbps) / 100 (Mbps)	Edit

If the 6402 has multiple WAN interfaces, you also can assign a physical interface to participate in the Load Balance function.

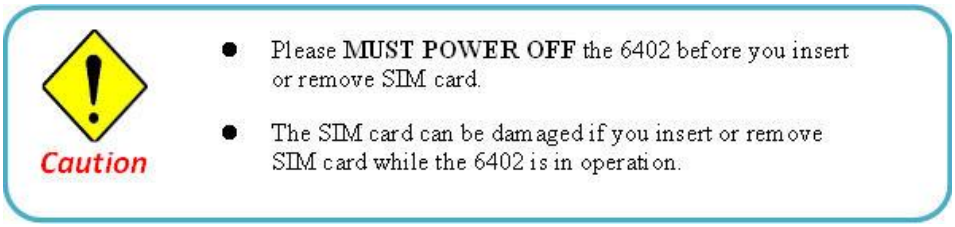
The screen shot below shows the Physical Interface List for a 6402

The 6402 Industrial ADSL router supports different types of WAN interfaces and connections. Typically, the 6402 Interfaces will be;

ADSL WAN: The 6402 has one built in ADSL modem that can be configured to be a WAN connection, plug in an RJ11 cable (normally the landline phone cable) to the DSL port and follow the GUI setting to setup.

Ethernet WAN: The 6402 has one or more RJ45 WAN ports that can be configured to be WAN connections. For each Ethernet WAN port, plug in an RJ45 cable from your external DSL modem to the port and follow the GUI configure. If the 6402 is behind a firewall, plug in an RJ45 cable from one of the Ethernet ports of firewall.

3G/4G WAN: The 6402 has one built-in 3G/4G modem that can be configured to be a WAN connection. For each built-in modem, there are 1 or 2 SIM cards which are inserted into the modem, please insert the SIM card and follow the GUI to setup.



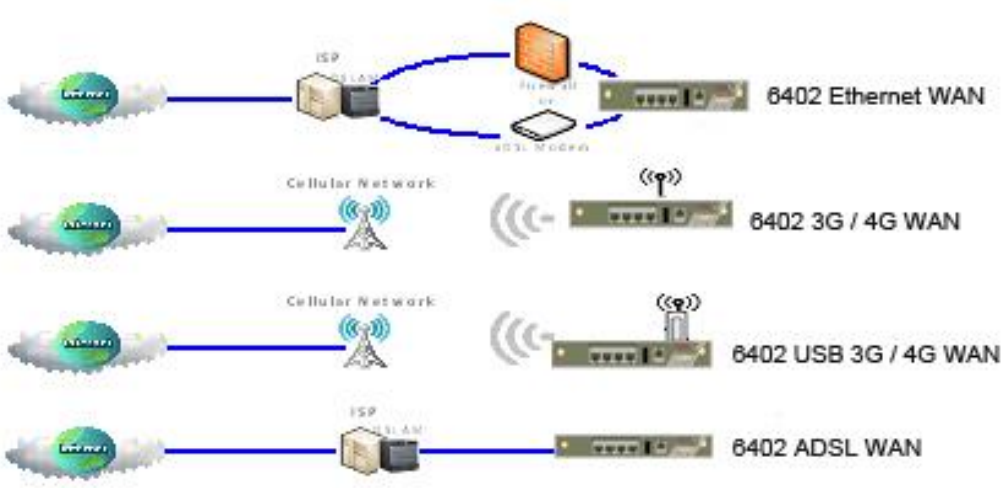
Operating Modes
There are three operating modes “Always on”, “Failover”, and “Disable” for the operation mode setting.

Always on:
Set the WAN interface to be active all the time. Only interfaces with "Always on" for their operational mode can share their bandwidth for load balancing. This means that when two or more Internet connections are established simultaneously as "Always on", outgoing data will be transferred through these WAN connections based on load balancing policies.
This mode is especially suitable for high bandwidth requirement, such as video streaming.

Failover:
A failover interface is a backup connection for the primary link. That means if the 6402 primary WAN connection is broken, the backup connection will be started to provide an alternate path to the Internet. In addition, there is a "Seamless" option for Failover mode. When the ‘Seamless’ option is activated by selecting the "Seamless" box, both the primary connection and the failover connection are started once the 6402 has rebooted. However only the primary connection transfers data, while the failover one just keeps the connection to the line alive. As soon as the primary connection is broken, the 6402 will switch to the failover path, allowing the routing change to be very rapid saving the dial up time, as the link has already been established.

Disable: Set this WAN interface to be inactive.

Line Speed
Specify the correct line speed (bandwidth) for each WAN interface to allow the 6402to operate its QoS and WAN Load Balancing. It is necessary to configure the parameters if you want to use QoS and WAN Load Balance functions on the 6402.



To determine the correct line speed for each WAN interface, the 6402 can use its QoS and WAN Load Balancing functions.
If you don't know the accurate line speed of your Internet service, the following are some suggestions:

- High Speed Ethernet WAN: Upload 100Mbps, Download 100Mbps;
- Gigabit Ethernet WAN: Upload 1000Mbps, Download 1000Mbps;
- CAT4 Built-in LTE Module: Upload 50Mbps, Download 150Mbps;
- CAT3 LTE USB Dongle: Upload 50Mbps, Download 100Mbps;
- 3G USB Dongle: Upload 5Mbps, Download 21Mbps;
- ADSL2+: Upload 2Mbps, Download 22Mbps.

4.1.2 Connection Setup

Basic Network> WAN & Uplink>Connection Setup> WAN Port(X) Edit
Internet Connection list – ADSL and Cellular WAN Ports

4.1.2.1 Internet Connection List

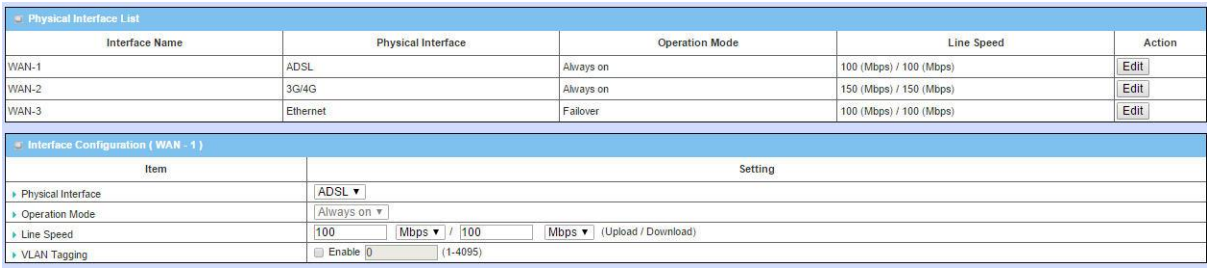
This is a top level menu which shows the WAN ports that have been configured.
Select Edit to the right of each WAN port to go into the physical configuration options.

The WAN Ports have a number of common parameters which will be described in WAN port 1 which apply equally to WAN ports 2 and 3.

Depending on the WAN Interface and the mode of operation the options are different.

THE WAN PORTS– Configuration options can be seen below

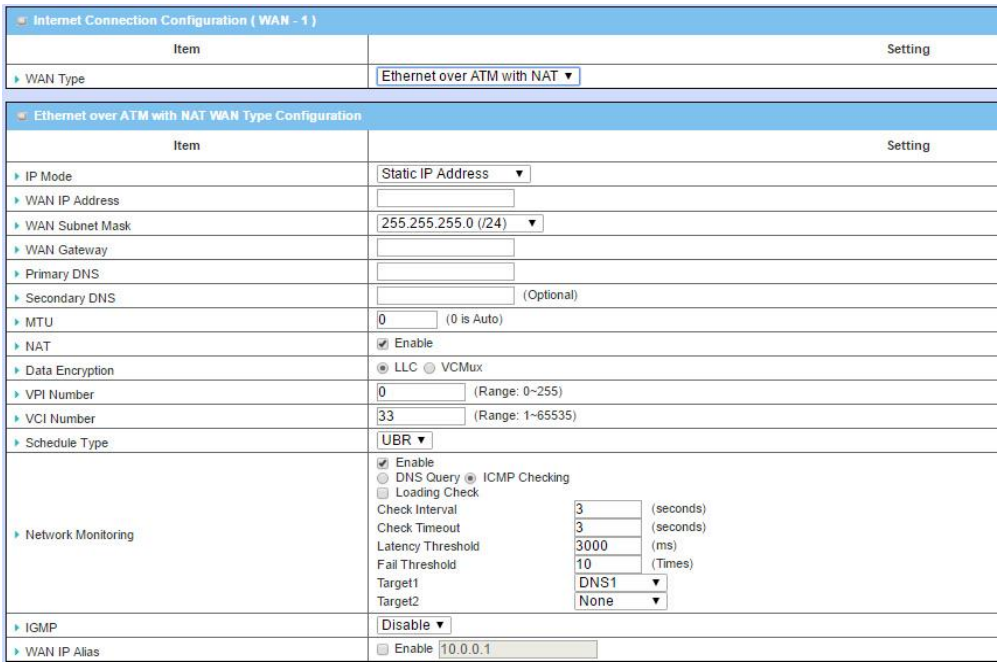
ADSL	Cellular	Ethernet
Ethernet Over ATM with NAT	2G / 3G / 4G / LTE	Static IP
IP Over ATM		Dynamic IP
PPPoE ADSL		PPPoE
PPP Over ATM		PPTP



The 6402 has the following WAN 1 options

4.1.2.2 WAN Port Options

Ethernet Over ATM with NAT



Ethernet over ATM with NAT WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	1. Mandatory 2. **Dynamic IP Address** is set by default	Specify the IP mode for the ADSL connection. It can be a **Dynamic IP Address**, or **Static IP address**. If you select Static IP address, you have to further specify the information of WAN IP Address, WAN Subnet Mask, and Primary/Secondary DNS.
Host Name	An optional setting	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your service provider. Or Click the **Clone** button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to the Internet.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. NAT is enabled by default.	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Data Encryption	1. Mandatory **2. LLC** is selected by default.	Specify the data encapsulation method for the ADSL connection. The options are **LLC** or **VCMux**. LLC (Logic Link Control) and VCMux (Virtual Circuit Multiplexing) mechanisms are methods for identifying the protocol carried in the ATM Adaptation Layer 5 (AAL5) frames specified by RFC 2684, Multi-protocol Encapsulation over ATM. These two options depend on your ISP.
VPI Number, VCI Number	1. Mandatory **2. (0,38)** is default for UK.	Enter the VPI, VCI values assigned to you. These values depend on your ISP setting. ***Value Range*:** 0 ~ 255 for VPI (Virtual Path Identifier); 1 ~ 65535 for VCI (Virtual Channel Identifier).
Schedule Type	1. Mandatory **2. UBR** is selected by default.	Select the schedule type from the dropdown list, depending on your ISP setting. The options are **UBR** (Unspecified Bit Rate) / **CBR** (Constant Bit Rate) / **VBR** (Variable Bit Rate) / **GFR** (Guaranteed Frame Rate).
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

4.1.2.3 IP Over ATM

The table below shows the configuration page for IP Over ATM

IP over ATM WAN Type Configuration		
Item	**Value setting**	**Description**
IP Mode	**1.Mandatory** . 2. **Static IP Address** is set by default	Specify the IP mode for the ADSL connection. It can be **Dynamic IP Address**, or **Static IP address**. If you select Static IP address, you have to further specify the information of WAN IP Address, WAN Subnet Mask, WAN 6402, and Primary/Secondary DNS.
Host Name	An optional setting	Enter the host name provided by your Service Provider.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your service provider. Or Click the **Clone** button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to Internet.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. NAT is enabled by default.	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Data Encryption	1. A Must filled setting **2. LLC** is selected by default.	Specify the data encapsulation method for the ADSL connection. It can be **LLC** or **VCMux**. LLC (Logic Link Control) and VCMux (Virtual Circuit Multiplexing) mechanisms are the method for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames specified by RFC 2684, Multi-protocol Encapsulation over ATM. These two options depend on your ISP setting.
VPI Number, VCI Number	1. Mandatory **2. (0,38)** is default for UK.	Enter the VPI, VCI values assigned to you. These values depend on your ISP setting. ***Value Range*:** 0 ~ 255 for VPI (Virtual Path Identifier); 1 ~ 65535 for VCI (Virtual Channel Identifier).
Schedule Type	1. Mandatory **2. UBR** is selected by default.	Select the schedule type from the dropdown list, depending on your ISP setting. The options are **UBR** (Unspecified Bit Rate) / **CBR** (Constant Bit Rate) / **VBR** (Variable Bit Rate) / **GFR** (Guaranteed Frame Rate).
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

4.1.2.4 PPPoE ATM

The table below shows the PPPoE ATM Configuration page

PPPoE (ADSL) WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	Mandatory	Enter the PPPoE User Name provided by your Service Provider.
PPPoE Password	Mandatory	Enter the PPPoE password provided by your Service Provider.
Primary DNS	Mandatory	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Service Name	An optional setting	Enter the service name if your ISP requires it
Assigned IP Address	An optional setting	Enter the IP address assigned by your Service Provider.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. NAT is enabled by default.	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Data Encryption	1. Mandatory **2. LLC** is selected by default.	Specify the data encapsulation method for the ADSL connection. It can be **LLC** or **VCMux**. LLC (Logic Link Control) and VCMux (Virtual Circuit Multiplexing) mechanisms are the method for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames specified by RFC 2684, Multi-protocol Encapsulation over ATM. These two options depend on your ISP setting.
VPI Number, VCI Number	1. Mandatory **2. (0,38)** is default for UK	Enter the VPI, VCI values assigned to you. These values depend on your ISP setting. ***Value Range*:** 0 ~ 255 for VPI (Virtual Path Identifier); 1 ~ 65535 for VCI (Virtual Channel Identifier).
Schedule Type	1. Mandatory **2. UBR** is selected by default.	Select the schedule type from the dropdown list, depending on your ISP setting. The options are **UBR** (Unspecified Bit Rate) / **CBR** (Constant Bit Rate) / **VBR** (Variable Bit Rate) / **GFR** (Guaranteed Frame Rate).
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

4.1.2.5 PPP over ATM

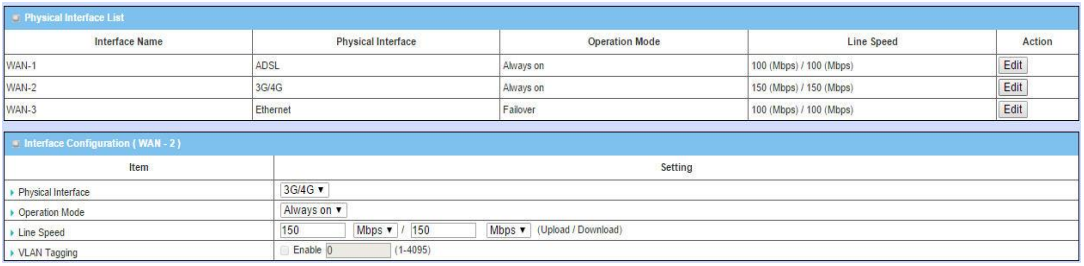
The Table below shows the PPP Over ATM (ADSL WAN) configuration page.

PPP over ATM WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoA Account	Mandatory	Enter the PPPoA User Name provided by your ISP
PPPoEAPass word	Mandatory	Enter the PPPoA password provided by your ISP
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Service Name	An optional setting	Enter the service name if your ISP requires it
Assigned IP Address	An optional setting	Enter the IP address assigned by your Service Provider.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. NAT is enabled by default.	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Data Encryption	1. Mandatory **2. LLC** is selected by default.	Specify the data encapsulation method for the ADSL connection. It can be **LLC** or **VCMux**. LLC (Logic Link Control) and VCMux (Virtual Circuit Multiplexing) mechanisms are the method for identifying the protocol carried in ATM Adaptation Layer 5 (AAL5) frames specified by RFC 2684, Multi-protocol Encapsulation over ATM. These two options depend on your ISP
VPI Number, VCI Number	1. Mandatory **2. (0,38)** is default for UK	Enter the VPI, VCI values assigned to you. These values depend on your ISP. ***Value Range*:** 0 ~ 255 for VPI (Virtual Path Identifier); 1 ~ 65535 for VCI (Virtual Channel Identifier).
Schedule Type	1. Mandatory **2. UBR** is selected by default.	These options select the schedule type from the dropdown list; these depend on your ISP. The options are **UBR** (Unspecified Bit Rate) / **CBR** (Constant Bit Rate) / **VBR** (Variable Bit Rate) / **GFR** (Guaranteed Frame Rate).
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

4.1.2.6 WAN 2 – 3G/4G Configuration options

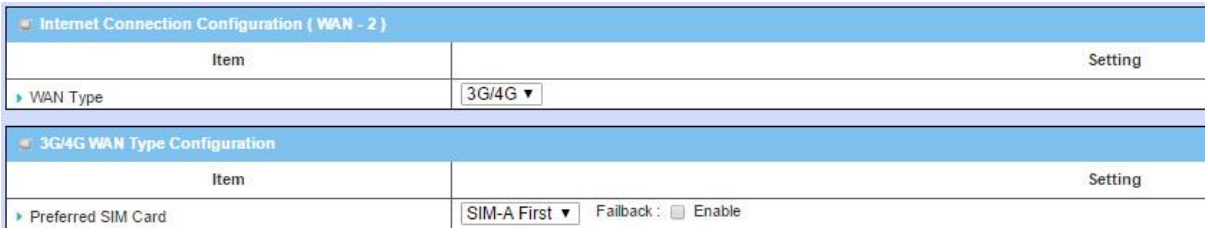
Basic Network > WAN & Uplink >Connection Setup> WAN 2 / Edit

The screen shot below shows the WAN 2 configuration options. By default, WAN 2 is a 3G / 4G Cellular port.



Physical Interface – WAN 2			
Item	**Default Value**	**Option**	**Notes**
Physical Interface	3G / 4G	None	
Operational Mode	Always On	Disabled or Failover	
Line Speed	150Mbps	150Mbps	Upload / Download rates Max 150
VLAN Tagging	Not Enabled	Enable	If enable set VLAN ID 1-4095

3G / 4G WAN Configuration

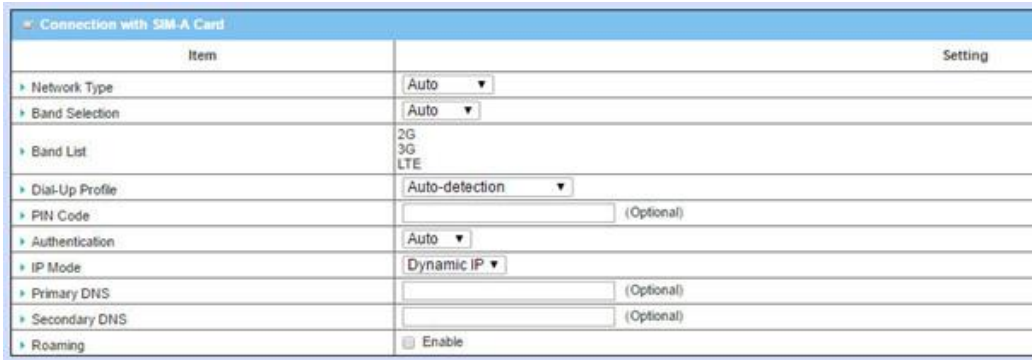


The screen shot above configures the WAN 2 port to be 3G / 4G and allows the option for the preferred SIM card. The table below allows you to set the order of SIMS used.

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	Mandatory 3G/4G is set by default	From the dropdown box, select the Internet connection method for your 3G/4G WAN Connection. Only **3G/4G** is available.
Preferred SIM Card	1. Mandatory 2. By default **SIM-A First** is selected 3. **Failback** is unchecked by default	Choose which SIM card you want to use for the connection. When **SIM-A First** or **SIM-B First** is selected, it means the connection is first established using SIM A/SIM B. And if the connection does not succeed, it will change to the other SIM card and keep trying to dial again, until the connection is established. When **SIM-A only** or **SIM-B only** is selected, it will try to dial up only using the SIM card you selected. When **Failback** is selected, if the connection is dialled-up not using the second SIM, it will failback to the main SIM and try to establish the connection periodically.

Connection with SIM Card A

This menu option allows you to set configurations for the cellular connection according to your situation or requirement.



Note_1: Configurations of SIM-B Card follows the same Configuration as for SIM-A Card. In the table below, we list SIM-A as the example.

Note_2: When establishing a **Connection with the A-SIM** and **Connection with B-SIM, the B-SIM** will pop up only when the **SIM-A First** or **SIM-B First** is selected, otherwise it only displays one of the SIMS.

3G/4G Connection Configuration		
Item	**Value setting**	**Description**
Network Type	1. Mandatory 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the network type. Select **2G Only** to register the 2G network only. Select **2G Prefer** to register the 2G network first if it is available. Select **3G only** to register the 3G network only. Select **3G Prefer** to register the 3G network first if it is available. Select **LTE only** to register the LTE network only. **Note_1**: Options may be different due to the specification of the module.
Band Selection	1. Mandatory 2. By default **Auto** is selected	Select **Auto** to register a network automatically, regardless of the band. Select **Manual** to choose specific bands you want to appoint to.
Band List	1. Mandatory 2. The box is all checked by default	When **Band Selection > Auto** is selected, all bands are enabled and can't be unchecked. When **Band Selection > Manual** is selected, at least one band needs to be checked in each network type.
Dial-Up Profile	1. Mandatory 2. By default **Auto-Detection** is selected	Select **Auto-Detection** to automatically bring out the configuration options while dialling-up, by comparing the IMSI of the SIM card to the record listed in the manufacture's database. Select **Manual-configuration** to set **APN** (Access Point Name), **Dial Number**, **Account**, and **Password** to what your carrier provides. Select the **APN Profile List** to set more than one profile to dial up in order, until the connection is established. It will pop up a new field, please go to **Basic Network > WAN & Uplink > Internet Setup > SIM-A APN Profile List** for details.
PIN code	String format: integer	Enter the PIN (Personal Identification Number) code if it needs to unlock your SIM card.
Authentication	1. Mandatory 2. By default **Auto** is selected	Select **PAP** (Password Authentication Protocol) and use such protocol to be authenticated with your ISP. Select **CHAP** (Challenge Handshake Authentication Protocol)to allow the 6402 to authenticate with your ISP's server When **Auto** is selected, it means the 6402 will authenticate with the server either **PAP** or **CHAP**.
IP Mode	1. Mandatory	When **Dynamic IP** is selected, it means it will get all IP configurations from the carrier's server and set to the device directly.

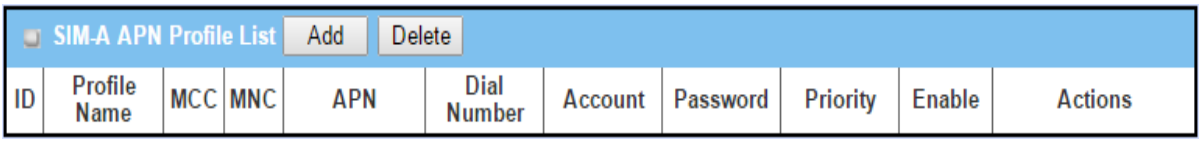
	2. By default **Dynamic IP** is selected	If you have specific application provided by the carrier, and want to set IP configurations on your own, you can switch to **Static IP** mode and fill in all parameters that required, such as IP address, subnet mask and 6402. **Note_1**: **IP Subnet Mask** is a mandatory setting, make sure you have the right configuration. Otherwise, the connection may get issues.
Primary DNS	String format: IP address (IPv4 type)	Enter the IP address to change the primary DNS (Domain Name Server) setting. If it is not filled-in, the server address is given by your ISP
Secondary DNS	String format: IP address (IPv4 type)	Enter the IP address to change the secondary DNS (Domain Name Server) setting. If it is not filled-in, the server address is provided by your ISP.
Roaming	The box is un-checked by default	Check the box to establish the connection even the registration status is roaming, not in home network. **Note_1**: The 6402 may incur additional charges if the connection is set to roaming.

The Connection for SIM B Card options are identical to SIM A card.

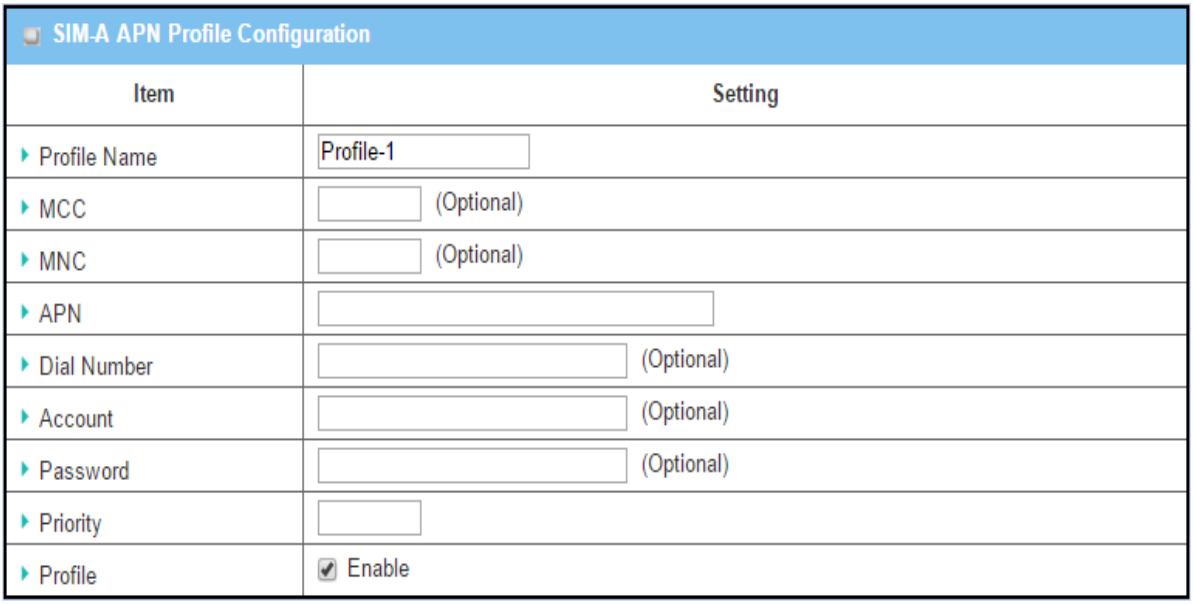
Create/Edit SIM-A / SIM-B APN Profile List

(Only Appears when Dial Up Profile set to APN Profile List)

You can add a new APN profile for the connection or modify the content of the APN profile you previously configured. This is only available when you select Dial-Up Profile as APN Profile List.



List all the APN profile you created, easily for you to check and modify. This option is only available when you select Dial-Up Profile as APN Profile List.

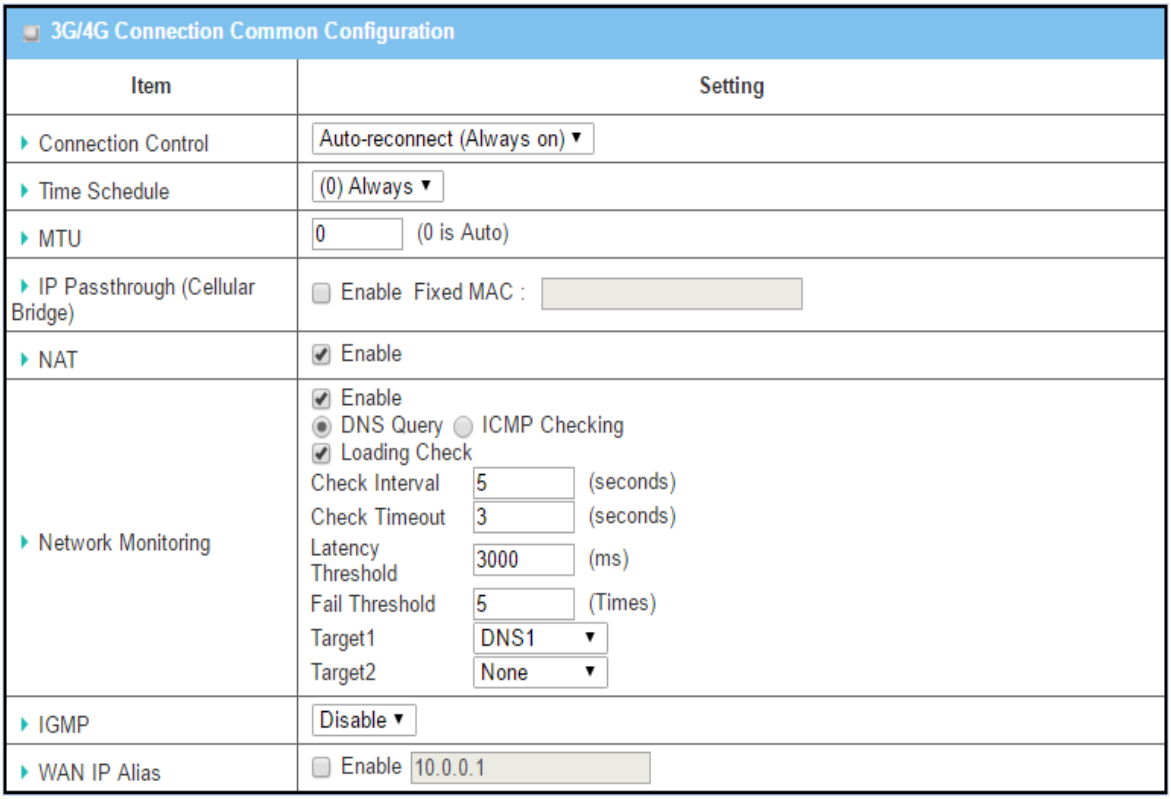


3G / 4G Connection Common Configuration

3G/4G Connection Common Configuration		
Item	**Value setting**	**Description**
Profile Name	1. By default **Profile-x** is listed 2. String format: any text	Enter the profile name you want to use to describe this profile.
MCC	String format: integer	Enter the **MCC** (Mobile Country Code) you want to use for this profile. **Note_1**: the **MCC** should be related to the **MNC**, this filed can't be invalid value if **MNC** is filled-in.
MNC	String format: integer	Enter the **MNC** (Mobile Network Code) you want to use for this profile. **Note_1**: the **MNC** should be related to the **MCC**, this filed can't be invalid value if **MCC** is filled-in.
APN	String format: any text	Enter the **APN** you want to use to establish the connection.
Dial Number	String format: integer, asterisk and number sign	Enter the **Dial Number** you want to use to establish the connection.
Account	String format: any text	Enter the **Account** you want to use for the authentication.
Password	String format: any text	Enter the **Password** you want to use for the authentication.
Priority	1. Mandatory 2. String format: integer	Enter the value for the dialling-up order. The valid value is from 1 to 16. It will start to dial up with the profile that assigned with the smallest number.
Profile	The box is checked by default	Check the box to enable this profile. Uncheck the box to disable this profile in dialling-up action.

Setup 3G/4G Connection Common Configuration

This menu allows you to change common configuration options for 3G/4G WAN.

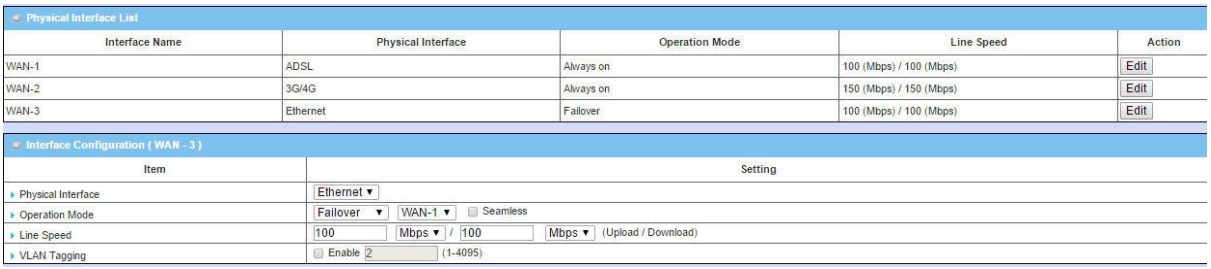


3G/4G Connection Configuration		
Item	**Value setting**	**Description**
Connection Control	By default, **Auto-reconnect (Always on)** is selected	When **Auto-reconnect (Always on)** is selected, it means the 6402 will keep the connection on all the time. When **Connect-on-demand** is selected, it means the connection will be established only when the 6402 detects data traffic. When **Connect Manually** is selected, it means you need to click the **Connect** button to dial up the connection manually. Go to Status > Network Status for details. **Note_1**: This field is available only when **Basic Network > WAN > Physical Interface > Operation Mode** is selected to **Always on**.
Time Schedule	1. Mandatory 2. By default **(0) Always** is selected	When **(0) Always** is selected, it means this 6402 WAN port is active all the time. Once you have set other schedule rules, there will be other options to select. Please go to **System > Scheduling** for details.
MTU	1. Mandatory 2. By default **0** is filled-in 3. String format: integer	Enter the **MTU** (Maximum Transmission Unit) you want to set the configuration.
IP Pass-through (Cellular Bridge)	1. The box is unchecked by default 2. String format for **Fixed MAC**: MAC address, e.g. 00:50:18:aa:bb:cc	When the **Enable** box is checked, it means the 6402 will assign a WAN IP address to the first local LAN client to connect. However, when an optional **Fixed MAC** is filled-in a non-zero value, it means only the client with this MAC address can get the WAN IP address. **Note_1**: This field is only available when 3G/4G is set to **WAN-1**. **Note_2**: When the **IP Pass-through** is enabled, it will disable other WAN (exclude 3G/4G WAN) if they are set. But if there are other 3G/4G WANs, the **IP Pass-through** will be enabled automatically when the one in WAN1 is checked. **Note_3**: When the **IP Pass-through** is on, **NAT** and **WAN IP Alias** will be unavailable until the function is disabled again.
NAT	The box is checked by default	Uncheck the box to disable **NAT** (Network Address Translation) function.
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	By default, **Disable** is selected	Select **Auto** to enable **IGMP** (Internet Group Management Protocol) function. Check the **Enable** box to enable **IGMP Proxy**.
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.

4.1.2.7 WAN 3 – Ethernet WAN Configuration options

Basic Network > WAN & Uplink >Connection Setup tab.

The screen shot below depicts WAN 3 which by default is an Ethernet port.

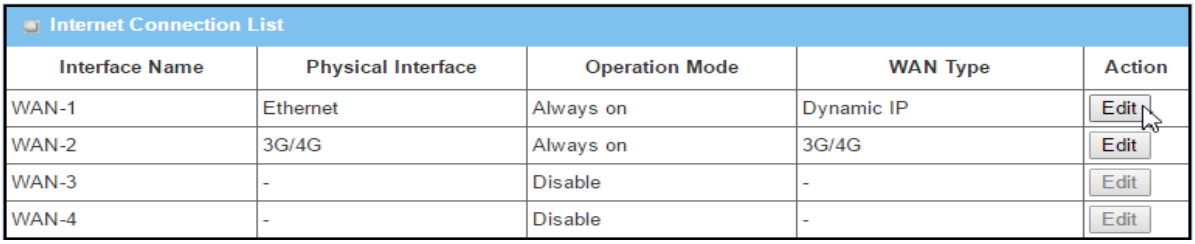


Physical Interface – WAN 3			
Item	**Default Value**	**Option**	**Notes**
Physical Interface	Ethernet	None	
Operational Mode	Always On	Disabled	
Line Speed	100Mbps	100Mbps	Upload / Download rates Max 100
VLAN Tagging	Not Enabled	Enable	If enable set VLAN ID 1-4095

The following sections explain how to configure the WAN Ports.

Internet Setup– Ethernet WAN Ports

This section explains the configuration of the 6402 using the 6402 Ethernet ports.



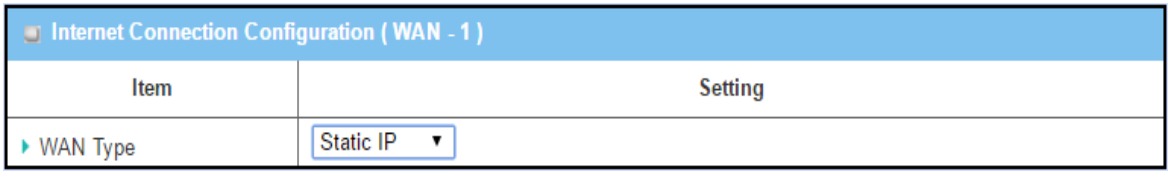
When the 6402 **Edit** button is selected the **Internet Connection Configuration** screen will appear.

Internet Connection Configuration		
Item	**Value setting**	**Description**
WAN Type	A Mandatory setting Dynamic IP is set by default	From the dropdown box, select Internet connection method for Ethernet WAN Connection. Detail settings are described in the next few pages. **Dynamic IP** **Static IP** **PPPoE** **PPTP** **L2TP**

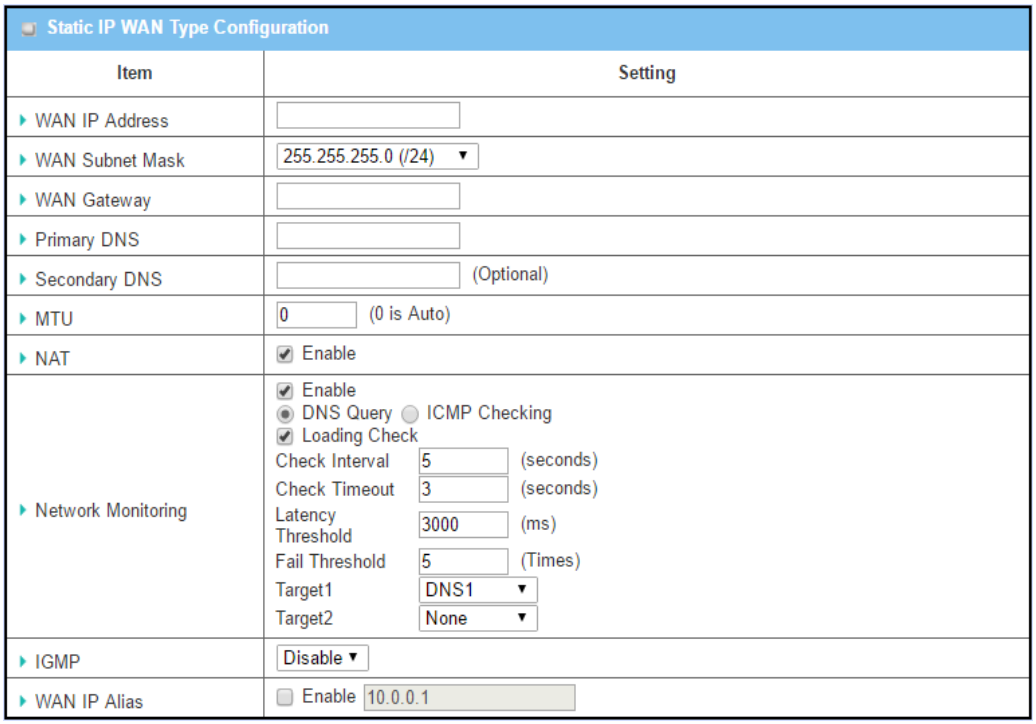
Dynamic IP (Ethernet WAN)

Dynamic IP WAN Type Configuration		
Item	**Value setting**	**Description**
Host Name	An optional setting	Enter the host name provided by your ISP.
ISP Registered MAC Address	An optional setting	Enter the MAC address that you have registered with your service provider. Or Click the **Clone** button to clone your PC's MAC to this field. Usually this is the PC's MAC address assigned to allow you to connect to Internet.
Connection Control	A Mandatory setting	There are three connection modes. **Auto-reconnect (Always on)** enables the 6402 to always keep the Internet connection on. **Connect-on-demand** enables the 6402 to automatically re-establish Internet connection as soon as user attempts to access the Internet. The 6402 Internet connection will be disconnected when it has been inactive for a specified idle time. **Connect Manually** allows the user to connect to the Internet manually**.** The Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	An optional setting NAT is enabled by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	**1.Mandaory** **2. Disable is set by default**	Enabling IGMP (Internet Group Management Protocol) allows the 6402 to listen to IGMP packets to discover which interfaces are connected to which device. The 6402 uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

Static IP (Ethernet WAN)



Basic Network

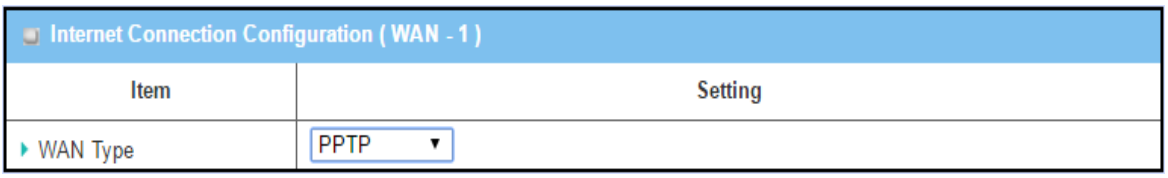


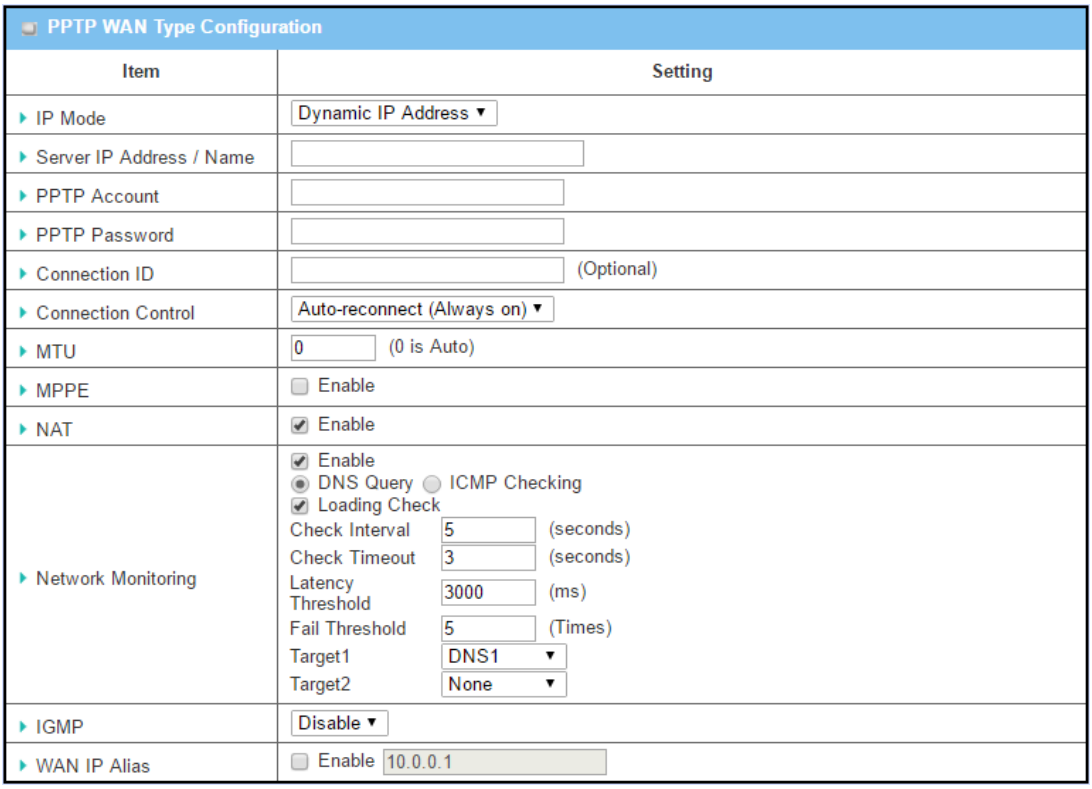
Static IP WAN Type Configuration		
Item	**Value setting**	**Description**
WAN IP Address	Mandatory Field	Enter the WAN IP address given by your ISP.
WAN Subnet Mask	Mandatory Field	Enter the WAN subnet mask given by your ISP.
WAN 6402	Mandatory Field	Enter the WAN 6402 IP address given by your ISP.
Primary DNS	Mandatory Field	Enter the primary WAN DNS IP address given by your ISP.
Secondary DNS	An optional setting	Enter the secondary WAN DNS IP address given by your ISP.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable.
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	**1.Mandaory** **2. Disable is set by default**	Enabling IGMP (Internet Group Management Protocol) allows the 6402 to listen to IGMP packets to discover which interfaces are connected to which device. The 6402 uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

PPPoE (Ethernet WAN)

PPPoE WAN Type Configuration		
Item	**Value setting**	**Description**
PPPoE Account	Mandatory	Enter the PPPoE User Name provided by your ISP.
PPPoE Password	Mandatory	Enter the PPPoE password provided by your ISP.
Primary DNS	An optional setting	Enter the IP address of Primary DNS server.
Secondary DNS	An optional setting	Enter the IP address of Secondary DNS server.
Connection Control	1. Mandatory 2. Auto-reconnect is set by default 3. Default idle time is 600s	There are three connection modes. **Auto-reconnect (Always on)** enables the 6402 to always keep the Internet connection on. **Connect-on-demand** enables the 6402 to automatically re-establish Internet connection as soon as user attempts to access the Internet. The Internet connection will be disconnected when it has been inactive for a specified idle time. **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
Service Name	An optional setting	Enter the service name if your ISP requires it
Assigned IP Address	An optional setting	Enter the IP address assigned by your Service Provider.
MTU	1. Mandatory **2. Auto** (value zero) is set by default. 3. Manual set range 1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable.
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the 6402 will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	**1.Mandatory** **2. Disable is set by default**	Enabling IGMP (Internet Group Management Protocol) allows the 6402 to listen to IGMP packets to discover which interfaces are connected to which device. The 6402 uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Box is un-checked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

PPTP (Ethernet WAN)

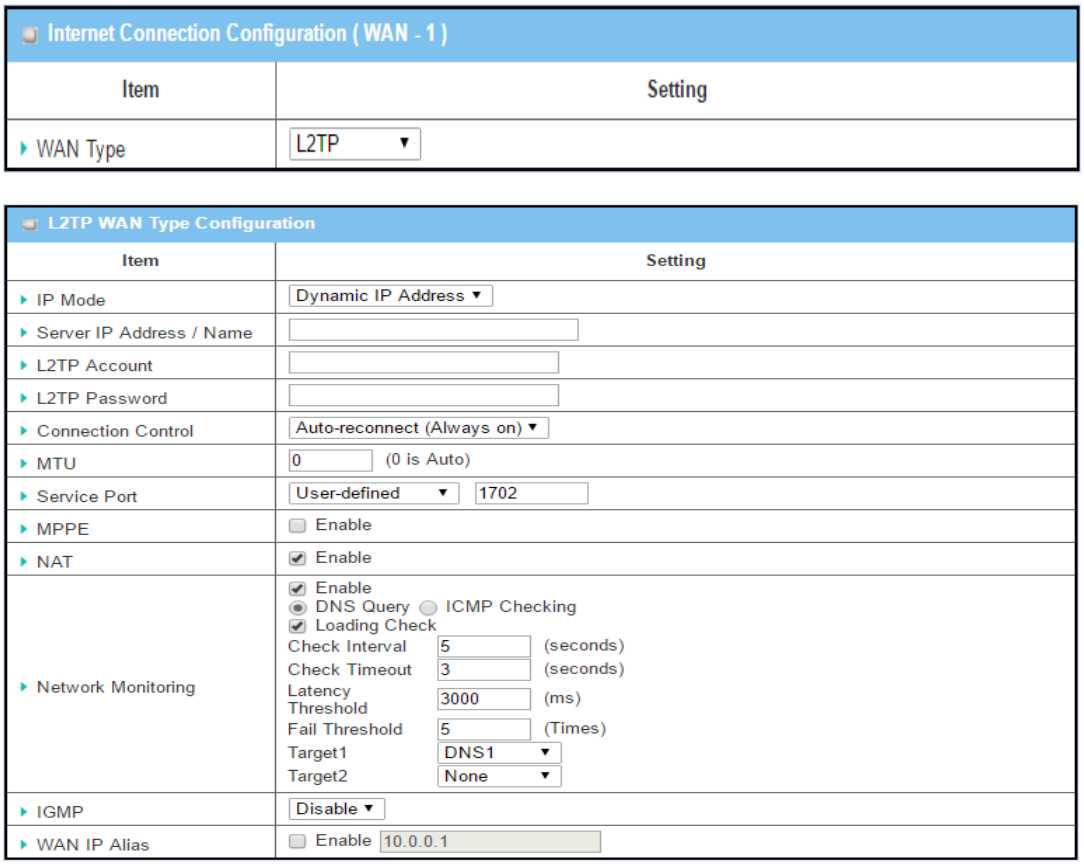




PPTP WAN Type Configuration		
Item	**Value**	**Description**
IP Mode	Mandatory field	Select either Static or Dynamic IP address for the PPTP Internet connection. When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask.** **WAN IP Address** (A Mandatory setting)**:**Enter the WAN IP address given by your Service Provider. **WAN Subnet Mask** (A mandatory setting)**:** Enter the WAN subnet mask given by your Service Provider. **WAN 6402** (A Mandatory setting)**:** Enter the WAN 6402 IP address given by your I.S.P When **Dynamic IP** is selected, there are no above settings required.
Server IP Address/Name	Mandatory field	Enter the PPTP server name or IP Address.
PPTP Account	Mandatory field	Enter the PPTP username provided by your Service Provider.
PPTP Password	Mandatory field	Enter the PPTP connection password provided by your ISP.
Connection ID	An optional setting	Enter a name to identify the PPTP connection.
Connection Control	Mandatory field	There are three connection modes. **Auto-reconnect (Always on)** enables the 6402 to always keep the Internet connection on. **Connect-on-demand** enables the 6402 to automatically re-establish Internet connection as soon as user attempts to access the Internet. The Internet connection will be disconnected when it has been inactive for a specified idle time. **Connect Manually** allows users to connect to Internet manually**.** **The** Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. Mandatory **2. Auto** (value zero) is set by	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission.

	default. 3. Manual set range 1200~1500	When set to **Auto** (value '0'), the router selects the best MTU for performance.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring .	An optional setting Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	Mandatory Disable is set by default	Enabling IGMP (Internet Group Management Protocol) allows the 6402 to listen to IGMP packets to discover which interfaces are connected to which device. The 6402 uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	An optional setting Box is un-checked by default	Enabling **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.
Save	*N/A*	Click **Save** to save the settings.
Undo	*N/A*	Click **Undo** to cancel the settings.

L2TP (Ethernet WAN)



L2TP WAN Type Configuration		
Item	**Value**	**Description**
IP Mode	Mandatory	Select either Static or Dynamic IP address for L2TP Internet connection. When **Static IP Address** is selected, you will need to enter the **WAN IP Address**, **WAN Subnet Mask,** and **WAN 6402**. **WAN IP Address** (A Must filled setting)**:**Enter the WAN IP address given by your Service Provider. **WAN Subnet Mask** (A Must filled setting)**:** Enter the WAN subnet mask given by your Service Provider. **WAN 6402** (A Must filled setting)**:** Enter the WAN 6402 IP address given by your Service Provider. When **Dynamic IP** is selected, there are no above settings required.
Server IP Address/ Name	Mandatory	Enter the L2TP server name or IP Address.
L2TPAccount	Mandatory	Enter the L2TP username provided by your Service Provider.
L2TP Password	Mandatory	Enter the L2TP connection password provided by your Service Provider.
Connection Control	Mandatory	There are three connection modes. **Auto-reconnect (Always on)** enables the 6402 to always keep the Internet connection on. **Connect-on-demand** enables the 6402to automatically re-establish Internet connection as soon as user attempts to access the Internet. Internet connection will be disconnected when it has been inactive for a specified idle time. **Connect Manually** allows user to connect to Internet manually**.** Internet connection will be inactive after it has been inactive for specified idle time.
MTU	1. Mandatory **2. Auto** (0) is set by default. 3. Manual set range1200~1500	**MTU** refers to Maximum Transmission Unit. It specifies the largest packet size permitted for Internet transmission. When set to **Auto** (value '0'), the router selects the best MTU for performance.
Service Port	Mandatory setting	Enter the service port that the Internet service. There are three options can be selected : **Auto:** Port will be automatically assigned. **1701 (For Cisco)**: Set service port to port 1701 to connect to CISCO server. **User-defined**: enter a service port provided by your Service Provider.
MPPE	An optional setting	Select **Enable** to enable MPPE **(**Microsoft Point-to-Point Encryption) security for PPTP connection.
NAT	1. An optional setting 2. Box is checked by default	Enable NAT to apply NAT on the WAN connection. Uncheck the box to disable NAT function.
Network Monitoring .	1. An optional setting 2. Box is checked by default	When the Network Monitoring feature is enabled, the router will use a DNS Query or ICMP Ping to periodically check the Internet connection **Refer to Network Monitoring later in this chapter**
IGMP	**1.Mandaory** **2. Disable is set by default**	Enabling IGMP (Internet Group Management Protocol) allows the 6402 to listen to IGMP packets to discover which interfaces are connected to which device. The 6402 uses the interface information generated by IGMP to reduce bandwidth consumption in a multi-access network environment to avoid flooding the entire network.
WAN IP Alias	1. An optional setting 2. Unchecked by default	Enable **WAN IP Alias** then enter the IP address provided by your I.S.P **WAN IP Alias** is used by the 6402 to provide dual WAN IP address on your LAN network.

4.1.3 Connection Control

This section determines how the 6402 will connect to the internet the options are:

- **Auto-reconnect (Always on):** The 6402 will establish the Internet connection automatically once it has been booted up and try to reconnect if the connection is down. It's recommended to choose this scheme for mission critical applications to ensure full-time Internet connection.
- **Dial-on-demand:** The 6402 won't start to establish an Internet connection until local data is ready to be sent to the WAN. After normal data transfer between the LAN and WAN, the 6402 will disconnect the WAN connection if the idle time reaches the value of the Maximum Idle Time.
- **Manually:** The 6402 Gateway won't start to establish a WAN connection until the network managers presses the "Connect" button on the web GUI. After normal data transfer between LAN and WAN, the 6402 will disconnect the WAN connection if the idle time reaches the value of Maximum Idle Time**.**

Note: If the WAN interface serves as the primary port for another WAN interface in a Failover role, the Connection Control parameter will not be available for you to configure, the system must set it to "Auto-reconnect (Always on)".

4.1.5.1 Auto-reconnect / Dial-on-demand / Manual Scenario:

In the table example below, WAN-1, WAN-2 and WAN-3 are all Ethernet interfaces with "Always on" operation mode. Their WAN Type is set to "Dynamic IP" but with different Connection Control approaches. WAN-1 uses "Auto-reconnect (Always on)", WAN-2 uses "Dial-on-demand" and WAN-3 uses "Manually". The following table lists the parameter configuration for these three WAN interfaces.

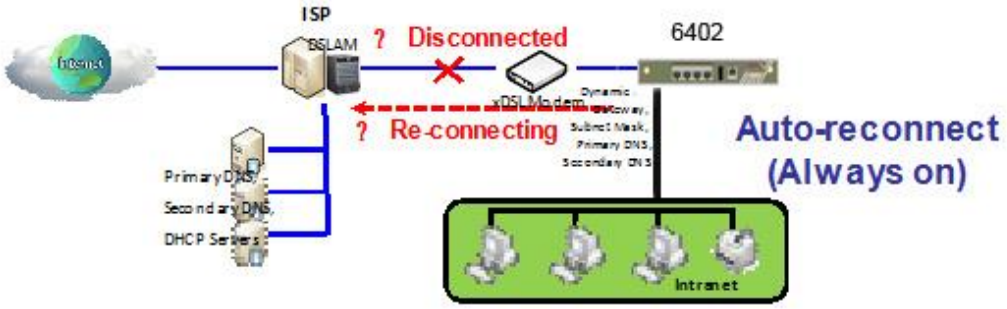
Note: If the Edit button is disabled for the Interface, you will need to enable the Interface first by going to Basic Network > WAN & Uplink > Physical Interface page. Then Click the Edit button then select Always on or Failover.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2,3		
Interface Name	WAN-1	WAN-2	WAN-3
Physical Interface	Ethernet	Ethernet	Ethernet
Operation Mode	Always on	Always on	Always on
Line Speed	100Mbps / 100Mbps	100Mbps / 100Mbps	100Mbps / 100Mbps
Interface Name	WAN-1	WAN-2	WAN-3
WAN Type	Dynamic IP	Dynamic IP	Dynamic IP
Interface Name	WAN-1	WAN-2	WAN-3
Connection Control	Auto-reconnect (Always	Dial-on-demand	Manually

The 6402 keeps the WAN connection alive. The connection control is controlled by the "Auto-reconnect (Always on)" option. After the 6402 boots up, the connection will be live and once the connection is down, the 6402 will re-connect it.

4.1.5.2 The 6402 Auto-Reconnect (Always On)

This scenario is shown in following diagram:



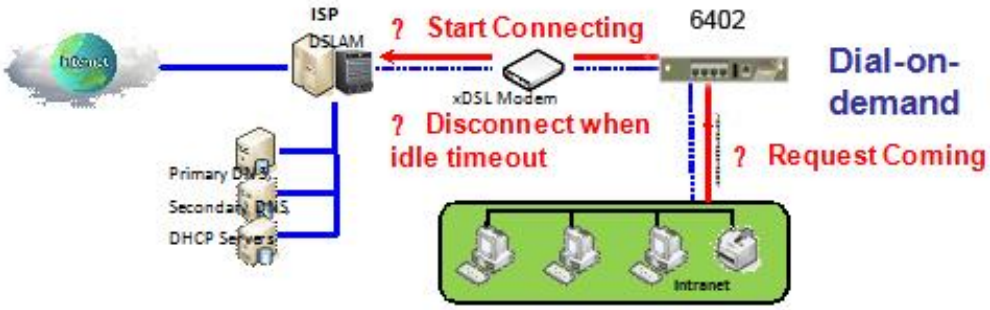
4.1.5.3 6402 Gateway Dial on Demand

Pre-state: After the 6402 boots up, the router tries to bring the WAN connection up.

S 1: When the system discovers the WAN connection has failed.

S 2: The 6402 starts to re-connect the WAN connection until it's in a connected state.

In the "Dial-on-demand" scenario, the 6402 Gateway will not establish the WAN connection until the 6402 receives an Internet access request from the local Intranet. The connection will keep the link alive only when there is still data to transfer. If there is no data transfer for a period longer than the Maximum Idle Time, the 6402 will disconnect the link and let the WAN connection go back to its initial 'state–disconnected'. The scenario is shown in following diagram.



4.1.5.4 6402 Gateway Dial on Demand steps:

Pre-state: After system booting up, the WAN connection is disconnected.

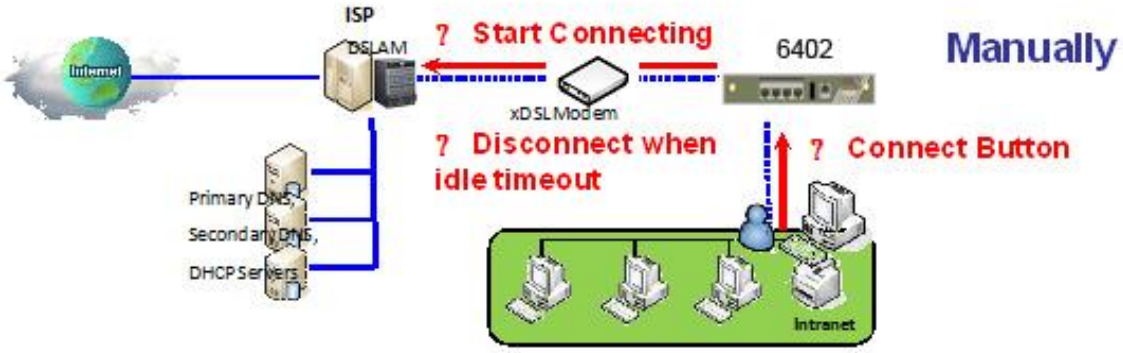
S 1: An Internet access request is fed into the 6402 from the Intranet.

S 2: The 6402 starts to establish the WAN connection until it connects successfully. The 6402 will keep the connection alive only when there still is data transfer to the Internet.

S 3: If the WAN connection times out, the 6402 will disconnect from the Internet and let it go back to Pre-state.

4.1.5.5 6402 Gateway working in Manual Mode

When working in a "Manual" mode, the 6402 will not establish a WAN connection until the administrator clicks on the "Connect" button in the "Network Status" configuration window.
The connection will stay alive only when there is still data to transfer. If there is no data to transfer for a period that is longer than the Maximum Idle Time, the 6402 will disconnect and let the WAN connection go back to its initial state –disconnected. The scenario is shown in following diagram.



4.1.5.6 6402 Manual Connect Scenario

Pre-state: After the 6402 boots up, the WAN connection does not connect.

S 1: It will connect when the administrator clicks on the "Connect" button in the "Network Status" configuration window.

S 2: The 6402 will keep trying to establish a WAN connection until it connects successfully. It keeps the connection alive only while there still is data transfer to the Internet.

S 3: If the WAN connection times out, the 6402 will disconnect and return to its Pre-state.

4.1.4 Network Monitoring

This is the mechanism by which the 6402 determines if a link has failed.
When the Network Monitoring feature is enabled, the router will use either the DNS Query or ICMP Ping to periodically check the Internet connection.

The 6402 Router supports a failover mechanism which depends on the correct decision when a connection goes down. The parameters used are;

Enable: This box allows the 6402 to enable or disable the Network Monitoring feature.

DNS Query / ICMP Checking: either one is used to check alive for a WAN connection.

Loading Checking: The response time of replies to the keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid the keep-alive feature causing problems with the data flow, enabling this option stops the 6402 sending the keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicates how often to send keep-alive packet.

Check Timeout: Set the time period to receive responses to keep-alive packets. If the 6402 doesn't receive a response within this time period, this 6402 will acknowledge this keep alive has failed.

Latency Threshold: Set acceptance for the response time. This 6402 will record the keep-alive check has failed if the response time for the reply packet is longer than this setting.

Fail Threshold: Number for failed packet replies. The 6402 WAN connection will be recognised as failed if the number of continuous failed keep-alive checking equals this value.

Target 1/Target 2: Set the host that is used for the keep alive checks. It can be DNS1, DNS2 or another host. For another you will need to input IP address manually.

Target2 (**None** set by default**)** specifies the second target for sending a DNS query/ICMP request.

None: to disable **Target2.**

DNS1: set the primary DNS to be the target.
DNS2: set the secondary DNS to be the target.

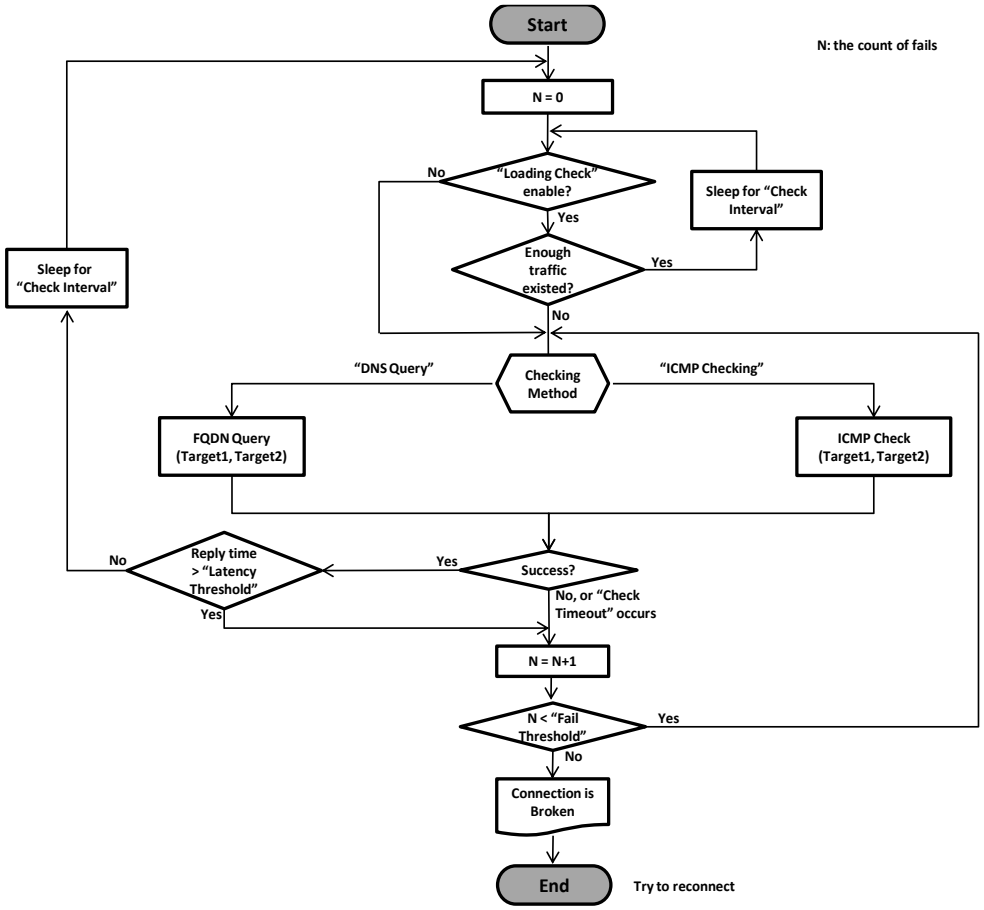
Other Host: enter an IP address to be the target

IGMP – Enable this option to transmit Pings to one of the targets.

WAN IP Alias – Add another address here to ping a different IP Address

The decision flow chart for the keep-alive checks for a WAN connection is shown as below.

Target2 (**None** set by default**)** specifies the second target of sending DNS query/ICMP request.



4.1.5 Load Balancing

Basic Network > WAN & Uplink>Load Balancing

The screen shot below shows the load balancing option page. To enable Load Balancing tick the box which says 'enable'. This allows you to select the following methods of load balancing within the 6402

"By Smart Weight" The 6402 system will operate the load balance function automatically based on the embedded 'Smart Weight' algorithm.

"By Specific Weight" This configuration option will let you define the ratio of transferred sessions between all the 6402 WAN interfaces.

"By User Policy" This option shows all the defined user policy entries, and the "User Policy Configuration" window will let you create and define one user policy for routing dedicated packet flow via one WAN interface.

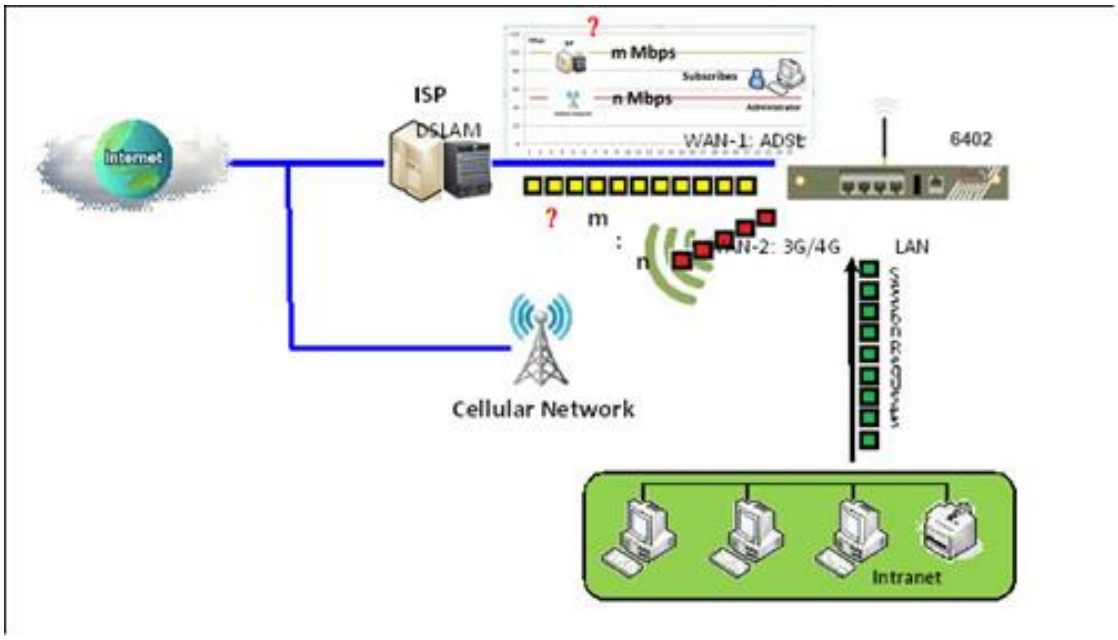
4.1.5.1 Enable/Select Load Balance Strategy

Configuration		
Item	**Value setting**	**Description**
Load Balance	Unchecked by default	Check the **Enable** box to activate Load Balance function.
Load Balance Strategy	**1. Mandatory setting** 2. **By Smart Weight** is selected by default.	There are three load balance strategies: **By Smart Weight**: The 6402 will operate load balance function automatically based on the embedded Smart Weight algorithm. **By Specific Weight**: The 6402 will adjust the ratio of transferred sessions among all WANs based on the specified weights for each WAN. **By User Policy**: The 6402 will route traffic through available WAN interface based on user defined rules.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

4.1.5.2 By Smart Weight Load Balance Strategy

When you select "By Smart Weight" load balancing, the 6402 will load balance automatically without additional parameters, except the available bandwidth (Line Speed) of each WAN interface, which is configured in **[Basic Network]-[WAN & Uplink]-[Physical Interface]** section.
The 6402 decides further routing ratios based on the connection flow to all the WAN interfaces and based on the current traffic flow (in bytes) on all WAN interfaces. The network manager may use this option as quick way to maximise the bandwidth utilisation of multiple WAN interfaces in the 6402.

The 6402 will take the line speed settings of all the WAN interfaces specified in the "Physical Interface" configuration page, as the default ratio among the WAN interfaces for data transfer. Based on the ratio of packet bytes via these WAN interfaces and based on historical data (for example 5 minutes),the 6402 decides how many sessions will be transferred via each WAN interface for current period of traffic loading as shown in the following illustration diagram.



The following table shows the parameter configuration for the above example load balancing diagram. The ratio m:n in this example is 22:11.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2	
Interface Name	WAN-1	WAN-2
Physical Interface	ADSL	3G/4G
Operation Mode	Always on	Always on
Line Speed	2Mbps / 22Mbps	1Mbps / 11Mbps
Load Balance	■ Enable	
Load Balance Strategy	By Smart Weight	

4.1.5.3 The way the Smart Weight algorithm works:

Pre-state: The 6402 takes the line speed settings of all the WAN interfaces as the initial ratio between all WAN interfaces for load balance.

S 1: The 6402 Counts the transferred packet bytes for all WAN interfaces in current time period, for example 5 minutes. At the end of time period, the new transferring ratio for each WAN interface will be changed to the ratio for the counted transferred data among all interfaces for next time period.

S 2: Based on the new ratio that is obtained at S1, the 6402 decides how many sessions will be transferred via each WAN interface for another time period. Loop S1 and S2 steps forever until the network administrator changes the load balance strategy.

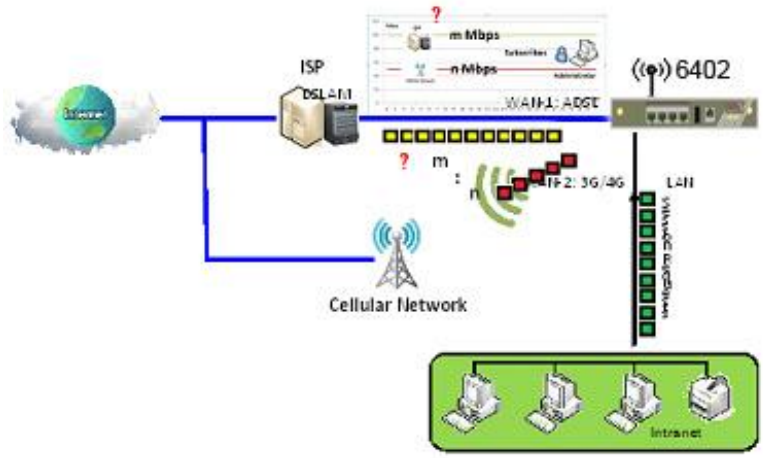
4.1.5.4 Specific Weight Load Balancing

When **By Specific Weight** is selected, the user needs to adjust the percentage of WAN loading. The 6402 will give a value according to the bandwidth ratio of each WAN Interface from the 6402'sinitial boot up and keep the value after clicking **Save** button.

Weight Definition		
WAN ID	Weight	Action
WAN - 1	86 %	Edit
WAN - 2	13 %	Edit

When you select "By Specific Weight" as a load balancing strategy, there is a list of two parameter pairs that are used for the load balancing:

WAN Interface & Weight (%). The line speed of each WAN interface serves as its default weight. This value is the ratio of its line speed to total line speed of all WAN interfaces. The network administrator also can fine tune the weight list based on the default list. The 6402's traffic control process will operate routing based on the dedicated weights on all WAN interfaces.
The following is another example diagram to illustrate the scenario.



At the beginning, the 6402 has two WAN interfaces and their download line speed are an ADSL link at 22Mbps (m Mbps) for WAN-1 interface and 3G/4G ISP11Mbps (n Mbps) for WAN-2. The network manager needs to configure these data rates.

The network manager fills these values in the line speed field for each WAN interface. Please refer to section **[Basic Network]-[WAN & Uplink]-[Physical Interface]**. So, the default routing ratio for both of these interfaces is 2:1 (=22:11) in load balance function as shown in following illustration diagram.

The value of m is 22 and n is 11.

Following table lists the 6402 configuration for the above example diagram for the load balance function. The ration m:n in this example is 22:11.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2	
Interface Name	**WAN-1**	**WAN-2**
Physical Interface	***ADSL***	***3G/4G***
Operation Mode	***Always on***	***Always on***
Line Speed	***2Mbps / 22Mbps***	***1Mbps / 11Mbps***
Load Balance	■ ***Enable***	
Load Balance Strategy	***By Priority***	
WAN ID	**WAN-1**	**WAN-2**
Priority (%)	***67%***	***33%***

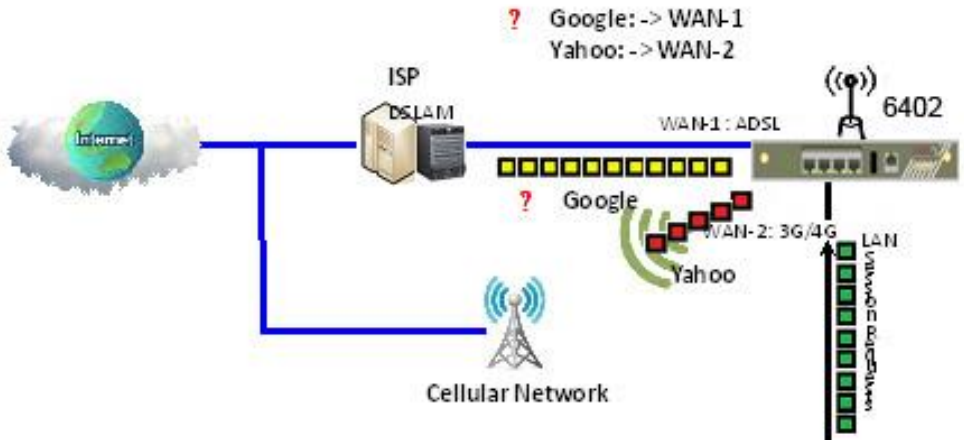
Weight Definition		
Item	**Value setting**	**Description**
WAN ID	NA	The Identifier for each available WAN interface.
Weight	1. Mandatory setting 2. Set with bandwidth ratio of each WAN by default.	Enter the weight ratio for each WAN interface. Initially, the bandwidth ratio of each WAN is set by default. Note: The sum of all weights can't be greater than 100%.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

4.1.5.5 User Policy Load Balancing Strategy

When the network manager selects "By User Policy" for their load balancing strategy, there are two more configuration windows: "User Policy List" and "User Policy Configuration".

When **By User Policy** is selected, a **User Policy List** screen will appear. With properly configured your policy rules, system will route traffic through available WAN interface based on user defined rules

The "User Policy List" shows all your defined user policy entries, and the "User Policy Configuration" window will let you configure one user policy for routing dedicated packet flow via one WAN interface. These are shown in following diagrams.



User Policy List | Add | Delete

ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions
1	Any	www.google.com	All	WAN - 1	☑	Edit ☐ Select
2	Any	www.yahoo.com	All	WAN - 2	☑	Edit ☐ Select

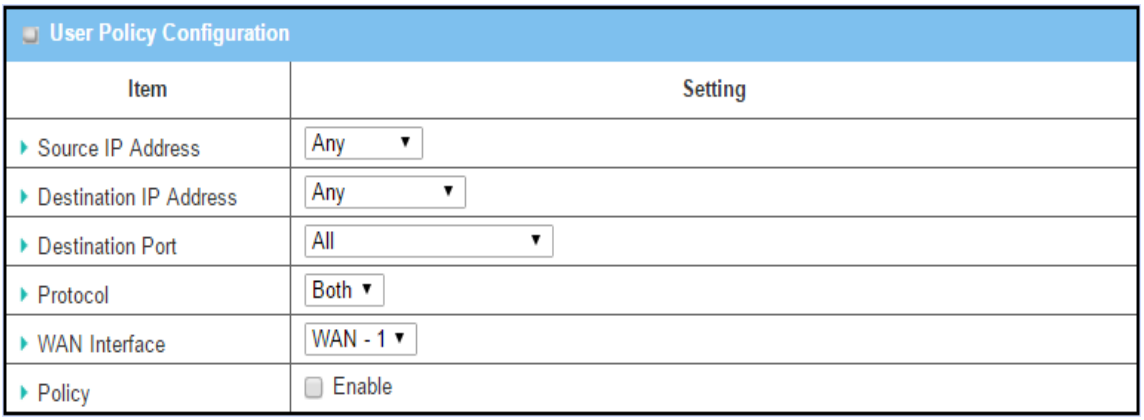
The example above shows that the network administrator hopes the packet flow (whose destination is "www.google.com", "www.yahoo.com") will be transferred via WAN-1, and WAN-2 respectively. Other un-specified packet flows will be routed by default via different WAN interfaces using "Smart Weight" load balance strategy.

To meet the load balance requirement in the above example diagram, the network administrator needs to configure the device based on following configuration table contents.

Configuration Path	[Physical Interface]-[Interface Configuration (WAN-n)] , n=1,2	
Interface Name	WAN-1	WAN-2
Physical Interface	ADSL	3G/4G
Operation Mode	Always on	Always on
Line Speed	2Mbps / 22Mbps	1Mbps / 11Mbps
Configuration Path	[Load Balance]-[Configuration]	
Load Balance	■ Enable	
Load Balance Strategy	By User Policy	
Configuration Path	[Load Balance]-[User Policy Configuration]	
ID	1	2
Source IP Address	Any	Any
Destination IP Address	Domain Name www.google.com	Domain Name www.yahoo.com
Destination Port	All	All
Protocol	Both	Both
WAN Interface	WAN-1	WAN-2
Policy	■ Enable	■ Enable

4.1.5.6 Creating a User Policy

When the ‘Add’ button is applied, User Policy Configuration screen will appear.



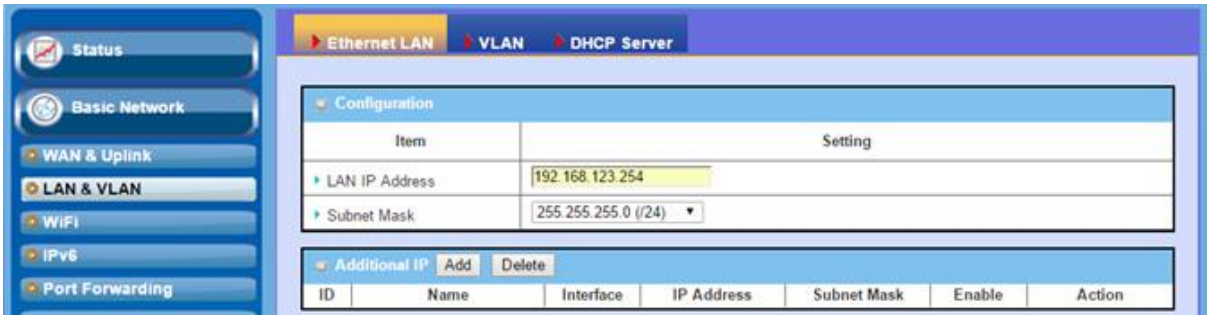
User Policy Configuration		
Item	**Value setting**	**Description**
Source IP Address	1. Mandatory 2. **Any** is selected by default.	There are four options which can be selected: **Any**: No specific Source IP is provided. The traffic may come from any source **Subnet**: Specify the Subnet for the traffics come from the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. **IP Range**: Specify the IP Range for the traffics come from the IPs **Single IP**: Specify a unique IP Address for the traffics come from the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101.
Destination IP Address	1. Mandatory 2. **Any** is selected by default.	There are five options which can be selected: **Any**: No specific destination IP is provided. The traffic may come to any destination. **Subnet**: Specify the Subnet for the traffics come to the subnet. Input format is: xxx.xxx.xxx.xxx/xx e.g. 192.168.123.0/24. **IP Range**: Specify the IP Range for the traffics come to the IPs **Single IP**: Specify a unique IP Address for the traffics come to the IP. Input format is: xxx.xxx.xxx.xxx e.g. 192.168.123.101. **Domain Name**: Specify the domain name for the traffics come to the domain
Destination Port	1. Mandatory **2.All** is selected by default.	There are four options which can be selected: **All**: No specific destination port is provided. **Port Range**: Specify the Destination Port Range for the traffics **3. Single Port**: Specify a unique destination Port for the traffics **4. Well-known Applications**: Select the service port of well-known application defined in dropdown list.
Protocol	1. Mandatory 2. **Both** is selected by default.	There are three options can be selected. They are **Both**, **TCP**, and **UDP**.
WAN Interface	1. Mandatory 2. **WAN-1** is selected by default.	The user can select the interface that traffic should go. **Note** that the WAN interface dropdown list will only show the available WAN interfaces.
Policy	Unchecked by default	Check the **Enable** checkbox to activate the policy rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

4.2. LAN and VLAN

4.2.1. Ethernet LAN

4.2.1.1 Configuration

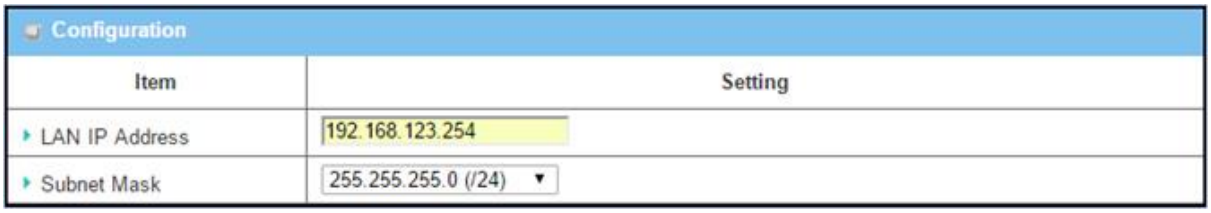
This section provides a brief description of the LAN and VLAN's (Virtual LANS)on the 6402, and also explains how to create and modify them.

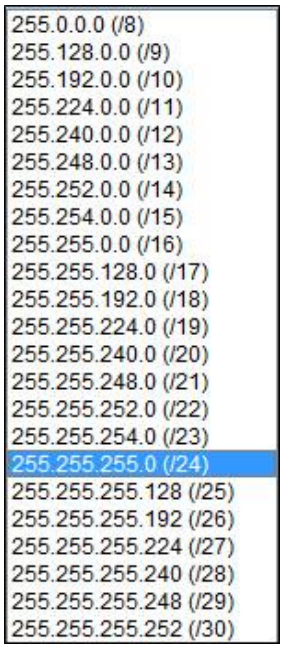


The Local Area Network (LAN) can be used to share data or files among computers attached to a network. Following diagram illustrates the network that wired and interconnects computers.

4.2.1.2 LAN IP Address Configuration

LAN IP Address: The computer on your network must use the same subnet as the 6402 to access the 6402 management; however, it's also possible to change the 6402 IP address. If you change the 6402 IP Address, you need to change your PC's IP Address to be on the same subnet as the 6402 LAN Port and type new 6402IP address in the browser to logon again.





Subnet Mask: Input your Subnet mask. The subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 x IP addresses are allowed in this subnet. However, one of them is occupied by the 6402 IP, so there are maximum 253 clients allowed on LAN network, the last IP Address is allocated to the Broadcast address.

The table to the left shows the subnet masks in the old and newer formats.

4.2.1.3 Additional IP Addresses

Select this option to add more IP Addresses.

4.2.2 6402 VLAN (Virtual Local Area Network)

Introduction - Basic Network > LAN & VLAN > VLAN Tab

A VLAN is a logical network which allows a switch or router to group client hosts on the same physical hardware but segment them into virtual networks with specific VLAN ID's. The 6402 supports both Port-based VLAN and Tag-based VLANs.

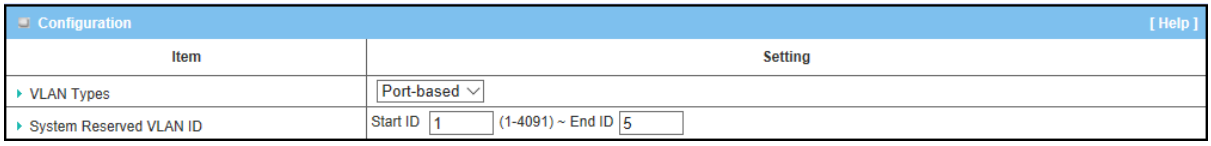
In Port-based VLANs – Where devices are on the same physical interface, all client hosts belonging to the same group are allowed to transfer data and are tagged with same VLAN ID within the 6402. However, they cannot communicate with devices on other ports that are not members of the port based VLAN.

In Tag-based VLAN's – In Tag based VLANS devices can be connected via different physical ports, however if they have the same VLAN ID's they will be treated as belonging to the same group with the same access property and QoS properties. It is especially useful when individuals of a VLAN group are located in different locations.

The VLAN function allows you to divide local networks into different "virtual LANs". In some cases, ISP's may need routers to support "VLAN Tag's" for certain kinds of services (e.g. IPTV) to work properly.

4.2.2.1 Configuration

The configuration screen shown below, allows the network manager to select whether a Port or Tag Based VLAN is used.

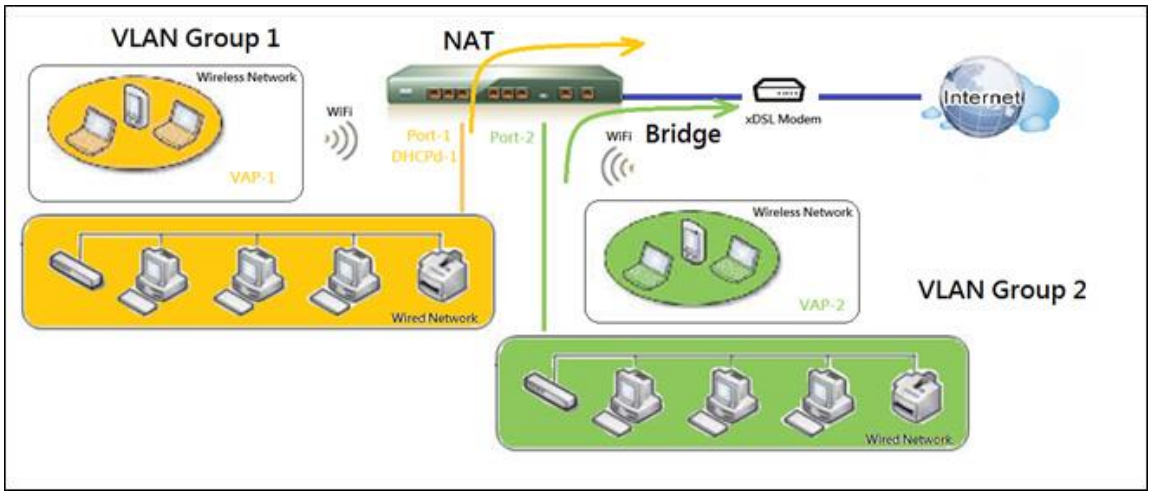


Configuration		
Item	**Value setting**	**Description**
VLAN Type	**Port-based** is selected by default	Select the VLAN type that you want to adopt for organizing your local subnets. **Port-based**: Port-based VLAN allows you to add a rule for each LAN port, and you can configure advanced control with its VLAN ID. **Tag-based**: Tag-based VLAN allows you to add a VLAN ID, and select member and DHCP Server for this VLAN ID. Go to **Tag based VLAN List** table.
System Reserved VLAN-ID	Default: Start -1 End -5	The VLANS reserved for management and system operations on the 6402
Save	NA	Click the **Save** button to save the configuration

All client hosts in the same department should have common access and QoS properties. You can select the operating mode, as either port-based VLAN or tag-based VLAN, and then configure according to your network configuration.
We have listed some common VLAN scenarios for the 6402 below.

4.2.2.2 Port-based VLANs

Port-based VLAN's can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP etc. Two operating modes, NAT and Bridge, can be applied to each VLAN group.

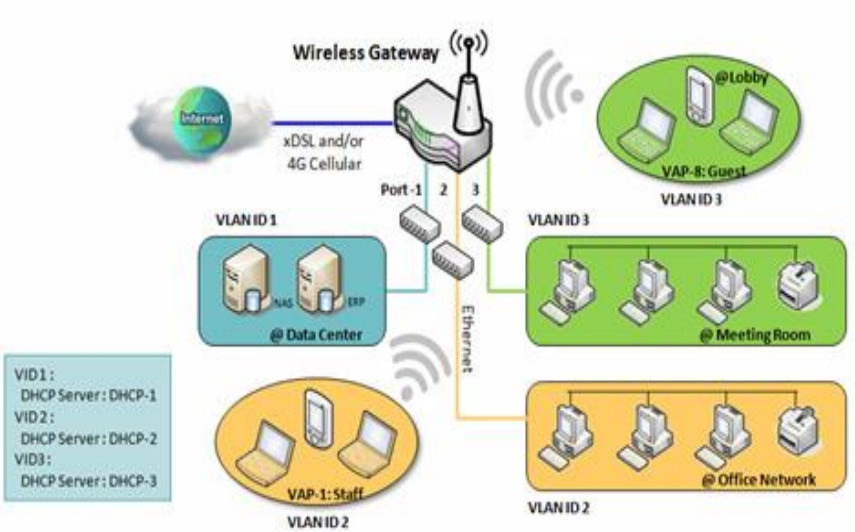


One DHCP server can be allocated for a NAT VLAN group to let a group host member to get its IP address.

A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless 6402's that form a logical LAN segment. The following is an example, where in a company, there could be 3 network segments,

- **Lobby/Meeting Room.**
- **Office.**
- **Data Centre.**

In the example below, the 6402 runs a Wireless network; the network manager configures a Lobby/Meeting Room segment with VLAN ID 3.
The VLAN group includes Port-3 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. The network administrator also configures the Office segment with VLAN ID 2.
The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode and DHCP-2 server equipped.
The network manager also configures the Data Centre segment with VLAN ID 1. The VLAN group includes Port-1 with NAT mode to WAN interface as shown in following diagram.

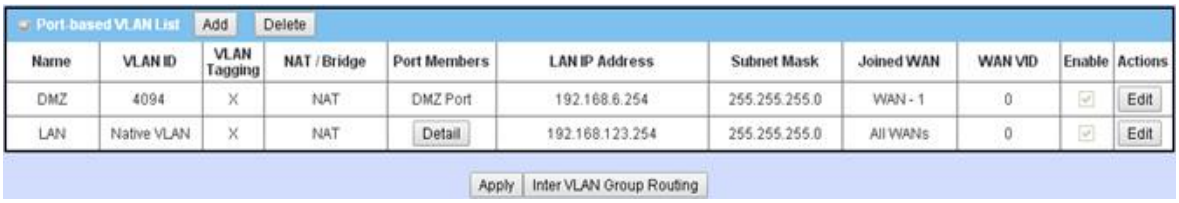


The example above is for 3 Ethernet LAN ports on the 6402. If we were just using one Ethernet port on the 6402 there will be only one VLAN group for the 6402. In this configuration, the 6402 still supports both NAT and Bridge mode for the Port-based VLAN configuration.

4.2.2.3 Port-based VLAN List

Basic Network>LAN & VLAN> Port Based VLAN List

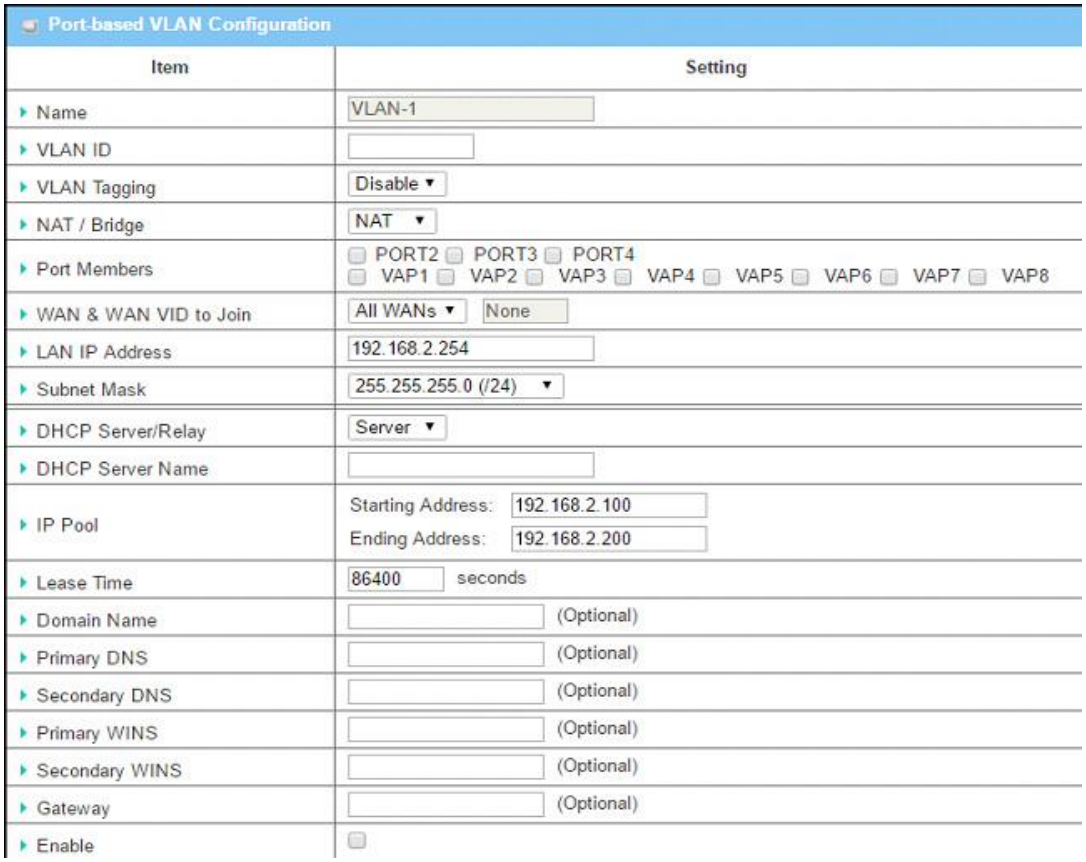
The port-based VLAN list allows you to customize each LAN port. There is a default rule that shows the configuration of all the 6402 LAN ports. If your device has a DMZ port, you will see the DMZ configuration as well. The maximum rule numbers are based on LAN port numbers.



When the 'Add' button is applied, the Port-based VLAN Configuration screen will appear, which includes 3 sections:

- Port-based VLAN Configuration,
- IP Fixed Mapping Rule List,
- Inter VLAN Group Routing (enter through a button)

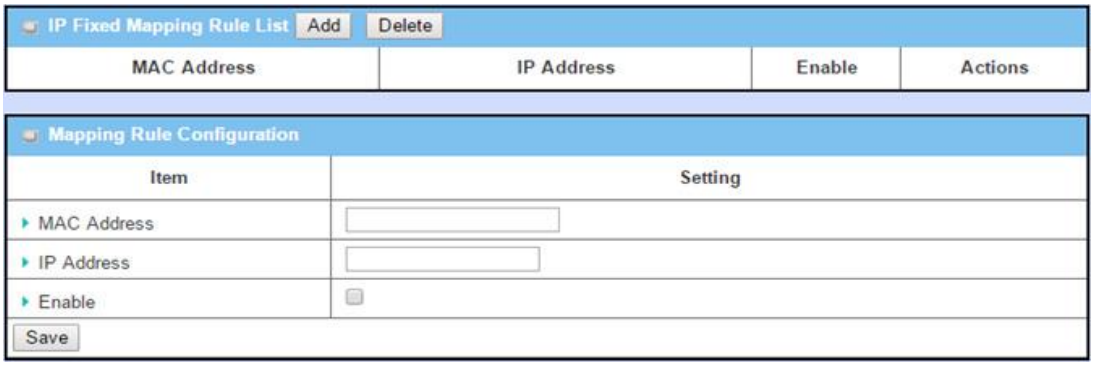
4.2.2.4 Port-based VLAN – Configuration



Port-based VLAN Configuration		
Item	**Value setting**	**Description**
Name	1. Mandatory 2. String format: already have default texts	Define the **Name** of this rule. This has a default text and cannot be modified.
VLAN ID	Mandatory	Define the VLAN ID number, range is 1~4094.
VLAN Tagging	**Disable** is selected by default.	The rule is activated according to **VLAN ID** and **Port Members** configuration when **Enable** is selected. The rule is activated according **Port Members** configuration when **Disable** is selected.
NAT / Bridge	**NAT** is selected by default.	Select **NAT** mode or **Bridge** mode for the rule.
Port Members	These box is unchecked by default.	Select which LAN port(s) and VAP(s) that you want to add to the rule. Note: The available member list can be different for the purchased product.
WAN & WAN VID to Join	**All WANs** is selected by default.	Select which **WAN** or **All WANs** that allow accessing Internet. Note: If Bridge mode is selected, you need to select a WAN and enter a VID.
LAN IP Address	Mandatory	Assign an **IP Address** for the DHCP Server that the rule used, this IP address is a 6402 IP.
Subnet Mask	**255.255.255.0(/24)** is selected by default.	Select a **Subnet Mask** for the DHCP Server.
DHCP Server /Relay	**Server** is selected by default.	Define the **DHCP Server** type. There are three types which can be selected: **Server**, **Relay**, and **Disable**. **Relay**: Select **Relay** to enable the DHCP Relay function for the VLAN group, and you only need to configure the **DHCP Server IP Address** field. **Server**: Select **Server** to enable the DHCP Server function for the VLAN group, you then need to configure the DHCP Server settings. **Disable**: Select **Disable** to disable the DHCP Server function for the VLAN group.
DHCP Server IP Address (for DHCP **Relay** only)	Mandatory	If you select **Relay** for the DHCP Server, assign a **DHCP Server IP Address** that the 6402 will relay the DHCP requests to the assigned DHCP server.
DHCP Server Name	Mandatory	Define name of the DHCP Server.
IP Pool	Mandatory	Define the IP Pool range. These are the **Starting Address** and **Ending Address** fields. If a client requests an IP address from this DHCP Server, it will assign an IP address within the range of the **IP pool**.
Lease Time	Mandatory	Define a period of time for an IP Address that the DHCP Server leases to a new device. By default, the **lease time** is 86400 seconds.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.
Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
6402	IPv4 format	The 6402 of this DHCP Server.
Enable	Unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting.

4.2.2.5 IP Fixed Mapping Rule

It's also possible to add IP rules in the **IP Fixed Mapping Rule List** if a DHCP Server for the VLAN groups is required.

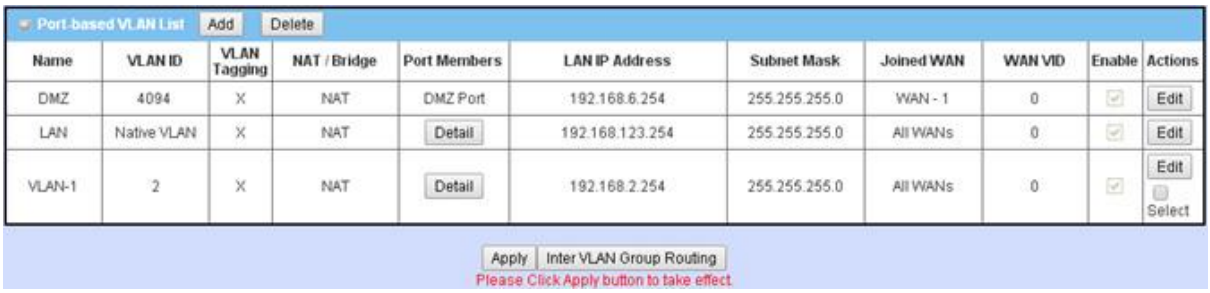


When the **Add** button is applied, the **Mapping Rule Configuration** screen will appear.

4.2.2.6 Mapping Rule Configuration

Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	A Mandatory setting	Define the **MAC Address** target that the DHCP Server wants to match.
IP Address	A Mandatory setting	Define the **IP Address** that the DHCP Server will assign. If there is a request from the MAC Address filled in the above field, the DHCP Server will assign this **IP Address** to the client whose **MAC Address** matched the rule.
Enable	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration

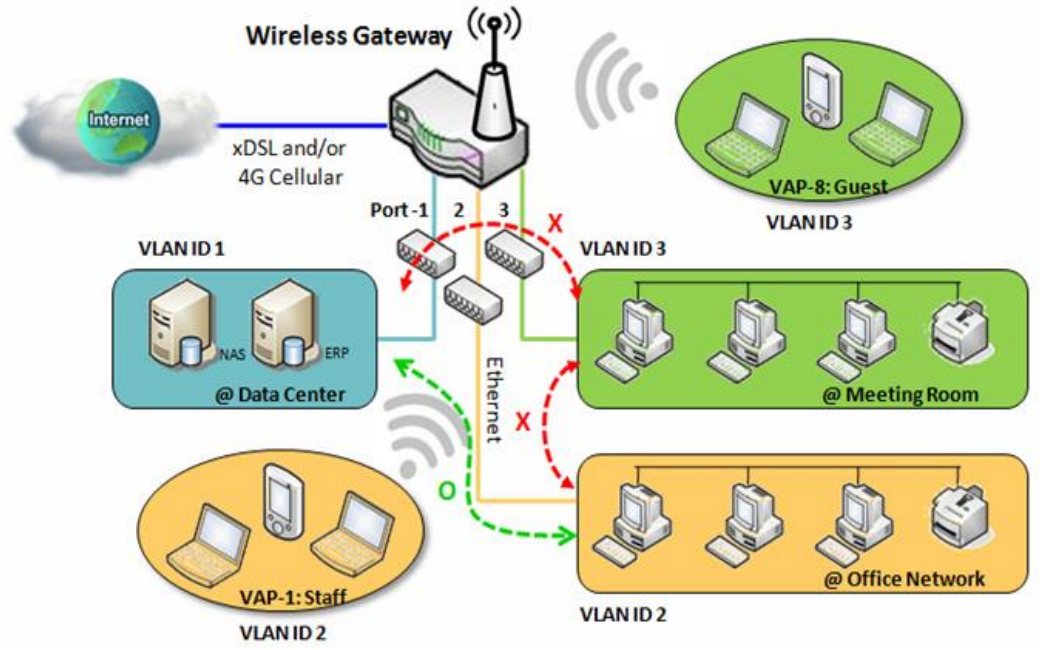
Note: Always click on the **Apply** button to apply the changes after the web browser has been refreshed it will take you back to the VLAN page.



4.2.2.7 Inter VLAN Group Routing:

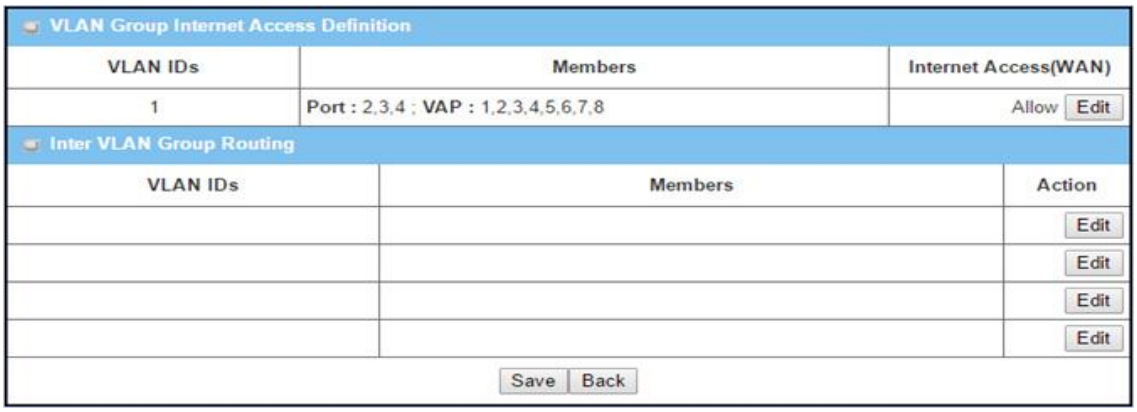
In a Port-based tagged configuration, the network manager can specify member hosts of one VLAN group to be able to communicate with the members of another VLAN group or they can configure them to be blocked. This allows device pairing, and one VLAN group can join many communication pairs. But communication pairs don't have the ability to communicate with VLANS that are not in the same pair.

In the example below 'A' can communicate with 'B', and 'B' can communicate with 'C', 'A' cannot communicate with 'C'. VLAN groups VID 1 and 2 can access each other but between VID 1 and VID 3 and between VID 2 and VID 3 can't access each other.

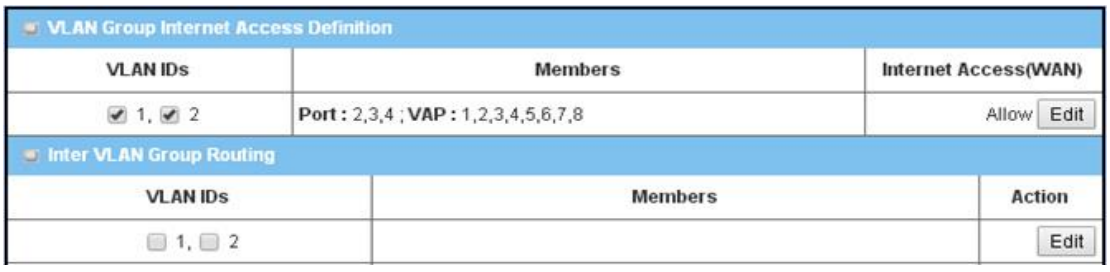


4.2.2.8 Port-based VLAN – Inter VLAN Group Routing

Click **VLAN Group Routing** button, the **VLAN Group Internet Access Definition** and **Inter VLAN Group Routing** screen will appear.



When the **Edit** button is applied, a screen similar to this will appear:



Inter VLAN Group Routing		
Item	**Value setting**	**Description**
VLAN Group Internet Access Definition	All boxes are checked by default.	By default, all boxes are checked , which means all **VLAN ID** members are allowed to access WAN interface. If a **VLAN ID is** unchecked, it means the VLAN ID member can't access Internet. **Note: VLAN ID 1** is always available; it is the default VLAN ID. The other **VLAN IDs** are available only when they are enabled.
Inter VLAN Group Routing	The box is unchecked by default.	Click the required **VLAN IDs** box to enable the Inter VLAN access function. By default, members in different **VLAN IDs** can't access each other. The 6402 supports up to 4 rules for **Inter VLAN Group Routing.** For example, if ID_1 and ID_2 are checked, it means members in VLAN ID_1 can access members of VLAN ID_2, and vice versa.
Save	N/A	Click the **Save** button to save the configuration

4.2.2.9 Tag-Based VLAN's

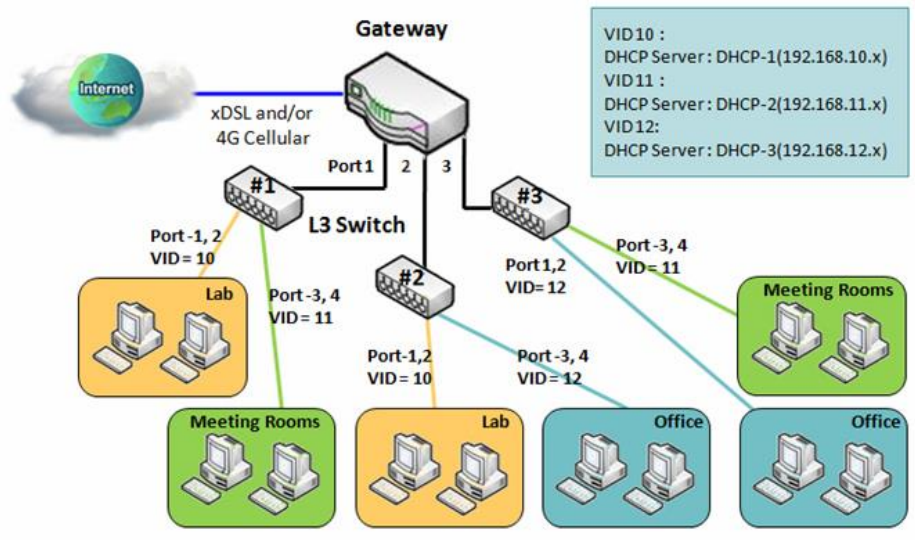
A Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and Wi-Fi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying subnets in the Intranet. All packet flows can carry different VLAN tags even on the same physical Ethernet port of the local subnet. These flows can be directed to different destinations because they have different tags. This option is very useful to group some hosts in different geographic location allowing them to be in the same workgroup.

Tag-based VLAN's are also called VLAN Trunks. A VLAN Trunk collects all packet flows with different VLAN IDs from the 6402 and delivers them over the local Intranet. VLAN membership in a tagged VLAN is determined by the VLAN ID information within the packets that are received on a port. The network administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID.

For example, in a company, the network manager configures 3 network segments,

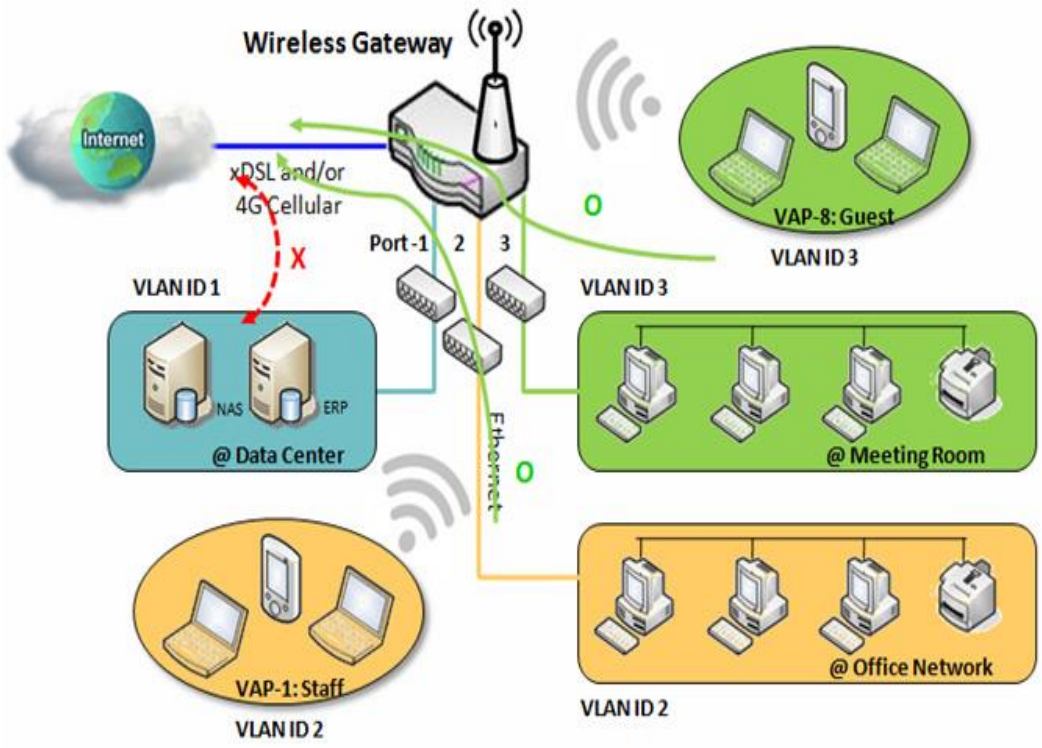
- **Lab.**
- **Meeting Rooms.**
- **Office.**

The 6402 network manager can configure the Office segment with VLAN ID 12.
The VLAN group is equipped with a DHCP-3 server to construct a 192.168.12.x subnet.
The 6402 manager has also configured the Meeting Rooms segment with VLAN ID 11.
The VLAN group is equipped with DHCP-2 server to apply a 192.168.11.x for the local subnet only. Any client host in VLAN 11 group can't access the Internet.
Finally, the network manager configures the Lab segment with VLAN ID 10. The VLAN group is equipped with theDHCP-1 server to construct a 192.168.10.x subnet.



4.2.2.10 VLAN Group Internet Access

The network manager can specify members of one VLAN group to be able to access the Internet or not. The following is an example that shows VLAN groups 2 and 3 can access Internet but VLAN ID 1 cannot access the Internet. This allows visitors in meeting room and staff in the office network to access the Internet. However, the computers/servers in the data centre cannot access the Internet. The servers in the data centre are only for trusted staff or are accessed via secure tunnels.



4.2.2.11 Tag-based VLAN List – Create/Edit VLAN Rules

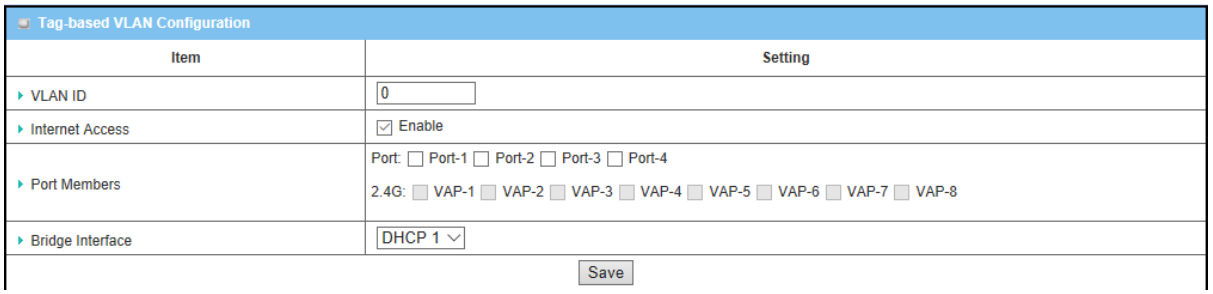
Tag-based VLAN's allows you to customise each LAN port according to its VLAN ID.
This allows multiple devices to share one physical subnet but to be members of different VLANS.
There is a default rule which shows the configuration of all LAN ports and all VAPs.
If your 6402 has a DMZ port, you will see the DMZ configuration.
The 6402 router supports up to a maximum of 128 tag-based VLAN rule sets.

Tag-based VLAN List | Add | Delete

VLAN ID	Internet	Port Members	Bridge Interface	IP Address	Subnet Mask	Actions
Native VLAN	☑	Port: ☑ Port-1 ☑ Port-2 ☑ Port-3 ☑ Port-4 2.4G: ☑ VAP-1 ☑ VAP-2 ☑ VAP-3 ☑ VAP-4 ☑ VAP-5 ☑ VAP-6 ☑ VAP-7 ☑ VAP-8	DHCP 1			Edit ☐ Select

4.2.2.12 Tag Based VLAN Configuration

When the Add button is applied, the Tag-based VLAN configuration screen will appear.



Tag-based VLAN Configuration		
Item	**Value setting**	**Description**
VLAN ID	A Mandatory setting	Define the **VLAN ID** number, range is 6~4094.
Internet Access	The box is checked by default.	Click the **Enable** box to allow the members in the VLAN group to access to internet.
Port Members	These boxes are unchecked by default.	Check the LAN port box(es) and/or Wi-Fi VAP box(es) to join the VLAN group.
Bridge Interface	**DHCP 1** is selected by default.	Select a **DHCP Server** to these members of this VLAN group. To create or edit DHCP server for VLAN, refer **to Basic Network > LAN & VLAN > DHCP Server**.
Save	N/A	Click **Save** button to save the configuration Note: After clicking **Save** button, always click **Apply** button to apply the settings.

4.2.3 6402DHCP Server

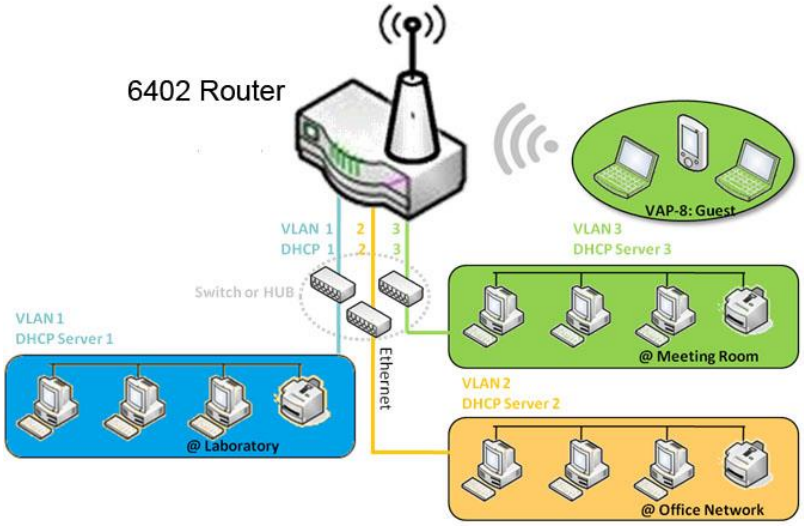
Introduction

The 6402 supports up to 4 DHCP servers to support DHCP requests from different VLAN groups (please refer to VLAN section for getting more usage details).

There is one default setting for those LAN IP Address on the same subnet as the6402 LAN interface. The default IP Pool range is set from “100” to “200” and the default Subnet Mask setting set to “255.255.255.0”. This as shown in the DHCP Server List page on the 6402.

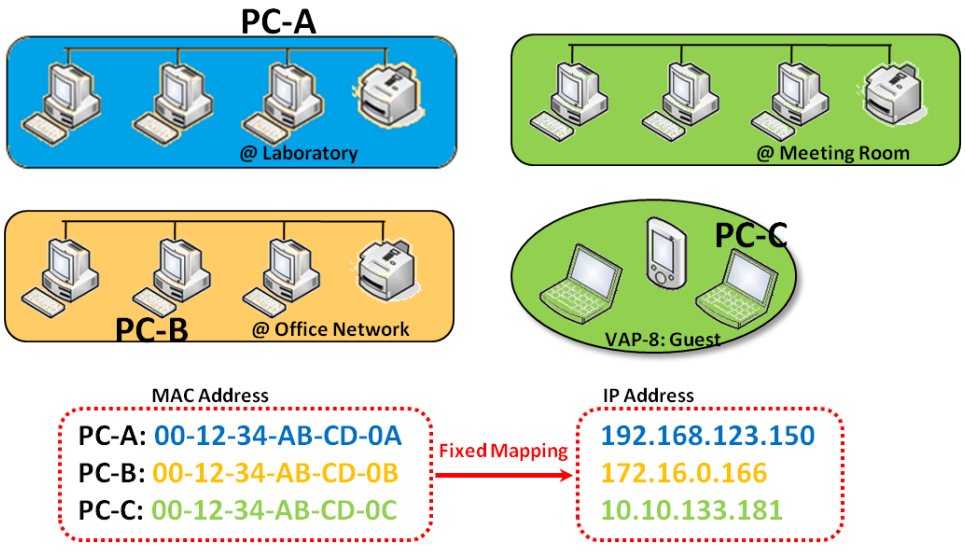
The network manager can add more DHCP server configurations by clicking on the “Add” button behind the “DHCP Server List”, or by clicking on the “Edit” button at the end of each DHCP Server list to edit its current settings.

The network manager can select a DHCP Server and delete it by clicking “Select” and the “Delete” button.



4.2.3.1. Fixed Mapping

The network manager can assign a fixed IP address to a specific client MAC address by selecting them and copying, the targets which already existed in the ***DHCP Client List***, or to add other Mapping Rules manually in advance.



4.2.3.2. DHCP Server List

The DHCP Server list allows user to create and customise DHCP Server policies to assign IP Addresses to the devices on the local area network (LAN).

Basic Network >LAN & VLAN> DHCP Server List

The 6402 allows you to customize your DHCP Server Policy. It supports up to a maximum of 4 policy sets.

DHCP Server List | Add | Delete | DHCP Client List | [Help]

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Enable	Actions
DHCP 1	192.168.1.254	255.255.255.0	192.168.1.100-192.168.1.200	900		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☑	Edit / Fixed Mapping

4.2.3.3. DHCP Server Configuration

Basic Network > LAN + VLAN > DHCP Server > DHCP Server List > Add

When the Add button is applied, the DHCP Server Configuration screen will appear.

DHCP Server Configuration

Item	Setting
DHCP Server Name	DHCP 2
LAN IP Address	192.168.2.254
Subnet Mask	255.0.0.0 (/8)
IP Pool	Starting Address: Ending Address:
Lease Time	86400 seconds
Domain Name	(Optional)
Primary DNS	(Optional)
Secondary DNS	(Optional)
Primary WINS	(Optional)
Secondary WINS	(Optional)
Gateway	(Optional)
Server	Enable

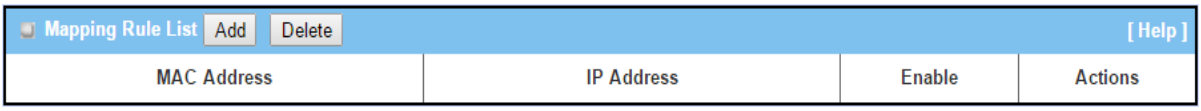
DHCP Server Configuration		
Item	**Value setting**	**Description**
DHCP Server Name	1. String format can be any text 2. A Mandatory setting	Enter a DHCP Server name. Enter a name that is easy for you to understand.
LAN IP Address	1. IPv4 format. 2. A Mandatory setting	The LAN IP Address of this DHCP Server.
Subnet Mask	255.0.0.0 (/8) is set by default	The Subnet Mask of this DHCP Server.
IP Pool	1. IPv4 format. 2. A Mandatory setting	The IP Pool of the DHCP Server. Its composed of a Starting Address entered in this field and Ending Address also entered in this field.
Lease Time	1. Numeric string format. 2. A Must filled setting	The Lease Time of this DHCP Server.
Domain Name	String format can be any text	The Domain Name of this DHCP Server.
Primary DNS	IPv4 format	The Primary DNS of this DHCP Server.
Secondary DNS	IPv4 format	The Secondary DNS of this DHCP Server.
Primary WINS	IPv4 format	The Primary WINS of this DHCP Server.

Secondary WINS	IPv4 format	The Secondary WINS of this DHCP Server.
6402	IPv4 format	The 6402 address of this DHCP Server.
Server	The box is unchecked by default.	Click **Enable** box to activate this DHCP Server.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	NA	When the **Back** button is clicked the screen will return to the DHCP Server Configuration page.

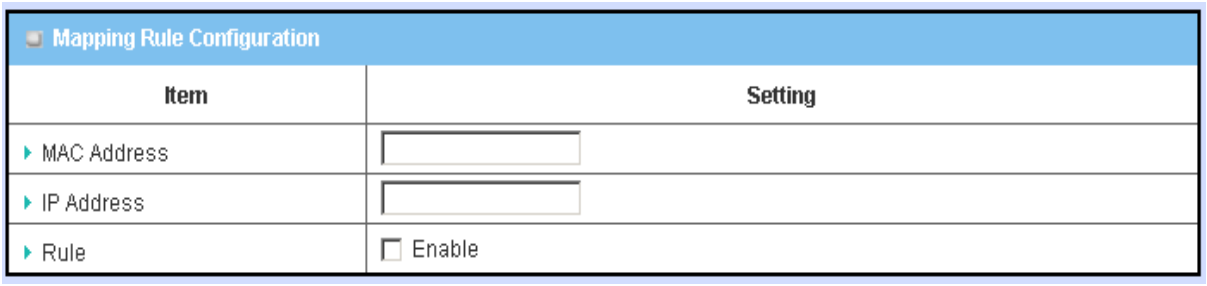
4.2.3.4. Create/Edit Mapping Rule List on DHCP Server

Basic Network > LAN + VLAN > DHCP Server > DHCP Server List > Fixed Mapping

The 6402 allows you to custom your Mapping Rule List on the DHCP Server. It supports up to a maximum of 64 rule sets. When the **Fix Mapping** button is applied, the **Mapping Rule List** screen will appear.



Basic Network > LAN + VLAN > DHCP Server > DHCP Server List > Fixed mapping > Add



Mapping Rule Configuration		
Item	**Value setting**	**Description**
MAC Address	1. MAC Address string format 2. A Mandatory setting	The MAC Address for this mapping rule.
IP Address	1. IPv4 format. 2. A Mandatory setting	The IP Address of this mapping rule.
Enabling the Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	N/A	When the **Back** button is clicked the screen will return to the **DHCP Server Configuration** page.

4.2.3.5. View/Copy DHCP Client List

Basic Network > LAN + VLAN > DHCP Server > DHCP Server List > DHCP Client List

When the DHCP Client List button is applied, the following DHCP Client List screen will appear.

DHCP Client List | Copy to Fixed Mapping

LAN Interface	IP Address	Host Name	MAC Address	Remaining Lease Time	Actions
Ethernet	Dynamic / 192.168.1.100	James-P45V	74:D0:2B:62:8D:42	00:10:37	Select

When the DHCP Client is selected and the 'Copy to Fixed Mapping' button is applied. The IP and MAC address of DHCP Client will be applied to the Mapping Rule List on the specified DHCP Server automatically.

4.2.3.6. DHCP Option List

Basic Network > LAN + VLAN > DHCP Server > DHCP Server Option List > Add

The DHCP Server Options setting allows a user to set DHCP OPTIONS 66, 72, or 114.

Click the Enable button to activate the DHCP option function, the DHCP Server will add the expected options and send out the DHCPOFFERDHCPACK packages.

Option	Meaning	RFC
66	TFTP server name	[RFC 2132]
72	Default World Wide Web Server	[RFC 2132]
114	URL	[RFC 3679]

4.2.3.7. Enabling the DHCP Server options

Click the 'enable' box to enable the DHCP Server option.

Configuration

Item	Setting
DHCP Server Options	Enable

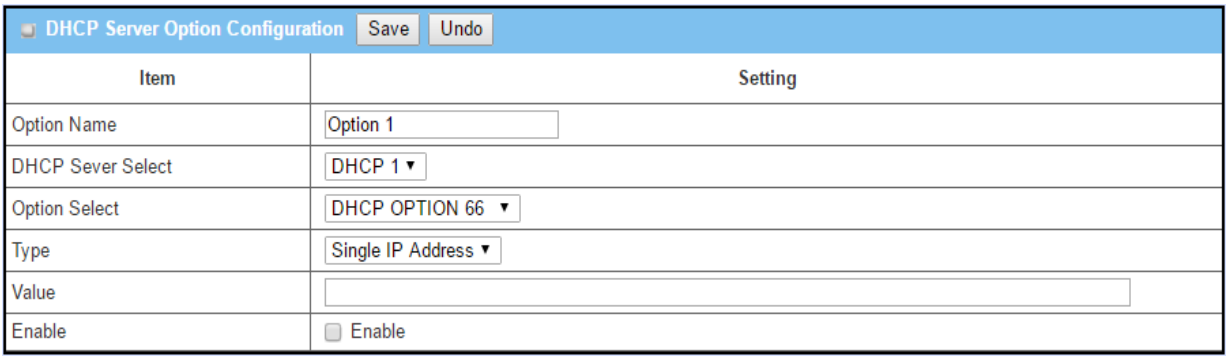
4.2.3.8. Create/Edit DHCP Server Options

The router supports up to a maximum of 99 option settings.

DHCP Server Option List | Add | Delete

ID	Option Name	DHCP Sever Select	Option Select	Type	Value	Enable	Actions

When the Add/Edit button is applied, DHCP Server Option Configuration screen will appear.



DHCP Option meanings

(**DHCP Option 66** gives the IP address or the hostname of a single TFTP server)

(**DHCP Option 72**gives the IP address of WEB Servers)

(**DHCP Option** 114 can be used to configure the URL of the provisioning server in Gigaset IP phones)

DHCP Server Option Configuration				
Item	**Value setting**	**Description**		
Option Name	1. String format can be any text 2. A Mandatory Setting	Enter a DHCP Server Option name. Enter a name that is easy for you to understand.		
DHCP Server Select	Dropdown list of all available DHCP servers.	Choose the DHCP server this option should apply to.		
Option Select	Dropdown list 66 - tftp 72 – www 114 - url	Choose the specific option you want to set.		
Type	Dropdown list of DHCP server option value's type	Each different option has different value types.		
		66	Single IP Address	
			Single FQDN	
		72	IP Addresses List, separated by ","	
		114	Single URL	
Value	1. IPv4 format 2. FQDN format 3. IP list 4. URL format 5. A Must filled setting	Should conform to Type :		
			Type	Value
		66	Single IP Address	IPv4 format
			Single FQDN	FQDN format
		72	IP Addresses List, separated by ","	IPv4 format, separated by ","
		114	Single URL	URL format
Enable	The box is unchecked by default.	Click **Enable** box to activate this setting.		
Save	*NA*	Click the **Save** button to save the setting.		
Undo	*NA*	When the **Undo** button is clicked the screen will return back with nothing changed.		

4.3 Wi-Fi

4.3.1. Introduction

The 6402can be used to provide a Wi-Fi interface for mobile devices or other devices wishing to connect to the network. The Wi-Fi system in the 6402 complies with the802.11ac/11n/11g/11b standard in 2.4GHz single band.

There are three wireless operation modes provided by the 6402. They are:

- **AP Router Mode**
- **WDS Only Mode**
- **WDS Hybrid Mode**

The network manager can select the mode from the wireless operation mode list.

In the first Wi-Fi Configuration section, it's necessary to complete most of the settings for using the Wi-Fi function, including the operation mode, optional VAP settings, Channel, Wi-Fi System, Authentication & Encryption key, and Station / VAP isolation settings.

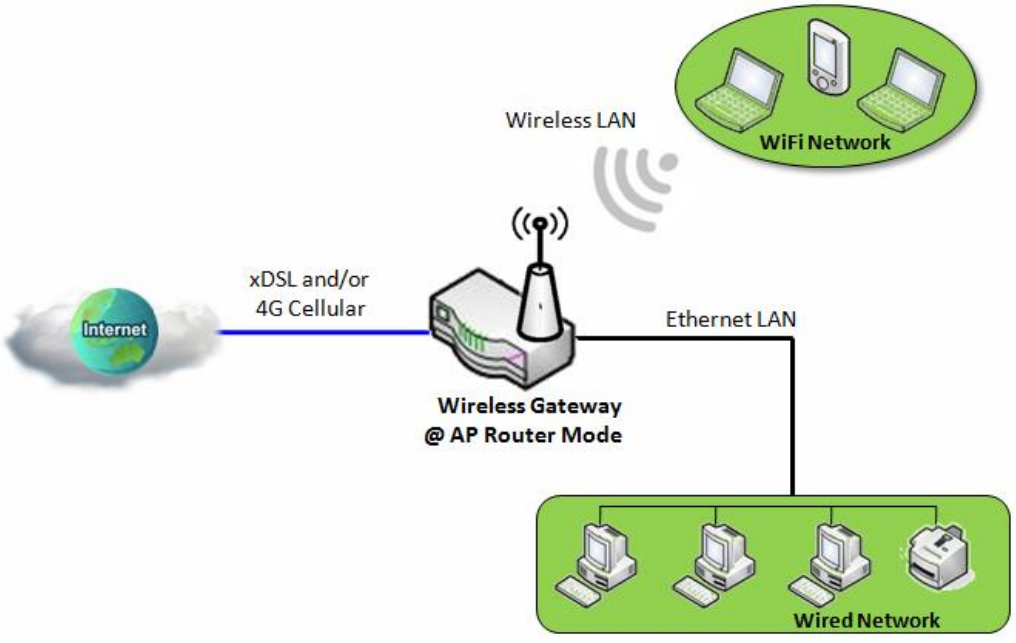
- **The Wireless Client List section provides a quick view of the connected wireless clients.**
- **The Advanced Configuration section provides more parameters for advanced user to fine tune the connectivity performance.**
- **There is also a subsection, called 'Uplink Profile', for some special models that provide Wi-Fi uplink function.**

The following is the scenarios for each wireless operation mode;

4.3.1.1. Access Point (AP)Router Mode

This mode allows you to connect your wired and wireless devices to create a subnet via the 6402 and provide access to the Internet using the 6402 NAT mechanism. In this mode the 6402 is working as a Wi-Fi AP, but also a Wi-Fi hotspot. It means local Wi-Fi clients can connect and go to the Internet. With its NAT mechanism, all the wireless clients don't need to get public IP addresses from ISP.

The following diagram illustrates the wireless 6402 that is running at AP Router operation mode.



4.3.1.2. WDS Only Mode & WDS Hybrid Mode

The WDS (Wireless Distributed System) Only mode, allows the 6402 to act as a wireless/ Wi-Fi repeater for its wired Intranet.

In WDS Hybrid mode the 6402 acts as an access point for its Wi-Fi Intranet and a Wi-Fi repeater for its Wi-Fi Intranets at the same time. Users can thus use the features to build up a large wireless network in large spaces like airports, hotels and schools …etc.

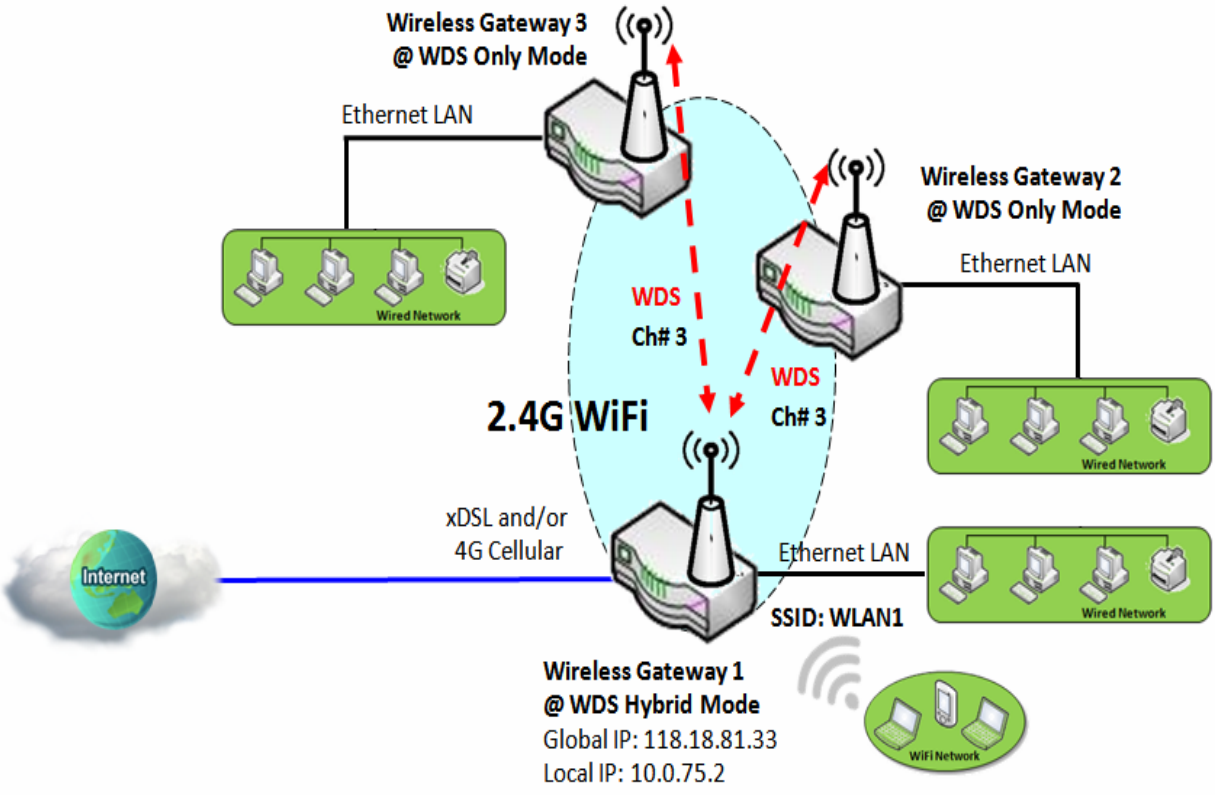
Acting as wireless bridges, multiple wireless 6402s running in "WDS Only" or in "WDS Hybrid" mode link together so that they can communicate with each other through wireless interface (with WDS). Thus, all client hosts in their wired Intranets and Wi-Fi Intranets can also communicate each other in the scenario.

The following diagram illustrates that there are two remote wireless 6402s running in "WDS Only" operation mode. They both use channel 3 to link to the local Wireless 6402, the local 6402 is running in "WDS Hybrid" mode and has an Internet connection.

The wired Intranets can thus access the Internet through 6402 Wireless Gateway 1 since these three wireless 6402s have been linked together using WDS.

Note that the 6402s running in "WDS Only" mode will disable any DHCP server by default, so the client hosts under the 6402s will request their IP address from the 6402 Wireless Gateway 1 that has at least one DHCP server working. 6402 Wireless Gateway 1 also executes the NAT mechanism for Internet access.

In "WDS Only" mode the 6402 provides a Wi-Fi bridge to other 6402s without the embedded the DHCP server and NAT. However, the 6402 Wireless Gateway 1 operating in "WDS Hybrid" mode joins in a WDS link network and provides DHCP servers for assigning IP Addresses and executes the NAT function for Internet access.



4.3.1.3. APOnly Mode

An Access Point uses an uplink Ethernet interface to link to an external 6402 and uses the Wi-Fi interface to serve as an access point for the "Wi-Fi Network" behind it.

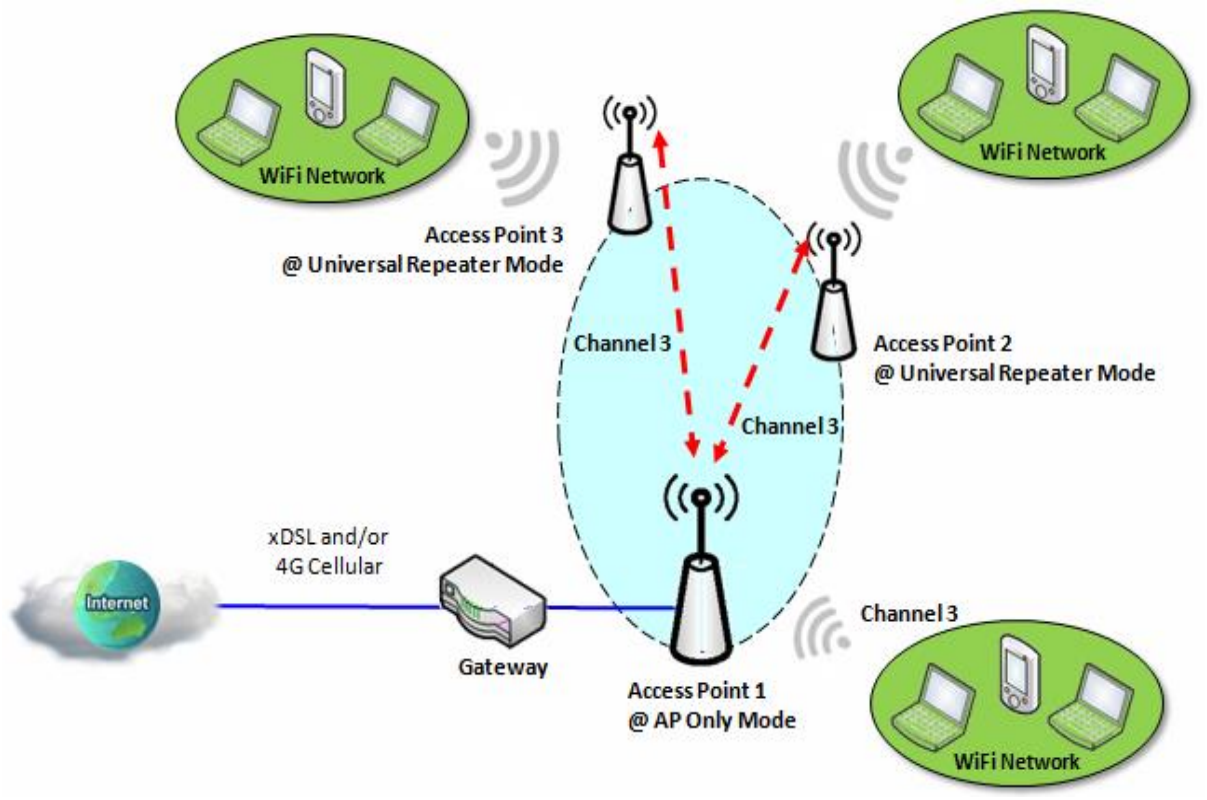
It also can accept association and linking requests from remote access points so that Wi-Fi networks in the vicinity of the 6402can link to the local access point through the Wi-Fi connection, using the same SSID. The local access point is running in "AP Only" mode.

The following diagram illustrates that there are two remote access points running in "Universal Repeater" operation mode, they are the Access Point 2 and the Access Point 3. They both serve as the access point for their respective "Wi-Fi Networks" but also serve as the Wi-Fi clients and try to link to Access Point 1, the Wi-Fi server, by using Wi-Fi.

However, the local access point is running in "AP Only" mode and uses an Ethernet uplink interface to connect to an external 6402 for to access the Internet. The remote Wi-Fi networks behind Access Points 2 and 3 can access the Internet through the Access Point 1 since those remote access points have connected to the local access point.

Note the access points running in "Universal Repeater" mode will disable any DHCP server by default, so the client hosts under the access points will request their IP address from the external 6402 that has at least one DHCP server working. The external 6402 also executes the NAT or routing mechanism for Internet Access from all client hosts behind the access points.

The access point in "Universal Repeater" mode provides a Wi-Fi bridge to the local access point without an embedded DHCP server and NAT. However, the local access point in "AP Only" mode accepts the association and linking requests from remote access points to establish Wi-Fi links for linking them all together. It also uses an Ethernet link to connect to an external 6402 that executes IP assigning and NAT/routing function for Internet accessing.

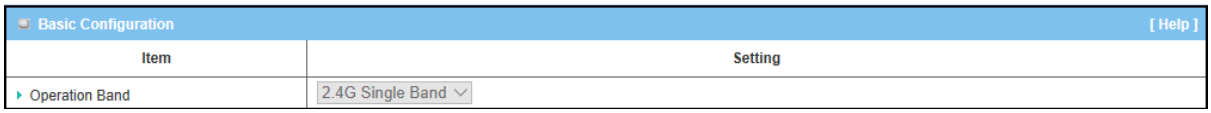


4.3.2. Wi-Fi Module One Configuration

Go to **Basic Network >Wi-Fi>Wi-Fi Module One** Tab.

If the 6402 is equipped with two Wi-Fi modules, it's possible to undertake similar configurations on both modules.

4.3.2.1 Basic Configuration



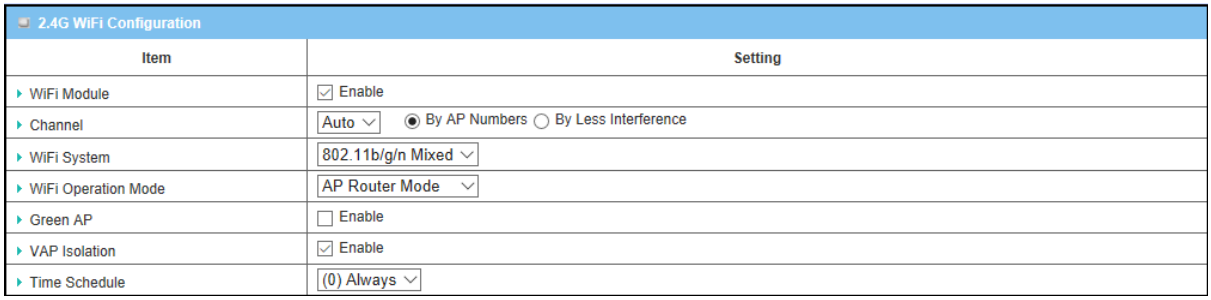
Basic Configuration		
Item	**Value**	**Description**
Operation Band	Mandatory	Specify the intended frequency band for the Wi-Fi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the product. However, there are some modules with selectable bands for user to choose according to his network environment. Under such situation, you can specify which operation band is suitable for the application. Currently this is 2.4GHz Single band only.

4.3.2.2 2.4GhzWi-Fi Configuration

In the screen shots below, specific configuration description for each Wi-Fi operating mode is given.

AP Router Mode – Menu Option

For the AP Router mode, the 6402 not only supports **stations connection** but also the **routing function**. The **WAN** port and the **NAT** function are **enabled**.



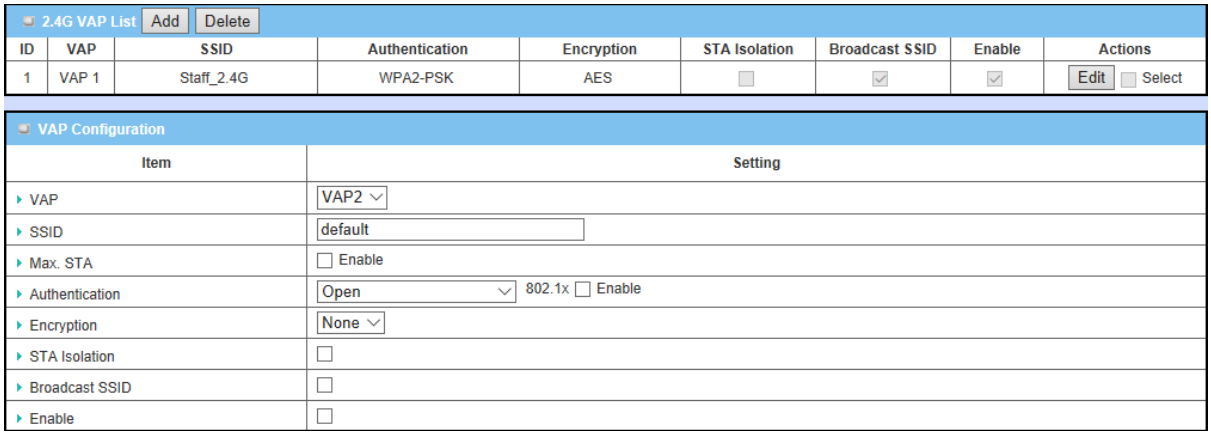
AP Router Mode		
Item	**Value**	**Description**
Wi-Fi Module	The box is checked by default	Check the **Enable** box to activate Wi-Fi function.
Channel	Auto and By AP Number	Specifies which Wi-Fi channel is used and the reason to select which channel is used. Auto is nearly always the best selection. By AP Number selects the next AP Channel number when the current channel has too much interference. By Less Interference select the AP Channel with the least amount of interference.
Wi-Fi System	802.11b/g/n Mixed	Specify the preferred WiFi System. The dropdown list of **Wi-Fi system** is based on **IEEE 802.11** standard. **2.4G Wi-Fi** can select b, g and n only or mixed with each other.
Wi-Fi Operation Mode		Specify the **Wi-Fi Operation Mode** according to your application. Go to the following table for **AP Router Mode**, **WDS Only Mode** and **WDS Hybrid Mode** settings. The available operation modes depend on the product specification.
Green AP	The box is	Check the **Enable** box to activate **Green AP** power saving functionality.

	unchecked by default.	
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	Mandatory	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition** >**Scheduling** > **Configuration** tab.

With the current version of software, the option to select **WPS Setup** has been disabled and greyed out.

VAP Configuration

On the 6402 Wi-Fi allows configuration of up to 8 Virtual Access Points. Each VAP can provide different SSID, Authentication, Encryption and even Access rights. Once configured each of these can be edited.

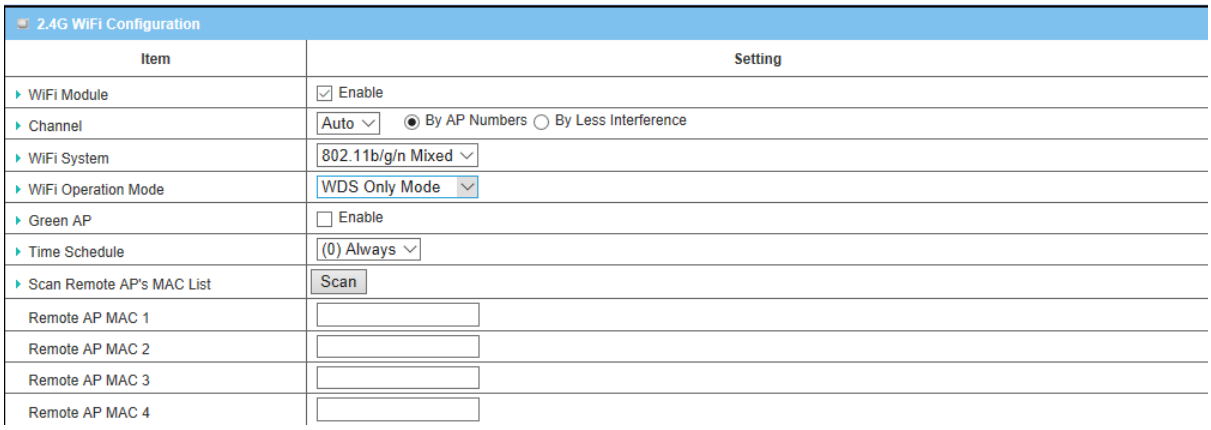


VAP Configuration		
Item	**Value**	**Description**
VAP	VAP number	Selects which VAP is to be added/edited.
SSID	String format: Any text	Enter the SSID for the VAP The **SSID** is used for identifying from another AP, and client stations will associate with AP according to SSID.
Max. STA	The box is unchecked by default	When checked allows configuration of the maximum number of STAs that have been successfully associated on the VAP.
Authentication	1. Mandatory 2.**Auto** is selected be default.	For security, there are several authentication methods supported. Client stations should provide the key when associate with this device.
		When **Open** is selected The check box named **802.1x** shows up next to the dropdown list. **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be authenticated by RADIUS server. **RADIUS Server IP**(The default IP is 0.0.0.0) **RADIUS Server Port**(The default value is 1812) **RADIUS Shared Key**
		When **Shared** is selected The pre-shared WEP key should be set for authenticating.
		When **Auto** is selected The device will select **Open** or **Shared** by requesting of client automatically. The check box named **802.1x** shows up next to the dropdown list. **802.1x** (The box is unchecked by default) When **802.1x** is enabled, it means the client stations will be

		authenticated by RADIUS server. **RADIUS Server IP**(The default IP is 0.0.0.0) **RADIUS Server Port**(The default value is 1812) **RADIUS Shared Key**
		When **WPA** or **WPA2** is selected They are implementation of IEEE 802.11i. **WPA** only had implemented part of IEEE 802.11i but owns the better **compatibility**. **WPA2** had fully implemented 802.11i standard and owns the highest **security**. **RADIUS Server** The client stations will be authenticated by RADIUS server. **RADIUS Server IP**(The default IP is 0.0.0.0) **RADIUS Server Port**(The default value is 1812) **RADIUS Shared Key**
		When **WPA** / **WPA2** is selected It owns the same setting as **WPA** or **WPA2**. The client stations can associate with this device via **WPA** or **WPA2**.
		When **WPA-PSK** or **WPA2-PSK** is selected It owns the same encryption system as WPA or WPA2. The authentication uses pre-shared key instead of RADIUS server.
		When **WPA-PSK** / **WPA2-PSK** is selected It owns the same setting as **WPA-PSK** or **WPA2-PSK**. The client stations can associate with this device via **WPA-PSK** or **WPA2-PSK**.
Encryption	1.Mandatory 2. **None** is selected be default.	Select a suitable encryption method and enter the required key(s). The available method in the dropdown list depends on the Authentication you selected. **None -**It means that the device is open system without encrypting. **WEP**-Up to 4 WEP keys can be set, and you must select one as current key. The key type can set to **HEX** or **ASCII**. If **HEX** is selected, the key should consist of (0 to 9) and (A to F). If **ASCII** is selected, the key should consist of ASCII table. **TKIP – If** TKIP was proposed instead of WEP without upgrading hardware. Enter a Preshared Key for it. The length of key is from 8 to 63 characters. **AES -** The newest encryption system in Wi-Fi, it also designed for the fast 802.11n high bitrates schemes. Enter a Pre-shared Key for it. The length of key is from 8 to 63 characters. You are recommended to use **AES** encryption instead of any others for security. **TKIP / AES** mixed mode. It means that the client stations can associate with this device via **TKIP** or **AES**. Enter a Preshared Key for it. The length of key is from 8 to 63 characters.
STA Isolation	The box is unchecked by default.	Check the **Enable** box to activate this function. When checked it means that stations which associated to the same VAP cannot communicate with each other.
Broadcast SSID	The box is unchecked by default.	If the broadcast SSID option is enabled, it means the SSID will be broadcasted, and the stations can associate with this device by scanning SSID.
Enable	The box is unchecked by default.	Enables the configured VAP

WDS Only Mode

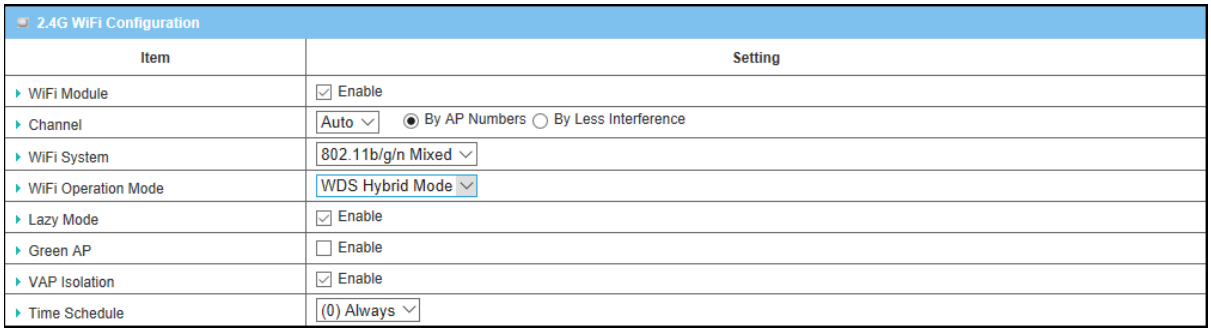
For the WDS Only mode, the 6402 only bridges the connected **wired** clients to another WDS-enabled Wi-Fi device which the 6402 is associated with. It also means the no wireless clients can connect to this 6402 while WDS Only Mode is selected.



WDS Only Mode		
Item	**Value**	**Description**
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
Time Schedule	Mandatory	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition** >**Scheduling** > **Configuration** tab.
Scan Remote AP's MAC List	N/A	Press the **Scan** button to scan the spatial AP information, and then select one from the AP list, the MAC of selected AP will be auto filled in the following Remote AP MAC table.
Remote AP MAC 1~4	Mandatory Setting	Enter the remote AP's MAC manually, or via auto-scan approach, the device will bridge the traffic to the remote AP when associated successfully.

WDS Hybrid Mode

In WDS Hybrid mode, the 6402 bridges all the wired **LAN** and **WLAN** clients to another WDS or WDS hybrid enabled Wi-Fi device which the 6402 is associated with.



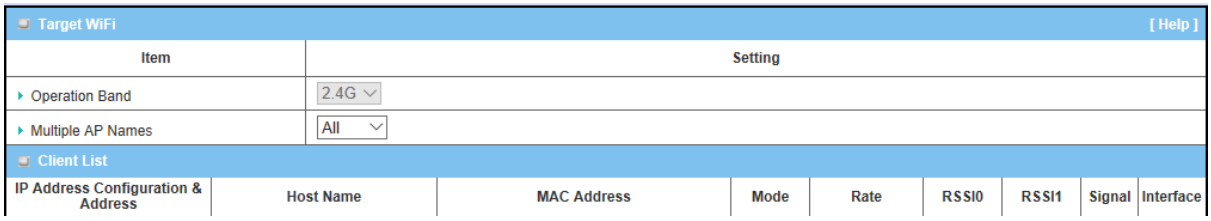
WDS Hybrid Mode		
Item	**Value setting**	**Description**
Lazy Mode	The box is checked by default.	Check the **Enable** box to activate this function. With the function been enabled, the device can auto-learn WDS peers without manually entering other AP's MAC address. But at least one of the APs has to fill remote AP MAC addresses.
Green AP	The box is unchecked by default.	Check the **Enable** box to activate **Green AP** function.
VAP Isolation	The box is checked by default.	Check the **Enable** box to activate this function. By default, the box is checked, it means that stations which associated to different VAPs cannot communicate with each other.
Time Schedule	Mandatory	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition** >**Scheduling** > **Configuration** tab.

4.3.3. Wireless Client List

The **Wireless Client List** page shows the information of wireless clients which are associated with this 6402.Go to **Basic Network >WiFi>Wireless Client List** Tab.

4.3.3.1 Target Wi-Fi

Target Configuration		
Item	**Value setting**	**Description**
Operation Mode	2.4G	Selects the W-Fi operation, only 2.4GHz is currently available.
Multiple AP Names	1. Mandatory 2. **All** is selected by default.	Specify the VAP to show the associated client's information in the following Client List. By default, All VAP is selected.



4.3.3.2 Show Client List

The following Client List shows the information for wireless clients that is associated with the selected VAP(s).

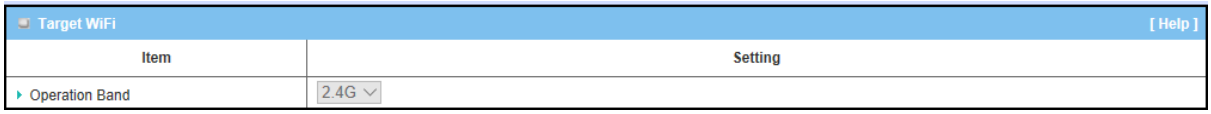
Target Configuration		
Item	**Value**	**Description**
IP Address Configuration & Address	N/A	It shows the Client's IP address and the deriving method. **Dynamic** means the IP address is derived from a DHCP server. **Static** means the IP address is a fixed one that is self-filled by client.
Host Name	N/A	It shows the host name of client.
MAC Address	N/A	It shows the MAC address of client.
Mode	N/A	It shows what kind of **Wi-Fi system** the client used to associate with this device.
Rate	N/A	It shows the **data rate** between client and this device.
RSSI0, RSSI1	N/A	It shows the RX sensitivity (RSSI) value for each radio path.
Signal	N/A	The **signal strength** between client and this device.
Interface	N/A	It shows the VAP ID that the client associated with.
Refresh	N/A	Click the **Refresh** button to update the Client List immediately.

4.3.4. Advanced Configuration

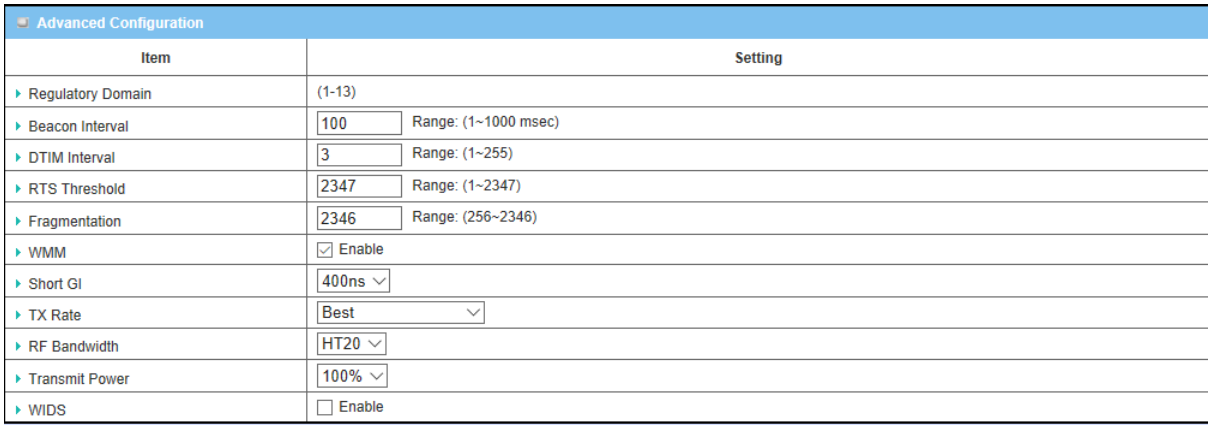
The 6402 provides an advanced wireless configuration option for advanced users to optimise the wireless performance under the specific installation environment. **NB.** if you are not familiar with Wi-Fi technology, leave the advanced configuration with its default values, or the connectivity and performance may get worse with improper settings.

Go to **Basic Network >WiFi>Advanced Configuration** Tab.

Select Target Wi-Fi



Target Configuration		
Item	**Value**	**Description**
Operation Band	Mandatory	Specify the intended operation band for the Wi-Fi module. Basically, this setting is fixed and cannot be changed once the module is integrated into the 6402. However, it's possible to fit other modules which operate on different bandwidths. Generally, this field will be fixed and greyed out



Advanced Configuration		
Item	**Value setting**	**Description**
Regulatory Domain	The default setting is according to where the product sale to	It limits the available radio channel of this device. The permissible channels depend on the **Regulatory Domain**.
Beacon Interval	100	It shows the time interval between each beacon packet broadcasted. The beacon packet contains **SSID**, **Channel ID** and **Security setting**.
DTIM Interval	3	A **DTIM (Delivery Traffic Indication Message)** is a countdown informing clients of the next window for listening to broadcast message. When the device has buffered broadcast message for associated client, it sends the next DTIM with a DTIM value.
RTS Threshold	2347	**RTS (Request to send) Threshold** means when the packet size is over the setting value, then active **RTS** technique. RTS/CTS is a **collision avoidance** technique. It means RTS **never** activated when the threshold is set to **2347**.
Fragmentation	2346	Wireless frames can be divided into smaller units (fragments) to **improve performance** in the presence of RF interference at the limits of RF coverage.
WMM	The box is checked by default	**WMM (Wi-Fi Multimedia)** can help control **latency** and **jitter** when transmitting **multimedia content** over a wireless connection.
Short GI	By default,**400ns** is selected	**Short GI (Guard Interval)** is defined to set the sending interval between each packet. Note that lower **Short GI** could **increase** not only the **transition rate** but also **error rate**.
TX Rate	By default, **Best** is selected	It means the **data transition rate**. When **Best** is selected, the device will choice a proper **data rat**e according to **signal strength**.
RF Bandwidth	By default, **Auto** is selected	The setting of RF bandwidth limits the maximum data rate.
Transmit Power	By default,**100%** is selected	Normally the wireless transmitter operates at 100% power. By setting the **transmit power** to control the Wi-Fi **coverage**.
WIDS	The box is unchecked by default	The WIDS (Wireless Intrusion Detection System) will analyze all the packet and make a statistic table in Wi-Fi status. Go to **Status**> **Basic Network**>**WiFi** tab for detailed WIDS status.
Save	N/A	Click the **Save** button to save the current configuration.
Undo	N/A	Click the **Undo** button to restore configuration to previous setting before saving.

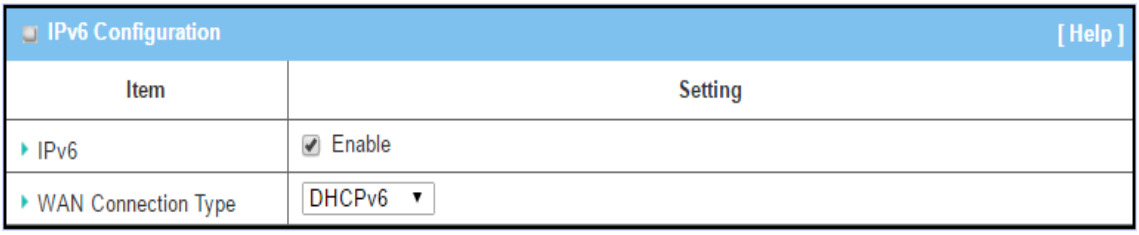
4.4. IPv6

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6** (**Internet Protocol version 6**) is a version of the Internet Protocol (IP) intended to succeed IPv4. IPv6 also implements additional features not present in IPv4. It simplifies aspects of address assignment (stateless address auto-configuration), network re-numbering and router announcements when changing Internet connectivity providers.

The 6402 supports various types of IPv6 connection (Static IPv6/DHCPv6 / PPPoEv6/6 to 4/6 in 4). **Please contact your ISP to determine type of IPv6 supported before you proceed with IPv6 setup.**

4.4.1. IPv6 Configuration

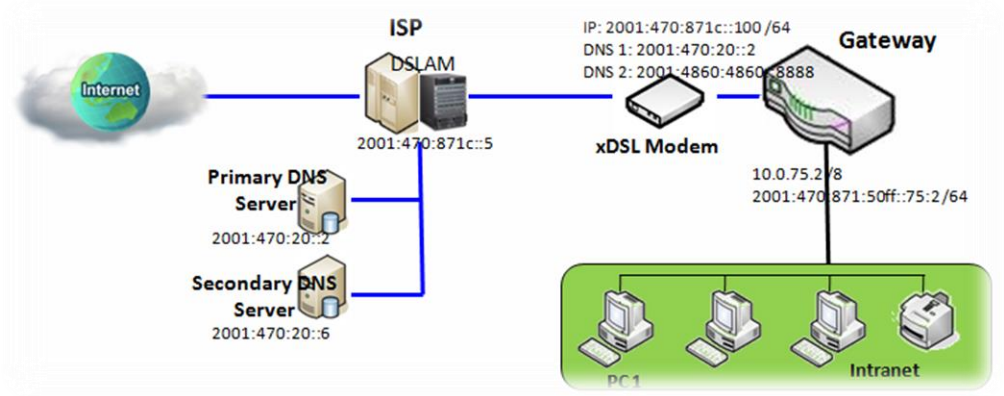
The IPv6 Configuration setting allows user to set the IPv6 connection type to access the IPv6 network. Go to **Basic Network > IPv6 > Configuration** Tab.

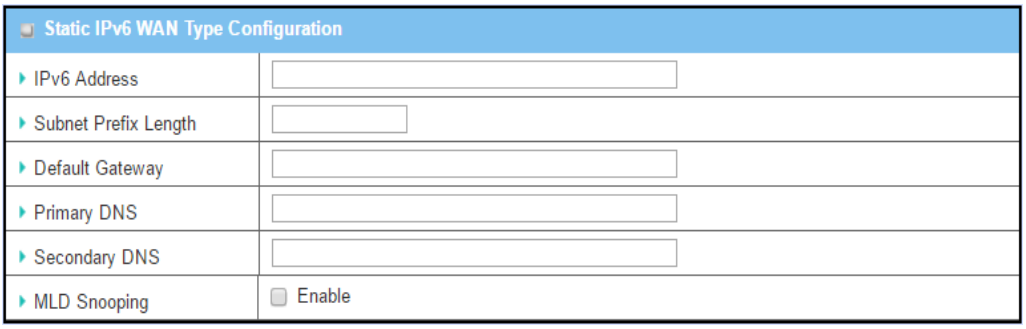


IPv6 Configuration		
Item	**Value setting**	**Description**
IPv6	The box is unchecked by default,	Check the **Enable** box to activate the IPv6 function.
WAN Connection Type	1. **This can only be selected when IPv6 has been Enabled** 2. A Mandatory	Define the selected IPv6 WAN Connection Type to establish IPv6 connectivity. **Select Static IPv6** if your ISP provides you with a set IPv6 addresses. Then go to **Static IPv6 WAN Type Configuration**. Select **DHCPv6**if your ISP provides you with DHCPv6 services. **SelectPPPoEv6**if your ISP provides you with PPPoEv6 account settings. **Select6to4** when you want to use IPv6 connection over IPv4. **Select6in4** when you want to use IPv6 connection over IPv4.

4.4.2. Static IPv6 WAN Type Configuration

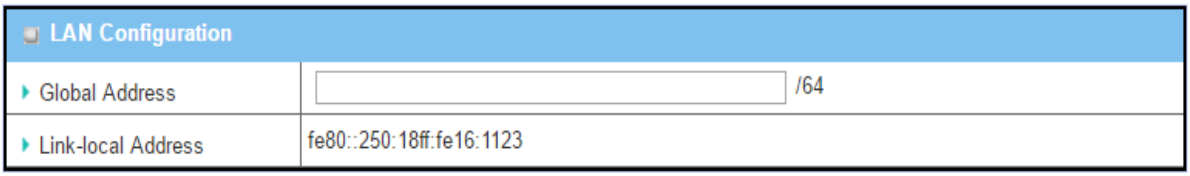
Static IPv6 provides the same function as static IPv4. The static IPv6 provides a manual setting of the IPv6 address, IPv6 default 6402 address, and IPv6 DNS.





Static IPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
IPv6 Address	Mandatory Setting	Enter the WAN **IPv6 Address** for the router.
Subnet Prefix Length	Mandatory Setting	Enter the WAN **Subnet Prefix Length** for the router.
Default 6402	Mandatory Setting	Enter the WAN **Default 6402** IPv6 address.
Primary DNS	An optional setting	Enter the WAN **primary DNS Server**.
Secondary DNS	An optional setting	Enter the WAN **secondary DNS Server**.
MLD Snooping	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

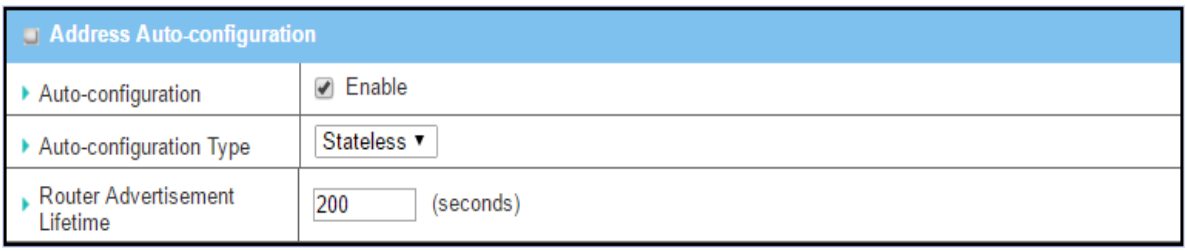


LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Mandatory setting	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

4.4.3. Address Auto-configuration – (same for all IPv6 options)

Go to **Address Auto-configuration (summary)**to set the LAN parameters.

Once the settings have been configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

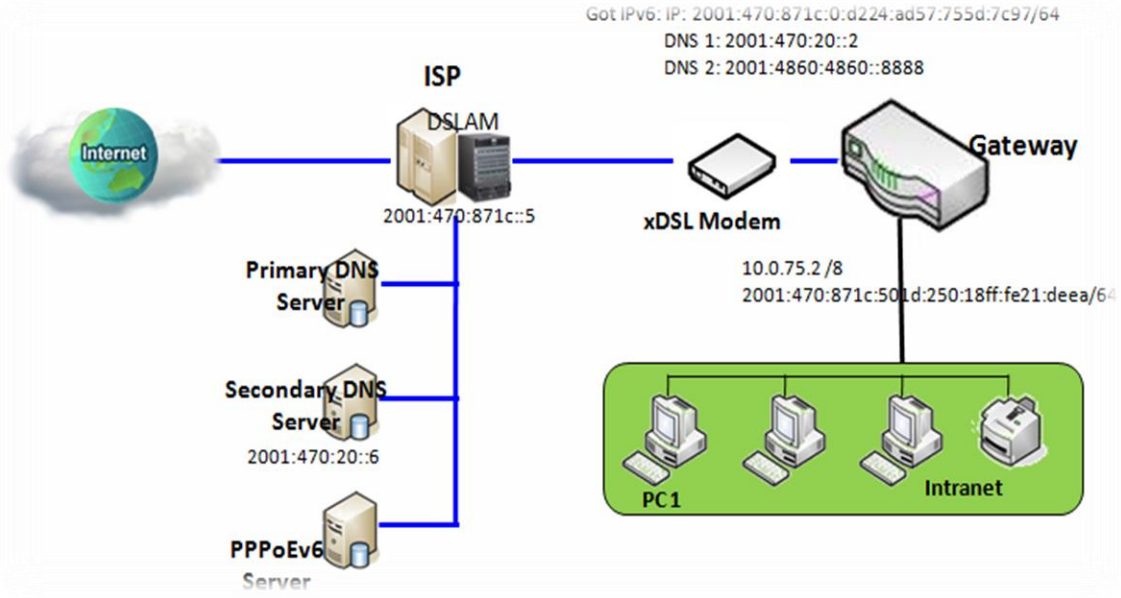


Address Auto-configuration	
Auto-configuration	Enable
Auto-configuration Type	Stateful
IPv6 Address Range(Start)	XXX:: /64
IPv6 Address Range(End)	XXX:: /64
IPv6 Address Lifetime	(seconds)

Address Auto-configuration		
Item	**Value setting**	**Description**
Auto-configuration	The box is unchecked by default	Check to enable the Auto configuration feature.
Auto-configuration Type	1. **Can only be selected when Auto-configuration enabled** 2. Stateless is selected by default	Define the selected IPv6 WAN Connection Type to establish the IPv6 connectivity. **Select Stateless** to manage the Local Area Network to be SLAAC + RDNSS **Router Advertisement Lifetime**(A Mandatory setting): Enter the Router Advertisement Lifetime (in seconds).200 is set by default. **Select Stateful** to set the Local Area Network to be Stateful (DHCPv6). **IPv6 Address Range(Start)** (A Mandatory setting): Enter the start IPv6 Address for the DHCPv6 range for your local computers. 0100 is set by default. **IPv6 Address Range(End)** (A Mandatory setting): Enter the end IPv6 Address for the DHCPv6 range for your local computers. 0200 is set by default. **IPv6 Address Lifetime** (A Mandatory setting): Enter the DHCPv6 lifetime for your local computers. 36000 is set by default.

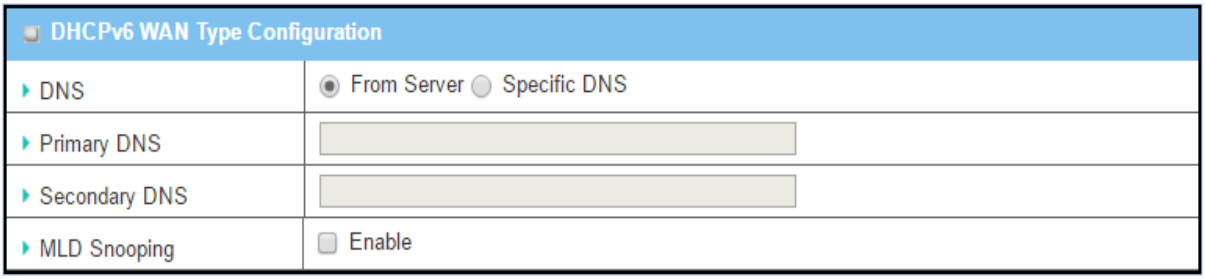
4.4.4. DHCPv6

DHCP within IPv6 provides the same function as DHCP in IPv4. The DHCP server sends an IP address, DNS server addresses and other data to the DHCP client. The server also sends a lease time for the address and time to re-contact the server for IPv6 address renewal. The client has then to resend a request to renew the IPv6 address.



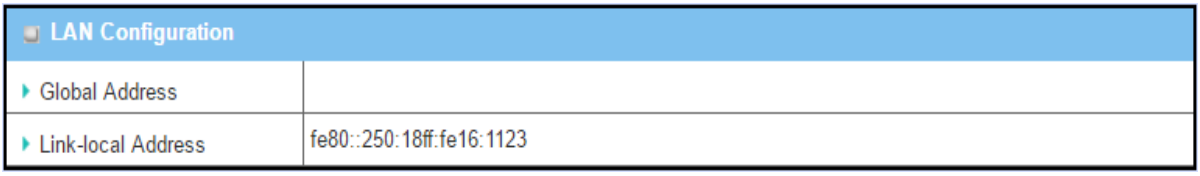
The above diagram depicts DHCP IPv6 IP addressing, the DHCPv6 server on the ISP side assigns IPv6 address, IPv6 default address, and IPv6 DNS to client host's automatically.

DHCPv6 WAN Type Configuration



DHCPv6 WAN Type Configuration		
Item	**Value setting**	**Description**
DNS	The option [From Server] is selected by default	Select the [Specific DNS] option to active Primary DNS and Secondary DNS. Then fill the DNS information.
Primary DNS	Cannot be modified by default	Enter the WAN **primary DNS Server**.
Secondary DNS	Cannot be modified by default	Enter the WAN **secondary DNS Server**.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration



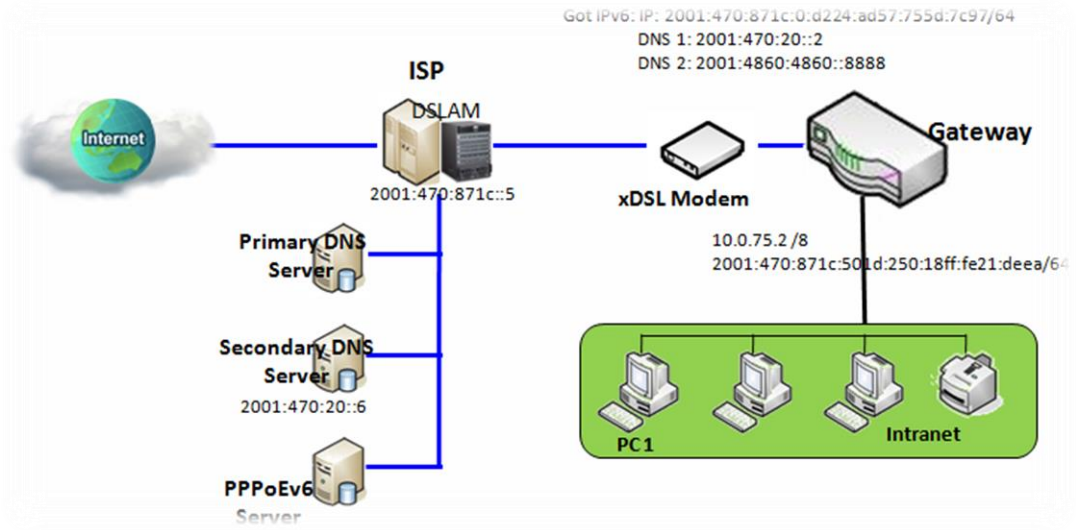
LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)** to set the LAN parameters.

Once the settings have been configured, click the **save button** to save the configuration and click the **reboot button** to reboot the router.

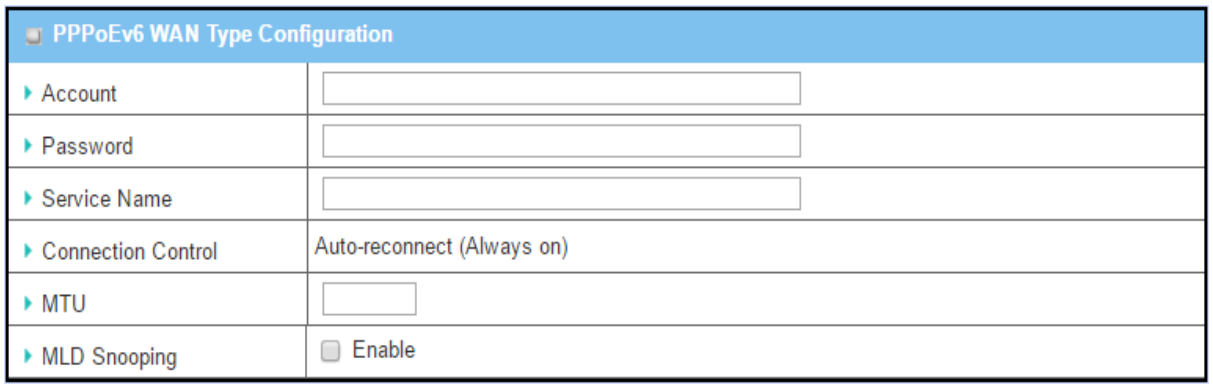
4.4.5. PPPoEv6

PPPoE V6 in IPv6 provides the same function as PPPoE in IPv4. The PPPoE v6 server provides configuration parameters based on the PPPoE v6 client request. When the PPPoE v6 server gets a client request and successfully authenticates it, the server sends IP address, DNS server addresses and other parameters to automatically configure the client.



The diagram above depicts the IPv6 addressing through PPPoE, the PPPoE v6 server (DSLAM) on the ISP side provides an IPv6 configuration upon receiving the PPPoE v6 client request. When the PPPoE v6 server gets a client request and successfully authenticates it, the server sends an IP address, DNS server addresses and other parameters to automatically configure the client.

PPPoEv6 WAN Type Configuration



PPPoEv6 WAN Type Configuration		
Item	**Value setting**	**Description**
Account	Mandatory Setting	Enter the Account to set up the PPPoEv6 connection. If you want more information, please contact your ISP.
Password	Mandatory Setting	Enter the Password to set up thePPPoEv6 connection. If you want more information, please contact your ISP.
Service Name	Mandatory Setting	Enter the Service Name to set up the PPPoEv6 connection. If you want more information, please contact your ISP.
Connection Control	Fixed value	The value is **Auto-reconnect(Always on)**.
MTU	Mandatory Setting	Enter the MTU to set up the PPPoEv6 connection. If you want more information, please contact your ISP.
MLD Snooping	The box is unchecked by default	Enable/Disable the MLD Snooping function

PPoEv6 LAN Configuration

LAN Configuration	
Global Address	
Link-local Address	fe80::250:18ff:fe16:1123

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	Value auto-created	The LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

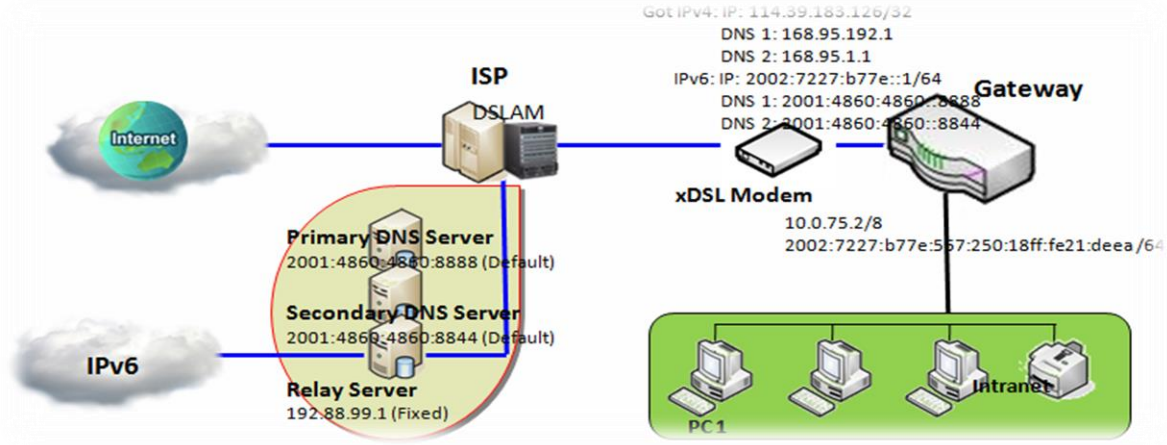
Go to **Address Auto-configuration (summary)**to configure the LAN parameters.

Once the settings have been configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

4.4.6. 6 to 4

6to4 is an Internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to version 6 (IPv6), a system that allows IPv6 packets to be transmitted over an IPv4 network (generally the IPv4 Internet) without the need to configure explicit tunnels. Special relay servers are also in place that allow 6to4 networks to communicate with native IPv6 networks

6 to 4 may be used by an individual host, or by a local IPv6 network. When used by a host, it must be connected to a global IPv4 address (e.g. host), and that host is responsible for the encapsulation of outgoing IPv6 packets and de capsulation of incoming 6 to 4 packets. If the host is configured to forward packets for other clients, often a local network, then it could be a router.



In the above diagram, the 6 to 4 means there is no need to set the 6402 address to "automatic". The Automatic setting means the 6402 will use the relay server, as defined in RFC 3068 which includes segments on 192.88.99.0/24 used as 6 to 4 relay of any-cast address to complete the 6 in4 setting.

6 to 4 WAN Type Configuration

6 to 4 WAN Type Configuration	
6 to 4 Address	
Primary DNS	
Secondary DNS	
MLD Snooping	Enable

6to4 WAN Type Configuration		
Item	**Value setting**	**Description**
6to4 Address	Value auto-created	IPv6 address for access the IPv6 network.
Primary DNS	An optional setting	Enter the WAN primary DNS Server.
Secondary DNS	An optional setting	Enter the WAN secondary DNS Server.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration

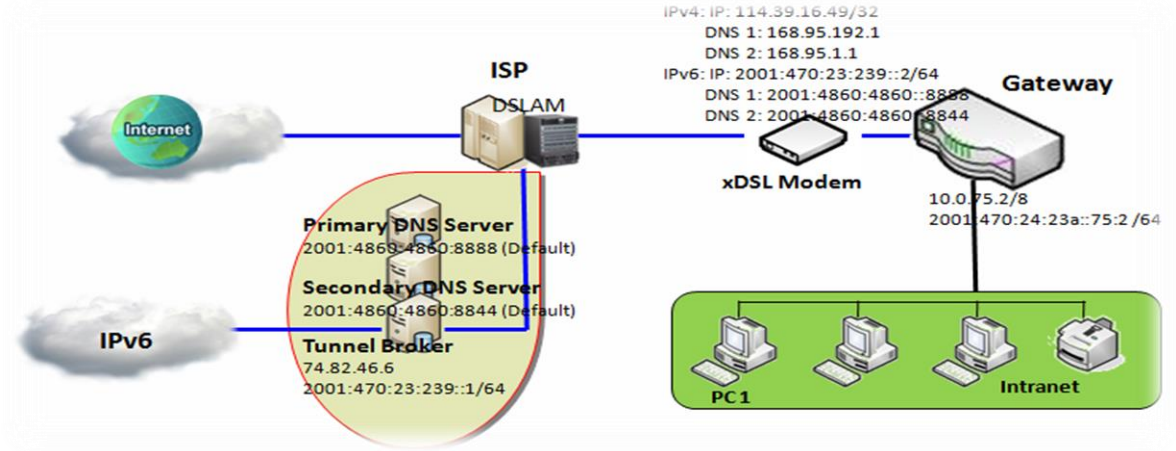
LAN Configuration	
Global Address	2002:0:0: ::1
Link-local Address	fe80::250:18ff:fe16:1123

LAN Configuration		
Item	**Value setting**	**Description**
Global Address	An optional setting	Enter the LAN **IPv6 Address** for the router.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)**to set the LAN parameters.
Once the settings have been configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

4.4.7. 6 in 4

6in4 is an Internet transition mechanism for migrating from Internet Protocol version 4 (IPv4) to IPv6. 6in4 uses tunnelling to encapsulate IPv6 traffic over explicitly-configured IPv4 links as defined in RFC 4213 (obsoletes RFC 2893 and RFC 1933). The 6in4 traffic is sent over the IPv4 Internet inside IPv4 packets whose IP headers have the IP protocol number set to 41. This protocol number is specifically designated for *IPv6 encapsulation*

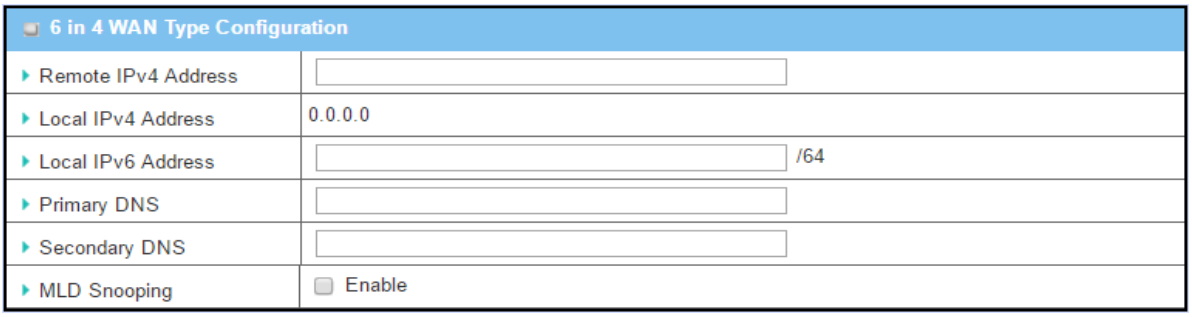


In the diagram above, the 6 in 4 usually needs to register to a 6 in 4 tunnel service, known as Tunnel Broker, in order to function. It also needs to know the end point global IPv4 addresses such as 114.39.16.49 to complete the 6 in 4 setting.

6 in 4 WAN Type Configuration

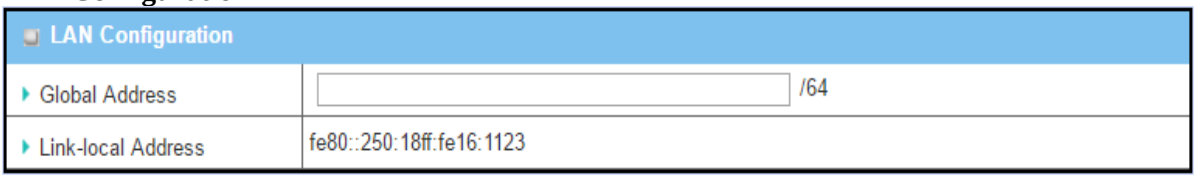
Look on the Internet to find suitable IPv6 tunnel brokers to establish your 6in4 tunnel. (You can find List of IPv6 tunnel brokers that support 6in4 service from wiki.)

Enter the **Local IPv4 address** of your 6402router into the **Client IPv4 Address** field in IPv6 tunnel broker setting page.



6in4 WAN Type Configuration		
Item	**Value setting**	**Description**
Remote IPv4 Address	A Mandatory Setting	Enter the **Server IPv4 Address** obtained from tunnel broker in this field.
Local IPv4 Address	Value auto-created	IPv4 address of this router.
Local IPv6 Address	A Mandatory Setting	Enter the **Client IPv6 Address** obtained from tunnel broker in this field.
Primary DNS	An optional setting	Enter the WAN primary DNS Server.
Secondary DNS	An optional setting	Enter the WAN secondary DNS Server.
MLD	The box is unchecked by default	Enable/Disable the MLD Snooping function

LAN Configuration



LAN Configuration		
Item	**Value setting**	**Description**
Global Address	A Must filled setting	Filled **Routed /64** gotten from tunnel broker in this field.
Link-local Address	Value auto-created	Show the link-local address for LAN interface of router.

Go to **Address Auto-configuration (summary)** for setting the LAN parameters.

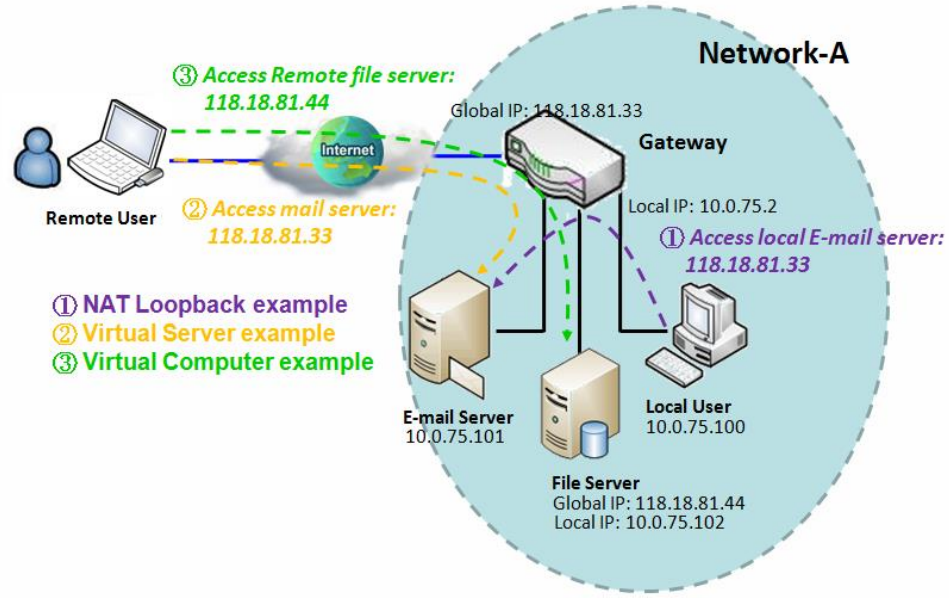
Once the settings have been configured, click the **save button** to save the configuration and click **reboot button** to reboot the router.

4.5 Port Forwarding

4.5.1. NAT Loopback

This feature allows you to access the WAN global IP address from your inside your 6402 Gateway NAT Local Area Network. It is useful when you run a server inside your network. For example, if you set a mail server on your local LAN, your local devices can access this mail server through the 6402's global IP address when the NAT Loopback feature is enabled.

NAT allows you to access the email server, either from the LAN side or WAN, without needing to change the IP address of the mail server, as shown in scenario ① of following diagram**.**



Scenario Application Timing

Users can access the organisations enterprise servers without any need to re-configure their PC's regardless of whether they are inside the company or coming in via the WAN

The network administrator must activate the "NAT Loopback" feature to enable this to work

Scenario Description

Local users can access mail server by using FQDN (Fully Qualified Domain Name)or global IP when NAT loop back is enabled. Global users can access the mail server only when the mail server is set as virtual server on the 6402

Parameter Setup Example

The following 2 tables list the parameter configuration as an example for the diagram above which shows the 6402 with the "NAT Loopback" feature activated.

Use default value for those parameters that are not mentioned in these tables.

Configuration Path	[Configuration]-[NAT Loopback]
NAT Loopback	■ ***Enable***

Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Server List]	
ID	1	2
Public Port	***25 (SMTP)***	***110 (POP3)***
Server IP	***10.0.75.101***	***10.0.75.101***
Private Port	***25 (SMTP)***	***110 (POP3)***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In the diagram above, the 6402 belongs to Network-A, and the subnet of its Intranet is 10.0.75.0/24. The 6402 has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a NAT router. Activate the NAT Loopback feature on the 6402.

Define the E-mail virtual server to be located as a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110.

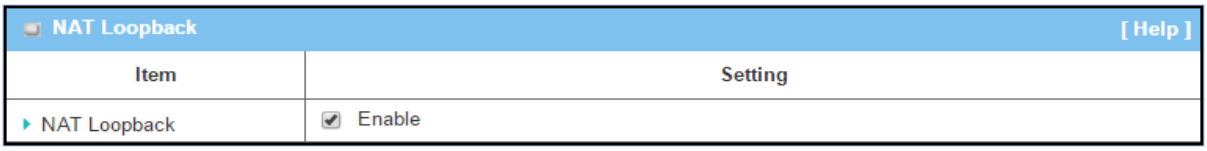
The local user at the host with IP address 10.0.75.100 can access the E-mail server by using the 6402 on IP 118.18.81.33. But in reality, the E-mail request packets from the local host will not go out of the WAN interface, but just loop back within the 6402 going to the E-mail server on the Intranet.

4.5.1.1. NAT Configuration Setting

Go to Basic Network > Port Forwarding > Configuration tab.

The NAT Loopback allows user to access the WAN IP address from inside your local network.

Enable NAT Loopback



Configuration		
Item	**Value setting**	**Description**
NAT Loopback	The box is checked by default	Check the **Enable** box to activate this NAT function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings

4.5.2 Virtual Server & Virtual Computer

A Virtual server is another name for port forwarding used by some routers.

In computer networking, port forwarding, or port mapping is an application like network address translation (NAT) that redirects a communication request from one address and port number to another network. This technique is most commonly used to make services on a host residing in a protected or masqueraded (internal) network available to hosts on the opposite side of the 6402 (external network), by remapping the destination IP address and port number of the packets to an internal host.

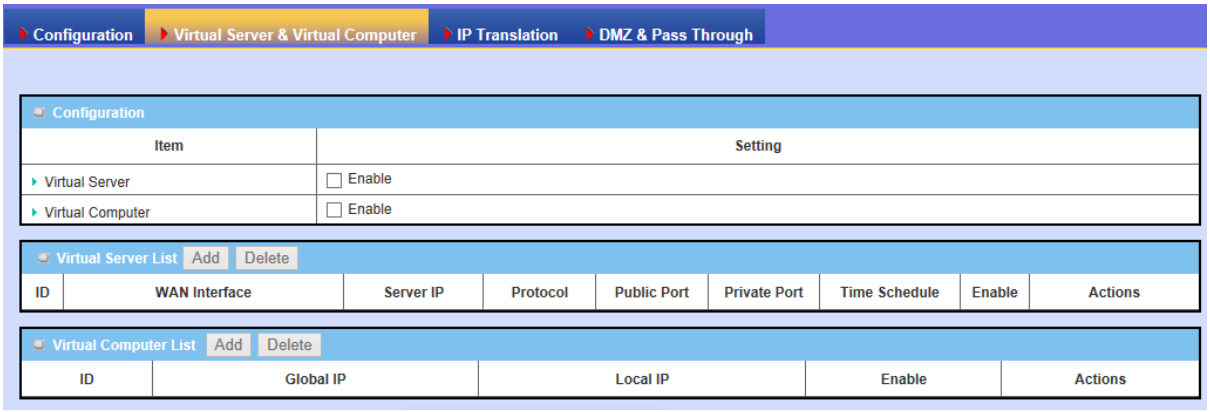
Port forwarding allows remote computers (on the Internet) to connect to a specific computer or service within a private local-area network (LAN). This allows the network manager to deploy some servers in their Intranet with the 6402 providing firewall protection. The 6402 NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind the 6402 are invisible to the outside world. The network manager can make some of them accessible by enabling the Virtual Server Mapping.

However, a virtual computer is a host on the Intranet whose IP address is global and visible to the outside world. Since it is in the Intranet, it is protected by the 6402 firewall acts like a node on the Internet.

In the "Virtual Server & Virtual Computer" menu options, there are two windows for all virtual servers and virtual computer. The "Virtual Server List" lists the public port used by devices from the Internet, and the private port used by devices on the Intranet. It’s possible to specify the protocol used for the service and to set a time schedule rule for the virtual servers.

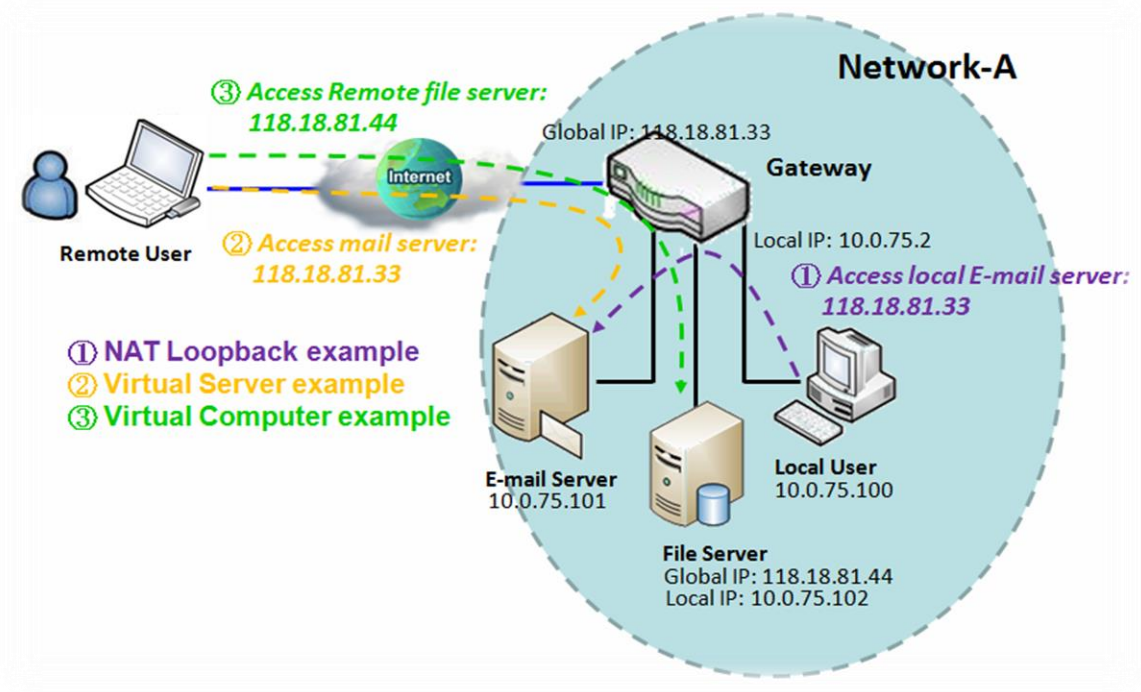
There is an "Add" button for you to add and create new virtual servers, and an "Edit" button to modify the existing virtual server settings.

The "Virtual Computer List", lists the mapping of the global IP address and the local IP address for all virtual computers. There is also an "Add" button for you to add and create a new virtual computer, and an "Edit" button to modify the existed virtual computer.



4.5.2.1. Virtual Server

The "Virtual Server" feature allows you to define servers with the global IP address or FQDN of the 6402 as though the servers exist on the Internet. However, these servers are located on the Intranet and are physically behind the 6402. The 6402 serves the service requests by port forwarding their requests to the LAN servers and transfers the replies from the LAN servers to the requester on the WAN side. For example, if you set an E-mail server on the LAN side with IP address 10.0.75.101, a remote user can access the 6402 for the E-mail service if you define a virtual E-mail server on the 6402 by using the real E-mail server on the LAN side, as shown in scenario ② in following diagram.



Scenario Application Timing

Set up application servers on the 6402 Intranet, which are protected by the 6402 firewall. The 6402 appears to be a physical server to the remote users, while the real server is, operating and providing service at the LAN side behind the 6402.

Scenario Description

The 6402 Gateway serves as an E-mail server for remote users wanting E-mail services.
The 6402 Gateway executes port forwarding transfers the E-mail service requests to the LAN servers and sends the replies from LAN servers to the requester.
The E-mail server on the LAN side of the 6402is the E-Mail server.

Parameter Setup Example

The table below list the configuration for scenario ②in above diagram. Please note that the E-mail service includes SMTP and POP3 service ports.
Use default value for those parameters that are not mentioned in the table.

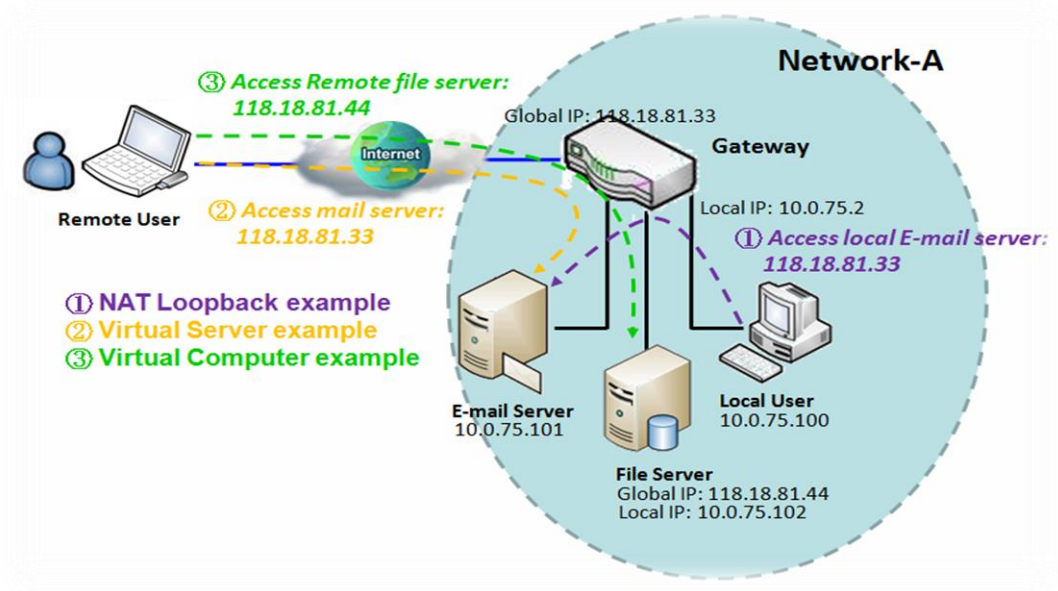
Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Server List]	
ID	***1***	***2***
Public Port	***25 (SMTP)***	***110 (POP3)***
Server IP	***10.0.75.101***	***10.0.75.101***
Private Port	***25 (SMTP)***	***110 (POP3)***
Rule	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

In above diagram, the 6402 Gateway is the gateway on Network-A and its local subnet is 10.0.75.0/24. The 6402 Gateway has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a NAT router. Define the E-mail virtual server to be located at a server with IP address 10.0.75.101 in the Intranet of Network-A, including SMTP service port 25 and POP3 service port 110. This will allow the remote user to access the E-mail server in the 6402 Gateway that has the global IP 118.18.81.33 on its WAN side. But the real E-mail server is located on the LAN side and the 6402 Gateway acts as the port forwarder for E-mail service.
A virtual server rule can be integrated with a schedule rule. This means, the virtual server rule can be activated only at the pre-defined time schedule.

4.5.2.2. Virtual Computer

The "Virtual Computer" feature allows you to assign LAN hosts to global IP addresses, so that they can be visible to the outside world. While visible to the outside world, they are also protected by the 6402 firewall much the same as when they are protected while acting as client hosts in the Intranet.
For example, if you set an FTP file server on the LAN side with a local IP address of 10.0.75.102 and global IP address of 118.18.82.44, a remote user can access the file server while it is hidden behind the NAT 6402 Gateway. The 6402 Gateway takes care of all request to the IP address 118.18.82.44, including forwarding the access requests to the file server, it also sends the replies from the server to outside world, as shown in scenario ③ in following diagram**.**



Example Description

To setup hosts on the 6402 Gateway Intranet which are visible to outside world but also protected by the 6402 Gateway NAT firewall, use the "Virtual Computer" feature in the 6402.
A LAN host is assigned with a global IP address to be visible to the outside world. The host has an embedded FTP file server and is protected by the 6402 Gateway firewall.
The 6402 acts as the Gateway between the LAN host and outside world to allow remote access.

Scenario Example Configuration

The following table lists the configuration for scenario ③in above diagram. Use the default value for those parameters that are not mentioned in the table.

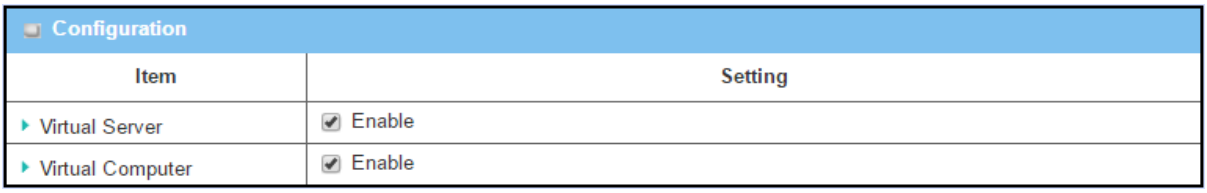
Configuration Path	[Virtual Server & Virtual Computer]-[Virtual Computer List]
ID	*1*
Global IP	*118.18.81.44*
Local IP	*10.0.75.102*
Rule	■ *Enable*

Scenario Operation Procedure

In the diagram above, the 6402 is the router on Network-A and the subnet of its Intranet is 10.0.75.0/24. The 6402 has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a NAT router.
A LAN host with private IP address 10.0.75.102 has an embedded FTP file server on it. The host is expected to be visible to the outside world with global IP address 118.18.81.44, but also protected by the 6402 firewall.
Configure a virtual computer in the 6402 for mapping between the global IP address 118.18.81.44 and the local IP address 10.0.75.102. The 6402 will take care of all connectivity to the FTP file server by using the server's global IP address, and it acts as a gateway between the LAN host and the outside world by using its "Virtual Computer" feature. This allows remote users to request file services from the FTP file server; even it is located on a LAN host.

4.5.2.3. Virtual Server & Virtual Computer Configuration

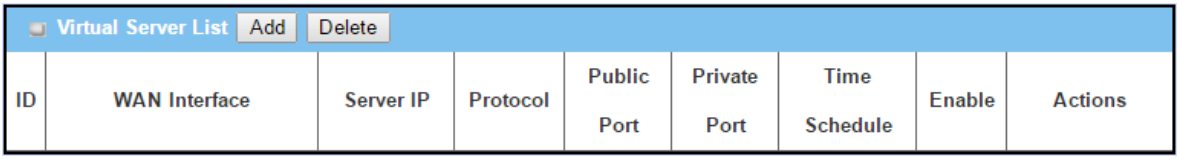
Go to Basic Network >Port Forwarding> Virtual Server & Virtual Computer tab.



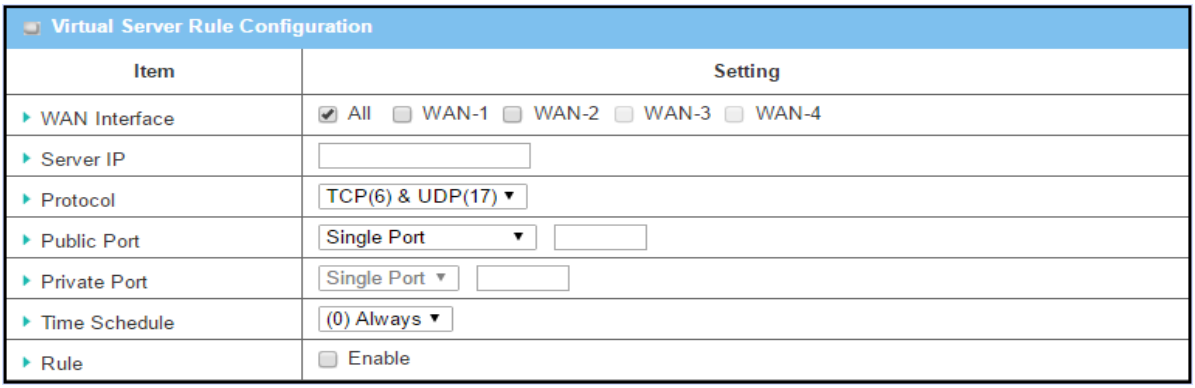
Configuration		
Item	**Value setting**	**Description**
Virtual Server	The box is unchecked by default	Check the **Enable** box to activate this port forwarding function
Virtual Computer	The box is checked by default	Check the **Enable** box to activate this port forwarding function
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings.

Create/Edit Virtual Server

The 6402 allows you to customise your Virtual Server rules. The router supports up to a maximum of 20 rule-based Virtual Server sets.



When the Add button is applied, the Virtual Server Rule Configuration screen will appear.



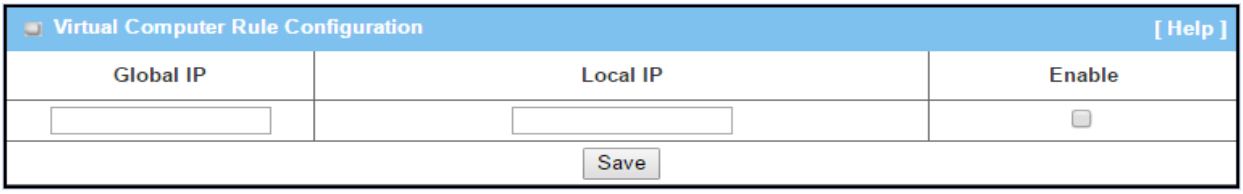
Virtual Server Rule Configuration		
Item	**Value setting**	**Description**
WAN Interface	1. A Mandatory setting 2. Default is **ALL**.	Define the interface for the packet to enter the 6402. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. These can be selected as **WAN-x** box when **WAN-x** enabled.
Server IP	Mandatory setting	This field is to specify the IP address of the interface selected in the WAN Interface setting above.
Protocol	A Mandatory Setting	When **"ICMPv4"** is chosen the option "Protocol" for the packet filter rule is ICMPv4. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Select **Enable** the box to enable this rule. When **"TCP"** is selected the "Protocol" for the packet filter rule is TCP. **Public Port** selects a predefined port from a **Well-known Service**, and **Private**

		Port is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. Apply Time Schedule to this rule, otherwise leave it as Always. (refer to Scheduling setting under Object Definition) Select **Enable** box to enable this rule. When **"UDP"** is selected, the "Protocol" for the packet filter rule is UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. When **"TCP & UDP"** is selected the "Protocol" option for the packet filter rule is TCP and UDP. **Public Port** selected a predefined port from **Well-known Service**, and **Private Port** is the same with **Public Port** number. **Public Port** is selected **Single Port** and specify a port number, and **Private Port** can be set a **Single Port** number. **Public Port** is selected **Port Range** and specify a port range, and **Private Port** can be selected **Single Port** or **Port Range**. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then check **Enable** box to enable this rule. When **"GRE"** is selected the "Protocol" for the packet filter rule is GRE. Apply **Time Schedule** to this rule, otherwise leave it as **Always**. **(**refer to **Scheduling setting** under **Object Definition)** Then select **Enable** box to enable this rule.
		When **"ESP"** is selected, the "Protocol" option for the packet filter rule is ESP. Apply Time Schedule to this rule, otherwise leave it as Always. (refer to Scheduling setting under Object Definition) Then check **Enable** box to enable this rule. Click the **Save** button to save the settings. When **"SCTP"** is selected -The "Protocol" option for the packet filter rule is SCTP. Apply Time Schedule to this rule, otherwise leave it as Always. (refer to Scheduling setting under Object Definition) Then check **Enable** box to enable this rule. When **"User-defined"** is selected the "Protocol" option for the packet filter rule is User-defined. For **Protocol Number**, enter a port number. Apply Time Schedule to this rule, otherwise leave it as Always. (refer to Scheduling setting under Object Definition) Then check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings.
Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filters Configuration page.

4.5.2.4. Create/Edit Virtual Computer

The 6402 allows you to custom your Virtual Computer rules, up to a maximum of 20 rule-based Virtual Computer sets.

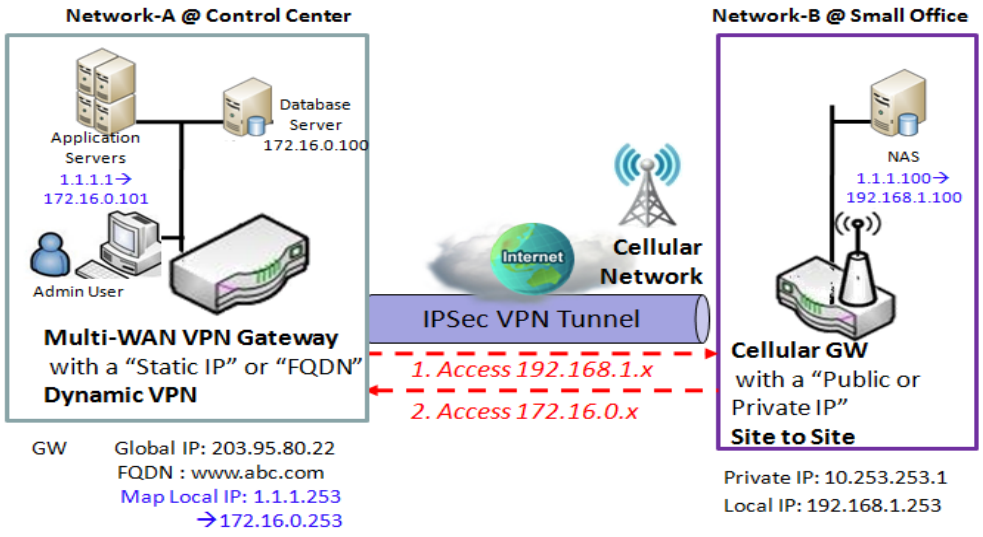
When Add button is applied, Virtual Computer Rule Configuration screen will appear.



Virtual Computer Rule Configuration		
Item	**Value setting**	**Description**
Global IP	A Mandatory setting	This field is to specify the IP address of the WAN IP.
Local IP	A Mandatory setting	This field is to specify the IP address of the LAN IP.
Enable	N/A	Then check **Enable** box to enable this rule.
Save	N/A	Click the **Save** button to save the settings.

4.5.3 IP Translation

IP Translation is similar to One-to-One NAT. It is a feature where you can configure the 6402 with multiple IP addresses issued by your ISP and map them to individual intranet devices with specific IP addresses. That is, configuring the IP Translation feature creates a one-to-one mapping between a public IP address and a private IP address of a local host.
The network manager may also map a private IP address range to a public IP address range.
This feature offers another way to allow systems to operate behind a firewall and configure private IP addresses to appear as though they do have public IP addresses.



1. Admin user can access Application server via IP Address 1.1.1.1 instead of 172.16.0.101
2. Admin user also can access NAS which mapped IP Address 1.1.1.100 instead of 192.168.1.100 via Remote VPN Tunnel

Example Description

The Network Manager setups IP Address 1.1.1.1 to substitute for 172.16.0.101 for the application server on intranet network.

The Network Manager setups IP Address 1.1.1.100 to substitute for 192.168.1.100 for the NAS Device on the remote intranet.

Users in the Control Centre can access application server via 1.1.1.1 or the NAS device via 1.1.1.100.

Example Configuration

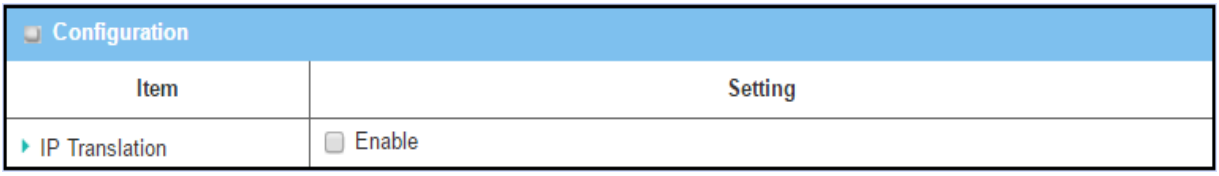
The following table lists the parameter configuration as an example for the 6402 in above diagram. Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Configuration]-[IP Translation]	
IP Translation	Enable ■	
ID	1	2
Mapping IP address	1.1.1.1 →172.16.0.101	1.1.1.100 → 192.168.1.100
Description	Application Server	Remote NAS
Rule	■ Enable	■ Enable

4.5.3.1 IP Translation Setting

Go to Basic Network > Port Forwarding > IP Translation tab.

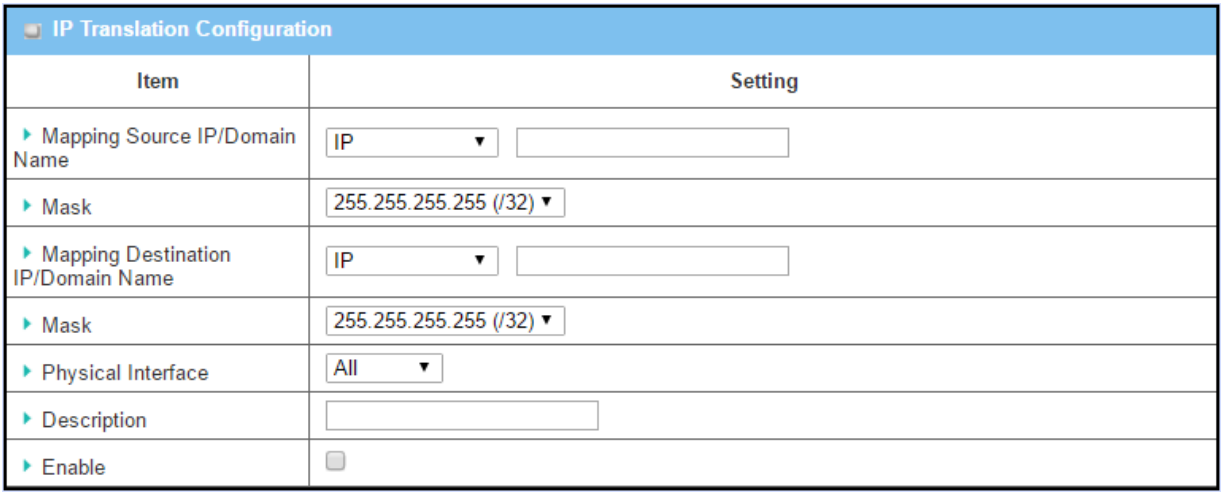
Enable IP Translation



Configuration		
Item	**Value setting**	**Description**
IP Translation	The box is unchecked by default	Check the **Enable** box to activate the IP translation function
Save	N/A	Click the **Save** button to save the settings.

Create/Edit IP Translation Rule

When the ‘Add’ button is applied, the IP Translation Configuration screen will appear.



IP Translation Configuration		
Item	**Value setting**	**Description**
Mapping Source IP/Domain Name	1. A mandatory setting 2.**IP** is selected by default.	Specify the original **IP** / **Domain Name** to be translated.
Mask	1. A mandatory setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Source IP** is specified above. It can be a single IP with 255.255.255.255 (/32) subnet mask, or an IP group limited with proper subnet setting.
Mapping Destination IP/Domain Name	1. A mandatory setting 2. **IP** is selected by default.	Specify the expected target **IP** / **Domain Name** that will be used to replace the original one.
Mask	1. A mandatory setting 2.**255.255.255.255(/32)** is selected by default.	Enter the required subnet mask if **Destination IP** is specified above. It can be a single IP with 255.255.255.255 (/32) subnet mask, or an IP group limited with proper subnet setting.
Physical Interface	1. A mandatory setting 2.**All** is selected by default.	Specify the interface to apply the translation rule. The enabled WAN Interface will be available in the dropdown list. By default, **All** is selected, and the translation rule will be applied to the traffics passing through all WAN interfaces.
Description	An optional setting.	Specify a brief description or rule name for this IP Translation rule.
Enable	The box is unchecked by default	Select the **Enable** box to activate the translation rule.

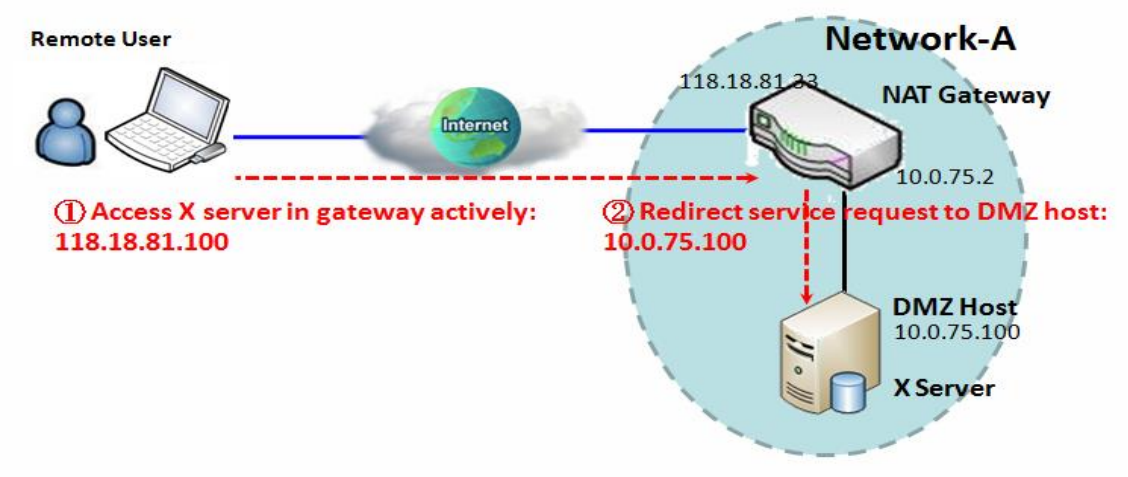
4.5.4 DMZ & Pass Through

A DMZ (De-Militarized Zone) Host is a host that is exposed to the Internet but still within the protection of the 6402 firewall. The DMZ function allows a computer to execute 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. In some cases when a specific application is blocked by the NAT mechanism, you can specify that the LAN computer is a DMZ host to solve this problem.

In the "DMZ" page, there is only one configuration window for the "DMZ" feature. The window lets you activate the DMZ function and specify the IP address on the 6402 local Intranet to be a DMZ host so that the host under the DMZ function can run applications freely that would, otherwise, blocked by the NAT mechanism. The incoming packets issued by an active application in the Internet are usually blocked outside of the 6402's NAT mechanism. But the DMZ host can receive those packets and make replies, however it is reactive to the outside world. In the meantime, it is also protected by the 6402 firewall.

The DMZ function allows you to ask the 6402 to pass through all normal packets to the DMZ host behind the 6402 NAT. The DMZ host is also protected by the 6402 firewall. Activate the feature and specify the DMZ host with a host in the Intranet when needed.

DMZ Example



Application Example

The6402 Network Manager wants to set up some service daemons in a host that is on the Intranet, which will allow remote users to request services from those hosts, even if the hosts are behind a 6402 NAT. But remote users think the 6402 provides those services, so users use the global IP of the 6402 to request their services. Apply the DMZ feature in the 6402 NAT to meet the application scenario. The client host is still protected by the 6402 firewall.

Scenario Description

The DMZ host is behind a 6402 NAT and receives all normal and active packets from the Internet. Remote users can access the DMZ host by using the IP address of the 6402, and the 6402 will skip the NAT checking on the DMZ host. The DMZ host is still protected by the 6402 firewall.

Example Configuration

The following table lists the parameter configuration as an example for the 6402 in above diagram with DMZ enabling.

Use the default value for those parameters that are not mentioned in the table.

Configuration Path	[DMZ]-[Configuration]
DMZ	IP Address of DMZ Host: ***10.0.75.100*■ *Enable***

Scenario Operation Procedure

In above diagram, the 6402 NAT Gateway is the router in Network-A and its subnet is 10.0.75.0/24. The 6402 Gateway has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface and it serves as a NAT router.

Configure a host with an IP Address of 10.0.75.100, in the 6402 subnet to be the DMZ Host and activate the rule.

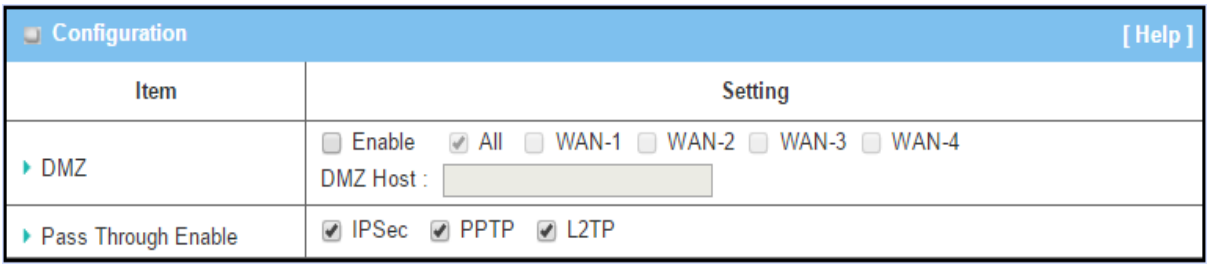
Assume there is an X server installed in the DMZ host. Then, the remote user can request services from the X server in the DMZ host by skipping the NAT checking by the 6402.

4.5.5 DMZ & Pass Through

The DMZ host is a host that is exposed to the Internet but still within the protection of the 6402 Gateway firewall

Go to Basic Network >Port Forwarding> DMZ& Pass through tab.

4.5.5.1. Enable DMZ and Pass Through



Configuration		
Item	**Value setting**	**Description**
DMZ	1. A Mandatory setting 2. Default is ALL.	Check the **Enable** box to activate this SDMZ function Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **WAN-x** then select **WAN-x** for this field. Select **ALL** for packets coming into the router from any interfaces. You can select the **WAN-x** box when **WAN-x** enabled. **DMZ Host** is to specify the IP address of Host LAN IP.
Pass Through Enable	The boxes are checked by default	Check the box to enable the pass-through function for the IPSec, PPTP, and L2TP. With the pass-through function enabled, the VPN hosts behind the 6402 can still connect to remote VPN servers.
Save	N/A	Click the **Save** button to save the settings.
Undo	N/A	Click **Undo** to cancel the settings

4.6. Routing

4.6.1 Introduction

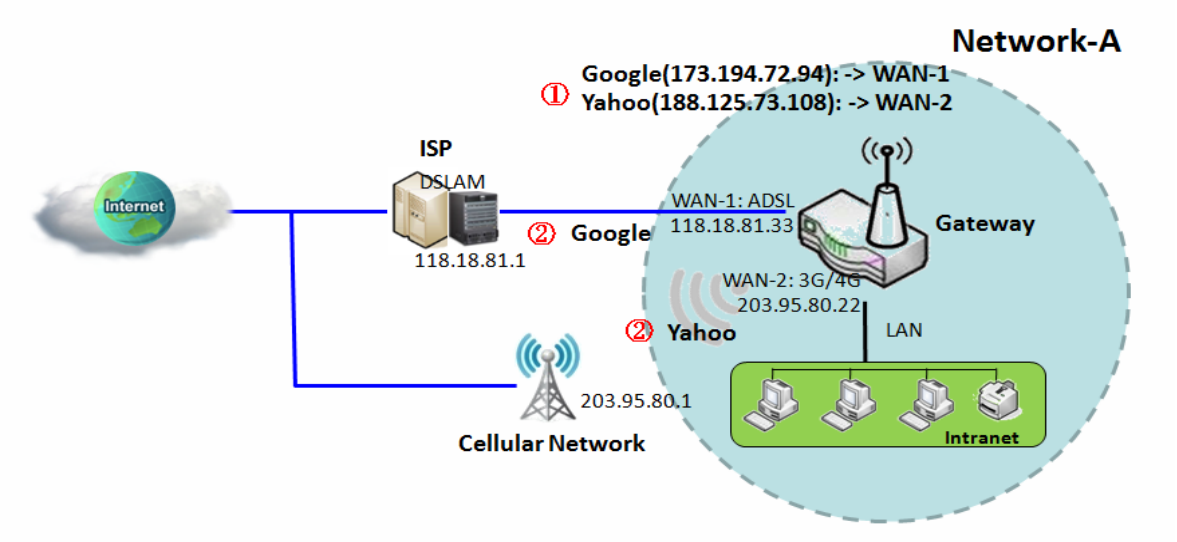
If you have more than one router and subnet, you will need to enable the 6402routing function to allow packets to find the correct routing path and allow different subnets to communicate with each other. The routing process usually forwards on the basis of routing tables which maintain a record of the routes to various network destinations. Thus, constructing routing tables, which are held in the router's memory, is very important for efficient routing. Most routing algorithms use only one network path at a time.

In Static routing the routing tables record your pre-defined routing paths for some specific destination subnets. However, in dynamic routing such as RIP, OSPF and BGP the routing tables record the routing paths from neighbouring routers.

Static Routing

The "Static Routing" function is configured by the network manager and lets them define the routing paths for some dedicated hosts/servers or subnets to store in the routing table of the 6402. The 6402 will route incoming packets to different routers based on the routing table.

Static Routing Example Diagram



4.6.1.1. Static Routing Example

Dedicated packet flows from the Intranet will be routed to their destination via the pre-defined 6402 Gateway and 6402 interface that are pre-define defined in the 6402routing table.
The following tables list the parameter configuration as an example of "Static Routing" for the 6402 in the diagram. Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[Static Routing]-[Configuration]	
Static Routing	■ ***Enable***	
Configuration Path	[Static Routing]-[Static Routing Rule List]	
ID (Interface)	1	2
Destination IP	***173.194.72.94***	***188.125.73.108***
Subnet Mask	***255.255.255.255***	***255.255.255.255***
6402	***118.18.81.1***	***203.95.80.1***
Metric	***255***	***255***
Rule	■ ***Enable***	■ ***Enable***

4.6.1.2. Static Routing Operation

In diagram above, the 6402 is the router in Network-A and its subnet is 10.0.75.0/24.
The 6402 has the IP address of 10.0.75.2 for its LAN interface, and 118.18.81.33 for its WAN-1 interface and IP Address of 203.95.80.22 for its WAN-2 interface. It serves as a NAT router.

For this example, we will configure two static routing rules for the 6402 Gateway.

The first one is to define the packets from the Intranet to the Google web site (173.194.72.94). These packets will be routed via the WAN-1 interface and the 6402 ADSL Link

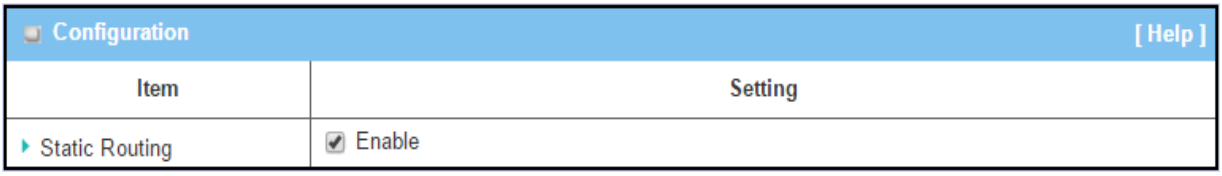
The second one is to define the packets sent the Yahoo web site (188.125.73.108). These will be routed via the WAN-2 interface and the Cellular Network.

4.6.2 Static Routing Setting

In the "Static Routing" page, there are three configuration windows for the static routing feature. They are the

- **"Configuration" window,**
- **"Static Routing Rule List" window**
- **"Static Routing Rule Configuration" window.**

The "Configuration" - window lets you activate the global static routing feature only. Even if you have defined many static routing rules for the 6402, you can disable them temporarily, by unchecking the Enable box. Go to **Basic Network** >**Routing**>**Static Routing** Tab.



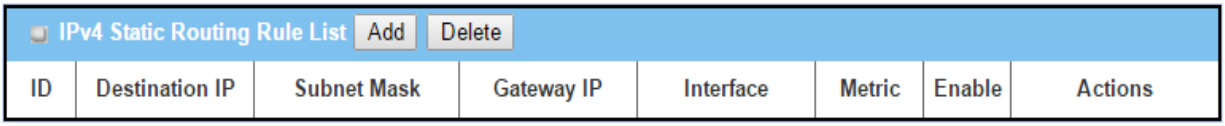
The "Static Routing Rule List" - window lists all your defined static routing rule entries. Using "Add" or "Edit" button to add and create one new static routing rule or to modify an existed one.

When "Add" or "Edit" button is applied the "Static Routing Rule Configuration" window will appear to let you define a static routing rule. The parameters include the destination IP address and subnet mask of a dedicated host/server or subnet, the IP address of peer router, the metric and the rule activation.

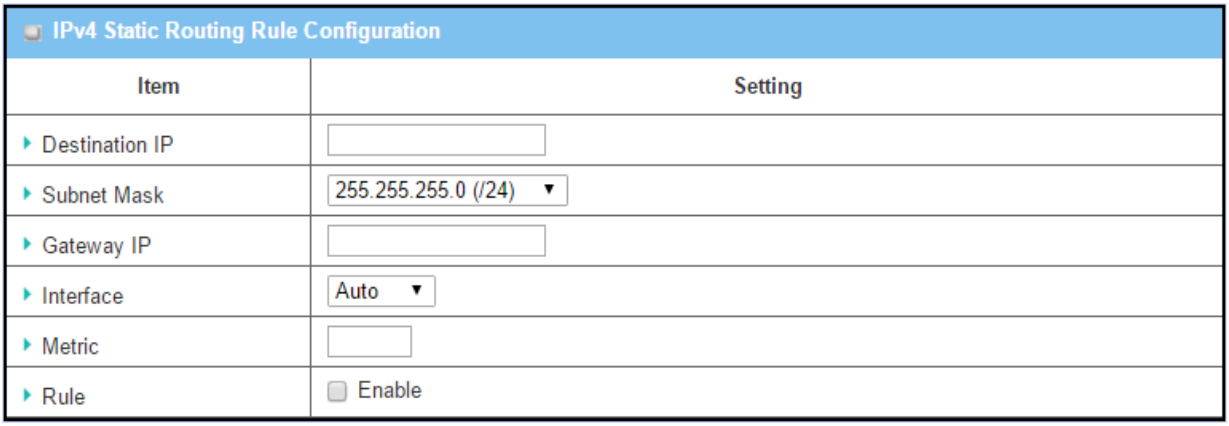
Static Routing		
Item	**Value setting**	**Description**
Static Routing	The box is unchecked by default	Check the **Enable** box to activate this function

Create/Edit Static Routing Rules

The Static Routing Rule List shows the setup parameters of all static routing rule entries. To configure a static routing rule, you must specify related parameters including the destination IP address and subnet mask of dedicated host/server or subnet, the IP address of the peer router, the metric and the rule activation.



The 6402allows you to custom your static routing rules. It supports up to a maximum of 64 rule sets. When Add button is applied, Static Routing Rule Configuration screen will appear, while the "Edit" button at the end of each static routing rule can let you modify the rule.



IPv4 Static Routing		
Item	**Value setting**	**Description**
Destination IP	1. IPv4 Format 2. Mandatory	The Destination IP of this static routing rule.
Subnet Mask	255.255.255.0 (/24) is set by default	The Subnet Mask of this static routing rule.
6402 IP	1. IPv4 Format 2. Mandatory	The 6402 IP of this static routing rule.
Interface	Auto is set by default	The Interface of this static routing rule.
Metric	1. Numeric String Format 2. Mandatory	The Metric of this static routing rule.
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	NA	Click the **Save** button to save the configuration
Undo	NA	Click the **Undo** button to restore what you just configured back to the previous setting. Please note that the restored setting may not be the factory default setting but a retrieve of what was saved in the memory.
Back	NA	When the **Back** button is clicked the screen will return to the Static Routing Configuration page.

4.6.3 Dynamic Routing

The Case Communications6402 supports dynamic routing protocols, including

- **RIPv1/RIPv2 (Routing Information Protocol),**
- **OSPF (Open Shortest Path First), and**
- **BGP (Border Gateway Protocol),**

The use of dynamic routing allows the 6402 to establish routing tables automatically.

Dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

4.6.4 Dynamic Routing Overview

The dynamic routing setting allows the network manager to customize RIP, OSPF, and BGP protocols.

In the "Dynamic Routing" page, there are seven configuration windows for dynamic routing feature. They are the "RIP Configuration" window, "OSPF Configuration" window, "OSPF Area List", "OSPF Area Configuration", "BGP Configuration", "BGP Neighbour List" and "BGP Neighbour Configuration" window. RIP, OSPF and BGP protocols can be configured individually.

The "RIP Configuration" window lets you choose which version of RIP protocol to be activated or you can disable it.

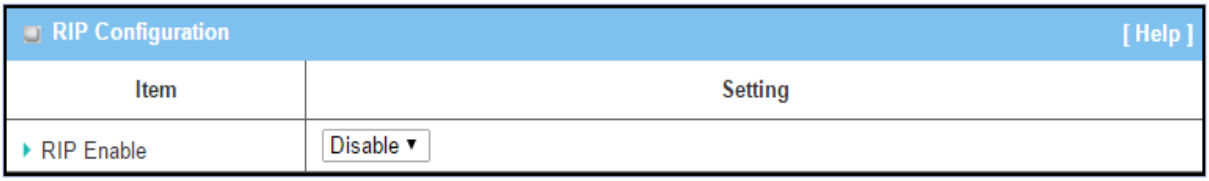
The "OSPF Configuration" window can let you activate the OSPF dynamic routing protocol and specify its backbone subnet. Moreover, the "OSPF Area List" window lists all defined areas in the OSPF network.

However, the "BGP Configuration" window can let you activate the BGP dynamic routing protocol and specify its self-ID. The "BGP Neighbour List" window lists all defined neighbours in the BGP network.

Go to **Basic Network** >**Routing**>**Dynamic Routing** Tab.

4.6.4.1. Enable RIP

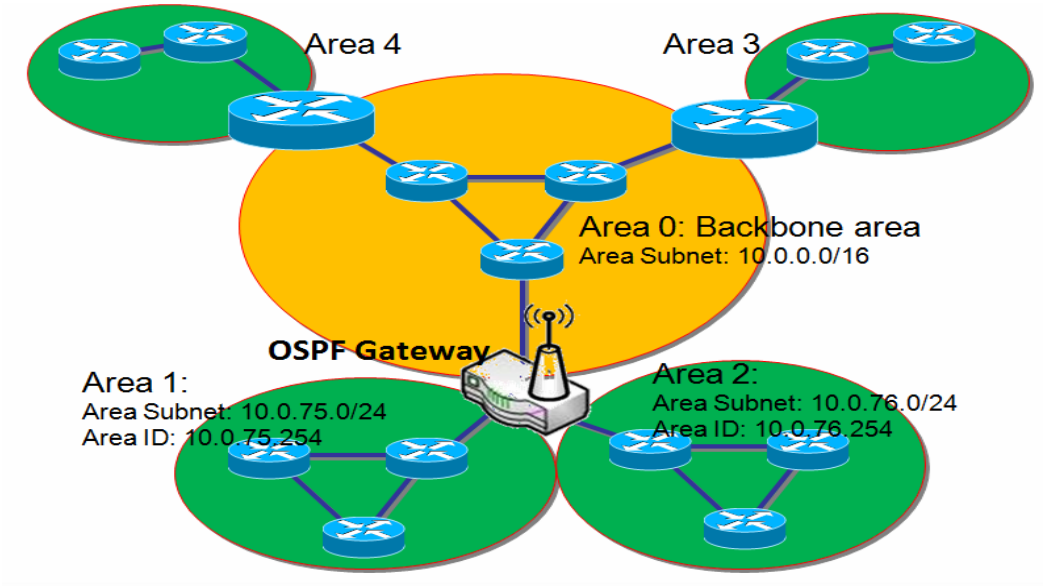
The RIP configuration setting allows user to customize RIP protocol through the router based on their office setting.



RIP Configuration		
Item	**Value setting**	**Description**
RIP Enable	Disable is set by default	Select **Disable** will disable RIP protocol. Select **RIP v1**will enable RIPv1 protocol. Select **RIP v2**will enable RIPv2 protocol.

4.6.4.2. OSPF Example

Open Shortest Path First (OSPF) is a routing protocol for (IP) networks and uses a link state routing algorithm and falls in



nario Application

Where a 6402 manager wao deploy a 6402 in a large network the router will learn its

Configuration Path	[Dynamic Routing]-[OSPF Configuration]	
OSPF	■ ***Enable***	
Backbone Subnet	**10.0.0.0/16**	
ID	1	2
Area Subnet	***10.0.75.0/24***	***10.0.76.0/24***
Area ID	***10.0.75.254***	***10.0.76.254***
Area	■ ***Enable***	■ ***Enable***

routing table using the OSPF proto

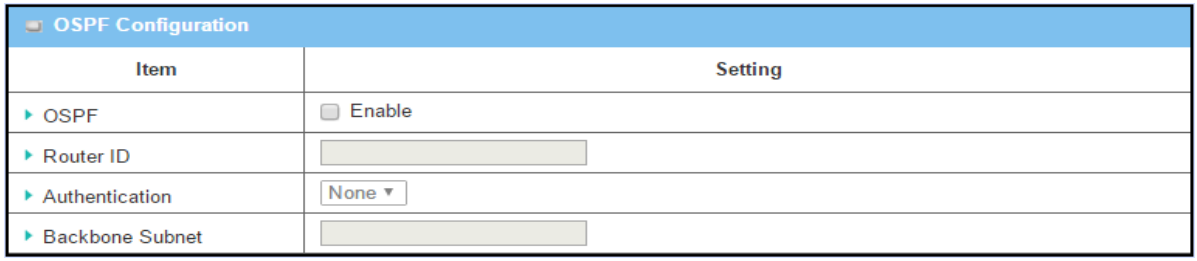
l from the enterprise backboneScenario Description

he 6402 gathers routing information from the ba

that are not mentioned in the tables.

Enable OSPF

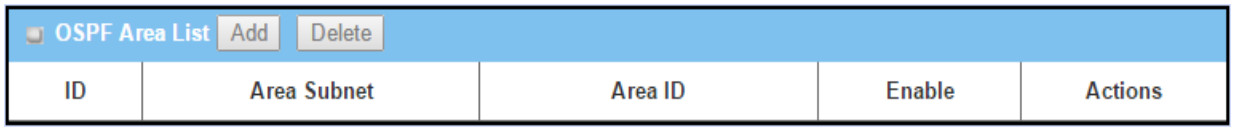
The OSPF configuration setting allows user to customize OSPF protocol through the router based on their office setting.



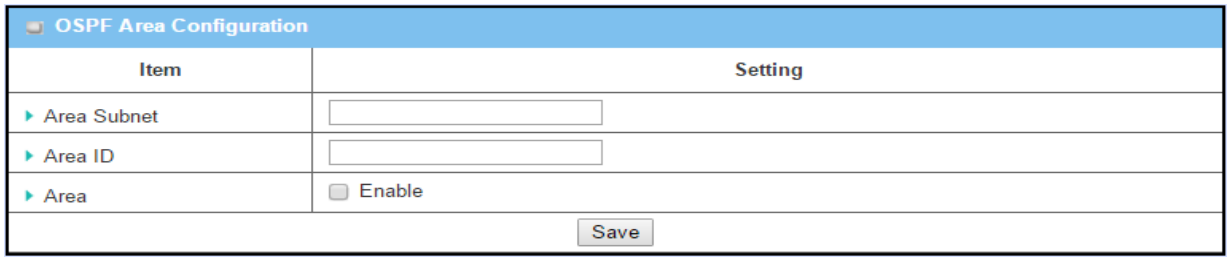
OSPF Configuration		
Item	**Value setting**	**Description**
OSPF	Disable is set by default	Click **Enable** box to activate the OSPF protocol.
Router ID	1. IPv4 Format 2. Mandatory	The Router ID of this router on OSPF protocol
Authentication	None is set by default	The Authentication method of this router on OSPF protocol. Select **None** will disable Authentication on OSPF protocol. Select **Text** will enable Text Authentication with entered the Key in this field on OSPF protocol. Select **MD5**will enable MD5 Authentication with entered the ID and Key in these fields on OSPF protocol.
Backbone Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Backbone Subnet of this 6402 using the OSPF protocol.

Create/Edit OSPF Area Rules

The router allows you to custom your OSPF Area List rules. It supports up to a maximum of 32 rule sets.



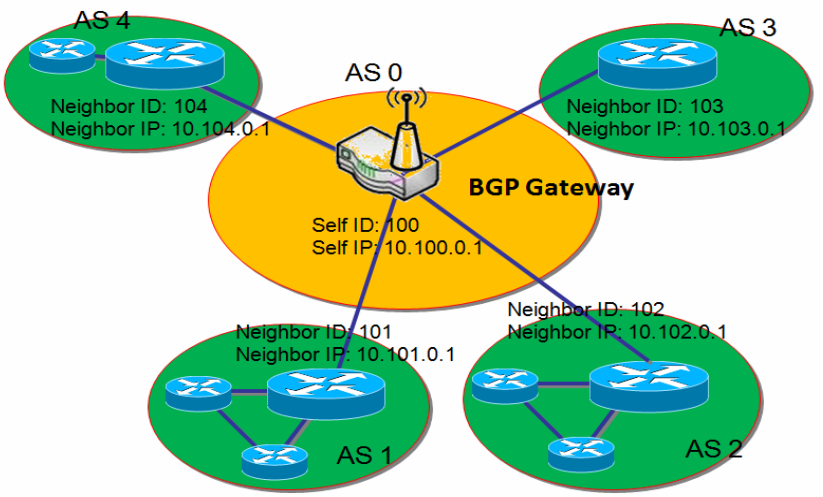
When Add button is applied, OSPF Area Rule Configuration screen will appear.



OSPF Area Configuration		
Item	**Value setting**	**Description**
Area Subnet	1. Classless Inter Domain Routing (CIDR) Subnet Mask Notation. (Ex: 192.168.1.0/24) 2. A Must filled setting	The Area Subnet of this router on OSPF Area List.
Area ID	1. IPv4 Format 2. A Must filled setting	The Area ID of this router on OSPF Area List.
Area	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

4.6.4.3. BGP Example

BGP may be used for routing within an AS. In this application it is referred to as a Gateway Interior Border Protocol, Internal BGP, or iBGP.



Scenario Application Timing

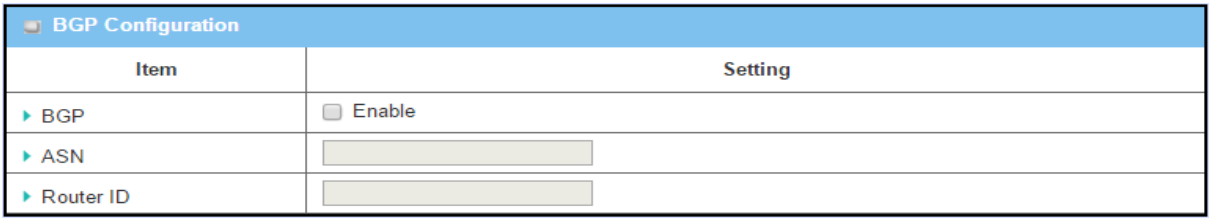
Most ISPs must use BGP to establish routing between one another (especially if they are multi-homed).

Configuration Path	[Dynamic Routing]-[BGP Configuration]			
BGP	■ ***Enable***			
Self ID	**100**			
ID	1	2	3	4
Neighbor IP	***10.101.0.1***	***10.102.0.1***	***10.103.0.1***	***10.104.0.1***
Neighbor ID	***101***	***102***	***103***	***104***
Neighbor	■ ***Enable***	■ ***Enable***	■ ***Enable***	■ ***Enable***

Scenario Operation Procedure

Enable BGP

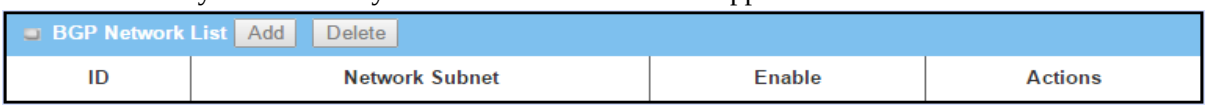
The BGP configuration setting allows user to customise the BGP protocol in the router.



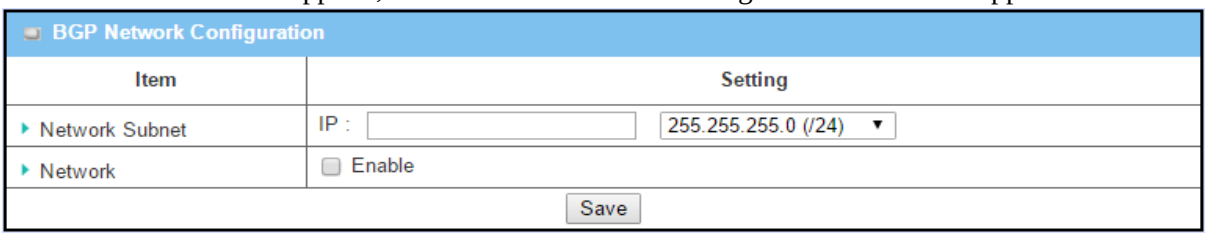
BGP Network Configuration		
Item	**Value setting**	**Description**
BGP	The box is unchecked by default	Check the **Enable** box to activate the BGP protocol.
ASN	1. Numeric String Format 2. A Mandatory Setting	The ASN Number of this router on BGP protocol.
Router ID	1. IPv4 Format 2. A Mandatory Setting	The Router ID of this router on BGP protocol.

Create/Edit BGP Network Rules

The 6402allows you to custom your BGP Network rules. It supports a maximum of 32 rule sets.



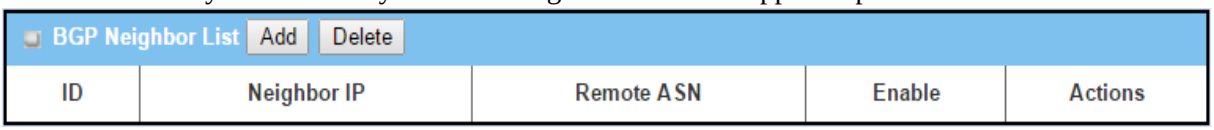
When the Add button is applied, the BGP Network Rule Configuration screen will appear.



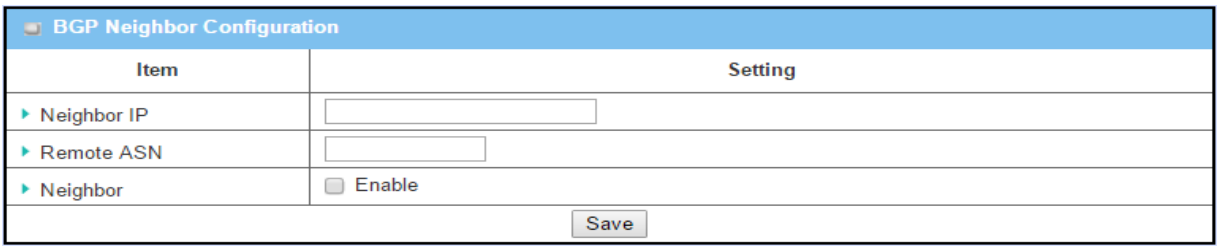
Item	Value setting	Description
Network Subnet	1. IPv4 Format 2. Mandatory setting	The Network Subnet of this router on BGP Network List. It composes of entered the IP address in this field and the selected subnet mask.
Network	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

Create/Edit BGP Neighbour Rules

The 6402 allows you to custom your BGP Neighbour rules. It supports up to 32 rule sets.



When the Add button is applied, the BGP Neighbour Rule Configuration screen will appear.



BGP Neighbour Configuration		
Item	**Value setting**	**Description**
Neighbour IP	1. IPv4 Format 2. A Mandatory Setting	The Neighbour IP of this router on BGP Neighbour List.
Remote ASN	1. Numeric String Format 2. A Mandatory setting	The Remote ASN of this router on BGP Neighbour List.
Neighbour	The box is unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration

4.6.5 Routing Information

The routing information allows network managers to view the routing table and policy routing information based on the router setting. Policy Routing Information is available when the Load Balancing function is enabled, and the Load Balance Strategy is set to 'By User Policy'.

Go to Basic Network > Routing > Routing Information Tab.

Routing Table

Destination IP	Subnet Mask	Gateway IP	Metric	Interface
192.168.1.0	255.255.255.0	0.0.0.0	0	LAN
169.254.0.0	255.255.0.0	0.0.0.0	0	LAN
239.0.0.0	255.0.0.0	0.0.0.0	0	LAN
127.0.0.0	255.0.0.0	0.0.0.0	0	lo

Routing Table		
Item	**Value setting**	**Description**
Destination IP	N/A	Routing record of Destination IP. IPv4 Format.
Subnet Mask	N/A	Routing record of Subnet Mask. IPv4 Format.
6402 IP	N/A	Routing record of 6402 IP. IPv4 Format.
Metric	N/A	Routing record of Metric. Numeric String Format.
Interface	N/A	Routing record of Interface Type. String Format.

Policy Routing Information

Policy Routing Source	Source IP	Destination IP	Destination Port	WAN Interface
Load Balance	-	-	-	-

Policy Routing Information		
Item	**Value setting**	**Description**
Policy Routing Source	N/A	Policy Routing of Source. String Format.
Source IP	N/A	Policy Routing of Source IP. IPv4 Format.
Destination IP	N/A	Policy Routing of Destination IP. IPv4 Format.
Destination Port	N/A	Policy Routing of Destination Port. String Format.
WAN Interface	N/A	Policy Routing of WAN Interface. String Format.

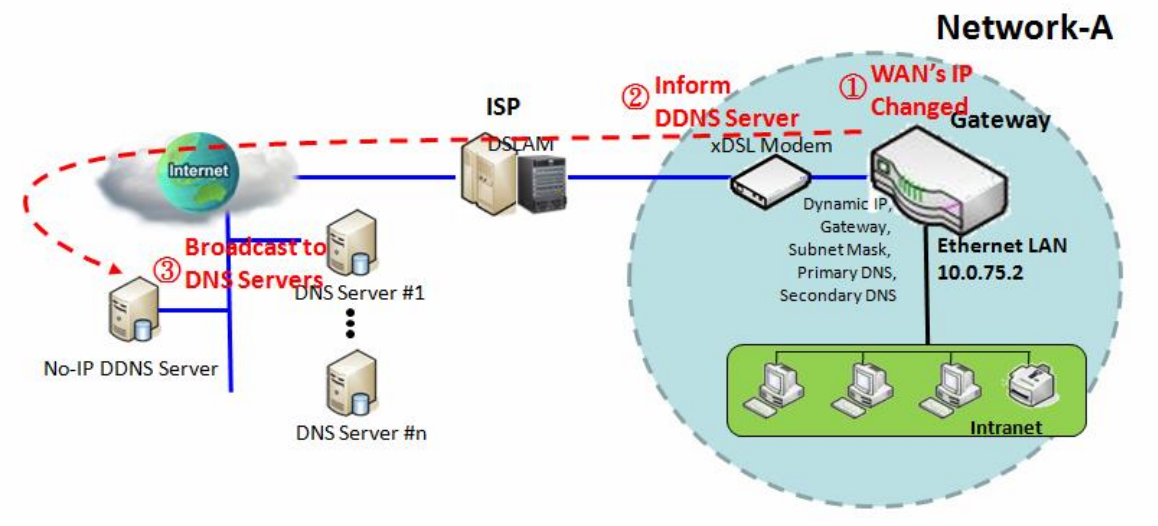
4.7 DNS & DDNS

How do users access your server if your WAN IP address changes all the time?
One way is to register a new domain name and maintain your own DNS server. Another simpler way is to apply a domain name to a third-party DDNS service provider. If you want to understand the basic concepts of DNS and Dynamic DNS, you can refer to Wikipedia website.

4.7.1. DNS & DDNS Configuration

To host your server on a dynamic (changing) IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the domain name. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect to your Internet service provider.
In short, the Dynamic DNS service allows the 6402 to alias a public dynamic IP address to a static domain name, allowing the 6402 to be more easily accessed from various locations on the Internet. The user has to register a domain name to a third-party DDNS service provider to use DDNS function.
Once the IP address of a WAN interface in the 6402 has changed, the dynamic DNS agent in the 6402 will inform the DDNS server of the new IP address. The server automatically re-maps your domain name with the changed IP address. So, other hosts in the Internet world will be able to link to your 6402 by using your domain name regardless of the changing global IP address.

Diagram Dynamic DNS Scenario



Application Example

When the IP address of the 6402 is dynamically changed by ISP, and other hosts in the Internet want to link to the 6402 by using its corresponding domain name, the 6402 must provide the dynamic DNS function to carry out the requirement.

It's necessary to open an account with a DDNS provider to be able to activate a DDNS service before the DDNS function can work in the 6402 . The 6402 asks the DDNS server to re-map the domain name and WAN's IP address of the 6402 once the IP address has been changed.

Configuration Example

Following table lists the parameter configuration for the 6402 in above diagram with "Dynamic DNS" enabled. Use default value for those parameters that are not mentioned in the table.

Configuration Path	[Dynamic DNS]-[Dynamic DNS]
DDNS	■ *Enable*
Provider	No-IP.com
Host Name	JP-NB
Username / E-mail	John Smith
Password / Key	ddnspassword

Scenario Operation Procedure

In above diagram, the 6402 is the router for Network-A with a subnet of10.0.75.0/24.

The 6402 has a LAN IP address of 10.0.75.2 and gets a dynamic IP of 118.18.81.33 for its WAN-1 interface. It serves as a NAT router.

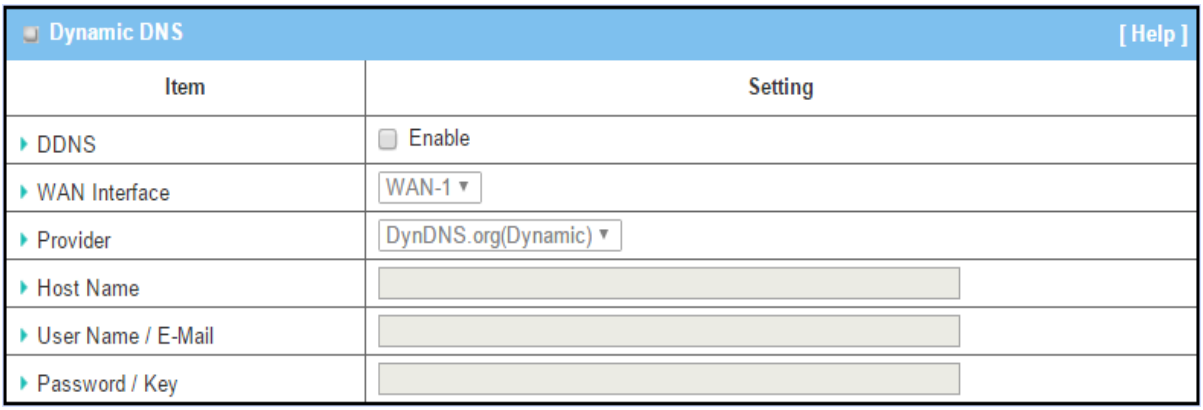
When the 6402 has booted up and has got a dynamic IP address for the WAN interface, the DDNS agent in the 6402 tries to request the DDNS server with the mapping between the domain name and the obtained WAN IP address of the 6402.

The DDNS server broadcasts the mapping to other DNS servers for their DNS hosting services on the Internet. This allows other hosts on the Internet to link to the 6402 by using the domain name.

Once the 6402 has dynamically changed its WAN IP address from its ISP, the DDNS agent tries again to request the DDNS server with the re-mapping between the domain name and the new WAN IP address of the 6402. Once again DDNS server broadcasts the new mapping to other DNS servers for provide that service on the Internet. Finally, other hosts in the Internet can still link to the 6402 by using the domain name, even the WAN IP address of the 6402 has changed.

4.7.2. Setup Dynamic DNS

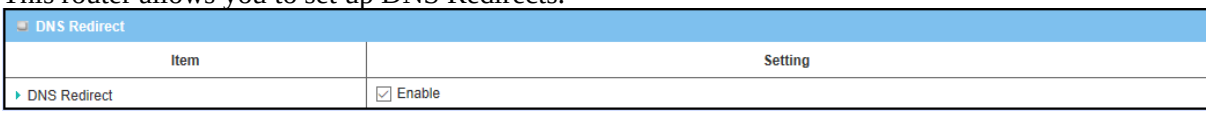
The router allows you to custom your Dynamic DNS settings.



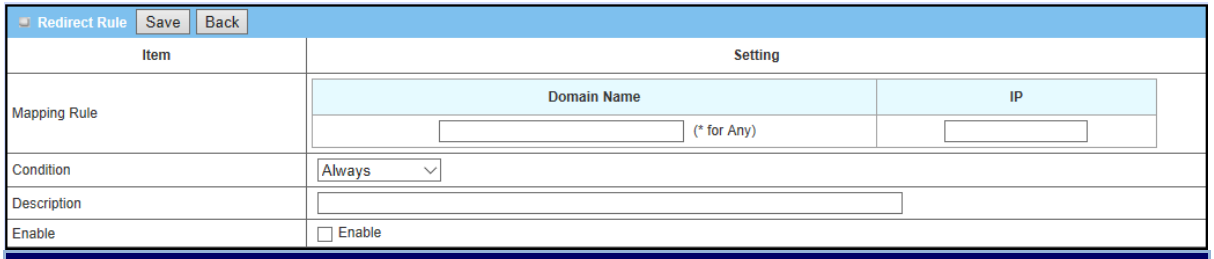
DDNS (Dynamic DNS) Configuration		
Item	**Value setting**	**Description**
DDNS	The box is unchecked by default	Select the **Enable** box to activate this function.
WAN Interface	WAN 1 is set by default	Select the WAN Interface IP Address of the router.
Provider	DynDNS.org (Dynamic) is set by default	Your DDNS provider of Dynamic DNS.
Host Name	1. String format can be any text 2. Mandatory Setting	Your registered host name of Dynamic DNS.
User Name / E-Mail	1. String format can be any text 2. Mandatory Setting	Your User name or E-mail adresses ofDynamic DNS.
Password / Key	1. String format can be any text 2. Mandatory Setting	Your Password or Key ofDynamic DNS.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

4.7.3. DNS Redirect

This router allows you to set up DNS Redirects.



Enable DNS Redirect and then Add a new Redirect Rule.



Redirect Rule		
Item	**Value setting**	**Description**
Mapping Rule	N/A	Configuration of the rule.
Domain Name	1. String format can be any text 2. Mandatory	Enter a domain name for that mapping the IP Address.
IP Address	1. IPv4 format 2. Mandatory	Enter an IP Addressfor that mapping the Domain Name.
Condition	**Always** or **WAN Blocked**	Default setting is **Always** **Always** sets the rule to be permanently active.

		WAN Blocked sets the rule to be active when WAN is inactive.
Description	Text entry	Description of the rule.
Save	N/A	Click **Save** to save the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Dynamic DNS configuration page.

4.8 QoS

The total amount of data traffic increases nowadays as the higher demand of mobile applications, like Games / Chat / VoIP / P2P / Video / Web access. In order to support the new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

4.8.1. Introduction

The goal of QoS (Quality of Service) is to prioritise incoming data and prevent data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritised data flow doesn't interfere with other data flows.

QoS helps to prioritise data as it enters the 6402, by attaching special identification marks or headers to incoming packets. QoS determines which queue the packets enter the 6402 buffers, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets rather than Web surfing data packets.

To maximize the available bandwidth the network manager must define bandwidth control rules and carefully balance the utilisation of the network bandwidth for all users.

The 6402 must satisfy the requirements of latency-critical applications, giving a guaranteed minimum bandwidth to mission critical applications and, fair bandwidth usage for higher bandwidth users.

The 6402 Security provides a Rule-based QoS to carry out these requirements.

4.8.2. QoS Configuration

This 6402 provides a large number of flexible rules for the network manager to set QoS policies. It's necessary to know three important pieces of information before you create your own policies.

- **First "who" needs to be managed?**
- **Second "what" kind of service needs to be managed?**
- **Third "how" you prioritize.**

Once you have this information, you can continue to learn functions in this section in more detail.

4.8.3. QoS Rule Configuration

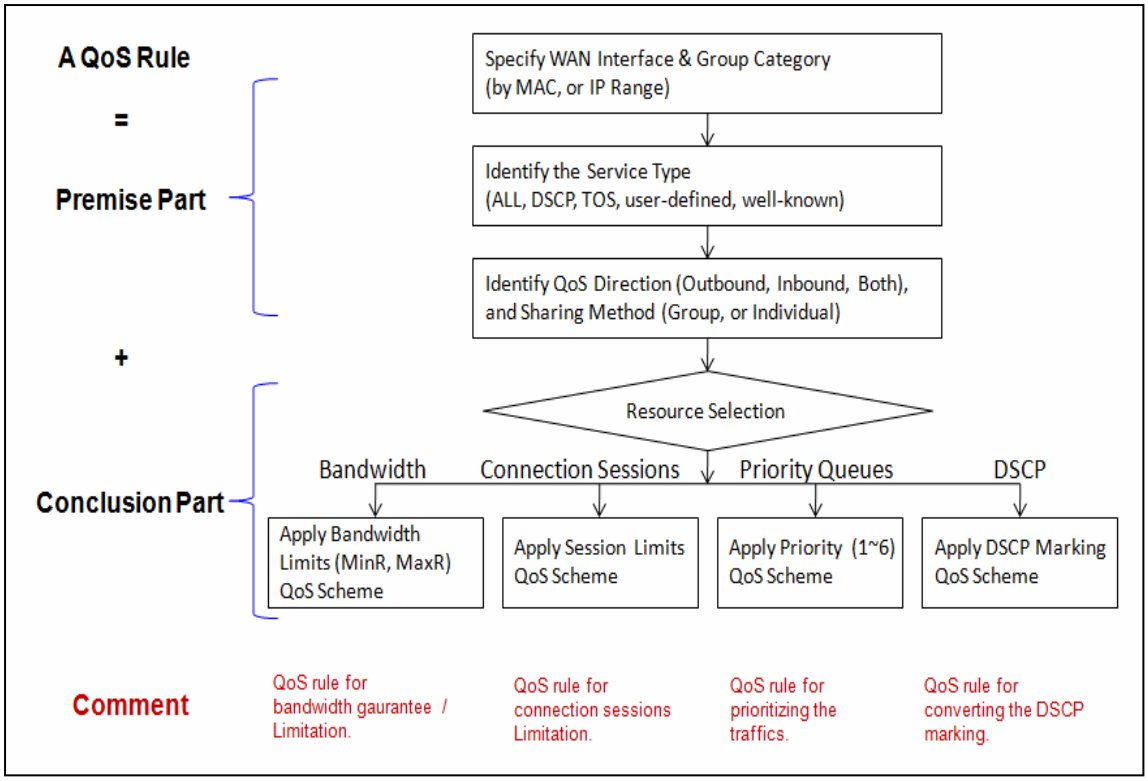
Basic Network >

When you want to add a new QoS rule or edit an already existing "QoS Rule Configuration" a window is displayed to allow you to undertake configure the setting.

The parameters in the rule include the following

- **WAN interfaces,**
- **The dedicated host group based on MAC address or IP address**
- **The dedicated kind of service packets**
- **The system resource to be distributed**
- **The corresponding control function for your specified resource**
- **The packet flow direction, the sharing method for the control function**
- **The integrated time schedule rule and the rule activation.**

The following diagram illustrates how to organize a QoS rule.



In the above diagram, a QoS rule is organised by the premise part and the conclusion part.
In the premise part, you must specify the WAN interface, host group, service type in the packets, packet flow direction to be watched and the sharing method of group control or individual control.
In the conclusion part, you must determine which kind of system resource to distribute and the control function based on your chosen resources for the rule.

The Rule-based QoS has following features.

Multiple Group Categories

Specify the group category in a QoS rule for the target objects to be applied on.
Group Category can be based on VLAN ID, MAC Address, IP Address, Host Name or Packet Length.

Differentiated Services

Specify the service type in a QoS rule for the target packets to be applied on.
Differentiated services can be based on 802.1p, DSCP, TOS, VLAN ID, User-defined

Services and Well-known Services.

Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110), Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), NetMeeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723).

Available Control Functions

There are 4 resources can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources.
For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth.
For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.

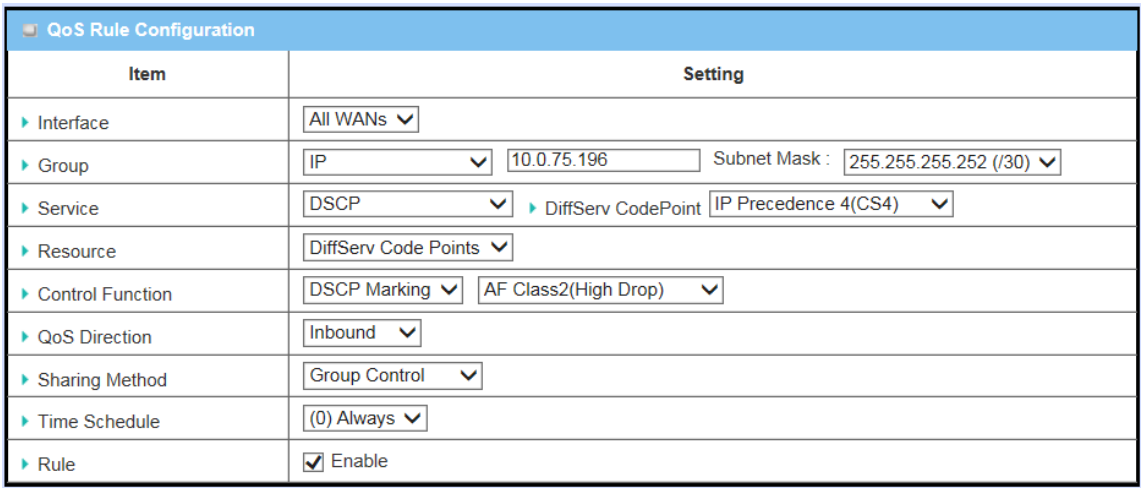
Individual / Group Control

One QoS rule can be applied to an individual member or whole group in the target group.
This feature depends on the version of software in the 6402.

Outbound / Inbound Control

One QoS rule can be applied to the outbound or inbound direction of packet flow or to both. This feature depends on the version of software installed Two QoS rule examples are listed below.

"DSCP" Type of QoS Rule Example



Scenario Application Timing

When the 6402 Manager wants to convert the code point value, "IP Precedence 4(CS4)", in the packets from a client hosts (IP 10.0.75.196~199) to the code value, "AF Class2 (High Drop)", they can use the "Rule-based QoS" function to carry out this rule by defining a QoS rule as shown in the diagram above.

Scenario Description

Convert the code point value from "IP Precedence 4(CS4)" to "AF Class2(High Drop)" for incoming packets from some client hosts in the Intranet.

Parameter Setup Example

The following tables list the parameter configuration as an example for the 6402 in above diagram with "Rule-based QoS" enabling.
Use default value for those parameters that are not mentioned in the tables.

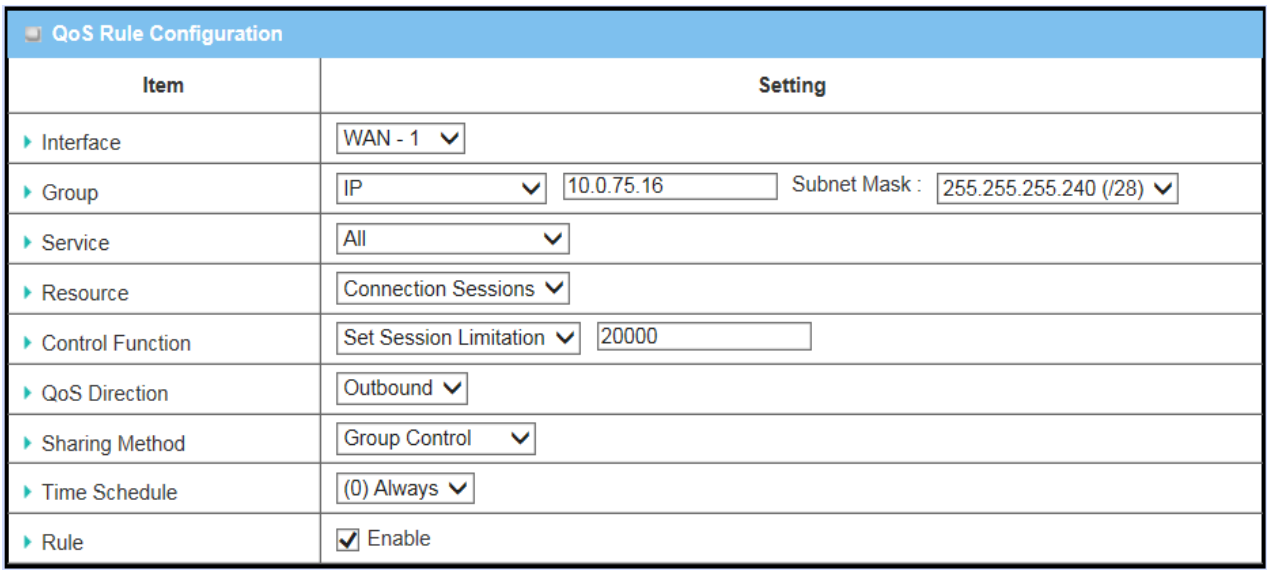
Configuration Path	[Rule-based QoS]-[Configuration]
Rule-based QoS	■ ***Enable***
Flexible Bandwidth Management	■ ***Enable***

Configuration Path	[Rule-based QoS]-[QoS Rule Configuration]
Interface	***All WANs***
Group	***IP 10.0.75.196***Subnet Mask: ***255.255.255.252 (/30)***
Service	***DSCP***DiffServ Code Point ***IP Precedence 4(CS4)***
Resource	***DiffServ Code Points***
Control Function	***DSCP Marking AF Class2(High Drop)***
QoS Direction	***Inbound***
Sharing Method	***Group Control***
Time Schedule	***(0) Always***
Rule	■ ***Enable***

Scenario Operation Procedure

This rule means IP packets from all WAN interfaces to the LAN IP address 10.0.75.196 ~ 10.0.75.199 (which have DiffServ code points with “IP Precedence 4(CS4)” value), will be modified by the “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

"Connection Sessions" Type of QoS Rule Example



Scenario Application

When the 6402 manager wants to limit the connection sessions from some client hosts for example(IP 10.0.75.16~31) to 20000 sessions in total for access to the Internet, they can use the "Rule-based QoS" facility and the ‘Control Resource’ tab to implement this feature as shown in above diagram.

Parameter Setup Example

The following tables list the configuration for the 6402 in above diagram with "Rule-based QoS" enabling.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[Rule-based QoS]-[Configuration]
Rule-based QoS	■ ***Enable***
Flexible Bandwidth Management	■ ***Enable***
Configuration Path	**[Rule-based QoS]-[QoS Rule Configuration]**
Interface	***WAN-1***
Group	***IP 10.0.75.16***Subnet Mask: ***255.255.255.240 (/28)***
Service	***All***
Resource	***Connection Sessions***
Control Function	***Set Session Limitation 20000***
QoS Direction	***Outbound***
Sharing Method	***Group Control***
Time Schedule	***(0) Always***
Rule	■ ***Enable***

Scenario Operation Procedure

This rule defines that all client hosts, whose IP address is in the range of 10.0.75.16~31, can access the Internet via "WAN-1" interface under the limitation of the maximum 20000connection sessions at any time

4.8.4. QoS Configuration Setting

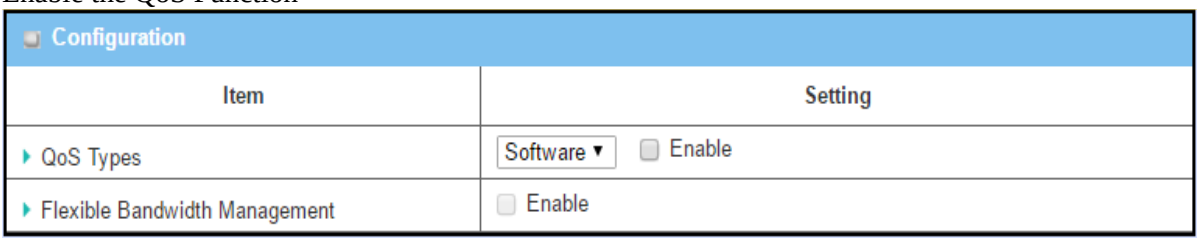
In the "QoS Configuration" page, there are some configuration windows for the QoS function. These are the;

- "Configuration" window,
- “System Resource Configuration” window,
- "QoS Rule List" window, and
- "QoS Rule Configuration" window.

The "Configuration" window can let you activate the Rule-based QoS function.

- First- you can enable the "Flexible Bandwidth Management" (FBM) feature for better utilization of system bandwidth using the FBM algorithm.
- Second -the “System Configuration” window can let you configure the total bandwidth and session of each WAN.
- Third -the "QoS Rule List" window lists all your defined QoS rules. At last, the "QoS Rule Configuration" window can let you define one QoS rule.

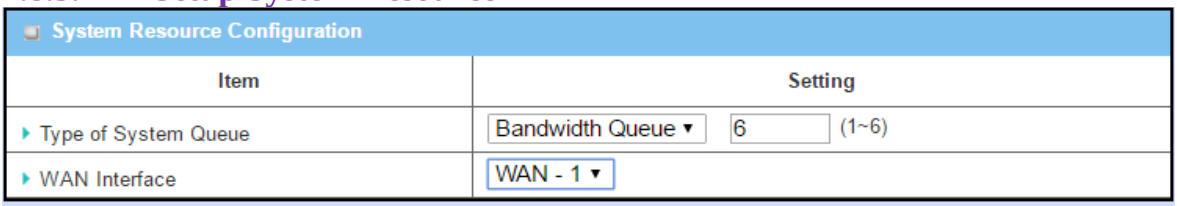
Go to Basic Network > QoS > Configuration tab.
Enable the QoS Function

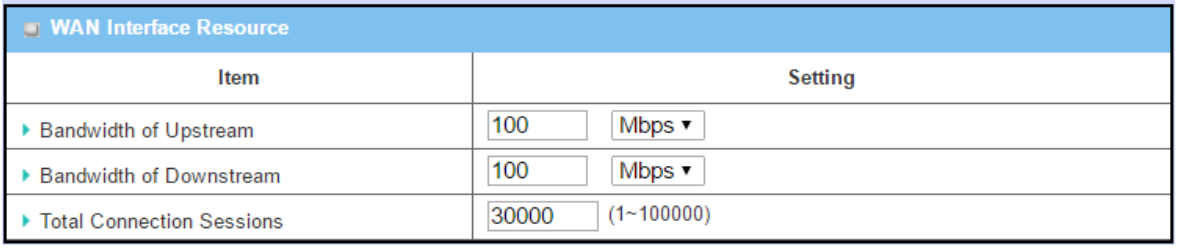


Configuration		
Item	**Value Setting**	**Description**
QoS Type	1. **Software** is selected by default. 2. The box is unchecked by default.	Select the QoS Type from the dropdown list, and then click **Enable** box to activate the QoS function. The default QoS type is set to **Software** QoS. For some models, there is another option for other **Hardware** QoS models.
Flexible Bandwidth Management	The box is unchecked by default	Click the **Enable** box to activate the Flexible Bandwidth Management function.
Save	N/A	Click the **Save** button to save the settings.

Check the "Enable" box to activate the "Rule-based QoS" function.
Also enable the FBM feature when needed. When FBM is enabled, the 6402 adjusts the bandwidth dynamically based on current bandwidth usage situation to reach maximum network performance while remaining transparent to all users.
The bandwidth subscription profiles of all current users are considered in the system's automatic adjusting algorithm.
Ensure QoS and Bandwidth are enabled and saved to further configure the detailed QoS settings.

4.8.5. Setup System Resource



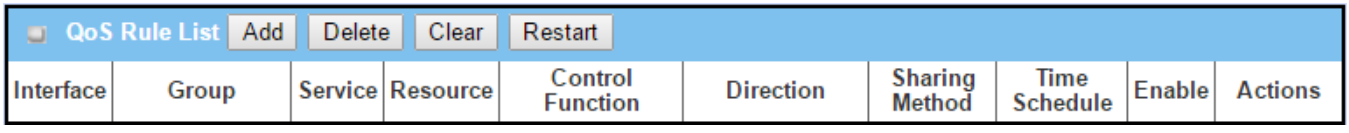


System Resource Configuration		
Item	**Value Setting**	**Description**
Type of System Queue	1. A Mandatory Setting 2. **Bandwidth Queue**, and**6** are set by default.	Define the system queues that are available for the QoS settings. The supported type of system queues are **Bandwidth Queue** and **Priority Queues.** ***Value Range***: 1 ~ 6.
WAN Interface	**WAN-1** is selected by default.	Select the WAN interface and then the following **WAN Interface Resource** screen will show the related resources for configuration. **Bandwidth of Upstream / Downstream** Specify total upload / download bandwidth of the selected WAN. Value Range: For Gigabit Ethernet:1~1024000Kbps, or 1~1000Mbps; For Fast Ethernet: 1~102400Kbps, or 1~100Mbps; For 3G/4G: 1~153600Kbps, or 1~150Mbps. **Total Connection Sessions** Specify total connection sessions of the selected WAN. *Value Range*: 1 ~ 10000.
Save	N/A	Click the **Save** button to save the settings.

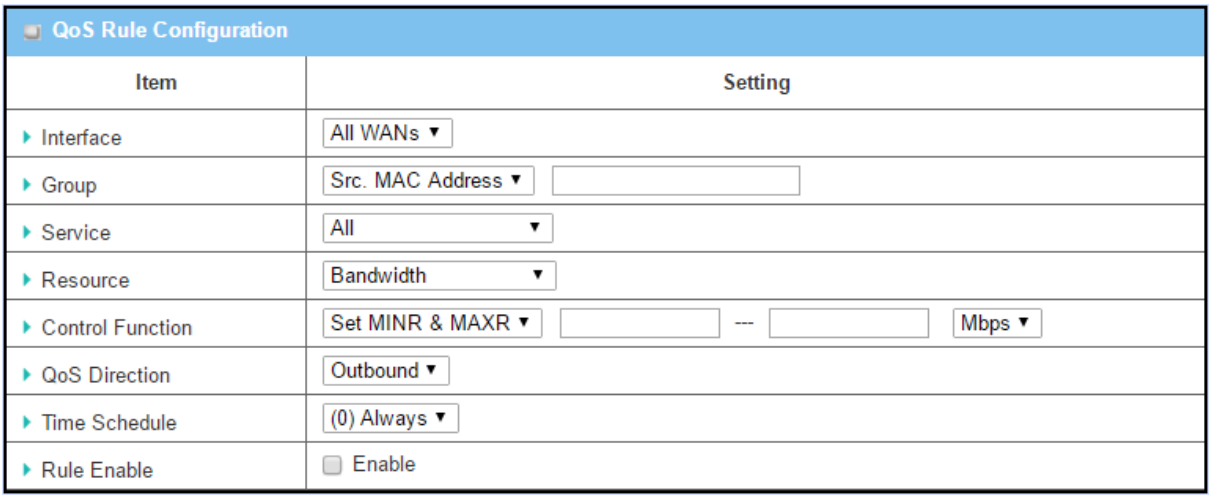
Each WAN interface should be configured carefully for its upstream bandwidth, downstream bandwidth and maximum number of connection sessions.

4.8.6. QoS Rule List

After enabling the QoS function and configuring the system resources, the network manager has to further specify some QoS rules to provide a better service for traffic. The 6402 supports up to a maximum of 128 rule-based QoS rule sets.



When the Add button is applied, QoS Rule Configuration screen will appear.



QoS Rule Configuration		
Item	**Value setting**	**Description**
Interface	1. Mandatory 2. **All WANs** are selected by default.	Specify the WAN interface to apply the QoS rule. Select **All WANs** or a certain **WAN-n** to filter the packets entering to or leaving from the interface(s).
Group	1. Mandatory 2. **Src. MAC Address** is selected by default.	Specify the **Group** category for the QoS rule. It can be **Src. MAC Address**, **IP**, or **Host Name.** Select **Src. MAC Address** to prioritize packets based on MAC; Select **IP** to prioritize packets based on IP address and Subnet Mask; **Host Name** to prioritize packets based on a group of a pre-configured group of host from the dropdown list. If the dropdown list is empty, ensure if any group is pre-configured. **Note:** The required host groups must be created in advance and corresponding QoS checkbox in the **Multiple Bound Services** field is checked before the **Host Group** option become available. Refer to **Object Definition > Grouping > Host Grouping.**
Service	1. Mandatory 2. **All** is selected by default.	Specify the service type of traffics that have to be applied with the QoS rule. It can be **All**, **DSCP**, **TOS**, **User-defined Service**, or **Well-known Service**. Select **All** for all packets. Select **DSCP** for DSCP type packets only. Select **TOS** for TOS type packets only. You have to select a service type (**Minimize-Cost**, **Maximize-Reliability**, **Maximize-Throughput**, or **Minimize-Delay**) from the dropdown list as well. Select **User-defined Service** for user-defined packets only. You have to define the port range and protocol as well. Select **Well-known Service** for specific application packets only. You have to select the required service from the dropdown list as well.
Resource, and **Control Function**	Mandatory	Specify the Resource Type and corresponding Control function for the QoS rule. The available Resource options are **Bandwidth**, **Connection Sessions**, **Priority Queues**, and **DiffServ Codepoints**. **Bandwidth**: Select **Bandwidth** as the resource type for the QoS Rule, and you have to assign the min rate, max rate and rate unit as the bandwidth settings in the **Control Function** / **Set MINR & MAXR** field. **Connection Sessions**: Select **Connection Sessions** as the resource type for the QoS Rule, and you have to assign supported session number in the **Control Function** / **Set Session Limitation** field. **Priority Queues**: Select **Priority Queues** as the resource type for the QoS Rule, and you have to specify a priority queue in the **Control Function** / **Set Priority** field. **DiffServ Code Points**: Select **DiffServ Code Points** as the resource type for the QoS Rule, and you have to select a DSCP marking from the **Control Function** / **DSCP Marking** dropdown list.
QoS	1. Mandatory	Specify the traffic flow direction for the packets to apply the QoS rule.

Direction	2. **Outbound** is selected by default.	It can be **Outbound**, **Inbound**, or **Both**. **Outbound**: Select **Outbound** to prioritise the traffic going to the Internet via the specified interface. Under such situation, the host are specified in the Group field is a source group. **Inbound**: Select **Inbound** to prioritise the traffic coming from the Internet via the specified interface. Under such situation, the hosts specified in the Group field is a destination group. **Both**: Select **both** to prioritise the traffics passing through the specified interface, both Inbound and Outbound are considered. Under such situation, the hosts specified in the Group field can be a source or destination group.
Sharing Method	1. Mandatory 2. **Group Control** is selected by default.	Specify the preferred sharing method for how to apply the QoS rule on the selected group. It can be **Individual Control** or **Group Control**. **Individual Control**: If **Individual Control** is selected, each host in the group will have his own QoS service resource as specified in the rule. **Group Control**: If **Group Control** is selected, all the group hosts share the same QoS service resource.
Time Schedule	1. Mandatory 2. **(0) Always** is selected by default.	Apply **Time Schedule** to this rule, otherwise leave it as (0) **Always**.(refer to **Object Definition > Scheduling > Configuration** settings)
Rule Enable	The box is unchecked by default.	Click **Enable** box to activate this QoS rule.
Save	N/A	Click the **Save** button to save the settings.

4.9 Redundancy

4.9.1. VRRP

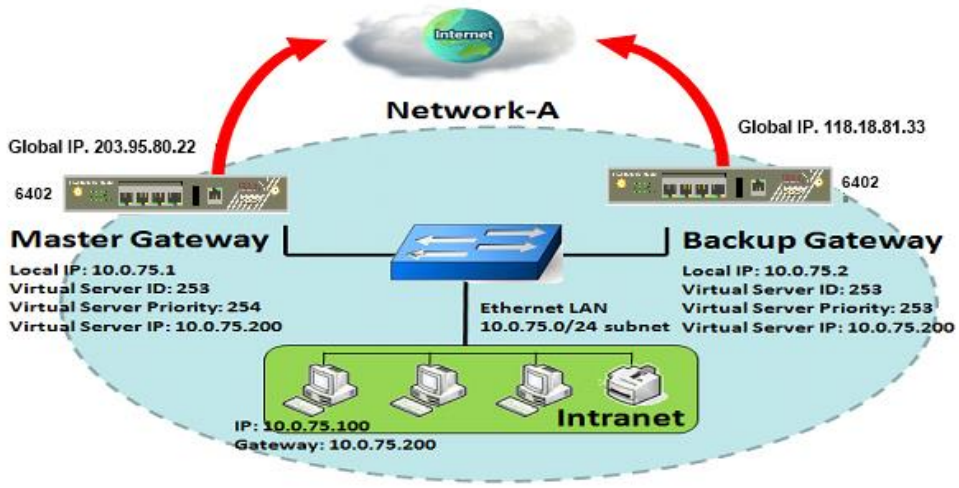
In engineering, redundancy is the duplication of critical components or functions of a system with the intention of increasing reliability of the system, usually in the form of a backup or fail-safe. In an IP network, the access router is a critical part of the networking system.

To provide a redundant solution requires a second 6402 router which backups the master 6402 and takes over the routing task if the master 6402 has failed. It does this by using the protocol VRRP (Virtual Router Redundancy Protocol)
VRRP allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default 6402 selections on an IP network.

The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group.
The default 6402 of a participating host is assigned as a virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.

A group of physical VRRP 6402 routers combine together to play a virtual server with one unique virtual server ID and one unique virtual server IP address. However, these VRRP 6402s have their own priority values to serve as the sequence for backing up the master 6402.

The 6402 with a VRRP function can join one group of redundant 6402s to serve as the backup unit for the master 6402. Fill in the same values of the virtual server ID's and IP addresses for these 6402s, and each 6402 owns its own priority as the sequence in the backup list. They construct a VRRP redundant 6402 group. Following diagram illustrates the group example with two member 6402s.



Application Example

Each member 6402 connects to different ISP to ensure redundant connections to the Internet. This ensures the internet connection is reliable even if the master connection fails.

If the master 6402 has a failed Internet connection, the backup 6402 with the highest priority among the routers with working Internet connections will take over the connection and become the master.

If the original 6402 recovers its link to the Internet and its priority if higher than the unit which has just become the master, then the link will return to the original 6402 and that will once again become the master.

Configuration Example

The following tables list the configuration as an example for the 6402sin above diagram. Use default values for those parameters that are not mentioned in the tables.

Master 6402

Configuration Path	[Ethernet LAN]-[Configuration] ([Basic Network]-[LAN&VLAN])
LAN IP Address	*10.0.75.1*
Subnet Mask	*255.255.255.0 (/24)*

Configuration Path	[VRRP]-[Configuration]
VRRP	■ *Enable*
Virtual Server ID	*253*
Priority of Virtual Server	*254*
Virtual Server IP Address	*10.0.75.200*

Backup 6402

Configuration Path	[Ethernet LAN]-[Configuration] ([Basic Network]-[LAN&VLAN])
LAN IP Address	*10.0.75.2*
Subnet Mask	*255.255.255.0 (/24)*

Configuration Path	[VRRP]-[Configuration]
VRRP	■ *Enable*
Virtual Server ID	*253*
Priority of Virtual Server	*253*
Virtual Server IP Address	*10.0.75.200*

Scenario Operation Procedure

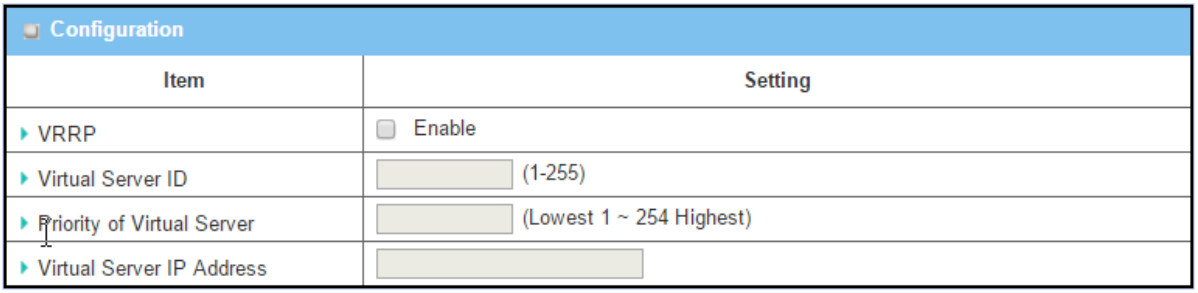
In the diagram above the Master 6402 Gateway and the Backup 6402 Gateway are the redundant router group of Network-A and the subnet of its Intranet is 10.0.75.0/24. The master 6402 has the IP address of 10.0.75.1 for LAN interface,203.95.80.22 for WAN-1 interface. However, the backup 6402 has the IP address of 10.0.75.2 for LAN interface,118.18.81.33 for WAN-1 interface. They both serve as NAT routers.

Specify the ID of VRRP virtual server to be "253" and its IP address to be "10.0.75.200". The priority of the master 6402 is 254 and it is larger than 253 which is what's set for the backup 6402.
Initially, all data from the local subnet will go through the master 6402 with the highest priority. Once the master's Internet connection is broken, the backup 6402 will take over as master and become the Gateway to the Internet.
If the original 6402 with its higher priority than current master 6402 recovers from its broken Internet connection, it will take over transmitting data again.

4.9.2. VRRP Setting

The Virtual Router Redundancy Protocol (VRRP) setting allows user to assign available routers to participating hosts automatically.

Go to Basic Network > Redundancy > VRRP tab.



VRRP		
Item	**Value setting**	**Description**
VRRP	The box is unchecked by default.	Check the **Enable** box to activate this VRRP function.
Virtual Server ID	1. Numeric String Format 2. A Must filled setting	Specify the Virtual Server ID on VRRP of the 6402. The value range is from 1 to 255.
Priority of Virtual Server	1. numeric String Format 2. A Must filled setting	Specify the Priority of Virtual Server on VRRP of the 6402. The value range is from 1 to 254.
Virtual Server IP Address	1. IPv4 Format 2. A Mandatory setting	Specify the Virtual Server IP Address on VRRP of the 6402.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.

This page left blank intentionally

SECTION 5

OBJECT DEFINITION

5.1 Object Definition

5.1.1. Scheduling

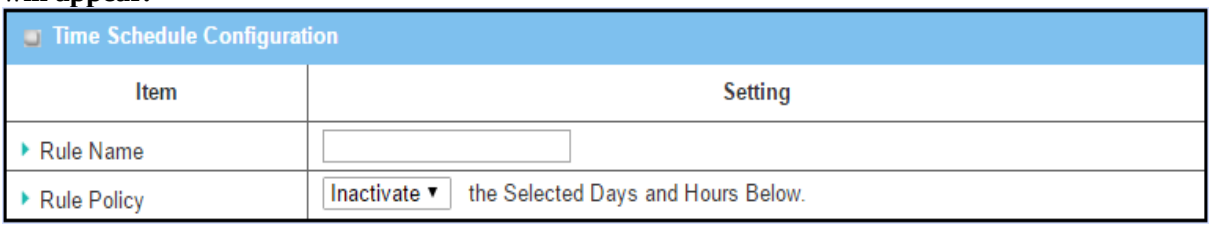
5.1.1.1. Time Schedule List

Scheduling provides the ability to add or delete time scheduled rules, which can be applied to other functionality.

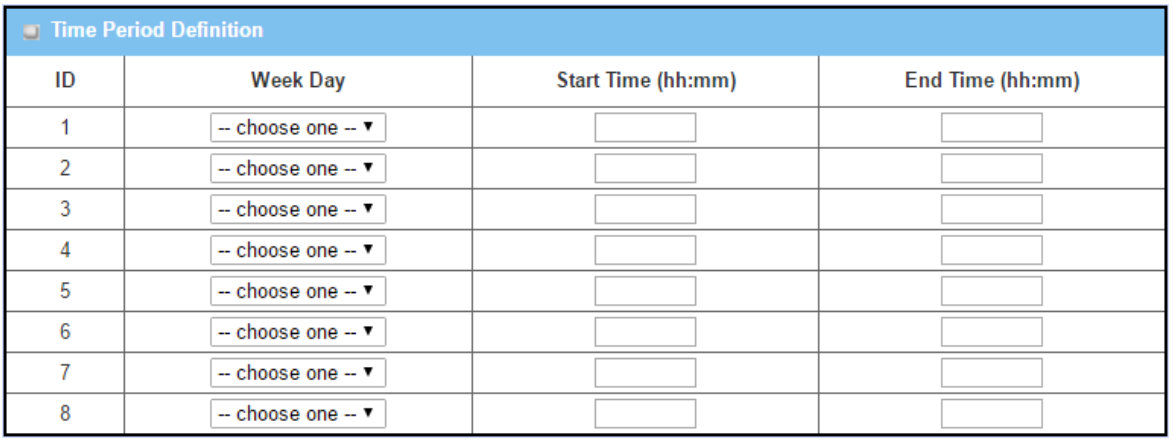
Go to Object Definition > Scheduling > Configuration tab.

Button description		
Item	**Value setting**	**Description**
Add	N/A	Click the **Add** button to configure time schedule rule
Delete	N/A	Click the **Delete** button to delete selected rule(s)

When Add button is applied, Time Schedule Configuration and Time Period Definition screen will appear.



Time Schedule Configuration		
Item	**Value Setting**	**Description**
Rule Name	String: any text	Set rule name
Rule Policy	Default Inactivate	Inactivate/activate the function been applied to in the time period below

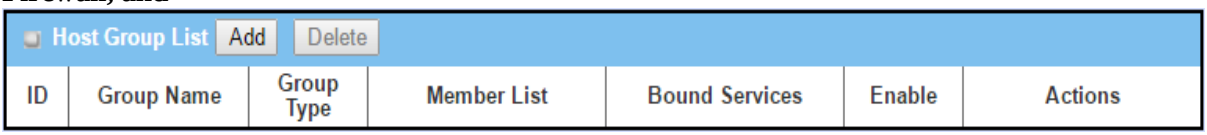


Time Period Definition		
Item	**Value Setting**	**Description**
Week Day	Select from menu	Select everyday or one of weekday
Start Time	Time format (hh :mm)	Start time in selected weekday
End Time	Time format (hh :mm)	End time in selected weekday

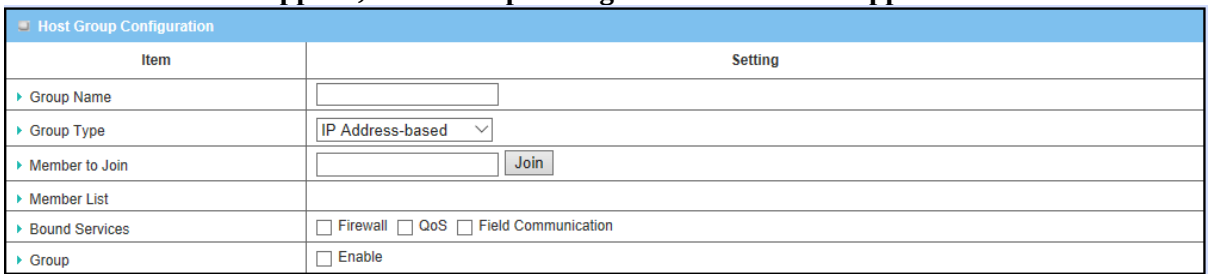
5.2 GROUPING

5.2.1. Host Grouping

Go to Object Definition >Grouping >Host Grouping tab.
The Host Grouping function allows user to make host group for some services, such as QoS, Firewall, and



When Add button is applied, Host Group Configuration screen will appear.



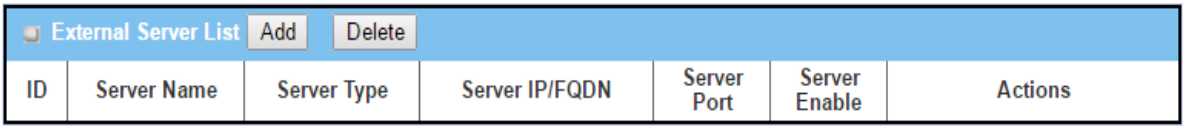
Host Group Configuration		
Item	**Value setting**	**Description**
Group Name	1. String format can be any text 2. Mandatory Setting	Enter a group name for the rule, use a name that is easy for you to understand. ***Value Range*:** at least 1 character is required.
Group Type	**1. IP Address-based** is selected by default. 2. Mandatory Setting	Select the member type for the host group. It can be **IP Address-based**, **MAC Address-based**, or **Host Name-based**. When **IP Address-based** is selected, only an IP address can be added for the Member to Join. When **MAC Address-based** is selected, only MAC address can be added in **Member to Join.** When **Host Name-based** is selected, only host name can be added in **Member to Join.**
Member to Join	N/A	Add the members to the group in this field. You can enter the member information as specified in the Member Type above and press the **Join** button to add. Only one member can be added at a time, so you must add the members of the group one by one.
Member List	NA	This field will indicate the hosts (members) contained in the group.
Bound Services	The boxes are unchecked by default	Binding the services that the host group can be applied. If you enable the **Firewall**, the produced group can be used in firewall service. Same as enabling **QoS** and **Bus& Protocol**.
Group	The box is un checked by default	Check the **Enable** checkbox to activate the host group rule. So that the group can be bound to selected service(s) for further configuration.

5.3 External Server

Allows the user to add an external server.

Go to Object Definition > External Server > External Server tab.

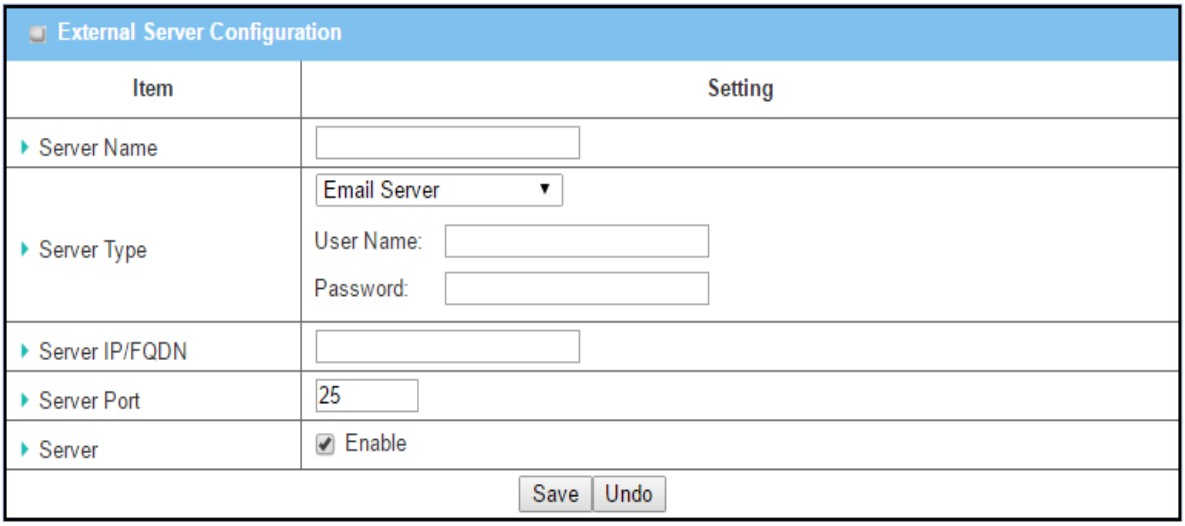
Create external server



When **Add** button is applied, **External Server Configuration** screen will appear.

The 6402 allows configuration of a remote RADIUS Server for VPN authentication and also management authentication of the 6402.

Note. The RADIUS Server serves to authenticate network managers wanting to access the 6402 management.



External Server Configuration		
Item	**Value setting**	**Description**
Sever Name	1. String format can be any text 2. A Mandatory Setting	Enter a server name. Enter a name that is easy for you to understand.
Server IP/FQDN	A Mandatory Setting	This field is to specify the external server IP.
Server Port	A Mandatory Setting	This field is to specify the external server port.
Server Type	A Mandatory Setting	Specify the Server Type of the external server and enter the required settings for the accessing the server.
		Email Server (A Mandatory setting) : When **Email Server** is selected, **User Name**, and **Password** are also required. **User Name** (String format: any text) **Password** (String format: any text) **RADIUS Server** (A Mandatory setting) : When **RADIUS Server** is selected, the following settings are also required. **Accounting Port** (A Mandatory Setting) Primary: **Shared Key** (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60.

		Idle Timeout: (By default 1) The values must be between 1 and 26. Secondary:
		Shared Key (String format: any text) Authentication Protocol (By default CHAP is selected) Session Timeout (By default **1**) The values must be between 1 and 60. Idle Timeout: (By default 1) The values must be between 1 and 26.
		Active Directory Server (A Mandatory setting) : When **Active Directory Server** is selected, **Domain** setting is also required. **Domain** (String format: any text)
		LDAP Server (A Mandatory setting) : When **LDAP Server** is selected, the following settings are also required. **Base DN** (String format: any text) **Identity** (String format: any text) **Password** (String format: any text)
		UAM Server (A Mandatory setting) : When **UAM Server** is selected, the following settings are also required. **Login URL** (String format: any text) **Shared Secret** (String format: any text) **N/AS/Gateway ID** (String format: any text) **Location ID** (String format: any text) **Location Name** (String format: any text)
		TACACS+ Server (A Mandatory setting) : When **TACACS+ Server** is selected, the following settings are also required. **Shared Key** (String format: any text) **Session Timeout** (String format: any number) The values must be between 1 and 60.
		SCEP Server (A Mandatory setting) : When **SCEP Server** is selected, the following settings are also required. **Path** (String format: any text, by default **cgi-bin** is filled) **Application** (String format: any text, by default **pkiclient.exe** is filled)
Server IP/FQDN	A Mandatory Setting	Specify the IP address or FQDN used for the external server.
Server Port	A Mandatory Setting	Specify the Port used for the external server. If you selected a certain server type, the default server port number will be set. For **Email Server** 25 will be set by default; For **Syslog Server**, port514 will be set by default; For **RADIUS Server**, port1812 will be set by default; For **Active Directory Server**, port389 will be set by default; For **LDAP Server**, port389 will be set by default; For **UAM Server**, port80 will be set by default; For **TACACS+ Server**, port49 will be set by default; For **SCEP Server**, port80 will be set by default;
Server	The box is checked by default	Click **Enable to** activate this External Server.
Save	N/A	Click the **Save button** to save the settings
Undo	N/A	Click the **Undo** button to cancel the settings
Refresh	N/A	Click the **Refresh** button to refresh the external server list.

5.3.1. Adding an Authentication Server

The 6402 can be configured to allow external authentication of management access either using an external RADIUS server or TACACS+ server. This document will only cover configuration of the 6402, please see the documentation of the RADIUS/TACACS+ 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.

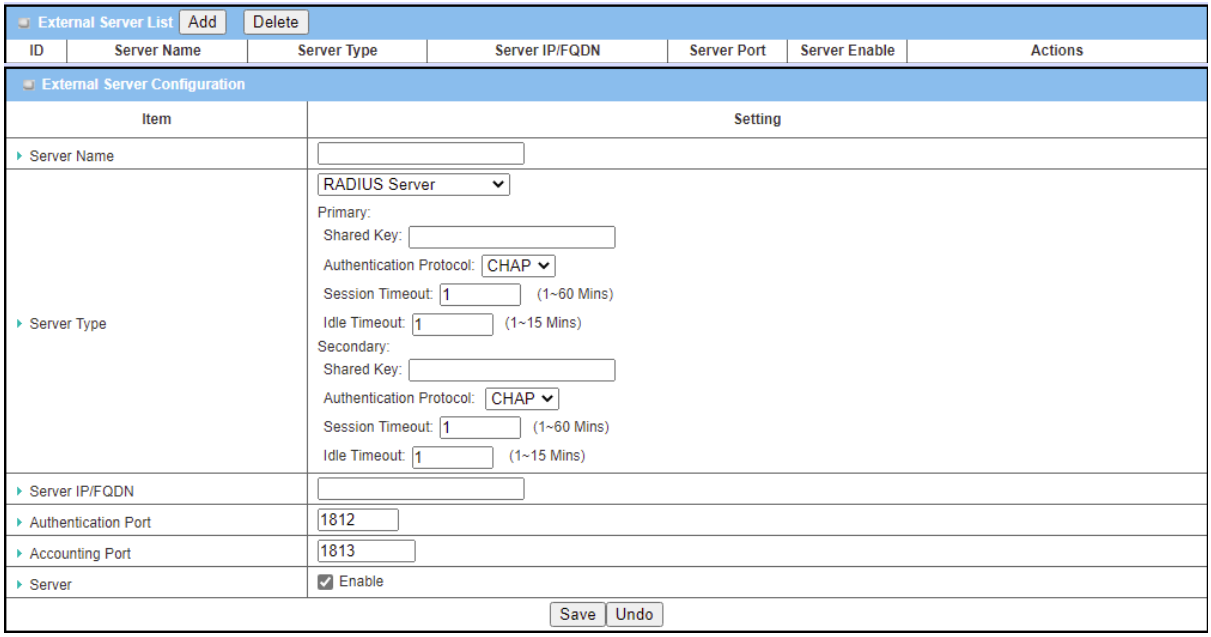
RADIUS is a client/server protocol that runs in the application layer and can use either TCP or UDP. The 6402 uses UDP for authentication requests to a RADIUS server.

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.

Note: The 6402 is configured with a username and password (default is *admin* for both username and password) which will always allow access to management of the 6402 in the event of the external authentication server being unavailable or offline. This user access will be logged by the external server when the server is available to the 6402, so it is recommended that this user is configured on the RADIUS server to provide accurate user logs.

5.3.1.1. Configure External RADIUS Server

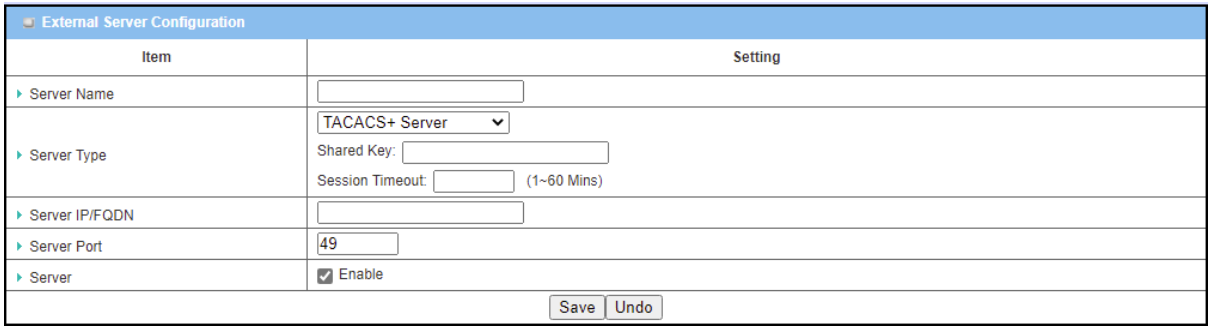
The first step is to configure the external server.
Go to **Object Definition > External Server**
Select Add to add the new server and select server type as RADIUS



External RADIUS Server Configuration		
Item	**Value setting**	**Description**
Server Name	Any alphanumeric string	This is the name shown in the 6402 to differentiate different servers.
Server Type	RADIUS Server	List of possible server types, selecting different type will change the other Items available on screen.
Primary Shared Key	Alphanumeric string	This is the PSK that is exactly the same as used on the RADIUS Server
Authentication Protocol	PAP or CHAP	Protocol used for authentication. CHAP is default
Session Timeout	1 to 60 minutes	Total number of minutes an authenticated user's session can last before being terminated.
Idle Timeout	1 to 15 minutes	Number of consecutive inactive minutes before an authenticated user's session is terminated.
Secondary Shared Key	Alphanumeric string	Secondary PSK used if the primary fails to authenticate.
Server IP/FQDN	IP address or domain name	IP address of Fully Qualified Domain Name of the RADIUS Server
Authentication Server	Number 0 to 65535	RADIUS Server Authentication UDP Port number, default is 1812
Accounting Port	Number 0 to 65535	RADIUS Server Accounting UDP Port number, default is 1813
Server	Enable	Tick to enable this External server configuration.

5.3.1.2. Configure an External TACACS+ Server

As an alternative to a RADIUS Server, users can be authenticated by an external TACACS+ Server. The details here are provided to show TACACS+ as a possibility for user management.

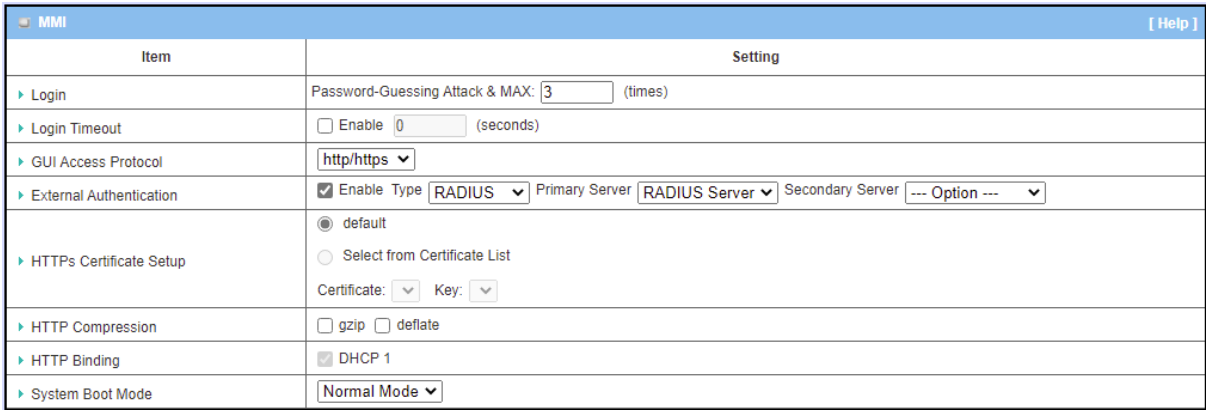


External TACACS+ Server Configuration		
Item	**Value setting**	**Description**
Server Name	Any alphanumeric string	This is the name shown in the 6402 to differentiate different servers.
Server Type	TACACS+ Server	Select TACACS+ Server from the list
Shared Key	Alphanumeric string	This is the key shared with the external TACACS+ server
Session Timeout	1 to 60 minutes	Total number of minutes before a user session is terminated
Server IP/FQDN	IP address or domain name	IP address of Fully Qualified Domain Name of the TACACS+ Server
Server Port	Number 0 to 65535	TACACS+ server's TCP port number, default if 49
Server	Enable	Tick to enable this External server configuration

5.3.1.3. Configuring the Authentication Server

Once the External Server has been configured the 6402 requires the external authentication to be enabled and the server selected.

Go to Administration > System Operation > Password & MMI tab > MMI > External Authentication



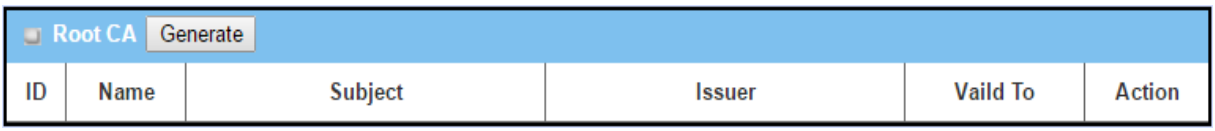
External Authentication Configuration		
Item	**Value setting**	**Description**
Enable	Tic	Tick to enable External Authentication
Type	RADIUS or TACACS+	Select the required external server
Primary Server	List of configured servers	Select the required, previously configured, server
Secondary Server	List of configured servers	Select the required, previously configured, server. Optional
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

5.4 Certificates

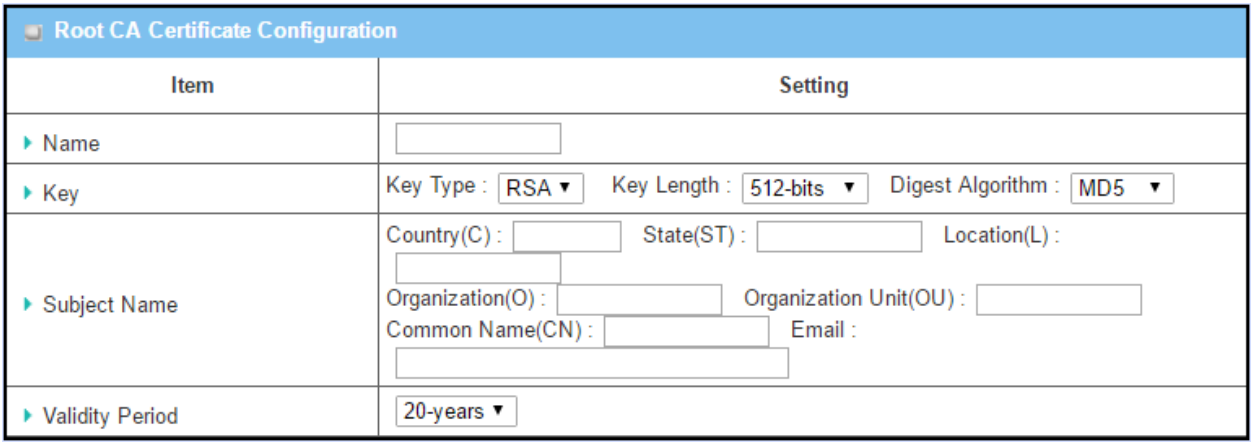
5.4.1. Generating a Root CA

is the top-most certificate of the tree, the private key of which is used to "sign" other certificates.

Go to Object Definition > Certificate > Configuration tab > Create root CA



When the **Generate** button is applied, the **Root CA Certificate Configuration** screen will appear. The information to be filled into the root CA includes the name, key, subject name and validity.



Root CA Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. Mandatory Setting	Enter a Root CA Certificate name. It will be a certificate file name
Key	A Mandatory Setting	This field is to specify the key attribute of certificate. **Key Type** to set public-key cryptosystems. It only supports RSA now. **Key Length** to set as the size measured in bits of the key used in a cryptographic algorithm. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates
Subject Name	A Mandatory Setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address style.
Validity Period	A Mandatory Setting	This field is to specify the validity period of certificate.

Note: CSR = Certificate Signing request

5.4.3.1. Setup SCEP

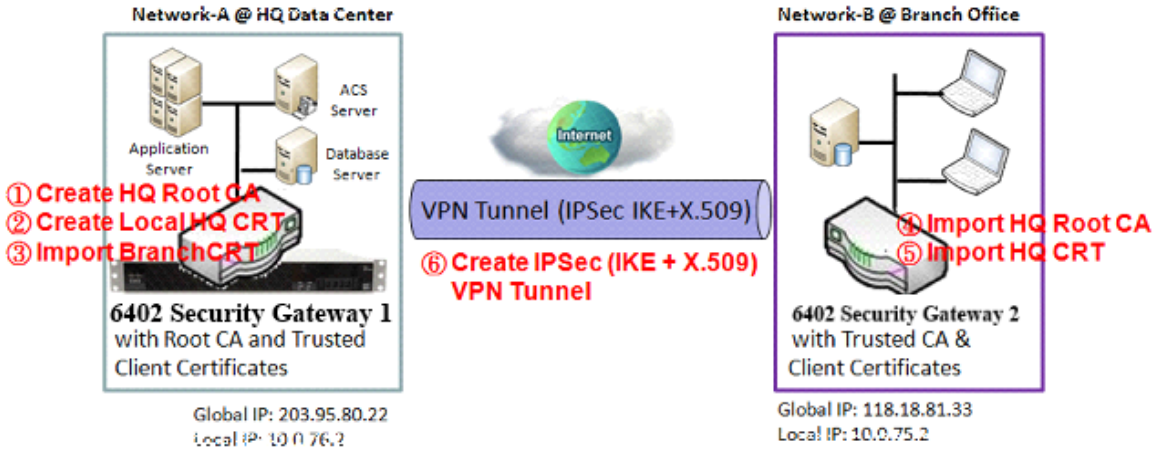
SCEP Configuration	
Item	Setting
SCEP	Enable
Automatically re-enroll aging certificates	Enable

SCEP Configuration		
Item	**Value setting**	**Description**
SCEP	The box is unchecked by default	Check the **Enable** box to activate SCEP function.
Automatically re-enrol aging certificates	The box is unchecked by default	When **SCEP** is activated, check the **Enable** box to activate this function. It will be automatically check which certificate is aging. If certificate is aging, it will activate SCEP function to re-enrol automatically.

5.4.2. My Certificate

My Certificate includes a Local Certificate List, which shows all generated certificates by the root CA for the 6402. It also stores the generated Certificate Signing Requests (CSR) which will be signed by other external CA's. The signed certificates can be imported as local certificates belonging to the 6402.

5.4.2.1. IPSec Certificate Example diagram



5.4.2.2. Root CA Certificate Configuration

Default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Root CA Certificate Configuration]
Name	***HQRootCA***
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***GB*** State(ST): ***England*** Location(L): ***London*** Organization(O): ***CASEHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQRootCA*** E-mail: ***hqrootca@casecomms.com***

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***HQCRT***Self-signed:■
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***GB*** State(ST): ***England***Location(L): ***High Wycombe*** Organization(O): ***CASEHQ*** Organization Unit(OU): ***HQRD*** Common Name(CN): ***HQCRT*** E-mail: ***admin@casecomms.com***
Configuration Path	**[IPSec]-[Configuration]**
IPSec	■ ***Enable***

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-101***
Interface	***WAN 1***
Tunnel Scenario	***Site to Site***
Operation Mode	***Always on***

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	***10.0.76.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.75.0***
Remote Netmask	***255.255.255.0***
Remote Gateway	***118.18.81.33***

Configuration Path	[IPSec]-[Authentication]
Key Management	***IKE+X.509***Local Certificate: ***HQCRT***Remote Certificate: ***BranchCRT***
Local ID	***User Name Network-A***
Remote ID	***User Name Network-B***

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	***Main Mode***
X-Auth	***None***

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[My Certificate]-[Local Certificate Configuration]
Name	***BranchCRT***Self-signed:□
Key	Key Type: ***RSA*** Key Length: ***1024-bits***
Subject Name	Country(C): ***UK***State(ST): ***England***Location(L): ***Reading*** Organization(O): ***Case Branch*** Organization Unit(OU): ***Case R&D*** Common Name(CN): ***BranchCRT*** E-mail: ***admin@casecomms.com***

Configuration Path	[IPSec]-[Configuration]
IPSec	■ ***Enable***

Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***s2s-102***
Interface	***WAN 1***
Tunnel Scenario	***Site to Site***
Operation Mode	***Always on***

Configuration Path	[IPSec]-[Local & Remote Configuration]
Local Subnet	***10.0.75.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.76.0***
Remote Netmask	***255.255.255.0***
Remote Gateway	***203.95.80.22***

Configuration Path	[IPSec]-[Authentication]
Key Management	***IKE+X.509***Local Certificate: ***BranchCRT***Remote Certificate: ***HQCRT***
Local ID	***User Name Network-B***
Remote ID	***User Name Network-A***

Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	***Main Mode***
X-Auth	***None***

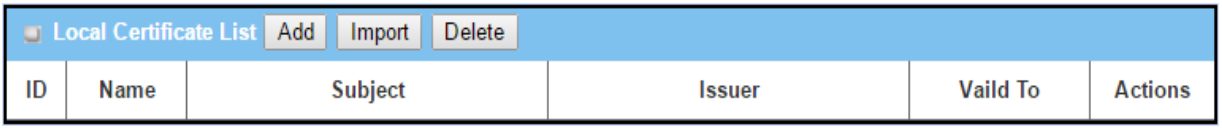
Operational Procedure – For above diagram

5.4.2.3. My Certificate Configuration

The My Certificate setting allows user to create local certificates. In "My Certificate" page, there are two configuration windows for the "My Certificate" function. The "Local Certificate List" window shows the stored certificates or CSRs representing the 6402. The "Local Certificate Configuration" window can let you fill required information necessary for corresponding certificate to be generated by itself, or corresponding CSR to be signed by other CAs.

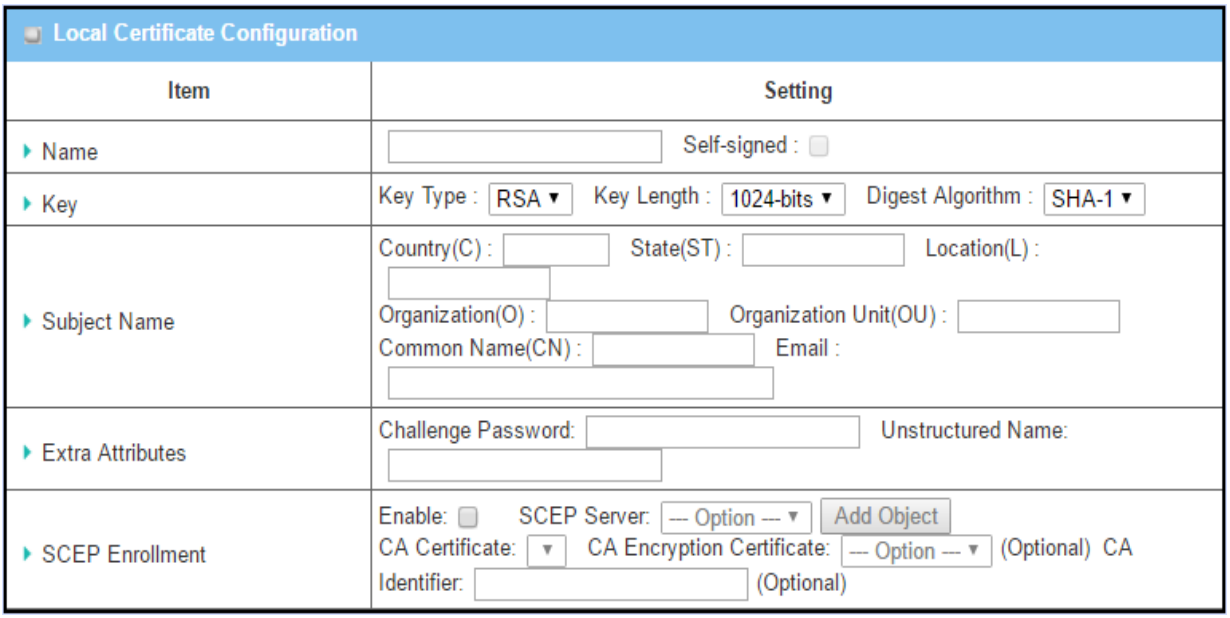
Go to Object Definition > Certificate > My Certificate tab.

5.4.2.4. Create local certificate



When the **Add** button is applied, **Local Certificate Configuration** screen will appear. The required information to be filled for the certificate or CSR includes the name, key and subject name.

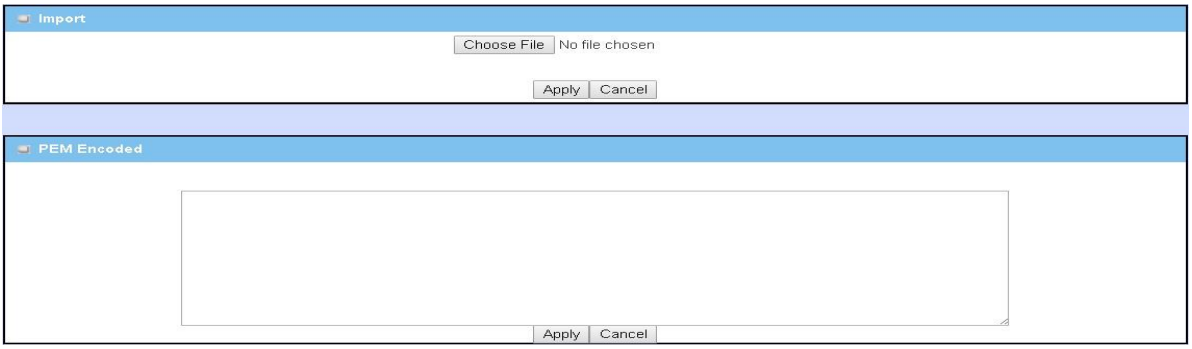
It is a certificate if the "Self-signed" box is checked; otherwise, it is a CSR.



Local Certificate Configuration		
Item	**Value setting**	**Description**
Name	1. String format can be any text 2. A Mandatory Setting	Enter a certificate name. It will be a certificate file name If **Self-signed** is checked, it will be signed by root CA. If **Self-signed** is not checked, it will generate a certificate signing request (CSR).
Key	A Mandatory Setting	This field is to specify the key attributes of certificate. **Key Type** to set public-key cryptosystems. Currently, only RSA is supported. **Key Length** to set the length in bits of the key used in a cryptographic algorithm. It can be 512/768/1024/1536/2048. **Digest Algorithm** to set identifier in the signature algorithm identifier of certificates. It can be MD5/SHA-1.
Subject Name	A Mandatory Setting	This field is to specify the information of certificate. **Country(C)** is the two-letter ISO code for the country where your organization is located. **State(ST)** is the state where your organization is located. **Location(L)** is the location where your organization is located. **Organization(O)** is the name of your organization. **Organization Unit(OU)** is the name of your organization unit. **Common Name(CN)** is the name of your organization. **Email** is the email of your organization. It has to be email address setting only.
Extra Attributes	A Mandatory Setting	This field is to specify the extra information for generating a certificate. **Challenge Password** for the password you can use to request certificate revocation in the future. **Unstructured Name** for additional information.
SCEP Enrolment	A Mandatory Setting	This field is to specify the information of SCEP. If user wants to generate a certificate signing request (CSR) and then signed by SCEP server online, user can check the **Enable** box. Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers. Refer to **Object Definition**>**External Server**>**External Server**. You may click **Add Object** button to generate. Select a **CA Certificate** to identify which certificate could be accepted by SCEP server for authentication. It could be generated in Trusted Certificates. Select an optional **CA Encryption Certificate**, if it is required, to

		identify which certificate could be accepted by SCEP server for encryption data information. It could be generated in Trusted Certificates. Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.

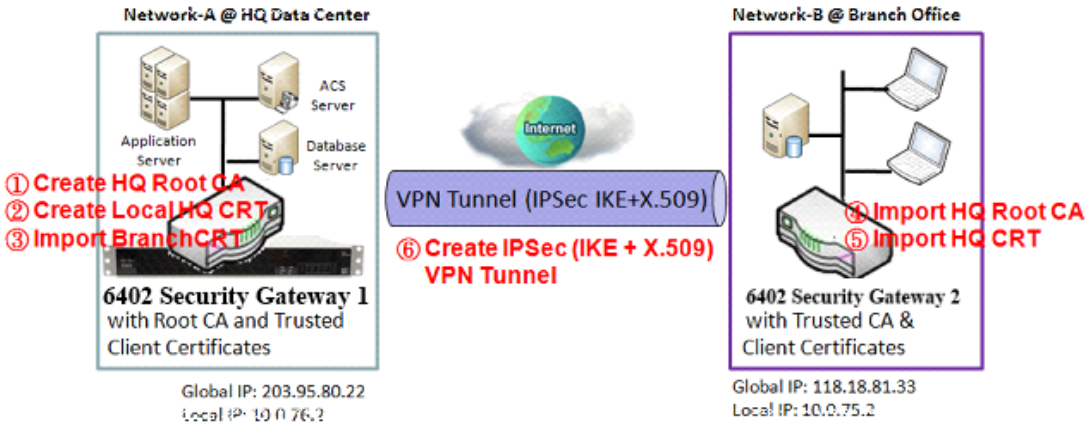
When Import button is applied, an Import screen will appear. You can import a certificate from an existed



Import		
Item	**Value setting**	**Description**
Import	A Mandatory Setting	Select a certificate file from user's computer and click the **Apply** button to import the specified certificate file to the gateway.
PEM Encoded	1. String format can be any text 2. A Mandatory Setting	This is an alternative approach to importing a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the My Certificates page.

5.4.3. Trusted Certificate

5.4.3.1. IPSec Certificate Examples



Application Scenario (this is same as the one described in "My Certificate" section)
When the enterprise gateway owns the root CA and VPN tunnelling function, it can generate its own local certificates signed by itself. It also imports the 'Trusted Certificates' for other CAs and Clients. These certificates can be used for two remote peers to confirm their identity during establishing a VPN tunnel.

5.4.3.2. IPSec Operation Description

6402 Gateway 1 - generates the root CA and a local certificate (HQCRT) signed by itself. It Imports a trusted certificate (BranchCRT) –a BranchCSR certificate of Gateway 2 signed by the root CA of Gateway 1.

6402 Gateway 2 -creates a CSR (BranchCSR) to let the root CA of the Gateway 1 sign it to be the BranchCRT certificate. Import the certificate into the Gateway 2 as a local certificate. In addition, also imports the certificates of the root CA of Gateway 1 into the Gateway 2 as the trusted ones. (Please also refer to "My Certificate" and "Issue Certificate" sections).
The 6402's establish an IPSec VPN tunnel with IKE and X.509 protocols by starting from either peer, so that all client hosts in these both subnets can communicate with each other.

5.4.3.3. Configuration Setup Example

For Network-A at HQ

The following tables list the configuration as an example for the "Trusted Certificate" function used in the user authentication of IPSec VPN tunnel as shown in diagram above.
The configuration example must be combined with the "My Certificate" and "Issue Certificate" sections to complete the setup example.

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	***BranchCRT.crt***

For Network-Bat Branch Office

The following tables list the example configuration for the "Trusted Certificate" used in the user authentication of IPSec VPN tunnel establishment, as shown in above diagram. The configuration example must be combined with the "My Certificate" and "Issued Certificate" sections to complete the setup.

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate List]
Command Button	***Import***

Configuration Path	[Trusted Certificate]-[Trusted CA Certificate Import from a File]
File	***HQRootCA.crt***

Configuration Path	[Trusted Certificate]-[Trusted Client Certificate List]
Command Button	***Import***

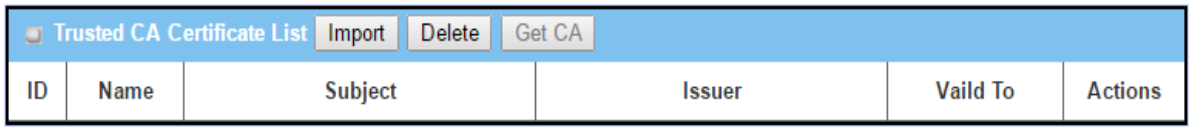
Configuration Path	[Trusted Certificate]-[Trusted Client Certificate Import from a File]
File	***HQCRT.crt***

"6402 Gateway 1" - is the 6402 Gateway for Network-A and its subnet is 10.0.76.0/24.
It has an IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN-1 interface.
"Gateway 2"- is the Gateway for Network-B and its subnet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN-1 interface.
They both serve as the NAT security gateways.
Gateway 2- imports the certificates of the root CA and HQCRT that were generated and signed by **Gateway 1-** into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of Gateway 2.

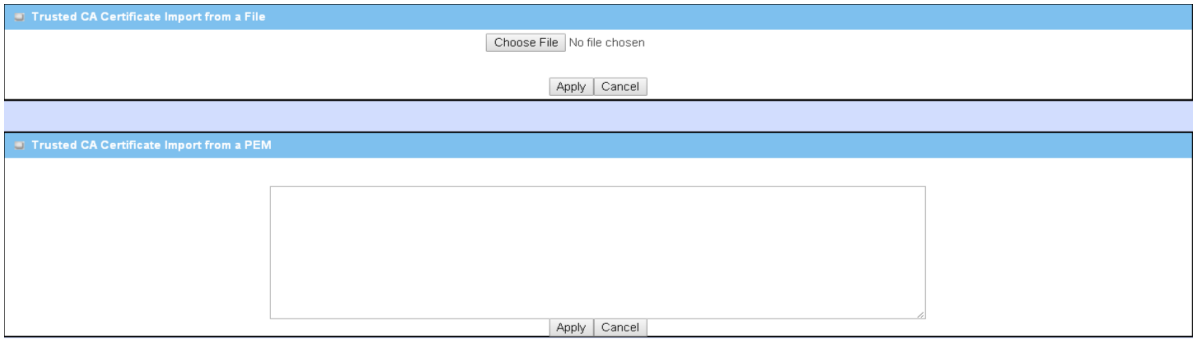
Gateway 2-imports the BranchCRT certificate (the derived BranchCSR certificate after Gateway 1's root CA signature) into the "Trusted Client Certificate List" of Gateway 1 and the "Local Certificate List" of the Gateway 2.
For more details, refer to the Network-B operation procedure in "My Certificate" section of this manual.
Gateway 2- can establish an IPSec VPN tunnel with "Site to Site" scenario and IKE and X.509 protocols to Gateway 1.

5.4.3.4. Trusted Certificate Setting

The Trusted Certificate setting allows user to import trusted certificates and keys.
Go to Object Definition > Certificate > Trusted Certificate tab.
Import Trusted CA Certificate

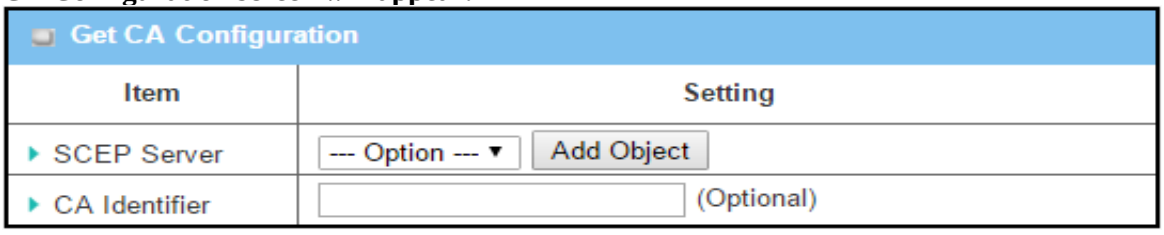


When Import button is applied, a Trusted CA import screen will appear. You can import a Trusted CA certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.



Trusted CA Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Mandatory Setting	Select a CA certificate file from user's computer and click the **Apply** button to import the specified CA certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Mandatory Setting	This is an alternative approach to import a CA certificate. You can directly fill in (Copy and Paste) the PEM encoded CA certificate string and click the **Apply** button to import the specified CA certificate to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

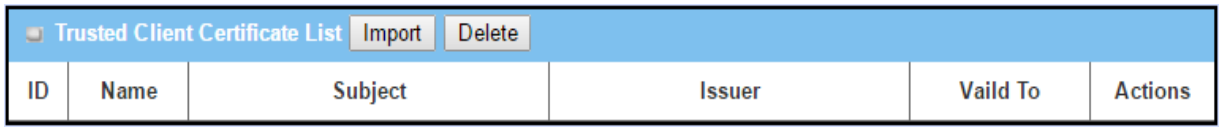
CA Configuration screen will appear.



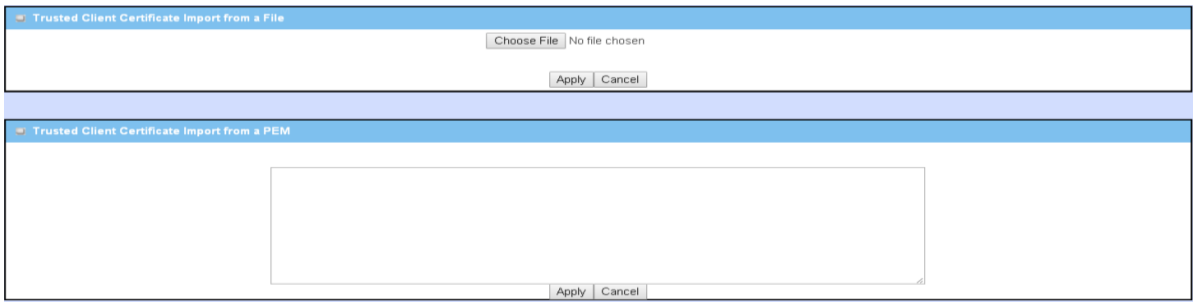
Get CA Configuration		
Item	**Value setting**	**Description**
SCEP Server	A Mandatory Setting	Select a **SCEP Server** to identify the SCEP server for use. The server detailed information could be specified in External Servers.

		Refer to **Object Definition**>**External Server**>**External Server**. You may click **Add Object** button to generate.
CA Identifier	1. String format can be any text	Fill in optional **CA Identifier** to identify which CA could be used for signing certificates.
Save	N/A	Click **Save** to save the settings.
Close	N/A	Click the **Close** button to return to the Trusted Certificates page.

5.4.3.5. Import Trusted Client Certificate

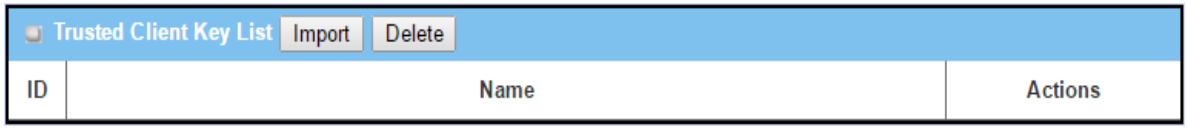


When the **Import** button is applied, a **Trusted Client Certificate Import** screen will appear. You can import a Trusted Client Certificate from an existed certificate file, or directly paste a PEM encoded string as the certificate.

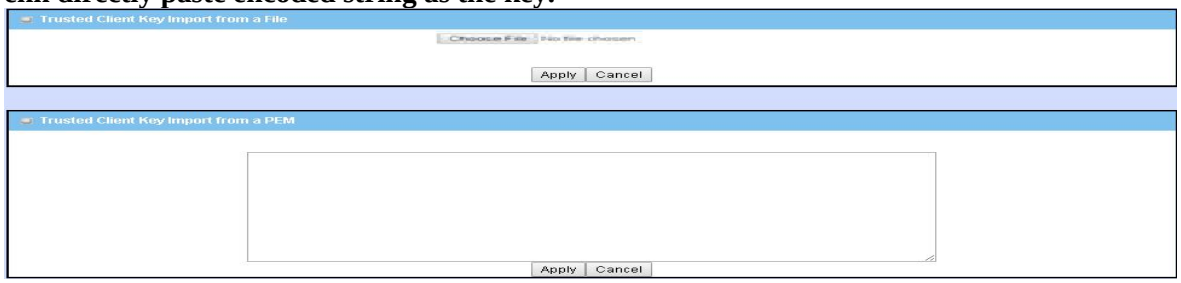


Trusted Client Certificate List		
Item	**Value setting**	**Description**
Import from a File	A Mandatory Setting	Select a certificate file from user's computer and click the **Apply** button to import the specified certificate file to the gateway.
Import from a PEM	1. String format can be any text 2. A Mandatory Setting	This is an alternative approach to import a certificate. You can directly fill in (Copy and Paste) the PEM encoded certificate string and click the **Apply** button to import the specified certificate to the gateway.
Apply	N/A	Click the **Apply** button to import certificate.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

5.4.3.6. Import Trusted Client Key



enn directly paste encoded string as the key.



Trusted Client Key List		
Item	**Value setting**	**Description**
Import from a File	A Mandatory Setting	Select a certificate key file from user's computer and click the **Apply** button to import the specified key file to the gateway.
Import from a PEM	1. String format can be any text 2. A Mandatory Setting	This is an alternative approach to import a certificate key. You can directly fill in (Copy and Paste) the PEM encoded certificate key string and click the **Apply** button to import the specified certificate key to the gateway.
Apply	N/A	Click the **Apply** button to import the certificate key.
Cancel	N/A	Click the **Cancel** button to discard the import operation and the screen will return to the Trusted Certificates page.

5.4.3.7. Signing Request to Import from a File

When you have a Certificate Signing Request (CSR) that needs to be certificated by the root CA of the 6402, you can issue the request here and let the Root CA sign it. There are two approaches to issuing a certificate.

1.From a CSR file imported from the managing PC

2. Copy-paste the CSR codes in 6402's web-based utility. Once you have done this click on the "Sign" button.

If the 6402 signs a CSR successfully, the "Signed Certificate View" window will show the signed certificate contents. In addition, a "Download" button is available for you to download the certificate to a file on the managing PC.

5.4.3.8. Parameter Setup Example

For Network-A at HQ

The following tables list an example configuration for the "Issue Certificate" function used in the user authentication of IPSec VPN tunnel establishment, as shown in the diagram' IPSec certificate Example' . The configuration example must be combined with the "My Certificate" and "Trusted Certificate" sections to complete the setup for whole user scenario.

Configuration Path	[Issue Certificate]-[Certificate Signing Request Import from a File]
Browse	***C:/BranchCSR***
Command Button	***Sign***
Configuration Path	[Issue Certificate]-[Signed Certificate View]
Command Button	***Download*** (default name is "issued.crt")

Scenario Operation Procedure

"Gateway 1" -is the 6402 Gateway for Network-A in headquarters and its subnet is 10.0.76.0/24. It has the IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN-1 interface.

"Gateway 2" - is the 6402 Gateway for Network-B in the branch office and its subnet is 10.0.75.0/24. It has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN-1 interface. They both serve as the NAT security gateways.

6402 Gateway 1 - generates the root CA and a local certificate (HQCRT) that is signed by itself. It imports the certificates of the root CA and HQCRT into the "Trusted CA Certificate List" and "Trusted Client Certificate List" of 6402 Gateway 2.

6402 Gateway 2 - generates a Certificate Signing Request (BranchCSR) for its own certificate BranchCRT to be signed by root CA (Please generate one not self-signed certificate in the Gateway 2 and click on the "View" button for that CSR. The 6402 just downloads it). Take the CSR to be signed by the root CA of 6402Gateway 1 and obtain the BranchCRT certificate (you need to rename it). Import the certificate into the "Trusted Client Certificate List" of6402 Gateway 1 and the "Local Certificate List" of 6402Gateway 2.

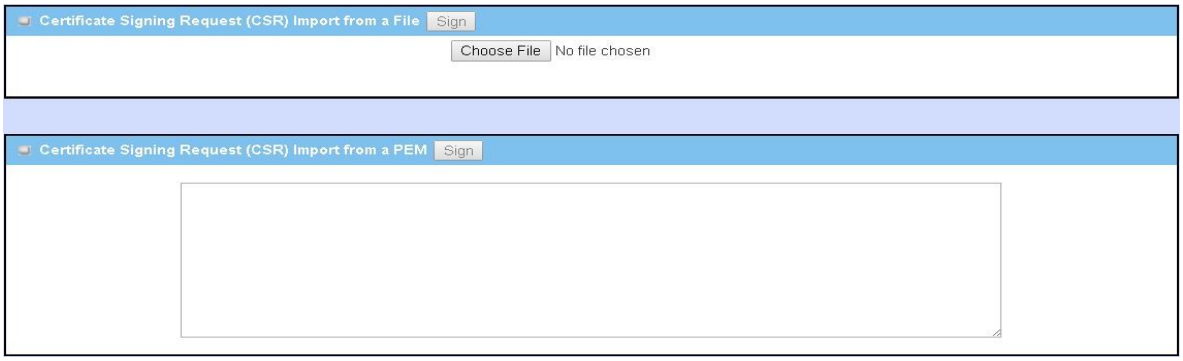
Gateway 2 can establish an IPSec VPN tunnel using the "Site to Site" scenario and IKE and X.509 protocols to 6402 Gateway 1.

5.4.3.9. Issue Certificate Setting

The Issue Certificate setting allows user to import Certificate Signing Request (CSR) to be signed by root CA.

Go to Object Definition > Certificate > Issued Certificate tab.

Import and Issue Certificate



Certificate Signing Request (CSR) Import from a File		
Item	**Value setting**	**Description**
Certificate Signing Request (CSR) Import from a File	A Mandatory setting	Select a certificate signing request file you're your computer for importing to the gateway.
Certificate Signing Request (CSR) Import from a PEM	1. String format can be any text 2. A Mandatory setting	Enter (copy-paste) the certificate signing request PEM encoded certificate to the gateway.
Sign	N/A	When root CA exists, click the **Sign** button sign and issue the imported certificate by root CA.

This page left blank intentionally

SECTION 6

FIELD COMMUNICATIONS

BUS

&

MODBUS

6. Bus & Protocol

6.1.1 Serial Port

The 6402 is equipped with a DB-9 male port for serial **c**ommunication use through an RS-232 or RS-485 serial device to an IP-based Ethernet LAN These communication protocols allow serial users access to devices anywhere on the LAN or LAN devices access to serial devices.

Serial Port Definition - Field Communication > Bus and Protocol> Port Configuration

Before using a field communication function, such as Virtual COM or MODBUS, you need to configure the physical communication port first. The options are

- Disabled
- Virtual Com
- MODBUS

For Async to Async Data Virtual Bus is the best option. Proceed to configure data rate, word size, parity stop bits etc.

Go to Field Communication > Bus & Protocol > Port Configuration tab.

Serial Port Definition

Serial Port Definition

Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
SPort-0	Virtual COM	RS-232	19200	8	1	None	None	Edit

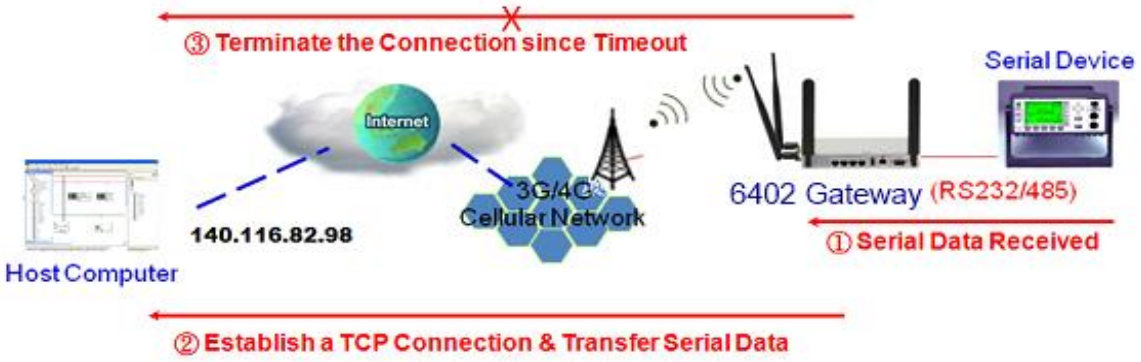
Port Configuration Window		
Item	**Value setting**	**Description**
Serial Port	*N/A*	It displays the serial port ID of the serial port. The number of serial ports varies from the purchased model.
Operation Mode	Disable is set by default	It displays the current selected operation mode for the serial interface. This can be Disabled, Virtual Com or MODBUS
Interface	RS-232 RS-485 RS232 is default	Select RS-232 or RS-485 physical interface for connecting to the access device(s) with the same interface specification.
Baud Rate	19200 is set by default	Select the appropriate baud rate for serial device communication. RS-232: 1200 / 2400 / 4800 / 9600 / 19200 / 38400 / 57600 / 115200 RS-485 can use higher baud rate for 230400 and 460800. It depends on the cable length and the installed environment. The longer cable, the lower baud rate for it.
Data Bits	8 is set by default	Select 8 or 7 for data bits.
Stop Bits	1 is set by default	Select 1 or 2 for stop bits.
Flow Control	None is set by default	Select None / RTS,CTS / DTS, DSR for Flow Control in RS-232 mode. The supporting of Flow Control depends on the purchased model.
Parity	None is set by default	Select None / Even / Odd for Parity bit.
Edit		Click Edit button to change the operation mode, or modify the parameters mentioned above for the serial interface communication.
Save		Click Save button to save the settings.

6.1.2. Virtual COM Port Introduction

Field Communications>Bus & Protocol > Virtual Com

6.1.2.1. TCP Client Operation

The 'Virtual COM' setting screen enables user to connect a Virtual COM port-based device to the Internet. It allows user to access serial data remotely. There are TCP Client, TCP Server, UDP, and RFC2217 modes for remote accessing the connected serial device. These operational modes are illustrated as below.



6.1.3. TCP Client Mode in On-demand Control Scenario

When the Network administrator wants the 6402 to actively establish a TCP connection to a pre-defined host computer the 6402 "Virtual COM" should be set to "TCP Client" and the remote end of the link set to TCP Server. The TCP Client makes a connection to the TCP Server, either set to 'Always On' when the connection is established permanently or 'dynamically' when the connection is established when there is data to send and broken when the data has been sent.

Operational Mode for the Serial Port

The first task in using the serial port is to set the mode and serial options as shown below.

Operation Mode Definition for each Serial Port

Serial Port	Operation Mode	Listen Port	Trust Type	Max Connection	Connection Control	Connection Idle Timeout	Alive Check Timeout	Enable	Action
SPort-0	TCP Client	4001 (1~65535)	Allow All	1	Always on	0 (0-3600secs)	0 (0-3600secs)	☑	Edit

Virtual Com

Serial Port Configuration Options – TCP Client Mode	
Serial Port	SPort-0 The 6402 Serial Port
Operation Mode	Set to disable, TCP Client, TCP Server, UDP, RFC 2217
Listen Port	Set the port to listen to. Default 4001
Trust Type	Allow All – fixed in TCP Client Mode
Max Connections	1
Connection Control	Always on - Fixed in this mode.
Connection Idle Timeout	Default 0 ms set to value between 0 and 3600 ms
Alive Check Timeout	Default 0 ms set to value between 0 and 3600 ms
Enable	This Box is greyed out

Data Packing for TCP Client, TCP Server and UDP Operation Mode

Data Packing (for TCP Client, TCP Server and UDP operation mode)

Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
SPort-0	0 (0~1024)	0 (Hex) ☐ Enable	0 (Hex) ☐ Enable	10 (0~1000ms)

Data Buffer Length	Default set to 0, value up to 1024
Delimiter Character 1	If required tick enable and enter Hex Value
Delimiter Character 2	If required tick enable and enter Hex Value
Data Timeout Transmit	(0-1000ms) NB. Default to 0. This is the delay after the 6402 receives data in its buffer that it starts to send that data. E.g. 20ms before sending

Legal Host IP / FQDN Definition

Legal Host IP/ FQDN Definition (for TCP Client operation mode)

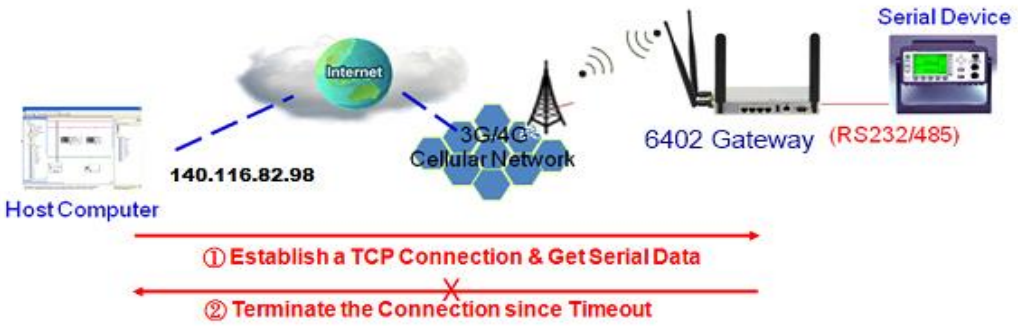
ID	To Remote Host	Remote Port	Serial Port	Definition Enable	Action
1	172.16.21.40	4001	SPort-0	☑	Edit
2		4001	SPort-0	☐	Edit
3		4001	SPort-0	☐	Edit
4		4001	SPort-0	☐	Edit

Set the IP Address of the hosts you wish to connect t in this option. Select Definition enable to enable this option.

Legal Host IP / FQDN Definition (For TCP Client Mode)				
ID	**To Remote Host**	**Remote Port**	**Serial Port**	**Definition Enable**
1	Add IP address of TCP Server 6402	Default 4001	Sport-0	Don't forget to enable
2	If FQDN Set destination in remote port	FQDN		

6.1.4. TCP Server Mode

In this mode the 6402 waits passively for a serial data request from a host computer, and on receiving that data the 'Virtual Com' function is activated and this becomes a 'TCP Server'
In this mode, the 6402 provides a unique "IP: Port" address on a TCP/IP network. It supports up to 4 simultaneous connections, so that multiple hosts can collect data from the same serial device at the same time.



Setting the Serial Port

Serial Port Definition – TCP Server								
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
Sport-0	Virtual Com	RS232	19200	8	1	RTS / CTS	None	Edit

Configuration Example

The following tables list the example configuration for the "TCP Server" mode in "Virtual COM" function, as shown in above diagram. Use default value for those parameters that are not mentioned in the tables.

Operational Mode for Each Serial Port – TCP Server

Operational Mode definition for each Serial Port – TCP server								
Serial Port	Operational Mode	Listening Port	Trust Type	Max Connection	Connection Control	Connection Idle timeout	Alive Check timeout	Enable
SP-0	TCP-Client	4001	Allow All	1	Always On	0	0	

Operation Mode Definition for each serial port – TCP Server		
Item	Value setting	Description
Serial Port	Sport-0	6402 Serial Port.
Operational mode	TCP Server	Set to TCP Server.
Listening Port	4001	Select the port number that the TCP Server will monitor
Trust Type	Select All	Select All if set to Specific IP's a new sub menu is shown
Max Connection	1	1 to 128
Connection Control	Always On	This is the only option in in this mode
Connection Idle Timeout	0 is set by default	Input the time period of alive check timeout. The TCP connection will be terminated if it doesn't receive response of alive-check longer than this timeout setting. *Value Range*: 0 ~ 3600 seconds
Alive Check Timeout	The box is unchecked by default.	Check the Enable box to activate the corresponding serial port in specified operation mode.
Save	*N/A*	Click Save button to save the settings.

Trusted IP definition for TCP server				
ID	**Host**	**Serial Port**	**Definition Enable**	**Action**
1	IP Address of host	Serial Port Sport-0	Tick to enable	Edit
2				Edit
3				Edit

Data Packing for TCP Server

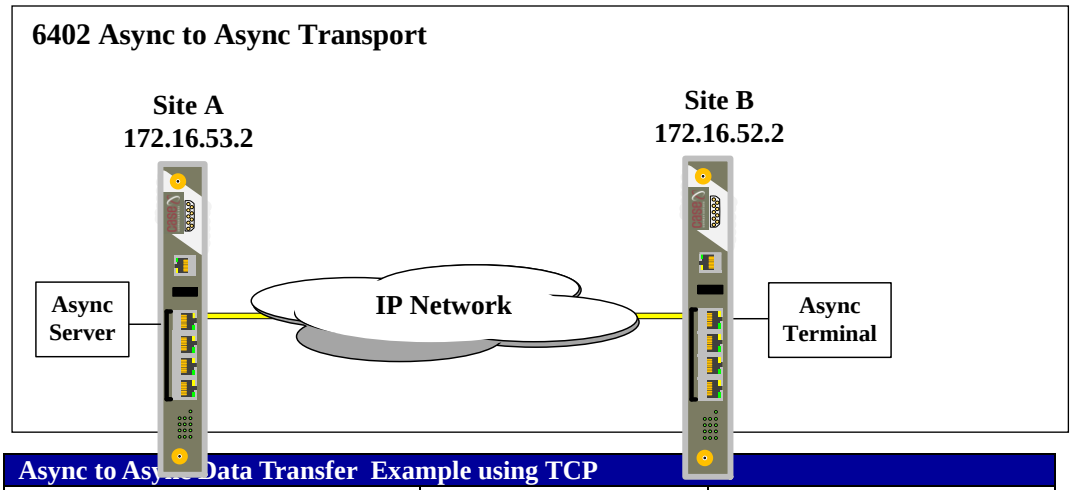
Data Packing for Server				
Serial Port	Data Buffer Length	De Limiter Character-1	De Limiter character-2	Data Timeout transmit
SP-0	0	Set in Hex if required	Set in Hex if required	10ms

Configuration Option	Virtual Com – Virtual Com Serial Definition
Serial Port	The serial Port being used ie SP-0
Data Buffer Length	Default set to 0, value up to 1024
Delimiter Character 1	If required enable and enter Hex Value
Delimiter Character 2	If required enable and enter Hex Value
Data Timeout Transmit	(0-1000ms) NB. Default to 0. This is the delay after the 6402 receives data in its buffer that it starts to send that data. E.g. 20ms before sending

Trusted IP definition for TCP server				
ID	**Host**	**Serial Port**	**Definition Enable**	**Action**
1	IP Address of host	Serial Port Sport-0	Tick to enable	Edit
2				Edit

6.1.5. Async to Async Data Transfer Using TCP Example

To run Async data using TCP its necessary to set one end to a TCP Client and the other end to a TCP Server as shown below.



Async to Async Data Transfer Example using TCP		
	Site A	**Site B**
Serial Port	Sport-0	Sport-0
Operation Mode	Virtual Com	Virtual Com
Interface	RS-232	RS232
Baud Rate	19,200bps	19,200bps
Data Bits	8	8
Stop Bits	1	1
Flow Control	None	None
Parity	None	None

Operational Mode Definition for each Serial Port		
	Site A	**Site B**
Serial Port	Sport-0	Sport-0
Operation Mode	TCP-Server	TCP-Client
Listening Port	4001	Not Applicable
Trust Type	Allow All	Not Applicable
Max Connections	1	1
Connection Control	Not Applicable	Always On
Idle Connection Timeout	0 ms	0 ms
Alive Check Timeout	0 ms	0 ms

Data Packing for TCP Client and Server				
Serial Port	Data Buffer Length	Delimiter Character 1	Delimiter Character 2	Data Timeout Transmit
Sport-0	0 (0~1024)	0 Hex Enable	0 Hex enable	0 ~ 1000ms

Data Packing for TCP Client and Server		
	Site A	**Site B**
Serial Port	Sport-0	Sport-0
Data Buffer Length	0	0
Delimiter character 1	Default not enabled	Default not enabled
Delimiter character 2	Default not enabled	Default not enabled
Data Timeout Transmit Some PLCs need a value eg 10ms	0ms default - try 10ms	0ms default try- 10ms

Set TCP Client to reach remote TCP Server						
ID	**To Remote Host**	**Remote Port**		**Serial Port**	**Definition Enable**	**Action**
1	172.16.53.2	4001		Sport-0	Ticked	

If Trust type on TCP Server set allowed IP addresses

Trusted IP Definition for TCP Server				
ID	Host	Serial Port	Definition Enable	Action
	172.16.52.2	Sport-0	Enable	Edit to change

6.1.6. UDP Mode

UDP Mode - Example

If both the IP Connected 'Host Computer; and the remote serial devices are expected to initiate data transfer mode then the 'Virtual COM' function for the 6402 should be set to UDP Mode.

In this mode, the UDP data can be transferred between the 6402 and multiple host computers from either peer, making this mode ideal for message display applications. It supports up to 4 legal host computers to connect to the serial device via the 6402.

A remote Internet host computer with an IP Address of 140.116.82.98 has a management system to collect serial data from or send data to the serial device via the 6402.

The Internet host computer can directly send UDP data to the serial device via the 6402, and also receive UDP data from the serial device via the 6402 at the same time. The 6402 supports up to 4 Internet host computers.

6.1.6.1. UDP Configuration Example

Following tables list the parameter configuration as an example for the "UDP" mode in "Virtual COM" function, as shown in above diagram.

Use default value for those parameters that are not mentioned in the tables.

6.1.6.2. Setting Port Configuration

Field Communications > Bus & Protocol > Port Configuration

Serial Port Definition – UDP Mode								
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
Sport-0	Virtual Com	RS232	19200	8	1	RTS / CTS	None	Edit

Virtual Com in UDP Mode

Operational Mode definition for each Serial Port - UDP								
Serial Port	Operational Mode	Listening Port	Trust Type	Max Connection	Connection Control	Connection Idle timeout	Alive Check timeout	Enable
SP-0	UDP	4001	Allow All	1	Greyed Out	Greyed Out	Greyed Out	

Operation Mode Definition for each serial port – UDP Operational Mode		
Item	Value setting	Description
Serial Port	Sport-0	6402 Serial Port.
Operational mode	UDP	Set to UDP Mode
Listening Port	4001	Select the port number that the TCP Server will monitor
Trust Type	N/A	Not Applicable in UDP Mode
Max Connection	128	Greyed out in this mode
Connection Control	Always On	This is the only option in this mode
Connection Idle Timeout	0	Greyed Out
Alive Check Timeout	0	Greyed Out
Save	*N/A*	Click Save button to save the settings.

6.1.6.3. Data Packing for UDP

Data Packing for UDP				
Serial Port	Data Buffer Length	De Limiter Character-1	De Limiter character-2	Data Timeout transmit
SP-0	0	Set in Hex if required	Set in Hex if required	10ms

Configuration Option	Virtual Com – Virtual Com Serial Definition
Serial Port	The serial Port being used ie SP-0
Data Buffer Length	Default set to 0, value up to 1024
Delimiter Character 1	If required enable and enter Hex Value
Delimiter Character 2	If required enable and enter Hex Value
Data Timeout Transmit	(0-1000ms) NB. Default to 0. This is the delay after the 6402 receives data in its buffer that it starts to send that data. E.g. 20ms before sending

Option to only allow specific IP Addresses.

Legal Host IP for UDP Mode				
	To Remote Host	**Remote Port**	**Serial Port**	**Enable**
1	Add IP address of TCP Server 6402	Default 4001	SP0	Don't forget to enable
2				

6.2. RFC 2217 Mode

RFC-2217 defines general COM port control options based on telnet protocol. A host computer with an RFC-2217 driver installed can monitor and manage the remote serial device attached to the 6402's serial port, as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the host computers to establish connection with.

Any 3rd party driver supporting RFC2217 can be installed in the host computer, the driver establishes a transparent connection between host and serial device by mapping the IP:Port of the 6402's serial port to a virtual local COM port on the host computer. The 6402 can support up to 4 remote devices.

6.2.1. Configuring RFC-2217 Mode

RFC-2217 defines general COM port control options based on telnet protocol. When running RFC-2217 mode, a remote host can monitor and manage remote serially attached devices, as though they were connected to the local serial port. When a virtual serial port on the local serial device is being created, it is required to specify the IP-address of the remote hosts to establish connection with.

Configure the serial port first

Serial Port Definition – TCP Server								
Serial Port	Operation Mode	Interface	Baud Rate	Data Bits	Stop Bits	Flow Control	Parity	Action
Sport-0	Virtual Com	RS232	19200	8	1	RTS / CTS	None	Edit

Virtual Comm Examples

Operational Mode definition for each Serial Port								
Serial Port	Operational Mode	Listening Port	Trust Type	Max Connection	Connection Control	Connection Idle timeout	Alive Check timeout	Enable
SP-0	RFC-2217	4001	Allow All	1	Greyed Out	0	0	

Configuration Option	Virtual Com – Virtual Com Serial Definition
Operation Mode	RFC 2217
Listening Port	4001 (1 – 65535)
Trust Type	Allow All – or specify IP Addresses
Maximum Connections	This option greyed out
Connection Control	Default 'Always on' in this mode cant be changed
Connection Idle Timeout	Set to 0 option 0 ~ 3600
Alive Checkout Timeout	Set to 0 option 0 ~ 3600
Enable	Tick this box to enable the option

Data Packing for RFC 2217

Data Packing for RFC 2217 Mode				
Serial Port	Data Buffer Length	De Limiter Character-1	De Limiter character-2	Data Timeout transmit
SP-0	0	Set in Hex if required	Set in Hex if required	Default 0ms
Configuration Option		**Virtual Com – Virtual Com Serial Definition**		
Serial Port		The serial Port being used ie SP-0		
Data Buffer Length		Default set to 0, value up to 1024		
Delimiter Character 1		If required enable and enter Hex Value		
Delimiter Character 2		If required enable and enter Hex Value		
Data Timeout Transmit		(0-1000ms) Default 0 but some PLC's require a value to be set try 20ms		

Menu Options to allow specific IP Addresses.

Trusted IP definition for RFC 2217			
	Host	**Serial Port**	**Enable**
1	IP Address of a host or select a range of IP addresses	Sport-0	Don't forget to enable
2			

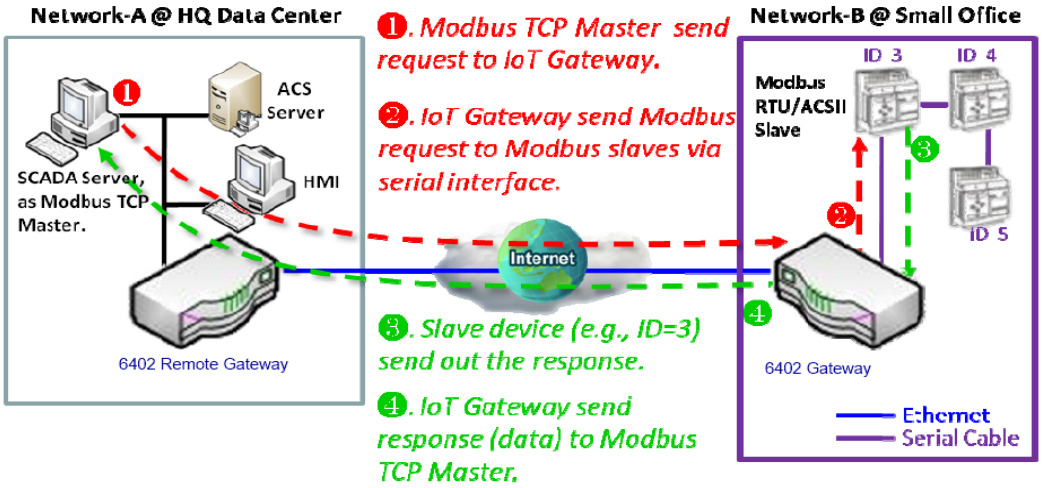
6.3. MODBUS

6.3.1. MODBUS Overview

MODBUS is one of the most popular automation protocols in the world, supporting traditional RS-232/422/485 devices and more recently Ethernet devices. Many industrial devices, such as PLCs, DCSs, HMIs, instruments, and smart meters, use the MODBUS protocol as the Industrial communication standard. It is used to establish master-slave communication between intelligent devices.

However, the Ethernet-based MODBUS protocol is very different from the original serial-based protocols. In order to integrate MODBUS networks, the 6402, includes a serial port that supports an RS-232 and RS-485 communication interface, and can automatically and intelligently translate between MODBUS TCP (Ethernet) and MODBUS RTU/ASCII (serial) protocols, allowing Ethernet-based PLCs to control instruments over RS-485 without additional programming or effort.

NOTE: When MODBUS devices are connected to the same serial port of the 6402, those MODBUS devices must use the same protocol with the same configuration (i.e., either MODBUS RTU or MODBUS ASCII with same Baud Rate setting).



6.3.1.1. MODBUS Receiving from a remote Modbus TCP Master

The example is for a 6402 Router to be a MODBUS Slave allowing it to receive requests from a remote MODBUS TCP Master.

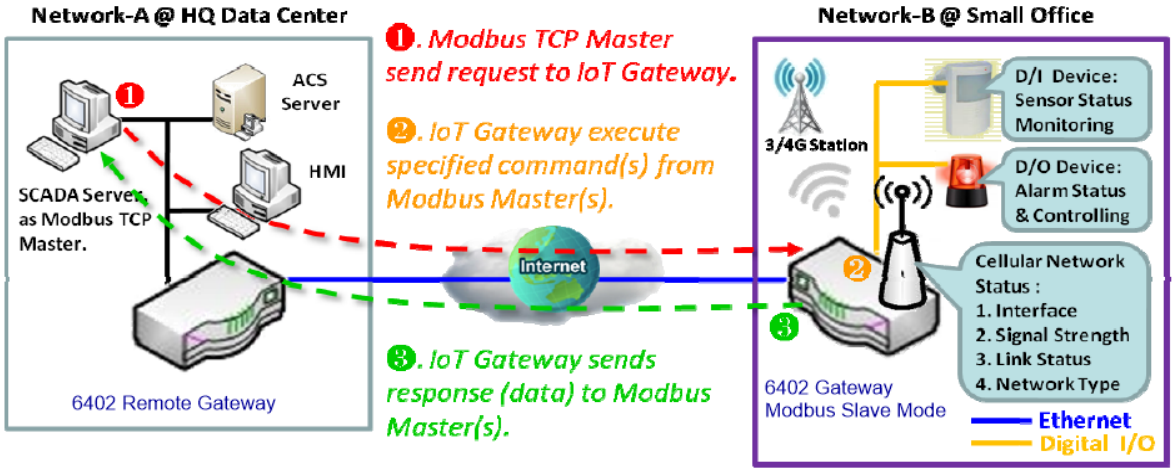
The MODBUS TCP Master requests information from or sends control commands to various MODBUS devices that are attached to the MODBUS 6402 Gateway. The 6402 Gateway executes corresponding processes and replies the MODBUS TCP Master with the results.

6.3.1.2. 6402 MODBUS Slave Example

The 6402 Remote Gateway serves as a MODBUS Slave and router to communicate with the MODBUS TCP Master.

The MODBUS TCP Master send a to the 6402 requesting MODBUS' information, e.g., Data Acquisition or Register/Value Modifications, via the link (in this example going over the Internet) and accessing, the remote 6402 which forwards the data.

6402 as MODBUS TCP/RTU Slave Scenario – Receiving requests from Modbus Master



6.3.2. 6402 MODBUS Slave

The 6402 MODBUS Slave communicates with the MODBUS Master devices, e.g. the SCADA Server, via the 6402 MODBUS serial port or via the Internet/Intranet to provide information on the status of 6402 and allow some configuration.

Serial Port Configuration

Go to Field Communication > Bus & Protocol > Port Configuration >

Serial Port Configuration							
Serial Port	**Operation Mode**	**Interface**	**Baud Rate**	**Data Bits**	**Stop Bits**	**Flow Control**	**Parity**
Sport-0	MODBUS	RS232	19200	8	1	None	None

Modbus Gateway Definition

Modbus Gateway Definition Options	
Serial Port	6402 Serial port Sport-0
Operation Mode	Set as MODBUS
Interface	Set as RS232 or RS485
Baud Rate	Set to required Baud Rate
Set Data Bits	7 or 8
Stop Bits	Set to None 1 or 2
Flow Control	Set to RST / CTS, TR / DSR or none

Modbus Gateway Serial as a slave

Modbus Gateway Definition – Serial as Slave					
Serial Port	**Gateway Mode**	**Device Slave Mode**	**Listen Port**	**Serial Protocol**	**Enable**
Sport-0	Serial as Slave	Slave Mode-Disable	502	RTU	

Modbus Gateway Definition Options	
Serial Port	6402 Serial port Sport-0
Gateway Mode	Set to Serial as Slave
Device Slave Mode	Disabled by default if enabled set Slave ID 1 to 247
Listening Port	Default 502 option to set from 1 to 65535
Serial Protocol	RTU or Ascii

Gateway Mode Configuration for Sport-0	
Response Timeout	Default 1000 (Range 1 ~ 65535) in milli-seconds
Timeout Retries	Default 0 (Times 0 to 5)
0Bh Exception	Enable – by default disabled
Tx Delay	Enable – by default disabled
TCP Connection Idle Time	300 (Range 1 to 65535)
Maximum TCP Connections	Default 1 (Range 1 ~ 4)
TCP Keep-alive	Enable
Modbus Master IP Access	Allow all or specific IP Addresses
Message Buffering	Default disabled (Options enable or disable)

6.3.3. Setting MODBUS to Serial Master

Modbus Gateway Definition – Serial as Master					
Serial Port	**Gateway Mode**	**Device Slave Mode**	**Listen Port**	**Serial Protocol**	**Enable**
Sport-0	Serial as Master	Slave Mode-Disable	502	RTU	

Set Device Slave Mode to enable and you have the option to select a slave ID 1 to 247

Modbus Gateway Definition Options	
Serial Port	6402 Serial port Sport-0
Gateway Mode	Set to Serial as Master
Device Slave Mode	Disabled by default if enabled set Slave ID 1 to 247
Listening Port	Default 502 option to set from 1 to 65535
Serial Protocol	RTU or Ascii

If set to Serial as Master the following menus appear

MODBUS TCP Slave List for Sport-0					
ID	IP	Port	ID Range	Enable	Action

ID	The ID Assigned to this device
IP	Enter the IP Address of the TCP Device
Port	Enter the Port Number
ID Range	Enter 1 ~ 247 Enter 1 ~ 247
Enable	Tick this box to enable this configuration

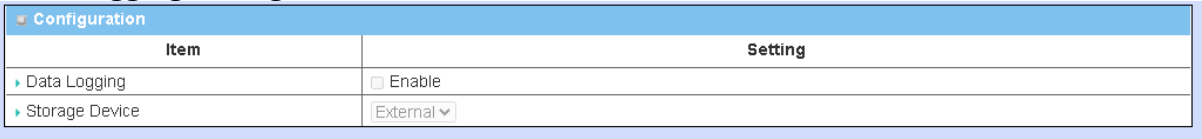
Gateway Mode Configuration for Sport 0

Gateway Mode Configuration for Sport-0	
Response Timeout	1000 (ms – 1 ~ 65535)
Timeout Retries	0 Times (0 ~5)
0Bh Exceptions	Enable
Tx Delay	Enable
TCP Connection Idle Time	300 sec (1 ~ 65535)
Maximum TCP Connections	1 ~ 4
TCP Keep alive	Enable
Modbus Master IP Access	Allow all or specify allowed IP Addresses
Message Buffer	Enable

6.4. Data Logging

Field and Bus Communications > Data Logging

Data Logging Configuration



MODBUS Proxy Rule List								
ID	Name	Modbus Slave Type	Slave ID	Function Code	Start Address	Number of Coils Register	Polling rate	Action

Modbus Proxy Rule List Configuration	
Name	Provide a Name for this configuration
Modbus Slave Type	Add the IP Address of the port or select local serial port (Sport-0)
Slave ID	Set this to between 1 and 247 for both devices
Function Code	Set this to read the desired Coils eg Read Coils 0x01, Read discrete inputs etc
Start Address	Select the start address 0 ~ 65535
Number of coils registers	1 ~ 125
Polling rate in ms	Default 1000ms range (500 ~ 99999)

Scheme Set-Up

Scheme Configuration	
Name	Give this Scheme a name
Mode	Sniffer, Off Line Proxy, Full Time Proxy, Sniffer and Off-Line Proxy, Sniffer and On-Line Proxy
Master Query Timeout (Sec)	60 (Range 1 ~ 99999)
Proxy rules	Not Applicable
Enable	

Log File Management

Note to configure MODBUS Events refer to Service > Configuration

This page left blank intentionally

CHAPTER 7

SECURITY

&

TUNNELLING

7.1. Virtual Private Network (VPN)

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of a private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two.
The 6402 supports different tunnelling technologies to establish secure tunnels between multiple sites for data transfer, such as IPSec, OpenVPN, PPTP, L2TP (over IPSec) and GRE. It also supports some advanced functions, like Full Tunnel, Tunnel Failover, Tunnel Load Balance, NetBIOS over IPSec, NAT Traversal and Dynamic VPN, are also supported.

7.1.1. IPSec

IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.
An IPSec VPN tunnel is established between an IPSec client and server. Sometimes, we call the IPSec VPN client the initiator and the IPSec VPN server as the responder.

There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase.

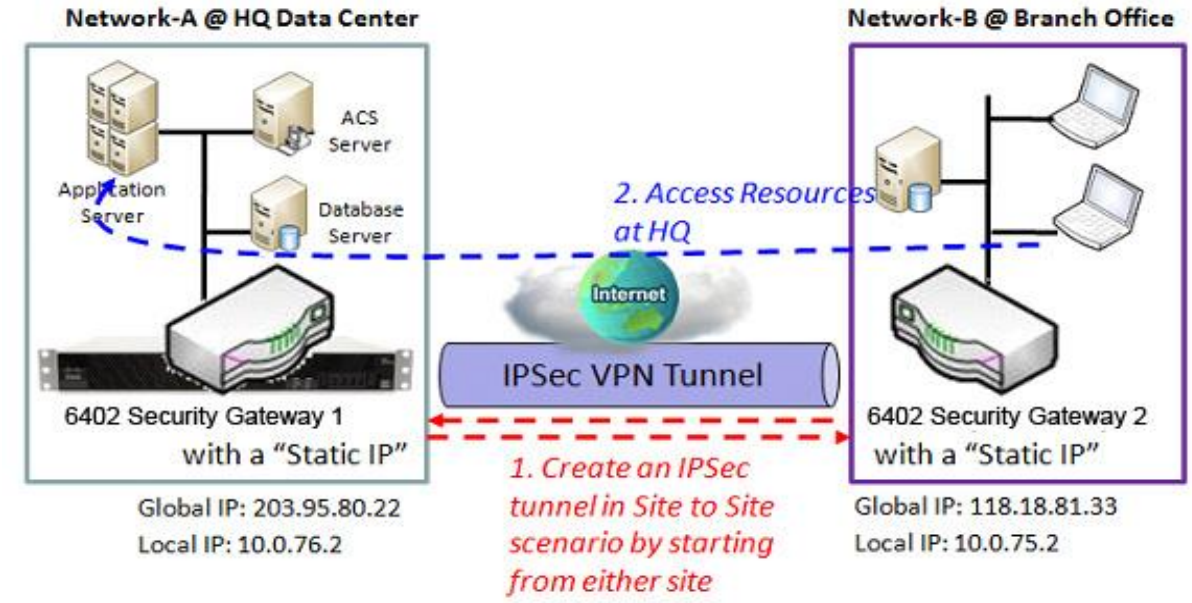
At the IKE phase, IKE authenticates the IPSec peers and negotiates an IKE SA (Security Association) to set up a secure channel for negotiating IPSec in phase 2.

The IKE Phase negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After both phases are complete, data can be transferred between IPSec peers.

Both the initiator and responder 6402's establishing the IPSec Tunnel must have a "Static IP" Address or use FQDN (Fully Qualified Domain Name) for "Site to Site" operation.
Before setting up the VPN connections, you may need to decide the type of tunnelling that is most suitable for your needs. There are three commonly used IPSec VPN connection scenarios as follows.

- When two sites wish to communicate securely over the Internet – IPSec provides an encrypted tunnel
- Both Peers need to establish a secure tunnel
- **Note** for IPSec both subnets must be on different subnets.
- **Note** for Static IPSec a maximum of 16 Tunnels is allowed – for dynamic tunnels more tunnels are supported.
- **Note** the less concurrent IPSec tunnels running, the better the performance and throughput of the 6402.

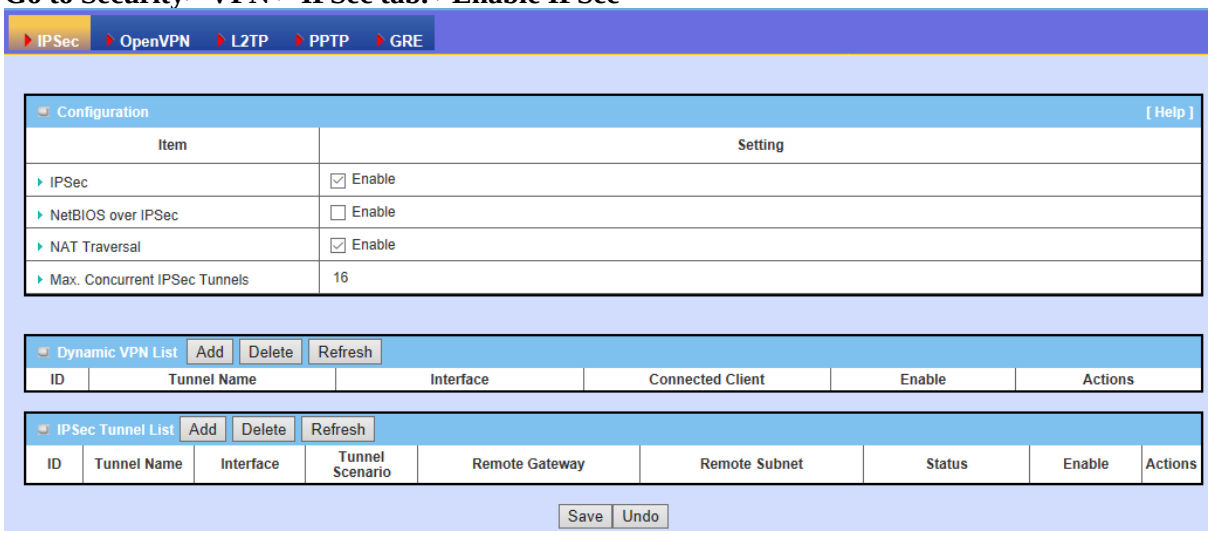
IPSec Site to Site Example Diagram



7.1.1.1 IPSec Configuration

IPSec allows users to create and configure IPSec tunnels. Before you proceed ensure that the VPN is enabled and saved. To enable VPN, go to **Security> VPN > Configuration** tab.

Go to Security> VPN > IPSec tab. >Enable IPSec



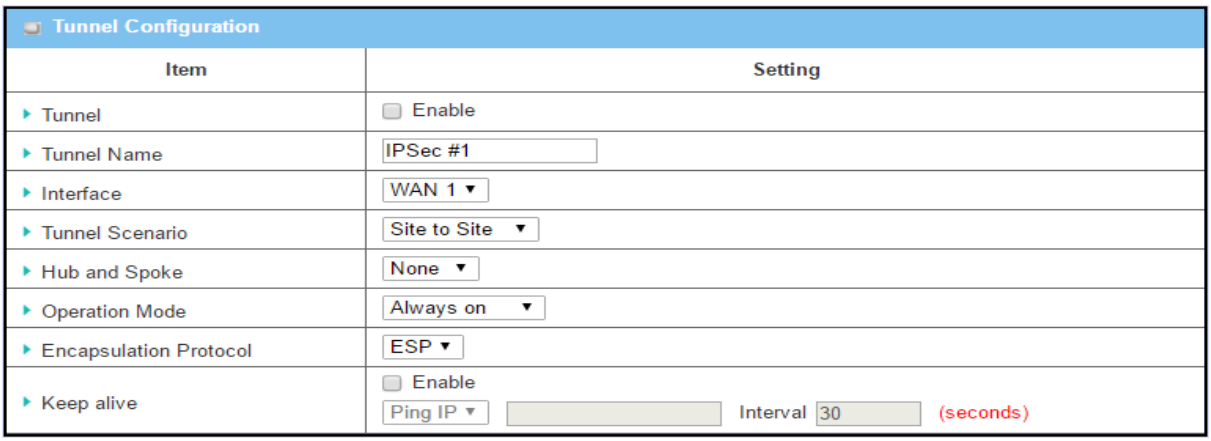
Configuration Window		
Item	**Value setting**	**Description**
IPSec	Unchecked by default	Click the **Enable** box to enable IPSec function.
NetBIOS over IPSec	Unchecked by default	Click the **Enable** box to enable NetBIOS over IPSec
NAT Traversal	Unchecked by default	Click the **Enable** box to enable NAT Traversal function.
Max. Concurrent IPSec Tunnels	16 is set by default	The specified value will limit the maximum number of simultaneous IPSec tunnel connection. The default value can be different for the purchased model.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

7.1.1.2 Create/Edit IPSec tunnel

Go to Security >IPSec (enable) >IPSec Server List

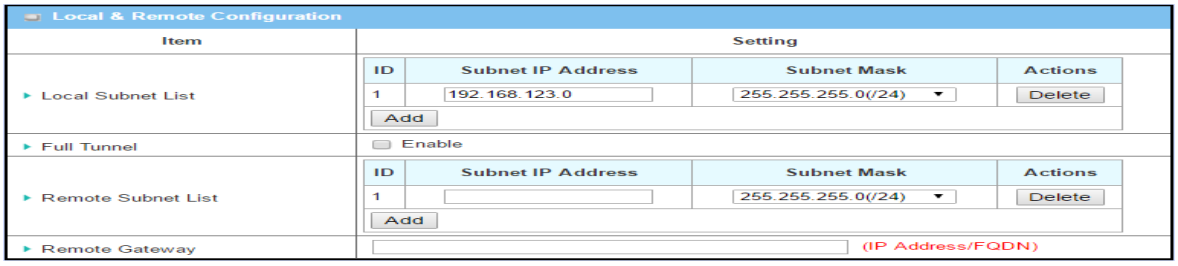
Ensure that the IPSec enable box is checked before further configuring any IPSec tunnel settings.

When the **Add/Edit** button is applied, a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. You must configure the tunnel details for both local and remote VPN devices.

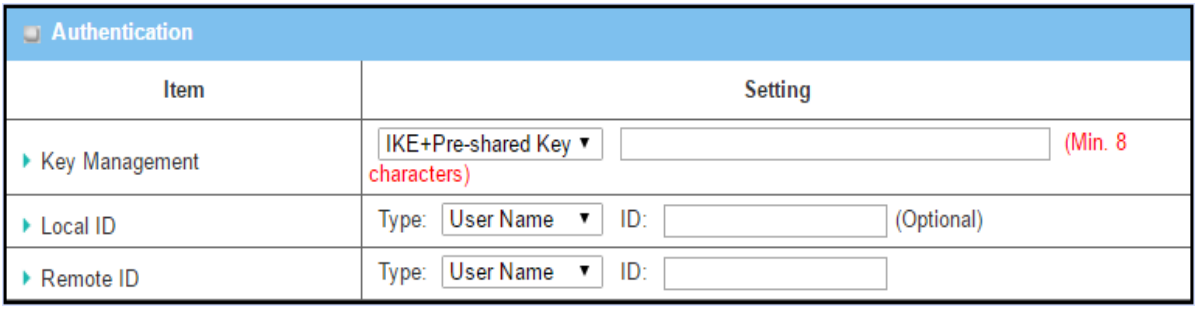


Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the IPSec tunnel
Tunnel Name	Mandatory Setting String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range*:** 1 ~ 19 characters.
Interface	Mandatory Setting WAN 1 is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	Mandatory Setting Site to site is selected by default	Select an IPSec tunnelling scenario from the dropdown box for your application. Select **Site-to-Site**, **Site-to-Host**, **Host-to-Site**, or **Host-to-Host**. With **Site-to-Site** or **Site-to-Host** or **Host-to-Site**, IPSec operates in tunnel mode. The difference among them is the number of subnets. With **Host-to-Host**, IPSec operates in transport mode.
Hub and Spoke	An optional setting None is set by default	Select from the dropdown box to setup your gateway for Hub-and-Spoke IPSec VPN Deployments. Select **None** if your deployments will not support Hub or Spoke encryption. Select **Hub** for a Hub role in the IPSec design. Select **Spoke** for a Spoke role in the IPSec design. Note: Hub and Spoke are available only for Site-to-Site VPN tunnelling specified in Tunnel Scenario. It is not available for Dynamic VPN tunnelling application.
Operation Mode	Mandatory Setting Always on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the IPSec tunnel is a failover tunnel function or an Always on tunnel. Note: If this IPSec is a failover tunnelling, you will need to select

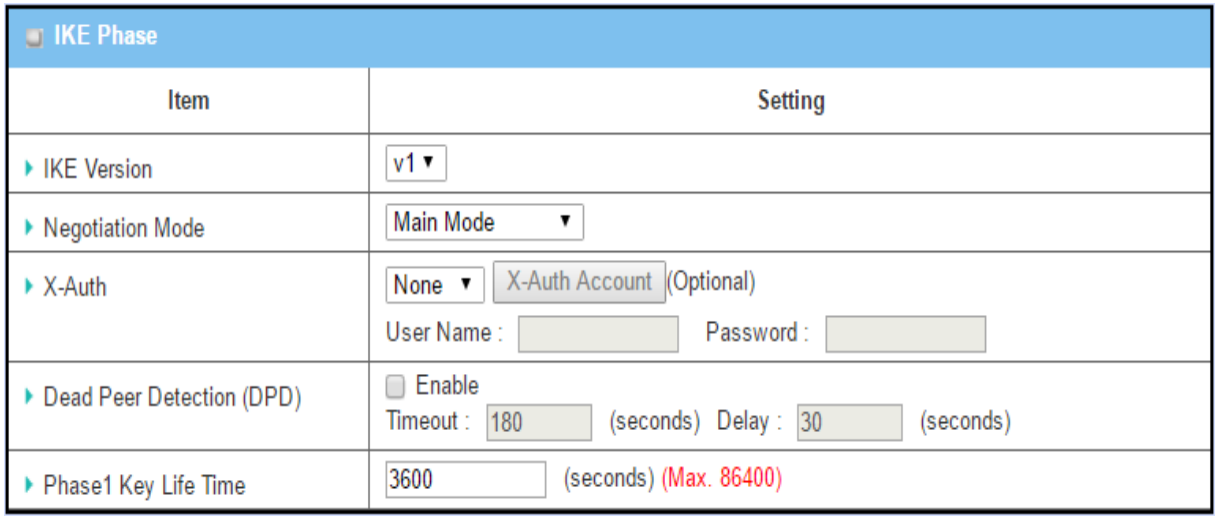
		a primary IPSec tunnel from which to failover to. **Load Balance** Define whether the IPSec tunnel connection will take part in load balance function of the gateway. You will not need to select with WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN > Load Balance tab. **Note**: Failover and Load Balance functions are not available for Dynamic VPN specified in Tunnel Scenario.
Encapsulation Protocol	Mandatory Setting ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.
Keep alive	Unchecked by default 30s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds. ***Value Range*:** 30 ~ 999 seconds. **Note**: Keep alive option is not available for Dynamic VPN specified in Tunnel Scenario.



Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet List	A Mandatory Setting	Specify the Local Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete a Local Subnet. **Note_1**: When Dynamic VPN option in Tunnel Scenario is selected, there will be only one subnet available. **Note_2**: When Host-to-Site or Host-to-Host option in Tunnel Scenario is selected, Local Subnet will not be available. **Note_3**: When Hub and Spoke option in Hub and Spoke is selected, there will be only one subnet available.
Full Tunnel	Unchecked by default	Click Enable box to enable Full Tunnel. **Note**: Full tunnel is available only for Site-to-Site specified in Tunnel Scenario.
Remote Subnet List	A Mandatory Setting	Specify the Remote Subnet IP address and Subnet Mask. Click the Add or Delete button to add or delete Remote Subnet setting.
Remote Gateway	A Mandatory Setting Format can be an ipv4 address or FQDN	Specify the Remote Gateway.



Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	A Mandatory setting Pre-shared Key8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key:**user needs to set a key (8 ~ 32characters). **IKE+X.509:** user needs Certificate to authenticate. IKE+X.509 will be available only when Certificate has been configured properly. Refer to Certificate section of this manual and also **Object Definition > Certificate** in web-based utility. **Manually:** user needs to enter key ID to authenticate. Manual key configuration will be explained in the following Manual Key Management section.
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select User Name for Local ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Local ID and enter the User@FQDN. Select Key ID for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Selected User Name for Remote ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Remote ID and enter the User@FQDN. Select Key ID for Remote ID and enter the Key ID (English alphabet or number) **Note**: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.



IKE Phase Window		
Item	**Value setting**	**Description**
IKE Version	A Mandatory setting v1 is selected by default	Specify the IKE version for this IPSec tunnel. Select v1 or v2 Note: IKE versions will not be available when Dynamic VPN option in Tunnel Scenario is selected, or AH option in Encapsulation Protocol is selected.
Negotiation Mode	Main Mode is set by default	Specify the Negotiation Mode for this IPSec tunnel. Select Main Mode or Aggressive Mode.
X-Auth	None is selected by default	Specify the X-Auth role for this IPSec tunnel. Select Server, Client, or None. Selected None no X-Auth authentication is required. Selected Server this gateway will be an X-Auth server. Click on the X-Auth Account button to create remote X-Auth client

		account. Selected Client this gateway will be a X-Auth client. Enter User name and Password to be authenticated by the X-Auth server gateway. Note: X-Auth Client will not be available for Dynamic VPN option selected in Tunnel Scenario.
Dead Peer Detection (DPD)	Unchecked by default Default Timeout 180s & Delay 30s	Click **Enable** box to enable **DPD** function. Specify the **Timeout** and **Delay** time in seconds. ***Value Range*:** 0 ~ 999 seconds for **Timeout** and **Delay**.
Phase1 Key Life Time	1. A Mandatory setting 2. Default 3600s 3. Max. 86400s	Specify the Phase1 Key Life Time. ***Value Range*:** 30 ~ 86400.

IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5	Group 2	Enable
3	DES	SHA1	Group 2	Enable
4	3DES	SHA1	Group 2	Enable

IKE Proposal Definition Window		
Item	**Value setting**	**Description**
IKE Proposal Definition	A Mandatory Setting	Specify the Phase 1 Encryption method. AES-auto/AES128/AES192/AES256/DES/3DES Specify the Authentication method. None/MD5/SHA1/SHA2-256/SHA2-512 Specify the DH Group None/Group1/ Group2/ Group5/ Group14/ Group15/ Group16/ Group17/ Group18/ Check Enable box to enable this setting

IPSec Phase

Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Phase Window		
Item	**Value setting**	**Description**
Phase2 Key Life Time	1. A Mandatory setting 2. 28800s is set by default 3. Max. 86400s	Specify the Phase2 Key Life Time in second. ***Value Range*:** 30 ~ 86400.

IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto	SHA1	Group 2	Enable
2	AES-auto	MD5		Enable
3	DES	SHA1		Enable
4	3DES	SHA1		Enable

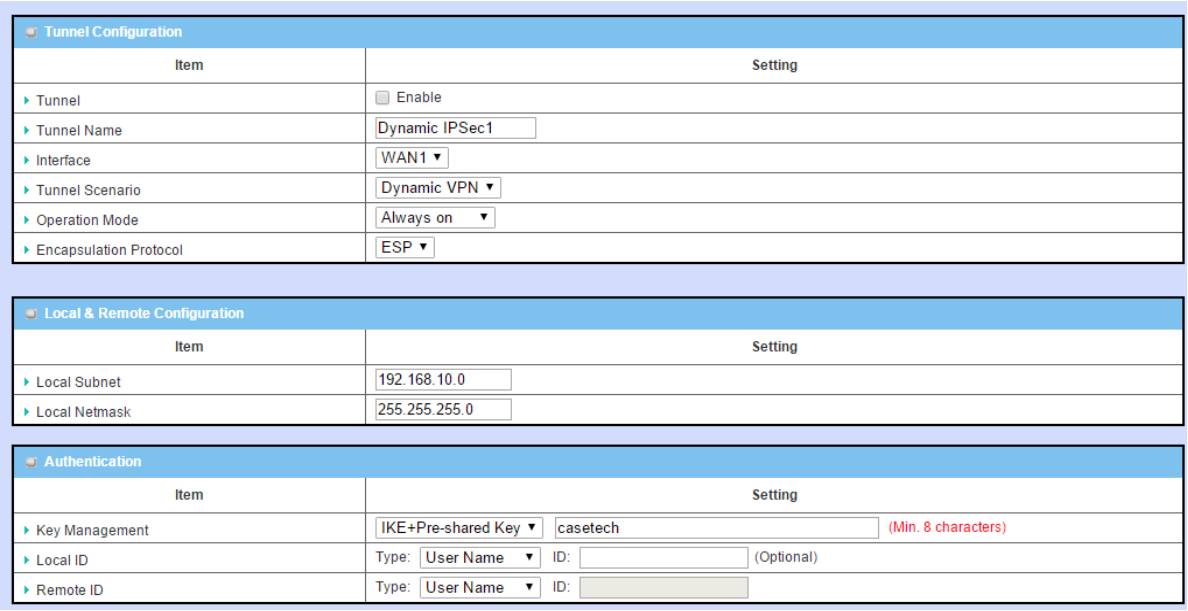
IPSec Proposal Definition Window		
Item	**Value setting**	**Description**
IPSec Proposal Definition	A Mandatory setting	Specify the Encryption method None/AES-auto/AES128/AES192/AES256/DES/3DES Specify Authentication method None/MD5/SHA1/SHA2-256/SHA2-512 Specify the PFS Group None/Group1/ Group2/ Group5/ Group14/ Group15/ Group16/ Group17/ Group18/ Click Enable to enable this setting
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** button to cancel the settings
Back	N/A	Click **Back** button to return to the previous page.

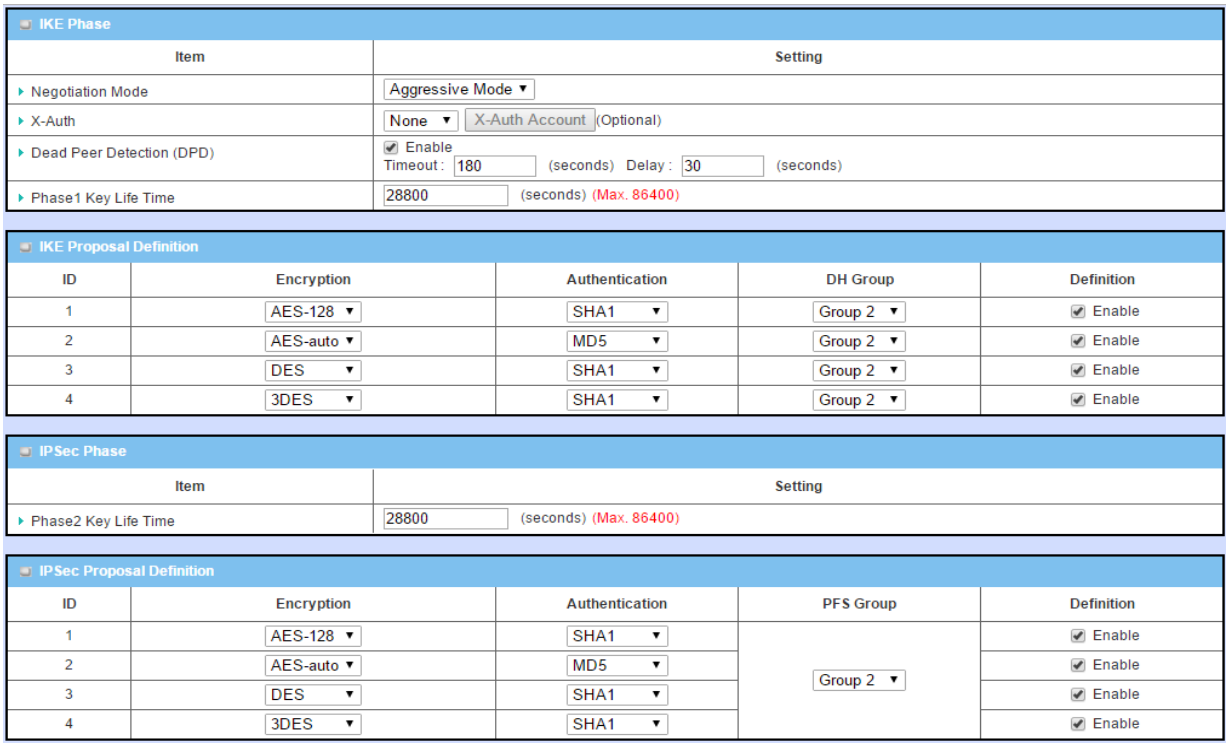
7.1.1.3 Dynamic IPSec

Dynamic IPSec is only configured with the local LAN subnet information and the basic Phase1/Phase2 and pre-shared key information. It learns the IP subnets of connected IPSec tunnels during the connection/authentication stages.

Dynamic IPSec can only be used on the central site with the remotes initializing the IPSec connections.

Go to Security >IPSec (enable) > Dynamic Server List > Add





IKE Phase

Item	Setting
Negotiation Mode	Aggressive Mode
X-Auth	None / X-Auth Account (Optional)
Dead Peer Detection (DPD)	Enable Timeout : 180 (seconds) Delay : 30 (seconds)
Phase1 Key Life Time	28800 (seconds) (Max. 86400)

IKE Proposal Definition

ID	Encryption	Authentication	DH Group	Definition
1	AES-128	SHA1	Group 2	Enable
2	AES-auto	MD5	Group 2	Enable
3	DES	SHA1	Group 2	Enable
4	3DES	SHA1	Group 2	Enable

IPSec Phase

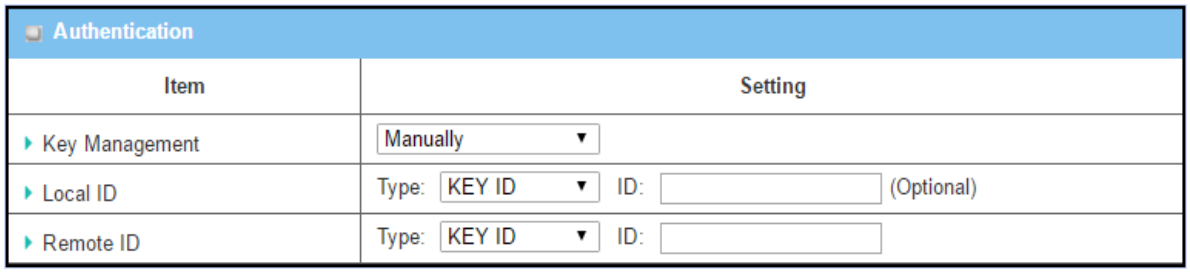
Item	Setting
Phase2 Key Life Time	28800 (seconds) (Max. 86400)

IPSec Proposal Definition

ID	Encryption	Authentication	PFS Group	Definition
1	AES-128	SHA1	Group 2	Enable
2	AES-auto	MD5		Enable
3	DES	SHA1		Enable
4	3DES	SHA1		Enable

7.1.1.4 Manual Key Management

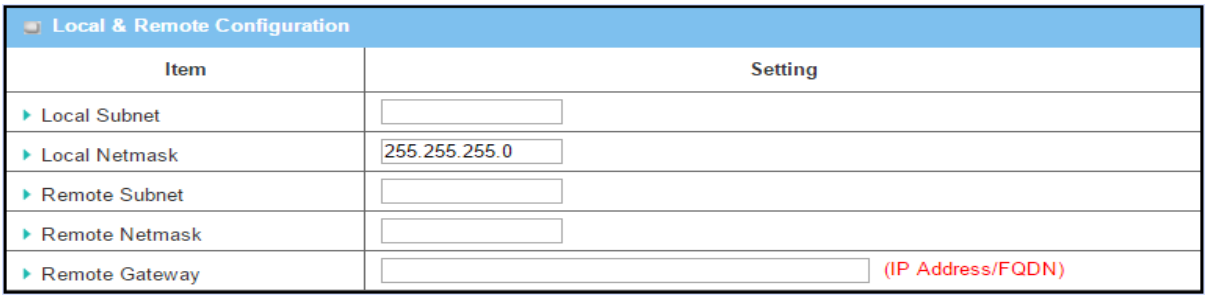
Under Authentication and 'Key Management' if 'Manually' is selected a series of windows to configure IPSec Manually is presented. The configuration windows are the Local & Remote Configuration, the Authentication, and the Manual Proposal.



Authentication

Item	Setting
Key Management	Manually
Local ID	Type: KEY ID ID: (Optional)
Remote ID	Type: KEY ID ID:

Authentication Window		
Item	**Value setting**	**Description**
Key Management	A Mandatory setting	Select Key Management from the dropdown box for this IPSec tunnel. In this section **Manually** is the option selected. For **IKE+Pre-shared Key** and **IKE+X.509** option, please refer to the table in previous 5 pages where key management is described.
Local ID	An optional setting	Specify the **Local ID** for this IPSec tunnel to authenticate. Select the **Key ID** for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the **Remote ID** for this IPSec tunnel to authenticate. Select **Key ID** for Remote ID and enter the Key ID(English alphabet or number).



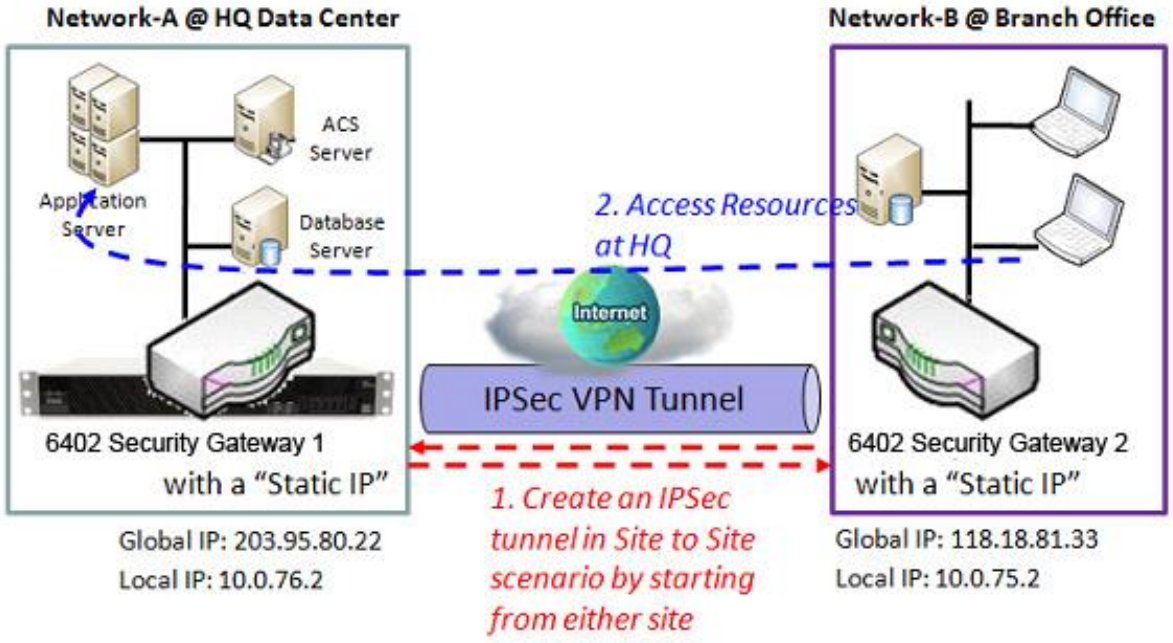
Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	A Mandatory setting	Specify the Local Subnet IP address and Subnet Mask.
Local Netmask	A Mandatory setting	Specify the Local Subnet Mask.
Remote Subnet	A Mandatory setting	Specify the Remote Subnet IP address
Remote Netmask	A Mandatory setting	Specify the **Remote** Subnet Mask.
Remote Gateway	A Mandatory setting An IPv4 address or FQDN format	Specify the Remote Gateway. The Remote Gateway

Under the 'Manually' Key Management authentication configuration, only one subnet is supported for both Local and Remote IPSec peer.

Manual Proposal Window		
Item	**Value setting**	**Description**
Outbound SPI	Hexadecimal format	Specify the Outbound SPI for this IPSec tunnel. ***Value Range***: 0 ~ FFFF.
Inbound SPI	Hexadecimal format	Specify the Inbound SPI for this IPSec tunnel. ***Value Range***: 0 ~ FFFF.
Encryption	1. A Mandatory setting 2. Hexadecimal format	Specify the Encryption Method and Encryption key Available encryption methods are DES/3DES/AES128/AES192/AES256 The key length for DES is 16, 3DES is 48, AES128 is 32, AES192 is 48, AES256 is 64. Note: When AH option in Encapsulation is selected, encryption will not be available.
Authentication	1. A Mandatory setting 2. Hexadecimal format	Specify the Authentication Method and Authentication key Available encryptions are None/MD5/SHA1/SHA2-256 Enter the key string (String length by the method which choose) The key length for MD5 is 32, SHA1 is 40, SHA2-256 is 64. Note: When AH option in Encapsulation Protocol is selected, None option in Authentication will not be available.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** button to cancel the settings
Back	N/A	Click **Back** button to return to the previous page.

7.1.1.5 IPSec Configuration Example

IPSec Site to Site Example Diagram



Network-A-is in the headquarters, and its subnet is 10.0.76.0/24. The 6402 for Network-A has the IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface.

Network-B - is in the branch office and has a subnet of 10.0.75.0/24. The 6402 at Network-B has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. Either side can initiate the IPSec VPN tunnel, allowing the Subnets of 10.0.75.0/24 and 10.0.76.0/24 to communicate securely.
Any peer gateway can be used as an Initiator or a Responder to establish the IPSec VPN tunnel.
Two phases (IKE and IPSec) are used to negotiate the IPSec VPN tunnel with pre-shared keys and optional X-Auth account / password.

IPSec VPN Configuration Example – Network A (HQ)
The following tables show the configuration for Network-A in the IPSec example network
Use default values for those parameters not shown in the table below.

Configuration Path	[IPSec]-[Configuration]
IPSec	■*Enable*
Configuration Path	**[IPSec]-[Tunnel Configuration]**
Tunnel	■ *Enable*
Tunnel Name	*s2s-101*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.75.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*118.18.81.33*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-A*
Remote ID	*User Name Network-B*
Configuration Path	**[IPSec]-[IKE Phase]**
Negotiation Mode	*Main Mode*
X-Auth	*None*

Configuration example for Network-B at Branch Office

The following table lists the configuration for Network B in the IPSec Example.

Note that the authentication parameters of both peers must match to establish the authentication process; this section provides an example configuration

Both negotiation Mode and X-Auth in "IKE Phase" the configuration window should match in both peers. There is at least one proposal entity in the IKE Proposal Definition at least one proposal entity in the IPSec Proposal definition must be the same for both peers.

Use default values for those parameters not shown in the table below.

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*
Configuration Path	**[IPSec]-[Tunnel Configuration]**
Tunnel	■ *Enable*
Tunnel Name	*s2s-201*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	*10.0.75.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.76.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*203.95.80.22*
Configuration Path	**[IPSec]-[Authentication]**
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-B*
Remote ID	*User Name Network-A*
Configuration Path	**[IPSec]-[IKE Phase]**
Negotiation Mode	*Main Mode*
X-Auth	*None*

7.1.1.6 IPSec Example Dynamic VPN Using FQDN

There are times when a remote user needs to access the resources on their organisation's server from a remote location which does not have a fixed IP address, such as from a mobile device or temporary location. Under these circumstances we need to use a dynamic address at the remote site (Initiator) and FQDN (Fully Qualified Domain Name) to establish an IPSec connection. They key features are;

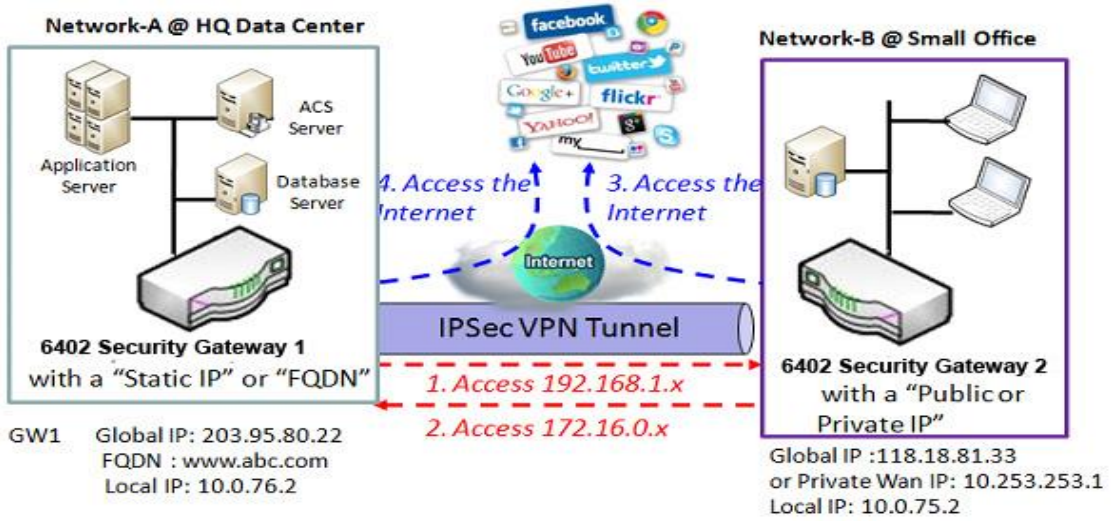
- IPSec where one end of the link uses a dynamic IP Address – i.e. mobile users
- One end (The host) requires a fixed IP address, remote sites can be dynamic and uses (FQDN) Fully Qualifies Domain Name

The remote dynamic address site has information within its packet which is recognised and accepted by the 6402 at central site which has a fixed IP Address. The packets carry an ID for the remote site including the ID of the remote 6402 subnet. **Note-** that the remote peer has to initiate the tunnel establishing process first in this application scenario.

IPSec FQDN – Configuration Example

In the example below the Initiator is using a mobile device with a dynamic IP address, only the Responder (Central site) has a "Static IP" or a "FQDN". Two phases (IKE and IPSec) will be used to negotiate the IPSec VPN tunnel with a pre-shared key and optional X-Auth account / password.
Network-A - (in the diagram above) is the headquarters and has a subnet of 10.0.76.0/24. The 6402 Gateway for Network-A has the IP address of 10.0.76.2 for its LAN and 203.95.80.22 (or FQDN for example www.abc.com) for its WAN interface.

Network-B - is the mobile office and has a subnet of 10.0.75.0/24. The 6402 at Network-B has a dynamic IP address of 118.18.81.33 for its WAN interface or private IP address of 10.253.253.1 on the Cellular Network
The 'Dynamic VPN IPSec tunnel' is started from the mobile site, allowing both subnets of 10.0.75.0/24 and 10.0.76.0/24 to securely communicate.



IPSec FQDN Configuration Example – Network A

The following table shows the configuration for Network-A in the IPSec FQDN example network
Use default value for those parameters not shown in the table below.

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*
Configuration Path	**[IPSec]-[Tunnel Configuration]**
Tunnel	■ *Enable*
Tunnel Name	*dvpn-101*
Interface	*WAN 1*
Tunnel Scenario	*Dynamic VPN*
Operation Mode	*Always on*
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*
Configuration Path	**[IPSec]-[Authentication]**
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-B*
Configuration Path	**[IPSec]-[IKE Phase]**
Negotiation Mode	*Main Mode*
X-Auth	*None*

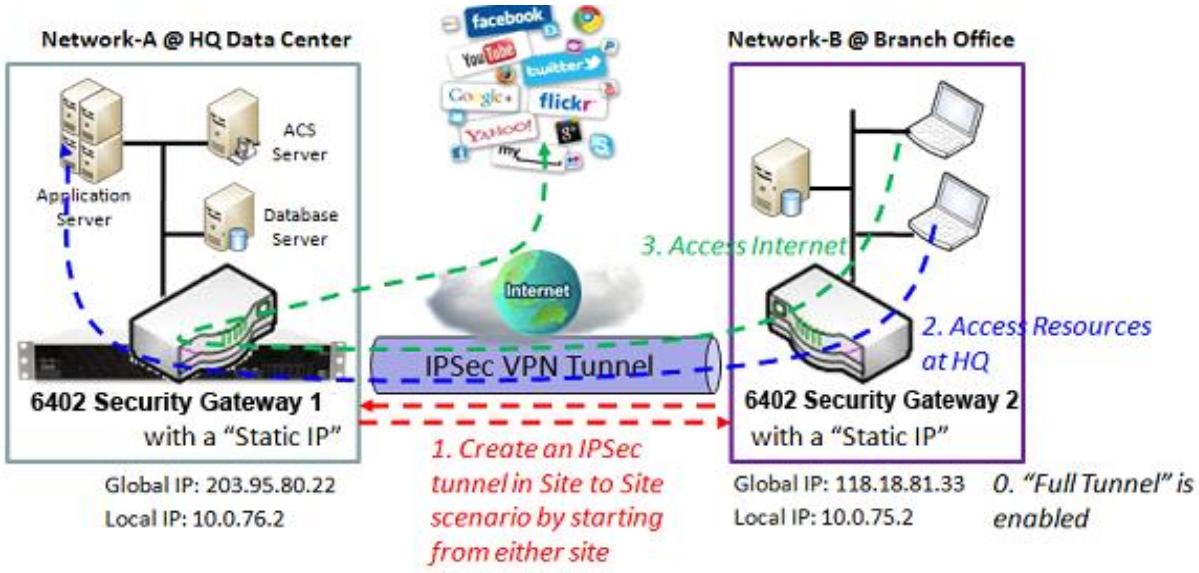
IPSec FQDN Example - Network-B Mobile Office

The following table lists the configuration for Site B in the FQDN IPSec VPN Example.
Note that the authentication parameters of both peers must match to complete the authentication process successfully.
Negotiation Mode and X-Auth in "IKE Phase" configuration window should match on both peers.
There must be at least one proposal entity in IKE Proposal Definition and at least one proposal entity in the IPSec Proposal Definition, these must be the same for both peers. Use the default values if they are not shown in following tables.

Configuration Path	**[IPSec]-[Configuration]**
IPSec	■ ***Enable***
Configuration Path	[IPSec]-[Tunnel Configuration]
Tunnel	■ ***Enable***
Tunnel Name	***dvpn-201***
Interface	***WAN 1***
Tunnel Scenario	***Site to Site***
Operation Mode	***Always on***
Keep alive	■ ***Enable*** ***Ping FQDN →www.abc.com, Interval 120 sec***
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	***10.0.75.0***
Local Netmask	***255.255.255.0***
Full Tunnel	***Disable***
Remote Subnet	***10.0.76.0***
Remote Netmask	***255.255.255.0***
Remote Gateway	***203.95.80.22 or www.abc.com*** ***PS: Some advanced users will use Dynamic DDS function to update Global IP address which is not fixed .We suggest enabling "Keep alive" item.***
Configuration Path	**[IPSec]-[Authentication]**
Key Management	***IKE+Pre-shared Key 12345678***
Local ID	***User Name Network-B***
Configuration Path	[IPSec]-[IKE Phase]
Negotiation Mode	***Main Mode***
X-Auth	***None***

7.1.1.7 Full Tunnel Site to Site Example

Example diagram for Full Tunnel Site to Site



Full Tunnel Site to Site VPN Requirements

- Enable the full Tunnel Feature to allow clients on remote site (Network B) – to access resources at headquarters via the secure VPN Tunnel
- Both Networks have their own subnets.
- Clients at the remote site (Network B) go over the VPN Tunnel to the 6402 at Network A (HQ) to access the internet. The 6402 at Network A controls Internet Access for users at site B
- Either the 6402 at Network A or Network B can be an initiator or responder.
- When the tunnel is enabled between Network A and Network B, all traffic will pass over the VPN Tunnel

Network-A -is in the headquarters, its subnet is 10.0.76.0/24. The 6402 at Network-A has the IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface.

Network-B - is in the branch office and its subnet is 10.0.75.0/24. The 6402 for Network-B has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface.

- Both Initiator and Responder in the IPSec tunnel must have a "Static IP" or a "FQDN" for "Site to Site" connection.
- Two phases (IKE and IPSec) are used to negotiate the IPSec VPN tunnel with a pre-shared key and optional X-Auth account / password.
- The "Full Tunnel" feature enables drives all packet flows from Network B to go over the established VPN tunnel.
- The HQ Gateway controls and secures the IP network requests from the branch office.

Note- that the authentication parameters of both peers must match to complete the authentication process.
In Negotiation Mode and X-Auth in the "IKE Phase" the configuration window should be matched by both peers.
There is at least one proposal entity in IKE Proposal Definition and at least one proposal entity in IPSec Proposal Definition , these must be the same for both peers. Use the setting in the setup example if they are not shown below.

Full Tunnel Example Configuration -Network-A at HQ

The following tables list the configuration for Network A in the above example diagram.
Use default value for those parameters that are not shown below.

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*
Configuration Path	**[IPSec]-[Tunnel Configuration]**
Tunnel	■ *Enable*
Tunnel Name	*s2s-101*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	*10.0.76.0*
Local Netmask	*255.255.255.0*
Full Tunnel	*Disable*
Remote Subnet	*10.0.75.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*118.18.81.33*

Configuration Path	[IPSec]-[Authentication]
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-A*
Remote ID	*User Name Network-B*
Configuration Path	**[IPSec]-[IKE Phase]**
Negotiation Mode	*Main Mode*
X-Auth	*None*

Full Tunnel Example Configuration - Network-B at Branch Office

The table lists the configuration for Network B in the example diagram above.
Use the default value for those parameters that are not mentioned in this table. Please note that the special parameter configuration options are shown below and depicted in red.

Configuration Path	[IPSec]-[Configuration]
IPSec	■ *Enable*
Configuration Path	**[IPSec]-[Tunnel Configuration]**
Tunnel	■ *Enable*
Tunnel Name	*s2s-201*
Interface	*WAN 1*
Tunnel Scenario	*Site to Site*
Operation Mode	*Always on*
Configuration Path	**[IPSec]-[Local & Remote Configuration]**
Local Subnet	*10.0.75.0*
Local Netmask	*255.255.255.0*
Full Tunnel	■ *Enable (Special Option)*
Remote Subnet	*10.0.76.0*
Remote Netmask	*255.255.255.0*
Remote Gateway	*203.95.80.22*
Configuration Path	**[IPSec]-[Authentication]**
Key Management	*IKE+Pre-shared Key 12345678*
Local ID	*User Name Network-B*
Remote ID	*User Name Network-A*
Configuration Path	**[IPSec]-[IKE Phase]**
Negotiation Mode	*Main Mode*
X-Auth	*None*

7.1.1.8 Create/Edit Dynamic VPN Server List

Dynamic server List	Add	Delete			
ID	Tunnel Name	Interface	Connected Client	Enable	Actions

Similar to creating an IPSec VPN Tunnel fora site/host scenario, when the Edit button is applied a series of configuration screens will appear. They are Tunnel Configuration, Local & Remote Configuration, Authentication, IKE Phase, IKE Proposal Definition, IPSec Phase, and IPSec Proposal Definition. Configure the tunnel details for the gateway as a Dynamic VPN server.

Tunnel Configuration	
Item	Setting
Tunnel	Enable
Tunnel Name	Dynamic IPSec1
Interface	WAN1
Tunnel Scenario	Dynamic VPN
Operation Mode	Always on
Encapsulation Protocol	ESP

Tunnel Configuration Window		
Item	**Value setting**	**Description**
Tunnel	Unchecked by default	Check the **Enable** box to activate the Dynamic IPSec VPN tunnel
Tunnel Name	A Mandatory setting String format can be any text	Enter a tunnel name. Enter a name that is easy for you to identify. ***Value Range*:** 1 ~ 19 characters.
Interface	A Mandatory setting WAN 1 is selected by default	Select WAN interface on which IPSec tunnel is to be established.
Tunnel Scenario	A Mandatory setting VPN is selected by default	The IPSec tunnelling scenario is fixed to Dynamic VPN.
Operation Mode	1. A Mandatory setting 2. Always on is selected by default	The available operation mode is Always On. Failover and Load Balance options are not available for the Dynamic IPSec scenario.
Encapsulation Protocol	A Mandatory setting ESP is selected by default	Select the Encapsulation Protocol from the dropdown box for this IPSec tunnel. Available encapsulations are ESP and AH.

Local & Remote Configuration	
Item	Setting
Local Subnet	
Local Netmask	

Local & Remote Configuration Window		
Item	**Value setting**	**Description**
Local Subnet	A Mandatory setting	Specify the Local Subnet IP address.
Local Netmask	A Mandatory setting	Specify the Local Subnet Mask.

Authentication	
Item	Setting
Key Management	IKE+Pre-shared Key (Min. 8 characters)
Local ID	Type: User Name ID: (Optional)
Remote ID	Type: User Name ID:

Authentication Configuration Window		
Item	**Value setting**	**Description**
Key Management	1. A Mandatory setting 2. Pre-shared Key 8 to 32 characters.	Select Key Management from the dropdown box for this IPSec tunnel. **IKE+Pre-shared Key:**user needs to set a key (Min. 8 characters).
Local ID	An optional setting	Specify the Local ID for this IPSec tunnel to authenticate. Select User Name for Local ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Local ID and enter the User@FQDN. Select Key ID for Local ID and enter the Key ID (English alphabet or number).
Remote ID	An optional setting	Specify the Remote ID for this IPSec tunnel to authenticate. Selected User Name for Remote ID and enter the username. The username may include but can't be all numbers. Select FQDN for Local ID and enter the FQDN. Select User@FQDN for Remote ID and enter the User@FQDN. Select Key ID for Remote ID and enter the Key ID (English alphabet or number) **Note**: Remote ID will be not available when Dynamic VPN option in Tunnel Scenario is selected.

7.1.2 OpenVPN Introduction

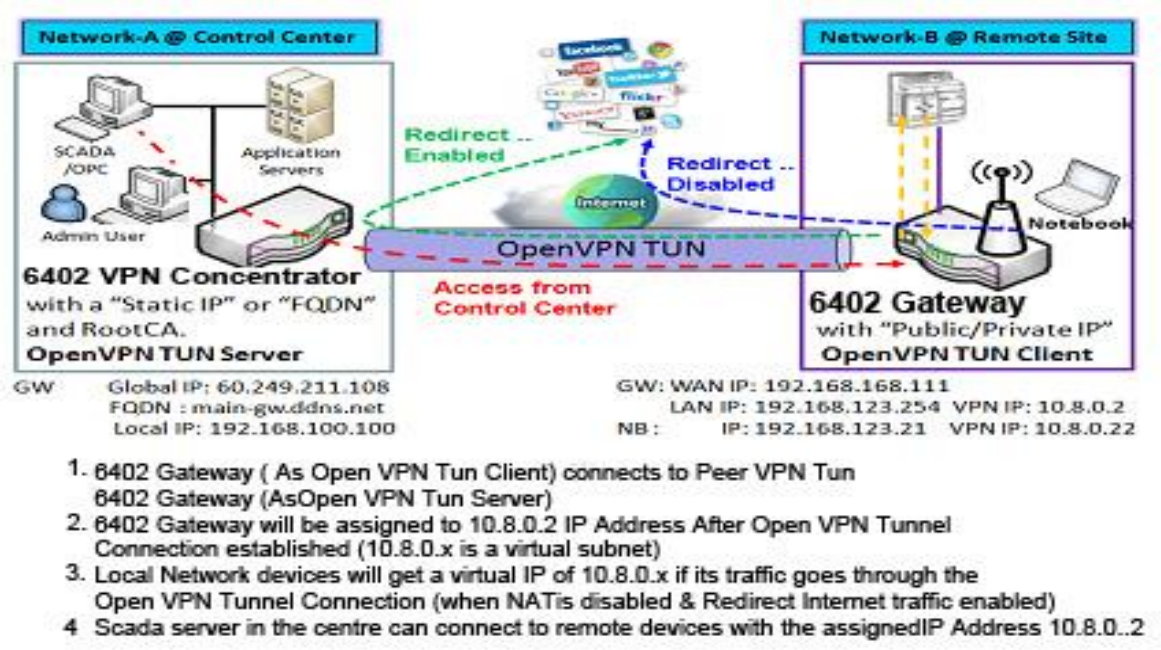
OpenVPN is an application that implements virtual private network (VPN) techniques for creating secure point-to-point or site-to-site connections routed or bridged.
The key features of Open VPN are

- Uses a custom security protocol that uses SSL / TLS for key exchange, which makes it capable of traversing Network Address Translation (NAT) and the Firewall.
- Open VPN Allows peers to authenticate each other using a Static Key (Pre-shared key) or certificates.
- When used in a multi-client server configuration it allows the server to release an authentication certificate for every client, using signature and certificate authority.
- It uses the OpenSSL encryption library, as well as the SSLv3/TLSv1protocol, and contains many security and control features.
- OpenVPN Tunnelling is a Client and Server based tunnelling technology.
- The OpenVPN Server must have a Static IP or a FQDN and maintain a Client list.
- The OpenVPN Client may be a mobile user or mobile site with a public IP or private IP and requesting the OpenVPN tunnel connection.
- The 6402 supports both OpenVPN Server and OpenVPN Client features to meet different application requirements.

7.1.2.1 Two Open VPN connection scenarios – TAP& TUN

The 6402 can create either a layer-3 based IP tunnel (TUN), or a layer-2 based Ethernet (TAP) that can carry any type of Ethernet traffic.
When configuring the device as a Server or Client, you have to specify which type of OpenVPN connection scenario is to be adopted.

7.1.2.2 Open VPN TUN- (Routed Mode) – Example



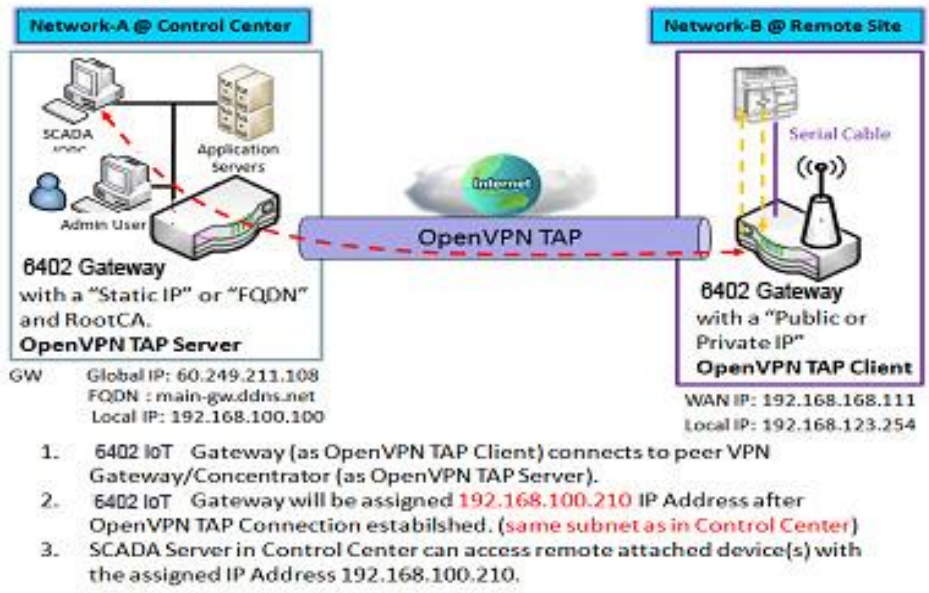
1. 6402 Gateway (As Open VPN Tun Client) connects to Peer VPN Tun 6402 Gateway (AsOpen VPN Tun Server)
2. 6402 Gateway will be assigned to 10.8.0.2 IP Address After Open VPN Tunnel Connection established (10.8.0.x is a virtual subnet)
3. Local Network devices will get a virtual IP of 10.8.0.x if its traffic goes through the Open VPN Tunnel Connection (when NATis disabled & Redirect Internet traffic enabled)
4. Scada server in the centre can connect to remote devices with the assignedIP Address 10.8.0..2

7.1.2.3 OpenVPN TUN Scenario

- The term "TUN" mode is referred to routing mode and operates with layer 3 packets.
- In routing mode, the VPN client is given an IP address on a different subnet to the local LAN under the Open VPN server.
- This virtual subnet is created for connecting to any remote VPN computers. In routing mode, the Open VPN server creates a "TUN" interface with its own IP address pool which is different to the local LAN. Remote hosts that dial-in will get an IP address inside the virtual network and will have access only to the server where Open VPN resides.
- If you want to offer remote access to a VPN server from client(s) and inhibit the access to remote LAN resources under VPN server, the Open VPN TUN mode is the simplest solution.
- In the diagram above, the 6402 Gateway is configured as an Open VPN TUN Client and connects to an Open VPN TUN Server.

Once the Open VPN TUN connection is established, the connected TUN client will be assigned a virtual IP Address of (10.8.0.2) which belongs to a virtual subnet that is different to the local subnet in the Control Centre. The local networked devices will get a virtual IP address of 10.8.0.x if its traffic goes through the Open VPN TUN connection when the Redirect Internet Traffic setting is enabled; The SCADA Server in the Control Centre can access remote attached serial device(s) with the virtual IP address (10.8.0.2).

7.1.2.4 OpenVPN TAP (Bridged Mode)Scenario



- The term "TAP" refers to bridge mode and operates with layer 2 packets.
- In bridge mode, the VPN client is given an IP address on the same subnet as the LAN where under the Open VPN server resides. Under such configuration, the OpenVPN client can directly access the resources on the LAN.
- If you want to offer remote access to the entire remote LAN for VPN client(s), you have to setup OpenVPN in “TAP” bridge mode.

As shown in the diagram above, the 6402 Gateway is configured as an Open VPN TAP Client and connects to an OpenVPN TAP Server. Once the OpenVPN TAP connection is established, the connected TAP client will be assigned a virtual IP address of (192.168.100.210) which is the same subnet as that of local subnet in Network A. With this connection, the SCADA Server in the Control Centre can access remote attached serial device(s) with the virtual IP address of (192.168.100.210).

7.1.2.5 Open VPN Configuration.

Go to Security > VPN > Open VPN tab.
The Open VPN setting allows user to create and configure OpenVPN tunnels.

Enable Open VPN

Enable Open VPN and select a configuration, either server or client, for the gateway to operate.

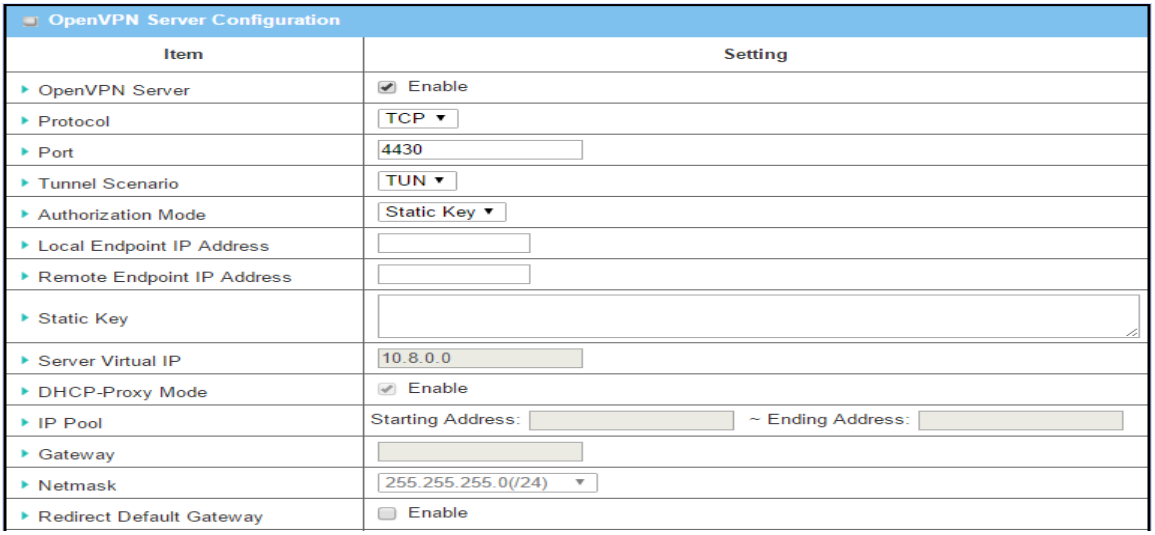
Configuration	
Item	Setting
OpenVPN	Enable
Server / Client	Server

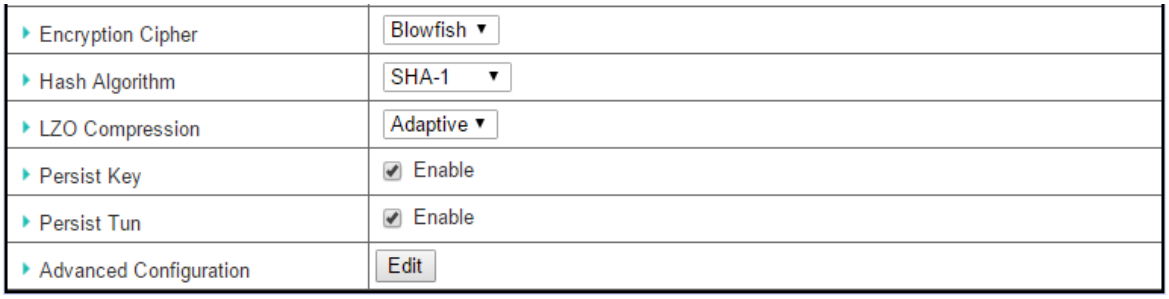
Configuration		
Item	**Value setting**	**Description**
OpenVPN	The box is unchecked by default	Check the **Enable** box to activate the Open VPN function.
Server/ Client	Server Configuration is selected by default.	When **Server** is selected, as the name indicated, server configuration will be displayed below for further setup. When **Client** is selected, you can specify the client settings in another client configuration window.

7.1.2.6 As an Open VPN Server

If Server is selected, an Open VPN Server Configuration screen will appear.

The Open VPN Server Configuration window can let you enable the Open VPN server function, and specify the virtual IP address of the Open VPN server, where the remote Open VPN clients dial in and the protocol authenticated



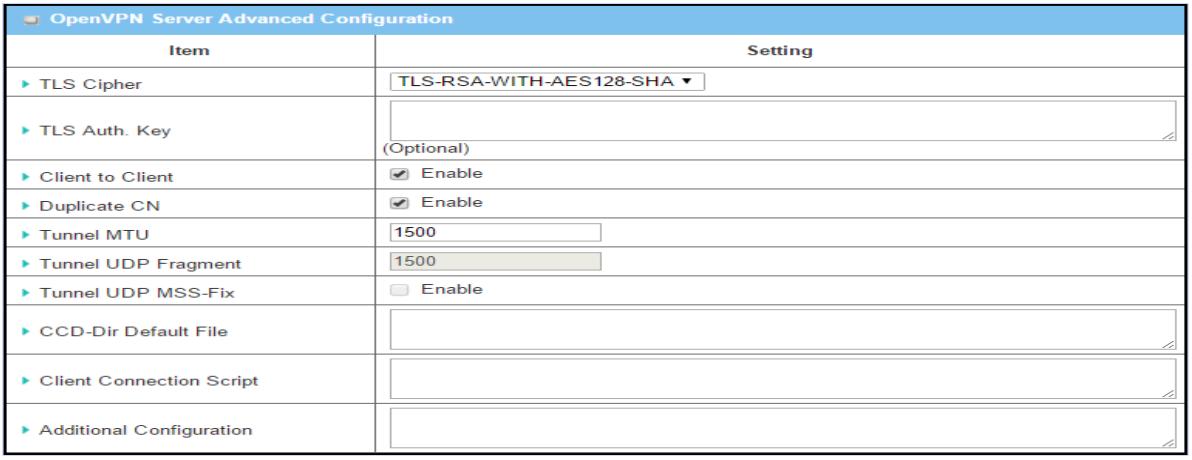


OpenVPN Server Configuration		
Item	**Value setting**	**Description**
Open VPN Server	The box is unchecked by default.	Click the **Enable** to activate OpenVPN Server functions.
Protocol	Mandatory Setting By default, **TCP** is selected.	Define the selected **Protocol** for connecting to the OpenVPN Server. • Select **TCP , or TCP /UDP** -> The TCP protocol will be used to access the OpenVPN Server, and **Port** will be set as 4430 automatically. • Select **UDP** -> The UDP protocol will be used to access the OpenVPN Server, and **Port** will be set as 1194 automatically.
Port	Mandatory Setting By default, **4430** is set.	Specify the **Port** for connecting to the OpenVPN Server. ***Value Range***: 1 ~ 65535.
Tunnel	Mandatory Setting	Specify the type of **Tunnel Scenario** for connecting to the

Scenario	By default, **TUN** is selected.	OpenVPN Server. It can be **TUN** for TUN tunnel scenario or **TAP** for TAP tunnel scenario.
Authorisation Mode	Mandatory Setting By default, **Static Key** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Server Cert.** and **DH PEM** will be displayed. **CA Cert.** could be generated in Certificate. Refer to **Object Definition**>**Certificate**>**Trusted Certificate**. **Server Cert.** could be generated in Certificate. Refer to **Object Definition**>**Certificate**>**My Certificate**. • **Static Key**->The OpenVPN will use static key (pre-shared) authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed. Note: Static Key will be available only when TUN is chosen in Tunnel Scenario.
Local Endpoint IP Address	A Mandatory Setting	Specify the virtual **Local Endpoint IP Address** of this OpenVPN gateway. ***Value Range*:** The IP format is 10.8.0.x, the range of x is 1~254. **Note**: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	A Mandatory Setting	Specify the virtual **Remote Endpoint IP Address** of the peer OpenVPN gateway. ***Value Range*:** The IP format is 10.8.0.x, the range of x is 1~254. **Note:** Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	A Mandatory Setting	Specify the **Static Key**. **Note**: Static Key will be available only when Static Key is chosen in Authorization Mode.
Server Virtual IP	A Mandatory Setting	Specify the **Server Virtual IP**. ***Value Range*:** The IP format is 10.y.0.0, the range of y is 1~254. **Note:** Server Virtual IP will be available only when TLS is chosen in Authorisation Mode.
DHCP-Proxy Mode	Mandatory Setting The box is checked by default.	Check the **Enable** box to activate the **DHCP-Proxy Mode**. Note: DHCP-Proxy Mode will be available only when TAP is chosen in Tunnel Device.
IP Pool	A Mandatory Setting	Specify the virtual **IP pool** setting for the OpenVPN server. You have to specify the **Starting Address** and **Ending Address** as the IP address pool for the OpenVPN clients. **Note**: IP Pool will be available only when TAP is chosen in Tunnel Device, &DHCP-Proxy Mode is unchecked (disabled).
Gateway	A Mandatory Setting	Specify the **Gateway** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. **Note**: Gateway will be available only when TAP is chosen in Tunnel Device, &DHCP-Proxy Mode is unchecked (disabled).
Netmask	By default **- select one -** is selected.	Specify the **Netmask** setting for the OpenVPN server. It will be assigned to the connected OpenVPN clients. ***Value Range*:** 255.255.255.0/24 (only support class C) **Note_1**: Netmask will be available when TAP is chosen in Tunnel Device, &DHCP-Proxy Mode is unchecked (disabled). **Note_2**: Netmask will also be available when TUN is chosen in Tunnel Device.
Redirect Default Gateway	Optional setting. Unchecked by default.	Check the **Enable** box to activate the **Redirect Default Gateway** function.
Encryption	Mandatory Setting	Specify the **Encryption Cipher** from the dropdown list.

Cipher	By default, **Blowfish** is selected.	It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default, **SHA-1** is selected.	Specify the **Hash Algorithm** from the dropdown list. It can be**SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**
LZO Compression	By default, **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Persis Key	1. Optional setting. 2. Checked by default.	Check the **Enable** box to activate the **Persis Key** function.
Persis Tun	Optional setting. Checked by default.	Check the **Enable** box to activate the **Persis Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.

When Advanced Configuration is selected, an OpenVPN Server Advanced Configuration screen shown below will appear.

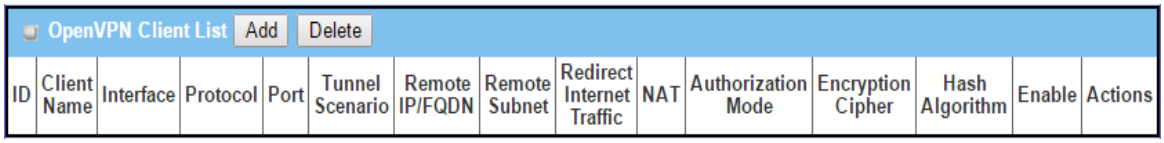


OpenVPN Server Advanced Configuration		
Item	**Value setting**	**Description**
TLS Cipher	Mandatory Setting **TLS-RSA-WITH AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **TLS-RSA-WITH-AES128-SHA / TLS-DHE-DSS-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-RSA-WITH-RC4-MD5 / None.** **Note**: TLS Cipher will be available only when TLS is chosen in Authorization Mode.
TLS Auth. Key	An Optional setting. String format: any text	Specify the **TLS Auth. Key.** **Note**: TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
Client to Client	The box is checked by default	Check the **Enable** box to enable the traffics among different OpenVPN Clients. **Note**: Client to Client will be available only when TLS is chosen in Authorization Mode
Duplicate CN	The box is checked by default	Check the **Enable** box to activate the **Duplicate CN** function. **Note**: Duplicate CN will be available only when TLS is chosen in Authorization Mode
Tunnel MTU	1. Mandatory Setting	Specify the **Tunnel MTU. (Default value is 1500)** ***Value Range*: 0 ~ 1500.**

Tunnel UDP Fragment	Mandatory Setting The value is **1500** by default	Specify the **Tunnel UDP Fragment.** By default, it is equal to **Tunnel MTU**. ***Value Range*:** 0 ~ 1500. **Note**: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	An Optional setting. The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** Function. **Note**: Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
CCD-Dir Default File	An Optional setting. String format: any text	Specify the **CCD-Dir Default File.** ***Value Range*:** 0 ~ 256 characters.
Client Connection Script	An Optional setting. String format: any text	Specify the **Client Connection Script.** ***Value Range*:** 0 ~ 256 characters.
Additional Configuration	An Optional setting. String format: any text	Specify the **Additional Configuration.** ***Value Range*:** 0 ~ 256 characters.

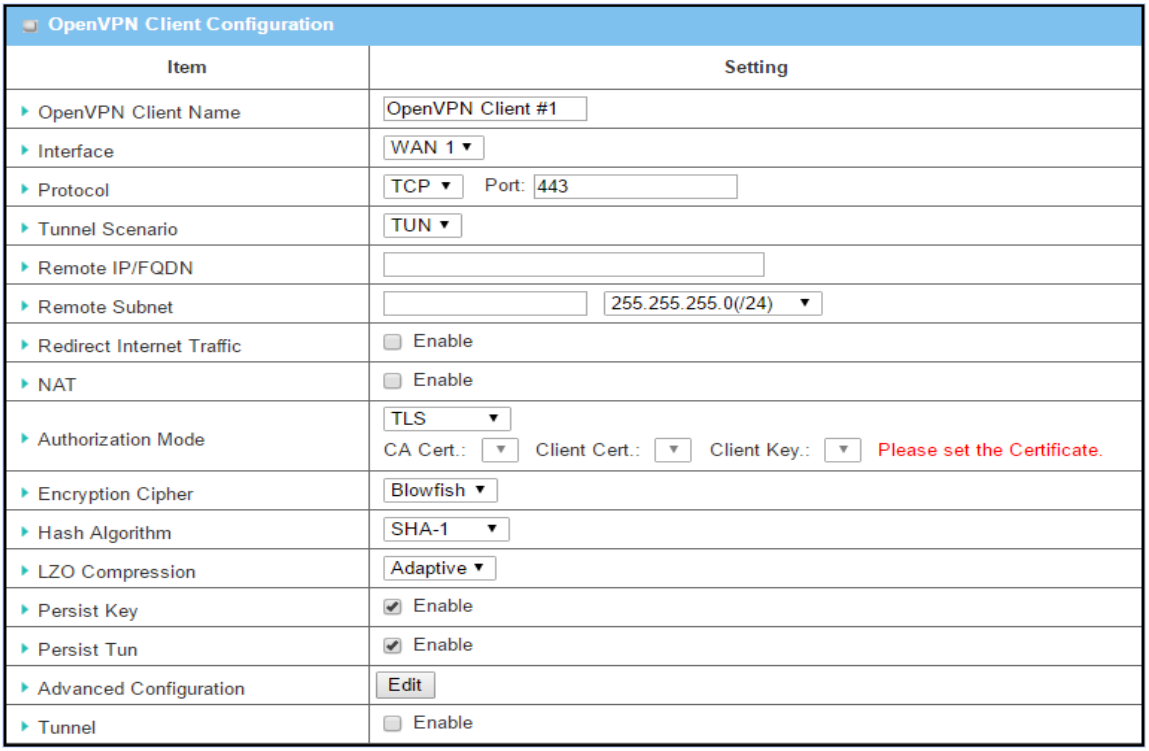
7.1.2.7 As an Open VPN Client

If **Client** is selected, an Open VPN Client List the following screen will appear.



When the Add button is applied, the Open VPN Client Configuration screen will appear.

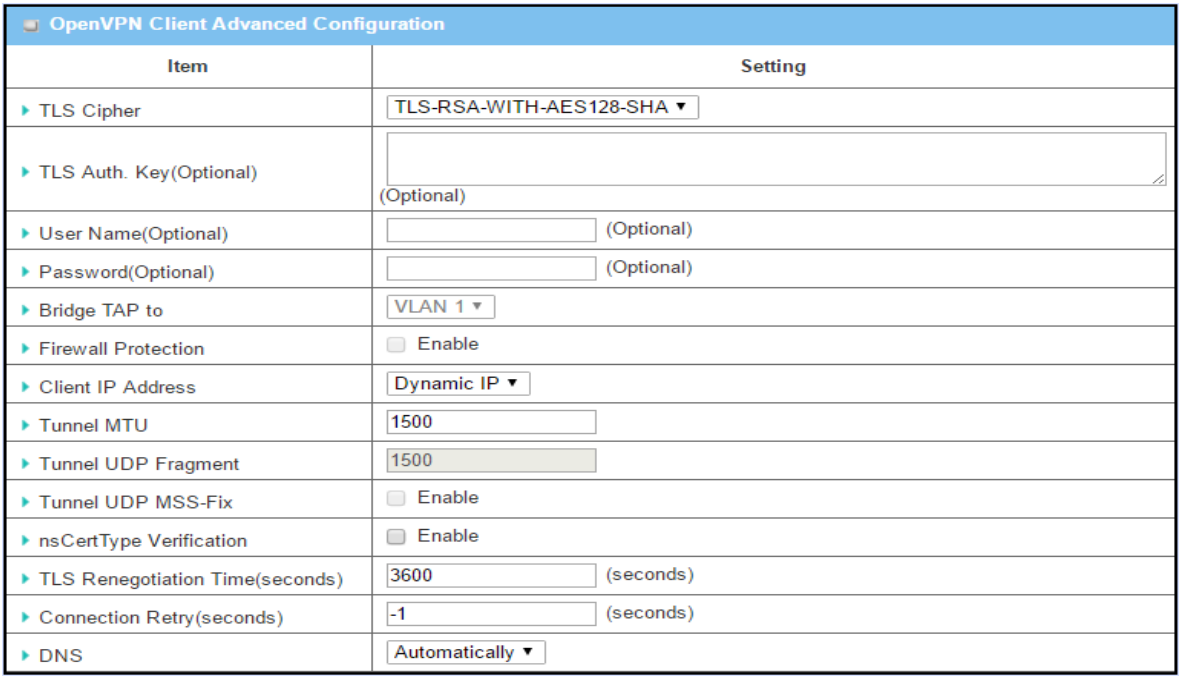
The OpenVPN Client Configuration window let you specify the required parameters for an Open VPN client, such as "OpenVPN Client Name", "Interface", "Protocol", "Tunnel Scenario", "Remote IP/FQDN", "Remote Subnet", "Authorisation Mode", "Encryption Cipher", "Hash Algorithm" and tunnel activation.



OpenVPN Client Configuration		
Item	**Value setting**	**Description**
OpenVPN Client Name	Mandatory Setting	The **OpenVPN Client Name** will be used to identify the client in the tunnel list. ***Value Range*:** 1 ~ 32 characters.
Interface	Mandatory Setting By default, **WAN-1** is selected.	Define the physical interface to be used for this OpenVPN Client tunnel.
Protocol	Mandatory Setting By default, **TCP** is selected.	Define the **Protocol** for the OpenVPN Client. • Select **TCP** - The OpenVPN will use TCP protocol, and **Port** will be set as 443 automatically. • Select **UDP** - The OpenVPN will use UDP protocol, and **Port** will be set as 1194 automatically.
Port	Mandatory Setting By default, **443** is set.	Specify the **Port** for the OpenVPN Client to use. ***Value Range*:** 1 ~ 65535.
Tunnel Scenario	Mandatory Setting By default, **TUN** is selected.	Specify the type of **Tunnel Scenario** for the OpenVPN Client to use. It can be **TUN** for TUN tunnel scenario or **TAP** for TAP tunnel scenario.
Remote IP/FQDN	Mandatory Setting	Specify the **Remote IP/FQDN** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
Remote Subnet	Mandatory Setting	Specify **Remote Subnet** of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the remote subnet address and remote subnet mask.
Redirect Internet Traffic	An Optional setting. The box is unchecked by default.	Check the **Enable** box to activate the **Redirect Internet Traffic** function.
NAT	An Optional setting. unchecked by default.	Check the **Enable** box to activate the **NAT** function.
Authorization Mode	Mandatory Setting By default, **TLS** is selected.	Specify the authorization mode for the OpenVPN Server. • **TLS** ->The OpenVPN will use TLS authorization mode, and the following items **CA Cert.**, **Client Cert.** and **Client Key** will be displayed. **CA Cert.** could be selected in Trusted CA Certificate List. Refer to **Object Definition**>**Certificate**>**Trusted Certificate**. **Client Cert.** could be selected in Local Certificate List. Refer to **Object Definition**>**Certificate**>**My Certificate**. **Client Key** could be selected in Trusted Client key List. Refer to **Object Definition**>**Certificate**>**Trusted Certificate**. • **Static Key** ->The OpenVPN will use static key authorization mode, and the following items **Local Endpoint IP Address**, **Remote Endpoint IP Address** and **Static Key** will be displayed.
Local Endpoint IP Address	Mandatory Setting	Specify the **Local Endpoint IP Address**. **Note**: Local Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Remote Endpoint IP Address	Mandatory Setting	Specify the **Remote Endpoint IP Address**. **Note**: Remote Endpoint IP Address will be available only when Static Key is chosen in Authorization Mode.
Static Key	Mandatory Setting	Specify the **Static Key**. **Note**: Static Key will be available only when Static Key is chosen in Authorization Mode.
Encryption Cipher	By default, **Blowfish** is selected.	Specify the **Encryption Cipher.** It can be **Blowfish/AES-256/AES-192/AES-128/None.**
Hash Algorithm	By default, **SHA-1** is selected.	Specify the **Hash Algorithm.** It can be**SHA-1/MD5/MD4/SHA2-256/SHA2-512/None/Disable.**

LZO Compression	By default, **Adaptive** is selected.	Specify the **LZO Compression** scheme. It can be **Adaptive/YES/NO/Default.**
Persist Key	An Optional setting. The box is checked by default.	Check the **Enable** box to activate the **Persist Key** function.
Persist Tun	An Optional setting. The box is checked by default.	Check the **Enable** box to activate the **Persist Tun** function.
Advanced Configuration	N/A	Click the **Edit** button to specify the **Advanced Configuration** setting for the OpenVPN server. If the button is clicked, **Advanced Configuration** will be displayed below.
Tunnel	The box is unchecked by default	Check the **Enable** box to activate this OpenVPN tunnel.
Save	N/A	Click **Save** to save the settings.
Undo	N/A	Click **Undo** to cancel the changes.
Back	N/A	Click **Back** to return to last page.

When the Advanced Configuration is selected, the 'OpenVPN Client Advanced Configuration' screen appears.



OpenVPN Advanced Client Configuration		
Item	**Value setting**	**Description**
TLS Cipher	Mandatory Setting **TLS-RSA-WITH-AES128-SHA** is selected by default	Specify the **TLS Cipher** from the dropdown list. It can be **TLS-RSA-WITH-AES128-SHA / TLS-DHE-DSS-AES256-SHA / TLS-DHE-DSS-AES128-SHA / TLS-RSA-WITH-AES256-SHA / TLS-RSA-WITH-RC4-MD5 / None.** Note: TLS Cipher will be available only when TLS is chosen in Authorisation Mode.
TLS Auth. Key	An Optional setting. String format: any text	Specify the **TLS Auth. Key** for connecting to an OpenVPN server, if the server required it. **Note:** TLS Auth. Key will be available only when TLS is chosen in Authorization Mode.
User Name	An Optional	Enter the **User account** for connecting to an OpenVPN server, if the

	setting.	server required it. **Note**: User Name will be available only when TLS is chosen in Authorization Mode.
Password	An Optional setting.	Enter the **Password** for connecting to an OpenVPN server, if the server required it. **Note**: User Name will be available only when TLS is chosen in Authorisation Mode.
Bridge TAP to	By default, **VLAN 1** is selected	Specify the setting of "**Bridge TAP to**" to bridge the TAP interface to a certain local network interface or VLAN. **Note**: Bridge TAP to will be available only when TAP is chosen in Tunnel Scenario and NAT is unchecked.
Firewall Protection	The box is unchecked by default.	Check the box to activate the **Firewall Protection** function. **Note:** Firewall Protection will be available only when NAT is enabled.
Client IP Address	By default, **Dynamic IP** is selected	Specify the virtual IP Address for the OpenVPN Client. It can be **Dynamic IP/Static IP.**
Tunnel MTU	Mandatory Setting The value is 1500 by default	Specify the value of **Tunnel MTU.** ***Value Range*:** 0 ~ 1500.
Tunnel UDP Fragment	The value is 1500 by default	Specify the value of **Tunnel UDP Fragment.** ***Value Range*:** 0 ~ 1500. **Note**: Tunnel UDP Fragment will be available only when UDP is chosen in Protocol.
Tunnel UDP MSS-Fix	The box is unchecked by default.	Check the **Enable** box to activate the **Tunnel UDP MSS-Fix** function. **Note:** Tunnel UDP MSS-Fix will be available only when UDP is chosen in Protocol.
nsCerType Verification	The box is unchecked by default.	Check the **Enable** box to activate the **nsCerType Verification** function. **Note**: nsCerType Verification will be available only when TLS is chosen in Authorization Mode.
TLS Renegotiation Time (seconds)	The value is 3600 by default	Specify the time interval of **TLS Renegotiation Time.** ***Value Range*:** -1 ~ 86400.
Connection Retry(seconds)	The value is -1 by default	Specify the time interval of **Connection Retry.** The default -1 means that it is no need to execute connection retry. ***Value Range*:** -1 ~ 86400, and -1 means no retry is required.
DNS	By default, **Automatically** is selected	Specify the setting of **DNS.** It can be **Automatically/Manually.**

7.1.3. L2TP Overview

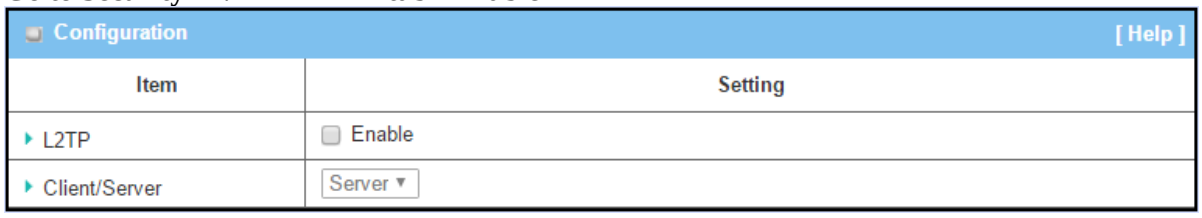
Layer 2 Tunnelling Protocol (L2TP) is a tunnelling protocol used to support virtual private networks (VPNs) or as part of the services delivered by ISPs.

- The L2TP Client's "Default Gateway / Remote Subnet" setting determines how the Internet traffic from L2TP client site is handled. Default sends all traffic down the L2TP tunnel, while 'Remote Subnet' means subnet to subnet traffic goes down the L2TP tunnel, while Internet Traffic goes out via the 6402 WAN Port.
- The L2TP over IPSec is usually used for BYOD devices to establish a secure VPN tunnel between mobile employees and the company office.
- L2TP protocol is used for establishing an L2TP VPN tunnel.
- L2TP Tunnelling is a Client and Server based tunnelling technology. The 6402 can operate as both a L2TP Server and Client at the same time
- The L2TP Server must have a Static IP or a FQDN and maintain a Client list (account / password); The Client may be a mobile user or mobile site and request the L2TP tunnel connection with its account / password.
- L2TP does not provide encryption, but replies on an encryption protocol that it passes within the tunnel to provide security
- Deploy a 6402 at the local office and establish a virtual private network with the remote gateway of another office by using L2TP tunnelling. All client hosts behind the local 6402 can communication with other users on the remote subnet.
- A 6402 in HQ supporting the L2TP VPN allows users to dial into the HQ 6402 gateway and access the HQ resources by establishing an L2TP VPN tunnel.

7.1.3.1 Configuring L2TP

The L2TP setting allows user to create and configure L2TP tunnels. Before you proceed ensure that the VPN is enabled and saved. To enable VPN, go to **Security> VPN > Configuration** tab.

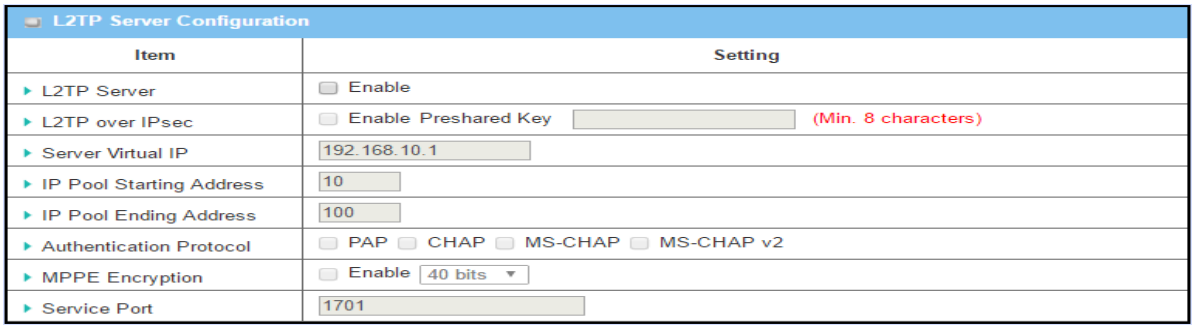
Go to Security > VPN > L2TP tab >Enable L2TP



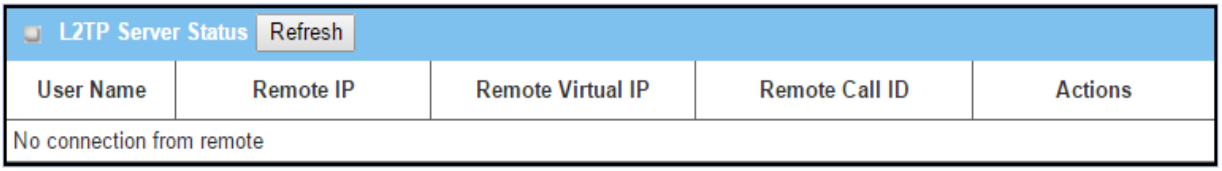
Enable L2TP Window		
Item	**Value setting**	**Description**
L2TP	Unchecked by default	Click the Enable box to activate L2TP function.
Client/Server	A Mandatory setting	Specify the role of L2TP. Select **Server** or **Client** role your 6402 will take. Below are the configuration windows for L2TP Server and for Client.
Save	N/A	Click Save button to save the settings

7.1.3.2 Configuring L2TP Server Mode

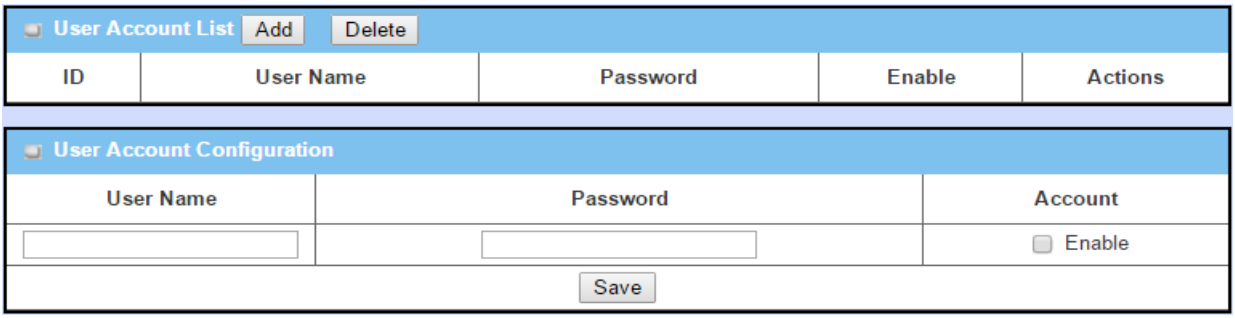
When you select L2TP Server in the Client/Server menu, the L2TP server Configuration will appear.



L2TP Server Configuration		
Item	**Value setting**	**Description**
L2TP Server	The box is unchecked by default	When click the **Enable** box It will active L2TP server
L2TP over IPSec	The box is unchecked by default	When click the **Enable** box. It will enable L2TP over IPSec and need to fill in the Pre-shared Key.
Server Virtual IP	Mandatory Setting	Specify the L2TP server Virtual IP It will set as this L2TP server local virtual IP
IP Pool Starting Address	Mandatory Setting	Specify the L2TP server starting IP of virtual IP pool It will set as the starting IP which assign to L2TP client
IP Pool Ending Address	Mandatory Setting	Specify the L2TP server ending IP of virtual IP pool It will set as the ending IP which assign to L2TP client
Authentication Protocol	Mandatory Setting	Specify the **Authentication Protocol** which this L2TP server allows. Selected PAP/CHAP/MS-CHAP/MS-CHAPv2 ->It will set as the authentication protocol which is checked.
MPPE Encryption	Mandatory Setting	Specify the **MPPE Protocol** which this L2TP server allowed. When Click the **Enable** box ->It will enable MPPE Selected 40 bits/56 bits/128 bits ->It will set as the MPPE encryption which is chose. **Note**: If Enable box is be clock, Authentication Protocol PAP/CHAP will be available.
Service Port	Mandatory Setting	Specify the **Service Port** which L2TP server use.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.

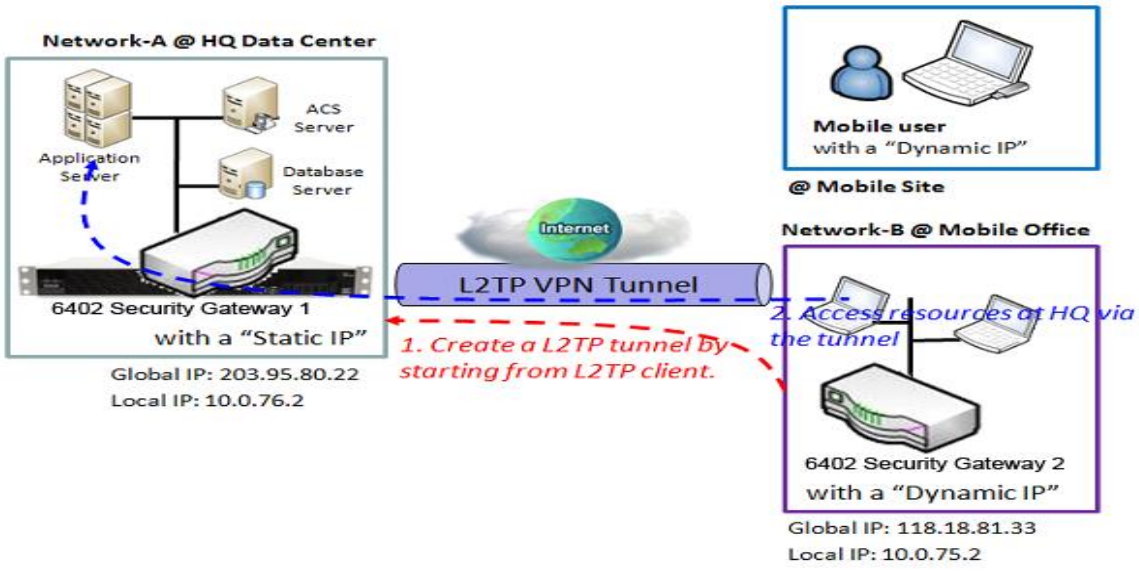


L2TP Server Status		
Item	**Value setting**	**Description**
L2TP Server Status	N/A	Show the L2TP client information which connect to this L2TP server. Click the **Refresh** button to renew the L2TP client information.



User Account List		
Item	**Value setting**	**Description**
User Account List	N/A	Specify the **User Account** which allow client to authenticate. Click **Add** button to add user account. Click **Delete** button to delete user account. Click **Enable** button to enable user account. Specify **Username** ->Fill in the username. Specify **Password** ->Fill in the password Click **save** button to save user account.

7.1.3.3 L2TPServer Mode Configuration Example.



In the diagram above the 6402 at headquarters is the L2TP Server. The L2TP Tunnel is established by the 6402 Gateway 2 at Network B. All devices on network B and the mobile users can access the resources on subnet A. The packets that are going to the Internet, go out directly from the 6402 WAN Interface, only the packets destined for Network A, go via the L2TP Tunnel.

L2TP Server Mode Setup Example - Network-A at HQ

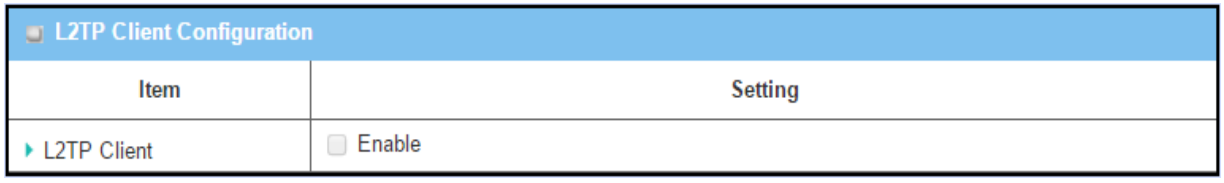
Network-A - is in the headquarters, and has a subnet of 10.0.76.0/24, has an IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface. It serves as an L2TP server.

The L2TP Server provides two user accounts, User 1 and User 2 for clients dialling in.

Configuration Path	[L2TP]-[Configuration]	
L2TP	■ Enable	
Client/Server	Server	
Configuration Path	**[L2TP]-[L2TP Server Configuration]**	
L2TP Server	■ Enable	
L2TP over IPSec	■ Enable Pre-share Key 12345678	
Server Virtual IP	192.168.101.253	
IP Pool Starting Address	10 (that means 192.168.101.10)	
IP Pool Ending Address	50 (that means 192.168.101.50)	
Authentication Protocol	MS-CHAP	
MPPE Encryption	■ Enable128 bits	
Service Port	1701	
Configuration Path	**[L2TP]-[User Account Configuration]**	
ID	1	2
User Name	User-1	User-2
Password	1234	4321
Account	■ Enable	■ Enable

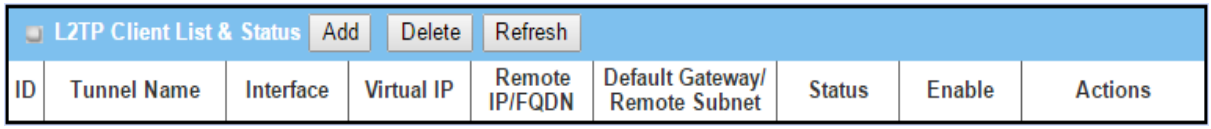
7.1.3.4 Configuring L2TP Client Mode

When you select Client in the Client/Server section, a L2TP Client Configuration will appear.

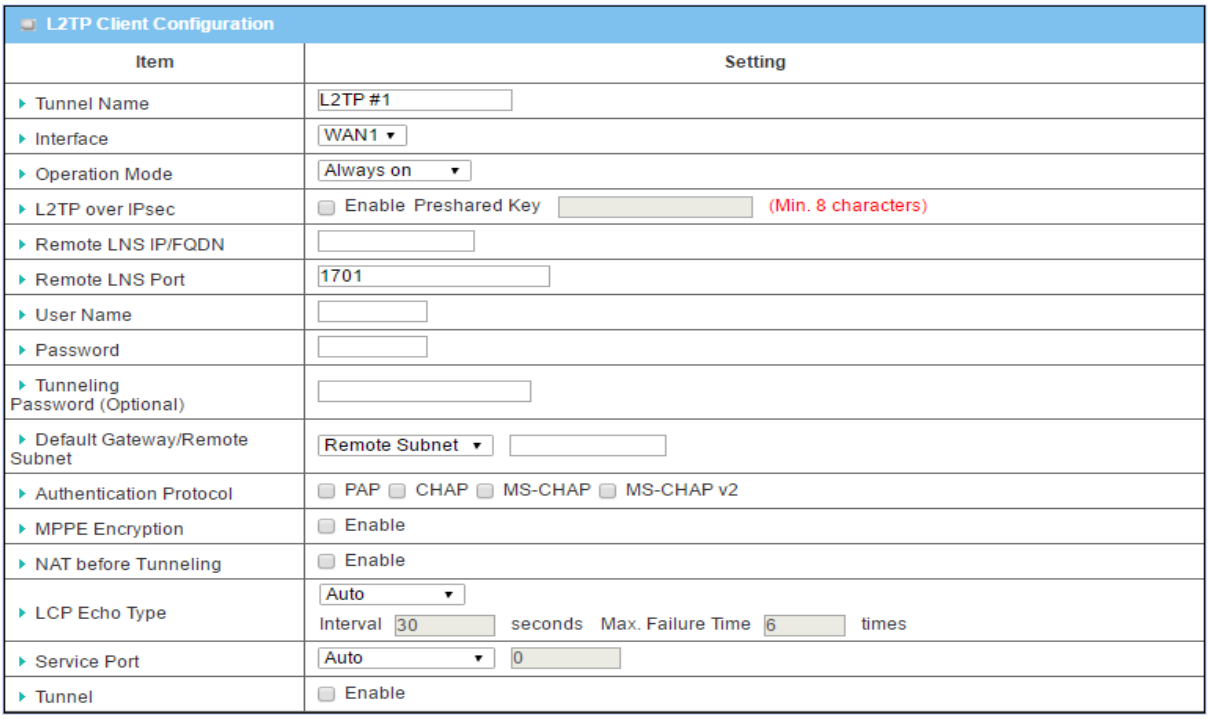


L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
L2TP Client	The box is unchecked by default	When click the **Enable** box It will activate L2TP Client.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.

Create/Edit L2TP Client



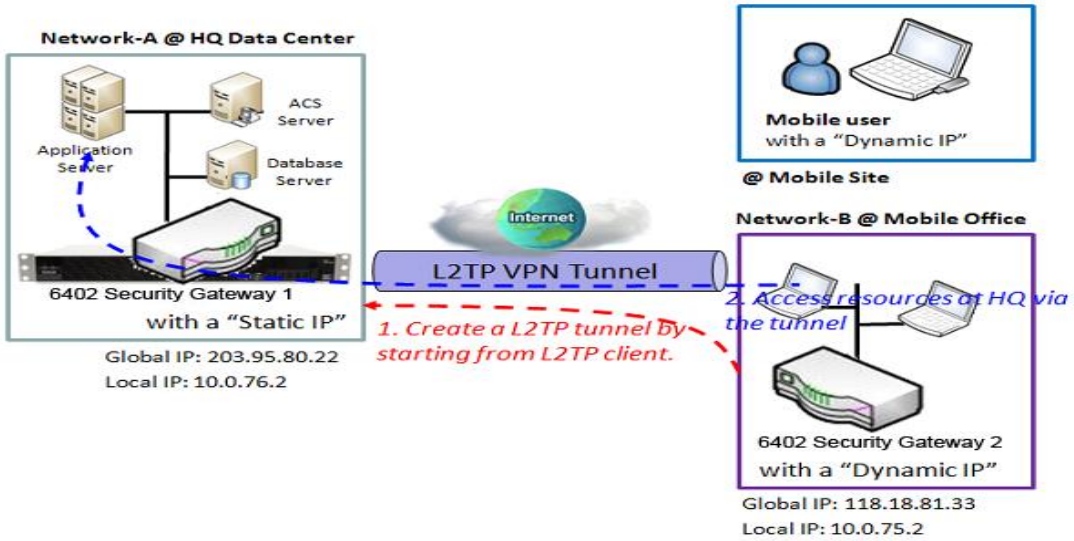
When Add/Edit button is applied a series of configuration screen will appear.



L2TP Client Configuration		
Item Setting	**Value setting**	**Description**
Tunnel Name	Mandatory Setting	Provide a name to identify it in the tunnel list
Interface	Mandatory Setting	Define the selected interface to be the used for this L2TP tunnel Select **WAN-1** for this IPSec tunnel using. (WAN-1 is available only when WAN-1 interface is enabled) The same applies to other WAN interfaces (i.e. **WAN-2).**
Operation Mode	Mandatory Setting Always on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the L2TP client is a failover tunnel function or an always on tunnel. Note: If this L2TP is a failover tunnel, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance** Define whether the L2TP tunnel connection will take part in load balancing for the 6402. You will not need to select which WAN interface as the system will automatically utilise the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On the 6402 web-based utility, go to Basic Network > WAN& Uplink> Load Balance tab.
L2TP over IPSec	Unchecked by default	Click the **Enable** box. This will enable L2TP over IPSec you then need to configure the Pre-shared Key.
Remote LNS IP/FQDN	Mandatory Setting	Specify the **Remote LNS IP/FQDN** for this L2TP tunnel. Fill in the IP address or FQDN.
Remote LNS Port	Mandatory Setting	Specify the **Remote LNS Port** for this L2TP tunnel. Fill in the value for LNS port.
Username	Mandatory Setting	Specify the **Username** for this L2TP tunnel to authenticate when connect to server. Fill in the string as username.
Password	Mandatory Setting	Specify the **Password** for this L2TP tunnel to authenticate when connect to server.
Tunnelling Password (Optional)	Unchecked by default	Specify the **Tunnel Password** for this L2TP tunnel to authenticate.
Default Gateway	Mandatory Setting	Specify Default Gateway/Remote Subnet for this L2TP tunnel.

/ Remote Subnet		Selected Default Gateway ->The IP address box will not be available. Selected the **Remote Subnet** ->Filled the remote subnet address/remote subnet mask.
Authentication Protocol	Mandatory Setting	Specify **Authentication Protocol** for this L2TP tunnel will can be used. Click the PAP/CHAP/MS-CHAP/MS-CHAP v2 ->The protocol will be enable which box is click.
MPPE Encryption	Unchecked by default	Select the **Enable** box to It will enable MPPE for this L2TP tunnel. **Note**_1: If Enable box is be selected the, Authentication Protocol PAP/CHAP will be not available.
NAT before Tunnelling	Unchecked by default	Select the **Enable** box ->It will enable NAT for this L2TP tunnel.
LCP Echo Type	Mandatory Setting	Specify the LCP Echo Type for this L2TP tunnel. Select **Auto** ->Auto setting the Interval and Max. Failure Time. Selected User-defined ->Fill in the Interval and Max. Failure Time for LCP. Selected **Disable** ->Disable LCP Echo and it will be not available.
Service Port	Mandatory Setting	Specify the **Service Port** for this L2TP tunnel to use.
Tunnel	Unchecked by default	Select Enable It will enable this L2TP tunnel
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to recovery the configuration.

7.1.3.5 L2TPClient Mode Configuration Example



L2TP VPN Client – Operation

In the diagram above the 6402 Gateway 2 or mobile devices operate as L2TP VPN Clients. Once the L2TP Tunnel has been established all the clients at Network B can access Networks A's subnet via the L2TP Tunnel. Any packets destined to go to the Internet will go out of the 6402 via its WAN Interface, unless the 'Default Gateway' has been set in which case all packets will go via L2TP.

The above diagram illustrates the 6402 Gateway 2 or the mobile device acting as a L2TP VPN client.

- The L2TP tunnel is established by the L2TP client making the tunnel connection request.
- The 6402 Gateway 1 in Network-A at headquarters serves as the L2TP VPN server responding to the request. Once the tunnel has been established, all client hosts behind 6402 Gateway 2 or the mobile device can access the resources on the subnet of Network-A via the L2TP tunnel.

- Under normal circumstance the hosts at site B access the internet via the WAN Interface of the 6402 at site B. Only the packets whose destination is the subnet on Network-A will be transferred via the L2TP tunnel.
- If the 6402 Client at network B is set to 'Default Gateway' then all packets from the 6402 will go down the L2TP Tunnel, including all the packets destined for the Internet, giving the 6402 Server at Network A, control of the Internet.

L2TP Client Mode Configuration Example - Network-B at Mobile Office

The following table lists the configuration for the example diagram of L2TP VPN clients in Network-B. Use default value for those parameters that are not shown in these tables.

Configuration Path	[L2TP]-[Configuration]
L2TP	■ Enable
Client/Server	Client
Configuration Path	**[L2TP]-[L2TP Client Configuration]**
L2TP Client	■ Enable

Configuration Path	[L2TP]-[Configuration for A L2TP Client]
L2TP Client Name	L2TP #1
Interface	WAN 1
L2TP over IPSec	■ Enable Pre-share Key: 12345678
Remote LNS IP/FQDN	203.95.80.22
Remote LNS Port	1701
User Name	User-1
Password	1234
Default Gateway/Remote Subnet	Default Gateway
Authentication Protocol	MS-CHAP
MPPE Encryption	■ Enable
Service Port	Auto
Tunnel	■ Enable

L2TP Operation Procedure

Network-A- is in the headquarters, and has a subnet of 10.0.76.0/24, and an IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface. It serves as a L2TP server.

Network-B- is in the mobile office and its subnet is 10.0.75.0/24 and has an IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a L2TP client.

There are two options, "Default Gateway" and "Remote Subnet".

Remote Subnet

When you choose "Remote Subnet", you need specify one more setting. Remote subnet refers to the 6402 Subnet of theL2TP VPN server.

At the L2TP client peer, the packets whose destination is Network A's subnet, will be transferred via the L2TP VPN tunnel. Other packets will be transferred based on the current routing policy of the 6402 gateway of the L2TP client peer.

Default Gateway

If you select the "Default Gateway" option for the 6402 L2TP client peer, (on Network B) will send all packets via the L2TP VPN tunnel. That means the 6402 L2TP VPN server controls the flow of all packets from the L2TP client peer.

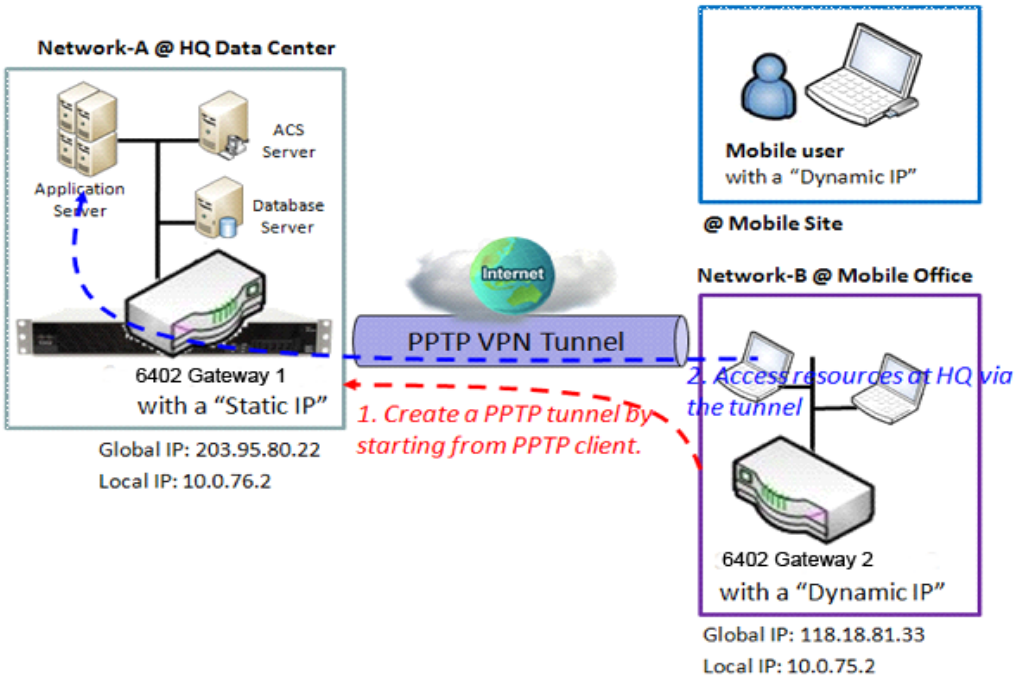
7.1.4 PPTP Overview

The Point-to-Point Tunnelling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel to encapsulate PPP packets.

- PPTP Tunnelling is a Client and Server based tunnelling technology.
- The PPTP Server must have a Static IP or a FQDN and maintain a Client list (account / password). The Client may be a mobile user or mobile site and requesting the PPTP tunnel connection with its account / password.
- PPTP protocol is used to establish a PPTP VPN tunnel.
- The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunnelled to implement security.
- The most common PPTP implementation shipping with the Microsoft Windows implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.
- The 6402 can act as either a "PPTP Server" or "PPTP Client" for a PPTP VPN tunnel, or both at the same time for different tunnels.

Users can dial into the 6402 at Network B and access the HQ resources by establishing a PPTP VPN tunnel. It is a virtual private network between your device and the HQ 6402 gateway.

7.1.4.1 PPTP VPN Server Example



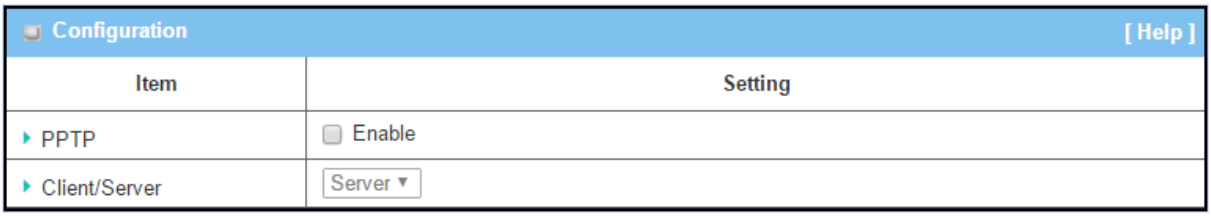
PPTP VPN Example

- 6402 Gateway 1 at headquarters acts as the PPTP VPN server. The PPTP tunnel is established by the 6402 Gateway at Network B, or from the mobile device.
- All client hosts behind the 6402 Gateway 2 can access the resources on the subnet of Network-A via the PPTP tunnel. Usually, the hosts at the PPTP client access the Internet directly via the WAN interface of the 6402 Gateway 2.Only the packets whose destination is the subnet of Network-A will be transferred via the PPTP tunnel.

7.1.4.2 Configuring PPTP

The PPTP setting allows users to create and configure PPTP tunnels. Before you proceed, ensure that the VPN is enabled and saved. To enable VPN, go to **Security> VPN > Configuration** tab.
Go to Security> VPN > PPTP tab.

Enable PPTP

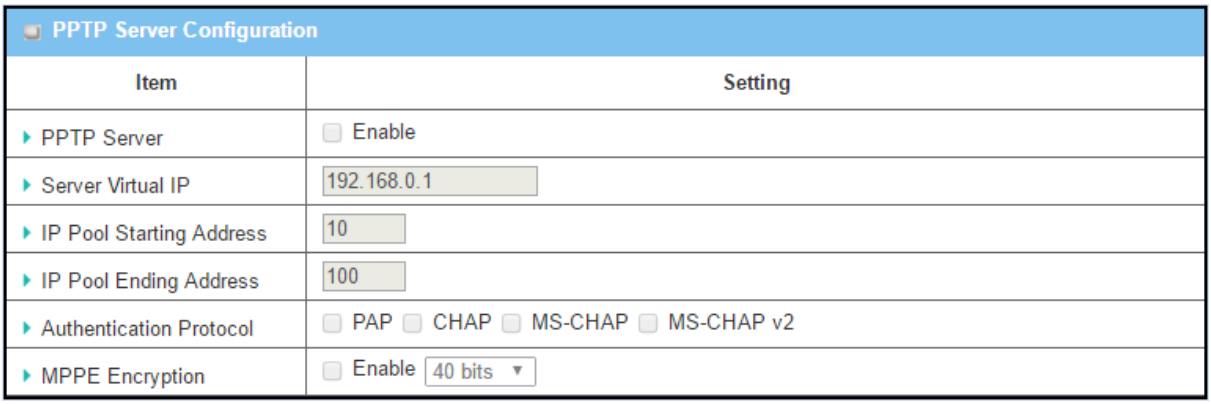


-

Enable PPTP Window		
Item	**Value setting**	**Description**
PPTP	Unchecked by default	Click the **Enable** box to activate PPTP function.
Client/Server	A Mandatory setting	Specify the role of PPTP. Select **Server** or **Client** role your gateway will take. Below are the configuration windows for PPTP Server and for Client.
Save	N/A	Click Save button to save the settings

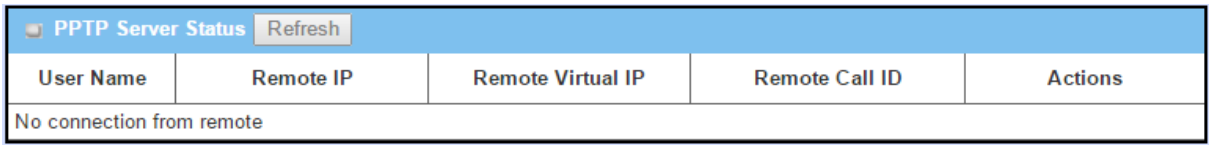
7.1.4.3 Configuring aPPTP Server

The 6402 supports up to a maximum of 10 PPTP user accounts.
When Server in the Client/Server field is selected, the PPTP server configuration window will appear.

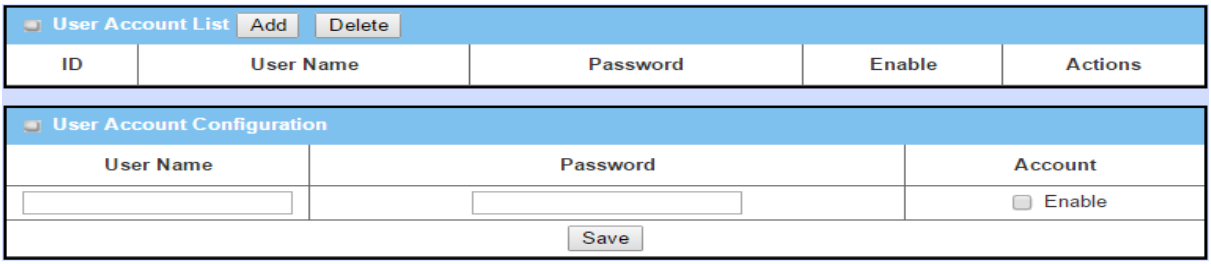


PPTP Server Configuration Window		
Item	**Value setting**	**Description**
PPTP Server	Unchecked by default	Check the **Enable** box to enable PPTP server role of the gateway.
Server Virtual IP	1. Default Setting 2. Default is 192.168.0.1	Specify the PPTP server Virtual IP address. The virtual IP address will serve as the virtual DHCP server for the PPTP clients. Clients will be assigned a virtual IP address from it after the PPTP tunnel has been established.
IP Pool Starting Address	1. Default Setting 2. Default is 10	This is the PPTP server's Virtual IP DHCP server. User can specify the first IP address for the subnet from which the PPTP client's IP address will be assigned.
IP Pool Ending Address	1. Default Setting 2. Default is 100	This is the PPTP server's Virtual IP DHCP server. User can specify the last IP address for the subnet from which the PPTP client's IP address will be assigned.
Authentication Protocol	1. Default Setting 2. Unchecked by default	Select single or multiple Authentication Protocols for the PPTP server with which to authenticate PPTP clients. Available authentication protocols are PAP/CHAP/MS-CHAP/MS-CHAPv2.
MPPE	Default Setting	Specify whether to support MPPE Protocol. Click the Enable box

Encryption		to enable MPPE and from dropdown box to select 40 bits/56 bits/128 bits. Note: when MPPE Encryption is enabled, the Authentication Protocol PAP/CHAP options will not be available.
Save	N/A	Click Save button to save the settings.
Undo	N/A	Click Undo button to cancel the settings.



PPTP Server Status Window		
Item	**Value setting**	**Description**
PPTP Server Status	N/A	It displays the User Name, Remote IP, Remote Virtual IP, and Remote Call ID of the connected PPTP clients.



User Account List Window		
Item	**Value setting**	**Description**
User Account List	Max of 10 user accounts	This is the PPTP authentication user account entry. You can create and add accounts for remote clients to establish PPTP VPN connection to the gateway device. Click **Add** button to add user account. Enter User name and password. Then check the enable box to enable the user. Click **Save** button to save new user account. The selected user account can permanently be deleted by clicking the **Delete** button.

7.1.4.4 PPTP Server Configuration Example

Network-A - at HQ, the following 3 tables list the configuration for the example above in the diagram for the 6402 server at Network-A.

Use default value for those parameters that are not shown in these tables.

Configuration Path	[PPTP]-[Configuration]	
PPTP	■ *Enable*	
Client/Server	Server	
Configuration Path	[PPTP]-[PPTP Server Configuration]	
PPTP Server	■ *Enable*	
Server Virtual IP	*192.168.101.253*	
IP Pool Starting Address	*10*(that means 192.168.101.10)	
IP Pool Ending Address	*50*(that means 192.168.101.50)	
Authentication Protocol	*MS-CHAP*	
MPPE Encryption	■ *Enable128 bits*	
Configuration Path	[PPTP]-[User Account Configuration]	
ID	1	2
User Name	*User-1*	*User-2*
Password	*1234*	*4321*
Account	■ *Enable*	■ *Enable*

PPTP Server Configuration Method of Operation

Network-A at headquarters, has a subnet of 10.0.76.0/24 and an IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface. It serves as a PPTP server.

Network-B is in the mobile office and has a subnet of 10.0.75.0/24, and an IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a PPTP client.

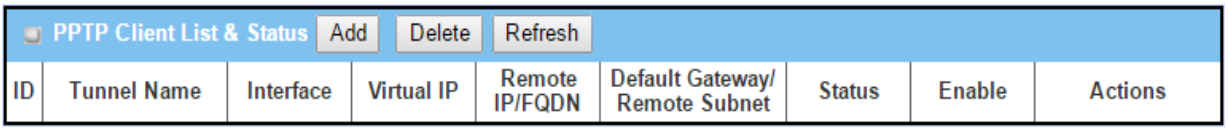
The PPTP server provides two user accounts, User-1 and User-2, for PPTP clients dialling in.
The client establishes the PPTP Sessions
Both subnets of 10.0.75.0/24 and 10.0.76.0/24 communicate securely with each other.
The client hosts in the subnet of Network-B at the mobile office can access the server or database resources on the subnet of Network-A at HQ over the secure link.

7.1.4.5 Configuring a PPTP VPN Client

When select Client in Client/Server, a series PPTP Client Configuration will appear.

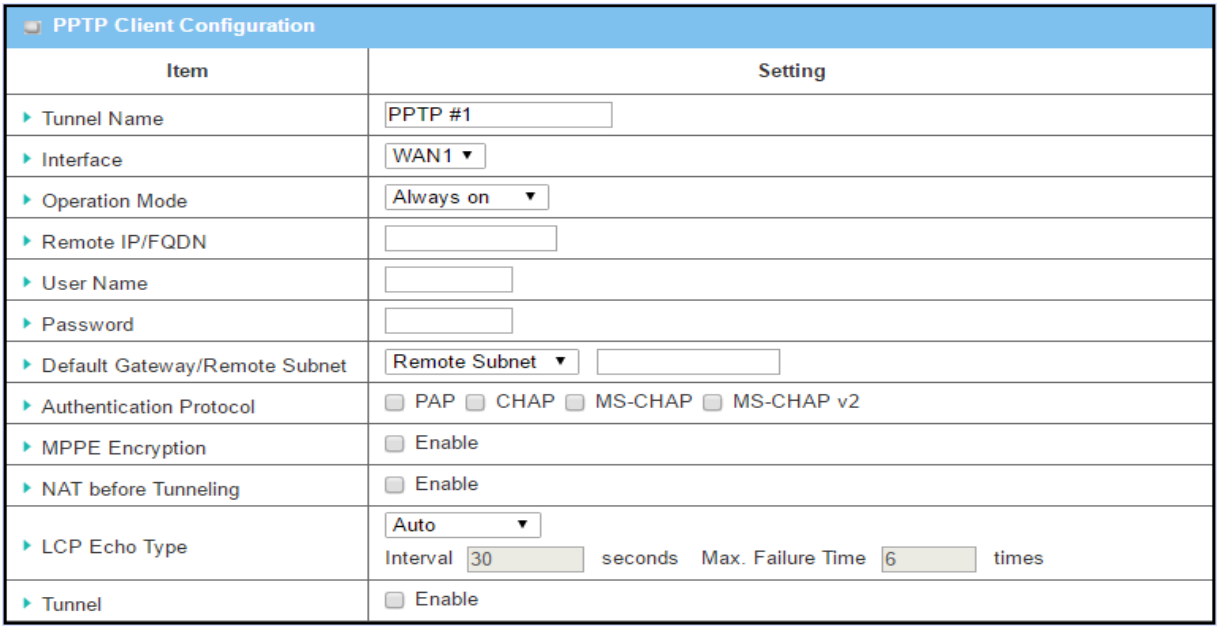
PPTP Client Configuration		
Item	**Value setting**	**Description**
PPTP Client	Unchecked by default	Check the **Enable** box to enable PPTP client role of the 6402
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.

7.1.4.6 Create/Edit PPTP Client



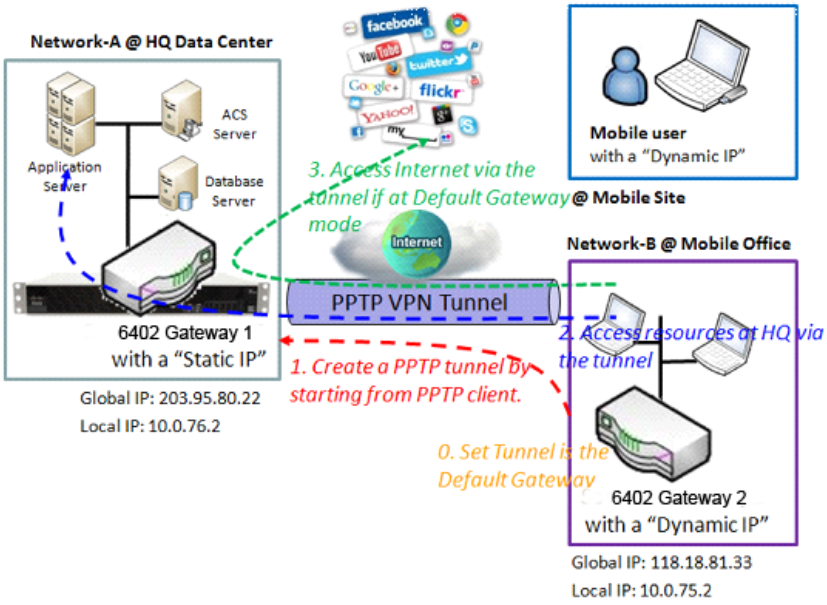
The 6402 supports up to a maximum of 32 simultaneous PPTP tunnels.

When the Add/Edit button is applied a series PPTP Client Configuration options will appear.



PPTP Client Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	Mandatory	Enter a tunnel name. Enter a name that is easy for you to identify.
Interface	Mandatory WAN1 is selected by default	Select WAN interface on which PPTP tunnelling is to be established.
Operation Mode	Mandatory Always on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the PPTP client is a failover tunnel function or an always on tunnel. Note: If this PPTP is a failover tunnelling, you will need to select a primary IPSec tunnel from which to failover to. **Load Balance** Define whether the PPTP tunnel connection will take part in load balance function of the gateway. You will not need to select which WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN& Uplink> Load Balance tab.
Remote IP/FQDN	Mandatory Format can be an ipv4 address or FQDN	Enter the public IP address or the FQDN of the PPTP server.
Username	Mandatory	Enter the **Username** for this PPTP tunnel to be authenticated when connect to PPTP server.
Password	Mandatory	Enter the **Password** for this PPTP tunnel to be authenticated when connect to PPTP server.
Default Gateway / Remote Subnet	Mandatory	Specify a gateway for this PPTP tunnel to reach PPTP server. If the gateway uses its gateway IP address to connect to the internet to connect to the PPTP server then select Default Gateway, otherwise, specified a subnet and its netmask –the remote subnet, if the default gateway is not used to connect to the PPTP server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
Authentication Protocol	Mandatory Unchecked by default	Specify one ore multiple **Authentication Protocol** for this PPTP tunnel. Available authentication methods are **PAP/CHAP/MS-CHAP/MS-CHAPv2**
MPPE Encryption	Unchecked by default An optional setting	Specify whether PPTP server supports **MPPE Protocol**. Click the **Enable** box to enable MPPE. **Note**: when MPPE Encryption is enabled, the Authentication Protocol PAP/CHAP options will not be available.
NAT before Tunnelling	Unchecked by default An optional setting	Check the **Enable** box to enable NAT function for this PPTP tunnel.
LCP Echo Type	Auto is set by default	Specify the LCP Echo Type for this PPTP tunnel. Auto, User-defined, Disable. **Auto** the system sets the Interval and Max. Failure Time. **User-defined** enter the Interval and Max. Failure Time. **Disable** – disables the LCP Echo.
Tunnel	Unchecked by default	Check the **Enable** box to enable this PPTP tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

7.1.4.7 PPTP VPN Client Configuration Example



PPTP VPN Client Operation

In the diagram above the 6402 Gateway 2 or the mobile device works as PPTP VPN client and The 6401 at Gateway 2 initiates the connection to the 6402 at Gateway 1 which acts as a PPTP Server. Once the tunnel has been established, all client hosts behind the 6402 Gateway 2 or the mobile device can access the resources on Network-A's subnet via the PPTP tunnel.

Normally these hosts access the Internet directly via the 6402Gateway 2's WAN interface. Only the packets whose destination is the subnet in Network-A will be transferred via the PPTP tunnel. However, if the 6402 PPTP client is configured to be a 'Default Gateway' all packets including packets destined for the Internet are sent to the 6402 Gateway 1 via the PPTP Tunnel;

Network A -is in the headquarters and has a subnet of 10.0.76.0 / 24 and an IP Address of 10.0.76.2 for its LAN Interface and 203.95.80.22 for its WAN Interface, and it works as a PPTP Server.

Network-B - is in the mobile office with a subnet of 10.0.75.0/24 and an IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a PPTP client.

The 6402 PPTP client at Network B uses a "User-1" user account to dial in to the PPTP server at HQ to establish a PPTP VPN tunnel, allowing subnets of 10.0.75.0/24 and 10.0.76.0/24 to communicate securely.

If the "Default Gateway/Remote Subnet" parameter in the 6402 Gateway 2 is configured to "Default Gateway", traffic destined for the Internet passes through the 6402 Client and passes down the PPTP VPN Tunnel to 6402 the Gateway 1, allowing that 6402 to control the site to site and site B to Internet traffic.

There are two options to, "Default Gateway" and "Remote Subnet".

When you choose "Remote Subnet", you need specify one more setting: The remote subnet for the PPTP VPN server. This means any traffic at Client Site B destined to go to subnet A, will go down the PPTP Tunnel to reach the subnet on site A. All other traffic will be routed according to the 6402's routing policy

However, if you select the "Default Gateway" option for the PPTP client peer, all packets will be transferred via the PPTP VPN tunnel. This means the remote PPTP VPN server gateway controls the packets flowing from the PPTP client peer, via the PPTP Tunnel.

Setup Example - For Network-B at Mobile Office

The following table lists the configuration for the above example diagram of PPTP VPN client in Network-B.
Use default value for those parameters that are not mentioned in these tables.

Configuration Path	[PPTP]-[Configuration]
PPTP	■ Enable
Client/Server	Client
Configuration Path	**[PPTP]-[PPTP Client Configuration]**
PPTP Client	■ *Enable*
Configuration Path	**[PPTP]-[Configuration for A PPTP Client]**
PPTP Client Name	PPTP #1
Interface	WAN 1
Remote IP/FQDN	203.95.80.22
User Name	User-1
Password	1234
Default Gateway/Remote Subnet	Default Gateway
Authentication Protocol	MS-CHAP
MPPE Encryption	■ Enable
Tunnel	■ Enable

Scenario Operation Procedure

Network A -is in the headquarters and has a subnet of 10.0.76.0 / 24 and an IP Address of 10.0.76.2 for its LAN Interface and 203.95.80.22 for its WAN Interface, and it works as a PPTP Server.

Network-B - is in the mobile office with a subnet of 10.0.75.0/24 and an IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a PPTP client.
The 6402 PPTP client at Network B uses a "User-1" user account to dial in to the PPTP server at HQ to establish a PPTP VPN tunnel, allowing subnets of 10.0.75.0/24 and 10.0.76.0/24 to communicate securely.

If the "Default Gateway/Remote Subnet" parameter in the 6402 Gateway 2 is configured to "Default Gateway", traffic destined for the Internet passes through the 6402 Client and passes down the PPTP VPN Tunnel to 6402 the Gateway 1, allowing that 6402 to control the site to site and site B to Internet traffic.

There are two options to, "Default Gateway" and "Remote Subnet".

When you choose "Remote Subnet", you need specify one more setting: The remote subnet for the PPTP VPN server. This means any traffic at Client Site B destined to go to subnet A, will go down the PPTP Tunnel to reach the subnet on site A. All other traffic will be routed according to the 6402's routing policy

If you select the "Default Gateway" option for the PPTP client peer, all packets will be transferred via the PPTP VPN tunnel. This means the remote PPTP VPN server gateway controls the packets flowing from the PPTP client peer, via the PPTP Tunnel.

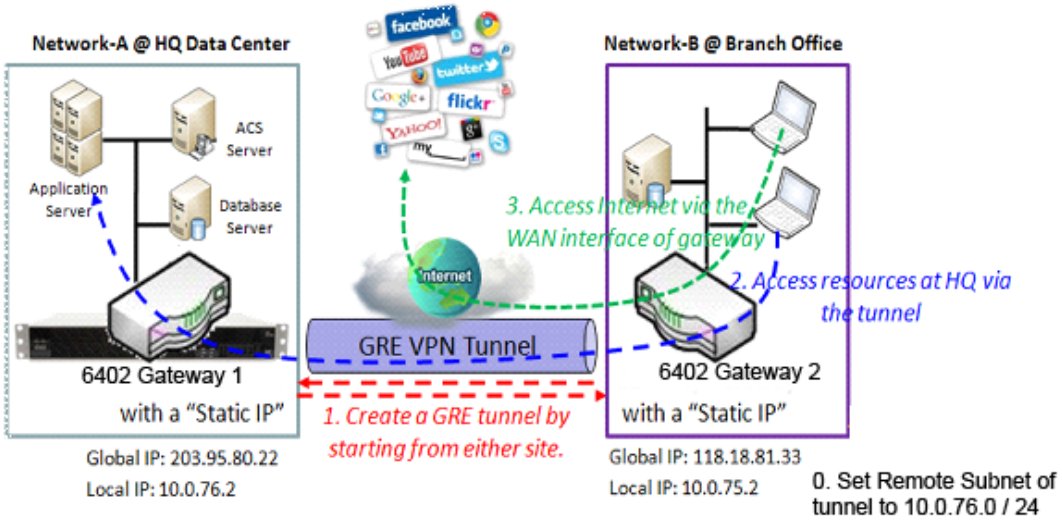
7.1.5 GRE Overview

Generic Routing Encapsulation (GRE) is a tunnelling protocol developed by Cisco Systems that encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an IP Network Link.

By installing a 6402 at a local office and establishing a virtual private network with a remote 6402 all client hosts behind the local 6402 can communicate with other sites via the 6402.

A typical scenario is for a 6402 Gateway to be installed at a branch office (Network B) for the users to access the host computers on Network A's subnet, where a 6402 Gateway supports GRE Tunnelling. The local 6402 at Network B establishes a GRE VPN Tunnel to Network A via the 6402.

GRE Tunnel at HQ Peer



GRE Example Diagram

Network-A in the headquarters, has a subnet of 10.0.76.0/24, and an IP address of 10.0.76.2 for its LAN interface and 203.95.80.22 for its WAN interface. It serves as a GRE server.

Network-B in the mobile office and has a subnet of10.0.75.0/24 has an IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for its WAN interface. It serves as a GRE client.

The GRE tunnel can be started from either site. In our example the GRE Client at Network B starts the tunnel, allowing all the devices on Network B's subnet to access the subnet at Network A via the GRE Tunnel.

Normally the hosts on the Client 6402 at Network B access the Internet directly via the 6402 WAN interface. Only the packets whose destination is on Network-A's subnet will be transferred via the GRE tunnel. However, if the "Default Gateway / Remote Subnet" parameter in 6402 Gateway 2 is configured to "Default Gateway", the users at Network B on the 6402 GRE Client wanting to access the Internet also go through the GRE VPN tunnel, allowing 6402 Gateway 1 to control access to the Internet.

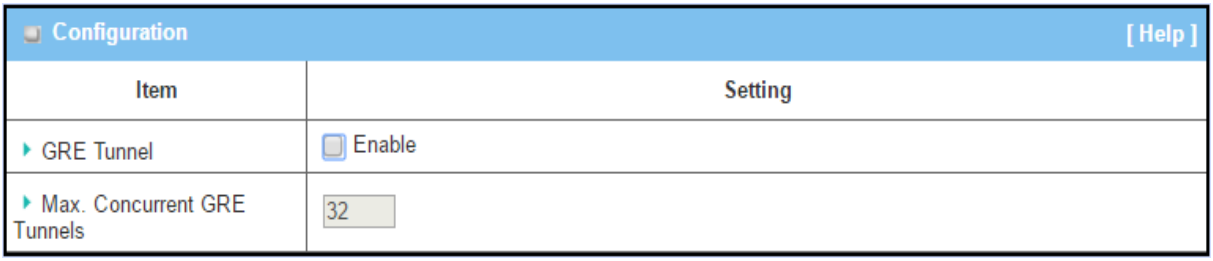
If the GRE server at HQ supports the DMVPN function, (for example as in a Cisco router operating as a VPN concentrator),the 6402 GRE client at the branch office can activate the DMVPN spoke function as supported by GRE Tunnelling over IPSec.

7.1.5.1 Configuring GRE

The GRE setting allows user to create and configure GRE tunnels. Before you proceed, ensure that the VPN is enabled and saved. To enable VPN, go to **Security> VPN > Configuration** tab.

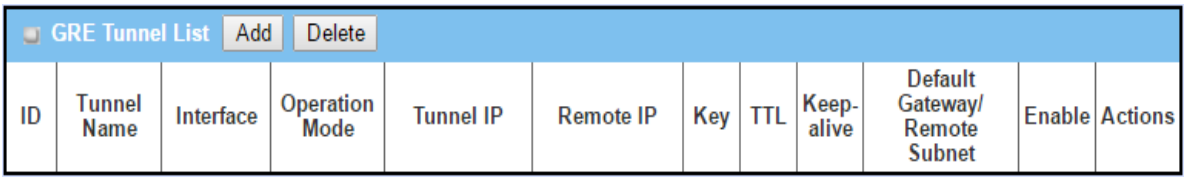
Go to Security> VPN > GRE tab.

Enable GRE

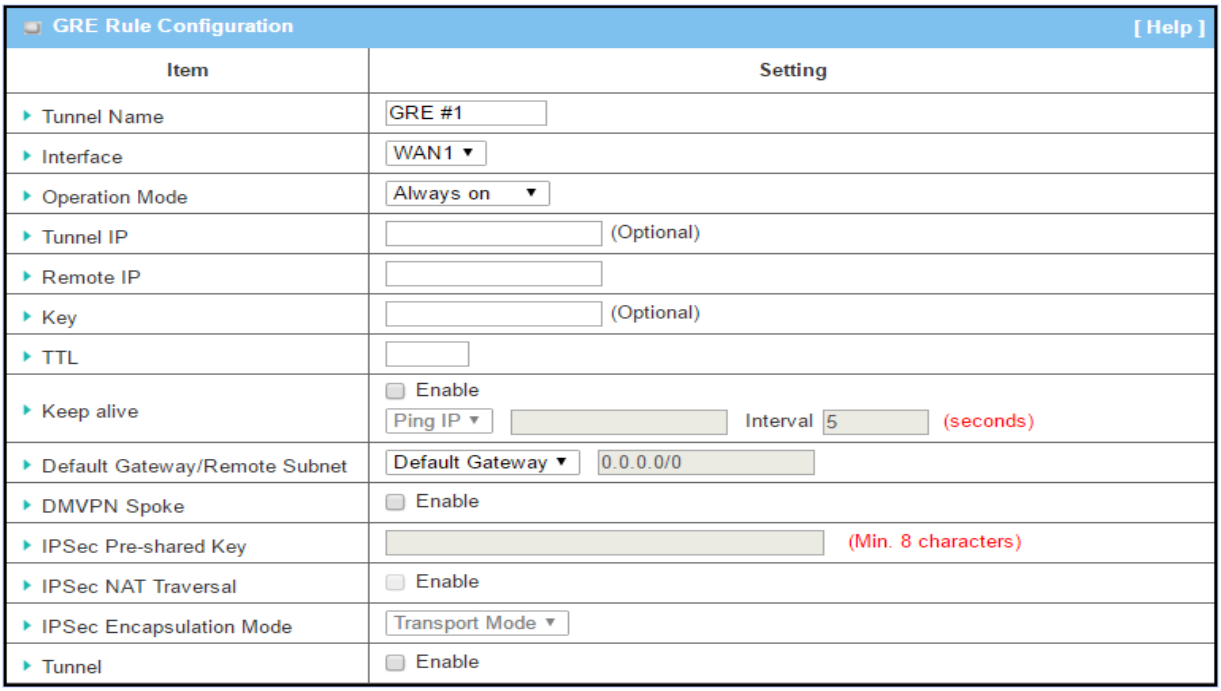


Enable GRE Window		
Item	**Value setting**	**Description**
GRE Tunnel	Unchecked by default	Click the **Enable** box to enable GRE function.
Max. Concurrent GRE Tunnels	32 is set by default Max. of 32 connections	It specifies the maximum number of simultaneous GRE tunnel connections. **Note:** The maximum supported tunnels can be different for the purchased gateway.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

7.1.5.2 Create/Edit GRE tunnel



When Add/Edit button is applied, a GRE Rule Configuration screen will appear.



GRE Rule Configuration Window		
Item	**Value setting**	**Description**
Tunnel Name	Mandatory setting	Enter a tunnel name. Enter a name that is easy for you to identify.
Interface	Mandatory WAN 1 is selected by default	Select WAN interface on which GRE tunnel is to be established.
Operation Mode	Mandatory setting Always on is selected by default	There are three available operation modes. Always On, Failover, Load Balance. **Failover/ Always** Define whether the GRE tunnel is a failover tunnel function or an Always on tunnel. **Note**: If this GRE is a failover tunnelling, you will need to select a primary GRE tunnel from which to failover to. **Load Balance** Define whether the GRE tunnel connection will take part in load balance function of the gateway. You will not need to select with WAN interface as the system will automatically utilize the available WAN interfaces to balance traffic loads. For more details on WAN Load Balance, refer to Load Balance Usage in this manual. On gateway's web-based utility, go to Basic Network > WAN& Uplink> Load Balance tab. **Note**: Failover and Load Balance functions are not available for Dynamic VPN specified in Tunnel Scenario.
Tunnel IP	An Optional setting	Enter the Tunnel IP address.
Remote IP	A Mandatory setting	Enter the Remote IP address of remote GRE tunnel gateway. Normally this is the public IP address of the remote GRE gateway.
Key	An Optional setting	Enter the Key for the GRE connection.
TTL	Mandatory setting 1 to 255 range	Specify **TTL** hop-count value for this GRE tunnel.
Keep alive	Unchecked by default 5s is set by default	Check the **Enable** box to enable Keep alive function. Select Ping IP to keep live and enter the IP address to ping. Enter the ping time interval in seconds.
Default Gateway / Remote Subnet	A Mandatory setting	Specify a gateway for this GRE tunnel to reach GRE server. If the gateway uses its gateway IP address to connect to the internet to connect to the GRE server then select Default Gateway, otherwise, specified a subnet and its netmask –the remote subnet, if the default gateway is not used to connect to the GRE server. The Remote Subnet format must be IP address/netmask (e.g. 10.0.0.2/24).
DMVPN Spoke	Unchecked by default	Specify whether the gateway will support DMVPN Spoke for this GRE tunnel. Check Enable box to enable DMVPN Spoke.
IPSec Pre-shared Key	Pre-shared Key 8 to 32 character length	Enter a DMVPN spoke authentication Pre-shared Key. **Note**: Pre-shared Key will not be available when DMVPN Spoke is not enabled.
IPSec NAT Traversal	Unchecked by default	Check Enable box to enable NAT-Traversal. Note: IPSec NAT Traversal will not be available when DMVPN is not enabled.
IPSec Encapsulation Mode	Unchecked by default	Specify IPSec Encapsulation Mode from the dropdown box. There are Transport mode and Tunnel mode supported. **Note**: IPSec Encapsulation Mode will not be available when DMVPN is not enabled.
Tunnel	Unchecked by default	Check **Enable** box to enable this GRE tunnel.
Save	N/A	Click **Save** button to save the settings.
Undo	N/A	Click **Undo** button to cancel the settings.
Back	N/A	Click **Back** button to return to the previous page.

When the Add button is applied, the OpenVPN Client Configuration screen will appear.

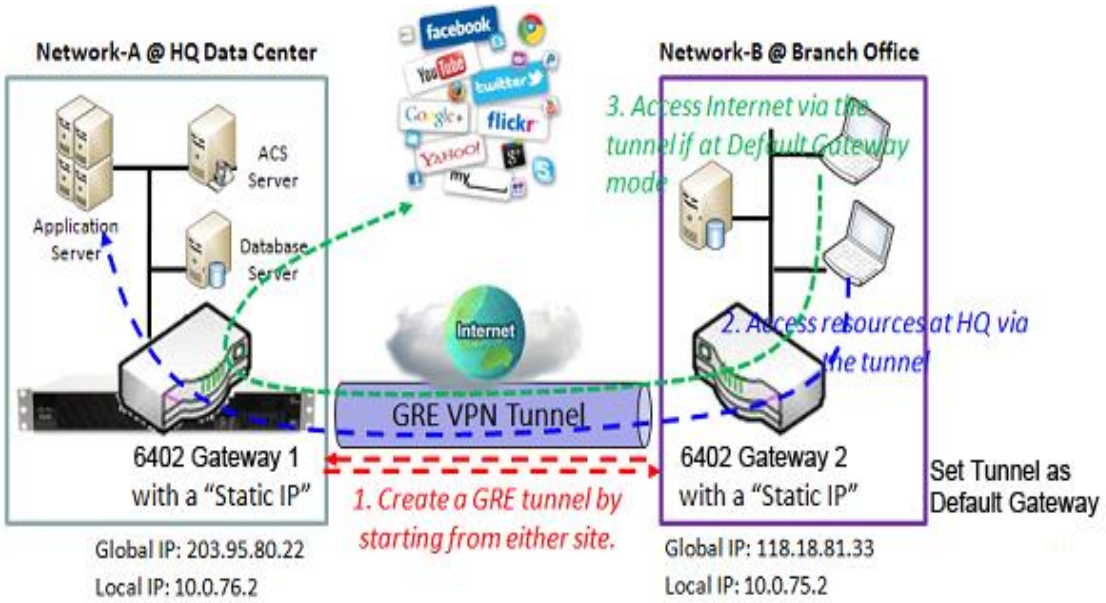
The OpenVPN Client Configuration window let you specify the required parameters for one of the OpenVPN VPN clients, such as "OpenVPN Client Name", "Interface", "Protocol", "Tunnel Scenario", "Remote IP/FQDN", "Remote Subnet", "Authorisation Mode", "Encryption Cipher", "Hash Algorithm" and tunnel activation.

OpenVPN Client Configuration

Item	Setting
OpenVPN Client Name	OpenVPN Client #1
Interface	WAN 1
Protocol	TCP Port: 443
Tunnel Scenario	TUN
Remote IP/FQDN	
Remote Subnet	255.255.255.0(/24)
Redirect Internet Traffic	Enable
NAT	Enable
Authorization Mode	TLS CA Cert.: Client Cert.: Client Key.: Please set the Certificate.
Encryption Cipher	Blowfish
Hash Algorithm	SHA-1
LZO Compression	Adaptive
Persist Key	Enable
Persist Tun	Enable
Advanced Configuration	Edit
Tunnel	Enable

When Advanced Configuration is selected, an OpenVPN Client Advanced Configuration screen will appear.

7.1.5.3 GRE Configuration Example For Network-A



The following table lists the parameter configuration for above example diagram of GRE VPN server in Network-A. Use default value for those parameters that are not mentioned in these tables.

Configuration Path	[GRE]-[Configuration]
GRE	■ *Enable*
Configuration Path	**[GRE]-[GRE Rule Configuration]**
Tunnel Name	*GRE HQ*
Interface	*WAN 1*
Operation Mode	*Always on*
Tunnel IP	*203.95.80.22*
Remote IP	*118.18.81.33*
Key	*1234*
TTL	255
Default Gateway/Remote Subnet	*Remote Subnet 10.0.75.0/24*
Tunnel	■ *Enable*

7.1.5.4 GRE Configuration Example For Network - B

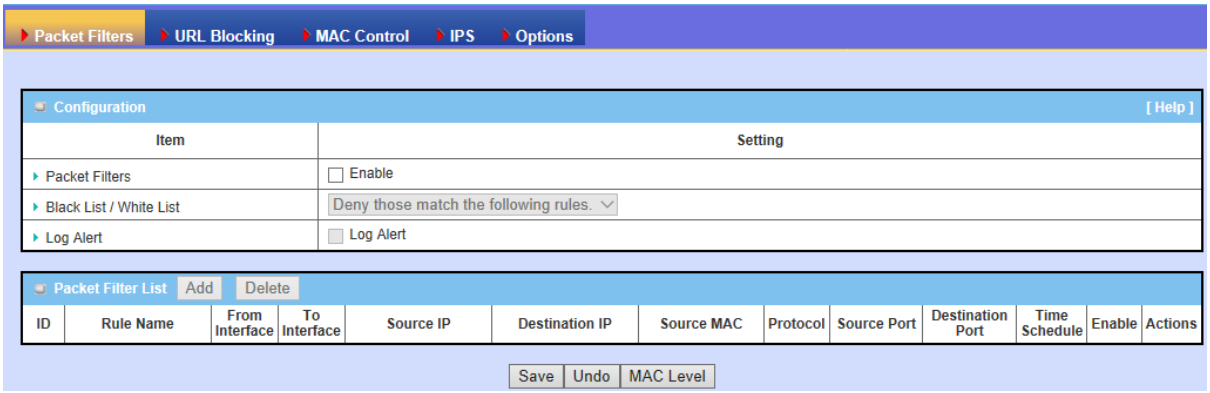
The following table lists the parameter configuration for above example diagram of GRE VPN server in Network-B. Use default value for those parameters that are not shown in these tables.

Configuration Path	[GRE]-[Configuration]
GRE	■Enable
Configuration Path	[GRE]-[GRE Rule Configuration]
Tunnel Name	GRE BO
Interface	WAN 1
Operation Mode	Always on
Tunnel IP	118.18.81.33
Remote IP	203.95.80.22
Key	1234
TTL	255
Default Gateway/Remote Subnet	Default Gateway
Tunnel	■ Enable

.

7.2. FIREWALL

The firewall functions include Packet Filters, URL Blocking, MAC Control, IPS and some firewall options. The supported function can be different for the purchased gateway.

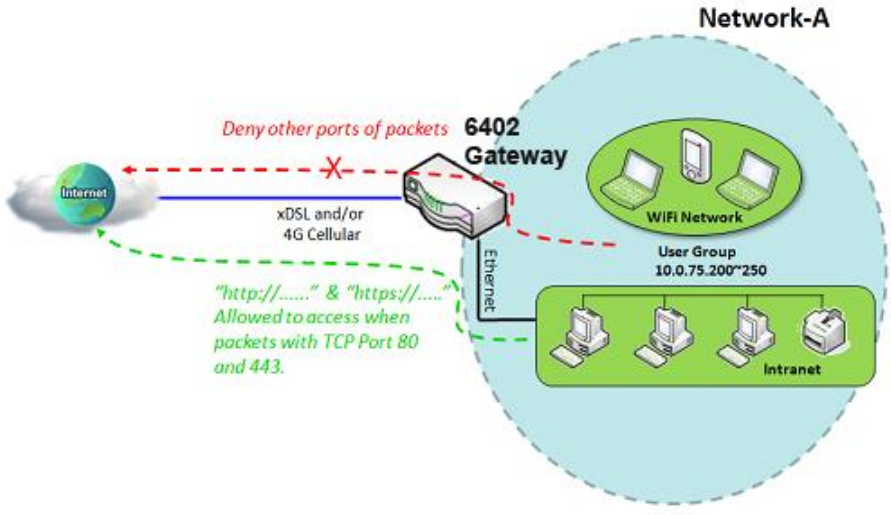


7.2.1. Packet Filter

The "Packet Filter" function allows a network manager to define filtering rules for incoming and outgoing packets. The 6402 can control which packets are allowed to pass or blocked. A packet filter rule should indicate the following

- Source Interface from which it entered the 6402.
- Destination port that the packet will leave the 6402
- The Source and destination IP Addresses
- Destination service port type
- Port Number
- The time schedule when the rule will be enabled

7.2.2.1. Packet Filter White List Example



7.2.2.2. Packet Filter Configuration Example

When the 6402 manager wants to only allow specific packets through the 6402, they can use the "Packet Filter" to allow specific packets to pass by defining a white list as shown in above diagram. When the administrator wants to deny specific packets from passing through the 6402, they can define a ‘Black List ‘ by using the "Packet Filter".

The following table lists the configuration as an example for the gateway in above diagram with "Packet Filters" enabled. Use default value for those parameters that are not mentioned in the tables.

Configuration Path	**[Packet Filter]-[Configuration]**	
Packet Filters	■ *Enable*	
Black List / White List	*Deny all to pass except those that match the following rules.*	
Configuration Path	**[Packet Filter]-[Packet Filter Rule List]**	
ID	1	2
Rule Name	*Access 80*	*Access 443*
Source IP	*IP Range: 10.0.75.200 ~ 10.0.75.250*	*IP Range: 10.0.75.200 ~ 10.0.75.250*
Destination IP	*Specific IP Address: 0.0.0.0*	*Specific IP Address: 0.0.0.0*
Destination Port	*User-defined Service: 80 ~ 80*	*User-defined Service: 443 ~ 443*
Protocol	*TCP*	*TCP*
Rule	■ *Enable*	■ *Enable*

7.2.2.3. Packet Filter Operation Example

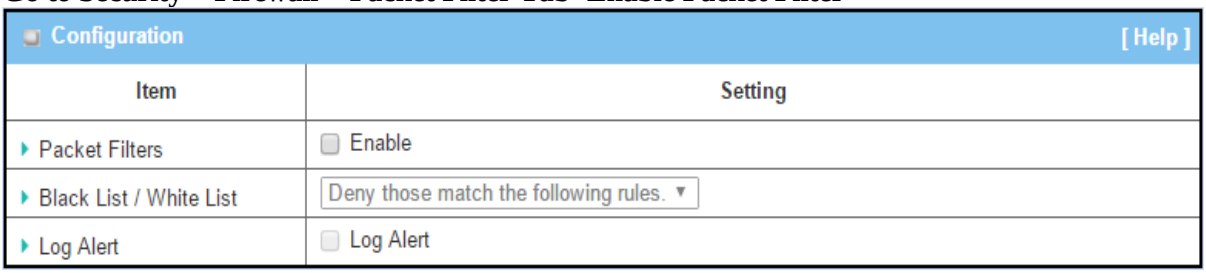
In above diagram, the 6402 is on Network-A with a subnet of 10.0.75.0/24, with an IP address of 10.0.75.2 for its LAN interface, and 118.18.81.33 for its WAN-1 interface. It serves as a NAT router. Enable the packet filter function and specify the "Packet Filter Rule List" is a white list and configure two packet filtering rules for the 6402. Create one rule to allow HTTP packets and the other rule to allow HTTPS packets to pass through the gateway.

The 6402 will allow only HTTP and HTTPS packet to pass through the 6402 for those hosts on the Subnet and with their IP addresses in the range from .200 to .250.

7.2.2.4. Packet Filter Setting

The packet filter setting allows user to create and customise packet filter policies to allow or reject specific inbound/outbound packets through the router based on their office setting.

Go to Security > Firewall > Packet Filter Tab>Enable Packet Filter

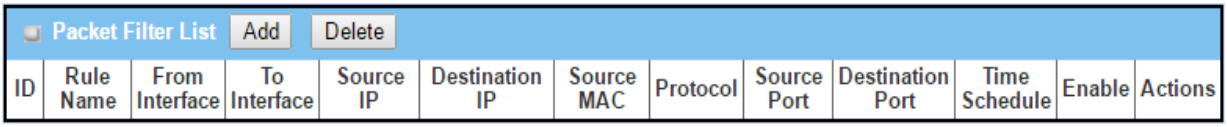


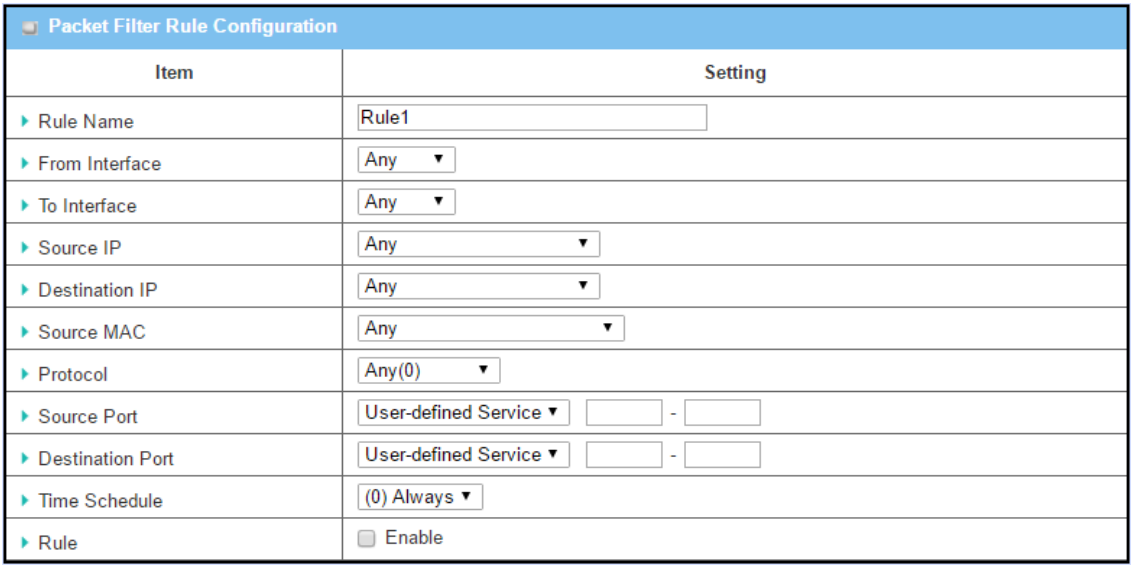
Enabling Packet Filters		
Item Name	**Value setting**	**Description**
Packet Filter	The box is unchecked by default	Check the **Enable** box to activate Packet Filter function
Black List / White List	Deny those match the following rules is set by default	When ***Deny those match the following rules*** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with ***Allow those match the following rules***, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Note: Packet Filter function is only available when Firewall feature is enabled. Refer to section Firewall

7.2.2.5. Create / Edit Packet Filter Rules

The 6402 allows you to customize your packet filtering rules. It supports up to a maximum of 20 filter rule sets.





Packet Filter Rule Configuration		
Item Name	**Value setting**	**Description**
Rule Name	1.String any text 2. Mandatory setting	Enter a packet filter rule name. Enter a name that is easy for you to remember.
From Interface	Mandatory setting By default, Any is selected	Define the selected interface to be the packet-entering interface of the router. If the packets to be filtered are coming from **LAN to WAN,** then select LAN for this field. Or **VLAN-1 to WAN** then select **VLAN-1** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets coming into the router from any interfaces. Please note that two identical interfaces are not accepted by the router. i.e. VLAN-1 to VLAN-1.
To Interface	A Mandatory setting By default, Any is selected	Define the selected interface to be the packet-leaving interface of the router. If the packets to be filtered are entering from **LAN to WAN, then** select **WAN** for this field. Or **VLAN-1 to WAN** then select **WAN** for this field. Other examples are VLAN-1 to VLAN-2. VLAN-1 to WAN. Select **Any** to filter packets leaving the router from any interfaces. Please note that two identical interfaces are not accepted by the router. i.e. VLAN-1 to VLAN-1.
Source IP	A Mandatory setting By default, Any is selected	This field is to specify the **Source IP address**. Select **Any** to filter packets coming from any IP addresses. Select **Specific IP Address** to filter packets coming from an IP address. Select **IP Range** to filter packets coming from a specified range of IP address. Select **IP Address-based Group** to filter packets coming from a pre-defined group. Note: group must be pre-defined before this option become available. Refer to **Object Definition**>**Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.

Destination IP	A Mandatory setting By default, Any is selected	This field is to specify the **Destination IP address**. Select **Any** to filter packets that are entering to any IP addresses. Select **Specific IP Address** to filter packets entering to an IP address entered in this field. Select **IP Range** to filter packets entering to a specified range of IP address entered in this field. Select **IP Address-based Group** to filter packets entering to a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition**>**Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button. Setting done through the **Add Rule** button will also appear in the **Host grouping** setting screen.
Source MAC	A. Mandatory setting By default, Any is selected	This field is to specify the **Source MAC address**. Select **Any** to filter packets coming from any MAC addresses. Select **Specific MAC Address** to filter packets coming from a MAC address. Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition**>**Grouping > Host grouping.** You may also access to create a group by the **Add Rule** shortcut button.
Protocol	A .Mandatory setting By default, Any(0) is selected	For **Protocol**, select **Any** to filter any protocol packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range.
		For **Protocol**, select **ICMPv4** to filter ICMPv4 packets
		For **Protocol**, select **TCP** to filter **TCP** packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range.
		For **Protocol**, select **UDP** to filter **UDP** packets Then for **Source Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range. Then for **Destination Port**, select a predefined port dropdown box when **Well-known Service** is selected, otherwise select **User-defined Service** and specify a port range.
		For **Protocol**, select **GRE** to filter **GRE** packets
		For **Protocol**, select **ESP** to filter **ESP** packets
		For **Protocol**, select **SCTP** to filter **SCTP** packets
		For **Protocol**, select **User-defined** to filter packets with specified port number. Then enter a pot number in **Protocol Number** box.
Time Schedule	Mandatory setting	Apply **Time Schedule** to this rule, otherwise leave it as Always. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition> Scheduling >Configuration tab**
Rule	The box is unchecked by default.	Click **Enable** box to activate this rule then save the settings.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	When the **Back** button is clicked the screen will return to the Packet Filters Configuration page.

7.2.2. URL Blocking

The "URL Blocking" function allows a network manager to define blocking or rule or rules to allow incoming and outgoing Web request packets. With defined rules, the 6402 can control the Web requests containing the following

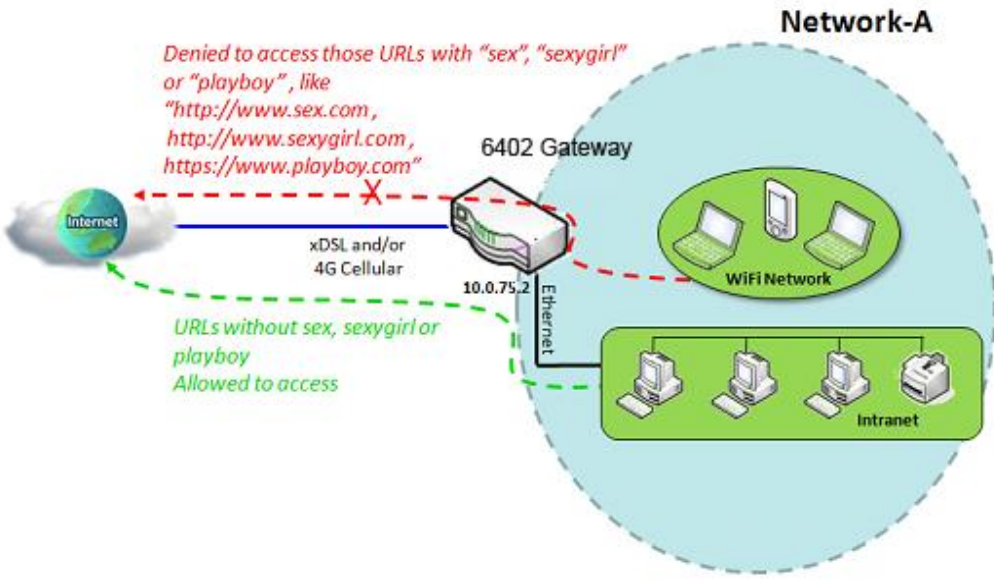
- Complete URL or
- Partial domain name or
- Pre-defined keywords.

For example, one can filter out or allow only the Web requests based on domain input suffixes like .com or .org or keywords like “bct” or “mpe”.

An URL blocking rule should specify the URL, partial domain name, or included keywords in the Web requests from and to the gateway and also the destination service port.

A specific time schedule can be applied to activate the URL Blocking rules
The 6402 will log and display the disallowed web access requests that match the defined URL blocking rule in the black-list or in the exclusion of the white-list.
When you choose "Allow all to pass except those that match the following rules" for the "URL Blocking Rule List", you are setting the defined URL blocking rules that belong to the black list. The packets, listed in the rule list, will be blocked if one pattern in the requests matches one of the rules
In contrast, when you choose "Deny all to pass except those that match the following rules" in the "URL Blocking Rule List", you are setting the defined packet filtering rules which belong to the white list. The Web requests, listed in the rule, will be allowed if one pattern in the request matches one rule. Other Web requests will be blocked.

7.2.3.1. URL Blocking with Black List Example



7.2.3.2. Black List Blocking Example Configuration

The following table lists the parameter configuration as an example for the gateway in above diagram with "URL Blocking" enabling.

Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[URL Blocking]-[Configuration]	
URL Blocking	■ Enable	
Black List / White List	Allow all to pass except those that match the following rules.	
Configuration Path	[URL Blocking]-[URL Blocking Rule List]	
ID	1	2
Rule Name	Block sex &porn	Block playboy
URL/Domain Name/Keyword	sex; porn	playboy
Rule	■ Enable	■ Enable

7.2.3.3. Example Operation Procedure

In above diagram, Network-A's 6402 Router has a subnet of 10.0.75.0/24 and IP Address of10.0.75.2 for its LAN interface, and 118.18.81.33 for its WAN-1 interface. It serves as a NAT router.

Enable the URL blocking function and specify the "URL Blocking Rule List" with a black list and configure two URL blocking rules for it.

Create the first rule to deny Web requests with "sex" or "porn" patterns and the other to deny Web requests with the pattern matching the text "playboy" from going through the 6402

The 6402 will block Web requests with "sex", "porn" or "playboy" from passing through the 6402.

7.2.3.4. URL Blocking Setting

The URL Blocking setting allows user to create and customize URL blocking policies to allow or reject http packets with specific keywords, domain names, or URL's.

In "URL Blocking" page, there are three configuration windows.

- They are the "Configuration" window,
- "URL Blocking Rule List" window,
- "URL Blocking Rule Configuration" window.

The "Configuration" window can let you activate the URL blocking function and specify a black list or white list packets as defined in the "URL Blocking Rule List" entry.

In addition, a log can be enabled to generate an alert and record any disallowed events.

Web request packets. Refer to "System Status" in the "System Related" section in this user manual to see how to view log.

The "URL Blocking Rule List" window lists all your defined URL blocking rule entries.

The "URL Blocking Rule Configuration" allows the network manager to define the URL blocking rules. The parameters in a rule include;

- The rule name.
- The Source IP or MAC.
- The URL/Domain Name/Keyword
- The destination service ports.
- The integrated time schedule rule and the rule activation.

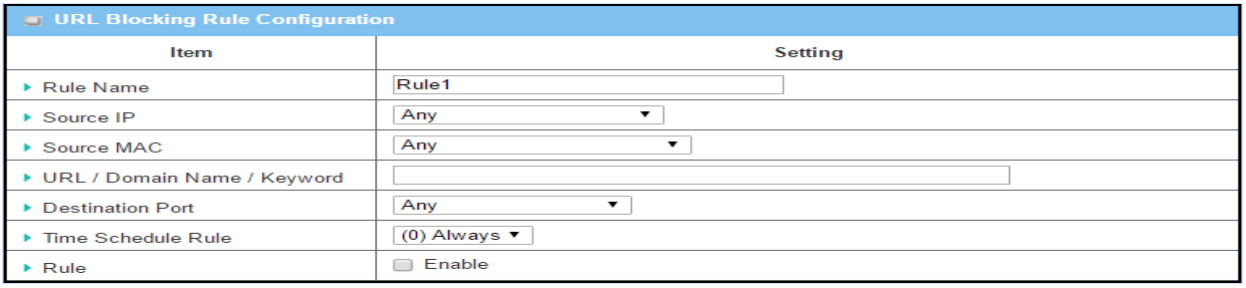
Go to Security > Firewall >URL Blocking Tab.

7.2.3.5. Enabling URL Blocking

Configuration		
Item	**Value setting**	**Description**
URL Blocking	The box is unchecked by default	Check the **Enable** box to activate URL Blocking function.
Black List / White List	Deny those match the following rules is set by default	Specify the URL Blocking Policy, either Black List or White List. Black List: When **Deny those match the following rules** is selected, as the name suggest, the matched Web request packets will be blocked. White List: When **Allow those match the following rules** is selected, the matched Web request packets can pass through the Gateway, and the others that don't match the rules will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	NA	Click **Save** button to save the settings
Undo	NA	Click **Undo** button to cancel the settings

7.2.3.6. Create/Edit URL Blocking Rules

The Gateway supports up to a maximum of 20 URL blocking rule sets. Ensure that the URL Blocking is enabled before we can create blocking rules.

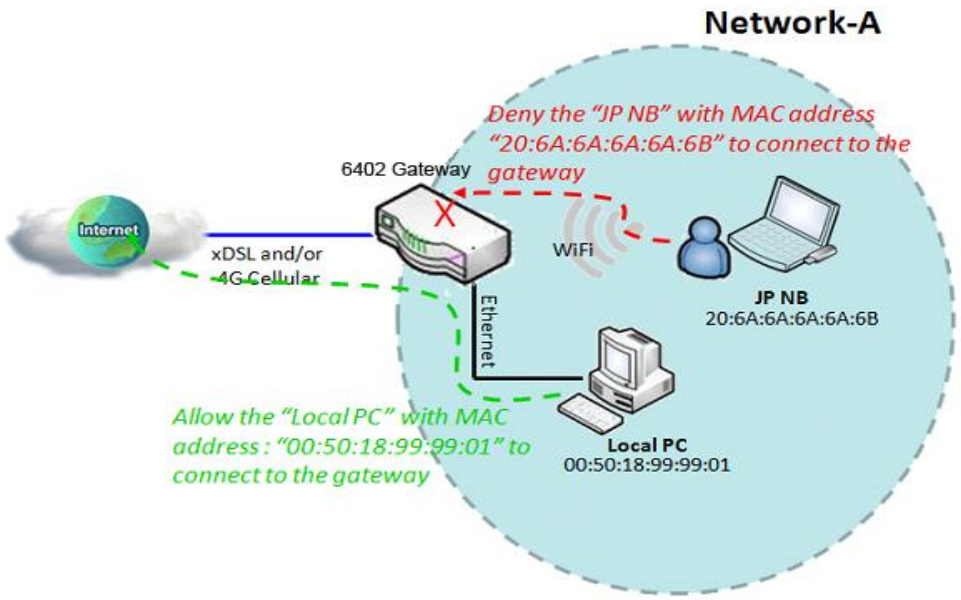


URL Blocking Rules Configuration		
Item	**Value setting**	**Description**
Rule Name	String format can be any text A Mandatory setting	Specify an URL Blocking rule name. Enter a name that is easy for you to understand.
Source IP	A Mandatory setting **Any** is set by default	This field is to specify the **Source IP address**. • Select **Any** to filter packets coming from any IP addresses. • Select **Specific IP Address** to filter packets coming from an IP address entered in this field. • Select **IP Range** to filter packets coming from a specified range of IP address entered in this field. • Select **IP Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this option become available. Refer to **Object Definition** >**Grouping > Host grouping**.
Source MAC	Mandatory setting **Any** is set by default	This field is to specify the **Source MAC address**. • Select **Any** to filter packets coming from any MAC addresses. • Select **Specific MAC Address** to filter packets coming from a MAC address entered in this field. • Select **MAC Address-based Group** to filter packets coming from a pre-defined group selected. Note: group must be pre-defined before this selection become available. Refer to **Object Definition** >**Grouping > Host grouping**.
URL / Domain Name / Keyword	1. A Mandatory setting 2. Supports up to a maximum of 10 Keywords in a rule by using the delimiter ";".	Specify URL, Domain Name, or Keyword list for URL checking. • In the **Black List** mode, if a matched rule is found, the packets will be dropped. • In the **White List** mode, if a matched rule is found, the packets will be accepted and the others which don't match any rule will be dropped.
Destination Port	A Mandatory setting **Any** is set by default	This field is to specify the **Destination Port number**. • Select **Any** to filter packets going to any Port. • Select **Specific Service Port** to filter packets going to a specific Port entered in this field. • Select **Port Range** to filter packets going to a specific range of Ports entered in this field.
Time Schedule Rule	A Mandatory setting	Apply a specific **Time Schedule** to this rule, otherwise leave it as **(0) Always**. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition** >**Scheduling > Configuration** tab.
Rule	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	*NA*	Click the **Save** button to save the settings.

7.2.4. MAC Control

"MAC Control" function allows you to assign the accessibility to the gateway for different users based on device's MAC address, including wired hosts or Wi-Fi stations.

MAC Control with Black List Scenario



7.2.4.1. Mac Control Example

When the 6402 Network Manager wants to reject client hosts with specific MAC addresses in the from the Internet that wants to connect to the 6402, they can use the "MAC Control" function to create a black list as shown in above diagram.

The Network Manager wants to allow only client hosts with dedicated MAC addresses to connect to the 6402, they can use the "MAC Control" function by defining a white list of MAC Addresses they would like to allow to connect. They can also reject any hosts with specific MAC Addresses listed in the Black List

7.2.4.2. Mac Control Example Configuration

Following tables list the parameter configuration as an example for the gateway in above diagram with "MAC Control" enabling.

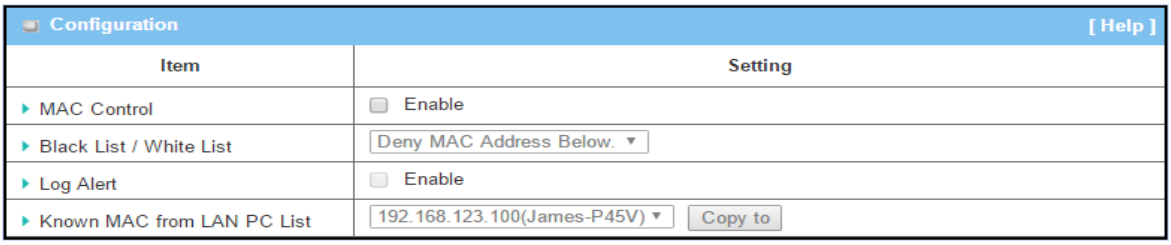
Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[MAC Control]-[Configuration]
MAC Control	■ *Enable*
Black List / White List	*Allow all to pass except those that match the following rules.*
Log Alert	■ *Enable*
Configuration Path	**[MAC Control]-[MAC Control Rule List]**
ID	1
Rule Name	*Block JP NB*
MAC Address	*20:6A:6A:6A:6A:6B*
Rule	■ *Enable*

7.2.4.3. MAC Control Setting

The MAC control setting allows user to create and customize MAC address policies to allow or reject packets with specific source MAC address. Before you proceed, ensure that the Firewall is enabled and saved. Go to Security > Firewall > Configuration tab.

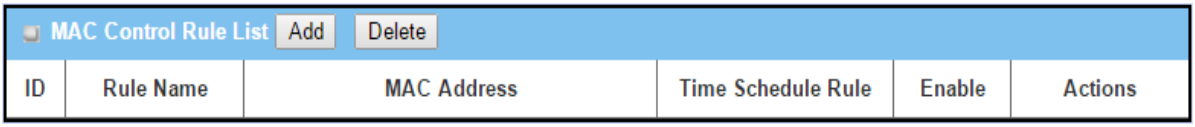
Go to Security > Firewall > MAC Control Tab>Enable MAC Control



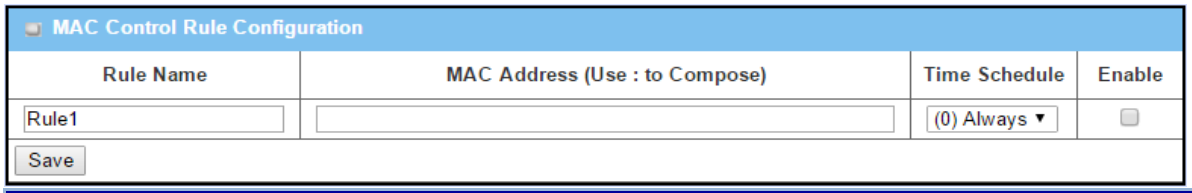
Enabling MAC Control		
Item	**Value setting**	**Description**
MAC Control	The box is unchecked by default	Check the **Enable** box to activate the MAC filter function
Black List / White List	Deny MAC Address Below is set by default	When ***Deny MAC Address Below*** is selected, as the name suggest, packets specified in the rules will be blocked –black listed. In contrast, with ***Allow MAC Address Below***, you can specifically white list the packets to pass and the rest will be blocked.
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Known MAC from LAN PC List	N/A	Select a MAC Address from LAN Client List. Click the **Copy to** copy the selected **MAC Address** to the filter rule.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

7.2.4.4. Create/Edit MAC Control Rules

The 6402supports up to a maximum of 20 filter rule sets. Ensure that the MAC Control is enabled before we can create control rules.



When Add button is applied, Filter Rule Configuration screen will appear.

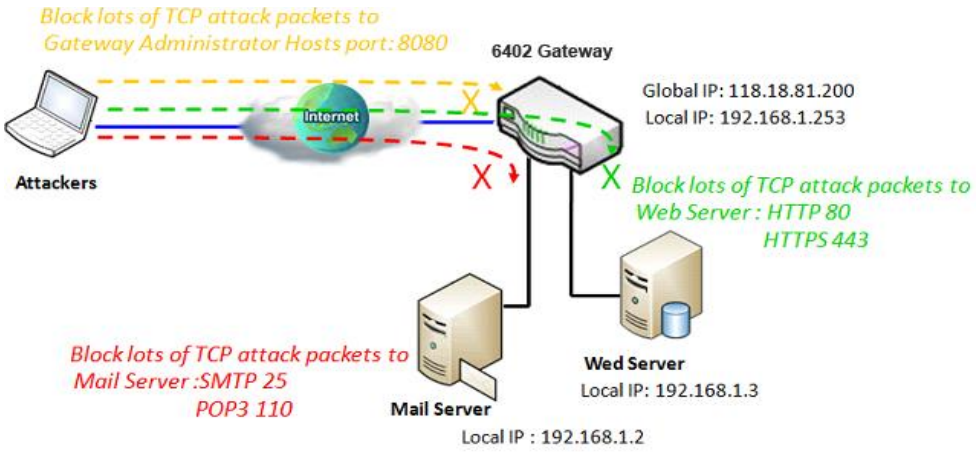


MAC Control Rule Configuration		
Item	**Value setting**	**Description**
Rule Name	String format can be any text Mandatory Setting	Enter a MAC Control rule name. Enter a name that is easy for you to remember.
MAC Address (Use: to Compose)	MAC Address string Format Mandatory Setting	Specify the **Source MAC Address** to filter rule.
Time Schedule	Mandatory Setting. (0) Always is selected by default	Apply **Time Schedule** to this rule, otherwise leave it as Always. If the dropdown list is empty, ensure **Time Schedule** is pre-configured. Refer to **Object Definition> Scheduling >Configuration** tab.
Enable	The box is unchecked by default.	Click the **Enable** box to activate this rule.
Save	N/A	Click the **Save** button to save the configuration.
Undo	N/A	Click the **Undo** button to restore what you just configured back to the previous setting.
Back	N/A	When the **Back** button is clicked, the screen will return to the MAC Control Configuration page.

7.2.5. IPS Overview

Intrusion Prevention System (IPS) is network security appliance that monitors network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempts to block/stop it and report it.
The network manager can enable the IPS function and select the intrusion activities.
There are some intrusion prevention items that require further Threshold parameter to work properly for intrusion detection. You can enable log alerting so that the 6402 will record Intrusion events when corresponding intrusions are detected.

IPS Example



7.2.5.1. IPS Application Example

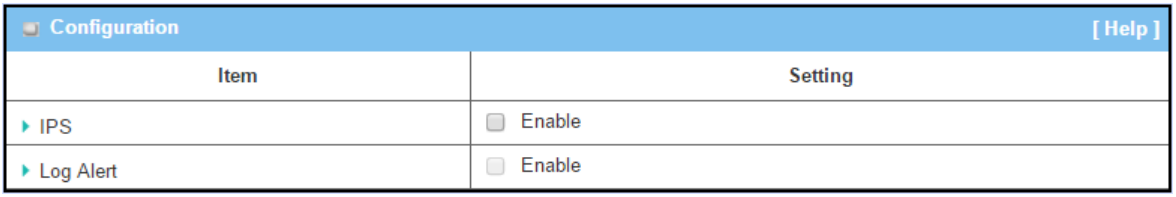
The Network Manager provides application servers on its subnet. There are some risks providing always open service ports accessible from the internet for admin users. In order to avoid such attacks, we need enable IPS functions.
On the 6402 we have an E-mail server, Web Server and open TCP-Port 8080 allowing user to access web-based utilities connected to the 6402, allowing remote users or unknown users to request those services from the gateway.

7.2.5.2. Configuring IPS

The Intrusion Prevention System (IPS) setting allows user to customize intrusion prevention rules to prevent malicious packets.

Go to Security > Firewall >IPS Tab

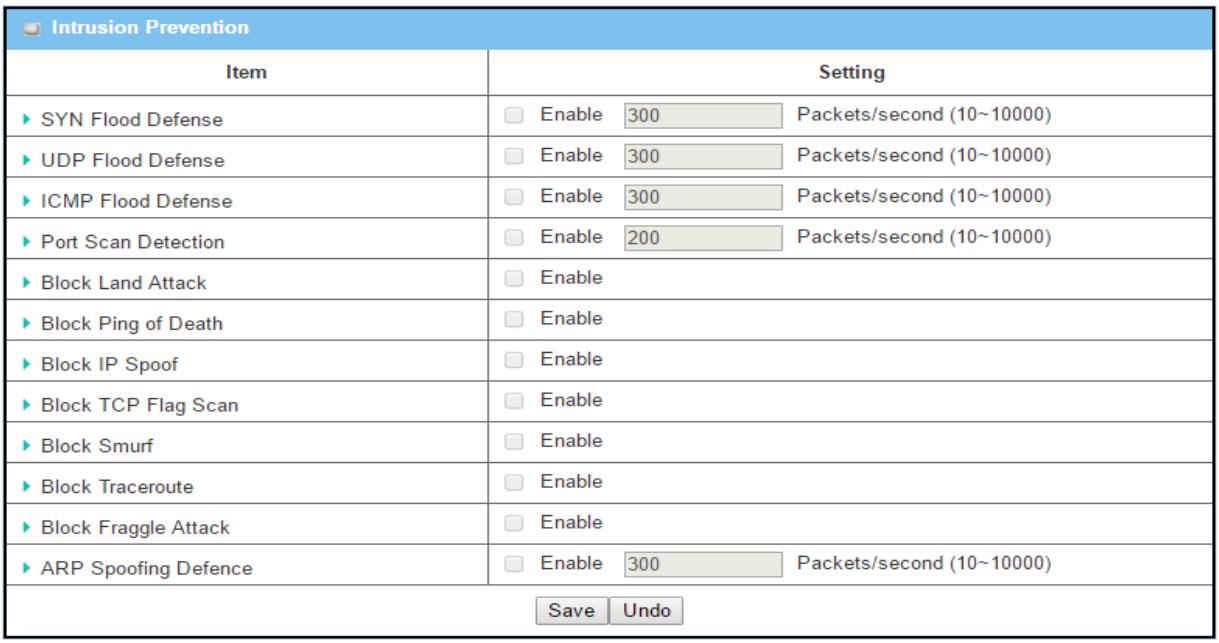
Enable IPS Firewall



Configuration		
Item	**Value setting**	**Description**
IPS	The box is unchecked by default	Check the **Enable** box to activate IPS function
Log Alert	The box is unchecked by default	Check the **Enable** box to activate Event Log.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

7.2.5.3. Intrusion Prevention Rules

The router allows you to select intrusion prevention rules you may want to enable. Ensure that the IPS is enabled before we can enable the defence function.



Intrusion Prevention		
Item	**Value setting**	**Description**
SYN Flood Defence UDP Flood Defence ICMP Flood Defence	1. A Mandatory Setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field. Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
Port Scan Defection	1. A Mandatory Setting 2. The box is unchecked by default. 3. Traffic threshold is set to 200 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.
Block Land Attack Block Ping of Death Block IP Spoof Block TCP Flag Scan Block Smurf Block Traceroute Block Fraggle Attack	The box is unchecked by default.	Click **Enable** box to activate this intrusion prevention rule.
ARP Spoofing Defence	1. A Mandatory Setting 2. The box is unchecked by default. 3. Traffic threshold is set to 300 by default 4. The value range can be from 10 to 10000.	Click **Enable** box to activate this intrusion prevention rule and enter the traffic threshold in this field.

7.2.5.4. IPS Setup Example

Following table lists the configuration for the 6402 in above diagram with "IPS" enabled.
Use default value for those parameters that are not shown in the table below

Configuration Path	[IPS]-[Configuration]
ISP	■ *Enable*
Log Alert	■ *Enable*
Configuration Path	**[IPS]-[Intrusion Prevention]**
SYN Flood Defence	■ *Enable 300 Packets/second*
Port Scan Detection	■ *Enable 200 Packets/second*
Block IP Spoof	■ *Enable*
Block TCP Flag Scan	■ *Enable*

Scenario Procedure

In above diagram, the 6402 detects incoming packets whose TCP ports are 25, 80,110,443 and 8080. The 6402 then forwards the E-mail service requests to the LAN servers and sends the replies from LAN servers back to the requester.

7.2.6. Other Options

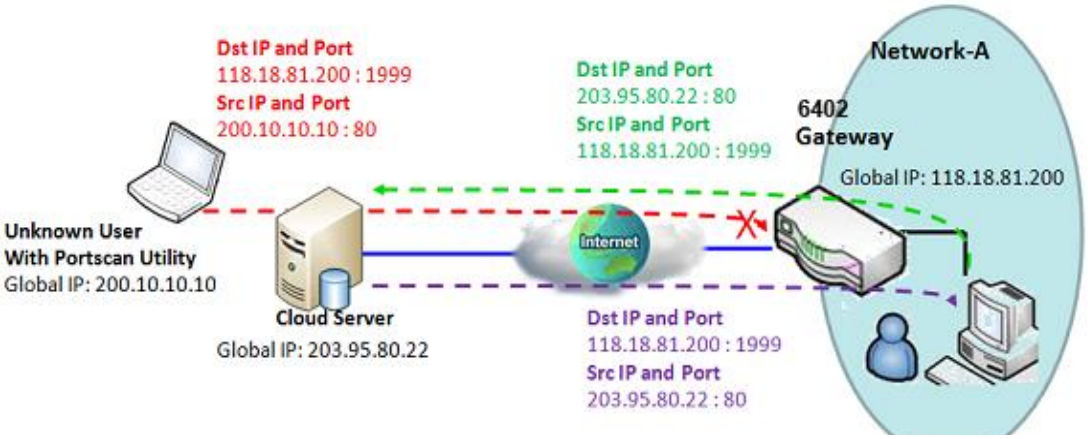
This page contains some additional options

- First, “Stealth Mode” stops the 6402 from responding to port scans from the WAN making it less susceptible to discovery and attacks from the Internet.
- Second, ”SPI” enables the 6402 to record the packet information such as IP address, port address, ACK, SEQ number and so on while they pass through the 6402. The 6402 checks every incoming packet to detect if this packet is valid.
- Third, “Discard Ping from WAN” prevents any host from the WAN from pinging the 6402 the 6402 won`t reply any ICMP packet from Internet.
- Lastly, “Remote Administrator Hosts” allows only users on the 6402 LAN to browse the web-based management on the 6402.

  This feature also enables you to perform administration task also from a remote host. If this feature is enabled, only specified IP address can be remote administrators.

  If the specified IP address is set to 0.0.0.0, any host can access the web-based manager. You can use subnet mask bits '/nn' notation to specify a group of trusted IP addresses for example, '10.1.2.0/24'.

7.2.6.1. SPI Example



7.2.6.2. SPI Application Scenario

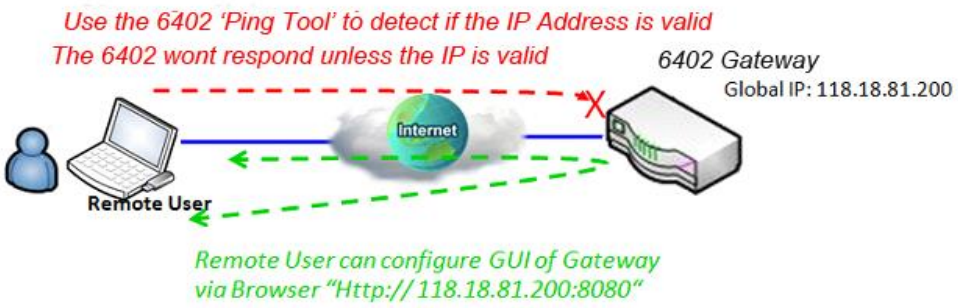
In above diagram, the 6402router on Network-A has a subnet of 10.0.75.0/24. And IP Address of 10.0.75.2 for its LAN interface and 118.18.81.200 for its WAN interface. It serves as a NAT router. Activate the SPI feature at the Gateway.
Users in Network-A initiate a connection to access a cloud server through the 6402which records connected sessions. Its possible unknown users will simulate the Packet but use different Src IP to masquerade. Enable the SPI function to prevent security leak when local users surf the internet.

7.2.6.3. SPI Setup Example

Following tables list the parameter configuration as an example for the gateway in above diagram with "SPI" enabling.

Configuration Path	[Options]-[Firewall Options]
SPI	■ ***Enable***

7.2.6.4. Discard Ping from WAN and Remote Hosts



Following table lists the configuration for the example in the above diagram.

Configuration Path	[Options]-[Firewall Options]
Discard Ping from WAN	■ *Enable*
Remote Administrator Hosts	■ *Enable HTTPS , ANY : 8080* *Please disable "SPI" Function.*

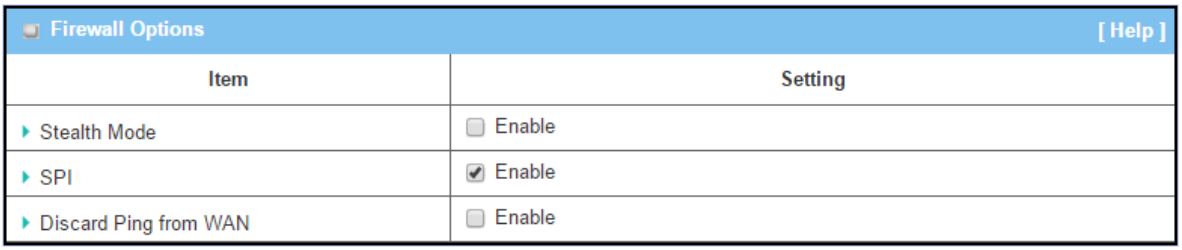
Scenario Operation Procedure

In above diagram, 6402 at Network-A has a subnet of 10.0.75.0/24, and LAN Interface of 10.0.75.2 and WAN Interface of118.18.81.200. It serves as a NAT router.
With this feature enabled on the 6402 remote users can't get responses to Pings but can access the web-based utility of Gateway via port 8080 of TCP.

7.2.7. Setting Firewall Options.

The firewall options setting allows network administrator to modify the behaviour of the firewall and to enable Remote Router Access Control.

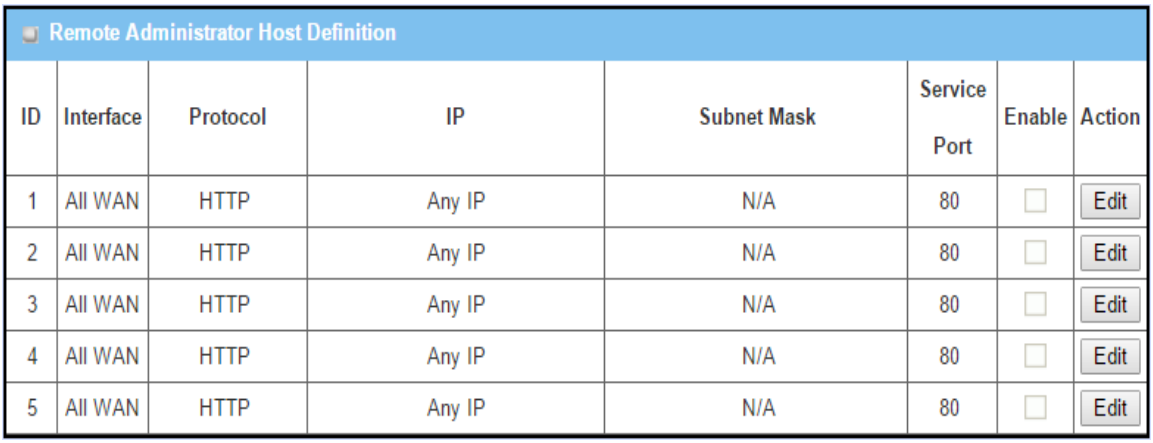
Go to Security > Firewall > Options Tab > Firewall Options



Firewall Options		
Item	**Value setting**	**Description**
Stealth Mode	The box is unchecked by default.	Check the **Enable** box to activate the Stealth Mode function
SPI	The box is checked by default.	Check the **Enable** box to activate the SPI function
Discard Ping from WAN	The box is unchecked by default.	Check the **Enable** box to activate the Discard Ping from WAN function

7.2.7.1. Define Remote Administrator Host

The 6402 allows the network manager to connect to the 6402 remotely to manage the unit. The network administrator can assign specific IP address and service port to allow accessing the router.



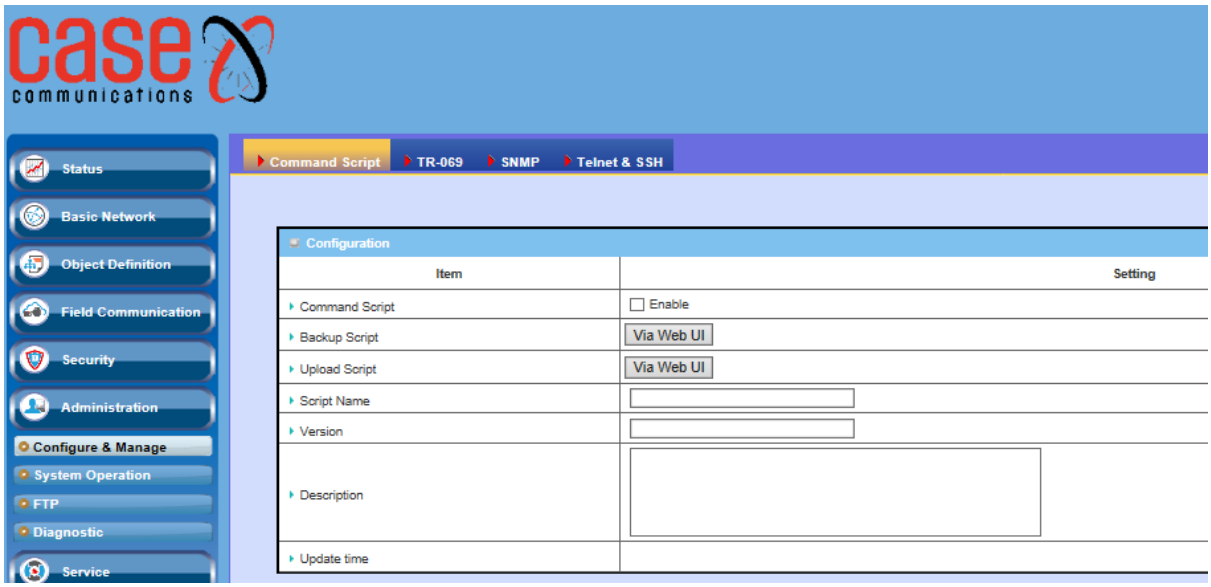
Remote Administrator Host Definition		
Item	**Value setting**	**Description**
Protocol	HTTP is set by default	Select **HTTP** or **HTTPS** method for router access.
IP	A Mandatory setting	This field is to specify the remote host to assign access right for remote access. Select **Any IP** to allow any remote hosts Select **Specific IP** to allow the remote host coming from a specific subnet. An IP address entered in this field and a selected **Subnet Mask** to compose the subnet**.**
Service Port	80 for HTTP by default 443 for HTTPS by default	This field is to specify a Service Port to HTTP or HTTPS connection.
Enabling the rule	Unchecked by default.	Click **Enable** box to activate this rule.
Save	N/A	Click **Enable** box to activate this rule then save the settings.
Undo	N/A	Click **Undo** to cancel the settings

This page left intentionally blank.

CHAPTER 8

ADMINISTRATION

8.1. Configure & Manage



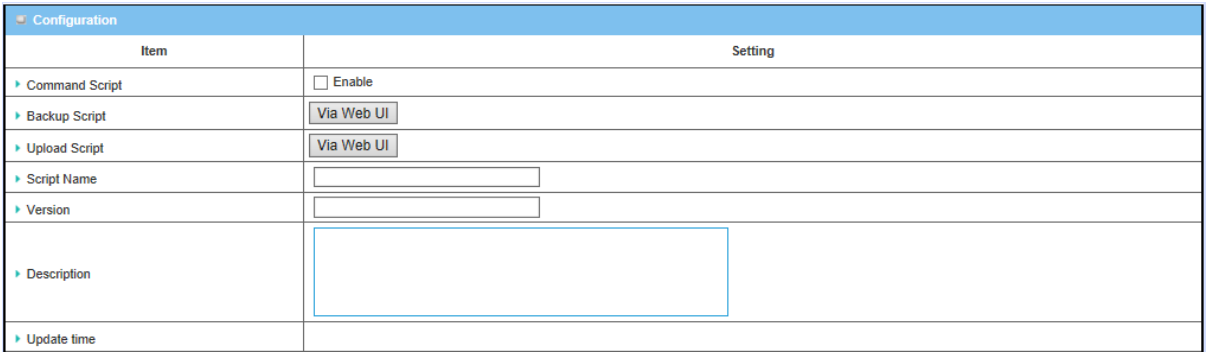
If a company only has a small network it may deem it too expensive to invest in a network management system, but where a number of devices are employed a Network Management can be invaluable to not only configure but monitor and diagnose problems. The Case Communications 6402 has management protocols, such as a Command Script, TR-069 and Telnet with a CLI. These are described in the 'Configure & Manage' section of this manual,

8.1.1. Command Script

Command script configuration is the application that allows administrator to setup the pre-defined configuration in plain text style and apply configuration on start-up.

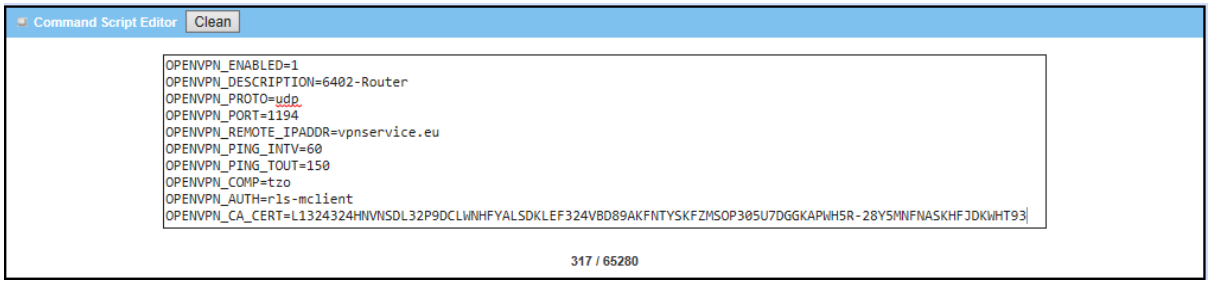
Go to Administration > Command Script > Configuration Tab.

Enable Command Script Configuration



Configuration		
Item	**Value setting**	**Description**
Command Script	The box is unchecked by default	Check the **Enable** box to activate the Command Script function.
Backup Script	Via Web UI	Clicking the "Via Web UI" button will save the script file to the PC.
Upload Script	Via Web UI	Clicking the "Via Web UI" button will allow you to select a previously backed up script file to the 642.
Script Name	Text Entry	Mandatory alphanumeric entry for the name of the script.
Version	Text Entry	Mandatory alphanumeric entry for the version of the script.
Description	Text Entry	Description for the script.
Update Time	N/A	Displays the time the scripts were created or uploaded to the 6402.

8.1.1.1. Edit/Backup Plain Text Command Script



You can edit the plain text configuration settings in the configuration screen as above.

Plain Text Configuration		
Item	**Value setting**	**Description**
Clean	*NA*	Clean text area. (You should click Save button to further clean the configuration already saved in the system.)
Save	*NA*	Save configuration

The plain text configuration items that are supported are shown in the following list. For the settings that can be executed with standard Linux commands, you can put them in a script file, and apply to the system configure with **STARTUP** command. For those configurations without corresponding Linux command set to configure, you can configure them with proprietary command set.

Configuration Content		
Key	**Value setting**	**Description**
OPENVPN_ENABLED	1: enable 0: disable	Enable or disable OpenVPN Client function.
OPENVPN_DESCRIPTION	Mandatory Setting	Specify the tunnel name for the OpenVPN Client connection.
OPENVPN_PROTO	udp tcp	Define the Protocol for the OpenVPN Client. Select TCP or TCP /UDP ->The OpenVPN will use TCP protocol, and Port will be set as 443 automatically. Select UDP -> The OpenVPN will use UDP protocol, and Port will be set as 1194 automatically.
OPENVPN_PORT	Mandatory Setting	Specify the Port for the OpenVPN Client to use.
OPENVPN_REMOTE_IPADDR	IP or FQDN	Specify the Remote IP/FQDN of the peer OpenVPN Server for this OpenVPN Client tunnel. Fill in the IP address or FQDN.
OPENVPN_PING_INTVL	seconds	Specify the time interval for OpenVPN keep-alive checking.
OPENVPN_PING_TOUT	seconds	Specify the timeout value for OpenVPN Client keep-alive checking.
OPENVPN_COMP	Adaptive	Specify the LZO Compression algorithm for OpenVPN client.
OPENVPN_AUTH	Static Key/TLS	Specify the authorization mode for the OpenVPN tunnel. TLS - The OpenVPN will use TLS authorization mode, and the following items CA Cert., Client Cert. and Client Key need to specify as well.
OPENVPN_CA_CERT	Mandatory Setting	Specify the Trusted CA certificate for the OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_CERT	Mandatory Setting	Specify the local certificate for OpenVPN client. It will go through Base64 Conversion.
OPENVPN_LOCAL_KEY	Mandatory Setting	Specify the local key for the OpenVPN client. It will go through Base64 Conversion.

OPENVPN_EXTRA_OPTS	Options	Specify the extra options setting for the OpenVPN client.
IP_ADDR1	IP	Ethernet LAN IP
IP_NETM1	Net mask	Ethernet LAN MASK
PPP_MONITORING	1: enable 0: disable	When the Network Monitoring feature is enabled, the router will use DNS Query or ICMP to periodically check Internet connection –connected or disconnected.
PPP_PING	0: DNS Query 1: ICMP Query	With DNS Query, the system checks the connection by sending DNS Query packets to the destination specified in PPP_PING_IPADDR. With ICMP Query, the system will check connection by sending ICMP request packets to the destination specified in PPP_PING_IPADDR.
PPP_PING_IPADDR	IP	Specify an IP address as the target for sending DNS query/ICMP request.
PPP_PING_INTVL	seconds	Specify the time interval for between two DNS Query or ICMP checking packets.
STARTUP	Script file	For the configurations that can be configured with standard Linux commands, you can put them in a script file, and apply the script file with STARTUP command. For example, STARTUP=#!/bin/sh STARTUP=echo “startup done” > /tmp/demo

8.1.1.2. Plain Text System Configuration with Telnet

In addition to the web-style plain text configuration as mentioned above, the 6402 also allow configuration via a Telnet CLI. An administrator can use the proprietary telnet command “*txtConfig*” and related action items to perform the plain system configuration.

The command format is:txtConfig (action) [option]

Action	Option	Description
clone	*Output file*	Duplicate the configuration content from database and stored as a configuration file. (ex: *txtConfig clone /tmp/config*) The contents in the configuration file are the same as the plain text commands mentioned above. This action is exactly the same as performing the “Backup” plain text configuration.
commit	an existing file	Commit the configuration content to database. (ex: *txtConfig commit /tmp/config*)
enable	*NA*	Enable plain text system config. (ex: *txtConfig enable*)
disable	*NA*	Disable plain text system config. (ex: *txtConfig disable*)
run_immediately	*NA*	Apply the configuration content that has been committed in database. (ex: *txtConfig run_immediately*)
run_immediately	an existing file	Assign a configuration file to apply. (ex: *txtConfig run_immediately /tmp/config*)

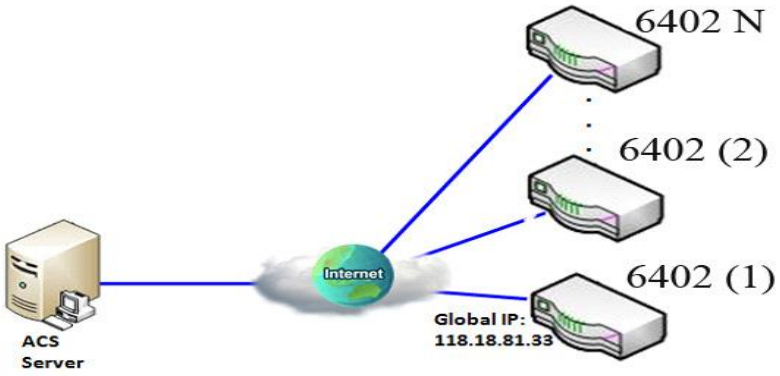
8.1.2. TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification titled ‘CPE WAN Management Protocol (CWMP)’. TR069 defines an application layer protocol for remote management of end-user devices, such as the Case Communications 6402. TR 069 is a customised feature generally used by ISP’s.

As a bi-directional SOAP/HTTP-based protocol, TR069 provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS).

It is recommended that network managers do not change the TR 069 configuration. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help.

Example- Managing 6402s through an ACS Server



8.1.2.1 TR 069 Scenario Example

When the enterprise data centre wants to use an ACS server to manage remote distributed 6402sthey can use an embedded TR-069 agent to communicate with the ACS server.
This allows the ACS server to configure, provide FW upgrade and monitor the 6402s and their corresponding Intranets.

8.1.2.2 TR 069 Scenario Description

The ACS server can configure, upgrade the 6402s with the latest FW and monitor them.
Remote 6402s send requests to the ACS server for tasks to do in each time period, and the ACS server can ask the 6402s to execute specific tasks.

8.1.2.3 TR 069 Example Configuration

Following tables list the parameter configuration as an example for the 6402 1 in above diagram with "TR-069" enabling. Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[TR-069]-[Configuration]
TR-069	■ *Enable*
ACS URL	URL of your TR069 Server
ACS User Name	*ACSUserName*
ACS Password	*ACSPassword*
Connection Request Port	*8099*
Connection Request User Name	*ConnReqUserName*
Connection Request Password	*ConnReqPassword*
Inform	■ *Enable Interval 900*

8.1.2.4 TR069 Example Operation Procedure

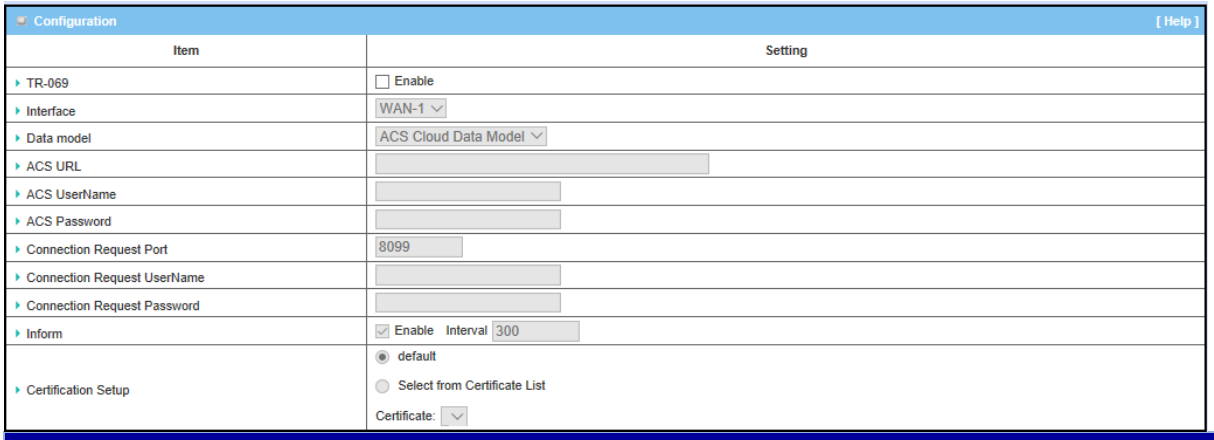
In above diagram, the ACS server can manage multiple 6402s in the Internet. The "6402 (1)" has an IP Address of118.18.81.33 for its WAN-1 interface.
When all remote 6402s have booted up, they will try to connect to the ACS server.
Once the connections are established successfully, the ACS server can configure, monitor and upgrade the 6402's with the latest FW.
Remote 6402s send enquires to the ACS server for tasks to undertake in each time period.
If the ACS server has high priority tasks, for the 6402s, it will issue a "Connection Request" command to those 6402s, and they will make immediate connections in response to the ACS server's request.

TR 069 Configuration

On the "TR-069" page, there is only one configuration window for TR-069 function.
In that window, you must specify the information for your security 6402 to connect to the ACS.
For the Drive function to work its necessary to specify the URL of the ACS server, the account information to login the ACS server, the service port and the account information for connection requesting from the ACS server, and the time interval for job inquiry.
Except the inquiry time, there are no activities between the ACS server and the 6402s until the next inquiry cycle. But if the ACS server has new jobs that are expected to be done urgently by 6402s, it will ask those 6402s by using connection request related information for immediate connections.

8.1.2.5 Configuring TR 069

Go to Administration > Configure & Manage > TR-069 tab.



TR-069		
Item	**Value setting**	**Description**
TR-069	The box is unchecked by default	Check the **Enable** box for activate TR-069
Interface	WAN-1 is selected by default.	When you finish set basic network wan 1~wan n, you can choose wan 1~wan n When you finish set **Security>VPN> IPSec/PPTP/L2TP/GRE**, you can choose IPSec/PPTP/L2TP/GRE tunnel, the interface like **"IPSec #1"**
Data Model	Standard is selected by default.	Select the TR-069 data model for the remote management. **Standard**: the ACS Server is a standard one, which is fully comply with TR-069. **Case's ACS Data Model**: Select this data model if you intend to use Case's Cloud ACS Server to managing the deployed 6402s.
ACS URL	Mandatory setting	You can ask ACS manager to provide ACS URL and manually set
ACS Username	Mandatory setting	You can ask ACS manager to provide ACS username and manually set
ACS Password	Mandatory setting	You can ask ACS manager to provide ACS password and manually set
Connection Request Port	1. Mandatory setting	You can ask ACS manager to provide ACS Connection Request Port and manually set. By default this is set to 8099
ConnectionRequest UserName	A Mandatory setting	You can ask ACS manager to provide ACS ConnectionRequest Username and manually set
ConnectionRequest Password	A Mandatory setting	You can ask ACS manager to provide ACS ConnectionRequest Password and manually set
Inform	Checked by default	When the **Enable** box is checked, the 6402 (CPE)will periodically send inform message to ACS Server.
Inform Interval	The value is 900 by default	This value decides how long send inform to ACS
Certification Setup	N/A	Allows configuration of the certificate used for security.

Default	Selected by default	Selects the default 6402 certificate.
Select from Certificate List	Alternative selection	Select to allow selection of one of the certificates on the 6402.
Certificate	Drop down list	Displays a list of all the certificates on the 6402, whether generated on the 6402 or uploaded to the 6402. Select the desires certificate.
Save	N/A	Click **Save** to save the settings

When you finish set **ACS URL ACS Username ACS Password,** your 6402 (CPE, Client Premium Equipment) can send information to the ACS Server.

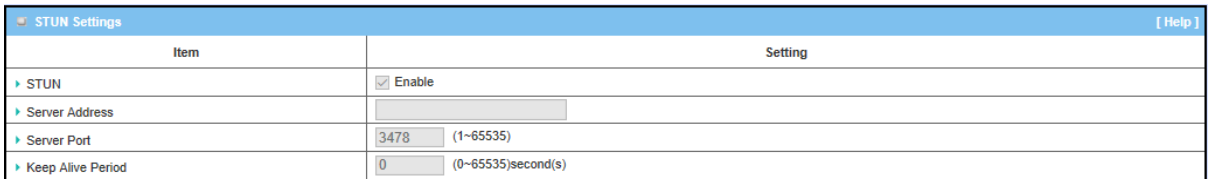
When you complete the configuration set the following

- **ConnectionRequest Port** (Default to 8099)
- **ConnectionRequest Username**
- **ConnectionRequest Password**,

The ACS Server can ask the 6402 (CPE) to send information to the ACS Server.

8.1.2.6 STUN Settings

The 6402 allows configuration of a STUN (Session Traversal Utilities for NAT) connection for security on the TR-069 connection.



STUN Settings		
Item	**Value setting**	**Description**
STUN	The box is unchecked by default	Check the **Enable** box to activate STUN for TR-069 security.
Server Address	IP	IP address of the STUN Server the 6402 connects to.
Server Port	UDP Port Number	The UDP port number the STUN Server allows for connection
Keep Alive Period	Number	Sets how often the 6402 sends a keep alive packet to the STUN Server.

8.1.3. SNMP

SNMP (Simple Network Management Protocol), is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

SNMP uses, one or more administrative computers, called Network Management Centres (NMC) or Network Management Systems (NMS), to monitor or manage a group of hosts or devices on a computer network. CaseView is a Case Communications NMC / NMS which can perform these tasks. Each Network Management System executes, a software component called an ‘Agent’ which collects and reports information from the network devices.

SNMP ‘Agents’ expose management data on the systems as ‘variables’.

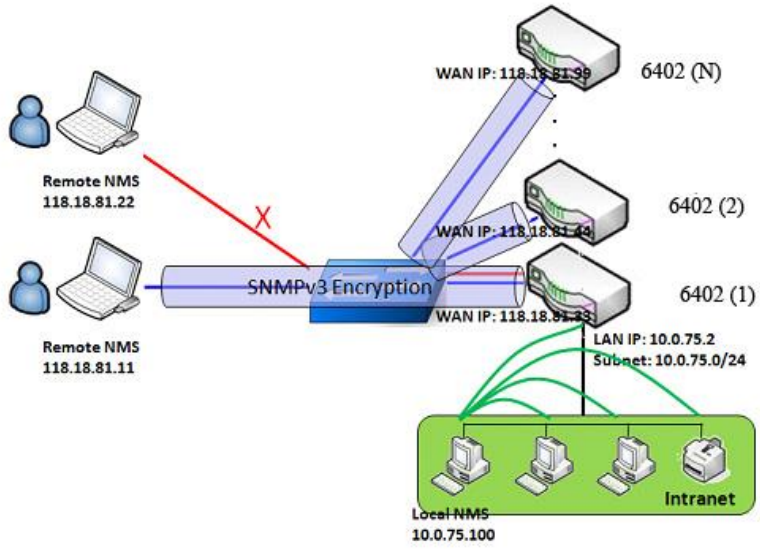
The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The 6402 supports several public MIBs and one private MIB for the SNMP agent.

Supported MIBs are as follows:

- MIB-II (RFC 1213, Include IPv6),
- IF-MIB, IP-MIB,
- TCP-MIB,
- UDP-MIB,
- SMIv1 and SMIv2,
- SNMPv2-TM and SNMPv2-MIB

8.1.3.1 SNMP Application Example



There are two application scenarios of SNMP Network Management Systems (NMS).
The Local NMS is on the local Subnet and manage all devices that support SNMP protocol in the subnet. Another scenario is a Remote NMS to manage devices via their WAN Interfaces using a switch or a router with UDP forwarding.
For an ISP managing a very large number of devices on the Internet, the TR-069 is a better solution.

8.1.3.2 SNMP Description

An NMS can monitor and configure managed devices by using the SNMP protocol, and any devices which use UDP packets to reach the NMS. Devices such as the 6402 which support SNMP can send urgent trap events to the NMS servers. For example, a cable being unplugged or link failing.
The SNMPv3 version of the SNMP protocol uses security to protect the transmitted SNMP commands and responses. An NMS with the correct level of privileged IP addresses can manage the devices, but other remote non-privileged NMS can't.

8.1.3.3 SNMP Setup Example

The following tables list the configuration of a6402 shown as numbered 1 in above diagram with "SNMP" enabled on the LAN and WAN interfaces.
Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[SNMP]-[Configuration]
SNMP Enable	■ *LAN*■ *WAN*
Supported Versions	■ *v1*■ *v2c*■ *v3*
Get / Set Community	*ReadCommunity / WriteCommunity*
Trap Event Receiver 1	*118.18.81.11*
WAN Access IP Address	*118.18.81.11*

Configuration Path	[SNMP]-[User Privacy Definition]		
ID	1	2	3
User Name	*UserName1*	*UserName2*	*UserName3*
Password	*Password1*	*Password2*	*Disable*
Authentication	*MD5*	*SHA-1*	*Disable*
Encryption	*DES*	*Disable*	*Disable*
Privacy Mode	*authPriv*	*authNoPriv*	*noAuthNoPriv*
Privacy Key	*12345678*	*Disable*	*Disable*
Authority	*Read/Write*	*Read*	*Read*
Enable	■ *Enable*	■ *Enable*	■ *Enable*

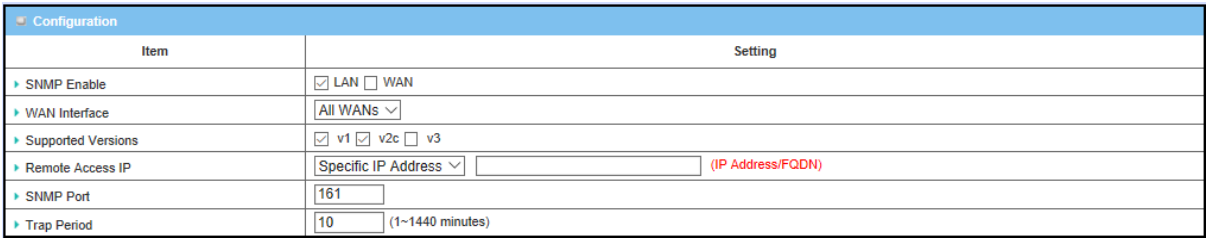
8.1.3.4 Scenario Operation Procedure

In above diagram, the NMS server can manage multiple devices on the subnet or devices available via the UDP-reachable network.
"6402 1" is one of the managed devices, and it has the IP address of 10.0.75.2 for its LAN interface and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.
Initially, the NMS manager prepares information for all the managed devices and records them in the NMS database system. Then the NMS checks and updates the status of all managed devices by using the SNMP get commands. Alternatively, many network managers prefer to connect using a Browser and configuring manually or uploading a configuration file.

8.1.3.5 SNMP Configuration Settings

SNMP allows users to configure SNMP relevant setting which includes interface, version, access control and trap receiver.

Go to Administration > Configure & Manage > SNMP tab.
Enable SNMP

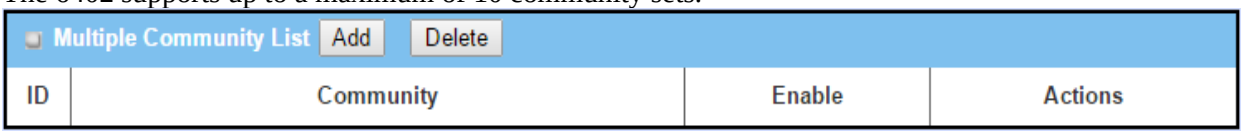


SNMP		
Item	**Value setting**	**Description**
SNMP Enable	1.The **LAN** box is checked by default	Select the interface for the SNMP and enable SNMP functions. When Check the **LAN** box. It will activate SNMP functions and you can access SNMP from LAN side. When Check the **WAN** box. It will activate SNMP functions and you can access SNMP from WAN side.
WAN Interface	Drop down list	Selects which WANs allow SNMP, optionally allow on all WANs.
Supported Versions	1.The **v1** box is checked by default 2.The **v2c** box is checked by default	Select the version for the SNMP When Check the **v1** box. It means you can access SNMP by version 1. When Check the **v2c** box. It means you can access SNMP by version 2c. When Check the **v3** box. It means you can access SNMP by version 3.
Remote Access IP	1. String format: any Ipv4 address 2. It is an optional item.	Specify the **Remote Access IP** for WAN. If you filled in the IP address. It means only this IP address can access SNMP from WAN side. If you not filled. It means any IP address can access SNMP from WAN side.

SNMP Port	1. String format: any port number 2. The default SNMP port is 161 3. A Mandatory setting	Specify the **SNMP Port**. You can fill in any port number. But you must ensure the port number is not to be used.
Trap Period	Numerical setting, 10 minutes by default	Sets the period between sending traps to the configured Trap Server.

8.1.3.6 Create/Edit Multiple Community

SNMP allows you to custom your access control for version 1 and version 2 user.
The 6402 supports up to a maximum of 10 community sets.

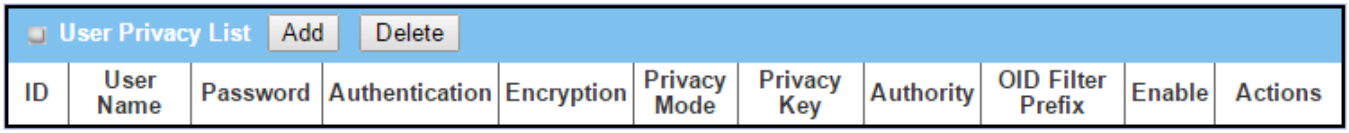


When the **Add** button is applied, **Multiple Community Rule Configuration** screen will appear.

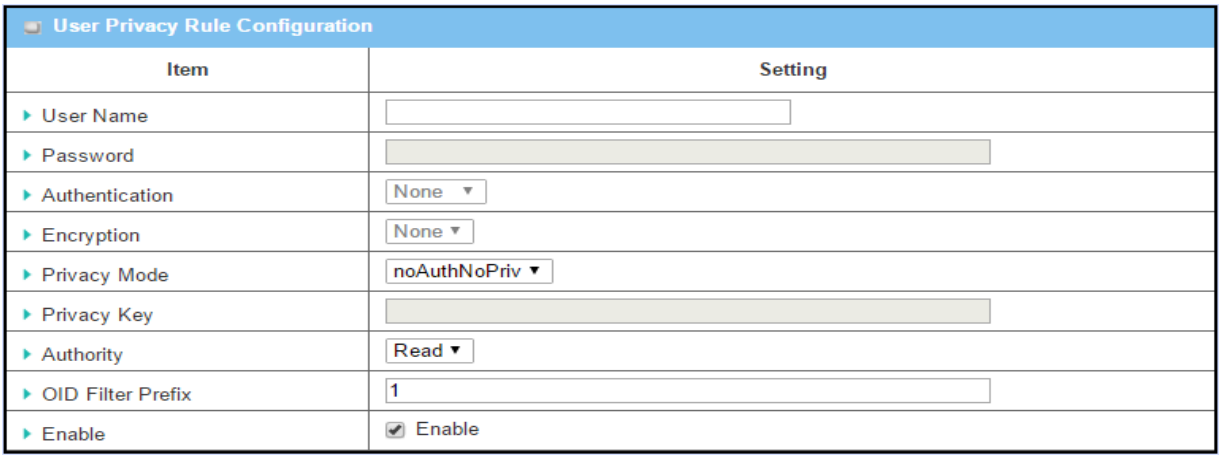
Multiple Community Rule Configuration		
Item	**Value setting**	**Description**
Community	1. Read Only is selected by default 2. A Mandatory setting 3. String format: any text	Specify this version 1 or version v2c user's community that will be allowed Read Only (GET and GETNEXT) or Read-Write (GET, GETNEXT and SET) access respectively. The maximum length of the community is 32.
Enable	1.The box is checked by default	Click the **Enable** button to enable this version 1 or version v2c user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click the **Undo** button to cancel the settings.
Back	N/A	Click the **Back** button to return to last page.

8.1.3.7 Create/Edit User Privacy

SNMP allows you to custom your access control for version 3 user. The router supports up to a maximum of 128 User Privacy sets.



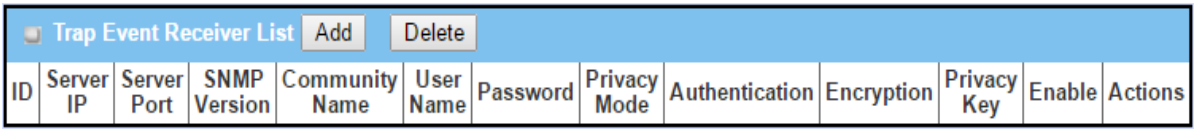
When **Add** button is applied, **User Privacy Rule Configuration** screen will appear.



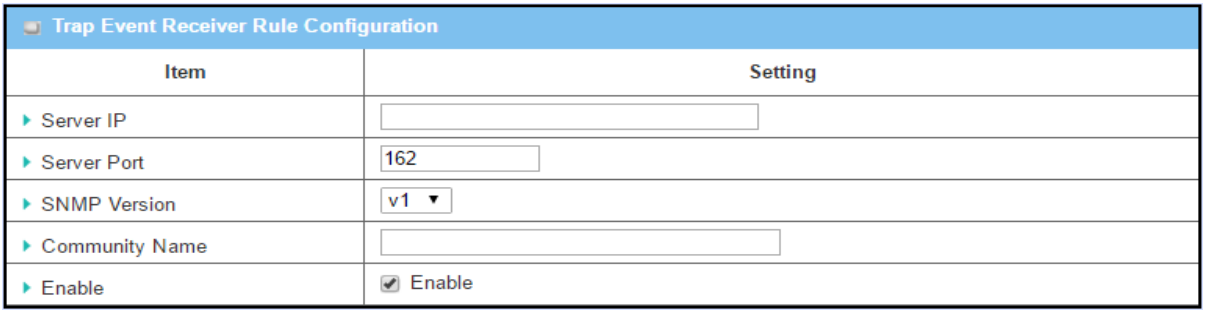
User Privacy Rule Configuration		
Item	**Value setting**	**Description**
User Name	1. A Mandatory Setting 2. String format: any text	Specify the **User Name** for this version 3 user. The maximum length of the user name is 32.
Password	1. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 user. The minimum length of the password is 8. The maximum length of the password is 64.
Authentication	1. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 user. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 user. Selected the encryption protocols **DES / AES** to use.
Privacy Mode	1. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 user. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Privacy Key	1. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** for this version 3 user. The minimum length of the privacy key is 8. The maximum length of the privacy key is 64.
Authority	1. **Read** is selected by default	Specify this version 3 user's **Authority** that will be allowed **Read Only** (GET and GETNEXT) or **Read-Write** (GET, GETNEXT and SET) access respectively.
OID Filter Prefix	1. The default value is 1 2. A Mandatory Setting 3. String format: any legal OID	The **OID Filter Prefix** restricts access for this version 3 user to the sub-tree rooted at the given OID. The range of the each OID number is 1-2080768.
Enable	1.The box is checked by default	Click **Enable** to enable this version 3 user.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show "Click on save button to apply your changes" remind user to click main page **Save** button.
Undo	N/A	Click **Undo** to cancel the settings
Back	N/A	Click the **Back** button to return the last page.

8.1.3.8 Create/Edit Trap Event Receiver

SNMP allows you to custom your trap event receiver. The 6402 supports up to a maximum of 4 Trap Event Receiver sets.

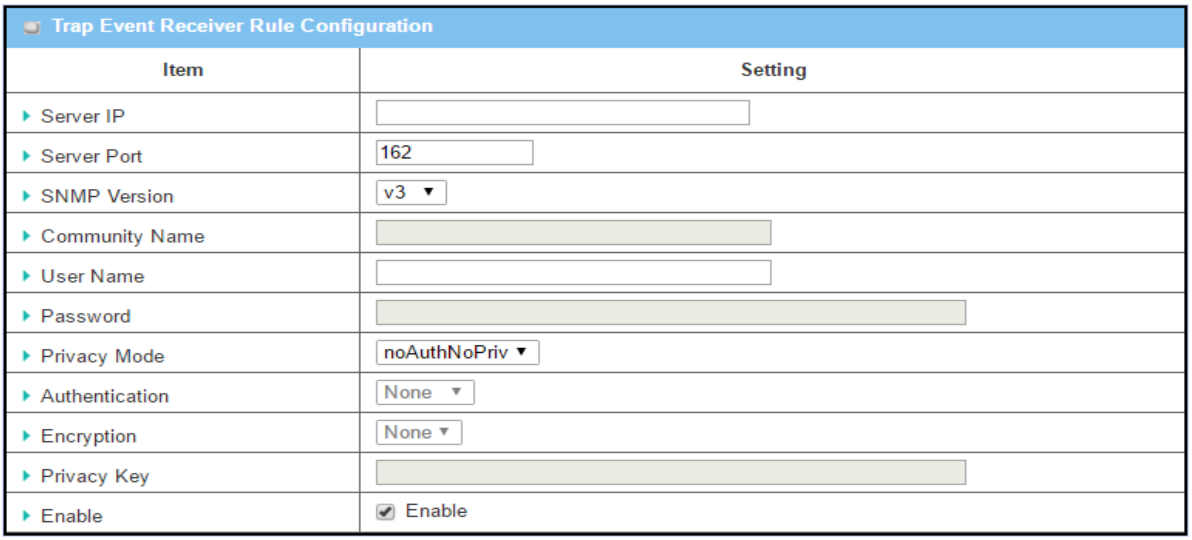


When the **Add** button is applied, the **Trap Event Receiver Rule Configuration** screen will appear. The default SNMP Version is v1. The configuration screen will display version 1 with mandatory items already filled in as shown below.



When you select v2c, the configuration screen is exactly the same as that of v1, except the version.

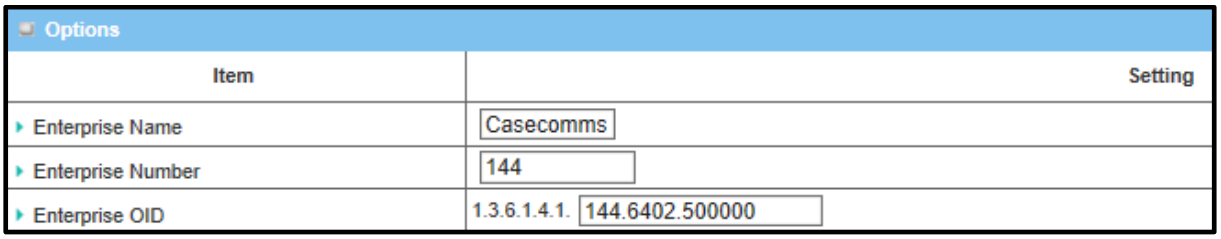
When you select v3, the configuration screen will provide more setting items for the version 3 Trap.



Trap Event Receiver Rule Configuration		
Item	**Value setting**	**Description**
Server IP	1. A Mandatory Setting 2. String format: any Ipv4 address	Specify the trap **Server IP**. The DUT will send trap to the server IP.
Server Port	1. String format: any port number 2. The default SNMP trap port is 162 3. A Mandatory setting	Specify the trap **Server Port**. You can fill in any port number. But you must ensure the port number is not to be used.
SNMP Version	1. **v1** is selected by default	Select the version for the trap Selected the **v1**. - The configuration screen will provide the version 1 mandatory items. Selected the **v2c**. - The configuration screen will provide the version 2c mandatory items. Selected the **v3**. - The configuration screen will provide the version 3 mandatory items.
Community Name	1. A **v1** and **v2c** A Mandatory Setting 2. String format: any text	Specify the **Community Name** for this version 1 or version v2c trap. The maximum length of the community name is 32.
User Name	1. A **v3** A Mandatory Setting 2. String format: any text	Specify the **User Name** for this version 3 trap. The maximum length of the user name is 32.
Password	1. A **v3** A Mandatory Setting 2. String format: any text	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Password** for this version 3 trap. The minimum length of the password is 8. The maximum length of the password is 64.
Privacy Mode	1. A **v3** A Mandatory Setting 2. **noAuthNoPriv** is selected by default	Specify the **Privacy Mode** for this version 3 trap. Selected the **noAuthNoPriv**. You do not use any authentication types and encryption protocols. Selected the **authNoPriv**. You must specify the **Authentication** and **Password**. Selected the **authPriv**. You must specify the Authentication, Password, Encryption and Privacy Key.
Authentication	1. A **v3** A Mandatory Setting 2. **None** is selected by default	When your **Privacy Mode** is **authNoPriv** or **authPriv**, you must specify the **Authentication** types for this version 3 trap. Selected the authentication types **MD5/ SHA-1** to use.
Encryption	1. A **v3** A Mandatory Setting 2. **None** is selected by default	When your **Privacy Mode** is **authPriv**, you must specify the **Encryption** protocols for this version 3 trap. Selected the encryption protocols **DES / AES** to use.
Privacy Key	1. A **v3** A Mandatory Setting 2. String format: any text	When your **Privacy Mode** is **authPriv**, you must specify the **Privacy Key** for this version 3 trap. The minimum length of the privacy key is 8. The maximum length of the privacy key is 64.
Enable	1.The box is checked by default	Click **Enable** to enable this trap receiver.
Save	N/A	Click the **Save** button to save the configuration. But it does not apply to SNMP functions. When you return to the SNMP main page. It will show “Click on save button to apply your changes” remind user to click main page **Save** button.
Undo	N/A	Click **Undo** to cancel the settings.
Back	N/A	Click the **Back** button to return the last page.

8.1.3.9 Edit SNMP Options

If you use some particular private MIB, you must fill the enterprise name, number and OID.



Options		
Item	**Value setting**	**Description**
Enterprise Name	2. A Must filled setting 3. String format: any text	Specify the Enterprise Name for the particular private MIB. The maximum length of the enterprise name is 10.
Enterprise Number	The default value is Case Object ID 2. Mandatory setting 3. String format: any number	Specify the Enterprise Number for the particular private MIB. The range of the enterprise number is 1-2080768.
Enterprise OID	1. The default value is Cases Object ID 2. A Mandatory Setting 3. String format: any legal OID	Specify the EnterpriseOID for the particular private MIB. The range of the each OID number is 1-2080768. The maximum length of the enterpriseOID is 31. The seventh number must be identical with the enterprise number.
Save	N/A	Click the Save button to save the configuration and apply your changes to SNMP functions.
Undo	N/A	Click Undo to cancel the settings.

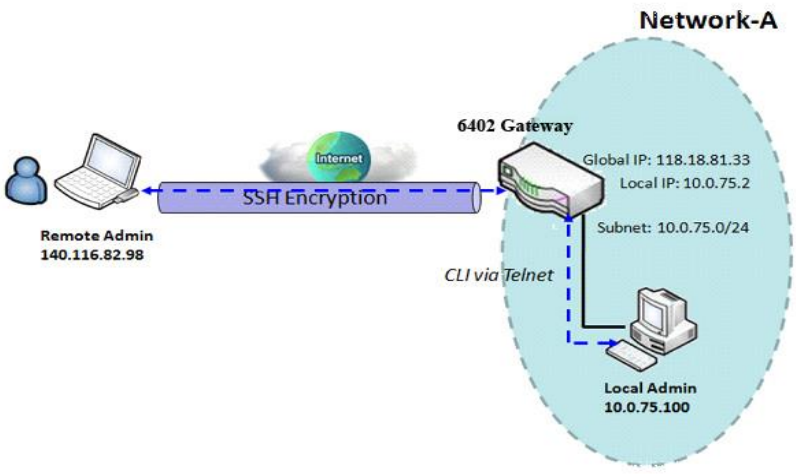
8.1.4. Telnet and SSH

A command-line interface (CLI), also known as ‘command-line interface’, and console user interface s a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines).

The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions.

Programs with command-line interfaces are generally easier to automate via scripting. The 6402 supports both Telnet and SSH (Secure Shell) CLI with default service port 23 and 22, respectively.

8.1.4.1 Telnet & SSH Scenario



8.1.4.2 Example explanation

The Local Administrator or Remote Administrator can manage the 6402 by using "Telnet" or "SSH" utility with a privileged user name and password.
The data packets between the Local or Remote Administrator and the 6402 can be plain text or encrypted text. Typically, we would use plain text (Telnet) for the local admin manager coming in from the subnet and encrypted text (Using SSH) for an admin manager accessing via the Internet.

8.1.4.3 Telnet /SSH Configuration Example

The table below lists the configuration for the6402's in the example diagram above with "Telnet with CLI" enabled at LAN and WAN interfaces. Use the default value for those parameters that are not mentioned in the table.

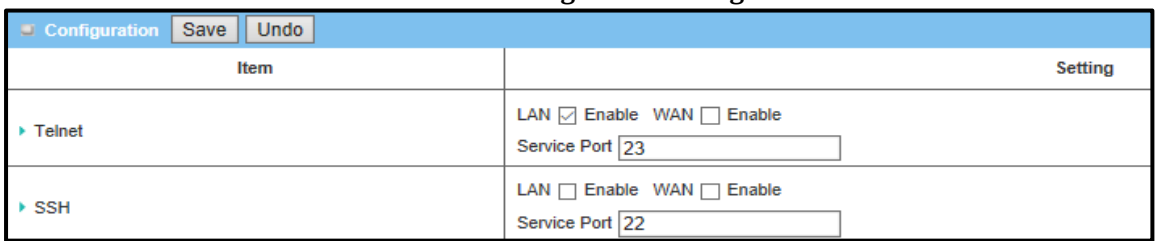
Configuration Path	[Telnet with CLI]-[Configuration]
Telnet with CLI	LAN: ■ *Enable*WAN:■ *Enable*
Connection Type	Telnet: Service Port *23* ■ *Enable* SSH: Service Port *22* ■ *Enable*

8.1.4.4 Telnet / SSH Scenario Operation

In diagram 8.1.4.1, "Local Admin" or "Remote Admin" can manage the "6402" via the subnet or Internet. The "6402" is the 6402 on Network-A, has a subnet IP Address of 10.0.75.0/24, its IP address is 10.0.75.2 for its LAN interface, and 118.18.81.33 for WAN-1 interface. It serves as a NAT router.
The "Local Admin" on the Subnet uses "Telnet" with a privileged account to log into the 6402.
Or the "Remote Admin" on the Internet uses the "SSH" utility with a privileged account to login the 6402. The administrator of the 6402 can control the router as though they were physically attached to the router.

8.1.4.5 Telnet and SSH Setting

The Telnet with CLI setting allows administrator to access this device through the traditional Telnet program. Before you can telnet (login) to the device, please configure the related settings and password with care. The password management part allows you to set root password for logging telnet and SSH. Go to **Administration > Configure & Manage > Telnet & SSH** tab

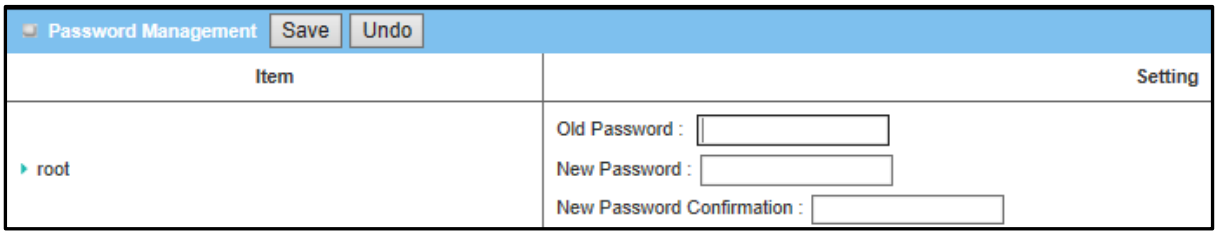


Configuration		
Item	**Value setting**	**Description**
Telnet	The LAN Enable box is checked by default. The WAN Enable box is unchecked by default.	Check the **Enable** box to activate the Telnet with CLI function for connecting from WAN/LAN interfaces.
Service Port	By default, **Telnet Service Port** is 23	Configures the required Telnet TCP port number.
SSH	The LAN Enable box is unchecked by default. The WAN Enable box is unchecked by default.	Check the **Enable** box to activate the SSH with CLI function for connecting from WAN/LAN interfaces.
Service Port	By default, **SSH Service Port** is 22.	Configures the required SSH TCP port number.
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

8.1.4.6 Password Management

This configures the password used for Telnet and SSH access to the 6402's CLI.

The Username is always **root** and the default password is **case**



Configuration		
Item	**Value setting**	**Description**
root	1. String: any text but no blank character 2. The default password for telnet is 'case'.	Type old password and specify new password to change root password. ***Note: You are highly recommended to change the default telnet password with yours before the device is deployed.***
Save	N/A	Click **Save** to save the settings
Undo	N/A	Click **Undo** to cancel the settings

Note: Access via Telnet, SSH or even the 6402's Console port will give access to the 6402's Linux operating system. So ensure that care is taken when access is granted.

8.2. System Operation

The System Operation section allows the network administrator to manage the 6402 system, settings such as web-based utility access password change, system information, system time, system log, firmware/configuration backup & restore, and reset & reboot.

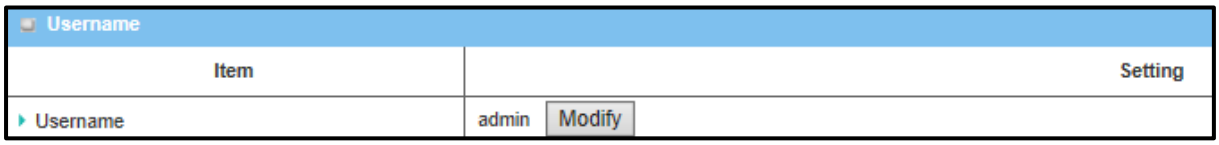
8.2.1. Password & MMI

Go to Administration > System Operation > Password & MMI tab.

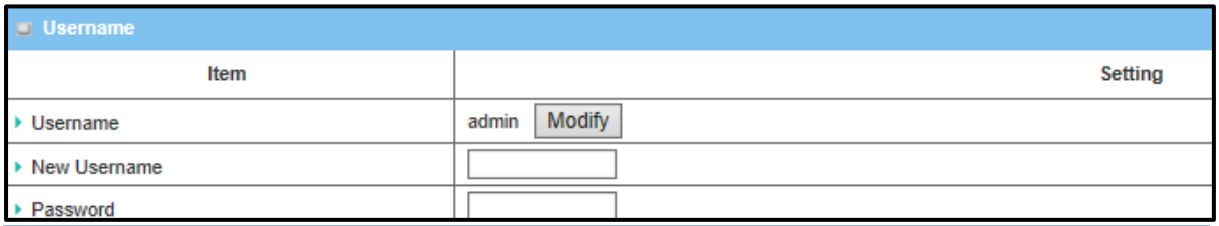
8.2.1.1 Host Name

Enter the host name for the gateway. This can be used to interact with external network servers for identifying the name of requesting device.

8.2.1.2 Username



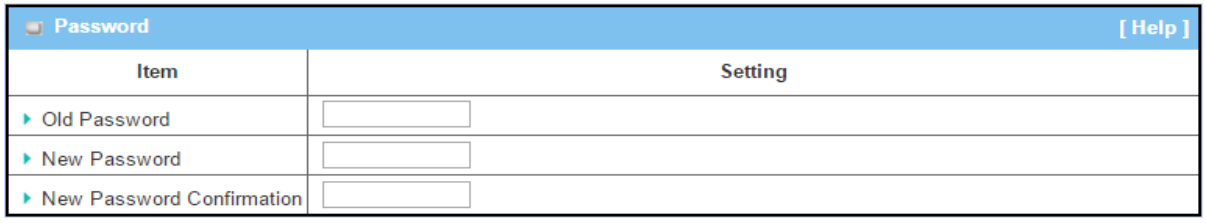
Allows configuration of the username used to access management of the 6402 through a web browser.



Username		
Item	**Value Setting**	**Description**
Username	Current set Username	Click Modify button to access the change.
New Username	String: any text	Enter new Username.
Password	String: any text	Enter current Password.

8.2.1.3 Change Password

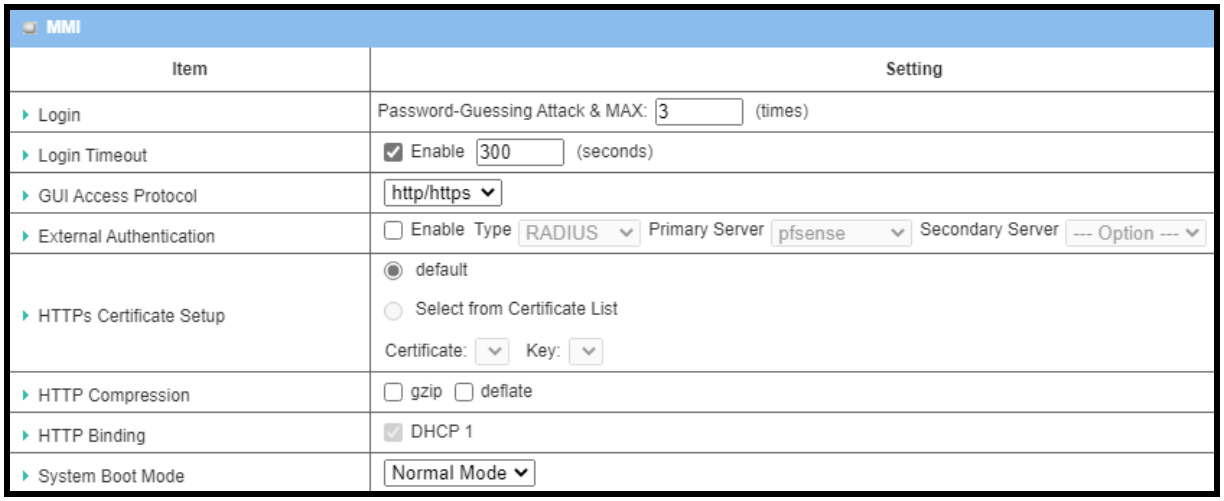
Change password screen allows network administrator to change the web-based MMI login password to access gateway.



Change Password		
Item	**Value Setting**	**Description**
Old Password	1. String: any text 2. The default password for web-based MMI is ‘admin’.	Enter the current password to enable you unlock to change password.
New Password	String: any text	Enter new password.
New Password Confirmation	String: any text	Enter new password again to confirm.

8.2.1.4 Change MMI Setting for Accessing

This is the 6402's web-based MMI which allows the administrator to access the 6402 management. The 6402 web-based MMI will automatically logout when the idle time has elapsed. This setting allows the 6402 administrator to enable automatic logout and set the logout idle time. If the login timeout is disabled, the system won't logout the administrator automatically.



Web UI		
Item	**Value Setting**	**Description**
Login	3 times is set by default	Enter the login trial counting value. If someone tried to login the web GUI with incorrect password for more than the counting value, a warning message "***Already reaching maximum Password-Guessing times, please wait a few seconds!***" will be displayed and ignore the following login trials.
Login Timeout	The Enable box is unchecked by default	Check the Enable box to activate the auto logout function and specify the maximum idle time as well.
GUI Access Protocol	http/https is selected by default.	Select the protocol that will be used for GUI access. It can be **http/https**, **http only**, or **https only**.
External Authentication	The Enable box is unchecked by default. Server selection will only show suitable servers that have already been configured.	Allows selection of the remote RADIUS or TACACS+ Servers that authorizes management access. When Enabled: Type: RADIUS or TACACS+ Primary Server: Selects the previously configured External Server that will act as the primary authentication service. Secondary Server: Selects the Secondary server in the event of the Primary being unavailable.
HTTPs Certificate Setup	Default selected	Allows selection of the certificate used for secure access to management of the 6402 through a browser.
HTTP Compression	gzip or deflateboth disabled by default	Selects the required content encoding algorithm. This compresses content like XHTML, CCS and other text files.
HTTP Binding	DHCP 1 selected by default	Sets automatic HTTP bindings using DHCP.
System Boot Mode	Normal Mode by default	Selects how the 6402 will boot for power up or reboot. **Normal Mode** allows the 6402 to go through its normal power up sequence including some power up testing. **Fast Mode** cuts down on the power up sequence time. **Quick Mode** cuts down the power up sequence even further.
Save	N/A	Click **Save** button to save the settings
Undo	N/A	Click **Undo** button to cancel the settings

8.2.2. System Information

System Information screen gives network administrator a quick look up on the firmware and kernel versions along with the current System time and Up-Time.

Go to Administration> System Operation> System Information tab.

System Information	
Item	
Model Name	6402
Device Serial Number	QCD-846652
Kernel Version	2.6.36
FW Version	0CBQO0.151_e52.0CB0_0905`1700
CPU Usage	6.86%
Memory Usage	63%
System Time	Tue, 18 Dec 2018 13:44:18 + 0000
Device Up-Time	0 day, 5hr, 12 min 53 sec

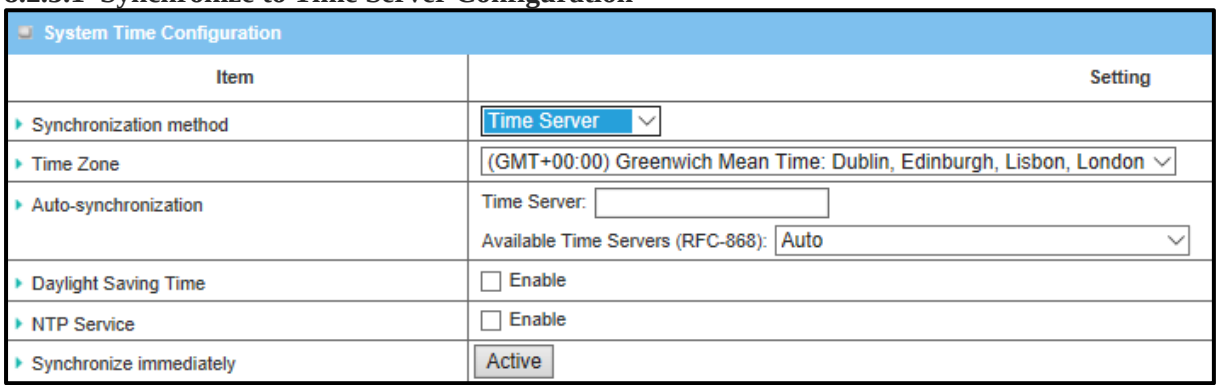
8.2.3. System Time

The 6402 provides manual and auto-synchronized methods for the administrator to setup the system time for the 6402

Go to Administration> System Operation> System Time tab.

This allows selection and configuration of how the router sets and corrects its internal time setting. There are a few different ways to configure the System Time.

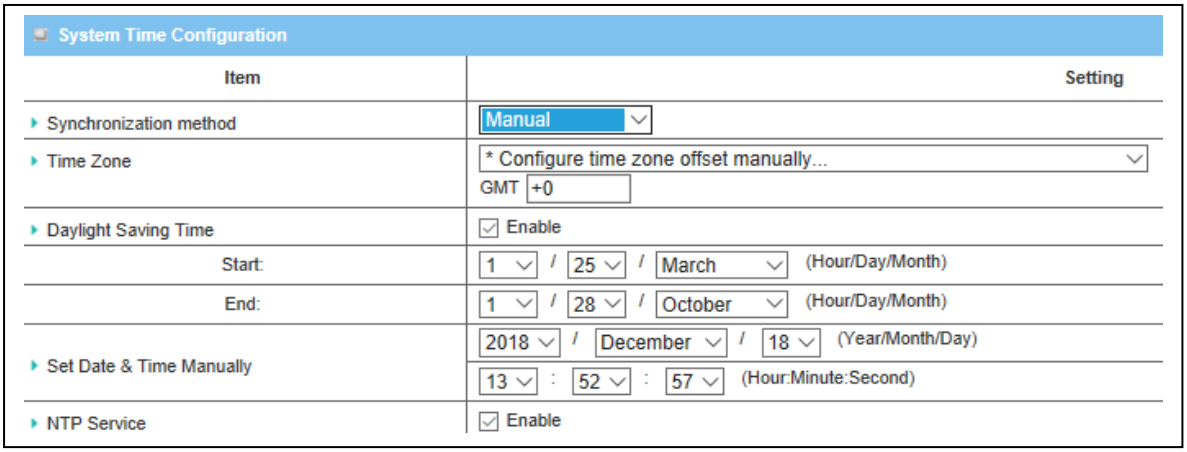
8.2.3.1 Synchronize to Time Server Configuration



System Time – Time Server		
Item	**Value Setting**	**Description**
Synchronization Method	Time Server by default	**Time Server –** the 6402 connects to the set server for correct time information.
Time Zone	1. It is an optional item. 2. Not yet configured is selected by default.	Select a time zone where this device locates.
Auto-synchronization	1. Checked by default. 2. Auto is selected by default.	Check the **Enable** button to activate the time auto-synchronization function with a certain NTP server. You can enter the IP or FQDN for the NTP server you expected or leave it as auto mode so that the available server will be used for time synchronization one by one.
Daylight Saving Time	1. It is an optional item. 2. Unchecked by default	Check the **Enable** button to activate the daylight saving function. When you enabled this function, you have to specify the start date and end date for the daylight saving time duration.

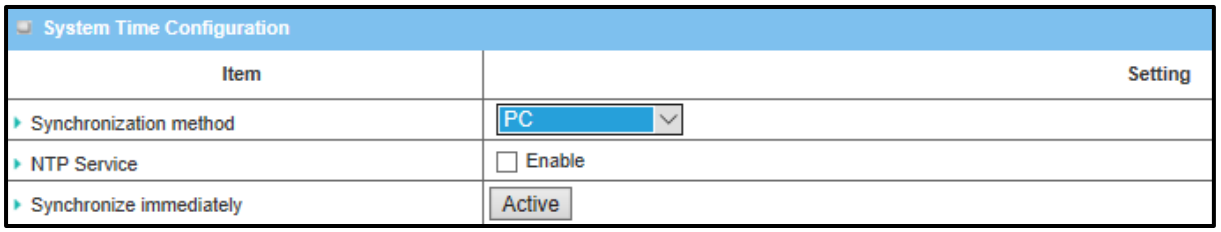
NTP Service	Checked by default	When checked the router can acts as an NTP server for local equipment.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system time immediately.

8.2.3.2 Manual Time Configuration



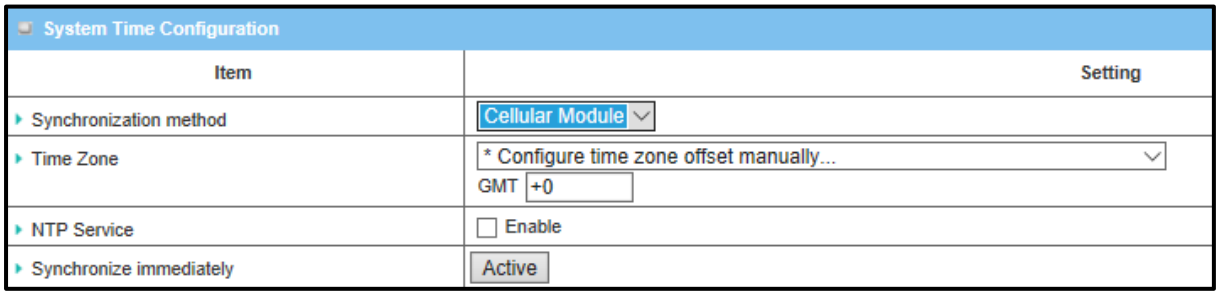
System Time – Manual		
Item	**Value Setting**	**Description**
Synchronization Method	Time Server by default	**Manual –** the use can set the time in the GUI. **PC–** the 6402 collects the time from the logged in computer. **Cellular Module–** the 6402 collects the time from the 3G network.
Time Zone	Mandatory setting.	Select a time zone where this device located. Optionally set it manually
GMT	Set to +0 by default	Set the time zone manually
Daylight Saving Time	1. It is an optional item. 2. Unchecked by default	Check the **Enable** button to activate the daylight-saving function. When you enabled this function, you must specify the start date and end date for the daylight-saving time duration.
Set Date & Time Manually	1.Optional item.	If you do not enable the time auto-synchronization function, you can also manually set the date (Year/Month/Day(and time (Hour:Minute:Second).
NTP Service	Checked by default	When checked the router can acts as an NTP server for local equipment.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system time immediately.

8.2.3.3 Synchronize to PC Configuration



System Time – Manual		
Item	**Value Setting**	**Description**
Synchronization Method	Time Server by default	**PC**– the 6402 collects the time from the logged in computer.
NTP Service	Checked by default	When checked the router can acts as an NTP server for local equipment.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system time immediately.

8.2.3.4 Synchronize to Cellular Module Configuration

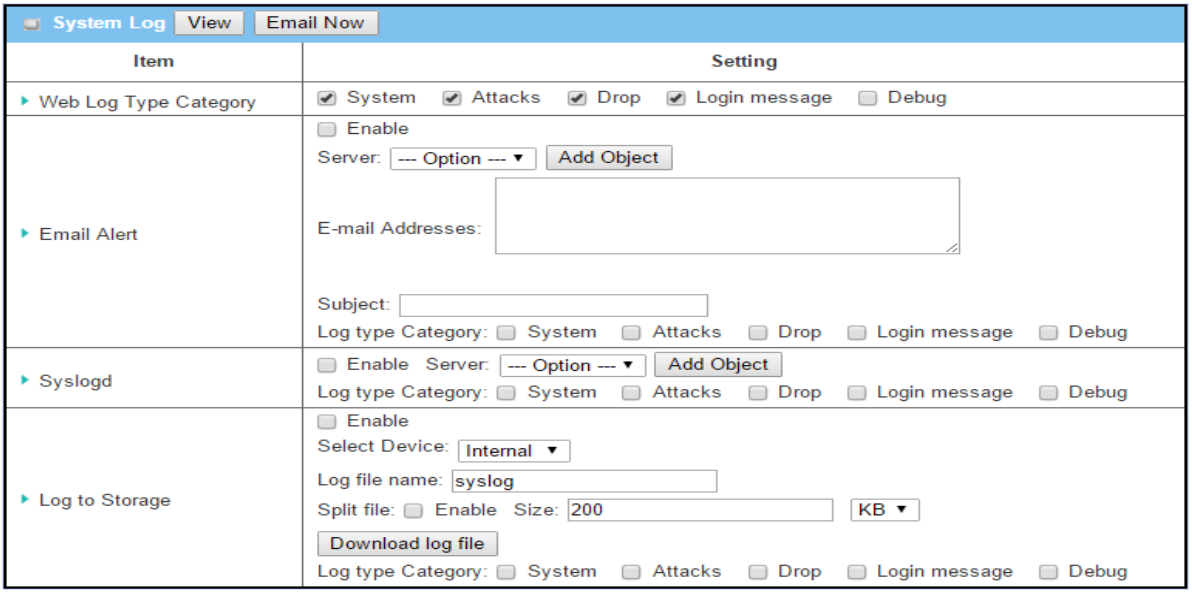


System Time – Manual		
Item	**Value Setting**	**Description**
Synchronization Method	Time Server by default	**Cellular Module**– the 6402 collects the time from the 3G network.
Time Zone	Mandatory setting.	Select a time zone where this device located. Optionally set it manually
GMT	Set to +0 by default	Set the time zone manually
NTP Service	Checked by default	When checked the router can acts as an NTP server for local equipment.
Save	N/A	Click **Save** button to save the settings.
Refresh	N/A	Click **Refresh** button to update the system time immediately.

8.2.4. System Log

The System Log screen contains various event log tools, allowing the network administrator to perform local event logging and remote reporting.

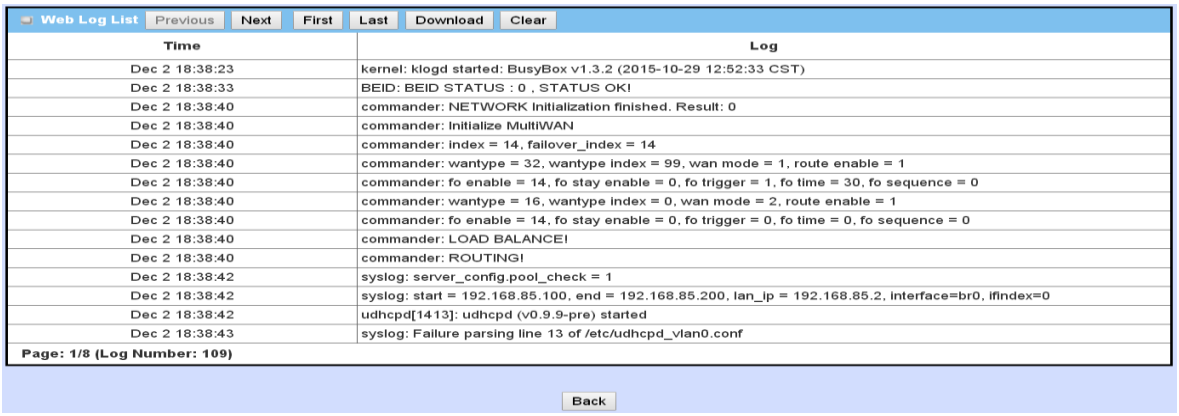
Go to Administration> System Operation> System Log tab.



8.2.4.1. View & Email Log History

View button is provided for network administrator to view log history on the gateway. **Email Now** button enables administrator to send instant Email for analysis.

View & Email Log History		
Item	**Value setting**	**Description**
View button	N/A	Click the **View** button to view Log History in Web Log List Window.
Email Now button	N/A	Click the **Email Now** button to send Log History via Email instantly.

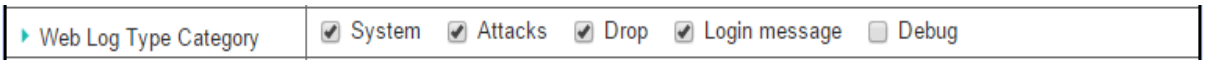


Web Log List Window		
Item	**Value Setting**	**Description**
Time column	N/A	It displays event time stamps
Log column	N/A	It displays Log messages

Web Log List Button Description		
Item	**Value setting**	**Description**
Previous	N/A	Click the **Previous** button to move to the previous page.
Next	N/A	Click the **Next** button to move to the next page.
First	N/A	Click the **First** button to jump to the first page.
Last	N/A	Click the **Last** button to jump to the last page.
Download	N/A	Click the **Download** button to download log to your PC in tar file format.
Clear	N/A	Click the **Clear** button to clear all log.
Back	N/A	Click **Back** button to return to the previous page.

8.2.4.2. Web Log Type Category

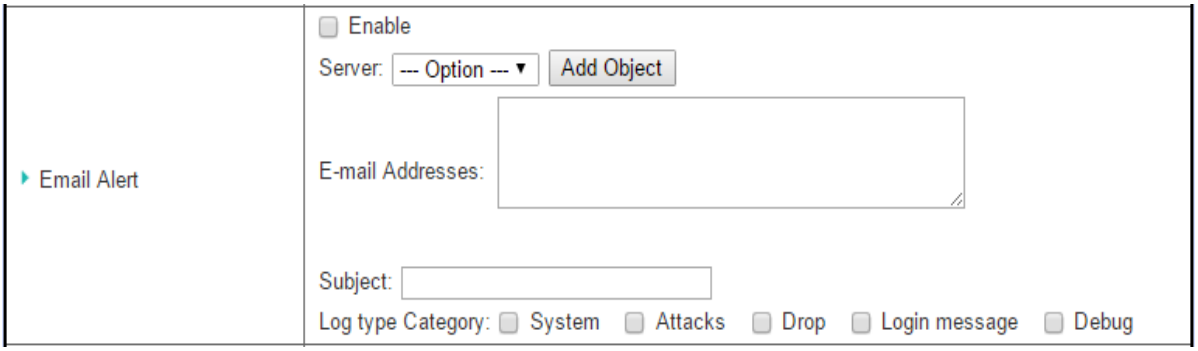
The Web Log Type Category screen allows network administrator to select the type of events to log and be displayed in the Web Log List Window as described in the previous section. Click on the View button to view Log History in the Web Log List window.



Web Log Type Category Setting Window		
Item	**Value Setting**	**Description**
System	Checked by default	Check to log system events and to display in the Web Log List window.
Attacks	Checked by default	Check to log attack events and to display in the Web Log List window.
Drop	Checked by default	Check to log packet drop events and to display in the Web Log List window.
Login message	Checked by default	Check to log system login events and to display in the Web Log List window.
Debug	Unchecked by default	Check to log debug events and to display in the Web Log List window.

8.2.4.3. Email Alert

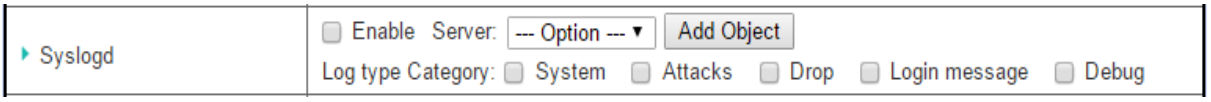
The Email Alert screen allows network administrator to select the type of event to log and be sent to the destined Email account.



Email Alert Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check **Enable** box to enable sending event log messages to destined Email account defined in the E-mail Addresses blank space.
Server	N/A	Select one email server from the Server dropdown box to send Email. If none has been available, click the **Add Object** button to create an outgoing Email server. You may also add an outgoing Email server from Object Definition > External Server > External Server tab.
E-mail address	String: email format	Enter the recipient's Email address. Separate Email addresses with comma ',' or semicolon ' ;' Enter the Email address in the format of '*myemail@domain.com*'
Subject	String: any text	Enter an Email subject that is easy for you to identify on the Email client.
Log type category	Default unchecked	Select the type of events to log and be sent to the designated Email account. Available events are System, Attacks, Drop, Login message, and Debug.

8.2.4.4. Syslogd

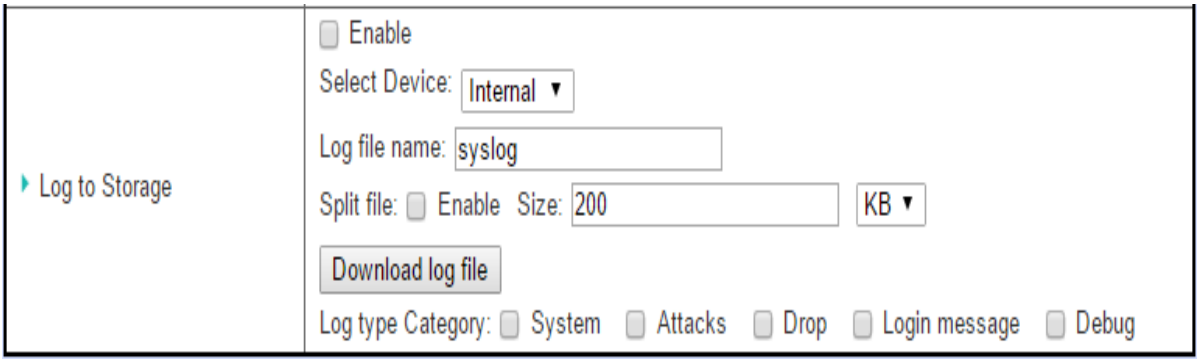
The Syslogd screen allows network administrator to select the type of event to log and be sent to the designated Syslog server.



Syslogd Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check Enable box to activate the Syslogd function, and send event logs to a syslog server
Server	N/A	Select one syslog server from the Server dropdown box to send event log to. If none has been available, click the **Add Object** button to create a system log server. You may also add a system log server from the Object Definition > External Server > External Server tab.
Log type category	Unchecked by default	Select the type of event to log and be sent to the destined syslog server. Available events are System, Attacks, Drop, Login message, and Debug.

8.2.4.5. Log to Storage

The Log to Storage screen allows network administrator to select the type of events to log and be stored at an internal or an external storage.



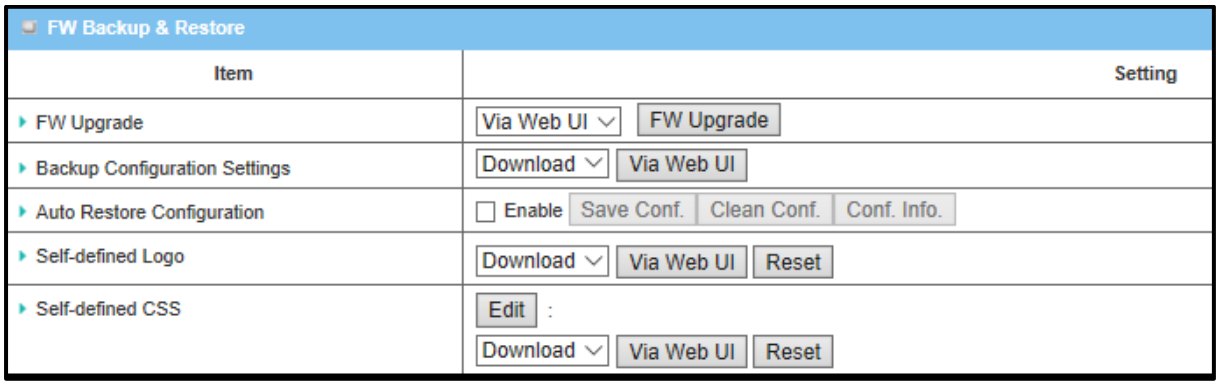
Log to Storage Setting Window		
Item	**Value Setting**	**Description**
Enable	Unchecked by default	Check to enable sending log to storage.
Select Device	Internal is selected by default	Select internal or external storage.
Log file name	Unchecked by default	Enter log file name to save logs in designated storage.
Split file Enable	Unchecked by default	Check **enable** box to split file whenever log file reaching the specified limit.
Split file Size	200 KB is set by default	Enter the file size limit for each split log file.
Log type category	Unchecked by default	Check which type of logs to send: System, Attacks, Drop, Login message, Debug

Log to Storage Button Description		
Item	**Value setting**	**Description**
Download log file	N/A	Click the **Download log file** button to download log files to a log.tar file.

8.2.5. Backup & Restore

In the Backup & Restore window, you can upgrade the device firmware when new firmware is available, and also backup / restore the device configuration.
In addition to the factory default settings, you can also customize a special configuration setting as a customized default value. With this customized default value, you can reset the device to the expected default setting if needed.

Go to Administration > System Operation > Backup & Restore tab.

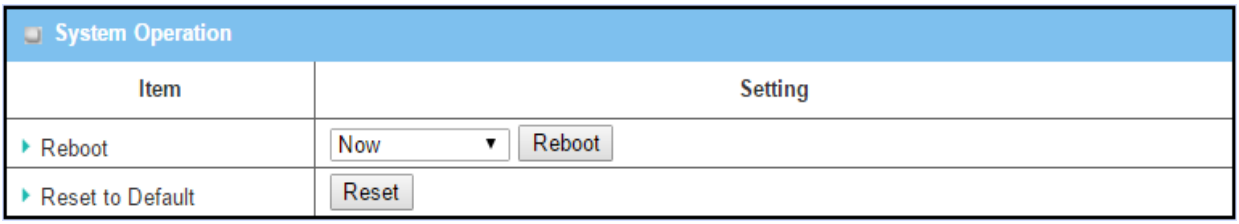


Log to Storage Setting Window		
Item	**Value Setting**	**Description**
FW Upgrade	Via Web UI is selected by default	If new firmware is available, click the **FW Upgrade** button to upgrade the device firmware **via Web UI**, or **Via Storage**. After clicking on the "FW Upgrade" command button, you need to specify the file name of new firmware by using "Browse" button, and then click "Upgrade" button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check "Accept unofficial firmware"
Backup Configuration Settings	Download is selected by default	You can backup or restore the device configuration settings by clicking the ***Via Web UI*** button. **Download**: for backup the device configuration to a config.bin file. **Upload**: for restore a designated configuration file to the device. **Via Web UI**: to retrieve the configuration file via Web GUI.
Auto Restore Configuration	The Enable box is unchecked by default	Chick the **Enable** button to activate the customized default setting function. Once the function is activated, you can save the expected setting as a customized default setting by clicking the **Save Conf** button or clicking the **Clean Conf.** button to erase the stored customized configuration.
Self-defined Logo	Download is selected by default	This allows changing the logo used on the GUI.
Self-defined CSS	Download is selected by default	This allows changing the look of the GUI, e.g. colours used.

8.2.6. Reboot & Reset

For some special situations, you may need to reboot the 6402 or reset the device 6402 to its default settings. This can be achieved using the Power ON/OFF, or pressing the reset button on the 6402 panel, but it can also be done through the web GUI.
In the Reboot & Reset window, you can reboot the 6402 by clicking the "Reboot" button and reset this device to default settings by clicking the "Reset" button.

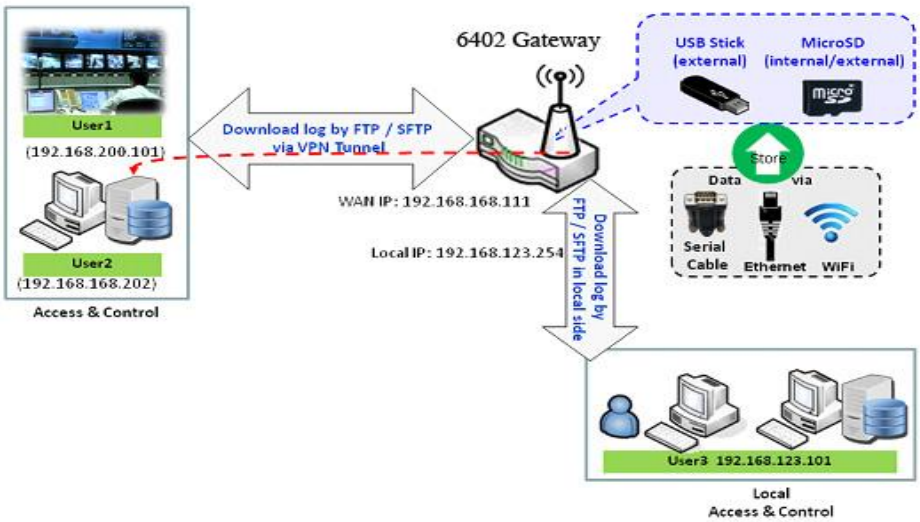
Go to Administration > System Operation > Reboot & Reset tab.



System Operation Window		
Item	**Value Setting**	**Description**
Reboot	Now is selected by default	Chick the **Reboot** button to reboot the gateway immediately or on a pre-defined time schedule. **Now**: Reboot immediately **Time Schedule**: Select a pre-defined auto-reboot time schedule rule to reboot the auto device on a designated time. To define a time schedule rule, go to **Object Definition > Scheduling > Configuration** tab.
Reset to Default	N/A	Click the **Reset** button to reset the device configuration to its default value.

8.3. FTP

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files between a client and server on a computer network. FTP is built on a client-server model and uses separate control and data connections between the client and the server.
FTP users may authenticate themselves with a clear-text sign-in protocol, normally in the form of a username and password, but can connect anonymously if the server is configured to allow it.
For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS). Besides, SSH File Transfer Protocol (SFTP) is sometimes also used instead but is technologically different.
The 6402 has an embedded FTP / SFTP server for the network administrator to download the log files to their computer or database.
In the following two sections, you can configure the FTP server and create the user accounts to allow users to login to the server. After login in to the FTP server, you can browse the log directory and have permission to download, stored log files and delete the files you have downloaded to make more storage space for further data logs.
The available log files can be system logs (refer to Administration > System Operation > System Log), Network Packets (refer to Administrator > Diagnostic > Packet Analyser), Data Log (refer to Field Communication > Data Logging > Log File Management), and GNSS Log (refer to Service > Location Tracking > GNSS). With proper configuration for the various log functions that supported on your purchased product, you can download the log via FTP / SFTP connections.

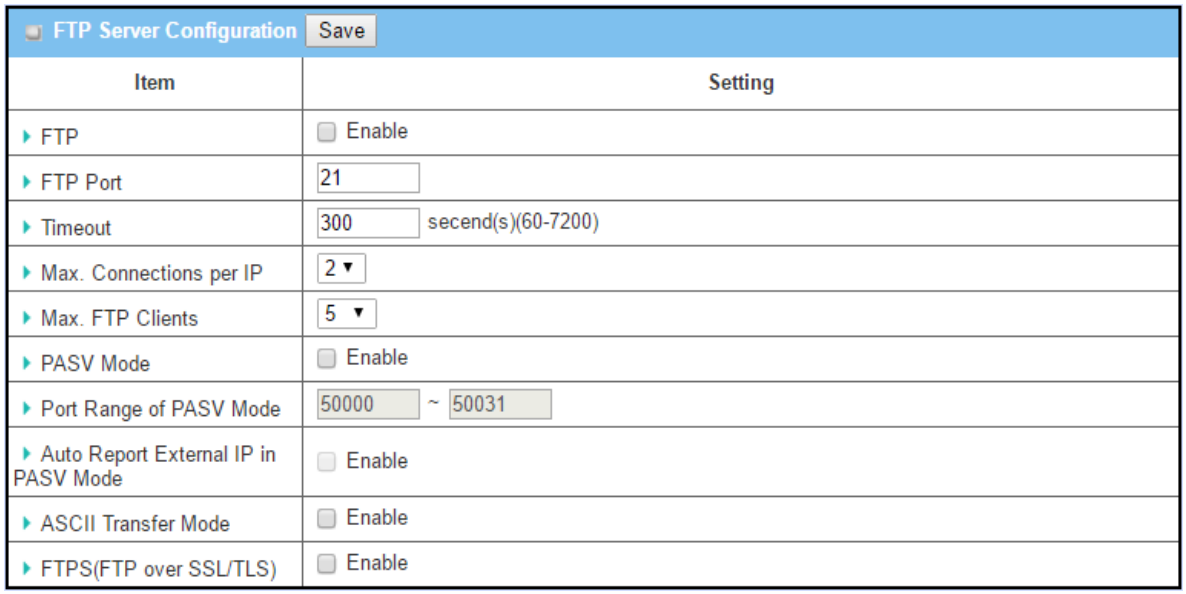


8.3.1. Server Configuration

This section allows user to setup the embedded FTP and SFTP server for retrieving the interested fog files.

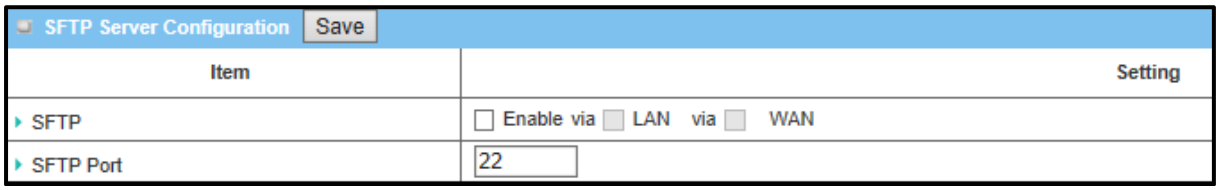
Go to Administration > FTP > Server Configuration tab.

Enable FTP Server



Configuration		
Item	**Value setting**	**Description**
FTP	The box is unchecked by default.	Check Enable box to activate the embedded FTP Server function. With the FTP Server enabled, you can retrieve or delete the stored log files via FTP connection. **Note**: The embedded FTP Server is only for log downloading, so write permission is not implemented for user file upload to the storage.
FTP Port	Port 21 is set by default	Specify a port number for FTP connection. The gateway will listen for incoming FTP connections on the specified port.
Timeout	300 seconds is set by default.	Specify the maximum timeout interval for the FTP connection. Supported range is 60 to 7200 seconds.
Max. Connections per IP	2 Clients are set by default.	Specify the maximum number of clients from the same IP address for the FTP connection. Up to 5 clients from the same IP address is supported.
Max. FTP Clients	5 Clients are set by default.	Specify the maximum number of clients for the FTP connection. Up to 32 clients is supported.
PASV Mode	Optional setting	Check the Enable box to activate the support of PASV mode for an FTP connection from FTP clients.
Port Range of PASV Mode	Port 50000 ~ 50031 is set by default.	Specify the port range to allocate for PASV style data connection.
Auto Report External IP in PASV Mode	Optional setting	Check the Enable box to activate the support of overriding the IP address advertising in response to the PASV command.
ASCII Transfer Mode	Optional setting	Check the Enable box to activate the support of ASCII mode data transfers. Binary mode is supported by default.
FTPS (FTP over SSL/TLS)	Optional setting	Check the Enable box to activate the support of secure connections via SSL/TLS.

8.3.3.1. Enable SFTP Server



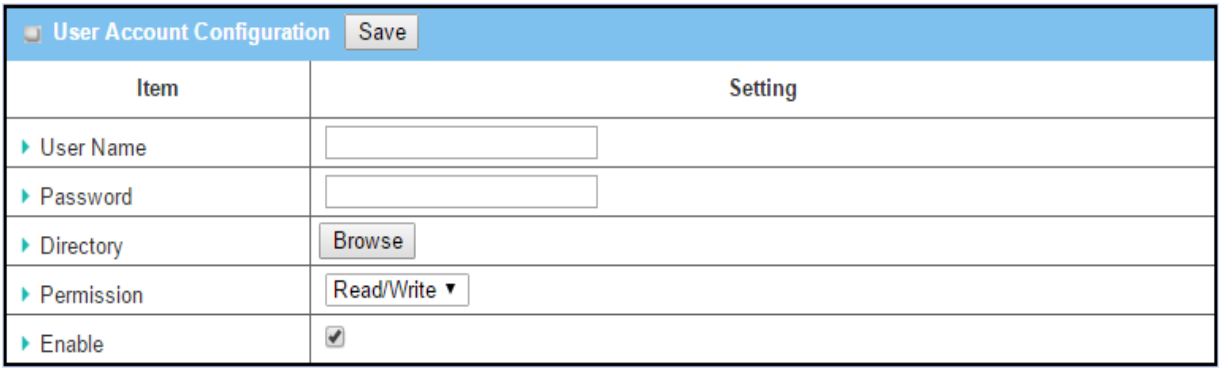
Configuration		
Item	**Value setting**	**Description**
SFTP	The box is unchecked by default.	Check Enable box to activate the embedded SFTP Server function. With the SFTP Server enabled, you can retrieve or delete the stored log files via secure SFTP connection.
Via LAN/WAN	Unselectable by default	When SFTP Server is enabled these can be selected. When checked the selected port will allow SFTP access.
SFTP Port	Default 22	Specify a port number for SFTP connection. The gateway will listen for incoming SFTP connections on the specified port.

8.3.3.2. User Account

This section allows user to setup user accounts for logging to the embedded FTP and SFTP server to retrieve the interested fog files.

Go to Administration > FTP > User Account tab. Create/Edit FTP User Accounts

When the **Add** button is applied, **User Account Configuration screen** will appear.



Configuration		
Item	**Value setting**	**Description**
User Name	String: non-blank string	Enter the user account for login to the FTP server.
Password	String: no blank	Enter the user password for login to the FTP server.
Directory	N/A	Select a root directory after user login.
Permission	Read/Write is selected by default.	Select the Read/write permission. **Note**: The embedded FTP Server is only for log downloading, so write permission is not implemented for user file upload to the storage, even Read/Write option is selected.
Enable	The box is checked by default.	Check the box to activate the FTP user account.

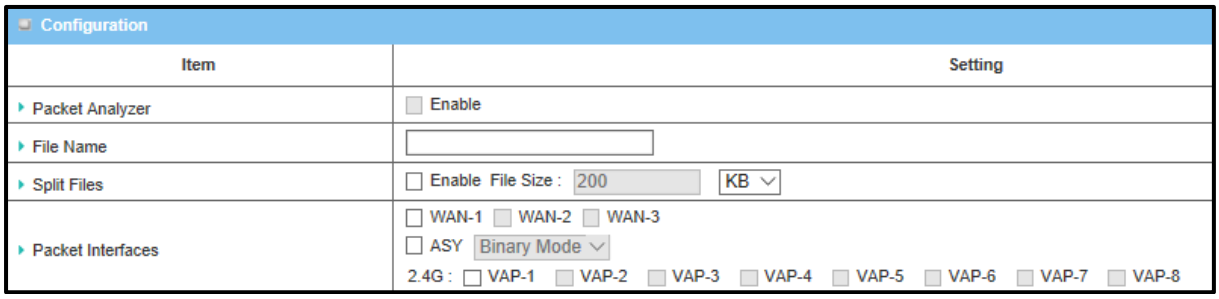
8.4 Diagnostics

This 6402 supports simple network diagnosis tools for the network administrator to troubleshoot and find the root cause of any abnormal behaviour passing through the 6402. The following chapter outlines the various diagnostic tools.

8.4.1. Packet Analyser

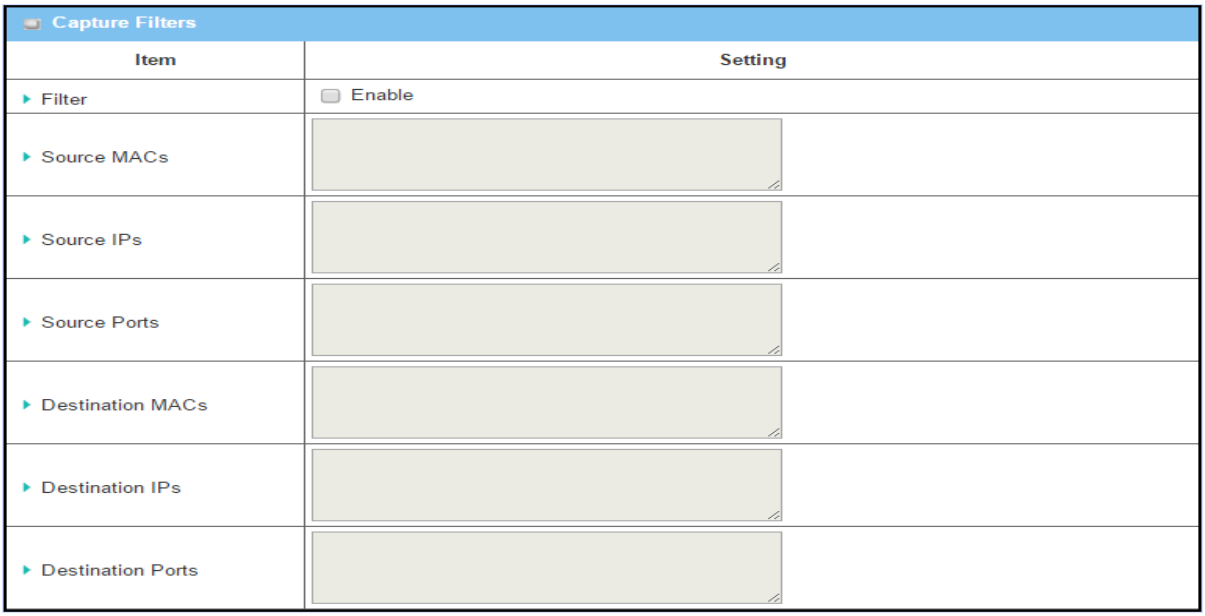
The Packet Analyser can capture packets depend on user settings. The User can specify which interfaces to capture packets and filter by setting rule. Ensure the log storage is available (an external USB Storage), otherwise Packet Analyser cannot be enabled.

Go to Administration > Diagnostic > Packet Analyser tab.



Configuration		
Item	Value setting	Description
Packet Analyser	The box is unchecked by default.	Check Enable box to activate the Packet Analyser function. If you cannot enable the checkbox, please check if storage is available. Plug in a USB stick for storage and then enable the Package Analyser function.
File Name	1. An optional setting 2. Blank is set by default, and the default file name is <Interface>_<Date>_<index>.	Enter the file name to save the captured packets in log storage. If the Split Files option is also enabled, the file name will be appended with an index code "_<index>". The extension file name is .pcap.
Split Files	1. An optional setting 2. The default value of File Size is 200 KB. 3. NOTE that File Size cannot be less than 4 KB	Check **enable** box to split file whenever log file reaching the specified limit. If the Split Files option is enabled, you can further specify the File Size and Unit for the split files.
Packet Interfaces	An optional setting	Define the interface(s) that Packet Analyser should work on. At least, one interface is required, but multiple selections are also accepted. The supported interfaces can be: WAN: When the WAN is enabled at Physical Interface, it can be selected here. ASY: This means the serial communication interface. It is used to capture packets appearing in the Field Communication. Therefore, it can only be selected when specific field communication protocol, like Modbus, is enabled. VAP: This means the Virtual AP. When WiFi and VAP are enabled, it can be selected here.
Save	N/A	Click the Save button to save the configuration.
Undo	N/A	Click the Undo button to restore what you just configured back to the previous setting.

Once you enable the Packet Analyser function on a specific Interface(s), you can further specify some filter rules to capture the packets which matched the rules.

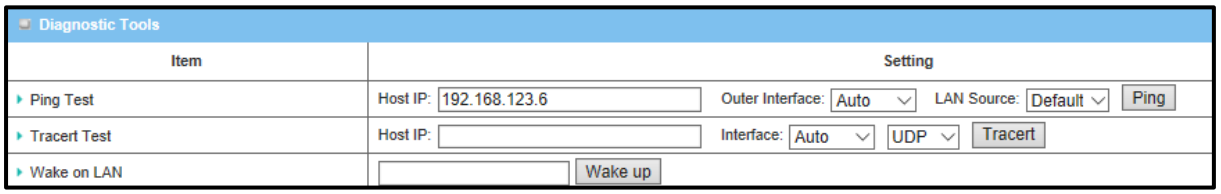


Capture Fitters		
Item	**Value setting**	**Description**
Filter	Optional setting	Check Enable box to activate the Capture Filter function.
Source MACs	Optional setting	Define the filter rule with Source MACs, which means the source MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “;”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Source IPs	Optional setting	Define the filter rule with Source IPs, which means the source IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”,e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Source Ports	Optional setting	Define the filter rule with Source Ports, which means the source port of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”,e.g. 80; 53 The packets will be captured when match any port in the rule.
Destination MACs	Optional setting	Define the filter rule with Destination MACs, which means the destination MAC address of packets. Packets which match the rule will be captured. Up to 10 MACs are supported, but they must be separated with “;”, e.g. AA:BB:CC:DD:EE:FF; 11:22:33:44:55:66 The packets will be captured when match any one MAC in the rule.
Destination IPs	Optional setting	Define the filter rule with Destination IPs, which means the destination IP address of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”, e.g. 192.168.1.1; 192.168.1.2 The packets will be captured when match any one IP in the rule.
Destination Ports	Optional setting	Define the filter rule with Destination Ports, which means the destination port of packets. Packets which match the rule will be captured. Up to 10 IPs are supported, but they must be separated with “;”, e.g. 80; 53The packets will be captured when match any port in the rule.

8.4.2. Diagnostic Tools

The Diagnostic Tools provide some frequently used network connectivity diagnostic tools for the network administrator to check the 6402‘s connectivity.

Go to Administration > Diagnostic > Diagnostic Tools tab.



Diagnostic Tools		
Item	**Value setting**	**Description**
Ping Test	Optional Setting	This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the **Ping** button. A test result window will appear beneath it.
Outer Interface	Auto selected by default	Selects which configured port (WAN or LAN) the ping is output to.
Lan Source	Default selected	Selects which LAN (if multiple LANs are configured) is the source of the ping.
Tracert Test	Optional setting	Trace route (tracert) command is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Trace route proceeds until all (three) sent packets are lost for more than twice, then the connection is lost, and the route cannot be evaluated. First, you need to specify an IP / FQDN, the test interface and the protocol (UDP or ICMP), and by default, it is **UDP**. Then, system will try to trace the specified host to test whether it is alive after clicking on the **Tracert** button. A test result window will appear beneath it.
Wake on LAN	Optional setting	WakeonLAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the **Wake up** command button.
Save	N/A	Click the **Save** button to save the configuration.

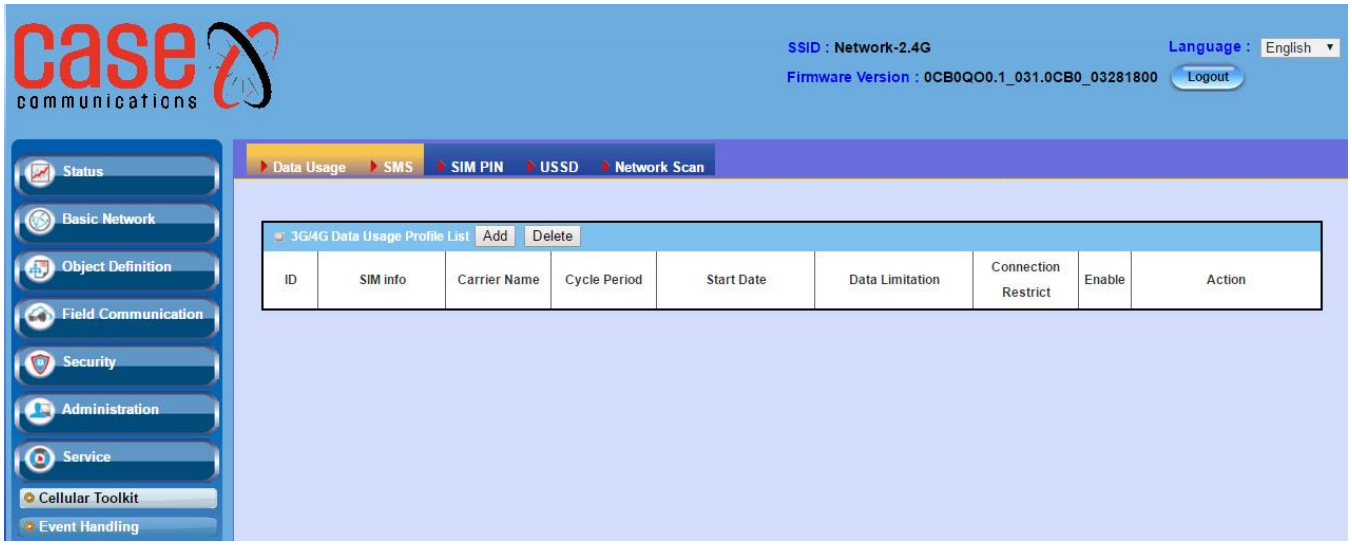
CHAPTER 9

SERVICE

Cellular Tool Kit

SMS and Event Handling

9.0. Service



9.1. Cellular Toolkit

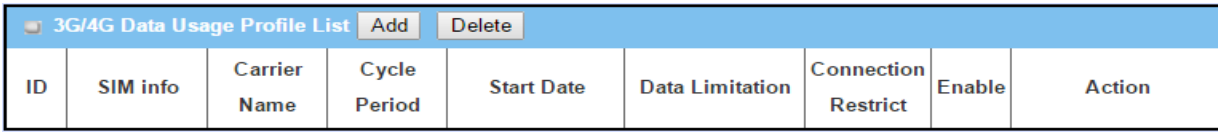
In Cellular Toolkit Service section, the device supports Data Usage, SMS, SIM PIN, USSD, and Network Scan. You can setup these aspects of cellular applications by using embedded 3G/LTE module in the device.

9.1.1. Data Usage

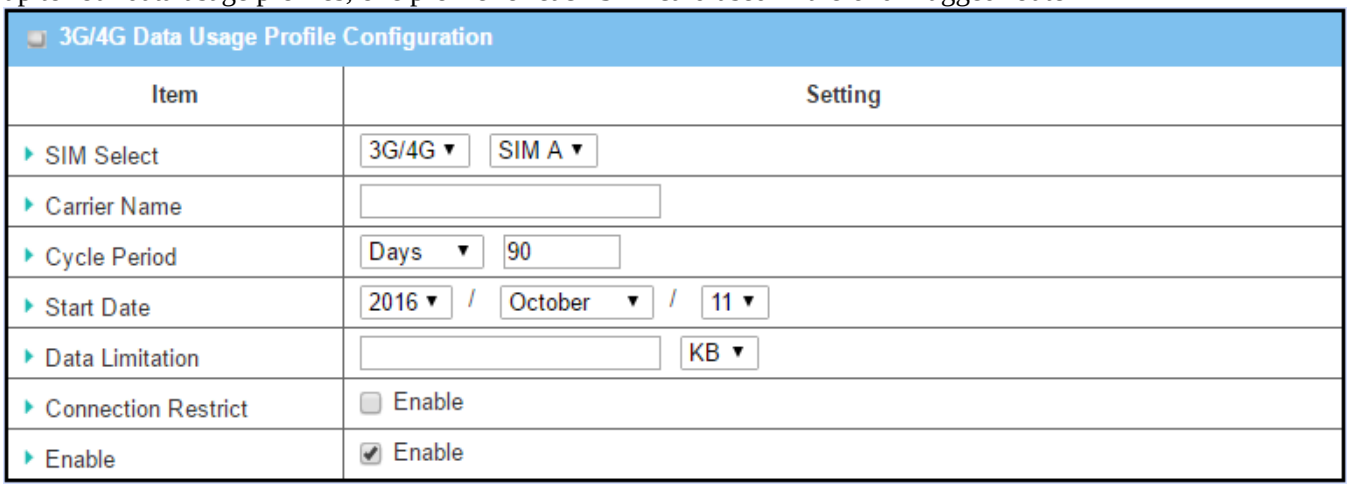
Most mobile phone users have no unlimited data plan so the telecom charges may exceed the bills upper limit. Data Usage feature can monitor the network traffic and show a simple chart so that users can easily control the condition.

9.1.1.1 3G / 4G Data Usage Profile

Go to System > System Related > Data Usage tab - Create / Edit 3G/4G Data Usage Profile



When the 'Add' button is applied, the 3G/4G Data Usage Profile Configuration screen will appear. You can create up to four data usage profiles, one profile for each SIM card used in the 6402 rugged router



3G/4G Data Usage Profile Configuration		
Item Setting	**Value setting**	**Description**
SIM Select	3G/4G-1 and SIM A by default.	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**), and a SIM card bound to the selected cellular interface to configure its data usage profile.
Carrier Name	It is an optional item.	Fill in the Carrier Name for the selected SIM card for identification.
Cycle Period	Days by default	The first box has three types for cycle period. They are **Days**, **Weekly** and **Monthly**. **Days**: For per Days cycle periods, you have to further specify the number of days in the second box. Its range is from 1 to 90 days. **Weekly**, **Monthly**: The cycle period is one week or one month.
Start Date	N/A	Specify the date to start measure network traffic. Please don't select the day before now, otherwise, the traffic statistics will be incorrect.
Data Limitation	N/A	Specify the allowable data limitation for the defined cycle period.
Connection Restrict	Un-Checked by default.	Check the **Enable** box to activate the connection restriction function. During the specified cycle period, if the actual data usage exceeds the allowable data limitation, the cellular connection will be forced to disconnect.
Enable	Un-Checked by default.	Check the **Enable** box to activate the data usage profile.

9.1.2. SMS

The Short Message Service (SMS) is a text messaging service used by a mobile phone, Web, or other communication systems. It uses standard communications protocols to allow fixed line or mobile phones to exchange short text messages.

SMS as used on modern handsets originated from radio telegraphy in radio memo pagers using standard phone protocols. These were defined in 1985 as part of the Global System for Mobile Communications (GSM) series of standards as a means of sending messages of up to 160 characters to and from GSM mobile handsets. Though most SMS messages are mobile-to-mobile text messages, support for the service has expanded to include other mobile technologies, such as ANSI CDMA networks and Digital AMPS, as well as satellite and landline networks. The SMS function allows a user to send an SMS, read and delete SMS's from a SIM Card.

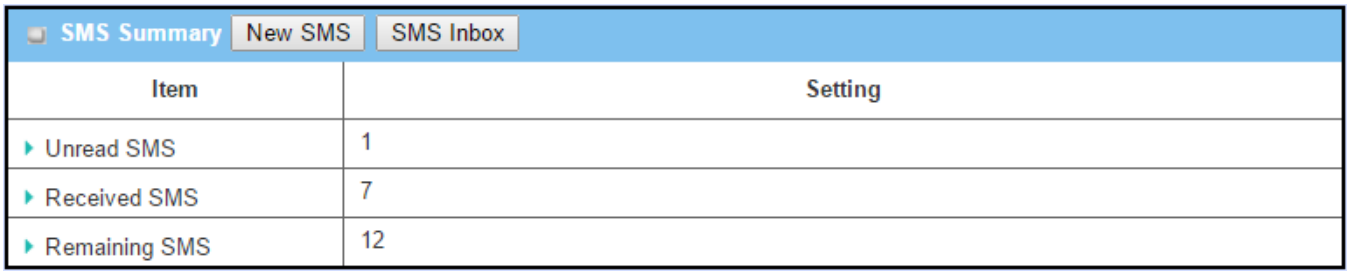
Go to **Service** > **Cellular Toolkit** > **SMS** tab

9.1.2.1. Setting up SMS Configuration

Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**) for the following SMS function configuration.
SMS	The box is checked by default	This is the SMS switch. If the box checked that the SMS function enable, if the box unchecked that the SMS function disable.
SIM Status	N/A	Depend on currently SIM status. The possible value will be **SIM_A** or **SIM_B**.
SMS Storage	The box is SIM Card Only by default	This is the SMS storage location. Currently the option only **SIM Card Only.**
Save	N/A	Click **Save** to save the settings

9.1.2.2. SMS Summary

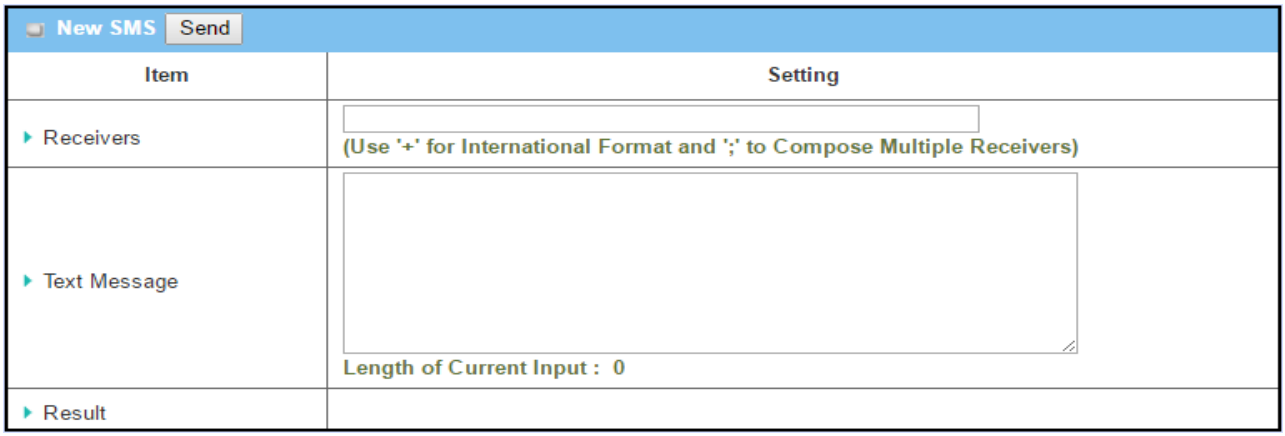
Show Unread SMS, Received SMS, Remaining SMS, and edit an SMS message, and read an SMS from SIM card.



SMS Summary		
Item	**Value setting**	**Description**
Unread SMS	N/A	If the SIM card is inserted into the router for the first time, the unread SMS value will be zero. If received but not read the new SMS will be a value of plus one.
Received SMS	N/A	This value record the existing SMS numbers from SIM card, When received the new SMS, the value is incremented by one.
Remaining SMS	N/A	This value is the capacity of the SMS to receive Text Messages after registering the existing text messages..
New SMS	N/A	Click **New SMS** button, a **New SMS** screen appears. User can set the SMS setting from this screen. Refer to New SMS in the next page.
SMS Inbox	N/A	Click **SMS Inbox** button, a **SMS Inbox List** screen appears. User can read or delete SMS, reply SMS or forward SMS from this screen. Refer to SMS Inbox List in the next page.

New SMS

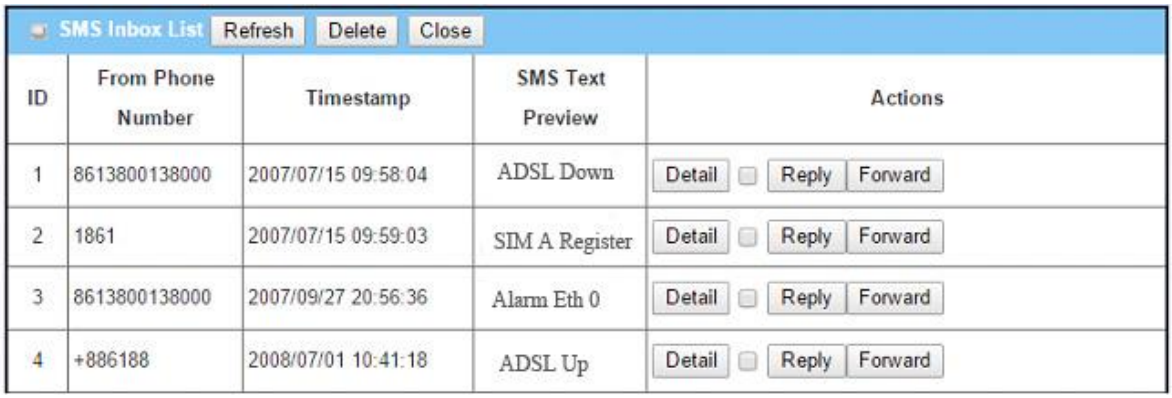
You can set the SMS setting from this screen.



New SMS		
Item	**Value setting**	**Description**
Receivers	N/A	Add the people who you want to receive the SMS. Add a semicolon and compose multiple receivers to join the SMS group.
Text Message	N/A	Write the SMS content to be sent as an SMS. The router supports up to a maximum of 1023 character for SMS message length.
Result	N/A	If sent SMS has been sent successfully the 6402 will receive a **Send OK**, message otherwise **Send Failed** will be displayed.
Send	N/A	By click the **Send** button, SMS will be sent.

SMS Inbox List

You can read or delete SMS, reply SMS or forward SMS from this screen.



SMS Inbox List		
Item	**Value setting**	**Description**
ID	N/A	The number or SMS.
From Phone Number	N/A	The phone number that sent the SMS
Timestamp	N/A	What time the SMS was sent
SMS Text Preview	N/A	Preview the SMS text. Click the **Detail** button to read a certain message.
Action	The box is unchecked by default	Click the **Detail** button to read the SMS; Click the **Reply** / **Forward** button to reply/forward SMS. You can check the box(es), and then click the **Delete** button to delete the checked SMS(s).
Refresh	N/A	Refresh the SMS Inbox List.
Delete	N/A	Delete the SMS for all checked box from Action.
Close	N/A	Close the Detail SMS Message screen.

SMS Sent

This table displays all the SMS Messages sent from this 6402, together with a Time stamp and preview.

SMS Sent Folder	Delete	Close			
ID	Receivers		Timestamp	SMS Text Preview	Action

9.1.3. SIM PIN

Its normal to use a PIN / Password on your mobile device to prevent un-authorised use

This password setting can be applied to an end devices (e.g. mobile phone) or SIM card.
In most cases, users need to insert a SIM card into a mobile devices to get onto a cellular network for voice services or data surfing. The SIM card is usually released by a mobile operators or service provider.
Each SIM card has a unique number (so-called ICCID) for the network owners or service providers to identify each subscriber. As the SIM card plays an important role between the service providers and subscribers, some security mechanisms are required on the SIM card to prevent any unauthorised access.

If a PIN code is activated on your 6402 SIM card, you will see a similar message (as shown below) when the 6402 is powered on. This requires you have the correct PIN code to unlock the SIM card. Otherwise, there is no way to use cellular-related functions, such as GSM voice service, SMS text, 3G or LTE Internet surfing …etc.

Step 1

Step 2

Step 3

The following steps show typical procedures for unlocking a SIM card on mobile phone.

Step 1: Press the "Unlock" button to unlock a SIM card.

Step 2: Enter the correct PIN code, and then press "OK".

Please note an important message "3 attempts remaining" at the top of screen. The maximum of failure to input a wrong PIN is 3. If you enter an incorrect PIN code three times, the SIM card will be locked. In this situation, you need to request a PUK (PIN Unlock Key) code from your service provider to reset PIN code on SIM card.

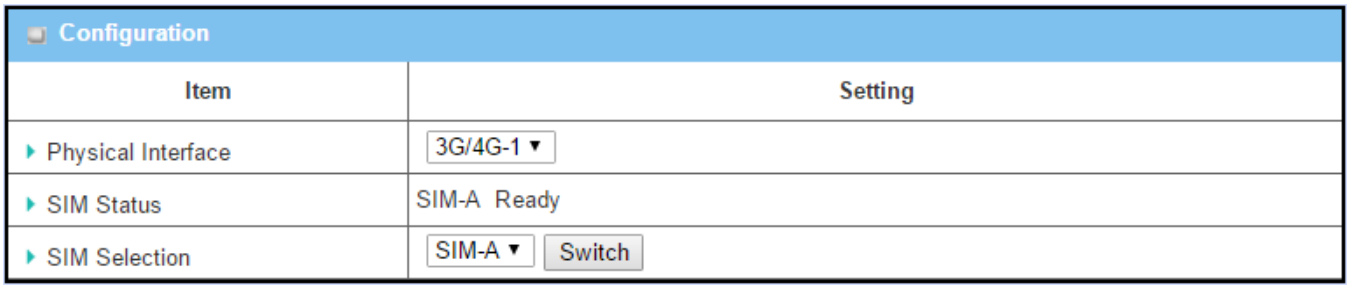
Step 3: If the PIN code is correct, you will see a successful message on screen. The mobile phone will start to connect to the cellular network and will provide cellular services.

The 6402 cellular gateway is similar to a mobile phone, meaning users need to insert SIM cards into 6402's SIM slot to get cellular-related functions. The 6402 has a metal SIM cover with screws fastened to protect SIM cards. It is recommended the PIN is activated on the SIM card before its installed on site.

9.1.3.1 SIM PIN Configuration

The SIM PIN Function window, allows you to enable or disable the SIM lock (which means protected by PIN code), or change the PIN code. You can also see data on any failed SIMS.

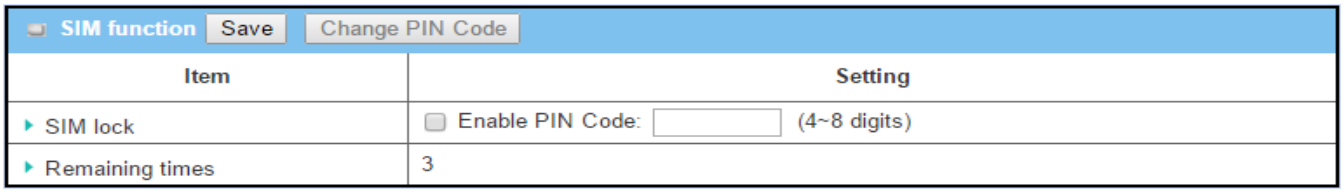
Go to Applications > Mobile Application > SIM PIN Tab > Select a SIM Card



Configuration Window		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to change the SIM PIN setting for the selected SIM Card. The 6402 supports 2 SIM Cards.
SIM Status	N/A	Indication for the selected SIM card and the SIM card status. The status could be Ready, Not Insert, or SIM PIN. Ready -- SIM card is inserted and ready to use. It can be a SIM card without PIN protection or that SIM card is already unlocked by correct PIN code. Not Insert -- No SIM card is inserted in that SIM slot. SIM PIN -- SIM card is protected by PIN code, and it's not unlocked by a correct PIN code yet. That SIM card is still at locked status.
SIM Selection	N/A	Select the SIM card for further SIM PIN configuration. Press the **Switch** button, then the Gateway will switch SIM card to another one. After that, you can configure the SIM card.

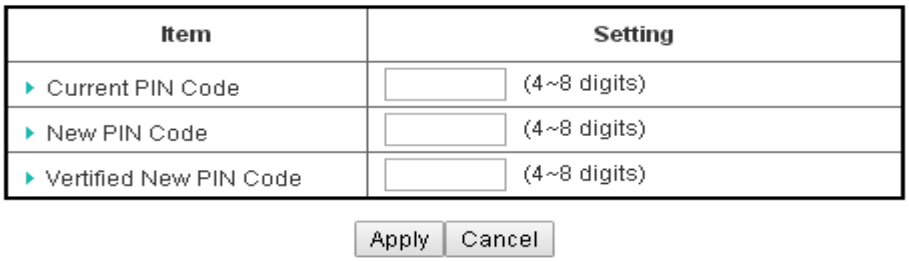
Enable / Change PIN Code

Enable or Disable the PIN code (password) function, and even change PIN code function.



SIM function Window		
Item Setting	**Value setting**	**Description**
SIM lock	Depend on SIM card	Click the **Enable** button to activate the SIM lock function. For the first time you want to enable the SIM lock function, you have to fill in the PIN code as well, and then click **Save** button to apply the setting.
Remaining times	Depend on SIM card	This displays the number of attempts left to unlock the SIM Card
Save	*NA*	Click the **Save** button to apply the setting.
Change PIN Code	*NA*	Click the **Change PIN code** button to change the PIN code (password). If the **SIM Lock** function is not enabled, the **Change PIN code** button is disabled. In the case, if you still want to change the PIN code, you have to enable the SIM Lock function first, fill in the PIN code, and then click the **Save** button to enable. After that, You can click the **Change PIN code** button to change the PIN code.

When the 'Change PIN' Code button is clicked, the following screen will appear.



Configuration		
Item Setting	**Value setting**	**Description**
Current PIN Code	A Mandatory setting	Fill in the current (old) PIN code of the SIM card.
New PIN Code	A Mandatory setting	Fill in the new PIN Code you want to change.
Verified New PIN Code	A Mandatory setting	Confirm the new PIN Code again.
Apply	*N/A*	Click the **Apply** button to change the PIN code with specified new PIN code.
Cancel	*N/A*	Click the **Cancel** button to cancel the changes and keep current PIN code.

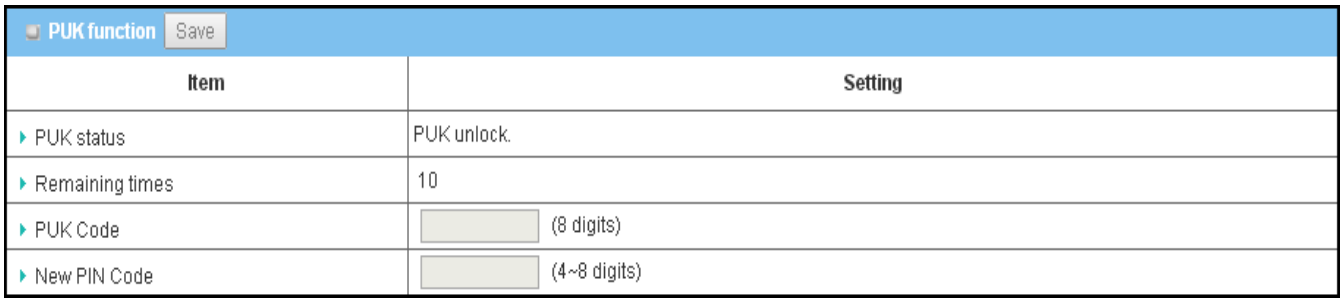
Note: If you changed the PIN code for a specific SIM card, you must also change the corresponding PIN code specified in the following page

Basic Network > WAN & Uplink > Internet Setup > Connection on the SIM Card page. Otherwise, you may get a message saying invalid (old) PIN Code.

9.1.3.2 PuK Function – Unlocking a PIN Code

The PUK Function window is only available if the SIM card is locked via a PUK code. It means that SIM card is locked and needs an additional PUK code to unlock it.

Usually this happens after too many attempts entering the incorrect PIN code, and the remaining time in SIM has gone to 0. In this situation, you need to contact your service provider and request a PUK code for your SIM card, and try to unlock the locked SIM card with the PUK code that you were given. After unlocking a SIM card with the PUK code successfully, the SIM lock function will be activated automatically.



PUK Function Window		
Item	**Value setting**	**Description**
PUK status	**PUK Unlock** / **PUK Lock**	Indication for the PUK status. The status could be **PUK Lock** or **PUK Unlock**. As already written the SIM card will be locked by a PUK code after too many failed attempts to enter a PIN code. In this case, the PUK Status will turns to **PUK Lock**. In a normal situation, it will display **PUK Unlock**.
Remaining times	Depend on SIM card	This displays the remaining attempts to unlock the PUK. Note : **DO NOT allow the remaining time to go down to zero, it will damage the SIM card FOREVER !** Call for your ISP's help to get a correct PUK and unlock the SIM if you don't have the PUK code.
PUK Code	A Mandatory setting	Fill in the PUK code (8 digits) to unlock the SIM card in PUK unlock status.
New PIN Code	A Mandatory setting	Fill in the New PIN Code (4~8 digits) for the SIM card. You have to determine your new PIN code to replace the old, forgotten one. Keep the PIN code (password) somewhere safe.
Save	N/A	Click the **Save** button to apply the setting.

Note: If you changed the PUK code and PIN code for a specific SIM card, you must also change the corresponding the

Scenario of activating Network Administrator would like to enable the SIM lock function with a default PIN code "0000" on a new SIM card. PIN code on SIM card

This SIM card was inserted into SIM-A slot for 3G/4G-1 WAN connection.

Configuration:

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[Configuration]
Physical Interface	*3G/4G-1*
SIM Status	*Ready*
SIM Selection	*SIM-A*

SIM Function

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[SIM Function]
SIM Lock	*Enable, PIN Code: 0000*
Remaining Times	*[Display Remaining Times]*

Scenario of changing PIN code on SIM card

A Network Administrator would like to change a PIN code from the default "0000" to "1234" on a SIM card. This SIM card has been inserted into SIM-A slot for 3G/4G-1 WAN connection.

SIM Function

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[SIM Function]-[Change PIN Code]
Current PIN Code	*0000*
New PIN Code	*1234*
Verified New PIN Code	*1234*

How to unlock a SIM card with a PUK code

A Network Administrator entered an incorrect PIN code for the 3G/4G-1 WAN, and then it caused that SIM card to be locked by the PUK code. He called the service number, and he was informed the PUK code for his SIM card is "12345678". He then unlocked that SIM card with the PUK code, and set a new PIN code "5678".

Configuration:

Configuration Path	[Cellular Toolkit]-[SIM PIN]-[Configuration]
Physical Interface	*3G/4G-1*
SIM Status	*SIM PIN*
SIM Selection	*SIM-A*

PUK Configuration Path

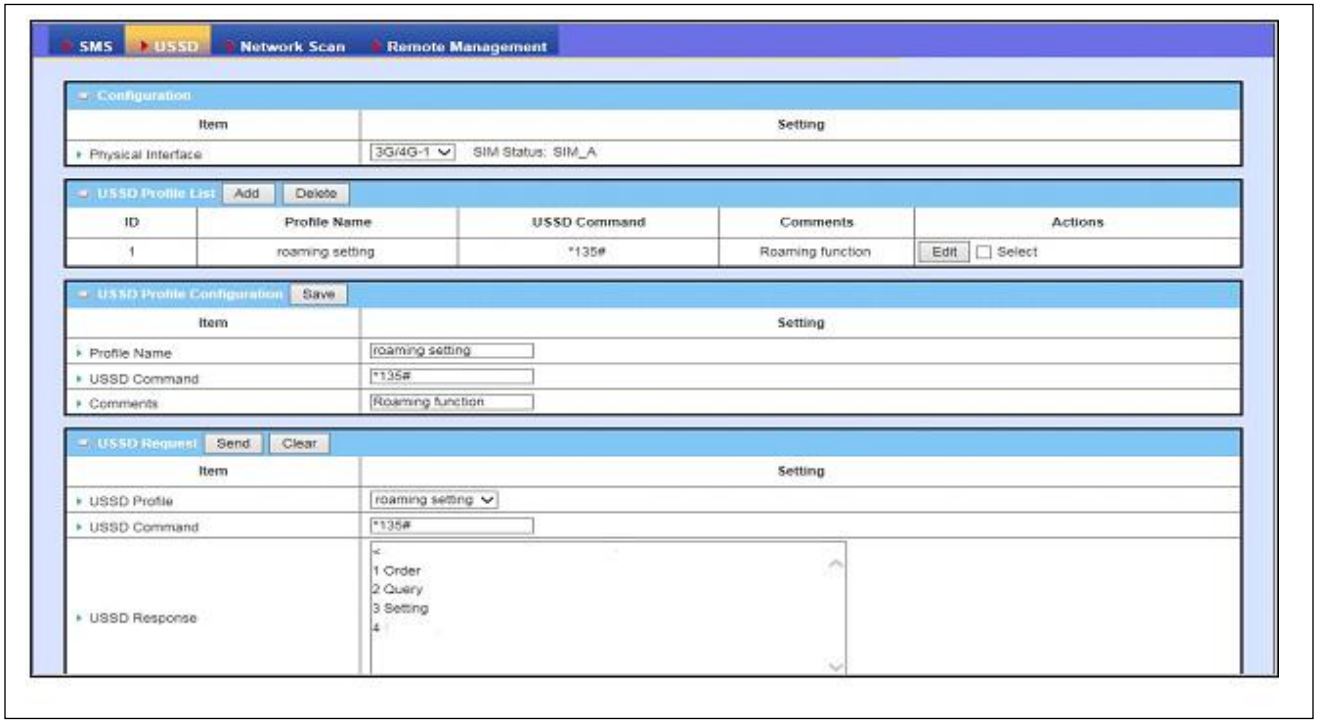
Configuration Path	[Service]-[SIM PIN]-[PUK Function]
PUK Status	*PUK Lock*
Remaining Times	*[Display Remaining Times]*
PUK Code	*12345678*
New PIN Code	*5678*

9.1.4. USSD

Note this menu option can only be seen if the 6402 has a SIM card and has connected to the network

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for WAP browsing, a prepaid call back service, mobile-money services, location-based content services, menu-based information services, and as part of configuring the phone on the network. [3]

An USSD message is up to 182 alphanumeric characters in length. Unlike Short Message Service (SMS) messages, USSD messages create a real-time connection during an USSD session. The connection remains open, allowing a two-way exchange of a sequence of data. This makes USSD more responsive than services that use SMS.13

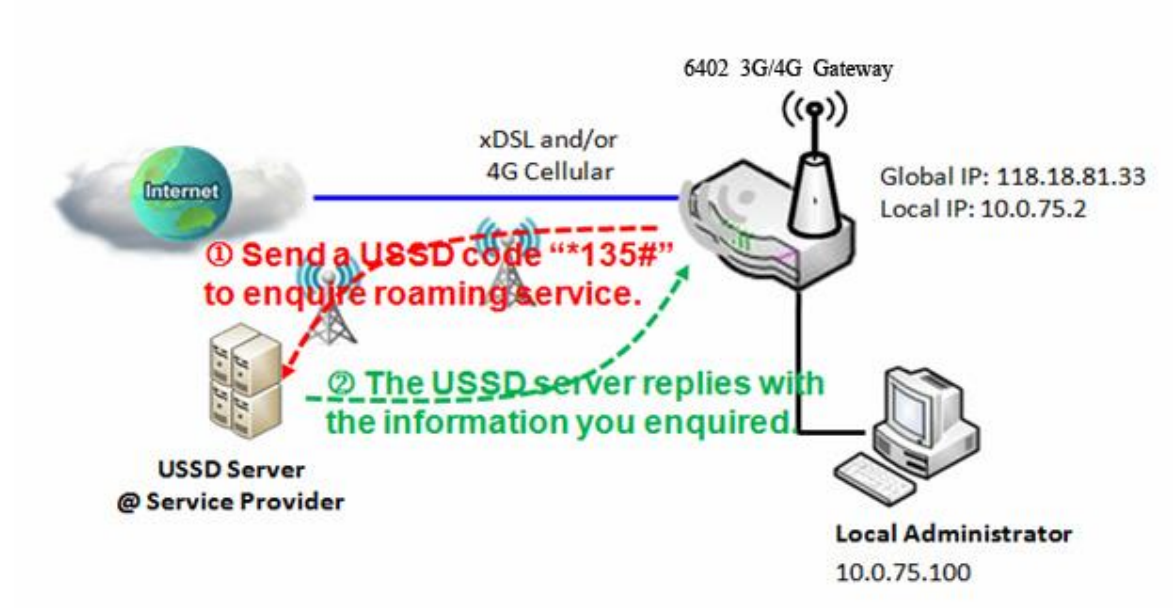


On the "USSD" page, there are four windows for the USSD function.

1. The "Configuration" window can let you specify which 3G/4G module (physical interface) is used for the USSD function, and system will show which SIM card in the module is the current used one.
2. The second window is the "USSD Profile List" and it shows all your defined USSD profiles that store pre-commands for activating an USSD session. An "Add" button in the window can let you add one new USSD profile and define the command for the profile.

3. The third window, is the "USSD Profile Configuration". When you want to start the activation of an USSD connection session to the USSD server, select the USSD profile or type in the correct pre-command, and then click on the "Send" button for the session.
4. The fourth window displays the responses from the USSD server. When commands typed in the "USSD Command" field are sent, received responses will be displayed in the "USSD Response" blank space. User can communicate with the USSD server by sending USSD commands and getting USSD responses via the gateway.

An USSD Session Scenario



9.1.4.1. Application Scenario

The following is example of the 6402 asking for ISP Services through a USSD Session via a roaming subscription with Vodafone.

Scenario Description

An USSD session can be established from the voice Vo3G Gateway to ask for services that are provided by ISP.

Parameter Setup Example

Following tables list the parameter configuration as an example for "USSD" function, as shown in above diagram. Use default value for those parameters that are not mentioned in the tables.

Configuration Path	[USSD]-[Configuration]
Physical Interface	*3G/4G-1* SIM Status: SIM_A
Configuration Path	**[USSD]-[USSD Profile Configuration]**
Profile Name	*roaming setting*
USSD Command	**135#*
Comments	*Roaming function*
Configuration Path	**[USSD]-[USSD Request]**
Profile Name	*roaming setting*
USSD Command	**135#*
USSD Response	*Vodafone Data Roaming Services* ***1.*** *Order* ***2.*** *Query* ***3.*** *Setting*

9.1.4.2. Scenario Operation Procedure

In the above diagram, the "6402 3G/4G Gateway" initiates a USSD session requesting data roaming services via Vodafone a UK mobile operator. The network administrator selects one of the 3G/4G modules as the physical interface for the USSD session.

Then the network administrator defines a USSD profile named as "roaming setting" with command "*135#" for further use.

In the "USSD Request" window, from the USSD Profile dropdown box select the "roaming setting" profile and the "USSD Command" field shows "*135#".

Click on the "Send" button to send out the USSD request via the 6402 gateway, and the received response will appear at "USSD Response" line.

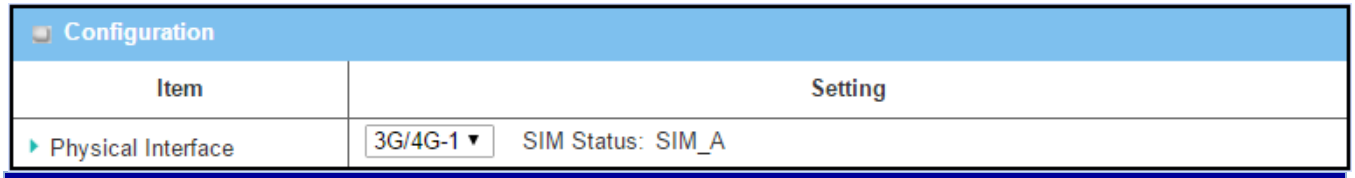
As the network manager types more commands into the "USSD Command" line, they will get more responses from the USSD server. It is an interactive communication session allowing the network administrator to request available services from their ISP via their USSD sessions.

9.1.4.3. USD Setting

The USSD function allow user to send USSD to ISP, then ISP will provide some service for user.

Go to **Service** > **Cellular Toolkit** > **USSD** tab.

USSD Configuration

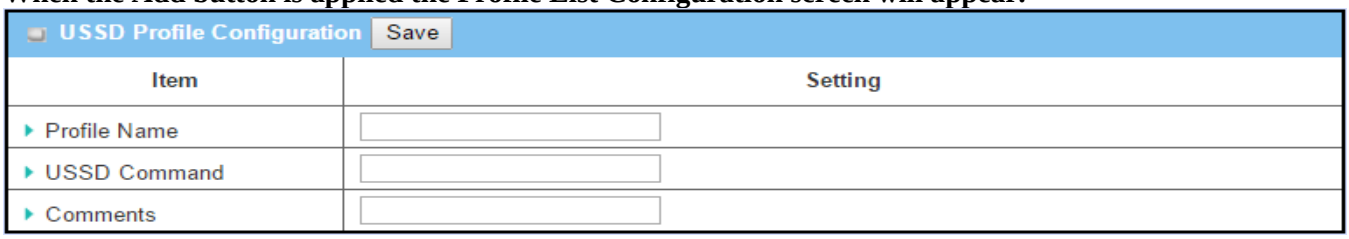


Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G-**1 or **3G/4G-2**) to configure the USSD setting for the connoted cellular service (identified with **SIM_A** or **SIM_B**).
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).

9.1.4.4. Create / Edit USSD Profile

The cellular gateway allows you to custom your USSD profile. It supports up to a maximum of 35 USSD profiles.

When the Add button is applied the Profile List Configuration screen will appear.



USSD Profile List		
Item	**Value setting**	**Description**
Profile Name	N/A	Enter a name for the USSD profile.
USSD Command	N/A	Enter the USSD command defined for the profile. Normally, it is a command string comprising a numeric keypad "0~9", "*", and "#". The USSD commands are related to the cellular service, please check with your service provider for the details.
Comments	N/A	Enter a brief comment for the profile.

9.1.4.5. Send USSD Request

When select the USSD command, the USSD Response screen will appear.

When you click the 'Clear' button, the USSD Response will disappear.

USSD Request		
Item	**Value setting**	**Description**
USSD Profile	N/A	Select a USSD profile name from the dropdown list.
USSD Command	N/A	The USSD Command string of the selected profile will be shown here.
USSD Response	N/A	Click the **Send** button to send the USSD command, and the **USSD Response** screen will appear. You will see the response message of the corresponding service, receive the service SMS.

9.1.5. Network Scan

The "Network Scan" function allows the network administrator to specify how to connect the 6402 for data communications on each of the 6402 3G/4G interfaces.
For example, the administrator can specify which generation of mobile network is used for example, 2G, 3G or LTE. They can also define their connection sequence for the 6402 to connect to the mobile network automatically. The Network Administrator can scan the mobile networks manually, select the target operator system and apply it. The manual scanning approach is used for problem diagnosis; however, the 6402 will scan the mobile network automatically during normal operation.

Go to **Service** > **Cellular Toolkit** > **Network Scan tab. - Network Scan Configuration**

Configuration

Item	Setting
Physical Interface	3G/4G-1 ▼ SIM Status: SIM_B
Network Type	Auto ▼
Band Selection	Auto ▼
Band List	2G ☑ GSM (850Mhz) ☑ GSM P-GSM 900 (900Mhz) ☑ GSM E-GSM 900 (900Mhz) ☑ GSM DCS 1800 (1800Mhz) ☑ GSM PCS 1900 (1900Mhz) 3G ☑ WCDMA (2100Mhz) ☑ WCDMA 1900 PCS (1900Mhz) ☑ WCDMA (850Mhz) ☑ WCDMA 900 (900Mhz) LTE ☑ Band1 (2100Mhz) ☑ Band3 (1800Mhz) ☑ Band7 (2600Mhz) ☑ Band8 (900Mhz) ☑ Band20 (800Mhz) ☑ Band40 (2300Mhz)
Scan Approach	Auto ▼

In the "Network Scan" page, there are two windows for the Network Scan function.

1. The first "Configuration" window allows you select which 3G/4G module (physical interface) is used to perform a Network Scan. The 6402 will show the current SIM card used in the module. You can configure each 3G/4G WAN interface by using the network scan one after other. You can also specify the connection sequence of the targeted generation of mobile system, 2G/3G/LTE.
2. The second window is the "Network Provider List" window and it appears when **Manual** Scan is selected in the Configuration window. Click on the "Scan" button and wait for 1 to 3 minutes, the mobile networks that have been discovered will be displayed for you to choose.

Click on the "Apply" button to force the 6402 to connect to that mobile network for the dedicated 3G/4G interface.

Configuration		
Item	**Value setting**	**Description**
Physical Interface	The box is 3G/4G-1 by default	Choose a cellular interface (**3G/4G-1** or **3G/4G-2**) for the network scan function.
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).
Network Type	Auto is selected by default.	When **Auto** selected, the network will be register automatically. If the **prefer** option selected, network will be register for your option first. If the **only** option selected, network will be register for your option only.
Band Selection	Auto is selected by default.	When **Auto** selected, **Band List** all box checked, and user can't select any option. If the **Manual** option is selected, you can change the **Band List** setting.
Band List	All box is checked by default.	The **Band List's** options depend on the embedded cellular module, and user need to select option at least one for all network type.
Scan Approach	Auto is selected by default.	When **Auto** selected, cellular module register automatically. If the **Manually** option is selected, a **Network Provider List** screen appears. Press **Scan** button to scan for the nearest base stations. Select (check the box) the preferred base stations then click **Apply** button to apply settings.
Save	N/A	Click **Save** to save the settings

Network Providers List	Scan	Apply	
Provider Name	**Mobile System**	**Network Status**	**Action**
Vodafone	4G	Current	☐ Select
EE	3G	Forbidden	☐ Select

9.2. Event Handling

Event handling is the application that allows the 6402 network administrator to setup the pre-defined events, handlers, or response behaviour with individual profiles.

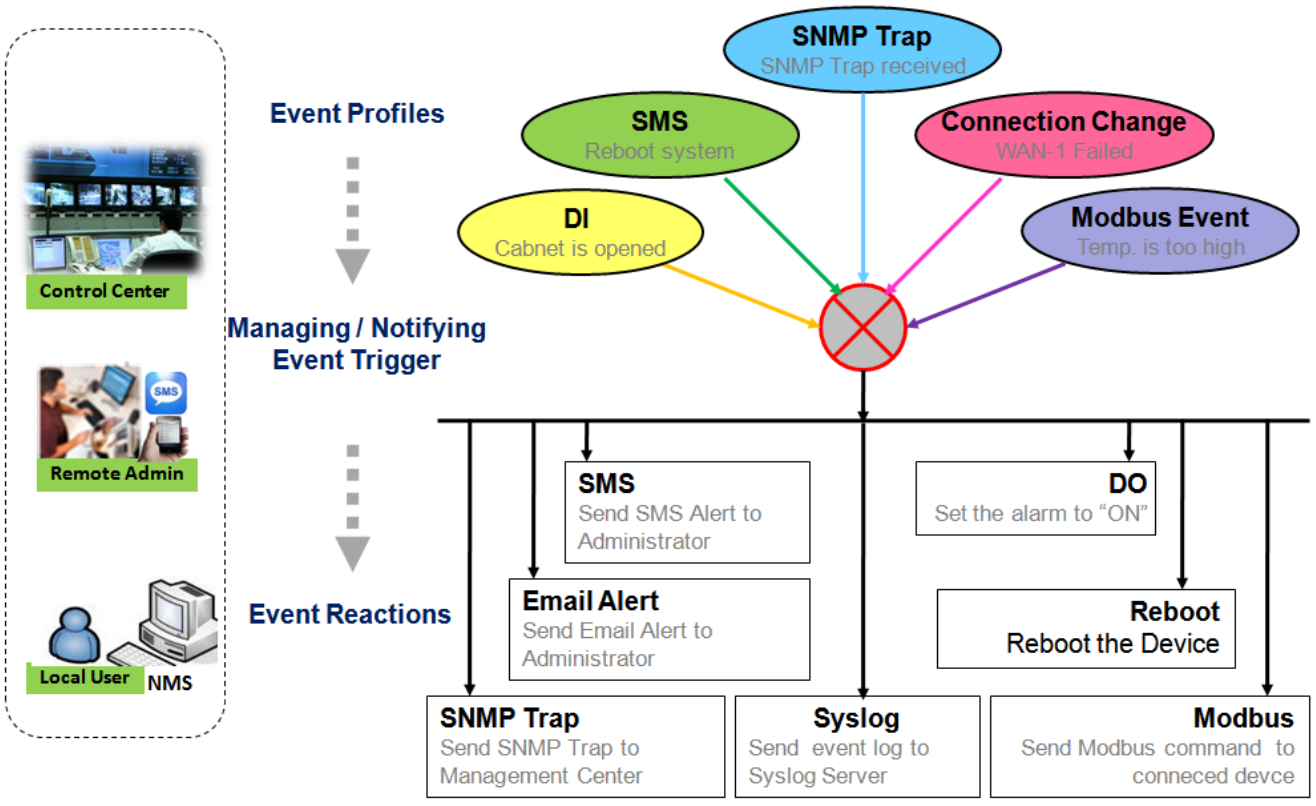
By configuring the event management function, the administrator can easily and remotely obtain the status and information via the 6402.

The 6402 network administrator can also handle and manage some important systems related functions, and send them to the field bus devices and D/O (Digital Output) devices.

Supported events are categorised into two groups: managing events and notifying events.

Managing events - are the events that are used to manage the gateway or change the setting / status of the specific functions of the 6402. On receiving the event, the 6402 will take action to change the function, collect the required status for administration, and also change the status of a certain connected field bus device simultaneously.

Notifying events - are the events that specific related objects have been triggered to take corresponding actions on when the events occur. It could be an event generated from a connected sensor, or a certain connected field bus device for alerting the 6402c administrator something happened with SMS message, Email, and SNMP Trap, etc.



The 6402 administrator can create and edit the common pre-defined management / notifying event profiles to take instant action on a certain event or manage the devices for some advanced actions.

For example, sending/receiving remote managing SMS for the 6402 ‘s routine maintaining, the field bus device status monitoring, digital sensors detection controlling, and so on. All management and notification function can be realised effectively via the Event Handling feature.

The following is the summary lists for the provided profiles, and events:

- Profiles (Rules):
- SMS Configuration and Accounts
- Email Accounts
- Digital Input (DI) profiles
- Digital Output (DO) profiles
- Modbus Managing Event profiles
- Modbus Notifying Event profiles

Managing Events:

- Trigger Type: SMS, SNMP Trap, and Digital Input (DI).
- Actions: Get the Network Status; or Configure the LAN/VLAN behavior, WIFI behavior, NAT behavior, Firewall behavior, VPN behavior, System Management, Administration, Digital Output behavior, and connected Modbus devices.

Notifying Events:

- Trigger Type: Digital Input, Power Change, Connection Change (WAN, LAN & VLAN, WiFi, DDNS), Administration, Modbus, and Data Usage.
- Actions: Notify the administrator with SMS, Syslog, SNMP Trap or Email Alert; Change the status of connected Digital Output or Modbus devices.

To use the event handling function follow these steps,
Enable the event management setting and configure the event details with the provided profile settings.
Create or edit pre-defined profiles for individual management / notifying events.
The profile settings are separated into several items, they are;

- SMS Account Definition
- Email Service Definition
- Digital Input (DI) Profile Configuration
- Digital Output (DO) Profile Configuration
- Modbus Definition

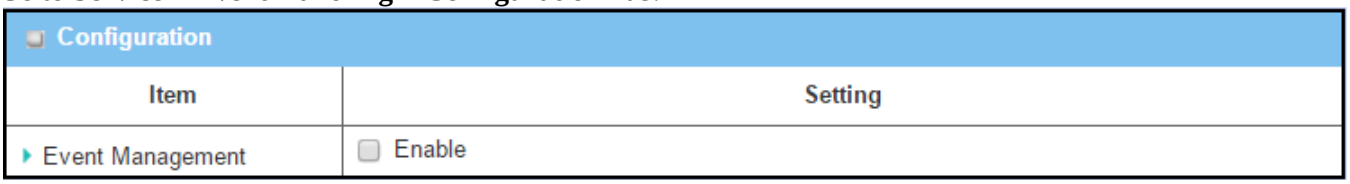
Its necessary to configure each management / notifying event with identifiable event trigger conditions, and set corresponding actions (reaction for the event) for the event.
For each event, more than one actions can be activated simultaneously.

9.2.1. Configuration

9.2.1.1. Configuring event Handling

Event handling is the service that allows the network administrator to setup pre-defined events, handlers, or response behavior with individual profiles.

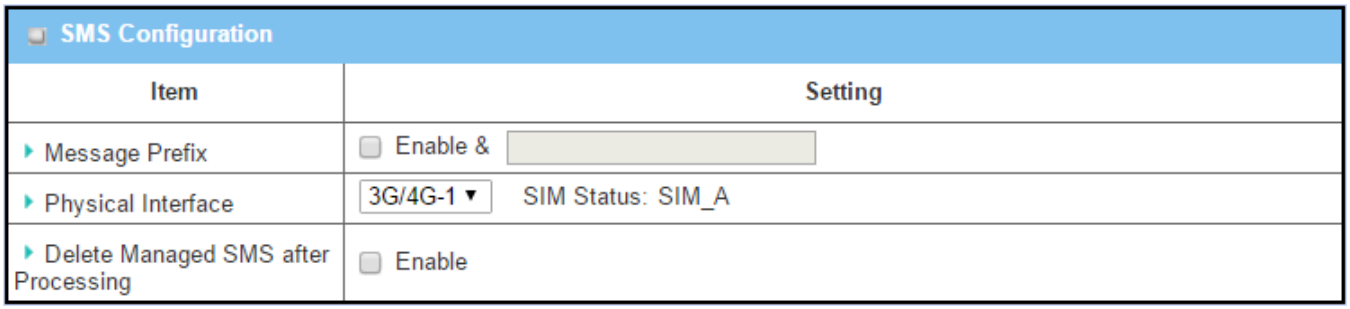
Go to **Service** > **Event Handling** > **Configuration** Tab.



Configuration		
Item	**Value setting**	**Description**
Event Management	The box is unchecked by default	Check the **Enable** box to activate the Event Management function.

9.2.1.2. SMS Configuration

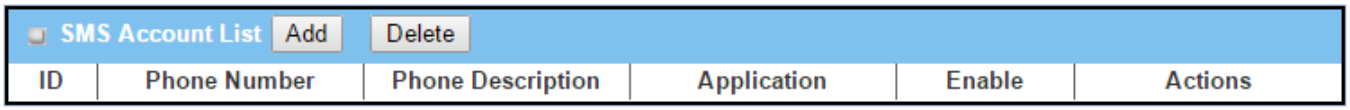
To use the SMS management function, you have to configure some settings first.



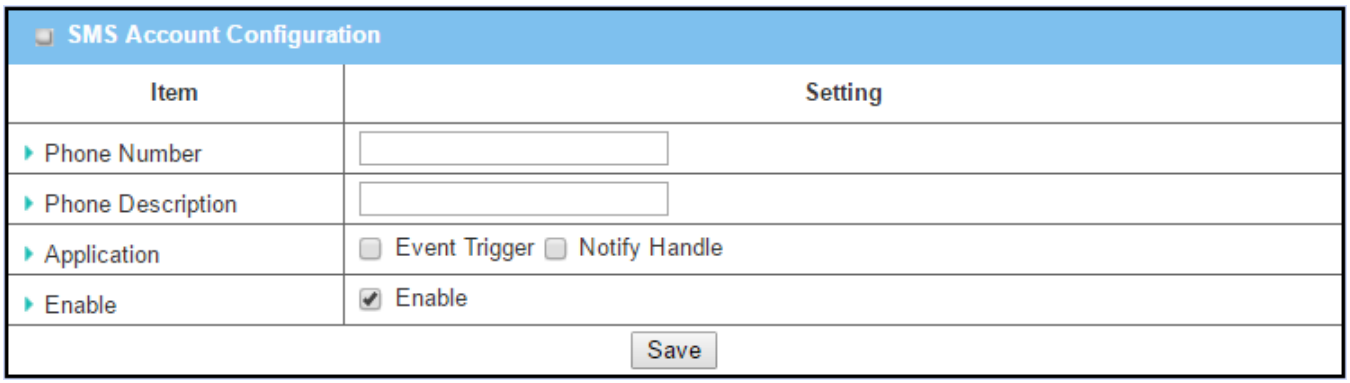
SMS Configuration		
Item	**Value setting**	**Description**
Message Prefix	The box is unchecked by default	Click the **Enable** box to enable the SMS prefix for validating the received SMS. Once the function is enabled, you have to enter the prefix behind the checkbox. The received managing events SMS must have the designated prefix as an initial identifier, then corresponding handlers will become effective for further processing.
Physical Interface	The box is 3G/4G-1 by default.	Choose a cellular interface (**3G/4G**-1 or **3G/4G-2**) to configure the SMS management setting.
SIM Status	N/A	Show the connoted cellular service (identified with **SIM_A** or **SIM_B**).
Delete Managed SMS after Processing	The box is unchecked by default	Check the **Enable** box to delete the received managing event SMS after it has been processed.

9.2.1.3. SMS Account List

Setup the SMS Account for managing the 6402 through the SMS. It supports up to a maximum of 5 accounts.



You can click the Add / Edit button to configure the SMS account.

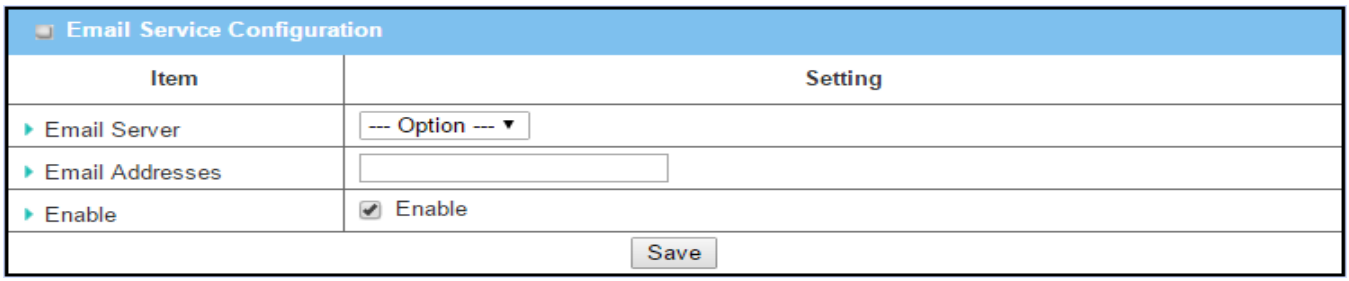


SMS Account Configuration		
Item	**Value setting**	**Description**
Phone Number	1. Mobile phone number format 2. A Mandatory Setting	Specify a mobile phone number as the SMS account identifier.
Phone Description	1. Any text 2. An Optional setting	Specify a brief description for the SMS account.
Application	A Mandatory Setting	Specify the application type. It could be **Event Trigger, Notify Handle,** or **both**.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration.

9.2.1.4. E.Mail Service List

Setup the Email Service Account for event notification. It supports up to a maximum of 5 accounts.

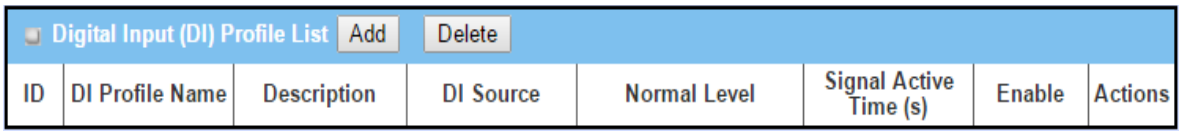
You can click the **Add / Edit** button to configure the Email account.



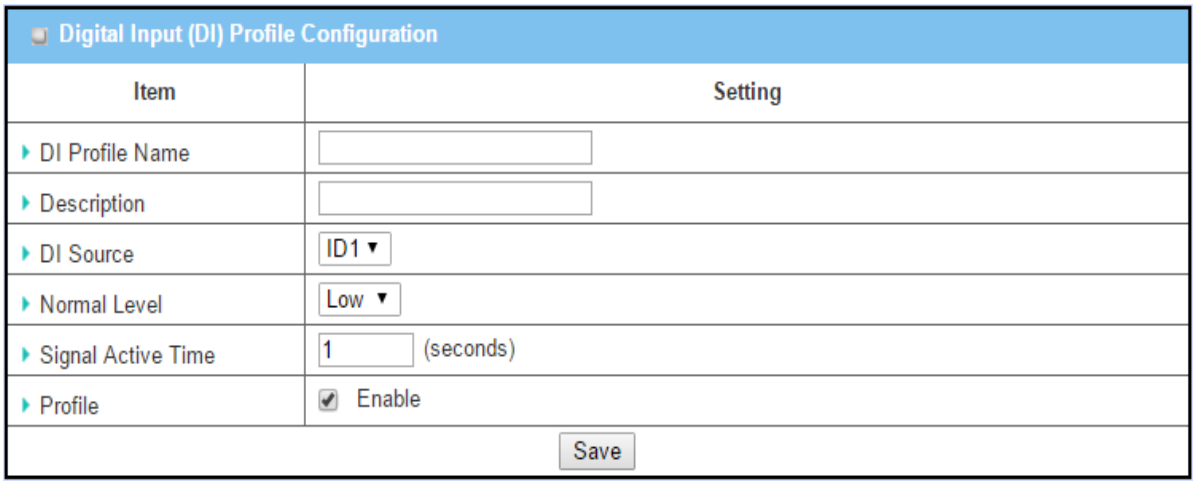
Email Service Configuration		
Item	**Value setting**	**Description**
Email Server	--- Option ---	Select an Email Server profile from **External Server** setting for the email account setting.
Email Addresses	1. Internet E-mail address format 2. Mandatory setting	Specify the Destination Email Addresses.
Enable	The box is unchecked by default.	Click **Enable** box to activate this account.
Save	*NA*	Click the **Save** button to save the configuration

Create/Edit Digital Input (DI) Profile Rule (DI/DO support required)

Setup the Digital Input (DI) Profile rules. It supports up to a maximum of 10 profiles.



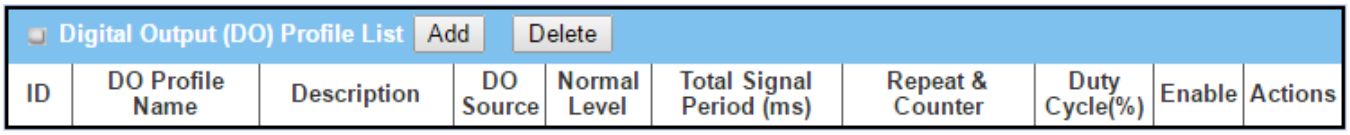
When Add button is applied, the Digital Input (DI) Profile Configuration screen will appear.



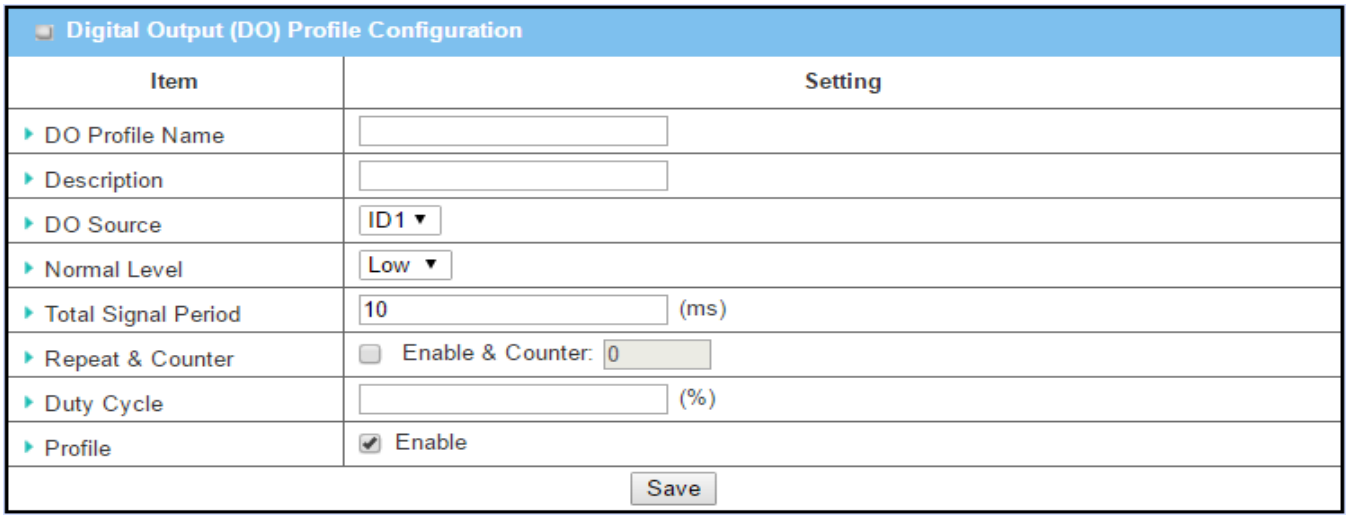
Digital Input (DI) Profile Configuration		
Item	**Value setting**	**Description**
DI Profile Name	1. String format 2. Mandatory Setting	Specify the DI Profile Name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DI Source	Digital Input 1 by default	Specify the DI Source. It could be **ID1** or **ID2**. The number of available DI source could be different for the purchased product.
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Signal Active Time	1. Numeric String format 2. Mandatory Setting	Specify the Signal Active Time. It could be from 1 to 10 seconds.
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

9.2.1.5. Digital Output (DO) Profile List

Setup the Digital Output (DO) Profile rules, the 6402 supports up to a maximum of 10 profiles.



When the Add button is applied, the Digital Output (DO) Profile Configuration screen will appear.



Digital Output (DO) Profile Configuration		
Item	**Value setting**	**Description**
DO Profile Name	1. String format 2. A Mandatory setting	Specify the DO Profile Name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
DO Source	Digital Output 1 by default	Specify the DO Source. Either DO 1 or DO 2
Normal Level	Low by default	Specify the Normal Level. It could be **Low** or **High**.
Total Signal Period	1. Numeric String format 2. A Mandatory Setting	Specify the Total Signal Period. It could be from 10 to 10000 milliseconds.
Repeat & Counter	The box is unchecked by default.	Check the Enable box to activate the repeated Digital Output, and specify the Repeat times. The Repeat Counter could be from 0 to 9999.
Duty Cycle	1. Numeric String format 2. A Must filled setting	Specify the Duty Cycle for the Digital Output. It could be from 1 to 100 %.
Profile	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration.

9.2.1.6. Modbus Notifying Events Profile List.

Setup the Modbus Notifying Events Profile, the 6402supports up to a maximum of 10 profiles.

Modbus Notifying Events Profile List Add Delete

ID	Modbus Name	Description	Read Function	Modbus Mode	IP	Port	Device ID	Register	Logic Comparator	Value	Enable	Actions
1	co2_level	read co2 level to check if it bigger than 60	Read Holding Registers (0x03)	TCP	122.22.33.44	987	78	3	>	60	☑	Edit ☐ Select

You can click the Add / Edit button to configure the profile.

Modbus Notifying Events Profile Configuration

Item	Setting
Modbus Name	
Description	
Read Function	Read Coils (0x01) ▼
Modbus Mode	Serial ▼
IP	
Port	
Device ID	
Register	
Logic Comparator	> ▼
Value	0
Enable	☑ Enable

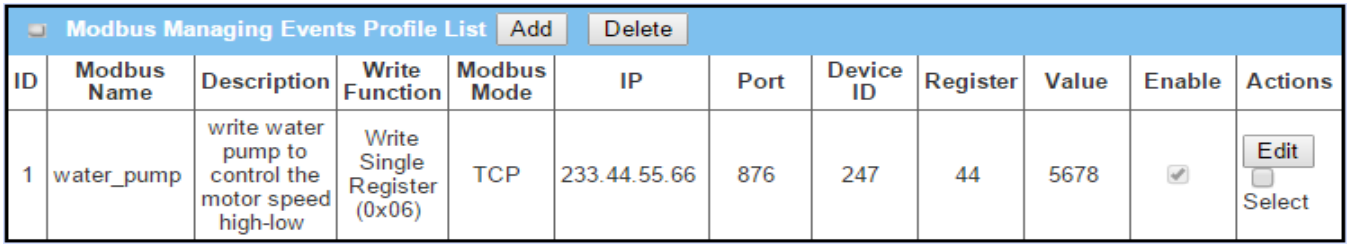
Save

Modbus Notifying Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. A Mandatory setting	Specify the Modbus profile name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Read Function	Read Holding Registers by default	Specify the Read Function for **Notifying Events**.
Modbus Mode	Serial is set by default	Specify the Modbus Mode. It can be **Serial** or **TCP**.
IP	1. NA for Serial on Modbus Mode. 2. A Mandatory Setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode. 2. A Mandatory setting for TCP on Modbus Mode.	Specify the Port for TCP on Modbus Mode. It could be from 1 to 65535.

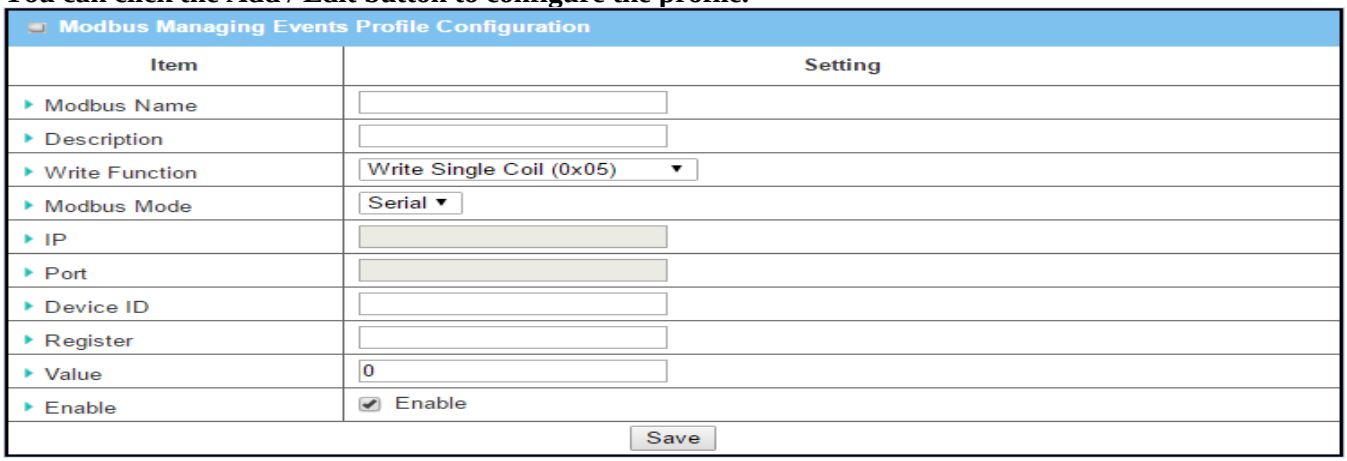
Device ID	1. Numeric String format 2. A Mandatory setting	Specify the Device ID of the Modbus device. It could be from 1 to 247.
Register	1. Numeric String format 2. A Mandatory setting	Specify the Register number of the modbus device. It could be from 0 to 65535.
Logic Comparator	Logic Comparator '>' by default.	Specify the Logic Comparator for **Notifying Events**. It could be '>', '<', '=', '>=', or '<='.
Value	1. Numeric String format 2. A Mandatory setting	Specify the Value. It could be from 0 to 65535.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

9.2.1.7. Modbus Managing Events Profile

Setup the Modbus Managing Events Profile. The 6402 supports up to a maximum of 10 profiles.



You can click the Add / Edit button to configure the profile.



Modbus Managing Events Profile		
Item	**Value setting**	**Description**
Modbus Name	1. String format 2. A Mandatory setting setting	Specify the Modbus profile name.
Description	1. Any text 2. An Optional setting	Specify a brief description for the profile.
Write Function	Write Single Registers by default	Specify the Write Function for Managing Events.
Modbus Mode	Serial by default	Specify the Modbus Mode. It could be Serial or TCP.
IP	1. NA for Serial on Modbus Mode. 2. A Mandatory setting for TCP on Modbus Mode.	Specify the IP for TCP on Modbus Mode. IPv4 Format.
Port	1. NA for Serial on Modbus Mode.	Specify the Port for TCP on Modbus Mode. 1 to

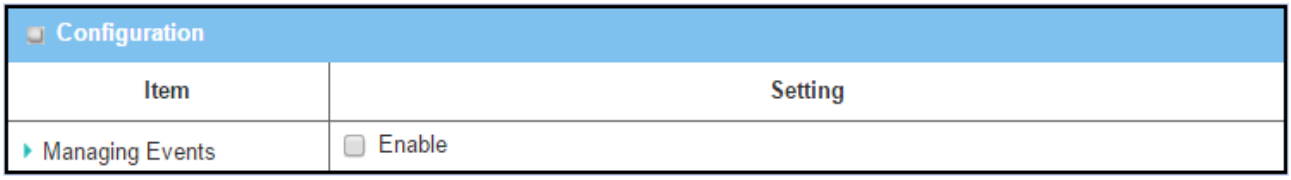
	2. A Mandatory setting for TCP in Modbus Mode.	65535.
Device ID	1. Numeric String format 2. A Mandatory setting	Specify the Device ID of the Modbus device. 1 to 247.
Register	1. Numeric String format 2. A Mandatory setting	Specify the Register number of the Modbus device. 0 to 65535.
Value	1. Numeric String format 2. A Must filled setting	Specify the Value. It could be from 0 to 65535.
Enable	The box is unchecked by default.	Click **Enable** box to activate this profile setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

9.2.2. Managing Events

9.2.2.1 Configuration

Managing Events allow administrator to define the relationship (rule) among event trigger, handlers and response.

Go to Service > Event Handling > Managing Events Tab. - Enable Managing Events

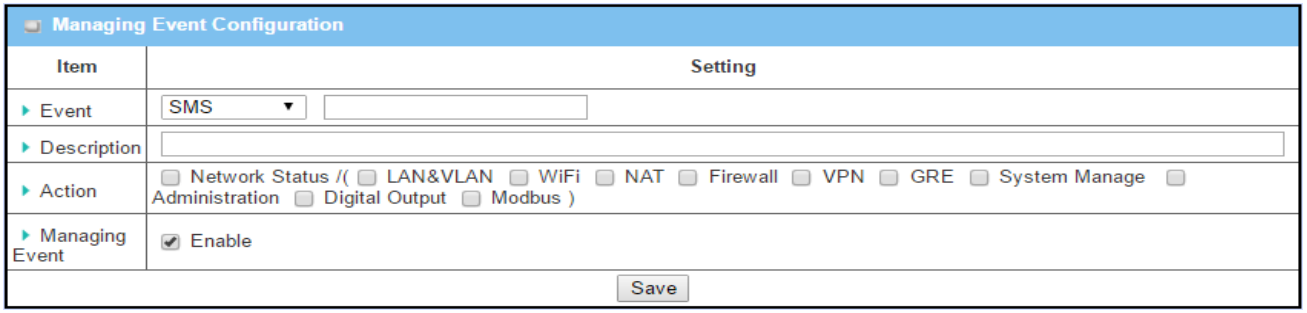


Configuration		
Item	**Value setting**	**Description**
Managing Events	The box is unchecked by default	Check the **Enable** box to activate the Managing Events function.

9.2.2.2 Create/Edit Managing Events Rules

Setup the Managing Event rules. It supports up to a maximum of 128 rules.

When the Add button is applied, the Managing Event Configuration screen will appear.



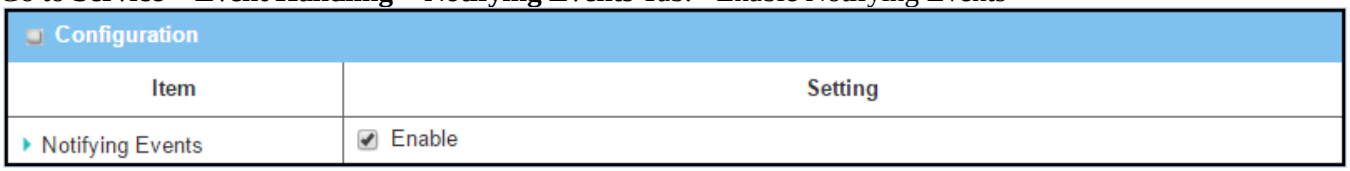
Managing Event Configuration		
Item	**Value setting**	**Description**
Event	**SMS** (or **SNMP Trap**) by default	Specify the Event type (**SMS**, **SNMP Trap**, or **DI**) and an event identifier / profile. **SMS**: Select **SMS** and fill the message in the textbox to as the trigger condition for the event; **SNMP**: Select **SNMP Trap** and fill the message in the textbox to specify SNMP Trap Event; **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event;
Description	String format : any text.	Enter a brief description for the Managing Event.
Action	Box is unchecked by default.	Specify **Network Status**, or at least one rest action to take when the expected event is triggered. **Network Status**: Select Network Status Checkbox to get the network status as the action for the event; **LAN&VLAN**: Select **LAN&VLAN** Checkbox and the interested sub-items (Port link On/Off), the gateway will to change the settings as the action for the event; **WiFi**: Select **WiFi** Checkbox and the interested sub-items (WiFi radio On/Off), the gateway will to change the settings as the action for the event; **NAT**: Select **NAT** Checkbox and the interested sub-items (Virtual Server Rule On/Off, DMZ On/Off), the gateway will to change the settings as the action for the event; **Firewall**: Select **Firewall** Checkbox and the interested sub-items (Remote Administrator Host ID On/Off), the gateway will to change the settings as the action for the event; **VPN**: Select **VPN** Checkbox and the interested sub-items (IPSec Tunnel ON/Off, PPTP Client On/Off, L2TP Client On/Off, OpenVPN Client On/Off), the gateway will to change the settings as the action for the event; **GRE**: Select **GRE** Checkbox and the interested sub-items (GRE Tunnel On/Off), the gateway will to change the settings as the action for the event; **System Manage**: Select **System Manage** Checkbox and the interested sub-items (WAN SSH Service On/Off, TR-069 On/Off), the gateway will to change the settings as the action for the event; **Administration**: Select **Administration** Checkbox and the interested sub-items (Backup Configuration, Restore Configuration, Reboot, Save Current Setting as Default), the gateway will to change the settings as the action for the event; **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **Modbus**: Select **Modbus** checkbox and a Modbus Managing Event profile you defined as the action for the event;
Managing Event	The box is unchecked by default.	Click **Enable** box to activate this Managing Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

9.2.3 Notifying Events

The Notifying Events Setting allows the 6402 network administrator to define the relationship (rule) between event triggers and handlers.

9.2.3.1 Configuration

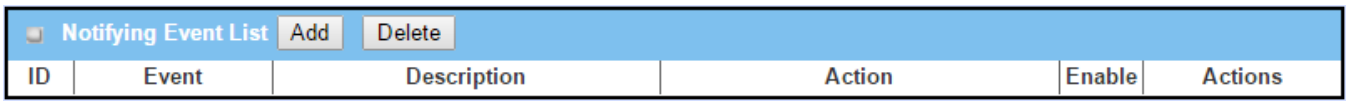
Go to **Service** > **Event Handling** > **Notifying Events** Tab. - Enable Notifying Events



Notifying Events		
Item	**Value setting**	**Description**
Notifying Events	The box is unchecked by default	Check the **Enable** box to activate the Notifying Events function.

9.2.3.2 Notifying Event List

Setup your Notifying Event rules. It supports up to a maximum of 128 rules.



Notifying Event Configuration		
Item	Default	Setting
Event	None	Digital Input-Power Change-WAN & VLAN, Wi-Fi, DDNS, Administration, Modbus, Data Usuage
	None	
	None	
Trigger Type	Period	Once (0~86,400 seconds)
Description		Free Form Field
Action		Tick one of multiple of the options – Digital Output – SMS – Syslog – SNMP Trap, Email Alert, Modbus, Remote Host
Time Schedule	Always	
Notifying Events		Tick the box to enable this feature
Save		

Amore detailed explanation is provided on the next page

.

Notifying Event Configuration		
Item	**Value setting**	**Description**
Event	**Digital Input** (or **WAN**) by default	Specify the Event type and corresponding event configuration. The supported Event Type could be: **Digital Input**: Select **Digital Input** and a DI profile you defined to specify a certain Digital Input Event; **WAN**: Select **WAN** and a trigger condition to specify a certain WAN Event; **LAN&VLAN**: Select **LAN&VLAN** and a trigger condition to specify a certain LAN&VLAN Event; **WiFi**: Select **WiFi** and a trigger condition to specify a certain WiFi Event; **DDNS**: Select **DDNS** and a trigger condition to specify a certain DDNS Event; **Administration**: Select **Administration** and a trigger condition to specify a certain Administration Event; **Modbus**: Select **Modbus** and a Modbus Notifying Event profile you defined to specify a certain Modbus Event; **Data Usage**: Select **Data Usage**, the SIM Card (Cellular Service) and a trigger condition to specify a certain Data Usage Event;.
Description	String format : any text.	Enter a brief description for the Notifying Event.
Action	All box is unchecked by default.	Specify at least one action to take when the expected event is triggered. **Digital Output**: Select **Digital Output** checkbox and a DO profile you defined as the action for the event; **SMS**: Select **SMS**, and the gateway will send out a SMS to all the defined SMS accounts as the action for the event; **Syslog**: Select **Syslog** and select/unselect the Enable Checkbox to as the action for the event; **SNMP Trap**: Select **SNMP Trap**, and the gateway will send out SNMP Trap to the defined SNMP Event Receivers as the action for the event; **Email Alert**: Select **Email Alert**, and the gateway will send out an Email to the defined Email accounts as the action for the event;
Time Schedule	**(0) Always** is selected by default	Select a time scheduling rule for the Notifying Event.
Notifying Events	The box is unchecked by default.	Click **Enable** box to activate this Notifying Event setting.
Save	*NA*	Click the **Save** button to save the configuration
Undo	*NA*	Click the **Undo** button to restore what you just configured back to the previous setting.

MODBUS Configuration can be found under Field Communication Bus and Protocol

This page left blank Intentionally

APPENDICES

10 Appendices

10.1 6402 Linux Access

Accessing the 6402 via the Console Port, Telnet or SSH will let a user access the Linux Operating System. From there the user can use standard Linux commands to change some basic settings of the 6402. It is strongly recommended that the 6402 is not configured using the Console as all changes made will be lost if/when the 6402 is powered off.

Note: Take care when using Linux commands on the 6402.

10.1.1 Accessing the Console Port

To access the Console Port connect the 6402 Console Cable to the port on the 6402 and a PC with a Terminal Emulator program. Set the Terminal Emulator to:

Baud Rate: 57600 bps, 8 Data Bits, 1 Stop Bit and no Parity.

When you have access you will be asked to login, the Login is **root** and the default password is **case**

10.1.2 Change LAN IP Address

Under some circumstances the IP address of the 6402 might be unknown and resetting the 6402 back to default settings using the Reset button and losing all of the current configuration is not an option. In instances like this it is possible to temporarily set the 6402's LAN IP address to give you access to management and from there permanently set the LAN IP address.

Access the Console Port as shown above, with access to Linux enter the following command:

ifconfig br0 x.x.x.x y.y.y.y

That is br0 with a zero.

x.x.x.x if the temporary IP Address.

y.y.y.y if the temporary Subnet Mask.

After several seconds the 6402's web GUI can be accessed using the IP Address x.x.x.x

With access ensure that the IP Address and Subnet Mask is set to the correct values.

Note: if the IP Address and Subnet Mask are not set using the GUI then their temporary values set in Linux will be lost when the 6402 is powered off.

10.2 External Server Management Authentication

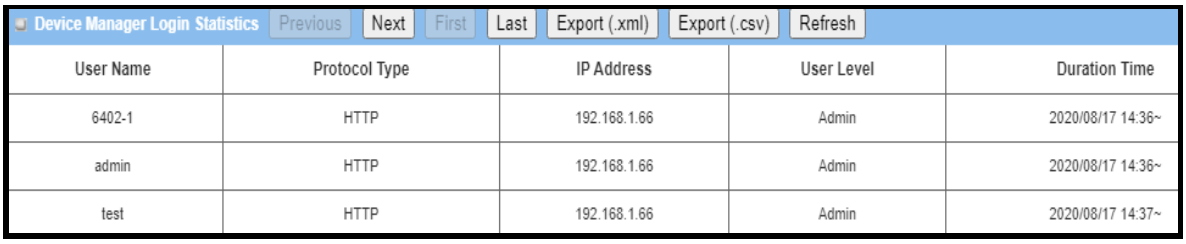
The 6402 can be configured to allow an external RADIUS or TACACS+ Server to authenticate management of the 6402 via a web browser.

The first step is to configure the primary external server, see Section **5.3 External Server** for details. A secondary external server, of the same type, can also be configured in the even if the primary server being unavailable.

The second step is to configure the 6402 to allow External Authentication, see Section **8.2.1 Password & MMI** for details.

Notes:
The Username and Password configured in the 6402 will always be authenticated no matter the status of the external servers. This will allow management in the even if the server being unavailable.

The 6402 will store details of all management access made since the last time it was powered up or rebooted. Management access will also be logged in the 6402's Syslog.
Both logs will be reset in the event of power loss or the 6402 rebooting.



User Name	Protocol Type	IP Address	User Level	Duration Time
6402-1	HTTP	192.168.1.66	Admin	2020/08/17 14:36~
admin	HTTP	192.168.1.66	Admin	2020/08/17 14:36~
test	HTTP	192.168.1.66	Admin	2020/08/17 14:37~

This page left blank intentionally

This page left blank intentionally

Technical Publications - 2022

www.casecomms.com